



Content Gateway Manager ヘルプ

Websense® Content Gateway

Websense Content Gateway オンライン ヘルプ

2012 年 5 月

R060612770

Copyright © 1996–2012 Yahoo, Inc., and Websense, Inc. All rights reserved.

本書には Yahoo, Inc および Websense, Inc の独占的情報および機密情報が含まれています。本書の内容の全部または一部を Websense, Inc の事前の書面による許可なしに第三者に開示したり、いかなる形式でも複写または複製することを禁じます。

Websense、Websense のロゴ、ThreatSeeker および YES! のロゴは、米国および/またはその他の国における Websense, Inc. の登録商標です。Websense は、米国において、および国際的に、多くの他の未登録商標を所有しています。すべての他の商標は、それぞれ該当する所有者の財産です。

本ガイドの内容の正確性については万全を期しています。しかしながら、Websense, Inc. および Yahoo, Inc. は、これを一切保証するものではなく、本製品の商品性および特定の用途に対する適合性についても同じく一切保証していません。Websense Inc. は、本ガイドまたはガイドに含まれる例の提供、性能、または使用にかかわる偶発的、副次的ないかなる損害に対しても責任を負いません。本書の情報は、通知なしに変更されることがあります。

Traffic Server は、Yahoo! Inc. の米国および他の国における商標または登録商標です。

Red Hat は Red Hat, Inc. の登録商標です。

Linux は Linus Torvalds の登録商標です。

Microsoft、Windows、Windows NT、および Active Directory は、Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Mozilla および Firefox は、Mozilla Foundation の登録商標です。

Netscape および Netscape Navigator は Netscape Communications Corporation の米国 および その他の国における登録商標です。

UNIX は、AT&T の登録商標です。

他のすべての商標は、それぞれの所有者の財産です。

制限付きの権利について

政府機関による本書に含まれる技術データの使用、複製、または開示は、DFARS 52.227-7013 の「技術データおよびコンピュータソフトウェアの権利」の項目のサブ項目 (c) (1)(ii) および FAR、DOD または NASA FAR の補足文書における同様の、または後継の条項に記載されている制限の対象となります。非公開の権利は、米国の著作権法の下で留保されています。契約業者/製造業者は、10240 Sorrento Valley Parkway, San Diego, CA 92121 を所在地とする Websense, Inc. です。

Websense Content Gateway の一部には、ライセンス契約に基づき使用された第三者の技術が含まれています。その旨の注記およびその所有権については、本マニュアルの他の箇所に掲載されています。

目次

第 1 章	概要	1
	TRITON Unified Security Center	2
	配備のオプション	3
	Web プロキシ キャッシュとして	3
	キャッシュ階層の中で	3
	管理されたクラスタの中で	4
	SSL サーバーとして	4
	DNS プロキシ キャッシュとして	5
	コンポーネント	5
	キャッシュ	5
	RAM キャッシュ	6
	Adaptive Redirection Module	6
	ホスト データベース	6
	DNS リゾルバ	7
	プロセス	7
	管理ツール	8
	プロキシ トラフィック分析の機能	8
	オンライン ヘルプ	9
	テクニカル サポート	10
第 2 章	使用開始にあたって	11
	Content Gateway Manager へのアクセス	11
	Content Gateway を二要素認証として設定する	13
	サブスクリプション キーの入力	15
	システム情報の設定	16
	プロキシがインターネット要求を処理していることの確認	16
	コマンドライン インターフェースの使用	17
	コマンド ラインでの Content Gateway の起動および停止	18
第 3 章	Web プロキシ キャッシング	21
	キャッシュ要求	21
	キャッシュされたオブジェクトの最新性の確認	22
	HTTP オブジェクトの最新性	22
	FTP オブジェクトの最新性	27
	ローカル キャッシュ コンテンツへの更新のスケジュール設定	27
	スケジュール設定した更新オプションの設定	28
	即時更新の強制	29
	キャッシュ内のコンテンツのピンニング	30
	キャッシュ ピンニング ルールの設定	30
	キャッシュ ピンニングの有効化	31

	キャッシュするか否か？	31
	HTTP オブジェクトのキャッシング	31
	クライアントの指令	31
	オリジン サーバーの指令	33
	設定の指令	36
	オブジェクト キャッシングの強制	37
	HTTP の代替のキャッシング	38
	Content Gateway が代替をキャッシュする方法の設定	38
	オブジェクトの代替の数の制限	39
	FTP オブジェクトのキャッシング	39
	HTTP 上の FTP キャッシングの無効化	40
第 4 章	明示的プロキシ	41
	手動でのブラウザの設定	41
	PAC ファイルの使用	42
	サンプルの PAC ファイル	44
	WPAD の使用	44
	明示的プロキシ環境での FTP クライアントの設定	46
	Content Gateway バージョン 7.7.0 による IPv6 のサポート	48
	IPv6 設定のまとめ	49
第 5 章	透過的プロキシと ARM	51
	ARM	52
	透過的遮断戦略	53
	レイヤー 4 スイッチによる透過的遮断	54
	WCCP v2 デバイスによる透過的遮断	55
	透過的遮断とマルチキャスト モード	71
	ポリシー ベースのルーティングによる透過的遮断	72
	ソフトウェア ベースのルーティングによる透過的遮断	73
	遮断の迂回	73
	動的バイパス ルール	74
	静的バイパス ルール	76
	現在のバイパス ルールのセットの表示	77
	接続負荷の軽減	77
	DNS ルックアップの削減	77
	IP スプーフィング	78
	IP スプーフィングとトラフィックのフロー	79
	IP スプーフィングの有効化	81
第 6 章	クラスタ	83
	管理クラスタ化	84
	SSL 管理クラスタ化	85
	SSL 管理クラスタ化の設定	86

	クラスタ構成の変更	86
	クラスタへのノードの追加	87
	クラスタからのノードの削除	89
	仮想 IP フェールオーバー	89
	仮想 IP アドレスとは?	90
	仮想 IP アドレス指定の有効化と無効化	90
	仮想 IP インターフェースの追加と編集	91
第 7 章	階層キャッシング	93
	HTTP キャッシュ階層	93
	親フェールオーバー	94
	HTTP 親キャッシュを使用する Content Gateway の構成	94
第 8 章	キャッシュの構成	97
	インストール後のキャッシュ ディスクの追加	98
	キャッシュ容量の変更	99
	キャッシュ サイズの確認	99
	キャッシュ容量の増加	99
	キャッシュ容量の削減	100
	キャッシュのパーティション区分	101
	プロトコルに対応するキャッシュ パーティションの作成	101
	パーティション サイズとプロトコルの変更	102
	オリジン サーバーまたはドメインに基づく キャッシュのパーティション区分	102
	キャッシュ オブジェクトのサイズ制限	104
	キャッシュのクリア	104
	RAM キャッシュのサイズ変更	104
第 9 章	DNS プロキシキャッシング	107
	DNS プロキシキャッシングの構成	108
第 10 章	システムの構成	111
	Content Gateway Manager	111
	設定モードの使用	111
	コマンドライン インターフェース	115
	設定ファイル	116
	構成の保存と復元	117
	構成のスナップショットを撮る	118
	構成のスナップショットの復元	118
	構成のスナップショットの削除	119
第 11 章	トラフィックのモニタリング	121
	統計の表示	121
	モニタ モードの使用	121

	コマンドラインからの統計の表示	124
	アラームの処理	125
	アラームの解除	126
	アラームを電子メール送信するように Content Gateway を構成する	127
	アラームのスクリプト ファイルの使用	127
	パフォーマンス グラフの使用	127
	SSL Manager によるレポートの作成	128
	認証機関	129
	Incidents (インシデント)	130
第 12 章	 Websense Data Security の使用	133
	Web Security Gateway での Threats ダッシュボード	133
	Websense Web Security Gateway Anywhere を使用する場合の WebDLP および Threats ダッシュボード	133
	WebDLP の仕組み	134
	Content Gateway と共にインストールされた Data Security コンポーネント	135
	ICAP を使用する Data Security	135
	Data Security の登録と構成	135
	登録と構成の詳細	137
	設定のオプション	138
	ICAP クライアントの構成	139
	ICAP フェールオーバーとロード バランシング	141
第 13 章	暗号化データの使用	145
	明示的プロキシ モードでの実行	147
	SSL Manager の有効化	149
	タスク	150
	証明書	150
	内部ルート CA	151
	ルート CA のインポート	152
	新しいルート CA の作成	152
	下位 CA の作成	153
	内部ルート CA のバックアップの作成	158
	証明書の管理	159
	証明書を確認	159
	証明書を削除	160
	証明書の許可 / 拒否ステータスの変更	160
	新しい認証機関の追加	160
	証明書のバックアップを作成	161
	証明書の復元	161
	復号化と暗号化	162

インバウンド トラフィックの場合の SSL Manager の構成	162
アウトバウンド トラフィックの場合の SSL Manager の構成	163
証明書 の 検 証	164
検 証 設 定 値 の 構 成	165
検 証 の バイパス	168
最新 の 取 り 消 し 情 報 を 保 持 す る	169
証 明 書 取 り 消 し の リ ス ト	169
Online certification status protocol (オンライン 証 明 書 ス テ ー タ ス プ ロ ト コ ル) (OCSP)	170
Web HTTPS サイト アクセス の 管 理	171
インシデント の 表 示	171
インシデント の ス テ ー タ ス の 変 更	173
インシデント の 削 除	173
メ ッ セ ー ジ の テ キ ス ト の 変 更	173
インシデント の 詳 細 の 表 示	174
インシデント リスト へ の Web サイト の 追 加	174
ク ラ イ ア ン ト 証 明 書	175
ク ラ イ ア ン ト 証 明 書 が 要 求 さ れ た 場 合	176
ク ラ イ ア ン ト 証 明 書 の イ ン ポ ー ト	176
ク ラ イ ア ン ト 証 明 書 が 常 に 要 求 さ れ た 場 合 : ホ ス ト	176
ク ラ イ ア ン ト 証 明 書 の 削 除	177
SSL Manager ロギング の 構 成	177
SSL ログ が 保 持 さ れ る 時 間	178
SSL ログ ファイル サイズ の 制 限	178
SSL アクセス ログ ファイル に 表 示 す る フ ィ ー ル ド	179
SSL 接 続 エ ラ ー メ ッ セ ー ジ の カ ス タ ム 化	180
証 明 書 検 証 フ ィ ー ル ド	180
SSL 接 続 エ ラ ー	181
第 14 章 セキュリティ	183
プロキシ へ の ク ラ イ ア ン ト アクセス の 制 御	183
Content Gateway Manager へ の アクセス の 制 御	184
管 理 者 ID お よ び パ ス ワ ー ド の 設 定	185
ユ ー ザ ー ア カ ウ ン ト の リ ス ト の 作 成	185
Content Gateway Manager へ の ホ ス ト アクセス の 制 御	186
セ キ ュ ア な 管 理 の た め の SSL の 使 用	186
FIPS 140-2 モード	187
フ ィ ル タ リ ン グ ル ー ル	188
フ ィ ル タ リ ン グ ル ー ル の 作 成	188
SOCKS ファイアウォール統合の 設 定	192
SOCKS サーバーの 設 定	193
SOCKS プロキシ オプションの 設 定	195

	SOCKS サーバー バイパスの設定.....	195
	Split DNS オプションの使用.....	196
	プロキシ ユーザー認証.....	197
	ブラウザの制約.....	199
	透過的プロキシ認証の設定.....	200
	統合 Windows 認証.....	201
	レガシー NTLM 認証.....	207
	LDAP 認証.....	210
	RADIUS 認証.....	213
	複数レルムの認証.....	216
第 15 章	ログ ファイルの使用.....	233
	イベント ログ ファイル.....	234
	イベント ログ ファイルの管理.....	235
	ログ記録ディレクトリの選択.....	235
	ログ記録スペースの管理.....	236
	イベント ログ ファイルのフォーマット.....	237
	標準フォーマットの使用.....	238
	カスタム フォーマット.....	239
	バイナリまたは ASCII の選択.....	242
	logcat によるバイナリ ログから ASCII ログへの変換.....	243
	イベント ログ ファイルの取り込み.....	244
	取り込みログ ファイルネーム フォーマット.....	245
	取り込み間隔.....	246
	ログ ファイル取り込みオプションの設定.....	247
	イベント ログ ファイルの分割.....	247
	HTTP ホスト ログ分割.....	248
	ログ分割オプションの設定.....	248
	イベント ログ ファイルの照合.....	249
	照合サーバーにするための Content Gateway の構成.....	250
	照合クライアントにするための Content Gateway の構成.....	251
	スタンドアロン照合サーバー.....	252
	ログ記録統計情報の表示.....	253
	ログ ファイルの表示.....	254
	イベント ログ ファイル エントリの例.....	255
	Squid フォーマット.....	256
	Netscape の例.....	257
付録 A	統計.....	259
	My Proxy (マイ プロキシ).....	259
	Summary (要約).....	259
	Node (ノード).....	261
	Graphs (グラフ).....	262

Alarms (アラーム)	262
Protocols (プロトコル)	263
HTTP	263
FTP	265
Security (セキュリティ)	266
Integrated Windows Authentication (統合 Windows 認証)	266
LDAP	268
Legacy NTLM (レガシー NTLM)	268
SOCKS	269
Data Security	269
Subsystems (サブシステム)	270
Cache (キャッシュ)	270
Clustering (クラスタ化)	272
Logging (ログ記録)	272
Networking (ネットワーク)	272
System (システム)	273
ARM	273
ICAP	275
WCCP	275
DNS Proxy (DNS プロキシ)	276
DNS Resolver (DNS リゾルバ)	277
Virtual IP (仮想 IP)	277
Performance (パフォーマンス)	277
SSL	280
SSL Key Data (SSL キー データ)	280
CRL Statistics (CRL 統計)	281
Reports (レポート)	281
付録 B コマンドと変数	283
Websense Content Gateway のコマンド	283
Websense Content Gateway 変数	285
統計情報	285
付録 C 設定のオプション	291
My Proxy (マイ プロキシ)	291
Basic (基本)	292
Subscription (サブスクリプション)	296
UI Setup (UI の設定)	297
Snapshots (スナップショット)	299
Logs (ログ)	301
Protocols (プロトコル)	302
HTTP	302
HTTP Responses (HTTP 応答)	311

HTTP Scheduled Update (HTTP スケジュール設定した更新)	312
HTTPS	313
FTP	314
Content Routing (コンテンツ ルーティング)	315
Hierarchies (階層)	315
Mapping and Redirection (マッピングおよびリダイレクト)	318
Browser Auto-Config (ブラウザ自動設定)	320
Security (セキュリティ)	320
Connection Control (接続の制御)	320
FIPS Security (FIPS セキュリティ)	321
Data Security	322
Access Control (アクセス制御)	323
SOCKS	334
Subsystems (サブシステム)	337
Cache (キャッシュ)	337
Logging (ログ記録)	339
Forensics Repository	343
Networking (ネットワーク)	343
Connection Management (接続管理)	344
ARM	345
WCCP	349
DNS Proxy (DNS プロキシ)	353
DNS Resolver (DNS リゾルバ)	353
ICAP	355
Virtual IP (仮想 IP)	356
SSL	357
付録 D イベントログ記録フォーマット	359
カスタム ログ記録フィールド	359
ログ記録フォーマット相互参照	362
Squid ログ記録フォーマット	363
Netscape Common ログ記録フォーマット	363
Netscape Extended ログ記録フォーマット	364
Netscape Extended-2 ログ記録フォーマット	364
付録 E 設定ファイル	367
URL 正規表現の指定 (url_regex)	367
例	369
auth.config	369
フォーマット	369
例	372
bypass.config	372
フォーマット	373

動的バイパス拒否ルール	373
例	374
cache.config	374
フォーマット	375
例	376
filter.config	377
フォーマット	378
例	379
hosting.config	380
フォーマット	381
例	381
ip_allow.config	382
フォーマット	382
例	382
ipnat.conf	383
フォーマット	383
例	383
log_hosts.config	383
フォーマット	384
例	384
logs_xml.config	385
フォーマット	385
例	390
WELF (WebTrends Enhanced Log Format)	391
mgmt_allow.config	392
フォーマット	392
例	392
parent.config	393
フォーマット	393
例	395
partition.config	396
フォーマット	396
例	397
records.config	397
フォーマット	398
例	398
設定変数	398
システム変数	400
ローカル マネージャー	402
プロセス マネージャー	405
仮想 IP マネージャー	405
アラーム設定	405

ARM	406
負荷軽減設定 (ARM)	409
認証基本レーム	410
LDAP	411
RADIUS 認証	412
NTLM	414
統合 Windows 認証	416
透過的認証	417
HTTP エンジン	418
親プロキシ設定	421
HTTP 接続タイムアウト (秒単位)	422
オリジン サーバー接続試行	424
否定応答キャッシング	425
プロキシ ユーザー変数	425
セキュリティ	427
キャッシュ コントロール	427
ヒューリスティック期限	429
ダイナミック コンテンツおよび コンテンツ ネゴシエーション	430
匿名 FTP パスワード	430
キャッシュされた FTP ドキュメントのライフタイム	431
FTP 転送モード	431
カスタムユーザー応答ページ	432
FTP エンジン	432
SOCKS プロセッサ	437
ネット サブシステム	438
クラスタ サブシステム	438
キャッシュ	439
DNS	440
DNS プロキシ	441
HostDB	442
ログ記録設定	442
URL リマップ ルール	448
スケジュール更新設定	449
SNMP の設定	450
プラグイン設定	450
WCCP の設定	450
FIPS (セキュリティ設定)	451
SSL 復号化	451
ICAP	453
Data Security	455
接続性、分析、および境界条件	455
remap.config	458

	フォーマット	458
	例	459
	socks.config	460
	フォーマット	460
	例	461
	socks_server.config	461
	フォーマット	461
	例:	462
	splitdns.config	462
	フォーマット	463
	例	463
	storage.config	464
	フォーマット	464
	update.config	465
	フォーマット	466
	例	466
	wccp.config	467
付録 F	エラー メッセージ	469
	Websense Content Gateway のエラー メッセージ	469
	処理の致命的エラー	469
	警告	470
	アラーム メッセージ	471
	クライアントに送信される HTML メッセージ	474
	標準 HTTP 応答メッセージ	477
付録 G	req_ca.cnf ファイル	479
付録 H	FAQ およびトラブルシューティングのヒント	481
	よく寄せられる質問 (FAQ)	481
	ディスク IO エラーはキャッシュにどのような影響を与えますか、 また、キャッシュ ディスクに障害が発生した場合 Content Gateway は何をしますか	482
	Content Gateway が大きなオブジェクトをダウンロード しているときにクライアントが切断した場合、 キャッシュにオブジェクトの一部が保存されますか	482
	Content Gateway は、Java アプレット、JavaScript プログラム、 またはそのほかの VBScript などのアプリケーション ファイルを キャッシュできますか	482
	マスタ管理者パスワードを忘れた場合に Content Gateway Manager にどのようにアクセスしますか ..	482
	logs.xml.config ファイルへの変更をクラスタ内の すべてのノードにどのように適用しますか	483
	Squid 形式および Netscape 形式のログ ファイルの	

キャッシュ戻り値は何を意味しますか.....	484
cqtx フィールドはカスタム ログ ファイルに 何を記録するのですか	485
Content Gateway はホスト データベース内のエントリが 一定期間使用されていない場合に、 それらのエントリを更新しますか.....	485
イメージ、動画 gif、および Java アプレットを使用して カスタム応答の外観を改善できますか.....	486
Content Gateway が透過的要求のみを処理するように 設定するにはどうすればよいですか.....	486
トラブルシューティングのヒント	488
Content Gateway Manager でスループット統計が不正確	488
Content Gateway コマンドを実行することができません.....	488
1 つのノードがクラスタ内の他のノードからオブジェクトを 取得するときに矛盾した動作が行われる.....	489
Web ブラウザがデータ欠落メッセージを示すエラー ドキュメントを表示することがある.....	489
Content Gateway がどんな Web サイトも解決しない	490
システム ログ ファイルでの最大ドキュメント サイズ 超過メッセージ	491
システム ログ ファイルでの DrainIncomingChannel メッセージ.....	491
システム ログ ファイルの cop ファイル メッセージがない.....	491
vaddrs.config の編集時のシステム ログ ファイルでの警告 (Linux).....	492
always_query_destination を有効化した後、 非透過的要求が失敗する	492
Content Gateway は実行しているが、 ログ ファイルが作成されない.....	493
Content Gateway エラーがネットワーク接続が 多すぎることを示す	493
低メモリの兆候	494
オリジン サーバーとの接続タイム アウト	495
IBM Web サーバーが Content Gateway で機能しない	495
Content Gateway が起動（または停止）しない	495
付録 I 用語集	497
付録 J 著作権	503
索引	507

1

概要

Websense® Content Gateway は、Websense Web Security Gateway および Websense Web Security Gateway Anywhere ソリューションの Web プロキシ コンポーネントです。

Content Gateway は、設定可能な高性能の Web プロキシであり、Websense Web Security と組み合わせて使用し、コンテンツがプロキシを通過するときに、必要に応じて、詳細なコンテンツ分析を正確に実行し、分析結果に基づき適切な Web Security ポリシーを適用することによって、不正で望ましくないコンテンツからユーザーおよびネットワークを保護します。このオンデマンドの分析は、ユーザーとネットワークを保護すると同時に、動的な Web 2.0 サイトを組織およびユーザーにとって安全にします。

コンテンツ分析の正確な適用は、各 Web Security Gateway (Anywhere) 環境の管理者によって設定されます。

Web プロキシ キャッシュ：Content Gateway はまた、頻繁にアクセスされる情報をネットワークの端にキャッシュしておくことによってネットワークの効率および処理能力を改善する高性能の Web プロキシ キャッシュとして機能するように構成することもできます。これによってコンテンツは物理的にエンドユーザーの近くに置かれ、迅速に配信でき、帯域幅の使用を減らすことができます。

Content Gateway は、下記のいずれかとして配備できます。

- ◆ *Web プロキシ キャッシュとして*
- ◆ *キャッシュ階層の中で*
- ◆ *管理されたクラスタの中で*
- ◆ *SSL サーバーとして*
- ◆ *DNS プロキシ キャッシュとして*

さらに、Content Gateway は、下記のようなセキュリティ機能を実行するように設定できます。

- ◆ プロキシへのクライアント アクセスを制御する。
- ◆ 名前解決の対象のホストがファイアウォールの内側か外側かによって、異なる DNS サーバーを使用する。これによって、社内ネットワーク構成を保護し、同時にインターネット上の外部サイトへの透過的アクセスを提供します。

- ◆ クライアントがコンテンツにアクセスする前に、必ず認証が行われるようにする。Content Gateway は、統合 Windows 認証、レガシー NTLM (NTLMSSP)、LDAP、および RADIUS をサポートします。
- ◆ インストールされている Data Security ポリシー エンジンまたは ICAP インターフェースを使用して、Websense Data Security を使用するサイトが Web ポスティングなどのアウトバウンド マテリアルを検査し、企業のポリシーに基づいてブロックまたは許可できるようにする。[Websense Data Security の使用, 133 ページ](#) を参照してください。
- ◆ 下記のどちらかの方法で Content Gateway Manager へのアクセスを制御する。
 - 暗号化され、認証されたアクセスの場合は、SSL(Secure Sockets Layer) 保護
 - ユーザー アカウントによって、どのユーザーが Content Gateway Manager にアクセスできるか、およびそれらのユーザーがどのアクティビティ (例、「統計の表示のみ」、「統計の表示と Content Gateway の設定」) を実行できるかを指定する。
- ◆ ユーザーのファイアウォールに統合し、SOCKS サーバーを通じてトラフィックを制御する。

[セキュリティ, 183 ページ](#) を参照してください。

関連項目：

- ◆ [TRITON Unified Security Center, 2 ページ](#)
- ◆ [配備のオプション, 3 ページ](#)
- ◆ [コンポーネント, 5 ページ](#)
- ◆ [プロキシトラフィック分析の機能, 8 ページ](#)
- ◆ [オンライン ヘルプ, 9 ページ](#)
- ◆ [テクニカル サポート, 10 ページ](#)

TRITON Unified Security Center

TRITON Unified Security Center は、TRITON Web Security、Data Security、および Email Security モジュールのための集中化された設定および管理コンソールです。これはまた、登録されている V シリーズ アプライアンスへのアクセスを提供します。

インストール時に、TRITON Unified Security Center は、1 つの管理者アカウント **admin** に対して、すべての TRITON モジュールおよび TRITON の設定への完全なアクセスを許可するように構成されます。このアカウントのパスワードは、インストール時に設定されます。

TRITON – Web Security セクションを使用して、Web セキュリティの動作を設定し、インターネット使用状況をモニタし、インターネット使用状況レポートを生成し、Websense Web Security の設定を管理します。[Settings (設定)]>

[Content Gateway Access (Content Gateway アクセス)] 画面を使用して、Content Gateway のインスタンスを登録できます。登録されているインスタンスにはシステム状態のインディケータが表示され、ポータル上の Content Gateway Manager ログへのリンクが提供されます。

TRITON Unified Security Center の詳細について知るには、TRITON Unified Security Center を開き、ヘルプ システムにアクセスしてください。

Websense Web Security での Content Gateway Manager の登録およびアクセスの詳細について知るには、TRITON Unified Security Center を開き、Web Security モジュールにアクセスし、[Help (ヘルプ)] をクリックしてください。

配備のオプション

Web プロキシ キャッシュとして

Content Gateway が Web プロキシ キャッシュとして配備されているとき、ユーザーによる Web コンテンツ要求は、宛先 Web サーバー（オリジン サーバー）への転送の途中で Content Gateway を通過します。Content Gateway キャッシュが要求されたコンテンツを含んでいる場合は、Content Gateway はそのコンテンツを直接に提供します。Content Gateway キャッシュが要求されたコンテンツを含んでいない場合は、Content Gateway はプロキシとして動作し、ユーザーのためにオリジン サーバーからコンテンツを取得し、将来の要求に対応できるようにコピーを保持します。

Content Gateway は、一般的には、下記のどちらかの方法でクライアントの要求を受信するように配備されます。

- ◆ **明示的プロキシ**として。この場合、ユーザーのブラウザまたはクライアント ソフトウェアは要求を直接に Content Gateway に送信するように設定されます。[明示的プロキシ, 41 ページ](#) を参照してください。
- ◆ **透過的プロキシ**として。この場合、ユーザーの要求は、宛先サーバーへの転送の途中で、透過的に Content Gateway にルーティングされます。ユーザーは通常の方法でインターネット コンテンツを要求し（ブラウザ側での設定なしに）、Content Gateway はそれらの要求を処理します。ユーザーのクライアント ソフトウェア（一般的にはブラウザ）は、プロキシと通信していることを認識しません。[透過的プロキシと ARM, 51 ページ](#) を参照してください。

キャッシュ階層の中で

Websense Content Gateway を柔軟なキャッシュ階層に組み込むことができます。そこでは、あるキャッシュで処理されなかったインターネット要求を、他のリージョナル キャッシュにルーティングでき、そのキャッシュのコンテンツと、要求元からの近接性を活用することができます。プロキシ サーバー階層内では、Content Gateway は、他の Content Gateway サーバーまたは他の

キャッシング サーバーの親または子として機能することができます。[階層キャッシング](#), [93 ページ](#) を参照してください。

管理されたクラスタの中で

Websense Content Gateway は、単一ノードから複数ノードに拡張でき、管理されたクラスタを形成することによって、システムの容量、パフォーマンス、および信頼性を高めます。

- ◆ 管理されたクラスタは、ノードの追加および削除を検出します。
- ◆ クラスタ ノードは、自動的に設定情報を共有し、それによってクラスタのメンバーをすべて同時に管理できます。
- ◆ SSL Manager が有効化されているとき、SSL 設定情報もクラスタ全体に適用されます。しかし、情報の同期化に使用するメカニズムは、他の情報の場合と違います。

仮想 IP フェールオーバー オプションが有効化されている場合、Content Gateway はクラスタのノードに割り当てる仮想 IP アドレスのプールを維持します。Content Gateway は、ノードの故障（電源または CPU 障害など）を検出し、故障したノードの IP アドレスを正常なノードに再割り当てします。詳細については、[仮想 IP フェールオーバー](#), [89 ページ](#) を参照してください。

Content Gateway が WCCP を備えた透過的プロキシとして構成されている場合、フェールオーバーは WCCP によって処理され、仮想 IP フェールオーバーは使用できません。[WCCP の負荷配分](#), [57 ページ](#) を参照してください。

詳細については、[クラスタ](#), [83 ページ](#) を参照してください。

SSL サーバーとして

SSL Manager が有効化されている場合、HTTPS データは復号化され、検査され、次に、クライアントとオリジン サーバーの間で転送される時に再-暗号化されます。

Content Gateway は HTTPS データをキャッシュしません。

SSL Manager は、認証処理機能の完全なセットを含んでいます。[暗号化データの使用, 145 ページ](#) を参照してください。



重要

SSL Manager が有効化されておらず、HTTPS が復号化されていないときでも、Content Gateway は HTTPS URL フィルタリングを実行します。つまり、各 HTTPS 要求に対して、URL ルックアップが実行され、ポリシーが適用されます。

明示的プロキシモードでは、SLL がオフにされたとき、Content Gateway は要求内のホスト名に基づき URL フィルタリングを実行します。サイトがブロックされている場合、Content Gateway はブロックページを提供します。一部のブラウザは、ブロックページの表示をサポートしません。この機能を無効にするには、クライアントがプロキシに HTTPS 要求を送信しないように設定します。

透過的プロキシモードでは、SLL がオフにされたとき、Content Gateway は、オリジンサーバーからの認証の中の共通名に基づき URL フィルタリングを実行します。サイトがブロックされている場合、クライアントとの接続が失われます。ブロックページは提供されません。WCCP と共に使用しているときこの機能を無効にするには、HTTPS のサービスグループを作成しないでください。

DNS プロキシ キャッシュとして

DNS プロキシ キャッシュとして、Content Gateway はクライアントの DNS 要求を解決できます。これによって、リモート DNS サーバーの負荷を減らし、DNS ルックアップの応答時間を短縮します。[DNS プロキシ キャッシング, 107 ページ](#) を参照してください。

コンポーネント

キャッシュ

キャッシュは、オブジェクトストアと呼ばれる高速オブジェクトデータベースから成ります。オブジェクトストアは、URL および関連付けられているヘッダに従ってオブジェクトにインデックスを付けます。オブジェクトストアは、同じオブジェクトの代替バージョン（言語または暗号化タイプが異なる）をキャッシュすることができ、また大小のドキュメントを保存でき、無駄なスペースを最小限にします。キャッシュがいっぱいになったとき、プロキシは陳腐化したデータを削除し、頻繁に要求されるオブジェクトが最新の状態であるようにします。

Content Gateway は、キャッシュ ディスク上のディスク障害を許容します。ディスクが完全に壊れた場合、Content Gateway はそのディスクに「破損」を表すマークを付け、残りのディスクを引き続き使用します。すべてのキャッシュ ディスクが機能しなくなった場合、Content Gateway はプロキシ専用モードに移行します。

キャッシュをパーティションで区切って、ディスク スペースを特定のプロトコルおよびオリジン サーバーのデータの保存用に予約することができます。[キャッシュの構成, 97 ページ](#) を参照してください。

RAM キャッシュ

Content Gateway は、非常によくアクセスされるオブジェクトの小さな RAM メモリ キャッシュを保持します。この RAM キャッシュは、最もよくアクセスされるオブジェクトをすばやく提供し、ディスクの負荷を減らします（特にトラフィック ピーク時に）。RAM キャッシュ サイズは設定可能です。[RAM キャッシュのサイズ変更, 104 ページ](#) を参照してください。

Adaptive Redirection Module

Adaptive Redirection Module (ARM) は、いくつかの重要な機能を提供します。1 つは、クラスタ通信インターフェース フェールオーバーのデバイス通知を送信する機能です。もう 1 つは、着信パケットを、IP レイヤーがそれを受け取る前に検査し、パケットを Content Gateway で処理するようにアドレス変更する機能です。

ARM は常にアクティブです。

ユーザーの要求をプロキシにリダイレクトするために、ARM は着信パケットのアドレスを変更します。パケットの宛先 IP アドレスはプロキシの IP アドレスに変更され、パケットの宛先ポートは使用されているプロトコルに応じて変更されます。たとえば、HTTP の場合、パケットの宛先ポートはプロキシの HTTP ポート（通常は 8080）に変更されます。

ARM は、プロキシ キャッシュで適切に処理できないサイトの自動バイパスをサポートします。

ARM はまた、クライアント要求の過負荷を防止します。クライアント接続の数が指定されている限度を超えたとき、ARM は着信した要求を直接にオリジン サーバーに転送します。[接続負荷の軽減, 77 ページ](#) を参照してください。

ホスト データベース

ホスト データベースは、プロキシが接続するオリジン サーバーの Domain Name Server (DNS) エントリを保存します。ホスト データベースは特に、以下の情報を追跡します。

- ◆ DNS 情報（ホスト名を IP アドレスにすばやく変換するため）
- ◆ 各ホストの HTTP バージョン（最新のプロトコル機能を、種々のサーバーを実行しているホストで使用できるようにするため）

- ◆ ホストの信頼性および可用性情報（機能していないサーバーからの応答待ちを避けるため）

DNS リゾルバ

透過的プロキシ環境では、プロキシは非同期 DNS リゾルバを含み、それによってホスト名の IP アドレスへの変換を簡素化します。Content Gateway は、DNS リゾルバをそのまま実装し、リゾルバのライブラリを利用せずに直接に DNS コマンド パケットを発行します。多くの DNS クエリーを同時に発行でき、また、高速 DNS キャッシュはよく使用するバインドをメモリに保持し、DNS トラフィックを削減します。



重要

Linux システムの DNS サーバの設定を変更した場合 (/etc/resolv.conf)、Content Gateway を再起動する必要があります。

プロセス

Content Gateway には 5 つの基本的なプロセスがあります。

プロセス名	説明
content_gateway	接続を受け入れ、プロトコル要求を処理し、キャッシュまたはオリジン サーバーからのドキュメントを提供します。
content_manager	content_gateway プロセスを開始、モニタ、および設定します。 content_manager プロセスはまた、Content Gateway Manager のユーザー インターフェース、プロキシ自動設定ポート、統計インターフェース、クラスタ管理、仮想 IP フェールオーバーを処理します。 content_manager プロセスは、 content_gateway プロセスの失敗を検出した場合、このプロセスを再起動し、また、すべての着信要求の接続キューを保持します。サーバーが再起動するまでの数秒間に着信した着信接続は接続キューに保存され、順に処理されます。この接続キューは、ユーザーをサーバーの再起動によるダウンタイムから保護します。
content_cop	content_gateway および content_manager の状態をモニタします。 content_cop プロセスは、定期的に（1分に数回） content_gateway および content_manager の状態を問い合わせるために、ハートビート要求を発行して合成 Web ページを取得します。タイムアウト時間内に応答を受け取らなかった場合、または不適切な応答を受け取った場合、 content_cop は、 content_manager および content_gateway を再起動します。
analytics_server	Content Classification Analytics のために発行された要求および生成されたプロセスを管理します。
download_service	定期的に行って、Websense Database Download Service で更新をチェックします。

管理ツール

関連項目：

- ◆ [Content Gateway Manager, 111 ページ](#)
- ◆ [コマンドライン インターフェース, 115 ページ](#)
- ◆ [設定ファイル, 116 ページ](#)

Websense Content Gateway は 3 つの管理モードを備えています。

- ◆ *Content Gateway Manager* は、ブラウザを通じてアクセス可能な Web ベースのインターフェースです。Content Gateway Manager は、Content Gateway のパフォーマンスとネットワークトラフィックをモニタするためのグラフおよび統計表示、およびプロキシの設定と微調整のためのオプションを備えています。Content Gateway Manager は、Content Gateway クラスタ全体に対して、パスワード保護され、SSL 暗号化された、シングルポイント管理を提供します。これは推奨する管理モードです。
- ◆ コマンドライン インターフェースによって、Content Gateway のパフォーマンスとネットワークトラフィックをモニタし、プロキシを設定できます。個別のコマンドを実行するか、またはシェルの中に一連のコマンドを記述することができます。この方法は、Content Gateway が Websense アプライアンス上にインストールされているときには、部分的にのみ利用できます。代わりに、Content Gateway Manager と Appliance Manager Command Line Utility を使用します。
- ◆ *設定ファイル*によって、ファイル編集およびシグナル処理インターフェースを通じた管理が可能になります。Content Gateway Manager またはコマンドライン インターフェースを使う代わりに、設定ファイルを編集することによって設定オプションを変更できます。Content Gateway Manager またはコマンドライン インターフェースを通じて行った変更は自動的に設定ファイルに反映されます。

プロキシ トラフィック分析の機能

Content Gateway は、ネットワークトラフィック分析およびモニタのための下記のオプションを提供します。

- ◆ *Manager 統計およびグラフ*は、ネットワークトラフィック情報を表示します。Content Gateway Manager からのグラフおよび統計を表示するか、またはコマンドライン インターフェースを使用して統計を収集し、処理します。
- ◆ 種々のパフォーマンスグラフは、仮想メモリ使用量、クライアント接続、ドキュメントのヒット率などに関する履歴情報を示します。パフォーマンスグラフを Content Gateway Manager に表示します。
- ◆ *Manager のアラーム*は、Content Gateway Manager に表示されます。Content Gateway は、検出したエラー条件に関するアラームを生成しま

す。アラームが発生したときサポート担当者に電子メールまたはページを送信するように Content Gateway を設定できます。

Content Gateway はまた、いくつかのアラームを TRITON - Web Security に送信します。そこではそれらはアラートと呼ばれます。要約アラートメッセージが TRITON - Web Security 「Status (ステータス)」 > 「Today (本日)」 ページに表示されます。完全なアラートメッセージは、「Alerts (アラート)」 ページに表示されます。TRITON - Web Security 管理者は、Content Gateway のどのような状態でアラートメッセージを生成するか、およびどのような方法でアラートを送信するか (電子メールまたは SNMP) を設定できます。

- ◆ トランザクション ロギングによって、プロキシが受け取る各要求およびプロキシが検出する各エラーに関してログ ファイルに情報を記録できます。ログを使用して、何人のユーザーがプロキシを使用し、各ユーザーがどのぐらいの量の情報を要求したか、また、どのページが最も人気があるかを判断します。トランザクションでエラーが発生した理由と、その時点でのプロキシ キャッシュの状態を確認できます。たとえば、Content Gateway が再起動したこと、またはクラスタ通信がタイムアウトになったことを確認できます。

Content Gateway はいくつかの標準ログ ファイル フォーマット (例、Squid、Netscape) および独自のカスタム フォーマットをサポートします。標準フォーマットのログ ファイルを既製の分析パッケージを使って分析できます。ログ ファイルを分割して、プロトコルまたはホストに固有の情報を含むようにしておくと、ログ ファイルの分析が容易になります。

トラフィック分析のオプションについては、[トラフィックのモニタリング, 121 ページ](#) を参照してください。ロギングのオプションについては、[ログ ファイルの使用, 233 ページ](#) を参照してください。

オンライン ヘルプ

Content Gateway Manager のどのページからでも、**[Get Help! (ヘルプを表示)]** をクリックすると、製品の使用に関する詳細な情報が表示されます。



重要

Microsoft Internet Explorer のデフォルト設定によって、ヘルプ システムの操作がブロックされている場合があります。セキュリティ アラートが表示された場合、[Help (ヘルプ)] を表示するには、**[Allow Blocked Content (ブロックされているコンテンツを許可)]** を選択します。

組織のセキュリティ標準によって許可されている場合、「Tools (ツール)」 > 「Internet Options (インターネット オプション)」 インターフェースの [Advanced (詳細設定)] タブで警告メッセージを永久に無効にすることができます ([Security (セキュリティ)] オプションの下の **[Allow active content to run in files on My Computer (マイコンピュータのファイルでのアクティブ コンテンツの実行を許可する)]** をオンにします)。

オンライン ヘルプの PDF バージョンにアクセスするか、または[リリースノート](#)、インストールおよび配備情報、FAQ、ヒント、および他の技術情報にアクセスするには、[Websense Technical Library](#) にアクセスします。

テクニカル サポート

Websense 製品に関する技術情報は、1 日 24 時間、下記のオンラインで入手できます：

<http://support.websense.com>

サポート サイトでは下記の情報を参照できます。

- ◆ ヒント
- ◆ カスタマ フォーラム
- ◆ 最新のリリース情報
- ◆ 検索可能な Websense Knowledge Base
- ◆ 最新のホットフィックスおよびパッチ
- ◆ Show-me チュートリアルとビデオ
- ◆ 製品マニュアル
- ◆ テクニカル ライブラリ
- ◆ よくある質問に対する回答
- ◆ 詳細な技術ペーパー
- ◆ 月別サポート ウェビナー
- ◆ テクニカル アラート
- ◆ 最も一般的なソリューション

Websense Support サイトは、Service Request ポータルを通じた「ケースの開始」を含む、すべてのテクニカル リソースへのアクセスを提供します。

2

使用開始にあたって

Content Gateway をシステムまたはクラスタ内のすべてのノードにインストールした後、プロキシは使用できる状態になります。

使用を開始するには下記の手順を参照してください。

- ◆ [Content Gateway Manager へのアクセス](#), 11 ページ
- ◆ [サブスクリプション キーの入力](#), 15 ページ
- ◆ [プロキシがインターネット要求を処理していることの確認](#), 16 ページ
- ◆ [コマンドライン インターフェースの使用](#), 17 ページ
- ◆ [コマンドラインでの Content Gateway の起動および停止](#), 18 ページ

Content Gateway Manager へのアクセス

Content Gateway Manager は、Content Gateway の管理コンソールです。

Content Gateway Manager は、下記のブラウザでサポートされています。

- ◆ Microsoft Internet Explorer 8 および 9
- ◆ Mozilla Firefox バージョン 5 以上
- ◆ Google Chrome 13 以上

他のブラウザおよびバージョンを使用すると予期しない動作を引き起こすことがあります。

Java および JavaScript は、ご使用のブラウザで有効化する必要があります。Java および JavaScript の有効化に関する詳細は、ご使用のブラウザのマニュアルを参照してください。

Content Gateway Manager にアクセスするには 3 つの方法があります。

- ◆ TRITON-Web Security の [Content Gateway] ボタンから。* TRITON - Web Security からのアクセスの設定については、TRITON - Web Security Help を参照してください。
- ◆ ブラウザで Content Gateway ホスト システムの IP アドレスおよびポートを入力する。下記を参照。
- ◆ Content Gateway が V シリーズ アプライアンスのモジュールである場合、V シリーズ Logon ポータルを開き、[Content Gateway] をクリックします。

*TRITON Unified Security Center で二要素認証（証明書認証）が設定されている場合、唯一の方法は、TRITON - Web Security シングル サイオンを通じて Content Gateway Manager にアクセスすることです。[Content Gateway を二要素認証として設定する, 13 ページ](#) を参照してください。



ご注意

シングル サイオンを使用しているとき、Content Gateway IP アドレス上にポップ-アップできるようにブラウザを設定する必要があります。

Content Gateway Manager に直接にアクセスするには、下記の手順を実行します。

1. Web ブラウザを開きます。
2. ブラウザで下記の場所を入力します。

`https://nodename:adminport`

ここで、*nodename* は IP アドレス、*adminport* は Content Gateway Manager に割り当てられたポート番号です（デフォルト：8081）。

Content Gateway Manager を起動するための HTTP の使用方法の詳細については、[セキュアな管理のための SSL の使用, 186 ページ](#) を参照してください。

3. 管理者 ID（デフォルト：admin）およびパスワード、またはユーザー アカウントを使用して Content Gateway Manager にログオンします。

Content Gateway Manager のパスワードはインストール時に設定されます。

ID およびパスワードを変更でき、またユーザー アカウントも作成および変更できます。[Content Gateway Manager へのアクセスの制御, 184 ページ](#) を参照してください。

Content Gateway Manager は、「**Monitor（モニタ）**」>「**My Proxy（マイ プロキシ）**」>「**Summary（要約）**」ページに開きます。このページは、サブスクリプションの機能および Content Gateway システムの詳細に関する情報を表示します。[Monitor（モニタ）] タブの詳細については、[統計の表示, 121 ページ](#) を参照してください。また Content Gateway Manager の設定オプションの詳細については、[システムの構成, 111 ページ](#) を参照してください。

セキュリティ証明書アラート

Content Gateway Manager とのセキュアなブラウザ ベースの通信のために、SSL 接続 が使用されます。この接続は、Websense, Inc. が発行するセキュリティ証明書を使用します。対応しているブラウザは Websense, Inc. を既知の Certificate Authority として認識しないので、新しいブラウザから Content Gateway Manager を最初に起動するとき証明書エラーが表示されます。このエラーを避けるためには、ブラウザ内にその証明書をインストールするか、

またはその証明書を「今後も受け入れる」ように設定します。詳細についてはご使用のブラウザのマニュアルを参照してください。



ご注意

Internet Explorer を使用している場合、その証明書を受け入れてからも証明書エラーが表示されます。このエラーメッセージを消去するには、ブラウザをいったん閉じて、再度開きます。

Windows 7 の考慮事項

Windows 7 オペレーティングシステムを使用している場合は、管理者としてブラウザを開いて、ActiveX コントロールを許可しなければなりません。

1. ブラウザ アプリケーションを右クリックし、[Run as administrator (管理者として実行)] を選択します。
2. Content Gateway Manager にログオンし、上の説明のようにセキュリティ証明書を受け入れます。

Content Gateway を二要素認証として設定する

二要素認証 (証明書認証) :

- ◆ TRITON Unified Security Center ログオンのみ設定され適用します。
- ◆ 管理者にログオン時に 2 つの形式の ID を提供することを要求します。
- ◆ 管理者が Content Gateway Manager にアクセスの前に TRITON Unified Security Center にログオンするよう強制することによって、Content Gateway Manager に適用させることができます。
- ◆ Content Gateway Manager へのアクセスを許可された管理者のためにシングルサインオンを設定することを要求します。
- ◆ Content Gateway でパスワード ログオン機能を無効化することを要求します。それによって、シングルサインオンが設定されていない管理者が Content Gateway Manager にアクセスするのを防止します。Content Gateway をアプライアンスに配備している場合、パスワードアクセスは Appliance Manager コマンドを使って無効化されます。V シリーズ Appliance Manager ヘルプを参照してください。

二要素認証の設定の詳細については、TRITON コンソール オンライン ヘルプの「証明書認証の設定」を参照してください。

Content Gateway パスワード ログオンの無効化および有効化

Content Gateway Manager パスワード ログオンを無効化することによって TRITON コンソールからの二要素認証またはシングル サインオン アクセスのみを許可することができます。



ご注意

Content Gateway が Websense アプライアンス上にインストールされている場合は、詳細については Appliance Manager を参照してください。

アプライアンスのパスワード ログオンを無効化するには、下記の手順を実行します。

1. TRITON – Web Security でシングル サインオンを設定します。
2. 二要素認証を使用する場合は、TRITON Unified Security Center で二要素認証を設定します。
3. Content Gateway ホスト システムにログオンし、ルート権限を取得します。
4. ディレクトリを “/etc” に変更し、“websense” サブディレクトリがあるかどうか確認します。ない場合は、“websense” サブディレクトリ (“mkdir websense”) を作成します。
5. ディレクトリを “websense” (パスは現在 “/etc/websense”) に変更し、ファイル “password-logon.conf” があるかどうか確認します。
6. ない場合は、そのファイル (“touch password-logon.conf”) を作成します。
7. “password-logon.conf” を編集します。
8. 行を追加するか、または既存の行を下記の通りに変更します。

```
password-logon=disabled
```
9. ファイルを保存し、終了します。

変更はすぐに有効になります。Content Gateway を再起動する必要はありません。

すべての管理者のパスワード ログオンを再有効化するには、下記の手順を実行します。

1. Content Gateway ホスト システムにログオンし、ルート権限を取得します。
2. ディレクトリを “/etc/websense” に変更します。
3. “password-logon.conf” を編集し、下記の通りに変更します。

```
password-logon=disabled
```

を下記のように変更します。

```
password-logon=enabled
```
4. ファイルを保存し、終了します。

変更はすぐに有効になります。Content Gateway を再起動する必要はありません。

サブスクリプション キーの入力

関連項目：

- ◆ [システム情報の設定, 16 ページ](#)

Content Gateway が Web Security Gateway または Web Security Gateway Anywhere と共に配備されている場合、Content Gateway Manager でサブスクリプション キーを入力する必要はありません。キーは、TRITON - Web Security で指定されたとき自動的に共有されます。



ご注意

使用される TRITON - Web Security インスタンスは、設定される Policy Server によって決められます。設定された Policy Server IP アドレスは、Content Gateway Manager の **[More Details (詳細)]** ビューが選択されたとき、「**Monitor**」>「**My Proxy**」>「**Summary**」ページに表示されます。

Policy Server を設定するには、下記の手順を実行します。

- ◆ V- シリーズ アプライアンスの Appliance Manager で「**Configuration (設定)**」>「**Web Security Components (Web Security コンポーネント)**」に移動します。
- ◆ ソフトウェアのインストール時に、`/opt/WCG/websense.ini` を編集し、**PolicyServerIP** の値を設定します。次に Content Gateway の処理を下記の通り一旦停止し、開始します。

```
/opt/WCG/WCGAdmin stop
```

```
/opt/WCG/WCGAdmin start
```

Content Gateway が Websense Data Security のみと共に配備されている場合は、Content Gateway Manager にサブスクリプション キーを入力する必要があります。

1. **[Configure]** > **[My Proxy]** > **[Subscription (サブスクリプション)]** > **[Subscription Management (サブスクリプション管理)]** タブで Websense によって提供されたサブスクリプション キーを入力します。
2. **[Apply (適用)]** をクリックします。
3. **[Configure]** > **[My Proxy]** > **[Basic (基本)]** > **[General (一般)]** ページで **[Restart (再起動)]** をクリックします。

システム情報の設定

Content Gateway が Websense Web Security のプロキシ統合である場合 (Web Security Gateway または Web Security Gateway Anywhere)、Policy Server IP アドレスおよびポートはインストール時に指定されています。

Policy Server および Filtering Service タイムアウトの条件および動作 (トラフィックを許可またはブロック) の設定を完了するには、下記の手順を実行します。

1. 「Configure」> 「My Proxy」> 「Subscription」> 「Scanning (スキャン)」タブに移動します。Filtering Service の IP アドレスおよびポートを確認します。これは、TRITON - Web Security をインストールしたとき入力した情報です。



ご注意

[Scanning] タブは、Web Security Gateway または Web Security Gateway Anywhere に登録している場合のみ表示されます。

2. [Communication Timeout (通信タイムアウト)] 設定値を確認します。これは Content Gateway が Policy Server または Filtering Service との通信で待機する時間 (ミリ秒) です。この時間を過ぎると、設定されている [Action for Communication Errors (通信エラーに対する処置)] がトリガされます。デフォルトのタイムアウト値は、5000 (5 秒) です。値を変更した場合、Content Gateway を再起動する必要があります。
3. 通信タイムアウト条件が発生した場合、[Action for Communication Errors] セクションで、トラフィックを許可またはブロックすることを選択する必要があります。タイムアウトが発生した場合、Content Gateway はその設定値を適用し、サービスに戻ることを検出するためにサービスを定期的にポーリングします。
4. [Apply (適用)] をクリックします。

プロキシがインターネット要求を処理していることの確認

プロキシをインストールした後、プロキシが Web コンテンツの要求を処理していることを確認します。

1. Content Gateway Manager を開きます。[Content Gateway Manager へのアクセス, 11 ページ](#) を参照してください。
2. 「Monitor」> 「My Proxy」> 「Summary」ページに移動し、ライセンス契約の詳細、データ ファイルのスキャンニング ステータス、および使用されているオブジェクトの数、ヒット率、他の基本プロキシ サービス情報を含むノードの詳細を確認します。

3. 「Monitor」>「Protocol (プロトコル)」>「HTTP」>「General」に移動して、[General HTTP Statistics (一般的な HTTP 統計)] テーブルを表示します。
4. テーブルの [Client (クライアント)] セクションの中の現在の [Total Document Bytes (合計のドキュメント バイト)] 統計を確認します。

この統計の値を調べます。

General HTTP Statistics		
Attribute	Current Value	
Client		
Total Document Bytes	1.8 GB	
Total Header Bytes	1.7 MB	
Total Connections	34,758	
Current Connections	0	
Transactions in Progress	0	
Server		
Total Document Bytes	1.7 GB	
Total Header Bytes	1.3 MB	
Total Connections	35,776	
Current Connections	0	
Transactions in Progress	0	

5. ブラウザをプロキシ ポートに設定します。
6. インターネットを参照します。
7. 再度 [Total Document Bytes] 統計を調べます。

この値は プロキシが HTTP 要求を処理する際に大きくなります。

コマンドライン インターフェースの使用

ブラウザへのアクセス権がない場合、または UNIX シェルのようなコマンド インターフェースを使用したい場合、コマンドライン インターフェースはプロキシ統計の確認および Content Gateway の設定を行うためのすばやい方法を提供します。



ご注意

コマンドライン インタフェースは、Content Gateway が Websense アプライアンス上にインストールされている場合は、利用できません。代わりに、Content Gateway Manager と Appliance Manager Command Line Utility を使用します。

個別のコマンドを実行するか、またはシェルの中に複数のコマンドを記述することができます。[Websense Content Gateway のコマンド, 283 ページ](#) を参照してください。

1. root に移動します。

```
su
```

2. Content Gateway の **bin** ディレクトリ (/opt/WCG/bin) に変更します。このディレクトリから Content Gateway のコマンドを実行します。
コマンドは下記の形式です。

```
content_line -command argument
```

3. **content_line** コマンドのリストで、下記の通り入力します。

```
content_line -h
```



ご注意

Content Gateway の **bin** ディレクトリがパス上にない場合、コマンドの先頭に ./ を付けます。

例えば :

```
./content_line -h
```

コマンドラインでの Content Gateway の起動および停止

コマンドラインから Content Gateway を停止または起動するには、下記の手順を実行します。line:

1. root に移動します。

```
su
```

2. Content Gateway のインストール ディレクトリ (/opt/WCG) に変更します。

プロキシを起動するには、下記の通り入力します。

```
./WCGAdmin start
```

プロキシを停止するには、下記の通り入力します。

```
./WCGAdmin stop
```

プロキシを再起動するには、下記の通り入力します。

```
./WCGAdmin restart
```

Content Gateway サービスが何を実行しているか確認するには、下記の通り入力します。

```
./WCGAdmin status
```



ご注意

コマンドラインから Content Gateway を停止するには、常に ./WCGAdmin stop コマンドを使用します。

Content Gateway をインストールした後、Content Gateway Manager (管理インターフェース) を開き、プロキシが実行していることを確認します。

[Content Gateway Manager へのアクセス, 11 ページ](#) および [プロキシがインターネット要求を処理していることの確認, 16 ページ](#) を参照してください。

3

Web プロキシ キャッシング

Web プロキシ キャッシングは、頻繁にアクセスされる Web オブジェクト（ドキュメント、イメージ、記事など）のコピーをユーザーに近い場所に保存し、この情報をユーザーに提供します。インターネット ユーザーはそれらの情報をより速く取得でき、インターネット帯域幅を他のタスクのために解放することができます。

インターネット ユーザーは、インターネット上のあらゆる場所の Web サーバーに要求を送信します。キャッシング サーバーがそれらの要求を処理するためには、Web プロキシ サーバーとして機能する必要があります。Web プロキシ サーバーは、Web オブジェクトに対するユーザーの要求を受け取り、それらの要求を処理するか、またはそれらの要求を *オリジン サーバー*（要求された情報のオリジナルのコピーを含んでいる Web サーバー）に転送します。

Content Gateway は、*透過的プロキシ環境*（ユーザーのクライアントソフトウェア（一般的にはブラウザ）はプロキシと通信していることを認識しません）、と *明示的プロキシ環境*（ユーザーのクライアントソフトウェアは要求を直接にプロキシに送信するように設定されています）の両方をサポートします。

キャッシュ要求

関連項目：

- ◆ [キャッシュされたオブジェクトの最新性の確認, 22 ページ](#)
- ◆ [ローカル キャッシュ コンテンツへの更新のスケジュール設定, 27 ページ](#)
- ◆ [キャッシュ内のコンテンツのピンニング, 30 ページ](#)
- ◆ [キャッシュするか否か?, 31 ページ](#)
- ◆ [HTTP オブジェクトのキャッシング, 31 ページ](#)
- ◆ [オブジェクト キャッシングの強制, 37 ページ](#)
- ◆ [HTTP の代替のキャッシング, 38 ページ](#)
- ◆ [FTP オブジェクトのキャッシング, 39 ページ](#)

以下の概要は、Content Gateway がユーザー要求を処理する方法を示しています。

1. Content Gateway は、Web オブジェクトに対するユーザーの要求を受け取ります。
2. プロキシは、Web アドレスを使用して、そのオブジェクト ストア（キャッシュ）の中で要求されたオブジェクトを探します。
3. オブジェクトがキャッシュ内にある場合、プロキシは、オブジェクトが十分に新しいバージョンであるかどうかを確認します。（[キャッシュされたオブジェクトの最新性の確認](#), 22 ページ を参照）。オブジェクトが新しい場合、プロキシは、それをユーザーにキャッシュ ヒットとして提供します。
4. キャッシュ内のデータが古くなっている場合、プロキシはオリジン サーバーに接続し、オブジェクトがまだ最新であるかどうかを照会します（再確認）。オブジェクトがまだ最新である場合、プロキシは、キャッシュされているコピーを直ちにユーザーに送信します。
5. オブジェクトがキャッシュ内にはない場合（キャッシュ ミス）、またはキャッシュされているコピーがもはや有効でない場合、プロキシはオリジン サーバーからオブジェクトを取得し、それをユーザーに送信し、同時にキャッシュに保存します。それ以降のそのオブジェクトに対する要求は、より速く処理されます。なぜならオブジェクトはキャッシュから直接に取得されるからです。

キャッシュされたオブジェクトの最新性の確認

Content Gateway は Web オブジェクトに対する要求を受け取ったとき、そのキャッシュ内で要求されたオブジェクトを探します。オブジェクトがキャッシュ内にある場合、プロキシは、オブジェクトが十分に新しいバージョンであるかどうかを確認します。

プロキシがキャッシュ内のオブジェクトの最新性を判断する方法はプロトコルによって異なります。

- ◆ HTTP オブジェクトは、作成者が指定した有効期限をサポートします。プロキシはこれらの有効期限に従います。そのような有効期限がない場合、プロキシはオブジェクトが変更される頻度と、管理者が選択した最新性のガイドラインに基づいて有効期間を選択します。さらに、オブジェクトがまだ最新であるかどうかをオリジン サーバーで確認することによって、オブジェクトを再確認できます。[HTTP オブジェクトの最新性](#), 22 ページ を参照してください。
- ◆ FTP オブジェクトは、指定された期間キャッシュ内に留まります。[FTP オブジェクトの最新性](#), 27 ページ を参照してください。

HTTP オブジェクトの最新性

Content Gateway は、キャッシュ内の HTTP オブジェクトが新しいかどうかを以下の方法によって判断します。

- ◆ **Expires** または **max-age** ヘッダーをチェックする

一部の HTTP オブジェクトは、オブジェクトをキャッシュできる期間を指定する **Expires** ヘッダーまたは **max-age** ヘッダーを含んでいます。現在の時刻と期限切れ時刻を比較することによって、プロキシにオブジェクトが新しいかどうかを知らせます。

- ◆ **Last-Modified / Date** ヘッダーの確認

HTTP オブジェクトに **Expires** ヘッダーまたは **max-age** ヘッダーがない場合、プロキシは下記の式を使用して最新性の限界値を計算できます。

$$\text{freshness_limit} = (\text{date} - \text{last_modified}) * 0.10$$

ここで、*date* はオブジェクトのサーバー応答ヘッダーの日付、*last_modified* は **Last-Modified** ヘッダーの日付です。Last-Modified ヘッダーがない場合は、プロキシはオブジェクトがキャッシュに書き込まれた日付を使用します。値を 0.10 (10 パーセント) 増減できます。[最新性計算のエイジング係数の変更, 23 ページ](#) を参照してください。

計算による最新性の限界値は、最小および最大境界によって設定されます。[絶対最新性限界値の設定, 24 ページ](#) を参照してください。

- ◆ 絶対最新性限界値の確認

HTTP オブジェクトに **Expires** ヘッダーがないか、または **Last-Modified** と **Date** の両方のヘッダーがない場合は、プロキシは最大および最小最新性限界値を使用します。[絶対最新性限界値の設定, 24 ページ](#) を参照してください。

- ◆ **cache.config** ファイル内の再確認ルールの確認

再確認ルールは、特定の HTTP オブジェクトに最新性限界値を適用します。たとえば、特定のドメインまたは IP アドレスから発信するオブジェクト、指定された正規表現を含む URL をもつオブジェクト、および特定のクライアントによって要求されたオブジェクトに対して最新性限界値を設定できます。[cache.config, 374 ページ](#) を参照してください。

最新性計算のエイジング係数の変更

オブジェクトに期限切れ情報が含まれていない場合、Content Gateway は、**Last-Modified** および **Date** ヘッダーからその最新性を推定できます。デフォルトでは、プロキシは、オブジェクトを最後に変更されてから経過した時間の 10% の間保存します。この比率を増減できます。

1. Content Gateway の **config** ディレクトリにある **records.config** ファイルを開きます。
2. 下記の変数を編集します。

変数	説明
<code>proxy.config.http.cache.heuristic_lm_factor</code>	最新性計算のためのエイジング係数を指定します。 デフォルト値は 0.10 (10 パーセント) です。

3. ファイルを保存して、閉じます。

4. 変更を適用するために、Content Gateway の `bin` ディレクトリで下記のコマンドを実行します。

```
content_line -x
```

絶対最新性限界値の設定

一部のオブジェクトには **Expires** ヘッダーがないか、または **Last-Modified** および **Date** の両方のヘッダーがありません。絶対最新性限界値を指定することによって、キャッシュ内でこれらのオブジェクトが最新であるとみなされる時間を制御できます。寿命時間が長いほど、オブジェクトはキャッシュ内に長く保持されます。ページをネットワークから検索する代わりにキャッシュから取得することによってパフォーマンスが向上します。

1. **[Configure]** > **[Protocols]** > **[HTTP]** > **[Cacheability (キャッシュ能力)]** タブに移動します。
2. **[Freshness (最新性)]** セクションの **[Minimum Heuristic Lifetime (最小ヒューリスティック寿命)]** 領域で、有効期限がない HTTP オブジェクトがキャッシュ内で最新とみなされる最小時間を指定します。この時間を過ぎるとオブジェクトは古くなっているとみなされます。デフォルト値は、3600 秒 (1 時間) です。
3. **[Maximum Heuristic Lifetime (最小ヒューリスティック寿命)]** フィールドで、有効期限がない HTTP オブジェクトがキャッシュ内で最新とみなされる最大時間を指定します。この時間を過ぎるとオブジェクトは古くなっているとみなされます。デフォルト値は、86400 秒 (1 日) です。
4. **[Apply]** をクリックします。

ヘッダー要件の指定

キャッシュ内のオブジェクトの最新性を確保するために、Content Gateway が指定したヘッダーを持つオブジェクトだけをキャッシュするように設定します。



警告

デフォルトでは、プロキシはすべてのオブジェクト（ヘッダーのないオブジェクトを含む）をキャッシュします。Websense では、プロキシの特別の事情がない限りデフォルト設定を変更しないことを推奨します。プロキシが **Expires** または **max-age** ヘッダーをもつ HTTP オブジェクトのみをキャッシュするように設定されている場合、キャッシュヒット率が大幅に下がります（明示的な期限切れ情報があるオブジェクトはごく少数です）。

1. **[Configure]** > **[Protocols]** > **[HTTP]** > **[Cacheability]** タブに移動します。
2. **[Behavior (動作)]** セクションの **[Required Headers (必要なヘッダー)]** 領域で、下記のいずれかを指定します。

- Expires ヘッダーまたは Cache-Control ヘッダーをもつ HTTP オブジェクトのみをキャッシュするには、[An Explicit Lifetime Header (明示的寿命ヘッダー)] を指定します。
- Expires ヘッダーまたは Last-Modified ヘッダーをもつ HTTP オブジェクトのみをキャッシュするには、[A Last-Modified Header (最後に変更したヘッダー)] を指定します。
- すべての HTTP オブジェクトをキャッシュする (特定のヘッダーを必要としない) には、[No Required Headers (ヘッダーを必要としない)] を指定します。これは、デフォルトです。

3. [Apply] をクリックします。

Cache-Control ヘッダー

キャッシュ内でオブジェクトが最新であると見なされる場合でも、クライアントまたはサーバーにはキャッシュからのオブジェクトの取得を禁止する制約が設定されていることがあります。たとえば、クライアントはオブジェクトがキャッシュから取得されたものでない、またはキャッシュから取得された場合にはオブジェクトを 10 秒以上キャッシュしないことを要求する場合があります。

Content Gateway は、キャッシュされたオブジェクトの可用性を Cache-Control ヘッダーを基に判断します。Cache-Control ヘッダーをクライアントの要求とサーバーの応答の両方に含めることができます。

下記の Cache-Control ヘッダーはオブジェクトがキャッシュから提供されるかどうかに影響を与えます。

- ◆ クライアントによって送信される no-cache ヘッダーは、プロキシに、オブジェクトをキャッシュから直接に提供しないこと、つまり常にオリジンサーバーからオブジェクトを取得することを指示します。クライアントの no-cache ヘッダーを無視するようにプロキシを設定できます ([クライアントの no-cache ヘッダーを無視するようにプロキシを設定する, 33 ページ](#) を参照)。
- ◆ サーバーによって送信される max-age ヘッダーは、オブジェクトの経過時間と比較されます。経過時間の値が max-age よりも小さい場合、オブジェクトは最新であり、提供できます。
- ◆ クライアントによって送信される min-fresh ヘッダーは、許容可能な最新性の許容値です。クライアントは、オブジェクトの最新性がこの値以上であることを求めます。キャッシュされたオブジェクトが将来、少なくともこの期間最新性を保たない場合、そのオブジェクトは再確認されます。
- ◆ クライアントによって送信される max-stale ヘッダーは、プロキシが少し古くなったオブジェクトを提供することを許可します。一部のブラウザは、パフォーマンスの向上と引き換えに、少し古いオブジェクトを受け入れます (特に、インターネットの可用性に制約がある期間に)。

プロキシは、HTTP 最新性基準の後に Cache-Control 可用性基準を適用します。たとえば、オブジェクトが最新と見なされる場合でも、その経過時間がその max-age よりも大きい場合、提供されません。

HTTP オブジェクトの再確認

クライアントがキャッシュ内の古くなった HTTP オブジェクトを要求した場合、Content Gateway はそのオブジェクトを再確認し、オブジェクトが変更されていないかどうかをオリジン サーバーに問い合わせます。再確認の結果は、以下のいずれかになります。

- ◆ オブジェクトがまだ最新である場合は、プロキシはその最新性限界値をリセットして、そのオブジェクトを提供します。
- ◆ オブジェクトの新しいコピーが利用できる場合は、プロキシは新しいオブジェクトをキャッシュし、古くなったコピーと置き換え、同時にユーザーにオブジェクトを提供します。
- ◆ オブジェクトがオリジン サーバーにない場合、プロキシはキャッシュされたコピーを提供しません。
- ◆ オリジン サーバーが再確認の問い合わせに応答しない場合、プロキシは確認を実行せず、キャッシュからの古くなったオブジェクトを提供します。

デフォルトでは、プロキシは、キャッシュ内の要求された HTTP オブジェクトが古くなっていると判断した場合、そのオブジェクトを再確認します。プロキシは、オブジェクトの最新性を [HTTP オブジェクトの最新性, 22 ページ](#) に記載している方法で評価します。プロキシが HTTP オブジェクトを再確認する頻度を設定できます。

1. **[Configure]** > **[Protocols]** > **[HTTP]** > **[Cacheability]** タブに移動します。
2. **[Behavior]** セクションの **[When to Revalidate (再確認する時期)]** 領域で下記のいずれかを選択します。
 - **Never Revalidate (再確認しない)**。要求された HTTP オブジェクトの最新性をオリジン サーバーに照会しない場合。
 - **Always Revalidate (常に再確認する)**。要求された HTTP オブジェクトの最新性を常にオリジン サーバーに照会する場合。
 - **Revalidate if Heuristic Expiration (ヒューリスティック期限切れで再確認)**。要求された HTTP オブジェクトの最新性について、そのオブジェクトに **Expires** ヘッダーまたは **Cache-Control** ヘッダーがない場合にオリジン サーバーに照会する場合。Content Gateway は、**Expires** ヘッダーまたは **Cache-Control** ヘッダーのないすべての HTTP オブジェクトを陳腐化していると見なします。
 - **Use Cache Directive or Heuristic (キャッシュ ディレクティブまたはヒューリスティックを使用)**。Content Gateway がキャッシュ内のオブジェクトを陳腐化していると見なす場合に、要求された HTTP オブジェクトの最新性をオリジン サーバーに照会する場合。これは、デフォルトです。

3. [Apply] をクリックします。

**ご注意**

また、`cache.config` ファイルで特定の再確認ルールを設定できます。[cache.config, 374 ページ](#) を参照してください。

FTP オブジェクトの最新性

FTP オブジェクトにはタイムスタンプや日付情報がなく、指定した期間 (15 分 ~ 2 週間)、キャッシュ内で最新であるとみなされます。この期間が過ぎると陳腐化していると見なされます。

FTP オブジェクトは、HTTP クライアント (ブラウザなど) から、または FTP クライアント (WS_FTP など) から要求することができます。Content Gateway は HTTP クライアントから要求された FTP オブジェクトのみをキャッシュします。

HTTP クライアントによって要求された FTP オブジェクト

HTTP クライアントによって要求された FTP オブジェクト (HTTP オブジェクト上の FTP) の絶対最新性限界値を設定できます。

**ご注意**

HTTP クライアントによって要求された FTP オブジェクトの絶対最新性限界値のほかに、`cache.config` ファイルで特定の FTP オブジェクトの最新性ルールを設定できます ([cache.config, 374 ページ](#) を参照)。

1. [Configure] > [Protocols] > [HTTP] > [Cacheability] タブに移動します。
2. [Freshness] セクションの [FTP Document Lifetime (FTP ドキュメントの寿命)] 領域で、HTTP クライアントによって要求された FTP オブジェクトが最新とみなされる期間を指定します。この期間を過ぎるとオブジェクトは古くなっているとみなされます。デフォルト値は、259200 秒 (3 日間) です。
3. [Apply] をクリックします。

ローカル キャッシュ コンテンツへの更新のスケジュール設定

パフォーマンスをさらに向上させ、HTTP および (HTTP クライアントから要求された) FTP オブジェクトがキャッシュ内で最新状態を保つように、[Scheduled Update (スケジュール設定した更新)] オプションを使用して、プ

ロキシがスケジュール設定した時刻に特定のオブジェクトをキャッシュに入れるように設定することができます。

[Scheduled Update] オプションを使用するには、以下の手順を実行します。

- ◆ 更新をスケジュール設定するオブジェクトを含む URL のリスト、更新を行う時刻、および URL の再帰の深さを指定します。
- ◆ Scheduled Update オプションを有効化し、オプションの再試行設定を設定します。

詳細は、[スケジュール設定した更新オプションの設定](#), 28 ページ を参照してください。

Content Gateway は、ユーザーが指定した情報を使用して、処理する URL を決定し、各 URL について（該当する場合）すべての再帰的 URL を導出します。次に一意な URL リストを生成します。プロキシは、このリストを使用して、未アクセスの各 URL に対して HTTP GET を開始し、それがどの時点においても HTTP の同時性についてのユーザー指定の限度内にあるようにします。



ご注意

システムは、すべての HTTP GET 処理の完了をログに記録し、この機能のパフォーマンスをモニタできるようにします。

[Force Immediate Update (直ちに更新を強制)] オプションは、指定された更新時刻を待たずに、URL を更新できるようにします。このオプションを使用して、スケジュール設定した更新の設定をテストできます。[即時更新の強制](#), 29 ページ を参照してください。

スケジュール設定した更新オプションの設定

1. [Configure] > [Protocols] > [HTTP Scheduled Update (HTTP スケジュール設定した更新)] > [Update URLs (URL を更新)] に移動します。
2. [Scheduled Object Update] 領域で、[Edit File (ファイル編集)] をクリックして、`update.config` ファイルの設定ファイル編集エディタを開きます。
3. 下記の情報を入力します。
 - [URL] フィールドに、更新のスケジュールを設定する URL を入力します。
 - オプション。[Request Headers (ヘッダーを要求)] フィールドに、各 GET 要求で渡されたヘッダーのセミコロン区切りのリストを入力します。HTTP 仕様に準拠する任意の要求ヘッダーを指定できます。
 - [Offset Hour (オフセット時間)] フィールドに、更新時間を導出するために使用する基準時間を入力します。00 から 23 までの値を指定できます。
 - [Interval (間隔)] フィールドに、更新が行われる（オフセット時間からの）間隔（秒）を入力します。

- **[Recursion Depth (再帰の深さ)]** フィールドに、参照されている URL が再帰的に更新される (指定した URL からの) 深さを入力します。たとえば、再帰の深さが 1 であれば、指定した URL と、元の URL からのリンクによって直接に参照されるすべての URL が更新されます。
4. **[Add (追加)]** をクリックし、次に **[Apply]** をクリックします。
 5. **[Close (閉じる)]** をクリックします。
 6. **[General (一般)]** タブをクリックします。
 7. **[Scheduled Update]** を有効化します。
 8. **[Maximum Concurrent Updates (最大同時更新)]** フィールドに、スケジュール設定した更新処理によってホストに過大な負荷をかけないようにするために、許容する同時更新要求の最大数を入力します。デフォルトは 100 です。
 9. **[Retry on Update Error (更新エラー時の再試行)]** セクションの **[Count (カウント)]** フィールドに、失敗した場合に URL のスケジュール設定した更新を再試行する回数を入力します。デフォルト設定は 10 です。
 10. **[Retry on Update Error]** セクションの **[Interval]** フィールドに、失敗した場合に URL のスケジュール設定した更新の各再試行間の間隔を秒単位で入力します。デフォルト設定は 2 です。
 11. **[Apply]** をクリックします。

即時更新の強制

[Force Immediate Update] オプションによって、**update.config** ファイルにリストされている URL を直ちに確認できます。このオプションは、**update.config** ファイルに含まれているオフセット時間および間隔設定を無視して、リストされている URL を更新します。



重要

Force Immediate Update オプションを有効化した場合、このオプションを無効化するまで、プロキシは、**update.config** ファイルで指定した URL を更新し続けます。

1. **[Configure] > [Protocols] > [HTTP Scheduled Update] > [General]** に移動します。
2. **Scheduled Update** が有効化されていることを確認します。
3. **[Update URLs]** タブをクリックします。
4. **[Force Immediate Update]** を有効化します。
5. **[Apply]** をクリックします。

キャッシュ内のコンテンツのピンニング

キャッシュ ピンニング オプションは、Content Gateway が特定の HTTP オブジェクト（および HTTP クライアントから要求された FTP オブジェクト）を指定した時間、キャッシュ内に保持するように設定します。このオプションを使用して、最もよくアクセスされるオブジェクトが必要なときにキャッシュにあり、プロキシが重要なオブジェクトをキャッシュから削除しないようにします。



ご注意

プロキシは、Cache-Control ヘッダーを監視し、オブジェクトがキャッシュ可能である場合にだけ、キャッシュ内でそのオブジェクトをピンニングします。

キャッシュ ピンニングを使用するために、下記のタスクを実行します。

- ◆ **cache.config** ファイルでキャッシュ ピンニング ルールを設定します。[キャッシュ ピンニング ルールの設定, 30 ページ](#) を参照してください。
- ◆ キャッシュ ピンニング オプションを有効化します。[キャッシュ ピンニングの有効化, 31 ページ](#) を参照してください。

キャッシュ ピンニング ルールの設定

1. **[Configure]** > **[Protocols]** > **[HTTP]** > **[Cacheability]** に移動します。
2. ページの終わりで **[Edit File (ファイルを編集)]** をクリックして、**cache.config** ファイルの設定ファイル エディタを表示します。
3. 表示されたフィールドに、下記の情報を指定します。
 - **[Rule Type (ルール タイプ)]** ドロップダウン ボックスから、**pin-in-cache** を選択します。
 - **[Primary Destination Type (一次宛先タイプ)]** ドロップダウン ボックスから、**url_regex** を選択します。
 - **[Primary Destination Value (一次宛先値)]** フィールドに、キャッシュでピンニングする URL を指定します。
 - **[Time Period (時間)]** フィールドに、キャッシュに含まれているプロキシがオブジェクトをピンニングする時間を指定します。
さらに、二次指定子（例、**Prefix**、**Suffix**）をルールに追加できます。すべてのフィールドは [HTTP, 302 ページ](#) で説明しています。
4. **[Add]** をクリックして、ルールをリストに追加し、**[Apply]** をクリックします。
5. **[Close]** をクリックします。

キャッシュ ピンニングの有効化

1. [Configure ()] > [Subsystems (サブシステム)] > [Cache (キャッシュ)] > [General] で、[Allow Pinning (ピンニングを許可)] を有効化します。
2. [Apply] をクリックします。

キャッシュするか否か？

Content Gateway がキャッシュに含まれていない Web オブジェクトの要求を受け取ったとき、オリジン サーバーから Web オブジェクトを取得し、それをクライアントに提供します。同時に、プロキシは、そのオブジェクトがキャッシュ可能かどうか調べてから、将来の要求に対応するためにそれをキャッシュ内に保存します。

Content Gateway は、オブジェクトがキャッシュ可能かどうかを、プロトコルをもとに判断します。

- ◆ HTTP オブジェクトの場合、プロキシは、クライアントおよびオリジンサーバーからのキャッシング指令に対応します。また、プロキシが特定のオブジェクトをキャッシュしないように設定できます。[HTTP オブジェクトのキャッシング, 31 ページ](#) を参照してください。
- ◆ FTP オブジェクトの場合、プロキシは、ユーザーが設定オプションおよびファイルを通じて指定するキャッシング指令に対応します。[FTP オブジェクトのキャッシング, 39 ページ](#) を参照してください。

HTTP オブジェクトのキャッシング

Content Gateway は、クライアントおよびオリジンサーバーからのキャッシング指令に対応し、またユーザーが設定オプションおよびファイルを通じて指定するキャッシング指令にも対応します。

この項は、下記のトピックについて解説します。

- ◆ [クライアントの指令, 31 ページ](#)
- ◆ [オリジンサーバーの指令, 33 ページ](#)
- ◆ [設定の指令, 36 ページ](#)

クライアントの指令

デフォルトでは、Content Gateway は、下記の要求ヘッダーが付いたオブジェクトをキャッシュしません。

- ◆ **Cache-Control : no-store**

◆ **Cache-Control : no-cache**



ご注意

プロキシが **Cache-Control: no-cache** ヘッダーを無視するように設定できます。[クライアントの no-cache ヘッダーを無視するようにプロキシを設定する, 33 ページ](#) を参照してください。

◆ **Cookie:** (テキスト オブジェクトの場合)

デフォルトでは、プロキシはオブジェクトがテキストでない限り、クッキーを含む要求に対応して提供されたオブジェクトをキャッシュします。プロキシがどのタイプのクッキーを含むコンテンツもキャッシュしない、または、クッキーを含むコンテンツをすべてキャッシュする、もしくはイメージタイプのクッキーを含むコンテンツのみをキャッシュするように設定できます。[クッキーを含むオブジェクトのキャッシング, 37 ページ](#) を参照してください。

◆ **Authorization:**



ご注意

HTTP クライアントから要求された FTP オブジェクトはまた、**Cache-Control : no-store**、**Cache-Control : no-cache**、または **Authorization** ヘッダーを含むことができます。HTTP クライアントから要求された FTP オブジェクトがそのようなヘッダーを含む場合、プロキシは明示的にキャッシュするように設定されていない限り、そのオブジェクトをキャッシュしません。

クライアントの no-cache ヘッダーを無視するようにプロキシを設定する

デフォルトでは、Content Gateway は、クライアントの **Cache Control:no-cache** 指令を監視します。要求されたオブジェクトが **no-cache** ヘッダーを含む場合、プロキシは、そのオブジェクトがキャッシュ内の新しいコピーであっても、その要求をオリジン サーバーに転送します。

クライアントの **no-cache** 指令を無視するようにプロキシを設定できます。この場合、プロキシは、クライアント要求から **no-cache** ヘッダーを無視し、そのオブジェクトをそのキャッシュから提供します。



重要

no-cache 指令の監視のデフォルトの動作は、ほとんどの場合適切です。ユーザーが HTTP 1.1 に関して熟知している場合のみクライアントの **no-cache** 指令を無視するように Content Gateway を設定します。

1. **[Configure]** > **[Protocols]** > **[HTTP]** > **[Cacheability]** に移動します。
2. **[Behavior]** セクションで **[Ignore no-cache in Client Requests (クライアントの要求内の no-cache を無視する)]** オプションを有効化します。
3. **[Apply]** をクリックします。



ご注意

Microsoft Internet Explorer の一部のバージョンは、ユーザーがブラウザの **[Refresh (リフレッシュ)]** ボタンを押した場合、透過的キャッシュからのキャッシュ再ロードを要求しません。それによって、コンテンツがオリジン サーバーから直接にロードされるのを防止します。Content Gateway が Microsoft Internet Explorer の要求をより慎重に処理するように設定できます。その場合、提供するコンテンツの最新性を向上させることができますが、キャッシュから提供できるドキュメントの数が少なくなります。Content Gateway Manager (**[Configure]** > **[Protocols]** > **[HTTP]** > **[Cacheability]** タブの **[Behavior]** セクション)で、プロキシが Microsoft Internet Explorer からの要求に対して **no-cache** ヘッダーを追加するように設定できます。

オリジン サーバーの指令

デフォルトでは、Content Gateway は、下記の要求ヘッダーが付いたオブジェクトをキャッシュしません。

- ◆ **Cache-Control : no-store**
- ◆ **Cache-Control : private**

◆ **WWW-Authenticate :**



ご注意

WWW-Authenticate ヘッダーを無視するようにプロキシを設定できます。[WWW-Authenticate ヘッダーを無視するようにプロキシを設定する, 35 ページ](#) を参照してください。

◆ **Set-Cookie :**

◆ **Cache-Control : no-cache**



ご注意

no-cache ヘッダーを無視するようにプロキシを設定できます。[サーバーの no-cache ヘッダーを無視するようにプロキシを設定する, 34 ページ](#) を参照してください。

◆ **Expires : 0 (ゼロ)** の値または過去の日付の付いたヘッダー

サーバーの no-cache ヘッダーを無視するようにプロキシを設定する

デフォルトでは、Content Gateway は、**Cache Control:no-cache** 指令を監視します。**no-cache** ヘッダーが付いたオリジン サーバーからの応答は、キャッシュ内に保存されず、キャッシュに含まれているオブジェクトの以前のすべてのコピーが削除されます。



重要

no-cache ヘッダーを無視するようにプロキシを設定した場合、プロキシは、**no-store** ヘッダーも無視します。



重要

no-cache 指令の監視のデフォルトの動作は、ほとんどの場合適切です。ユーザーが HTTP 1.1 に関して熟知している場合のみオリジン サーバーの **no-cache** 指令を無視するようにプロキシを設定します。

オリジン サーバー の **no-cache** ヘッダーを無視するようにプロキシを設定できます。

1. Content Gateway **config** ディレクトリにある **records.config** ファイルを開きます。

2. 下記の変数を編集します。

変数	説明
<code>proxy.config.http.cache.ignore_server_no_cache</code>	サーバーの指令を無視してキャッシュをバイパスするには 1 に設定します。

3. ファイルを保存して、閉じます。
4. 変更を適用するには、Content Gateway `bin` ディレクトリから下記のコマンドを実行します。

```
content_line -x
```

WWW-Authenticate ヘッダー を無視するようにプロキシを設定する

デフォルトでは、Content Gateway は、**WWW-Authenticate** 応答ヘッダーが含まれているオブジェクトをキャッシュしません。**WWW-Authenticate** ヘッダーは、認証チャレンジ応答をオリジン サーバーと比較するときクライアントが使用する認証パラメータを含んでいます。



重要

デフォルトの動作、つまり **WWW-Authenticate** ヘッダーが付いたオブジェクトをキャッシュしないという設定は、ほとんどの場合に適切です。ユーザーが HTTP 1.1 に関して熟知している場合のみサーバーの **WWW-Authenticate** ヘッダーを無視するようにプロキシを設定します。

オリジン サーバーの **WWW-Authenticate** ヘッダーを無視するようにプロキシを設定できます。その場合 **WWW-Authenticate** ヘッダーの付いたオブジェクトは今後の要求に対応するためにキャッシュに保存されます。

1. Content Gateway `config` ディレクトリにある `records.config` ファイルを開きます。
2. 下記の変数を編集します。

変数	説明
<code>proxy.config.http.cache.ignore_authentication</code>	WWW-Authenticate ヘッダーの付いたオブジェクトをキャッシュするには 1 に設定します。

3. ファイルを保存して、閉じます。
4. 変更を適用するには、Content Gateway `bin` ディレクトリから下記のコマンドを実行します。

```
content_line -x
```

設定の指令

クライアントおよびオリジン サーバーの指令のほかに、Content Gateway は、ユーザーが設定オプションおよびファイルを通じて指定する指令に対応します。

プロキシを下記のいずれかに設定できます。

- ◆ どの HTTP オブジェクトもキャッシュしない。 [. HTTP オブジェクトキャッシングの無効化, 36 ページ](#) を参照してください。
- ◆ ダイナミック コンテンツをキャッシュする（疑問符 (?)、セミコロン (;)、cgi を含むまたは .asp で終了する URL を含むオブジェクト） [ダイナミックコンテンツのキャッシング, 36 ページ](#) を参照してください。
- ◆ **Cookie:** ヘッダーに対応して提供したオブジェクトをキャッシュする [クッキーを含むオブジェクトのキャッシング, 37 ページ](#) を参照してください。
- ◆ **cache.config** ファイルに含まれている never-cache ルールを監視します。 [cache.config, 374 ページ](#) を参照してください。

HTTP オブジェクト キャッシングの無効化

デフォルトでは、Content Gateway は、**cache.config** ファイルで never-cache ルールを設定した HTTP オブジェクトを除くすべての HTTP オブジェクトをキャッシュします。HTTP オブジェクトのキャッシングを無効化できます。それによってすべての HTTP オブジェクトはオリジン サーバーから提供され、キャッシュされません。

1. **[Configure]** > **[Protocols]** > **[HTTP]** > **[Cacheability]** タブに移動します。
2. HTTP キャッシングを無効化します。
3. **[Apply]** をクリックします。

ダイナミック コンテンツのキャッシング

URL が疑問符 (?)、セミコロン (;)、cgi を含むか、または .asp で終了する場合、その URL はダイナミックと見なされます。デフォルトでは、Content Gateway は、ダイナミック コンテンツをキャッシュしません。しかし、このコンテンツをキャッシュするようにプロキシを設定できます。



警告

専用のプロキシが割り当てられている場合にのみ、プロキシがダイナミック コンテンツをキャッシュするように設定することを推奨します。

1. **[Configure]** > **[Protocols]** > **[HTTP]** > **[Cacheability]** に移動します。
2. **[Dynamic Caching (ダイナミック キャッシング)]** セクションで、**[Caching Documents with Dynamic URLs (ダイナミック URL を含むドキュメントのキャッシュ)]** を有効化します。

3. **[Apply]** をクリックします。

クッキーを含むオブジェクトのキャッシング

デフォルトでは、Content Gateway は、オブジェクトがテキストでない限り、クッキーを含む要求に対応して提供されたオブジェクトをキャッシュします。プロキシはクッキーを含むテキスト コンテンツをキャッシュしません。なぜならオブジェクトとともにオブジェクト ヘッダーも保存され、パーソナライズされたクッキー ヘッダー値がオブジェクトとともに保存される可能性があるからです。

テキストでないオブジェクトの場合、パーソナライズされたヘッダーが配信されたり使用されたりする可能性はありません。

1. **[Configure]** > **[Protocols]** > **[HTTP]** > **[Cacheability]** に移動します。
2. **[Dynamic Caching]** セクションの **[Caching Response to Cookies (クッキーへの応答のキャッシング)]** 領域で、下記のいずれかのキャッシング オプションを選択します。
 - テキストであるコンテンツを除くすべてのクッキーを含むコンテンツをキャッシュするには、**[Cache All but Text (テキストを除くすべてをキャッシュ)]** を選択します (これはデフォルト設定です)。
 - イメージであるクッキーを含むコンテンツをキャッシュするには、**[Cache Only Image Types (イメージ タイプのみキャッシュ)]** を選択します。
 - すべてのタイプのクッキーを含むコンテンツをキャッシュするには、**[Cache Any Content Type (すべてのコンテンツ タイプをキャッシュ)]** を選択します。
 - どのタイプのクッキーを含むコンテンツもキャッシュしない場合は、**[No Cache on Cookies (クッキーをキャッシュしない)]** を選択します。
3. **[Apply]** をクリックします。

オブジェクト キャッシングの強制

特定の URL (ダイナミック URL を含む) を指定した期間、**Cache-Control** 応答ヘッダーとは無関係にキャッシュするように Content Gateway を強制できます。

1. **[Configure]** > **[Protocols]** > **[HTTP]** > **[Cacheability]** に移動します。
2. ページの終わりで **[Edit File]** をクリックして、**cache.config** ファイルの設定ファイル エディタを表示します。
3. 表示されたフィールドに、下記の情報を指定します。
 - **[Rule Type]** ドロップダウン ボックスから、**ttl-in-cache** を選択します。

- **[Primary Destination Type]** ドロップダウン ボックスから、`url_regex` を選択します。
 - **[Primary Destination Value]** フィールドに、キャッシュを強制する URL を指定します。
 - **[Time Period]** フィールドに、プロキシがキャッシュから URL を処理できる時間を指定します。
さらに、二次指定子 (例、**Prefix**、**Suffix**) をルールに追加できます。すべてのフィールドは [HTTP, 302 ページ](#) で説明しています。
4. **[Add]** をクリックし、次に **[Apply]** をクリックします。
 5. **[Close]** をクリックします。

HTTP の代替のキャッシング

一部のオリジン サーバーは、種々のオブジェクトが含まれている同一の URL への要求に応答します。これらのオブジェクトのコンテンツは、サーバーが種々の言語のコンテンツを配信するか、種々のプレゼンテーションスタイルを持つ種々のブラウザを対象としているか、または種々のドキュメントフォーマット (HTML、PDF) を提供するかどうかによって異なります。同一のオブジェクトの種々のバージョンを代替と言い、**Vary** 応答ヘッダーに基づいて Content Gateway によってキャッシュされます。

Content Gateway が代替をキャッシュする方法の設定

プロキシがキャッシングの代替として識別する特定のコンテンツ タイプに追加的な要求および応答ヘッダーを指定できます。

1. **[Configure]** > **[Protocols]** > **[HTTP]** > **[Cacheability]** に移動します。
2. **[Vary Based on Content Type (コンテンツタイプに基づいて変動)]** セクションで、**[Enabled (有効化)]** をクリックして **[Vary]** ヘッダーを含んでいない HTTP ドキュメントの代替バージョンをキャッシュします。
3. プロキシ サーバーが識別する追加的な要求および応答ヘッダーを指定します。
 - **[Vary by Default on Text (テキストの場合にデフォルトで変動)]** フィールドに、テキスト (例、HTML ドキュメント) の要求の場合に変動させる HTTP ヘッダー フィールドを入力します。
 - **[Vary by Default on Images (イメージの場合にデフォルトで変動)]** フィールドに、イメージ (例、.gif ファイル) の要求である場合に変動させる HTTP ヘッダー フィールドを入力します。

- [Vary by Default on Other Document Types (他のドキュメント タイプの場合にデフォルトで変動)] フィールドに、テキストまたはイメージ以外の要求の場合に変動させる HTTP ヘッダー フィールドを入力します。



ご注意

I 上記のフィールドで変動させるヘッダー フィールドとして [Cookie (クッキー)] を指定した場合、[Dynamic Caching] セクションの [Caching Response to Cookies] 領域で適切なオプションが有効化されていることを確認します。たとえば、[Caching Response to Cookies] 領域で [Cache Only Image Types] オプションを有効化し、[Vary Based on Content Type] セクションで [Vary by Default on Text] オプションを有効化した場合、クッキーを使用する代替はテキストに適用されません。

4. [Apply] をクリックします。

オブジェクトの代替の数の制限

Content Gateway がオブジェクトごとにキャッシュできる代替の数を制限できます。代替のデフォルト数は、3 です。



ご注意

代替の数が大きくなると、すべての代替が同一の URL をもちますからプロキシのパフォーマンスに影響を与える場合があります。Content Gateway は、インデックスに含まれている URL を非常にすばやく検索しますが、オブジェクトストアに含まれている利用可能な代替を順にスキャンする必要があります。

1. [Configure] > [Protocols] > [HTTP] > [Cacheability] に移動します。
2. [Maximum Alternates (代替の最大数)] フィールドに、プロキシがキャッシュするオブジェクトの代替バージョンの最大数を入力します。デフォルト値は 3 です。
3. [Apply] をクリックします。

FTP オブジェクトのキャッシング

FTP オブジェクトは、HTTP クライアント (ブラウザなど) から、または FTP クライアント (WS_FTP など) から要求することができます。

HTTP クライアントから要求された FTP オブジェクト (HTTP 上の FTP) の場合、プロキシが何をキャッシュに保存するかを決定するために、下記の設定を実行します。

- ◆ HTTP 上の FTP のキャッシングを無効化し、プロキシが HTTP クライアントから要求されたすべての FTP オブジェクトをキャッシュしないようにします ([HTTP 上の FTP キャッシングの無効化](#), 40 ページ を参照)。
- ◆ `cache.config` ファイルで `never cache` ルールを設定します ([cache.config](#), 374 ページ を参照)。
- ◆ クライアントの `Cache-Control:no-store` または `Cache-Control: no-cache` ヘッダーを無視するようにプロキシを設定します ([クライアントの no-cache ヘッダーを無視するようにプロキシを設定する](#), 33 ページ を参照)。

FTP クライアントから要求された FTP オブジェクトの場合、キャッシングは、サポートされていません。

HTTP 上の FTP キャッシングの無効化

HTTP 上の FTP オプションを無効化することによって、HTTP クライアントから要求されたすべての FTP オブジェクトをキャッシュしないように Content Gateway を設定できます。プロキシは要求を FTP サーバーに転送することによってそれらの要求を処理しますが、要求されたすべてのオブジェクトをキャッシュしません。

1. **[Configure]** > **[Protocols]** > **[HTTP]** > **[Cacheability]** に移動します。
2. **[Caching]** セクションで、**[FTP over HTTP Caching (HTTP 上の FTP のキャッシング)]** を無効化します。
3. **[Apply]** をクリックします。

4

明示的プロキシ

インターネット要求が透過的に Layer 4 スイッチまたはルータを経由して Content Gateway へとルーティングされていない場合 ([透過的プロキシと ARM, 51 ページ](#)を参照)、クライアントのインターネット ブラウザを設定することによってトラフィックを Content Gateway に**明示的に**ルーティングする必要があります (これを *明示的プロキシ環境*と言います)。

クライアントは下記の 3 つのいずれかの方法で Web ブラウザを設定できます。

- ◆ ブラウザが直接にプロキシに要求を送信するように、ブラウザを直接に設定する。[手動でのブラウザの設定, 41 ページ](#)を参照してください。
- ◆ ブラウザが PAC (Proxy Auto-Config) ファイルからプロキシ設定の指示をダウンロードするように設定する。[PAC ファイルの使用, 42 ページ](#)を参照してください。
- ◆ WPAD (Web Proxy Auto-Discovery Protocol) を使用して、WPAD サーバーからプロキシ設定の指示をダウンロードするようにする (Microsoft Internet Explorer のみ)。[WPAD の使用, 44 ページ](#)を参照してください。

また、Content Gateway が FTP トラフィックをプロキシに転送するように設定されている場合、FileZilla や WS_FTP などの FTP クライアントアプリケーションは、明示的にプロキシに要求を送信するように設定されている必要があります。[明示的プロキシ環境での FTP クライアントの設定, 46 ページ](#)を参照してください。

手動でのブラウザの設定

ブラウザが Content Gateway に要求を送信するように設定するには、クライアントは、プロキシによる処理を希望する各プロトコルについて以下の情報を提供する必要があります。

- ◆ プロキシのホスト名または IP アドレス。



重要

ユーザー認証のために統合 Windows 認証が設定されている場合、Fully Qualified Domain Name (完全修飾ドメイン名) を使用する必要があります。IP アドレスを指定すると、認証が失敗します。[統合 Windows 認証, 201 ページ](#)を参照してください。

- ◆ プロキシ サーバー ポート。Content Gateway のデフォルトのサーバーポートは 8080 です。



重要

Content Gateway プロキシの IP アドレスを仮想 IP アドレスに設定してはいけません。

Content Gateway Manager は仮想 IP アドレスの入力を禁じていませんが、VIP を使用した場合プロキシは適切に機能しません。

また、クライアントは特定のサイトに対してはプロキシを使用しないように指定できます。リストされたサイトへの要求は直接にオリジン サーバーに送信されます。

Microsoft Internet Explorer バージョン 7.0 以上の場合、プロキシ設定は [Tools] > [Internet Options (インターネット オプション)] > [Connections (接続)] > [LAN Settings (LAN の設定)] に含まれています。デフォルトでは Microsoft Internet Explorer は、すべてのプロトコルを同じプロキシ サーバーに設定します。各プロトコルを別々に設定するには、[LAN Settings] セクションに含まれている [Advanced (詳細設定)] をクリックします。プロキシ設定の手順の詳細については、ブラウザのマニュアルを参照してください。

Mozilla Firefox 4.0 以上の場合、プロキシ設定は、[Tools] > [Options] > [Advanced] > [Network] > [Settings (設定)] > [Connection Settings (接続設定)] > [Manual Proxy Configuration (手動のプロキシ設定)] に含まれています。デフォルトでは、各プロトコルを個別に設定する必要があります。しかし、[Use this proxy server for all protocols (このプロキシ サーバーをすべてのプロトコルに使用)] を選択することによって、すべてのプロトコルを同じサーバーに設定できます。

手動で設定したブラウザからの要求を受け入れるために、プロキシで設定オプションを設定する必要はありません。

PAC ファイルの使用

PAC ファイルは、ブラウザが要求を処理する方法を決定するために呼び出す JavaScript 関数定義です。クライアントは自分のブラウザ設定の中で、PAC ファイルをロードする URL を指定する必要があります。

PAC ファイルをプロキシに保存し、このファイルの URL をクライアントに提供できます。**proxy.pac** ファイルがある場合は、それを Content Gateway の **config** ディレクトリにコピーします。



ご注意

PAC ファイルはネットワーク内のどのサーバーにも常駐できます。

SSL Manager を使用している場合、HTTPS トラフィックに使用する PAC ファイルの詳細について、[明示的プロキシ モードでの実行, 147 ページ](#) を参照してください。

1. 既存の **wpad.dat** ファイルがある場合、Content Gateway の **config** ディレクトリに含まれている **wpad.dat** ファイルを既存のファイルに置き換えます。
2. **[Configure]** > **[Content Routing (コンテンツ ルーティング)]** > **[Browser Auto-Config (ブラウザ自動設定)]** > **[PAC]** タブに移動します。
3. **[Auto-Configuration Port (ポートの自動設定)]** フィールドで、Content Gateway が PAC ファイルを提供するために使用するポートを指定します。デフォルト ポートは 8083 です。
4. **[PAC Settings (PAC 設定)]** 領域に **proxy.pac** ファイルが表示されます。
 - 既存の PAC ファイルを Content Gateway の **config** ディレクトリにコピーした場合、**proxy.pac** ファイルは、ユーザーのプロキシの設定を含みます。設定値を確認し、必要な場合変更を行います。
 - 既存の PAC ファイルを Content Gateway の **config** ディレクトリにコピーしていない場合は、**[PAC Settings]** 領域は空です。プロキシサーバーの設定を提供するスクリプトを入力します。サンプルのスクリプトを [サンプルの PAC ファイル, 44 ページ](#) に示しています。[Websense Technical Library](#) の「PAC File Best Practices」という表題の記事も参照してください。
5. **[Apply]** をクリックします。
6. **[Configure]** > **[My Proxy]** > **[Basic]** > **[General]** を順に選択して **[Restart (再起動)]** をクリックします。
7. ユーザーに、ブラウザがこの PAC ファイルを選択するように設定するよう指示します。

たとえば、PAC ファイルが置かれているプロキシサーバーのホスト名が **proxy1** であり、Content Gateway がデフォルト ポート 8083 を使用してファイルを提供する場合、ユーザーはプロキシ設定で下記の URL を指定する必要があります。

```
http://proxy1.company.com:8083/proxy.pac
```

PAC ファイルの場所の指定の手順はブラウザによって異なります。たとえば、Microsoft Internet Explorer の場合、**[Tools]** > **[Internet Options]** > **[Connections]** > **[LAN Settings]** から **[Use automatic configuration script (自動設定スクリプトを使用)]** で PAC ファイルの場所を設定します。Mozilla Firefox の場合、プロキシの設定は、**[Tools]** > **[Options]** > **[Advanced]** > **[Network]** >

[Settings] > [Connection Settings] > [Automatic proxy configuration URL (手動のプロキシ設定 URL)] に含まれています。詳細についてはご使用のブラウザのマニュアルを参照してください。

サンプルの PAC ファイル

以下のサンプル PAC ファイルは、ブラウザに対して、完全に修飾されたドメイン名のないすべてのホスト、およびローカルドメインに含まれているすべてのホストに直接に接続するよう指示します。他のすべての要求は、**myproxy.company.com** という名前のプロキシ サーバーに送られます。

```
function FindProxyForURL(url, host)
{
  if (isPlainHostName(host) || dnsDomainIs(host,
".company.com"))
    return "DIRECT";
  else
    return "PROXY myproxy.company.com:8080; DIRECT";
}
```

WPAD の使用

Internet Explorer バージョン 7 以上で WPAD を使用すると、プロキシ サーバーの設定を提供するサーバーを自動的に検出できます。クライアントは、ブラウザがプロキシ サーバに要求を送信するように設定する必要はありません。1 つのサーバーがネットワーク上のすべてのクライアントに設定を提供します。



ご注意

WPAD は、透過的プロキシ環境に適合します。

Internet Explorer バージョン 7 以上のブラウザは、起動時に、プロキシ サーバーの設定を提供する WPAD サーバーを検索します。このサーバーの現在の完全修飾ドメイン名の前にホスト名 WPAD を付けます。たとえば、**x.y.company.com** に含まれるクライアントは **wpad.x.y.company.com** にある WPAD サーバーを検索します。検索が失敗した場合、ブラウザは最下位のドメインを削除し、再度検索を試みます。たとえば **wpad.y.company.com** で検索します。ブラウザは、WPAD サーバーを検出したとき、または 3 番目のレベルのドメイン **wpad.company.com** に達したとき、検索を中止します。このアル

ゴリズムは 3 番目のレベルで停止しますから、ブラウザは現在のネットワークの外側を検索しません。



ご注意

デフォルトでは、Microsoft Internet Explorer バージョン 7 以上は自動的に WPAD サーバーを検出するように設定されています。しかし、ブラウザユーザーはこの設定を無効化することができます。

Content Gateway を WPAD サーバーとして使用するよう設定できます。

1. 既存の `wpad.dat` ファイルがある場合、Content Gateway の `config` ディレクトリに含まれている `wpad.dat` ファイルを既存のファイルに置き換えます。
2. Content Gateway Manager にログオンし、**[Configure]** > **[Content Routing]** > **[Browser Auto-Config]** > **[WPAD]** に移動し、`wpad.dat` ファイルを表示します。
3. **[WPAD Settings (WPAD の設定)]** 領域に `wpad.dat` ファイルが表示されます。
 - 既存の `wpad.dat` ファイルを Content Gateway の `config` ディレクトリにコピーした場合、ファイルは、ユーザーのプロキシの設定を含みます。設定値を確認し、必要な場合変更を行います。
 - 既存の `wpad.dat` ファイルを Content Gateway の `config` ディレクトリ (`/opt/WCG/config`) にコピーしていない場合は、**[WPAD Settings]** 領域は空です。プロキシサーバーの設定を提供するスクリプトを入力します。サンプルスクリプトを [サンプルの PAC ファイル, 44 ページ](#) に示しています (`wpad.dat` ファイルは `proxy.pac` ファイルと同じスクリプトを含むことができます)。
4. **[Apply]** をクリックします。
5. **[Configure]** > **[Networking]** > **[ARM]** に移動します。
6. **[Network Address Translation (NAT) (ネットワークアドレス変換)]** セクションで **[Edit File (ファイルを編集)]** をクリックし、`ipnat.conf` ファイルに特別のリマップルールを追加します。
7. 表示される下記のフィールドに情報を入力し、**[Add]** をクリックします。
 - **[Ethernet Interface (イーサネットインターフェース)]** フィールドに、ブラウザからの WPAD 要求を受け取るネットワークインターフェース (例、`hme0` or `eth0`) を入力します。
 - **[Connection Type]** ドロップダウン リストから `tcp` を選択します。
 - **[Destination IP]** フィールドに Content Gateway サーバーの IP アドレスを入力します。この IP アドレスは、ローカル名前サーバーの後に `/32` を付けることによって WPAD サーバー名に解決されます。
`123.456.7.8/32`。
 - **[Destination Port]** フィールドに、`80` と入力します。
 - **[Redirected Destination IP (リダイレクト宛先 IP)]** フィールドに **[Destination IP]** フィールドで入力した同じ IP アドレスを、`/32` を省いて入力します。

- [Redirected Destination Port (リダイレクト宛先ポート)] フィールドに 8083 と入力します。
- 8. [Add] をクリックします。
- 9. 左側の矢印キーを使用して新しい規則をファイルの最初の行に移動します。
- 10. [Apply] をクリックし、次に [Close] をクリックします。
- 11. [Configure] > [My Proxy] > [Basic] > [General] を順に選択して、[Restart] をクリックします。

明示的プロキシ環境での FTP クライアントの設定

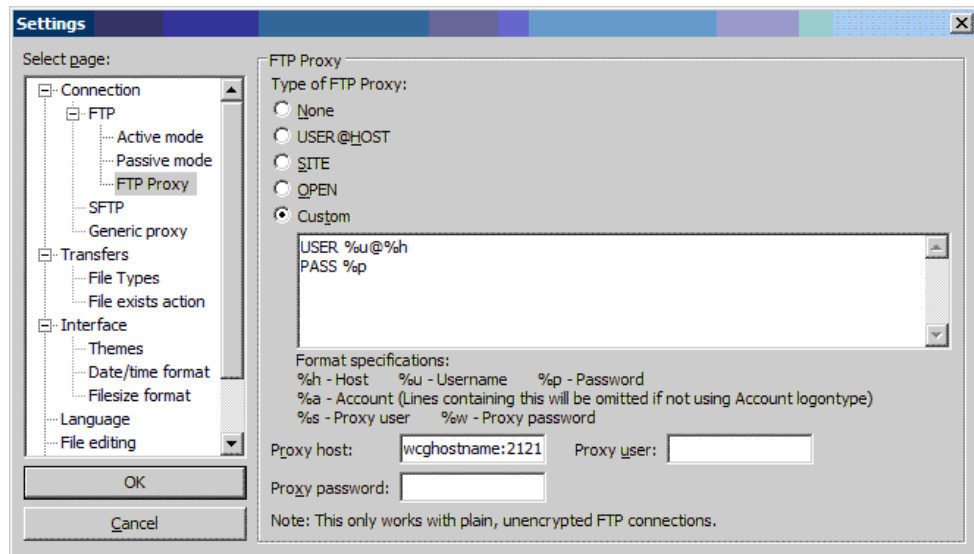
Content Gateway が FTP トラフィックをプロキシに転送するように設定されている場合 ([FTP, 314 ページ](#) を参照)、FileZilla や WS_FTP などの FTP クライアント アプリケーションは、明示的にプロキシに要求を送信するように設定されている必要があります。そのように設定した場合、FTP クライアント アプリケーションをプロキシが存在しないかのように使用できます。

FTP サーバーに接続するには、通常、下記の 4 つの情報がが必要です。これらの情報は、下記のようにマップされます。

マップ元:	マップ先:
FTP サーバー ホスト名	FTP <i>プロキシ</i> ホスト名
FTP サーバー ポート番号	FTP <i>プロキシ</i> ポート番号 (デフォルトは 2121)
FTP サーバー ユーザー名	FTP_server_username@FTP_server_hostname 例: anon@ftp.abc.com
FTP サーバー パスワード	FTP サーバー パスワード

一部の FTP クライアント アプリケーションには、FTP プロキシ情報を指定するための設定ページがあります。これらの設定を Content Gateway FTP プロキシを指定するように更新します。ご使用の FTP クライアント アプリケーションのマニュアルを参照してください。

これは FileZilla の最新のバージョンを使った設定の例です。



[FTP Proxy] 領域で下記の手順を実行します。

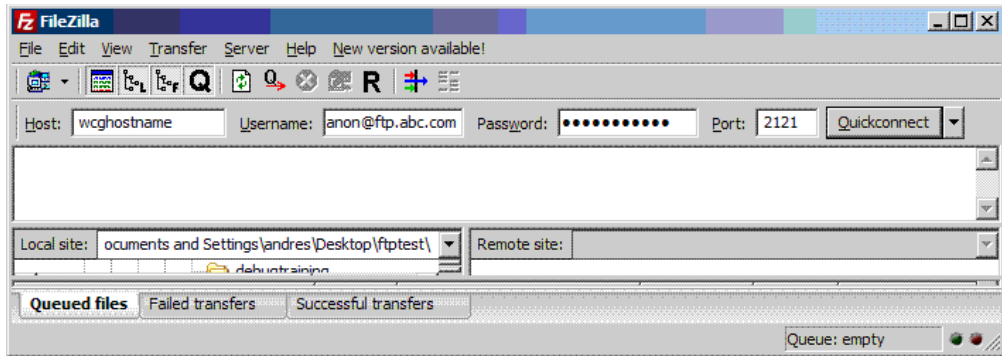
1. [FTP Proxy] を [Custom (カスタム)] に設定し、上記のように USER および PASS を指定します。
2. [Proxy host (Proxy ホスト)] を Content Gateway の FTP プロキシ ホスト名 およびポート番号に設定します。
3. [OK] をクリックして設定を適用します。

次に、通常の、プロキシが存在しない場合と同様の方法で FTP 接続情報を入力します。例：

```
Host :          ftp.abc.com
Username :      anon
Password :      123abc
```

FTP クライアント アプリケーションが設定されていない場合、下記のように FTP 要求を入力する必要があります。

```
Host :          Content Gateway の プロキシ ホスト名
Username :      anon@ftp.abc.com
Password :      123acb
Port :          2121
```



Content Gateway バージョン 7.7.0 による IPv6 のサポート

TRITON Enterprise のバージョン 7.7 (Content Gateway プロキシ コンポーネントを含む) は、IPv6 の増分サポートを提供します。



重要

サポートは、明示的プロキシ環境の場合のみ提供されます。

Content Gateway による IPv6 のサポートは、下記を含みます。

- ◆ デュアル IP スタック イーサネット インタフェース上の IPv6
- ◆ 次のプロトコルをサポートします : HTTP、HTTPS、FTP、DNS
- ◆ インターネット、クライアント、および PAC ファイル サーバーへの IPv6 トラフィック
- ◆ IPv6 仮想 IP アドレス (vaddrs.config)
- ◆ クライアント IPv6 アドレス範囲に基づく認証ルール
- ◆ プロキシへのアクセスを許可または禁止するクライアント IPv6 アドレスおよびアドレス範囲 (ip_allow.config)
- ◆ Content Gateway Manager へのアクセスを許可または禁止するクライアント IPv6 アドレスおよびアドレス範囲 (mgmt_allow.config)
- ◆ プロキシ フィルタリング ルール (filter.config)、キャッシュ ルール (cache.config)、およびチェーンの中の親プロキシ サーバー (parent.config) に含まれる IPv6 一次宛先値および送信元 IP 値
- ◆ SSL Manager Incident List (インシデント リスト) に含まれる IPv6 アドレス
- ◆ IPv6 データに対する SNMP トラップおよびカウンタ

制限と制約 :

- ◆ IPv6 専用の内部ネットワークはサポートされません。

- ◆ Content Gateway クラスタの他のメンバーを含むすべての TRITON コンポーネント間の通信には、IPv4 を使用する必要があります（マルチキャスト アドレス）。



ご注意

Content Gateway Manager に組み込まれている記述テキストとは異なり、マルチキャスト グループ アドレスは IPv4 でなければなりません ([Configure] > [My Proxy] > [Basic] > [Clustering (クラスタ化)])。

- ◆ すべてのユーザー認証で、Domain Controller が IPv4 アドレスでアクセスできなければなりません。
- ◆ ARM は IPv6 アドレスをサポートしません。これはリダイレクト ルール (ipnat.config) および静的バイパス ルール (bypass.config) においてもです。
- ◆ チェーンの中の親プロキシが IPv6 であってはなりません。
- ◆ IP スプーフィングはサポートされていません。
- ◆ SOCKS プロキシはサポートされていません。

IPv6 プロキシの統計：

Content Gateway は IPv6 トラフィックを追跡します。「Monitor」>「Networking」>「System」ページを順に選択すると統計が表示されます。

IPv6 のイベント ログへの影響

IPv6 を有効化した場合、イベント ログの入力項目が IPv6 フォーマットに標準化されます。たとえば、“10.10.41.200” は、“::ffff:10.10.41.200” とログされます。

カスタム ログの “10.10.41.200” でクライアントをフィルタリングするには、下記のフィルタが必要です。

```
<LogFilter>
  <Name = "IPv6_Test_Machine"/>
  <Condition = "chi MATCH ::ffff:10.10.41.200"/>
  <Action = "ACCEPT"/>
</LogFilter>
```

IPv6 設定のまとめ

IPv6 サポートはデフォルトでは無効化されています。

Content Gateway が Websense Appliance に配備されている場合、最初に Appliance Manager [Configuration] > [Network Interfaces] > [IPv6] タブで IPv6 を有効化します。

IPv6 は、Content Gateway Manager の「Configure」>「My Proxy」>「Basic」ページの [Network] セクションで有効化されます。有効化されたとき、前の項で列挙したすべての機能領域のサポートが有効化されます。

IPv6 アドレスを受け入れるフィールドでは、アドレスを標準に適合する任意の形式で入力できます。例：

- ◆ 16 ビット値の中の先頭の 0 を省略できます
- ◆ 連続する 0 の 1 つのグループをダブル コロンに置換できます

IPv6 を無効化すると、IPv6 エントリ フィールドは非表示にされ、IPv6 値が設定ファイルから削除されます。

DNS Resolver を使用している場合、「**Configure**」>「**Network**」>「**DNS Resolver**」ページに移動し、IPv4 または IPv6 の優先設定を設定します。IPv4 がデフォルトです。

5

透過的プロキシと ARM

透過的プロキシ オプションによって Content Gateway は、クライアントのインターネット要求に対して、ユーザーにブラウザの再構成を要求することなしに応答できます。そのために、トラフィックが遮断された – 多くの場合、レイヤー 4 (L4) のスイッチまたはルーターによって – 後で要求のフローをプロキシへ、リダイレクトします。

透過的プロキシ環境

1. プロキシはスイッチまたはルーターによってクライアントからオリジンサーバーへの要求を遮断します。[透過的遮断戦略, 53 ページ](#)を参照してください。
2. Adaptive Redirection Module (ARM) は、着信パケットの宛先 IP アドレスをプロキシの IP アドレスに変更し、宛先ポートをプロキシポートに変更します (もし異なる場合)。(ARM は常に有効化されます。)
3. プロキシは遮断されたクライアント要求を受信し、処理を開始します。要求がキャッシュヒットである場合、プロキシは要求されたオブジェクトを提供します。要求がヒットしない場合、プロキシはオリジンサーバーからオブジェクトを取得し、クライアントに対してそれを提供します。
4. クライアントへの応答では、ARM は送信元 IP アドレスをオリジンサーバーの IP アドレスに変更し、送信元のポートをオリジンサーバーのポートに変更します。



重要

複数のインターフェースまたはゲートウェイがある透過的プロキシ構成では、Content Gateway はオペレーティングシステムのルーティングテーブルにクライアントおよびインターネットへの適切なルートを確認していなければなりません。

HTTP では、プロキシは問題があるクライアントおよびサーバーを識別でき、ARM はそのようなクライアントおよびサーバーの遮断を無効化し、そのトラフィックを直接にオリジンサーバーへ渡します。また、クライアントおよびサーバーをプロキシへのリダイレクトから除外するための ARM 静的バイパ

ス ルールを作成することもできます。[遮断の迂回](#), 73 ページ を参照してください。

関連項目

- ◆ [透過的遮断戦略](#), 53 ページ
- ◆ [遮断の迂回](#), 73 ページ
- ◆ [接続負荷の軽減](#), 77 ページ
- ◆ [DNS ルックアップの削減](#), 77 ページ
- ◆ [IP スプーフィング](#), 78 ページ

ARM

Content Gateway ARM は着信パケットを、IP レイヤーがそれを受け取る前に検査し、パケットを Content Gateway で処理するようにアドレス変更します。

ARM は着信パケット アドレスに 2 つの変更を行うことができます。その宛先 IP アドレスと宛先ポートを変更できます。たとえば、HTTP パケットの宛先 IP アドレスがプロキシの IP アドレスにアドレス変更され、宛先 HTTP ポートが Content Gateway HTTP プロキシ ポート（通常はポート 8080）にアドレス変更されます。

クライアントへの応答では、ARM は送信元 IP アドレスをオリジン サーバーの IP アドレスに変更し、送信元のポートをオリジン サーバーのポートに変更します。

ARM コンポーネントはいくつかのファイルと 1 つのカーネル モジュールから成り、製品インストール時にインストールされます。インストール プログラムはまた、プロキシ コンピュータの IP アドレスとデフォルトのポート割り当てを使って、パケットのアドレス変更を行うリダイレクト ルールを作成することができます。ARM は常にアクティブです。

プロキシが HTTP、HTTPS、FTP、または DNS 要求を透過的に処理するためには、`ipnat.conf` ファイルの中のリダイレクト ルールを確認し、必要に応じて変更する必要があります。WCCP を使って透過的な遮断を行う場合、すべてのアクティブ サービス グループですべてのポートに対してリダイレクト ルールが設定されていなければなりません。デフォルトでは、標準ポートに対するルールが設定されています。ARM リダイレクト ルールを表示し、処理するには、以下の手順を実行します。

1. Content Gateway Manager にログオンし、「**Configure (設定)**」>「**Networking (ネットワーキング)**」>「**ARM**」>「**General (一般)**」タブへ移動します。

[**Network Address Translation (NAT) (ネットワーク アドレス変換 (NAT))**] セクションに `ipnat.conf` ファイルの中のリダイレクト ルールが表示されます。リダイレクト ルールを確認し、必要な変更を行います。

- a. リダイレクト ルールを変更するには、[Edit File (ファイルの編集)] をクリックして、ipnat.conf ファイルの編集のための設定ファイル エディタを開きます。
 - b. 編集するルールを選択し、変更対象のフィールドを編集および変更します。[Set (設定)] をクリックし、次に [Apply (適用)] をクリックして変更を適用します。設定ファイル エディタを終了するためには、[Close (閉じる)] をクリックします。
- すべてのフィールドは [ARM, 345 ページ](#) で説明されています。
2. [Configure (設定)] > [My Proxy (マイ プロキシ)] > [Basic (基本)] > [General (一般)] で [Restart (再起動)] をクリックします。

透過的遮断戦略

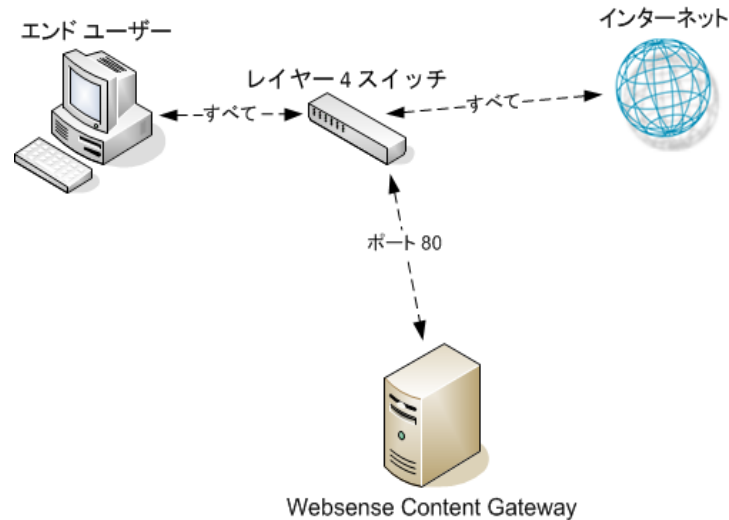
Websense Content Gateway は、以下の透過的遮断ソリューションをサポートします。

- ◆ レイヤー 4 スイッチ。 [レイヤー 4 スイッチによる透過的遮断, 54 ページ](#) を参照してください。
- ◆ WCCP v2 をサポートするルーターとスイッチ。Cisco IOS ベースのルーターが最も一般的です。 [WCCP v2 デバイスによる透過的遮断, 55 ページ](#) を参照してください。
- ◆ ポリシー ベースのルーティング [透過的遮断とマルチキャスト モード, 71 ページ](#) を参照してください。
- ◆ ソフトウェア ルーティング [ソフトウェア ベースのルーティングによる透過的遮断, 73 ページ](#) を参照してください。

クライアント要求がプロキシに到達する経路はネットワーク トポロジーに依存します。複合的なネットワークでは、どのクライアントを透過的に処理するかを決定し、そのネットワーク デバイスとプロキシがその要求を遮断するように配置されていることを確認する必要があります。Content Gateway または Content Gateway に接続しているルーターまたはスイッチは多くの場合、インターネットへの幹線または集約パイプ上に配置されています。

レイヤー 4 スイッチによる透過的遮断

レイヤー 4 スイッチはサポートされているプロトコルをプロキシにリダイレクトし、他のすべてのインターネットトラフィックをその宛先に直接に渡します (HTTP について、下図に示しています)。



レイヤー 4 スイッチは、スイッチのタイプに応じて、以下の機能を提供します。

- ◆ ネットワーク上の停止しているホストを検知し、トラフィックをリダイレクトできるレイヤー 4 スイッチは、信頼性を向上させます。
- ◆ 1 つのレイヤー 4 スイッチが複数のプロキシ サーバーに接続している場合、スイッチは Content Gateway ノードの間でのロード バランシングを処理します。スイッチの種類によってロード バランシングの方法 (ラウンドロビン、ハッシュなど) が異なります。ノードが使用不可能になった場合、スイッチは負荷を再配分します。ノードが復旧したとき、いくつかのスイッチがノードを元の作業負荷に戻しますから、ノード キャッシュを再ポピュレートする必要はありません。この機能を キャッシュ アフィニティーと言います。



ご注意

クラスタ構成でスイッチがロード バランシングを提供している時は、Content Gateway の仮想 IP フェールオーバーを有効化しないことを推奨します。

WCCP v2 デバイスによる透過的遮断

関連項目

- ◆ [WCCP の負荷配分, 57 ページ](#)
- ◆ [WCCP v2 ルーターの構成, 59 ページ](#)
- ◆ [Content Gateway で WCCP v2 を有効化, 65 ページ](#)
- ◆ [ARM 迂回と WCCP, 57 ページ](#)

Content Gateway は、WCCP v2 対応のルーターおよびスイッチによる透過的遮断をサポートします。

HTTP、HTTPS、FTP、および DNS プロトコルがサポートされています。標準ポートには HTTP、HTTPS、および FTP のためのデフォルトの ARM リダイレクト ルールが含まれています。

セットアップの概要の後に、[WCCP v2 でサポートされている機能](#)のリストを示しています。



重要

ネットワーク クライアント、Content Gateway プロキシ サーバー、宛先 Web サーバー（デフォルト ゲートウェイ）は別々のサブネット上に常駐していなければなりません。

以下は WCCP v2 のセットアップの概要です。

1. WCCP v2 デバイスをインストールし、システム設定します。
各 WCCP v2 デバイスに対して、以下のことを行います。
 - サービス グループを設定します。
 - 必要なら、パスワード セキュリティを設定します。
 - 必要なら、マルチキャスト通信を設定します。
[WCCP v2 ルーターの構成, 59 ページ](#)を参照してください。
2. Content Gateway を WCCP デバイスとともに使用できるように設定します。
 - 対応するサービス グループを定義します。
ネットワーク インターフェース、プロトコル、ポート、認証（使用する場合）、およびマルチキャスト通信（使用する場合）のほかに、下記を設定します。
 - ・ WCCP v2 デバイスの IP アドレス。
 - ・ Packet Forward Method（パケット転送方法）と Packet Return Method（パケット返送方法）。
 - ・ Content Gateway がクラスタ内に配備されている場合、（必要な場合）**assignment method（割り当て方法）**による負荷の配分
 - 非標準ポートのための ARM NAT ルールを作成します。

[Content Gateway で WCCP v2 を有効化, 65 ページ](#) および [ARM, 52 ページ](#) を参照してください。

3. テスト トラフィックを使って構成を検証します。

WCCP v2 でサポートされている機能

Content Gateway は、以下の WCCP v2 機能をサポートします。

- ◆ 1 つのプロキシ クラスタ内の複数のルーター
- ◆ 1 つのサービス グループに複数のポート
- ◆ 1 つのプロトコルに複数のサービス グループ 異なる WCCP デバイスに異なるサービス グループを割り当てる必要がある、またはそうすることが便利である場合があります。たとえば、Cisco ASA ファイアウォールでは、ネットワーク内の WCCP デバイスごとに異なるサービス グループが必要とされます。
- ◆ **assignment method** HASH または MASK、および **weight** によるプロキシ クラスタ内の動的負荷配分。[WCCP の負荷配分, 57 ページ](#) を参照してください。
- ◆ Packet Return Method および Packet Forward Method ネゴシエーション
- ◆ サービス グループごとの MD5 パスワード セキュリティ
- ◆ マルチキャスト モード

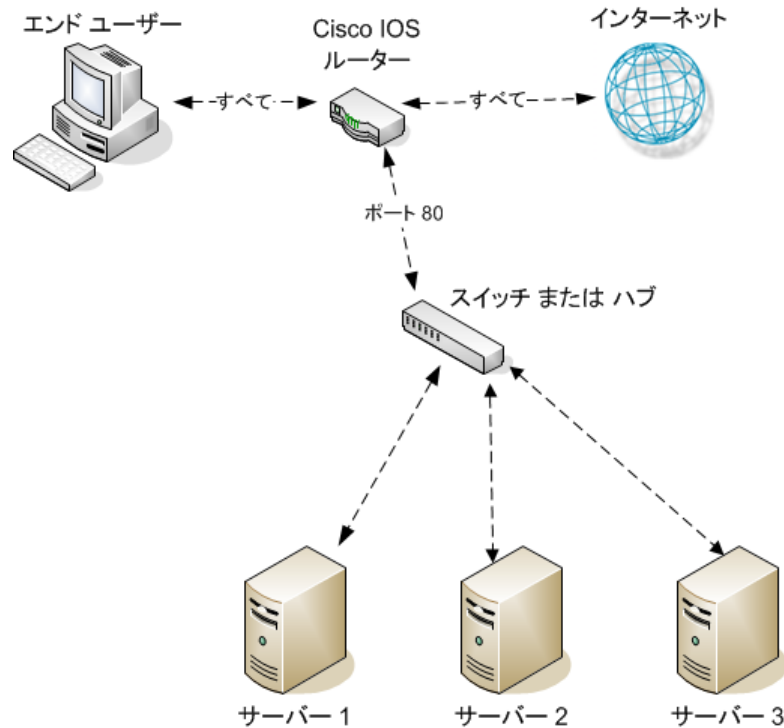
Content Gateway クラスタでは、WCCP 環境で仮想 IP フェールオーバーを有効化しないことを推奨します。WCCP v2 および Content Gateway の設定は、ノードの障害および再起動を処理します。([WCCP の負荷配分, 57 ページ](#) および [仮想 IP フェールオーバー, 89 ページ](#) を参照。)

Content Gateway はまた、キャッシュ アフィニティをサポートします。ノードが使用不可能になり、その後復旧したとき、ノード キャッシュを再ポピュレートする必要はありません。

WCCP v2 遮断の仕組み

1. WCCP v2 デバイスは、サービス グループの設定に従って、プロキシ サーバーまたはサーバーのクラスタに HTTP、HTTPS、FTP および DNS トラフィックを送信します。
2. ARM はトラフィックのアドレスを変更します。たとえば、ポート 80 上の HTTP トラフィックは、Content Gateway ポート 8080 にアドレス変更されます。
3. プロキシは通常通りに要求を処理し、クライアントに応答を返送します。

4. ARM は応答ヘッダーの中のプロキシ ポートをポート 80 にアドレス変更します（プロキシへの転送の際に行ったアドレス変更を元に戻す）。その結果、ユーザーには、応答があたかもオリジン サーバーから直接に送信されたかのように示されます。



ARM 迂回と WCCP

Content Gateway に ARM 迂回ルール（[遮断の迂回, 73 ページ](#) を参照）がある場合、Content Gateway は特定のクライアント要求を直接にオリジン サーバーに転送します。

ARM は迂回された要求を変更せず、クライアントの送信元 IP アドレスはそのまま保持されます。

WCCP v2 では、特定のルーター インターフェースをリダイレクトから除外することができます。Content Gateway ARM バイパス ルールは、Content Gateway が接続されているルーター インターフェースを WCCP リダイレクトから除外している場合にのみ機能します。そのためには、Content Gateway に接続しているインターフェースを選択し、ルーター設定コマンド `ip wccp redirect exclude in` を発行します。これによってルーターは指定したインターフェース上での着信トラフィックをすべてのリダイレクト ルールから除外します。

WCCP の負荷配分

WCCP プロトコルはクラスタ内の動的対称および非対称負荷配分の **assignment method** を提供します。WCCP は、ノードの障害を検出し、Content Gateway によって通知された設定をもとに再配分を実行します。

- ◆ 負荷配分は Content Gateway Manager で設定され、WCCP デバイスにプッシュされます。
- ◆ 負荷配分はサービスグループごとに設定されます。各サービスグループで、以下のように設定します。
 - 関係するクラスタメンバーは、サービスグループに登録されていなければなりません。(WCCP デバイスはロードバランシングについて何も決定しません。)
 - assignment method として HASH または MASK を選択します。HASH は一般的には GRE forward/return method と共に使用し、MASK は L2 forward/return method と共に使用します。



重要

MASK は Cisco Catalyst シリーズ スイッチのために特に開発されており、これらのプラットフォーム上のハードウェアで WCCP 遮断の適切な実行を可能にする主要な特性の 1 つです。これはサポートが文書化されているデバイスでのみ使用します。

- 1 つ以上の**配分属性**を選択します。一般的には、宛先の IP アドレスを使用します。
- 負荷を異なるクラスタメンバーに異なる割合で配分する場合は、各クラスタメンバーに **weight** の値を設定します。この値は、それぞれのメンバーが受け取る要求の割合を、他のメンバーのそれに対する相対的な値で指定します。

weight の値を使用する非対称的負荷配分は、次のような場合に便利です。

- ・ 処理能力が異なる複数の Content Gateway サーバー（例、V シリーズ V10000 と V10000 G2）を使用する。
- ・ 特定のオリジンサーバー（および宛先 IP アドレス）を優先するために、インターネットトラフィックプロファイルが均等な配分に適さない。

動的再配分の仕組み

WCCP デバイスがクラスタメンバーがオフラインであることを検出した時に、動的再配分が実行されます。このとき、WCCP デバイスは自動的に、負荷配分の設定をもとに、残りのクラスタメンバーに負荷を再配分します。クラスタメンバーが復旧し、WCCP デバイスによって検出されたとき、再び、その設定をもとに負荷配分が自動的に再調整されます。

設定の手順については [Content Gateway Manager でのサービスグループの設定, 66 ページ](#) を参照してください。

weight 値による非対称負荷配分の仕組み

weight 値を使用する場合は、この値をクラスタ内の各ノード上で設定しなければなりません。weight 値は、各サービスグループおよびノードに固有です。weight 値は、クラスタ全体には適用されません。

weight の値は、他のクラスタ メンバーに対する設定に対する相対的な値であり、WCCP がそのノードに転送するトラフィックの割合を決定します。

デフォルトでは、weight は 0 に設定されています。この場合、トラフィックはすべてのクラスタ メンバーに均等に分配されます。

非対称負荷分配を実行するためには、weight 値をクラスタ内の他のメンバーの値に対する相対的値として設定します。たとえば、クラスタに 3 つのノードが含まれるとします。

ノード	weight 値	負荷配分
Node1	50	50%
Node2	25	25%
Node3	25	25%

Node1 がオフラインになった場合、Node2 と Node3 が同じ量のトラフィックを受け取ります。Node3 がオフラインになった場合、Node1 はトラフィックの 3 分の 2 を受け取り、Node2 はトラフィックの 3 分の 1 を受け取ります。

weight 値は他のクラスタ ノードに設定されている値に対する相対的な値ですから、weight 値がそれぞれ 10、5、5 でも同じ配分が得られます (weight 値の範囲は 0-255 です)。

weight をデフォルト値の 0 から変更する場合、クラスタ内のすべてのノードに対して weight 値を設定する必要があります。

WCCP v2 ルーターの構成

WCCP v2 の構成と処理能力に関する情報について、マニュアルおよび製造者のサポート サイトを参照することを強く推奨します。大部分のデバイスを、ハードウェア ベースのリダイレクトを最大限に活用するように構成する必要があります。Cisco デバイスでは、通常は IOS の最新バージョンが最も適切です。

WCCP v2 デバイスをプロキシとともに使用するよう準備するには、以下のことを行います。

1. 使用するプロトコルに対して、1 つ以上のサービス グループを設定します。1 つのサービス グループは 1 つ以上のプロトコルを処理できます。[WCCP デバイス上のサービス グループを設定, 60 ページ](#) を参照してください。
2. これらのサービス グループに対する WCCP 処理を可能にするようにルーターを設定します。[サービス グループに対する WCCP 処理の有効化, 61 ページ](#) を参照してください。

- 任意に、ルーターのセキュリティを有効化します。Content Gateway 内のサービスグループに対してもルーターのセキュリティを有効化しなければなりません。[ルーター上で WCCP v2 セキュリティの有効化](#), 64 ページを参照してください。



ご注意

使用しているルーターの構成に関する指示は、ハードウェアベンダーによるマニュアルを参照してください。Cisco ルーターについては <http://www.cisco.com/univercd/cc/td/doc/product/core/> を参照し、ご使用の IOS およびデバイスのバージョンを検索してください（例、IOS 12.4）。

- ルーターの構成が完了したとき、Content Gateway Manager で WCCP を有効化しなければなりません。[Content Gateway Manager で WCCP v2 を有効化](#), 65 ページを参照してください。

WCCP デバイス上のサービスグループを設定

WCCP は、サービスグループを使って、Content Gateway（および他のデバイス）にリダイレクトするトラフィックを指定します。

サービスグループは、1 つ以上のポート上で、1 つ以上のプロトコルを遮断できます。

- 1 つ以上のポート上
- 1 つ以上のプロトコル

サービスグループには 0 ~ 255 の範囲の固有の整数の識別子 (ID) が割り当てられます。

サービスグループ ID はユーザー定義であり、デフォルトのポートまたはトラフィックタイプはありません。

下の表は、ネットワーク内でよく使用されるサービスグループ定義のセットを示しています。IP スプーフィングを設定する場合、[IP スプーフィング](#), 78 ページの表に示している、よく使用されるリバース サービスグループ ID を参照してください。

サービス ID	ポート	トラフィックタイプ
0	80	HTTP
5	21	FTP
70	443	HTTPS (SSL Manager が必須)

サービスグループは、ルーター上、および Content Gateway 内で設定しなければなりません。

最善の方法は、ルーターを先に設定し、次に Content Gateway を設定することです。

詳細についてはルーターのマニュアルに従ってください。一般的には、下記のように行います。

1. ルーターで WCCP に対して何が設定されているかを確認するために、次のように入力します。

```
show running-config | include wccp
```

2. WCCP v2 を有効にするために、次のように入力します。

```
ip wccp version 2
```

3. ルーターで、Content Gateway の前に別のプロキシ キャッシュを使用した場合、前に使用したサービス ID を無効化します。たとえば、Cisco ルーターを使用している場合、下記のコマンドを発行することによってサービス ID **web-cache** を無効化します。

```
no ip wccp web-cache
```

4. Content Gateway で使用するサービス グループ ID を指定します。使用するコマンドについては、ルーターのマニュアルを参照してください。ルーターによってサポートされている各サービス グループを個別に設定しなければなりません。ルーターを一括で設定することはできません。

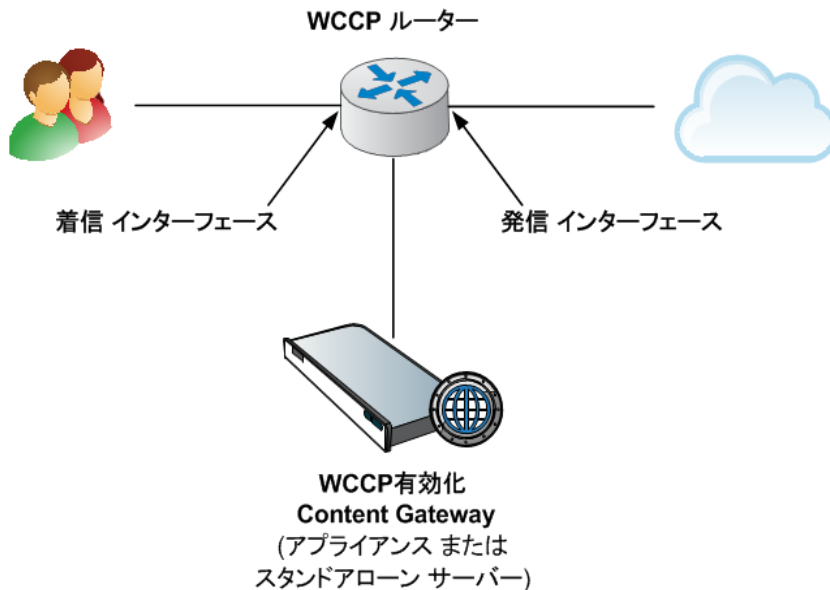
サービス グループに対する WCCP 処理の有効化

設定するそれぞれの WCCP v2 サービス グループに対して、WCCP 処理を有効化しなければなりません。

WCCP v2 ルーターは、下記のような複数のネットワーク インターフェースを含んでいます。

- ◆ 着信 (ingress) クライアント トラフィックを受信する 1 つ以上のインターフェース
- ◆ Content Gateway に接続している 1 つ以上のインターフェース

- ◆ インターネットに向けた発信 (egress) トラフィックのための専用のインターフェース



以下は、ルーター上のサービスグループのための WCCP 処理を有効化するためのいくつかのガイドラインです。詳細についてはルーターのマニュアルの手順を参照してください。

1. WCCP 機能をオンにします。

```
ip wccp <service group ID> password [0-7] <passwd>
```
2. ルーターまたはスイッチ インターフェース上で、着信 (ingress) パケットまたは発信 (egress) パケットのリダイレクトを有効化します。

✓ ご注意

ハードウェアおよびネットワーク トポロジによってサポートされる場合、ingress インタフェース上でリダイレクトを実行する (“redirect in” コマンドを使用) ことを推奨します。

以下は例です。必ずルーター上で指定したサービスグループ ID に置換してください。

はじめに、設定するインターフェースを選択します。

```
interface <type> <number>
```

次に、リダイレクト ルールを設定します。

```
ip wccp <service group ID> redirect in
```

着信リダイレクトの例

以下のコマンドは、サポートする各プロトコルに対して、ただし、着信 (ingress) トラフィック専用のインターフェース上でのみ実行します。

たとえば、HTTP 宛先ポート トラフィックのリダイレクトをオンにするには、下記のように入力します。

```
ip wccp 0 redirect in
```

HTTPS 宛先ポート トラフィックのリダイレクトをオンにするには、下記のように入力します。

```
ip wccp 70 redirect in
```

FTP 宛先ポート トラフィックのリダイレクトをオンにするには、下記のように入力します。

```
ip wccp 5 redirect in
```

HTTP 送信元ポート トラフィックのリダイレクトをオンにする - IP スプーフィングのために必須 - には、下記のように入力します。

```
ip wccp 20 redirect in
```

発信 (egress) リダイレクトの例

以下のコマンドは、サポートする各プロトコルに対して、**ただし、発信 (egress) トラフィック専用のインターフェース上でのみ実行します。**

はじめに、設定するインターフェースを選択します。

```
interface <type> <number>
```

次に、リダイレクト ルールを設定します。

```
ip wccp <service group ID> redirect out
```

たとえば、HTTP のリダイレクトをオンにするには、下記のように入力します。

```
ip wccp 0 redirect out
```

HTTPS のリダイレクトをオンにするには、下記のように入力します。

```
ip wccp 70 redirect out
```

FTP のリダイレクトをオンにするには、下記のように入力します。

```
ip wccp 5 redirect out
```

3. **重要：ARM 動的または静的迂回が有効化されているか IP スプーフィングが有効化されていて、着信 (egress) インターフェース上のリダイレクトがオンになっている時、Content Gateway の egress トラフィックを処理するルーター インターフェース上の Content Gateway の発信パケットのリダイレクトを除外します。下の図を参照してください。**

- a. Content Gateway の egress トラフィックを処理するインターフェースを選択します。

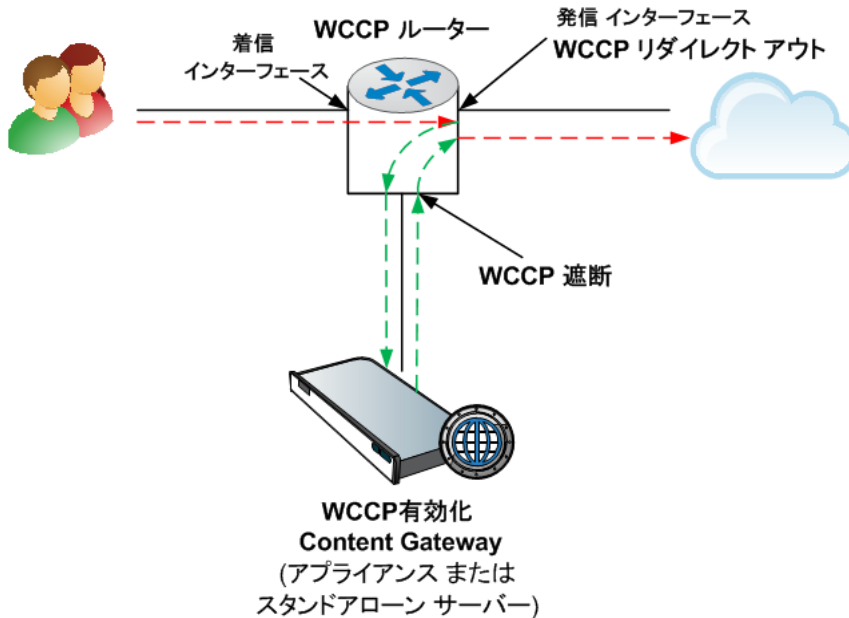
```
interface <type> <number>
```

- b. このインターフェース上の Content Gateway 発信トラフィックを、ルーター上のすべてのリダイレクト ルールから除外します。

```
ip wccp redirect exclude in
```

ARM 迂回が行われた時、または IP スプーフィングが有効化されている時、プロキシは元の送信元の IP アドレスでトラフィックをインターネット

トに送信します。“redirect exclude in” コマンドは、ルーターがトラフィックをループに入れて、Content Gateway に戻すのを防止します。



サービス グループに対する WCCP 処理の無効化

何らかの理由で WCCP 処理を無効化する必要がある場合、このコマンドを発行して WCCP 機能をオフにします。

```
no ip wccp <service group ID> password [0-7] <passwd>
```

ルーター上での WCCP v2 セキュリティの有効化

WCCP v2 を実行している場合、Content Gateway ノード上でセキュリティを有効化して、プロキシとルーターが相互に認証できるようにすることができます。ルーターによってサポートされている各サービス グループに対して個別にセキュリティを有効化しなければなりません。Content Gateway の場合とは違って、ルーターを一括で設定することはできません。

セキュリティ オプションの有効化と認証パスワードの提供は、Content Gateway Manager で行います。

遮断する各サービス グループについて、指定する認証パスワードとルーター上で設定されている認証パスワードが一致しなければなりません。以下の手順は、異なるサービス グループに認証パスワードを設定する方法の例です。

1. Telnet でルーターに接続し、Enable モードに切り換えます。
2. プロンプトに対して、下記のコマンドを入力して、端末からルーターを設定します。

```
configure terminal
```

3. ルーター上で WCCP を有効化した時にパスワードを定義した場合は、ステップ 4 に進みます。そうでない場合は、ルーターが遮断する各サービスグループに対して、下記のコマンドを入力します。

```
hostname(config)# ip wccp service_group password password
```

ここで、*hostname* は設定しているルーターのホスト名、*service_group* はサービスグループ ID (たとえば、HTTP の場合は 0)、*password* は Content Gateway を認証するために使用するパスワードです。このパスワードは、このサービスグループに対して Content Gateway 設定の中で指定したパスワードに一致しなければなりません。

4. ルーター設定を終了し、保存します。

Content Gateway で WCCP v2 を有効化

関連項目

- ◆ [WCCP v2 ルーターの構成, 59 ページ](#)
- ◆ [WCCP デバイス上のサービスグループを設定](#)
- ◆ [サービスグループに対する WCCP 処理の有効化](#)
- ◆ [ルーター上での WCCP v2 セキュリティの有効化, 64 ページ](#)

WCCP v2 ルーターの設定が完了した後、以下の手順が残っています。

1. [Content Gateway Manager で WCCP v2 を有効化](#)
2. [Content Gateway Manager でのサービスグループの設定](#)
3. Content Gateway の再起動



重要

Content Gateway を再起動する前に、設定が以下の要件を満たしていることを確認してください。

- ◆ Cisco IOS デバイスが IOS のごく最近のバージョンを実行しており、すべての関連するパッチが適用されている。
- ◆ WCCP ルーターに適切なサービスグループおよび他の機能がプログラミングされている。

Content Gateway Manager で WCCP v2 を有効化

1. [Configure] > [My Proxy] > [Basic] > [General] の順に選択します。
2. [Features (フィーチャ)] テーブルの [Networking (ネットワーク)] のセクションで WCCP を見つけ、[On] をクリックし、[Apply] をクリックします。Content Gateway を再起動してはいけません。

Content Gateway Manager でのサービスグループの設定

トラフィックを Content Gateway サーバーへリダイレクトするすべての WCCP サービスグループは、Content Gateway サーバーまたはクラスタの中に対応するサービスグループが定義されていなければなりません。



重要

サービスグループの有効/無効状態、指定されているネットワークインターフェース、**weight** 以外のすべてのサービスグループ属性はクラスタ全体に適用されます。

したがって、

- ◆ クラスタ内では、サービスグループの設定は一度だけ必要です。
- ◆ ただし、有効/無効の設定、指定されているネットワークインターフェース、および **weight** は、(使用する場合は)、各ノード上で設定しなければなりません。

これによって特定のノード上で、特定のサービスグループアクティビティを除外できます。また、**weight** を除外することによって、比例的な負荷配分が可能になります ([WCCP の負荷配分](#)を参照)。

- ◆ サービスグループを定義するには、**[Configure] > [Networking] > [WCCP]** を順に選択します。

Service Groups テーブルは、設定されているサービスグループのリストと、そのシステム設定のサブセットを表示します。

このエントリは、**wccp.config** ファイルに保存されます。

[Refresh (リフレッシュ)] ボタンをクリックすると、**wccp.config** が再読み込みされ、テーブルがリフレッシュされます。

- ◆ サービスグループを追加、編集、削除、順序変更するには、**[Edit File (ファイルの編集)]** をクリックします。

サービスグループの設定 (**wccp.config** の編集)

1. **[Configure] > [Networking] > [WCCP]** で **[Edit File]** をクリックし、エディタで **wccp.config** を開きます。

このページの上部に、定義済みのサービスグループの一覧が表示されます。リストの中のエントリをクリックすると、その詳細が表示され、編集または順序変更を行うことができます。

エントリが選択されている時、その左側の上および下向き矢印を使ってそのエントリのリスト内での位置を変更できます。

「X」をクリックすると選択したエントリが削除されます。

2. サービスグループの情報

- a. **サービスグループのステータス**: サービスグループを有効化するには、[Enabled (有効化)] を選択します。サービスグループを定義し、非アクティブにしておくことができます。有効/無効のステータスはクラスタ全体には適用されません。
- b. **サービスグループの名前**: 固有のサービスグループ名を指定します。サービスグループ名は管理に役立ちます。
- c. **サービスグループの ID**: WCCP サービスグループの識別番号を 0 ~ 255 の範囲で指定します。この ID は、ルーターで設定されている対応するサービスグループ番号と一致していなければなりません。[WCCP デバイス上のサービスグループを設定](#)を参照してください。
- d. **プロトコル**: サービスグループに適用されるネットワークプロトコルを指定します (TCP または UDP)。
- e. **ポート**: このサービスグループが使用するポートを指定します。カンマ区切り形式のリストで最大 8 つのポートを選択できます。



重要

サービスグループ内の各ポートには、トラフィックを Content Gateway にリダイレクトするために、対応する ARM NAT が指定されていなければなりません。[ARM](#) を参照してください。

- f. **ネットワークインターフェースドロップダウンリスト**から、このサービスグループが使用する Content Gateway ホストシステム上のネットワークインターフェースを選択します。**ネットワークインターフェース**の値はクラスタ全体には適用されません。したがって、**サービスグループのステータス**の値と同様に、クラスタのメンバーごとに指定しなければなりません。
3. **モードのネゴシエーション**

ルーターまたはスイッチの能力および場所に適したモードを選択する必要があります。

Packet Forward Method は、遮断されたトラフィックが WCCP ルーターからプロキシへ送信される方法を決定します。

Packet Return Method は、遮断されたトラフィックを WCCP ルーターへ返送する方法を決定します。

一般的には、ルーターは 1 つの方法だけをサポートします。

一般的にはパケット転送方法とパケット返送方法は一致しています。

- a. **Packet Forward Method**: L2 または GRE を選択します。

L2 を選択した場合、返送方法としては L2 が自動的に選択されます (GRE は選択できません)。

- b. **Packet Forward Method:** L2 または GRE を選択します。



重要

L2 を選択するには、ルーターとスイッチが Content Gateway と Layer 2-adjacent (同じサブセットにある) であることが必要です。

GRE は WCCP マルチキャスト モードでは使用できません。

Content Gateway がルーターによってサポートされていない Forward/Return 方法を使用するように設定されている場合、プロキシはルーターによってサポートされている方法を使用しようと試みます。

4. **詳細設定**

- a. **割り当て方法:** 遮断されたトラフィックをクラスタ内の複数のノードで配分するために使用するパラメータを指定します。これは **Weight** との組み合わせによって動的な負荷配分を行うために使用できます。WCCP 負荷配分機能の詳細については、[WCCP の負荷配分, 57 ページ](#) を参照してください。

HASH は選択した配分属性にハッシュ演算を適用します。

- ・ HASH では、2 つ以上の配分属性を選択できます。
- ・ ハッシュ演算の結果によって、トラフィックを受信するクラスタメンバーが決まります。

MASK は選択した配分属性にマスク演算を適用します。

- ・ 1 つの配分属性 (通常は IP アドレス) だけを選択できます。
- ・ マスク演算の結果によって、トラフィックを受信するクラスタメンバーが決まります。

次の配分属性を選択することができます。

- ・ Destination IP address (宛先 IP アドレス)
- ・ Destination Port (宛先ポート)
- ・ Source IP address (送信元 IP アドレス)
- ・ Source Port (ソースポート)

MASK 値は最大 6 つの有効ビットまで適用されます (1 つのクラスタで、合計 64 個の bucket が作成されます)。割り当て方法 HASH および MASK 演算の詳細については WCCP のマニュアルを参照してください。ご使用のデバイスに、製造業者のマニュアルで推奨されている値を使用してください。

- b. **Weight** 比例的負荷配分のために、0 ~ 255 の範囲の値を指定します。この値はクラスタ内のサーバー間での比例的負荷配分を決定します。デフォルトではすべてのクラスタメンバーに値 0 が割り当てられています。この設定では、トラフィックは均等に配分されます。weight が 1 以上の値に設定されている場合、この値はノード間の比例的配分の基準となります。たとえば、クラスタ内に 3 つのノードがあり、

Proxy1 の weight が 20、Proxy2 の weight が 10、Proxy3 の weight が 10 である場合、Proxy1 がトラフィックの半分を処理し、Proxy2 と Proxy3 がそれぞれトラフィックの 4 分の 1 を処理します。



重要

クラスタのいずれかのメンバーに対して 0 より大きい **weight** 値が設定されている時、weight 値が 0 のクラスタ メンバーにはトラフィックは**転送されません**。weight を使用する場合、必ずクラスタの各メンバーに weight を設定してください。



ご注意

weight の値は負荷の比例的配分を、他のクラスタ メンバーに対する相対的な値として決定しますから、**weight** 値はクラスタ全体には適用されません。

負荷配分の詳細については、[WCCP の負荷配分, 57 ページ](#) を参照してください。

- c. リバース サービス グループ ID リバース サービス グループ ID を指定できます。

IP スプーフィングが有効化されている時、それぞれの HTTP および HTTPS (有効化されている場合) フォワード サービス グループにリバース サービス グループを定義しなければなりません。



ご注意

IP スプーフィングでは、HTTP および HTTPS のみがサポートされます。

Content Gateway は、指定された ID を使用して、フォワード サービス グループのミラーであるリバース サービス グループを作成します。たとえば、フォワード サービス グループの割り当て方法が宛先 IP アドレスを基準にしている場合、リバース サービス グループでは割り当て方法は送信元 IP アドレスを基準にします。



ご注意

IP スプーフィングは、宛先および送信元の両方の属性に対してハッシュ割り当て方法を使用するサービス グループに対してはサポートされません。そのようなサービス グループに対して IP スプーフィングを有効化すると、アラームが生成され、IP スプーフィングは無効化されます。

5. ルーター情報



ご注意

新しいプロキシ サーバーがサービス グループに追加されたとき、ルーターがそれを報告するまでに最大で 1 分かかります。

- a. セキュリティ オプションの WCCP 認証を使用するには、**[Enabled]** を選択し、ルーター上のサービス グループ認証に使用するのと同じパスワードを入力します。[ルーター上での WCCP v2 セキュリティの有効化, 64 ページ](#) を参照してください。
- b. マルチキャスト マルチキャスト モードで実行するには、**[Enabled]** を選択し、マルチキャスト IP アドレスを入力します。マルチキャスト IP アドレスは、ルーター上で指定されているマルチキャスト IP アドレスと一致していなければなりません。[透過的遮断とマルチキャストモード, 71 ページ](#) を参照してください。



重要

GRE パケットの Forward/Return 方法はマルチキャスト モードでは使用できません。

- c. **WCCP ルーター**: 最大 10 個の WCCP ルーター IP アドレスを指定します。これらのルーターは、対応するサービス グループと合わせて構成しなければなりません。GRE が Packet Forward Method または Packet Return Method に選択されている場合は、各ルーターの仮想 IP アドレスと、ゲートウェイの IP アドレスも指定します。仮想 IP アドレスは一意でなければなりません。



ご注意

WCCP ルーターに複数の IP アドレスが設定されている場合 - たとえばルーターが複数の VLAN をサポートするように設定されている時 - **[Monitor] > [Networking] > [WCCP]** の統計で報告される IP アドレスが、ここで設定される IP アドレスを異なる場合があります。これは、ルーターが常に最も高いアクティブ IP アドレスにおけるトラフィックを報告するからです。

ルーターが常に同じ IP アドレスを報告するようにする 1 つの方法は、ルーターのループバック アドレスをルーターの最も高い IP アドレスよりも高い値に設定することです。それによってループバック アドレスが常にルーターの IP アドレスとして報告されるようになります。この設定を使用することを推奨します。

6. **[Add]** をクリックしてエントリを追加するか、または **[Set]** をクリックして既存のエントリへの変更を保存します。

7. [Close] をクリックして、エディタを閉じます。
8. [Configure] > [Networking] > [WCCP] ページで [Apply] をクリックして変更を適用します。[Apply] をクリックする前に別のページへ移動すると、すべての変更が失われます。
9. プロキシを再起動して変更を有効にします。[Configure] > [My Proxy] > [Basic] > [General] の順に選択して、[Restart] をクリックします。



ご注意

ルーターがプロキシにトラフィックを送信していることを確認するために、Content Gateway Manager の「Monitor」ペインの統計を調べます。たとえば、[My Proxy] > [Summary] セクションの [Objects Served (処理されたオブジェクト)] の統計値が増えていることを確認します。

透過的遮断とマルチキャスト モード

Content Gateway がマルチキャスト モードで実行するように設定するには、マルチキャスト モードを有効化し、Content Gateway Manager でマルチキャスト IP アドレスを指定します。



重要

GRE パケットの Forward/Return 方法はマルチキャスト モードでは使用できません。

さらに、ルーター上で、遮断する各サービス グループ (HTTP、FTP、DNS、SOCKS) に対してマルチキャスト アドレスを設定しなければなりません。以下の手順は、WCCP v2 対応のルーター上で異なるサービス グループにマルチキャスト アドレスを設定する方法の例です。

1. Telnet でルーターに接続し、Enable モードに切り換えます。
2. プロンプトに対して、下記のコマンドを入力して、端末からルーターを設定します。

```
configure terminal
```

3. プロンプトが表示された時に、ルーターが遮断する各サービス グループに対して下記のコマンドを入力します。

```
hostname(config)# ip wccp service_group group-address  
multicast_address
```

ここで *hostname* は設定しているルーターのホスト名、*service_group* はサービス グループ ID (たとえば、HTTP の場合は 0)、*multicast_address* は IP マルチキャスト アドレスです。

4. プロンプトに対して、下記のコマンドを入力して、ネットワーク インターフェイスを設定します。

```
interface interface_name
```

ここで *interface_name* は、ルーター上の、遮断されリダイレクトされるネットワーク インターフェースです。

5. プロンプトが表示された時に、ルーターが遮断する各サービス グループに対して下記のコマンドを入力します。

```
hostname(config-if)# ip wccp service_group group-listen
```

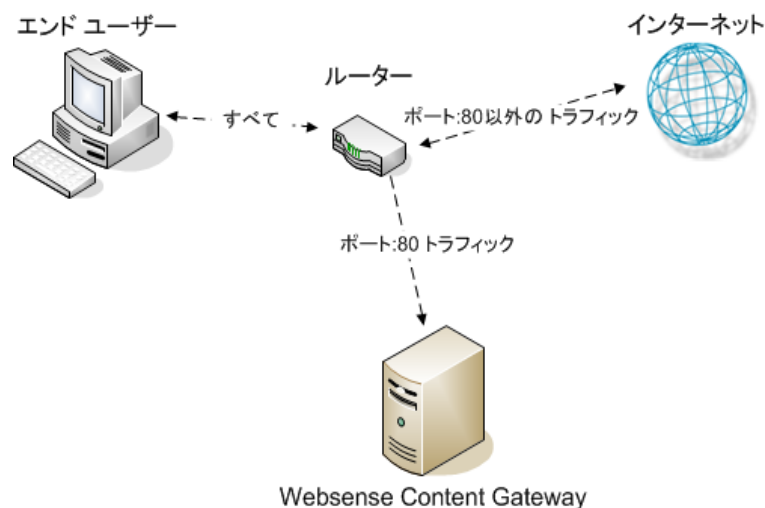
6. ルーター設定を終了し、保存します。

ポリシー ベースのルーティングによる透過的遮断

WCCP プロトコルの代わりに、ルーターのポリシー ルーティング機能を使用して Content Gateway へトラフィックを送信することができます。一般的には、この設定には WCCP またはレイヤー 4 スイッチを使用するのが適切です。なぜなら、ポリシー ベースのルーティングはルーターの処理能力に影響を及ぼし、また、ポリシー ベースのルーティングはロードバランシングやハートビート メッセージングをサポートしないからです。

- ◆ クライアントのすべてのインターネット トラフィックは、Content Gateway に接続しているルーターに送信されます。
- ◆ ルーターはポート 80 (HTTP) トラフィックをプロキシに送信し、残りのトラフィックを次のホップ ルーターに送信します。
- ◆ ARM は、遮断された要求を Content Gateway 要求に変換します。
- ◆ 変換された要求はプロキシへ送信されます。
- ◆ 透過的に処理する Web オブジェクトは、ARM によって、クライアントへの返送パス上でアドレス変更されます。それによってドキュメントはオリジン サーバーから送信されたように見えます。

仮想 IP フェールオーバー機能を持つ Content Gateway クラスタは、信頼性を高めます。一方のノードが停止したとき、他方のノードがその透過要求を引き受けます。[仮想 IP フェールオーバー](#), [89 ページ](#) を参照してください。



ソフトウェア ベースのルーティングによる透過的遮断

Content Gateway ノード上でルーティング ソフトウェアを使用することによって、ルーターまたはスイッチを追加することなしに Content Gateway を配備できます。この場合、Content Gateway はソフトウェア ルーターで、すべてのトラフィックをプロキシ コンピュータを通じて転送します。このソリューションは、プロキシ コンピュータをルーターとして使用した場合の処理能力への影響がそれほど大きくないような低トラフィック環境で便利です。

Linux システムでは、**routed** および **gated** デーモンをソフトウェア ベースのルーティング ソリューションとして使用できます。**routed** デーモンは、通常のすべての Linux 配布のバンドルされている部分です。**gated** デーモンは、Merit GateD Consortium からの包括的な商業用ソフトウェア パッケージです。

ルーティング ソフトウェアを Content Gateway と合わせて使用すると、下記のようになります。

- ◆ すべてのインターネット トラフィックは、ネットワーク内の Content Gateway の背後にあるコンピュータから Content Gateway を通過します。
- ◆ ルーティング ソフトウェアは、すべての非透過的要求をインターネットにルーティングします。このソフトウェアはポート 80 HTTP 要求をプロキシ キャッシュにルーティングします。
- ◆ ARM は、遮断された要求をプロキシ要求に変換します。
- ◆ 変換された要求はプロキシへ送信されます。
- ◆ 透過的に処理する Web オブジェクトは、ARM によって、クライアントへの返送パス上でアドレス変更されます。それによってオブジェクトはオリジン サーバーから送信されたように見えます。



ご注意

Content Gateway コンピュータはルーターとして機能しますが、明示的にルーターとして設計されているわけではありません。信頼性を高めるために、Content Gateway クラスタと仮想 IP フェールオーバー オプションを合わせて使用することができます。一方のノードが停止した場合に、他方のクラスタ ノードが代替します。[仮想 IP フェールオーバー, 89 ページ](#) を参照してください。) Content Gateway クラスタのフェールオーバーのメカニズムは Hot Standby Router Protocol (HSRP) と似ています。

遮断の迂回

一部のクライアントおよびサーバーは Web プロキシを使用する時に正しく機能しません。この問題の原因として以下のことが考えられます。

- ◆ クライアント ソフトウェアが通常のソフトウェアでない (カスタマイズされている、非商業用ブラウザ)。

- ◆ サーバー ソフトウェアが通常のソフトウェアでない。
- ◆ アプリケーションがセキュリティ上の制限を回避する方法として、HTTP ポート上で非 HTTP トラフィックを送信する。
- ◆ サーバー IP アドレスの認証（オリジン サーバーがアクセスを一部のクライアント IP アドレスに制限しているが、Content Gateway IP アドレスが異なるために、そのクライアント IP アドレスがサーバーにアクセスできない）。この方法は頻繁には用いられていません。なぜなら、多くの ISP はクライアントの IP ダイアルアップ アドレスを動的に割り当てており、現在ではもっと安全な暗号化プロトコルが、より一般的に使用されるようになっているからです。

Web プロキシは企業ネットワークやインターネットでは非常に一般的に使用されていますから、相互運用性の問題は稀です。しかし、Content Gateway は、透過的プロキシ処理によって起こる相互運用性の問題を認識し、オペレーターの介入なしにトラフィックが自動的にプロキシ サーバーを迂回するようにする適応学習モジュールを備えています。

Content Gateway は 2 つのタイプのバイパス ルールに従います。

- ◆ **動的**（「適応型」とも言います）バイパス ルールは、Content Gateway がポート 80 で非 HTTP トラフィックを検出した、または何らかの HTTP エラーが発生した時にキャッシュを迂回するように設定している場合に、動的に生成されます。[動的バイパス ルール, 74 ページ](#) を参照してください。
- ◆ **静的**バイパス ルールは、`bypass.config` ファイルで手動で設定しなければなりません。[静的バイパス ルール, 76 ページ](#) を参照してください。



ご注意

ARM バイパス ルールとクライアント アクセス制御リストを混同しないでください。バイパス ルールは、相互運用性の問題に対応するために作成されます。クライアント アクセス制御は、[プロキシへのクライアント アクセスの制御, 183 ページ](#)で説明しているように、単にプロキシにアクセスできるクライアントの IP アドレスを制限するだけです。

動的バイパス ルール

関連項目

- ◆ [動的バイパス ルールの設定, 75 ページ](#)
- ◆ [動的バイパス統計の表示, 76 ページ](#)

プロキシは、プロトコルの相互運用性のエラーを監視します（そうするように設定されている場合）。プロキシはエラーを検出したとき、ARM がエラーの原因となったクライアントとサーバーに対してプロキシを迂回するように設定します。

これによって、プロキシで正常に処理されない一部のクライアントまたはサーバーが自動的に検出され、プロキシ キャッシング サーバーを迂回するようになり、継続的に機能できるようになります（ただしキャッシュに入れることはできません）。

下記のいずれかのエラーが発生した時にプロキシが動的に自分を迂回するように設定することができます。

エラー コード	説明
N/A	ポート 80 上の非 HTTP トラフィック
400	不適切な要求
401	無許可
403	禁止（認証に失敗）
405	メソッドが許可されていない
406	許可されない（アクセス）
408	要求の時間切れ
500	内部サーバー エラー

たとえば、Content Gateway が認証失敗 (**403 Forbidden**) 時に迂回するように設定されている場合、オリジン サーバーへのいずれかの要求が 403 エラーを返した時、Content Gateway はオリジン サーバーの IP アドレスに対する宛先バイパス ルールを生成します。プロキシを再起動するまで、そのオリジンサーバーへのすべての要求は迂回されます。

もう 1 つの例として、クライアントがポート 80 上で特定のオリジン サーバーへの非 HTTP 要求を送信している時、Content Gateway は送信元 / 宛先ルールを生成します。そのクライアントからオリジン サーバーへのすべての要求は迂回され、他のクライアントからの要求は迂回されません。

動的に生成されたバイパス ルールは、Content Gateway が再起動したときにページされます。動的に生成されたルールを残しておきたい場合は、現在のバイパス ルールのセットのスナップショットを保存することができます。[現在のバイパス ルールのセットの表示, 77 ページ](#)を参照してください。

Content Gateway が特定の IP アドレスを動的に迂回しないようにするために、`bypass.config` ファイルで動的バイパス拒否ルールを設定することができます。バイパス拒否ルールは、プロキシが自分を迂回することを禁止できます。動的バイパス拒否ルールの設定の詳細については、[bypass.config, 372 ページ](#)を参照してください。

動的バイパス ルールの設定

デフォルトでは、Content Gateway は HTTP エラーが発生した場合や、ポート 80 上で非 HTTP トラフィックが検出された場合に、自分を迂回するようには設定されていません。適当なオプションを設定することによって動的バイパス ルールを有効化しなければなりません。

1. [Configure] > [Networking] > [ARM] > [Dynamic Bypass (動的バイパス)] を順に選択します。
2. [Dynamic Bypass] ボタンを有効化します。
3. [Behavior (動作)] のセクションで、使用する動的バイパス ルールを選択します。
4. [適用] をクリックします。
5. [Configure] > [My Proxy] > [Basic] > [General] タブで [Restart] をクリックします。

動的バイパス統計の表示

Content Gateway は動的バイパスのトリガーの種類別に、迂回された要求を集計します。たとえば、Content Gateway は 401 エラーに対応して迂回されたすべての要求をカウントします。

- u [Monitor] > [Networking] > [ARM] の順に選択します。

この統計はテーブルの [HTTP Bypass Statistics (HTTP バイパス統計)] のセクションに表示されます。

静的バイパス ルール

特定のクライアントからの要求や、特定のオリジン サーバーへの要求を、プロキシを迂回して転送するためのルールを設定できます。動的バイパス ルールはプロキシを再起動したときにパーズされますが、静的バイパス ルールは設定ファイルに保存されます。

3 つのタイプの静的バイパス ルールを設定できます。

- ◆ 送信元バイパス。Content Gateway は特定の送信元 IP アドレスまたは IP アドレスの範囲を迂回します。たとえば、このソリューションを使って、キャッシュ ソリューションを回避したいクライアントを迂回することができます。
- ◆ 宛先バイパス。Content Gateway は特定の宛先 IP アドレスまたは IP アドレスの範囲を迂回します。たとえば、クライアントの実際の IP アドレスを基に IP 認証を使用するオリジン サーバーを迂回できます。宛先バイパス ルールは Content Gateway がサイト全体をキャッシュするのを防止します。迂回したサイトが人気のあるサイトである場合、ヒット率への影響が顕著に表れます。
- ◆ 送信元 / 宛先ペアのバイパスでは、Content Gateway は指定した送信元から指定した宛先への要求を迂回します。たとえば、IP 認証が破られた、または帯域外の HTTP トラフィックの問題があるクライアント / サーバー ペアを迂回することができます。

送信元 / 宛先バイパス ルールは、宛先サーバーを、問題が発生した特定のユーザーに対してのみブロックしますから、宛先バイパス ルールよりも適切です。

静止バイパス ルールを設定するには、`bypass.config` ファイルを編集します ([bypass.config, 372 ページ](#)を参照)。

現在のバイパス ルールのセットの表示

ARM `print_bypass` という名前のサポート ユーティリティがあり、それによって現在の動的および静的バイパス ルールを表示することができます。

現在のすべての動的および静的バイパス ルールを表示します。

1. Content Gateway ノードにログオンし、次に、ディレクトリを Content Gateway bin directory (`/opt/WCG/bin`) に変更します。
2. プロンプトに対して下記のコマンドを入力し、**[Return]** をクリックします。

```
./print_bypass
```

現在のすべての静的および動的バイパス ルールが画面に表示されます。ルールは IP アドレスによってソートされています。`print_bypass` の出力をファイルに転送して、保存することができます。

接続負荷の軽減

負荷軽減機能は、クライアント要求の過負荷を防止します。クライアント接続の数が指定されている限度を超えたとき、ARM は着信した要求を直接にオリジン サーバーに転送します。デフォルトのクライアント接続の数は 100 件です。

1. **[Configure]** > **[Networking]** > **[Connection Management (接続管理)]** > **[Load Shedding (負荷の削減)]** の順に選択します。
2. **[Maximum Connections (最大接続)]** フィールドで、許可されるクライアント接続の最大数を指定します。この数を超えると ARM は要求を直接にオリジン サーバーに転送しはじめます。
3. **[適用]** をクリックします。
4. **[Configure]** > **[My Proxy]** > **[Basic]** > **[General]** の順に選択し、**[Restart]** をクリックします。

DNS ルックアップの削減

Content Gateway を透過プロキシ モードで実行している場合、*[Always Query Destination (常に宛先を照会する)]* オプションを有効化することによって DNS ルックアップの数を減らし、応答時間を改善することができます。Always Query Destination オプションが有効化されている時、プロキシは常に ARM から着信する要求の元の宛先 IP アドレスを取得するように設定されます。この場合、Content Gateway は、要求のホスト名について DNS ルックアップを実行するのではなく、その IP アドレスを使ってオリジン サーバー

を判別します。クライアントがすでに DNS ルックアップを実行していますから、Content Gateway は DNS ルックアップを実行する必要はありません。



ご注意

Content Gateway が明示および透過の両方のプロキシ モードで実行している場合、Always Query Destination オプションを有効化しないことを推奨します。Content Gateway を透過プロキシ モードのみで実行する方法については、[Content Gateway が透過的要求のみを処理するように設定するにはどうすればよいですか](#)、[486 ページ](#)を参照してください。明示のプロキシ モードでは、クライアントはオリジン サーバーのホスト名について DNS ルックアップを実行しませんから、プロキシが DNS ルックアップを実行しなければなりません。また、カテゴリー ルックアップは IP アドレスを基に実行されます。これは常に URL ベースのルックアップと同等に正確であるとは限りません。

また、IP アドレスではなくドメイン名をログ サーバーにキャプチャーする場合は、Always Query Destination オプションを有効化してはいけません。

Always Query Destination オプションを有効化するには、以下の手順を実行します。

1. Content Gateway の **config** ディレクトリ (`/opt/WCG/config`) の **records.config** ファイルを開きます。
2. 下記の変数を編集します。

変数	説明
<code>proxy.config.arm.always_query_dest</code>	Always Query Destination オプションを無効化するには、0 に設定します。ドメイン名がキャプチャーされます。 Always Query Destination オプションを有効化するには、1 に設定します。IP アドレスがキャプチャーされます。ドメイン名はキャプチャーされません。

3. ファイルを保存して閉じます。
4. 変更を適用するために、Content Gateway の **bin** ディレクトリで下記のコマンドを実行します。

```
content_line -x
```

IP スプーフィング

IP スプーフィングでは、プロキシは、オリジン サーバーと通信する時に、プロキシ自身の IP アドレスではなくクライアントの IP アドレスを使用する

ように構成されます。その結果、要求はプロキシからではなくクライアントから発行されたように示されます。

- ◆ IP スプーフィングは HTTP および HTTPS トラフィックに対してのみサポートされています。
- ◆ IP スプーフィングが有効化されているとき、HTTP と HTTPS の両方に適用されます。1つのプロトコルにのみ適用するように設定することはできません。
- ◆ IP スプーフィングは透過的トラフィックに対してのみサポートされています。
- ◆ IP スプーフィングには ARM が必要です。



警告

IP スプーフィングを配備するためには、ネットワーク上のルーティングパスを正確に制御する必要があり、TCP ポート 80 および 443 上で実行する通常のルーティングプロセスを無効にする必要があります。

IP スプーフィングを有効化している時、従来のデバッグツール（例、`traceroute`、`ping`）の用途は限られます。

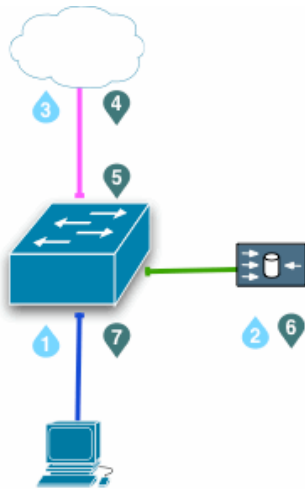


重要

プロキシ カーネル ルーティング テーブルが透過的プロキシ環境に及ぼす影響については、Solution Center に掲載されている「Web sites in the Static or Dynamic bypass list fail to connect (静的または動的バイパス リストに含まれる web サイトに接続できない)」というタイトルの記事を参照してください。

IP スプーフィングとトラフィックのフロー

以下は、WCCP で IP スプーフィングを使用している時の HTTP および HTTPS トラフィックのフローを説明しています。ポリシー ベースのルーティングを導入することによって同じ結果を得ることもできます。図の中の番号は、番号付きのリストで説明している動作に対応しています。



1. クライアント要求が、経路指定されているポート、または、宛先ポートが HTTP (80) または HTTPS (443) であるトラフィックを探している Switched Virtual Interface (SVI) に到達します。
2. スイッチはクライアント要求を Content Gateway (プロキシ) へリダイレクトし、Content Gateway は内部的にトラフィックを自分の IP アドレスのポート 8080 (HTTP) または 8070 (HTTPS) へ経路指定します。
必要な場合、プロキシは元のクライアント IP アドレスを使用して Web のオリジン サーバーへの接続を作成します。
3. 要求はスイッチ、NAT、および (または) ファイアウォールを通じて Web のオリジン サーバーへ送信されます。
4. オリジン サーバーの応答が返されたとき、IP パケットにはクライアント IP アドレスが宛先として使用されています。
5. オリジン サーバーの応答が、経路指定されているポート、または、送信元ポートが HTTP (80) または HTTPS (443) であるトラフィックを探している Switched Virtual Interface (SVI) に到達します。下の注記を参照してください。
6. スイッチはオリジン サーバーの応答をプロキシにリダイレクトし、プロキシから Web サーバーへの TCP 接続を完了します。
7. クライアントへのプロキシ応答が生成され、プロキシからクライアントへの TCP 接続を通じてクライアントへ返されます。



ご注意

IP スプーフィングが有効化されている時、プロキシはそれぞれの有効化されている WCCP サービスに対して、リバース サービス グループを公告します。リバース サービス グループは、プロキシのリターン パスに適用されなければなりません。

WCCP サービス グループ ID はユーザー定義であり、WCCP デバイス上、および Content Gateway 内でプログラミングされていなければなりません ([WCCP デバイス上のサービス グループを設定](#) および [Content Gateway Manager でのサービス グループの設定](#)を参照)。

以下は推奨する定義のセットです。

サービス ID	ポート	トラフィック タイプ
0	宛先ポート 80	HTTP
20	送信元ポート 80	HTTP
70	宛先ポート 443	HTTPS (SSL Manager が必須)
90	送信元ポート 443	HTTPS

ポリシー ベースのルーティング (PBR) は、アクセス制御リスト (ACL) を使ってフローを識別し、リダイレクトします。PBR 環境では、すべてのシステム設定はルーター上で行われ、対応する Content Gateway 側の設定はありません。PBR 環境は、オリジン サーバーのポート 80 および 443 から返されるトラフィックを Content Gateway にリダイレクトしなければなりません。

IP スプーフィングの有効化

1. [Configure] > [Networking] > [ARM] > [General] の順に選択します。
2. [IP Spoofing] を選択します。
3. [適用] をクリックします。
4. [Configure (設定)] > [My Proxy (マイ プロキシ)] > [Basic (基本)] > [General (一般)] で [Restart (再起動)] をクリックします。



警告

ARM は Content Gateway の不可欠のコンポーネントであり、無効化してはいけません。IP スプーフィングを有効化している時に ARM が無効化されている場合、クライアント要求は [cannot display Web page (web ページを表示できない)] エラーを受け取り、エラー メッセージが /var/log/messages に記録されます。

WCCP ルーターの設定については、[WCCP v2 ルーターの構成, 59 ページ](#) を参照してください。

6

クラスタ

関連項目

- ◆ [SSL 管理クラスタ化, 85 ページ](#)
- ◆ [クラスタ構成の変更, 86 ページ](#)
- ◆ [クラスタへのノードの追加, 87 ページ](#)
- ◆ [クラスタからのノードの削除, 89 ページ](#)
- ◆ [仮想 IP フェールオーバー, 89 ページ](#)

Websense Content Gateway は 1 つのノードから 15 以上のノードのクラスタまで拡張可能であり、迅速に容量を拡大し、システムの処理能力と信頼性を向上させることができます。

- ◆ Content Gateway はクラスタ内のノードの追加および削除を検出し、ノードが停止した時にそれを検出できます。
- ◆ いつでもクラスタ内のノードを追加または削除できます。
- ◆ ノードをクラスタから除去したとき、Content Gateway は除去したノードへのすべての参照を除去します。
- ◆ クラスタ内の 1 つのノードを再起動すると、クラスタ内のすべてのノードが再起動します。
- ◆ [仮想 IP フェールオーバー](#) 機能が有効化されている時、クラスタ内のアクティブなノードが、停止しているノードのトラフィックを引き受けることができます。
- ◆ クラスタ内のノードは自動的に設定情報を共有します。



ご注意

Filtering Service および Policy Service の IP アドレスはクラスタ全体には適用されません。

WCCP での透過的プロキシ環境では、サービスグループの有効/無効状態はクラスタ全体には適用されません。[WCCP v2 デバイスによる透過的遮断, 55 ページ](#) を参照してください。

Content Gateway はクラスタ化のための専用プロトコルを使用します。これはノード検出用にはマルチキャストされ、クラスタ内のすべてのデータ交換用にはユニキャストされます。



重要

Content Gateway クラスタ通信には専用のネットワーク インターフェースを使用することを推奨しますが、**例外として**、ホストが V シリーズ アプライアンスである場合には P1 (eth0) インターフェースを推奨します。



重要

プロキシの階層の中で、クラスタ内のノードに HTTP の親と子が混在することはできません。Content Gateway クラスタの各ノードは階層の中の単一ノードとして構成しなければなりません。なぜなら、それは共通の構成を共有するからです。

管理クラスタ化

管理クラスタ化モードでは、すべての Content Gateway ノードを同時に管理することができます。なぜなら、クラスタ ノードは構成情報を共有するからです。



ご注意

クラスタ内のノードの数は、15 以上です。

配備環境の拡張については、Websense のアカウント担当者にご相談ください。

- ◆ Content Gateway は、クラスタ内のすべてのノードについて 1 つのシステム イメージを維持するために、マルチキャスト管理プロトコルを使用します。
- ◆ クラスタのメンバー、構成、例外に関する情報は、すべてのノードで共有されます。
- ◆ `content_manager` プロセスは、構成変更をクラスタ内のノードに適用します。
- ◆ SSL Manager が有効化されている時、SSL 構成をクラスタ全体に適用できますが、そのためには異なるメカニズムを使用します。次のセクションを参照してください。

SSL 管理クラスタ化

クラスタ内で SSL Manager が有効化されている時、SSL 構成情報をクラスタ全体に適用できますが、そのためには異なるメカニズムを使用し、それを別途に設定する必要があります。

SSL Manager が構成情報をクラスタ全体に適用するように設定するには、1 つのノードを、すべての SSL 構成変更を行うプライマリー ノードとして選択しなければなりません。プライマリー ノードは **SSL Manager Configuration Server** と呼ばれます。他のすべてのノードは **セカンダリー** です。

- ◆ プライマリー ノードで行われた設定はセカンダリー ノードにも適用されます。
- ◆ セカンダリー ノードは定期的にプライマリー ノードをポーリングして、未適用の変更がないか調べます。未適用の変更があれば、各セカンダリー ノードがそれをプルダウンします。
- ◆ セカンダリー ノードで変更が行われた場合、それらの変更はプライマリー ノードからマスター構成がプルダウンされた時に上書きされます。
- ◆ プライマリー ノードが停止した場合、アラームが生成され、セカンダリー ノードはプライマリー ノードが復旧するか、新しいプライマリー ノードが構成されるまで、その現在の構成で動作を継続します。

SSL Manager クラスタ化が設定されている時、以下の構成設定がクラスタ全体に適用されます。

- ◆ プライマリー ノードの IP アドレス
- ◆ [Configure] > [SSL] > [Certificates (証明書)] > [Certificate Authorities (証明機関)]
- ◆ [Configure] > [SSL] > [Certificates] > [Add Root CA (ルート CA の追加)]
- ◆ [Configure] > [SSL] > [Certificates] > [Restore Certificates (復旧証明書)]
- ◆ [Configure] > [SSL] > [Decryption / Encryption: all settings (復号化 / 暗号化: すべての設定)]
- ◆ [Configure] > [SSL] > [Validation: all settings (確認: すべての設定)]
- ◆ [Configure] > [SSL] > [Client Certificates: all settings (クライアント証明書: すべての設定)]
- ◆ [Configure] > [SSL] > [ロギング: all settings (ロギング: すべての設定)]
- ◆ [Configure] > [SSL] > [Internal Root CA (内部ルート CA)] > [Import Root CA (ルート CA のインポート)]
- ◆ [Configure] > [SSL] > [Internal Root CA] > [Create Root CA (ルート CA の作成)]
- ◆ 動的に生成された証明書およびインシデント

SSL 管理クラスタ化の設定

1. 管理クラスタ化を設定および開始します。[クラスタ構成の変更](#)を参照してください。
2. クラスタ内のいずれかのノードで、Content Gateway Manager にログオンします。
3. **[Configure] > [My Proxy] > [Basic] >** を順に選択し、「**Clustering (クラスタ化)**」タブを選択します。
4. **[SSL Manager Configuration Server]** フィールドで、SSL Manager Configuration Server (プライマリー ノード) の IP アドレスを入力します。このフィールドが編集可能でなければ、このシステムはクラスタのメンバーではありません。
5. **[Apply]** をクリックして Content Gateway を再起動します。すべての Content Gateway ノードが再起動します。再起動によって、プライマリー ノードがすべてのクラスタ メンバーに認識され、SSL クラスタ化がアクティブになります。

この設定は、「**Monitor**」>「**My Proxy**」>「**Summary (要約)**」ページの **[Node Details (ノードの詳細)]** セクションの下部で確認できます。**SSL Manager Configuration Server** の IP アドレスがリンクである場合、サーバーはクラスタ内の別のノードです。リンクをクリックして **SSL Manager Configuration Server** にログオンします。

クラスタ構成の変更

クラスタ化は通常、プロキシをインストールする時に設定されます。しかし、あとで、いつでも、Content Gateway Manager でクラスタ化を設定できます。

1. Content Gateway Manager で、**[Configure] > [My Proxy] > [Basic] >** を順に選択し、「**Clustering**」タブを選択します。
2. **[Cluster Type (クラスタ タイプ)]** 領域で、クラスタ化モードを選択します。
 - このプロキシをクラスタに含める場合は、**[Management Clustering (管理クラスタ化)]** を選択します。
 - このプロキシをクラスタに含めない場合は、**[Single Node (単一ノード)]** を選択します。
3. **[Cluster Interface (クラスタ インターフェース)]** 領域で、ネットワーク インターフェースの名前を入力します。これは Content Gateway がクラスタ内の他のノード (例、eth0) との通信に使用するインターフェースです。専用のセカンダリー インターフェースを使用することを推奨します。ノード構成情報は、プレーン テキストとして、同じサブネット中の他の Content Gateway ノードにマルチキャストされます。したがって、Websense は、クライアントを Content Gateway ノードから独立したサブネット上に配置する (クラスタ化のためのマルチキャスト通信はルーティングされません) ことを推奨します。

V シリーズ アプライアンス上では、P1 (eth0) が推奨インターフェースです。しかし、クラスタ管理トラフィックを隔離したい場合には、P2 (eth1) を使用してもかまいません。

4. **[Cluster Multicast Group Address (クラスタ マルチキャスト グループ アドレス)]** 領域で、クラスタの全メンバーが共有するマルチキャスト グループ アドレスを入力します。
5. **SSL Manager** を使用していて、SSL 構成情報をクラスタ全体に適用したい場合、SSL Manager Configuration Server の IP アドレスを入力します。クラスタ内では、SSL 構成情報は別のメカニズムによって管理されます。この機能を効果的に使用するためには、このメカニズムに習熟していなければなりません。[SSL 管理クラスタ化](#) を参照してください。
6. **[適用]** をクリックします。
7. **[Configure (設定)] > [My Proxy (マイ プロキシ)] > [Basic (基本)] > [General (一般)]** で **[Restart (再起動)]** をクリックします。



重要

Content Gateway はクラスタ化モードの変更を、クラスタ内のすべてのノードには適用しません。各ノードのクラスタ化モードを個別に変更しなければなりません。

クラスタへのノードの追加

Content Gateway はネットワーク上で新しい Content Gateway ノードを検出し、それをクラスタに追加し、新しいクラスタ メンバーに最新の構成情報を適用します。これによって新しいコンピュータのブートストラップを簡単に行うことができます。

ノードを Content Gateway クラスタに接続するための操作は、新しいノード上に Content Gateway ソフトウェアをインストールすることだけです。この時、クラスタ名とポート割り当てが既存のクラスタのそれと同じであることを確認してください。これによって Content Gateway は自動的に新しいノードを認識します。



重要

クラスタ内のノードは均質でなければなりません。つまり、各ノードは同じハードウェア プラットフォーム上にあり、オペレーティング システムの同じバージョンを使用しており、Content Gateway が同じディレクトリ (/opt/WCG) にインストールされていなければなりません。

1. 適切なハードウェアをインストールし、それをネットワークに接続します。(ハードウェアのインストールの方法については、ハードウェアのマニュアルを参照してください。)

2. クラスタ ノードをインストールするための適切な手順を使用して Content Gateway ソフトウェアをインストールします。詳細については、『*Content Gateway インストール ガイド*』を参照してください。インストール手順の中で、以下の条件が満たされていることを確認してください。
 - 新しいノードに割り当てるクラスタ名が、既存のクラスタのクラスタ名と同じである。
 - 新しいノードのポート割り当てが、クラスタ内の他のノードで使用するポート割り当てと同じである。
 - マルチキャスト アドレスとマルチキャスト経路設定を追加した。
3. Content Gateway の再起動 [コマンドラインでの Content Gateway の起動および停止, 18 ページ](#) を参照してください。

すでに Content Gateway がインストールされていて、そのサーバーをクラスタに追加する場合、ノード上に Content Gateway を再インストールする必要はありません。代わりに、既存の Content Gateway ノード上の構成変数を編集することができます。

1. クラスタに追加するノード上で、`/opt/WCG/config` 中の `records.config` ファイルを開きます。
2. 下記の変数を編集します。

変数	説明
<code>proxy.local.cluster.type</code>	クラスタ モードを指定します。 2 = 管理モード 3 = クラスタ化しない
<code>proxy.config.proxy_name</code>	Content Gateway クラスタの名前を指定します。クラスタ内のすべてのノードは同じ名前を使用しなければなりません。
<code>proxy.config.cluster.mc_group_addr</code>	クラスタ通信のためのマルチキャスト アドレスを指定します。クラスタ内のすべてのノードは同じマルチキャスト アドレスを使用しなければなりません。
<code>proxy.config.cluster.rsport</code>	信頼できるサービス ポートを指定します。信頼できるサービス ポートはクラスタ内のノード間でデータを送信するために使用します。クラスタ内のすべてのノードは同じ信頼できるサービス ポートを使用しなければなりません。デフォルト値は 8087 です。

変数	説明
<code>proxy.config.cluster.mcport</code>	マルチキャスト ポートを指定します。マルチキャスト ポートの値は、ノードの識別のために使用します。クラスタ内のすべてのノードは同じマルチキャスト ポートを使用しなければなりません。デフォルトポート番号は 8088 です。
<code>proxy.config.cluster.ethernet_interface</code>	クラスタ トラフィックのためのネットワーク インターフェイスを指定します。クラスタ内のすべてのノードは同じネットワーク インターフェイスを使用しなければなりません。

3. ファイルを保存して閉じます。
4. Content Gateway を再起動します (`/opt/WCG/WCGAdmin restart`)。

管理モードから単一モードへ、またはその逆の変更

1. Content Gateway Manager にアクセスします。
2. **[Configure]** > **[My Proxy]** > **[Basic]** > **[Clustering]** の順に選択します。
3. **[Cluster Type]** 領域で、適当なタイプ (**[Single]** または **[Management]**) を選択します。
4. **[適用]** をクリックします。
5. **[Configure]** > **[My Proxy]** > **[Basic]** > **[General]** で **[Restart]** をクリックします。

クラスタからのノードの削除

クラスタから除去するノードで、以下の手順を実行します。

1. **[Configure]** > **[My Proxy]** > **[Basic]** > **[Clustering]** の順に選択します。
2. **[Cluster Type]** 領域で、**[Single Node]** を選択します。
3. **[適用]** をクリックします。
4. **[Configure]** > **[My Proxy]** > **[Basic]** > **[General]** で **[Restart]** をクリックします。

仮想 IP フェールオーバー

仮想 IP フェールオーバー機能によって、Content Gateway は必要に応じてクラスタ内のノードに割り当てる仮想 IP アドレスのプールを維持します。これらのアドレスは仮想です。つまり、特定のコンピュータに関連付けられているわけではありません。Content Gateway はそれを任意のノードに割り当てることができます。クラスタの外に対しては、これらの仮想 IP アドレスは Content Gateway サーバーのアドレスです。

仮想 IP フェールオーバーによって、クラスタ内の 1 つのノードが停止しても、他のノードが停止したノードの役割を引き受けることができます。Content Gateway は仮想 IP フェールオーバーを以下の方法で処理します。

- ◆ **content_manager** プロセスはクラスタ通信を維持します。ノードは自動的に、マルチキャスト通信を通じて統計情報および構成情報を交換します。いずれかのクラスタ ノードからマルチキャスト ハートビートが受信されない場合、他のノードはそのノードが使用不能であると認識します。
- ◆ **content_manager** プロセスは、約 30 秒以内に、停止しているノードの IP アドレスを残りのアクティブなノードに再割り当てし、それによってサービスが中断なしに継続できるようにします。
- ◆ IP アドレスが新しいネットワーク インターフェースに割り当てられ、新しい割り当てがローカル ネットワークにブロードキャストされます。IP の再割り当ては *ARP リバインド* と呼ばれる処理を通じて行われます。

仮想 IP アドレスとは？

関連項目

- ◆ [仮想 IP アドレス指定の有効化と無効化, 90 ページ](#)
- ◆ [仮想 IP インターフェースの追加と編集, 91 ページ](#)

仮想 IP アドレスは、特定のコンピューターに結合されていない IP アドレスです。したがって、これらのアドレスは Content Gateway クラスタ内のノード間で持ち回りで使用できます。

1 台のコンピューターが同じサブネット上の複数の IP アドレスを持つことは、よくあることです。このコンピューターは、そのインターフェースカードに関連付けられているプライマリー、または実 IP アドレスを持ち、また、多くの仮想アドレスに対応できます。

ユーザー ベースが、Content Gateway コンピューターの実 IP アドレスを使用するのではなく、仮想 IP アドレスへの DNS ラウンドロビン ポインティングを使用するようにセットアップすることができます。

仮想 IP アドレスは特定のコンピューターに結合されていませんから、Content Gateway クラスタは、非アクティブのノードからアドレスを取り上げ、それを残りのアクティブなノードの間で配分することができます。

専用の管理プロトコルを使って Content Gateway ノードはそのステータスを、ピアのノードに通知することができます。ノードが停止したとき、そのピアのノードはそれを認識し、残りのノードのうちのどれが、停止したノードの仮想インターフェースを引き継ぐことによって障害をマスクするかを折衝します。

仮想 IP アドレス指定の有効化と無効化

1. **[Configure]** > **[My Proxy]** > **[Basic]** > **[General]** の順に選択します。

2. [Features (機能)] テーブルの [Networking (ネットワーキング)] セクションで、[Virtual IP (仮想 IP)] に対して [On] または [Off] を選択して仮想 IP を有効化または無効化します。
3. [適用] をクリックします。
4. [Configure] > [My Proxy] > [Basic] > [General] で [Restart] をクリックして、クラスタ内のすべてのノード上で Content Gateway を再起動します。

仮想 IP インターフェースの追加と編集

仮想 IP アドレスは、他のすべての IP と同様に、Content Gateway に割り当てる前に事前予約されていなければなりません。



警告

不適切な IP アドレス指定の結果、システムが使用不能になることがあります。必ず、仮想 IP アドレスを変更する前に、仮想 IP アドレスの仕組みを理解しておいてください。

1. [Configure] > [Networking] > [Virtual IP] の順に選択します。
[Virtual IP Addresses] 領域は、Content Gateway によって管理される仮想 IP アドレスを表示します。



ご注意

[Virtual IP] ボタンは、[Configure] > [My Proxy] > [Basic] > [General] の [Features] テーブルで [Virtual IP] オプションを有効化した場合にだけ表示されます。

2. 新しい仮想 IP アドレスを追加するか、既存の仮想 IP アドレスを編集するために、[Edit File (ファイルの編集)] をクリックします。
3. 仮想 IP アドレスを編集するには、ページ上部のテーブルからそれを選択し、表示されたフィールドを編集し、[Set (設定)] をクリックします。
選択した IP アドレスを削除するには、[Clear Fields (フィールドの消去)] をクリックします。
仮想 IP アドレスを追加するには、表示されたフィールドに仮想 IP アドレス、イーサネット インターフェース、およびサブインターフェースを指定し、[Add (追加)] をクリックします。
4. [Apply] をクリックし、次に [Close] をクリックします。
5. [Configure] > [My Proxy] > [Basic] > [General] で [Restart] をクリックします。

7

階層キャッシング

Websense Content Gateway を [HTTP キャッシュ階層](#), 93 ページ に組み込むことができます。そこでは、あるキャッシュで処理されなかったインターネット要求を他のリージョナル キャッシュにルーティングでき、そのキャッシュのコンテンツと要求元からの近接性を活用することができます。

キャッシュ階層は、相互に交信する複数のレベルのキャッシュによって成り立っています。Content Gateway は、いくつかのタイプのキャッシュ階層をサポートしています。すべてのキャッシュ階層は親と子という概念を認識します。親キャッシュは階層の上位のキャッシュであり、プロキシはこれに対して要求を転送することができます。子キャッシュは、プロキシを親とするキャッシュです。

HTTP キャッシュ階層

HTTP キャッシュ階層では、Content Gateway ノードが要求されたオブジェクトを自分のキャッシュで見出せないとき、そのオブジェクトをオリジン サーバーから取得する前に親キャッシュで探すことができ、またこの親キャッシュは他のキャッシュで探すことができます。

1 つ以上の HTTP 親キャッシュを使用するように Content Gateway ノードを構成し、ある親が利用できないとき、別の親が要求に対応できるようにする

ことができます。これは親フェイルオーバーといい、その説明は [親フェイルオーバー](#)、[94 ページ](#) にあります。



ご注意

すべての要求が親キャッシュに向かうのを避けるために、`parent.config` 構成ファイル ([parent.config, 393 ページ](#) 参照) で親プロキシルールを設定することにより、プロキシが特定の要求 (特定の URL を含む要求など) をオリジンサーバーに直接にルーティングするように構成することができます。



ご注意

要求されたコンテンツが親キャッシュでキャッシュされていない場合、親はそのコンテンツをオリジンサーバー (または、親の構成によっては、別のキャッシュ) から取得します。親はコンテンツをキャッシュし、次にコピーをプロキシ (その子) に送り、この送り先でそれはキャッシュされ、クライアントに提供されます。

親フェイルオーバー

プロキシが複数の親キャッシュを使用するように構成されているとき、プロキシは、ある親が利用できないことを検出すると、処理されなかった要求を別の親キャッシュに送ります。3 つ以上の親キャッシュが指定されているとき、それらの親キャッシュが問い合わせを受ける順序は親の設定ファイル中で構成されている親プロキシルール ([parent.config, 393 ページ](#) 参照) によって異なります。デフォルトでは、親キャッシュに対する問い合わせは親の設定ファイルでそれらがリストされている順序に従って行われます。

HTTP 親キャッシュを使用する Content Gateway の構成

1. [Configure (構成)] > [Content Routing (コンテンツ ルーティング)] > [Hierarchies (階層)] > [Parenting (親)] ページで [Parent Proxy (親プロキシ)] を有効にします。
2. [Edit File (ファイルの編集)] をクリックして、[parent.config](#) ファイルの編集のために設定ファイル エディタを開きます。
3. 表示されるフィールドに情報を入力し、[Add (追加)] をクリックします。すべてのフィールドについて、[Hierarchies \(階層\), 315 ページ](#) で説明しています。
4. [Apply (適用)] をクリックし、次に [Close (閉じる)] をクリックします。

5. [Parenting] タブで [Apply] をクリックして、設定ファイルを保存します。



重要

子プロキシ上でこの手順を実行します。親について、いかなる変更もしないでください。

8

キャッシュの構成

キャッシュは、オブジェクトストアと呼ばれる高速オブジェクト データベースから成ります。オブジェクト ストアは、URL および関連付けられているヘッダに従ってオブジェクトのインデックスを作成し、Websense Content Gateway が Web ページおよび Web ページの一部を保存、取得、および提供できるようにし、最大限の帯域幅の節約を可能にします。オブジェクト ストアは、オブジェクト管理を使用して、同じオブジェクトの代替バージョン（言語または暗号化タイプが異なる）をキャッシュすることができ、また大小のドキュメントを保存でき、無駄なスペースを最小限にします。キャッシュがいっぱいになると、Content Gateway は陳腐化したデータを除去します。

Content Gateway は、キャッシュ ディスク上のディスク障害を許容します。ディスクが壊れると、Content Gateway はそのディスクを「破損」としてマークし、残りのディスクを引き続き使用します。壊れたディスクを明示するアラームが Content Gateway Manager に送られます。すべてのキャッシュ ディスクが壊れると、Content Gateway はプロキシ専用モードに移行します。

下記のようなキャッシュ構成設定タスクを行なうことができます：

- ◆ インストール後にキャッシュ ディスクを追加する。[インストール後のキャッシュ ディスクの追加, 98 ページ](#) を参照してください。
- ◆ キャッシュに割り当てられているディスク スペースの総容量を変更する。[キャッシュ容量の変更, 99 ページ](#) を参照してください。
- ◆ キャッシュ ディスク スペースを特定のプロトコル、オリジン サーバー、ドメインなどに予約して、キャッシュをパーティションに区分する。[キャッシュのパーティション区分, 101 ページ](#) を参照してください。
- ◆ キャッシュで許容されるオブジェクトのサイズの限度を指定する。[キャッシュ オブジェクトのサイズ制限, 104 ページ](#) を参照してください。
- ◆ キャッシュ中のすべてのデータを削除する。[キャッシュのクリア, 104 ページ](#) を参照してください。
- ◆ RAM キャッシュのサイズを変更する。[RAM キャッシュのサイズ変更, 104 ページ](#) を参照してください。

RAM キャッシュ

Content Gateway には、非常によくアクセスされるオブジェクトの小さな RAM キャッシュがあります。この RAM キャッシュは最もよくアクセスされるオブジェクトをすばやく提供し、特にトラフィック ピーク時にディスクの

負荷を軽減します。RAM キャッシュ サイズは設定可能です。[RAM キャッシュのサイズ変更](#), [104 ページ](#) を参照してください。

インストール後のキャッシュ ディスクの追加

キャッシュ ディスクを追加するには、下記のものが必要です：

- ◆ 未フォーマットの物理ディスク デバイス (OS インストールによって作成されます)。サイズ (バイト数) を書き留めておきます。
- ◆ raw キャラクタ デバイス (mknod によって作成されます)

デバイスを追加するには、物理ディスクを raw キャラクタ デバイスにマッピングしなければなりません。

以下の例では、ほとんどの場合、HP DL360 とその RAID コントローラのコマンドを扱っています。(すべてのディスクは RAID 0 です。)

1. raw デバイスをセットアップし、パーミッションを変更します：

```
mknod /etc/udev/devices/raw c 162 0
chmod 600 /etc/udev/devices/raw
```

2. キャッシュ ディスク物理デバイス名を確認し、サイズ (バイト数) を書き留めておきます (後で使用します)：

```
fdisk -l | grep "^Disk"
Disk /dev/cciss/c0d1: 146.7 GB, 146778685440 bytes
```

3. ノードを作成し、そのノードの所有者を変更し、その raw ノードを物理ディスクにマッピングします。追加されるディスクごとに最後の引数が 1 だけインクリメントすることに注意してください：

```
mknod /etc/udev/devices/raw_c0d1 c 162 1 デバイス名を fdisk -l コマンドによって返されたデバイス名に変えることができます。
chown Websense /etc/udev/devices/raw_c0d1 mknod ステートメントで使用したデバイス名を使用します。
chown Websense /etc/udev/devices/raw_c0d1 mknod ステートメントで使用したデバイス名を使用します。
```

4. 再起動によって変更を有効にし、同じ `/usr/bin/raw` コマンドを `/etc/init.d/content_gateway` の 6 行目に追加します：

```
...
case "$1" in
'start')
/usr/bin/raw /etc/udev/devices/raw_c0d1 /dev/cciss/c0d1 mknod ステートメントで使用したデバイス名を使用します。
...

```

5. `fdisk -l` によって戻された raw ノードとサイズ (ブロック数) を使用して、デバイスを `/opt/WCG/config/storage.conf` に追加します：

```
/etc/udev/devices/raw_c0d1 146778685440
mknod ステートメントで使用したデバイス名を使用します。
```


6. キャッシングが有効になっていることを確認します。インストール時にキャッシュディスクがセットアップされていないと、キャッシングは無効になります：
 - a. Content Manager で **[Configure]** > **[Protocols]** > **[HTTP]** へ進み、**[Cacheability (キャッシュ機能)]** タブをクリックします。
 - b. **[HTTP Caching (HTTP キャッシング)]** で **[Enabled (有効)]** を選択します。
 - c. **[Apply]** をクリックし、Content Gateway を再起動します。

キャッシュ容量の変更

全体のディスク キャッシュの最大サイズは 147 GB です。このサイズはシステム リソースの最大限の活用を実現し、またエンドユーザーに快適な環境を提供します。

ディスク キャッシュの最小サイズは 2 GB です。

関連項目：

- ◆ [キャッシュ サイズの確認, 99 ページ](#)
- ◆ [キャッシュ容量の増加, 99 ページ](#)
- ◆ [キャッシュ容量の削減, 100 ページ](#)

キャッシュ サイズの確認

構成されている全体のキャッシュ サイズを調べるには、Content Manager を開き、**[Monitor (モニタ)]** > **[Subsystems (サブシステム)]** > **[Cache (キャッシュ)]** に進みます。**[Cache Size (キャッシュ サイズ)]** フィールドの **[Current Value (現在の値)]** 列で、キャッシュ サイズ (バイト数) を確認できます。

あるいは、Content Gateway の bin ディレクトリ (`/opt/WCG/bin`) から下記のコマンドを実行して、キャッシュ サイズを表示します：

```
content_line -r proxy.process.cache.bytes_total
```

キャッシュ容量の増加

既存のディスク上でキャッシュに割り当てられている総ディスク スペースを増加するか、または Content Gateway ノードに新しいディスクを追加するには、下記の手順を実行します：

1. Content Gateway を停止します。[コマンドラインでの Content Gateway の起動および停止, 18 ページ](#) を参照してください。
2. 必要であれば、ハードウェアを追加します。
 - a. raw デバイスをセットアップし、パーミッションを変更します：例：

```
mknod /etc/udev/devices/raw c 162 0
chmod 600 /etc/udev/devices/raw
```

- b. キャッシュ ディスク物理デバイス名を確認し、サイズ（バイト数）を書き留めておきます（後で使用します）: 例:

```
fdisk -l | grep "^Disk"
```

```
Disk /dev/cciss/c0d1: 146.7 GB, 146778685440 bytes
```

- c. 実際のディスクの 1 つ 1 つについて、それぞれノードを作成し、そのノードの所有者を変更し、その raw ノードを物理ディスクにマッピングします。追加されるディスクごとに最後の引数が 1 だけインクリメントすることに注意してください:

ノードを作成するには、次のコマンドを実行します:

```
mknod /etc/udev/devices/raw_c0d1 c 162 1
```

デバイス名を、ステップ b で `fdisk -l` コマンドから戻された名前に変更することができます。

所有者を変更するには、次のコマンドを実行します:

```
chown Websense /etc/udev/devices/raw_c0d1
```

所有者はインストール ユーザーです（デフォルトは Websense です）。`mknod` ステートメントで使用されているデバイス名を使用します。

raw ノードを物理ディスクにマッピングするには、次のコマンドを実行します:

```
/usr/bin/raw /etc/udev/devices/raw_c0d1 /dev/cciss/c0d1
```

`mknod` ステートメントで使用されているデバイス名を使用します。

- d. 同じ `/usr/bin/raw` コマンドを `/etc/init.d/content_gateway` ファイルに追加し、変更が再起動により有効になるようにします。例えば、6 行目において下記の追加を行います:

```
...
case "$1" in
'start')
/usr/bin/raw /etc/udev/devices/raw_c0d1 /dev/cciss/c0d1
```

- Content Gateway `config` ディレクトリ (`/opt/WCG/config`) 中の `storage.config` ファイルを編集し、既存のディスク上のキャッシュに割り当てられているディスク スペースの容量を増加するか、または新しいディスク デバイスを追加します。[storage.config, 464 ページ](#) を参照してください。
- Content Gateway を再起動します。

キャッシュ容量の削減

既存のディスク上のキャッシュに割り当てられているディスク スペースの総容量を削減するか、または Content Gateway ノードからディスクを除去することができます。

- Content Gateway を停止します。
- 必要であれば、ハードウェアを除去します。

3. `storage.config` ファイルを編集して、既存のディスク上のキャッシュに割り当てられているディスク スペースの容量を削減するか、または除去しようとするハードウェアへの参照を削除します。[storage.config, 464 ページ](#) を参照してください。
4. ディスクを除去する場合は、`/etc/rc.d/init.d/content_gateway` ファイルを編集して、そのディスクの raw ディスク バインドを除去しなければなりません。
5. Content Gateway を再起動します。

**重要**

`storage.config` ファイル中で、フォーマット済みディスクまたは raw ディスクは少なくとも 2 GB でなければなりません。

キャッシュのパーティション区分

個々のプロトコルに対応する異なるサイズのキャッシュパーティションを作成することによって、キャッシュ スペースを効率的に管理し、ディスクの使用状況を改善することができます。特定のオリジン サーバーやドメインからのデータを保存するためのパーティションを構成することもできます。

**重要**

HTTP が現時点でサポートされている唯一のプロトコルです。

**重要**

パーティション構成は、クラスタ中のすべてのノードで同一でなければなりません。

プロトコルに対応するキャッシュ パーティションの作成

個々のプロトコルに基づいてコンテンツを保存する個別のパーティションをキャッシュで作成することができます。この構成によって、特定のプロトコルのために一定のディスク スペースを確保できるようになります。

**重要**

HTTP が現時点でサポートされている唯一のプロトコルです。

Content Gateway Manager で下記の手順を実行します：

1. [Configure] > [Subsystems] > [Cache] > [Partition (パーティション)] タブに進みます。
2. [Cache Partition (キャッシュパーティション)] エリアで [Edit File (ファイルの編集)] をクリックして、`partition.config` ファイルのための設定ファイル エディタを開きます。
3. 表示されるフィールドに情報を入力し、[Add (追加)] をクリックします。すべてのフィールドについて、[Cache \(キャッシュ\), 337 ページ](#) で説明しています。
4. [Apply] をクリックして情報を保存し、次に [Close] をクリックします。

パーティション サイズとプロトコルの変更

プロトコルに基づくキャッシュパーティションを作成したら、その構成をいつでも変更できます。変更する前に、下記のことにご注意してください：

- ◆ キャッシュ サイズとプロトコル割り当てを変更する前に、Content Gateway を停止しなければなりません。
- ◆ パーティションのサイズを大きくするとき、パーティションのコンテンツは削除されません。しかし、パーティションのサイズを小さくするとき、パーティションのコンテンツが削除されます。
- ◆ パーティション番号を変更するとき、サイズとプロトコルタイプに変更がなくても、パーティションは削除され、つづいて再作成されます。
- ◆ 新しいディスクを Content Gateway ノードに追加するとき、パーセンテージで指定されているパーティション サイズは比例的に大きくなります。
- ◆ パーティション サイズを何度も変更するとディスクが断片化し、そのためパフォーマンスとヒット率に影響します。キャッシュパーティションのサイズを何度も変更する前に、キャッシュをクリアすべきでしょう ([キャッシュのクリア, 104 ページ](#) を参照してください)。

オリジン サーバーまたはドメインに基づくキャッシュのパーティション区分

サイズとプロトコルに基づいてキャッシュをパーティションに区分したら、それらのパーティションを特定のオリジン サーバーとドメインに割り当てることができます。

1つのパーティションを単一または複数のオリジン サーバーに割り当てることができます。しかし、1つのパーティションを複数のオリジン サーバーに割り当てると、そのキャッシュで各オリジン サーバーが利用できるスペースについて問題が発生するかもしれません。コンテンツは使用頻度に基づいてパーティションに保存されます。

特定のオリジン サーバーとドメインにパーティションを割り当てただけでなく、リストされないすべてのオリジン サーバーとドメインからのコンテンツを保存するための汎用パーティションを割り当てなければなりません。この

汎用パーティションは、特定のオリジン サーバーまたはドメインのためのパーティションが破損した場合にも使用されます。



重要

汎用パーティションを割り当てないと、Content Gateway プロキシ専用モードで動作します。



ご注意

特定のホストまたはドメインにパーティションを割り当てる前に Content Gateway を停止する必要は**ありません**。しかし、この種の構成タスクはメモリの使用状況にスパイクをもたらす可能性があり、その作業は時間がかかります。パーティション割り当ての構成タスクはトラブルシューティングが少ないときに行うべきでしょう。

ホスト名とドメインに基づくキャッシュのパーティション区分は Content Gateway Manager で行なうことができます。

Content Gateway Manager では、下記の手順になります：

1. [parent.config, 393 ページ](#) の説明に従って、サイズとプロトコルに基づくキャッシュパーティションを構成します。

各ホストおよびドメインについてプロトコル (HTTP のみ) に基づく個別のパーティションと、それらのオリジン サーバーまたはドメインに属しないコンテンツで使用される汎用パーティションを作成しなければならない。例えば、2つの異なるオリジン サーバーからそれぞれ別個のコンテンツが必要であると、少なくとも3つの異なるパーティションを作成しなければなりません：各オリジン サーバーのためのそれぞれ1つの HTTP ベースパーティションと他のすべてのオリジン サーバーのための汎用パーティション（これらのパーティションは同じサイズでなくても結構です）。

2. **[Configure]** タブで **[Subsystems]** をクリックし、次に **[Cache]** をクリックします。
3. **[Hosting (ホスティング)]** タブをクリックし、**[Cache Hosting (キャッシュホスティング)]** エリアで **[Edit File]** をクリックして、**hosting.config** ファイルのための設定ファイル編集エディタを開きます。
4. 表示されるフィールドに情報を入力し、**[Add]** をクリックします。すべてのフィールドについて、[Cache \(キャッシュ\), 337 ページ](#) で説明しています。
5. **[Apply]** をクリックし、次に **[Close]** をクリックします。

キャッシュ オブジェクトのサイズ制限

デフォルトでは、Content Gateway はキャッシュであらゆるサイズのオブジェクトを許容します。このデフォルト動作を変更し、キャッシュ中のオブジェクトについてサイズの制限を指定することができます。

1. **[Configure]** > **[Subsystems]** > **[Cache]** > **[General]** を選択します。
2. **[Maximum Object Size (最大オブジェクト サイズ)]** フィールドで、キャッシュで許容されるオブジェクトの最大サイズ(バイト数)を入力します。サイズ制限を設けない場合は、0(ゼロ)を入力します。
3. **[Apply]** をクリックします。

キャッシュのクリア

キャッシュをクリアすると、ホスト データベースのデータを含めて、すべてのデータがキャッシュ全体から除去されます。パーティション区分のようなキャッシュ構成タスクを行う前に、キャッシュをクリアします。



ご注意

Content Gateway が動作していると、キャッシュのクリアはできません。

1. Content Gateway を停止します。[コマンドラインでの Content Gateway の起動および停止, 18 ページ](#) を参照してください。
2. 次のコマンドを入力して、キャッシュをクリアします:

```
content_gateway -Cclear
```



警告

clear コマンドは、オブジェクト ストアとホスト データベースのすべてのデータを削除します。Content Gateway は削除の確認を求めません。

3. Content Gateway を再起動します。

RAM キャッシュのサイズ変更

Content Gateway は、頻繁に使用される小さなオブジェクトの迅速な取得のために専用の RAM キャッシュを用意しています。デフォルトの RAM キャッシュ サイズは、すでに構成されているパーティションの数とサイズに基づい

て算出されます。RAM キャッシュのサイズを大きくすることによって、キャッシュのヒット パフォーマンスを改善することができます。



警告

RAM キャッシュのサイズを大きくして、Content Gateway パフォーマンスの低下（遅延の増大など）が認められる場合、オペレーティング システムがネットワーク リソースのためにメモリの増大を必要としている可能性があります。RAM キャッシュ サイズを以前の大きさに戻します。



ご注意

プロトコルまたはホストに基づいてキャッシュがパーティションに区分されている場合、各パーティションに対応する RAM キャッシュのサイズはそのパーティションのサイズと比例します。

1. **[Configure]** > **[Subsystems]** > **[Cache]** > **[General]** を選択します。
2. **[Ram Cache Size (RAM キャッシュ サイズ)]** フィールドで、RAM キャッシュに割り当てようとするスペースの容量（メガバイト）を入力します。ユーザー インターフェイスは大きな値を受け入れますが、**512 MB を上まわらないようにしてください**。
デフォルトのサイズは 104857600 (100 MB) です。



ご注意

値を“-1”にすると、Content Gateway は RAM キャッシュのサイズをディスク キャッシュ 1 GB につき約 1 MB にします。

3. **[Apply]** をクリックします。
4. **[Configure]** > **[My Proxy]** > **[Basic]** > **[General]** で **[Restart (再起動)]** をクリックします。

9

DNS プロキシ キャッシング

通常、クライアントは DNS 要求を DNS サーバーに送り、ホスト名を解決しようとしています。しかし、DNS サーバーがしばしば過負荷状態になったり、またクライアントから遠く離れている場合があります、そのために DNS ルックアップが遅くなったり、要求の達成にとってボトルネックになることがあります。

DNS プロキシ キャッシング オプションにより、Content Gateway がクライアントに代わって DNS 要求を解決することができます。このオプションによって、リモート DNS サーバーの負荷が軽減され、DNS ルックアップの応答時間が短くなります。



重要

DNS プロキシ キャッシング オプションはレイヤー 4 (L4) スイッチ、または WCCP v2 を実行している Cisco ルータでだけ利用できます。

以下の概要は、Content Gateway が DNS 要求を処理する方式を示しています。

1. クライアントが DNS 要求を出します。この要求は、ポート 53 上のすべての DNS トラフィックを Content Gateway にリダイレクトするように構成されているルータまたは L4 スイッチによって捕捉されます。
2. ARM がその DNS パケットを調べます。DNS 要求が**タイプ A** (応答) であると、ARM はその要求を Content Gateway に転送します。ARM は、**タイプ A** でないすべての DNS 要求を DNS サーバーに転送します。
3. Content Gateway はその DNS キャッシュをチェックし、当該 DSN についてホスト名 /IP アドレスのマッピングがあるかどうかについて調べます。そのマッピングが DNS キャッシュにあると、Content Gateway はその IP アドレスをクライアントに送ります。マッピングが DNS キャッシュにないと、Content Gateway はホスト名を解決するために DNS サーバーと通信します。Content Gateway が DNS サーバーから応答を受け取ると、ホスト名 /IP アドレス マッピングをキャッシングし、その IP アドレスをク

クライアントに送ります。ラウンドロビンが使用されていると、Content Gateway は IP アドレス マッピングのリスト全体をクライアントに送り、ラウンドロビンの順序が厳格に守られます。



ご注意

ホスト名 /IP アドレス マッピングが DNS キャッシュにないと、Content Gateway は `/etc/resolv.conf` ファイルで指定されている DNS サーバーと通信します。このサーバーは、当初において DNS 要求で予定されていた DNS サーバーとは異なるものになるでしょう。

DNS キャッシュはメモリで維持され、ディスクでバックアップされます。Content Gateway は 60 秒毎にディスク上のデータを更新します。TTL (残り寿命) は、あらゆるホスト名 /IP アドレス マッピングで厳格に守られます。

DNS プロキシ キャッシングの構成

Content Gateway を DNS プロキシ キャッシュとして構成するには、下記の手順を実行します：

- ◆ `ipnat.conf` ファイルに `remap` ルールを追加します。
- ◆ DNS プロキシ オプションを有効にし、Content Gateway が DNS プロキシ トラフィックで使用するポートを指定します。



重要

DNS プロキシ キャッシング オプションは、レイヤー 4 (L4) スイッチ、または WCCP v2 を実行している Cisco ルーターでだけを利用できます。

Content Gateway Manager で下記の手順を実行します：

1. **[Configure]** > **[Networking (ネットワーク)]** > **[ARM]** > **[General]** タブへ進みます。
2. **[Network Address Translation (ネットワーク アドレス変換: NAT)]** セクションで **[Edit File]** をクリックして、`ipnat.conf` ファイルのためにファイル エディタを開きます。
3. 表示される各フィールドで情報を入力します：
 - **[Ethernet Interface (イーサネット インターフェース)]** フィールドで、クライアント DNS 要求がルーティングされる Content Gateway イーサネット インターフェースを入力します。例、`eth0`。
 - **[Connection Type (接続のタイプ)]** ドロップダウン リストで `udp` を選択します。

- [Original Destination IP (元の宛先 IP アドレス)] フィールドで **0.0.0.0** と入力し、すべてのクライアントからの DNS 要求を受け入れます。
 - [Original Destination CIDR (元の宛先 CIDR)] フィールド (オプション) で CIDR マスク値を入力します。[Original Destination IP] フィールドで 0.0.0.0 を指定している場合は、ここで '0' を入力します。
 - [Original Destination Port (元の宛先ポート)] フィールドで、DNS 要求が Content Gateway に送られるとき使用されるポートを入力します。デフォルトのポートは 53 です。
 - [Local Client IP (ローカル クライアント IP)] フィールドで Content Gateway の IP アドレスを入力します。
 - [Local Client Port (ローカル クライアント ポート)] フィールドで、Content Gateway が DNS サーバーとの通信で使用するポートを入力します。デフォルトのポートは 5353 です。
 - [User Protocol (ユーザー プロトコル)] ドロップダウン リストで **dns** を選択します。
4. [Add] をクリックし、次に [Apply] をクリックし、さらに [Close] をクリックします。
 5. [My Proxy] > [Basic] に移り、[Features (機能)] テーブルで [Networking] セクションの [DNS Proxy] を有効にして、[Apply] をクリックします。
 6. [Networking] > [DNS Proxy] に移ります。
 7. [DNS Proxy Port (DNS プロキシ ポート)] フィールドで DNS プロキシ ポートを入力します。デフォルトのポートは 5353 です。
 8. [Apply] をクリックし、Content Gateway を再起動します。

10

システムの構成

Websense Content Gateway は、システムを構成するための複数のオプションを提供します。

- ◆ [Content Gateway Manager](#), 111 ページ
- ◆ [コマンドライン インターフェイス](#), 115 ページ
- ◆ [設定ファイル](#), 116 ページ
- ◆ [構成の保存と復元](#), 117 ページ

構成を変更したときは必ず Content Gateway を再起動しなければなりません。

Content Gateway Manager

Content Gateway Manager は、Content Gateway を構成するための Web ベースのユーザー インターフェイスを提供します。



ご注意

一部のオプションは、`records.config` ファイルで、またはコマンドライン インターフェイスから設定変数の編集によってのみ変更できます。[コマンドライン インターフェイス](#), 115 ページ および [設定ファイル](#), 116 ページ を参照してください。

Content Gateway Manager へのログインの手順については、[Content Gateway Manager へのアクセス](#), 11 ページ を参照してください。

設定モードの使用

デフォルトでは、Content Gateway Manager は、モニタ モードで開きます。

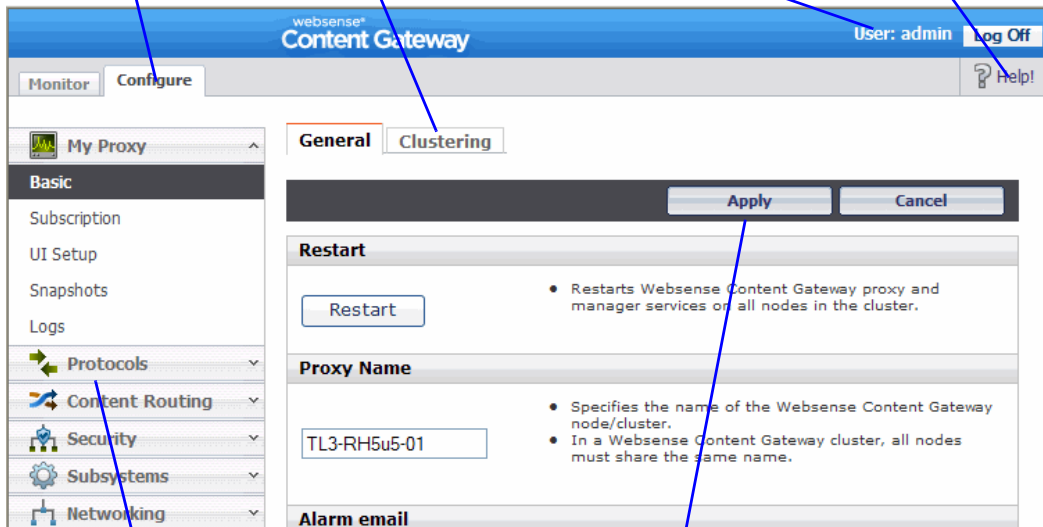
設定モードのボタンを表示するには、**[Configure (設定)]** タブをクリックします。

[Configure] ボタンを表示するには、このタブをクリックします。

より多くのオプションを表示するには、このタブをクリックします。

Content Gateway Manager にログインしている現在のユーザーを表示します。

オンラインヘルプシステムを表示するには [Help! (ヘルプ!)] をクリックします。



当該の設定オプションを表示するには、ボタンをクリックします。

設定の変更を現在のタブに保存するには、**[Apply (適用)]** をクリックします。

設定モードでは、Content Gateway Manager は、一連のボタンを表示します。各ボタンは、設定オプションのグループを表します。

設定モードで利用可能なすべての設定オプションについては、[設定のオプション](#)で説明しています。

My Proxy (マイ プロキシ)

- ◆ **[Basic (基本)]** は、プロキシおよびマネージャ サービスの再起動 (一部の設定オプションは、変更後に再起動する必要があります)、Content Gateway ノードの名前の指定、アラーム電子メールの設定、および種々の機能 (FTP 処理、プロキシ ユーザー認証、WCCP、クラスタ オプションなど) の有効化または無効化を行う時に使用します。
- ◆ **[Subscription (サブスクリプション)]** はサブスクリプション キーを表示する時に使用します。サブスクリプションのキーおよびスキャンのオプションの詳細については、Web Security Manager のヘルプ システムを参照してください。Content Gateway が Data Security Suite とのみ統合されている場合は、入力フィールドに Data Security サブスクリプション キーを入力します。
- ◆ **[UI Setup (UI の設定)]** は、ブラウザが Content Gateway Manager との接続に使用するポートを指定および変更する時、Content Gateway Manager

への SSL 接続を有効化する時、Content Gateway Manager が [Monitor (モニタ)] タブの統計を更新する頻度を指定する時、および Content Gateway Manager とのアクセスを確保するためにアクセス制御リスト、管理者アカウント、およびユーザー アカウントを設定する時に使用します。

- ◆ 構成のスナップショットを撮るおよび復元するには、[Snapshots (スナップショット)] をクリックします。
- ◆ [Logs (ログ)] は、選択したログ ファイルを表示する、削除する、またはローカル ファイル システムへコピーする時に使用します。

Protocols (プロトコル)

- ◆ [HTTP] は、HTTP キャッシングを設定する時、および HTTP タイムアウトを微調整するために使用します。
- ◆ [HTTP Responses (HTTP 応答)] は、プロキシがクライアント トランザクションで HTTP の問題 (オリジン サーバーが利用できない、認証要件、プロトコル エラーなど) を検出した時にクライアントに送信する HTTP 応答を指定するために使用します。
- ◆ [HTTP Scheduled Update (HTTP スケジュール設定した更新)] は、スケジュール設定した時刻にプロキシが特定のオブジェクトをキャッシュにロードするように設定するために使用します。
- ◆ [FTP] は FTP のオプションを設定し、FTP タイムアウトを微調整するために使用します。

FTP のオプションは、FTP のクライアントから発信される要求にのみ影響を与えます。HTTP グループの HTTP クライアントから発信する FTP 要求に影響を与えるオプションを設定できます。[FTP] ボタンは、「Configure (設定)」> 「My Proxy (マイ プロキシ)」> 「Basic (基本)」> 「General (一般)」の [Features (フィーチャ)] テーブルで FTP 処理を有効化した場合だけ、表示されます。

- ◆ [HTTPS] は、インバウンドおよびアウトバウンドの HTTPS トラフィックのポート情報を指定するために使用します。

Content Routing (コンテンツ ルーティング)

- ◆ [Hierarchies (階層)] は、HTTP 親キャッシングを設定する時に使用します。
- ◆ [Mapping and Redirection (マッピングとリダイレクト)] は、URL 再マッピングおよび FTP 再マッピングのルールを設定する時に使用します。
- ◆ [Browser Auto-Config (ブラウザ自動設定)] は、ブラウザ自動設定ファイルをダウンロードするために使用するポートを特定する時や、PAC および WPAD オプションを設定する時に使用します。

Security (セキュリティ)

- ◆ [Connection Control (接続の制御)] は、プロキシへのアクセスを許可するクライアントを指定するために使用します。
- ◆ [FIPS Security (FIPS セキュリティ)] は、HTTPS 接続で FIP 140-2 レベルのセキュリティを有効化するために使用します。

- ◆ **[Access Control (アクセス制御)]** は、フィルタリング ルールおよびプロキシ認証オプション (統合 Windows 認証、複数レルム認証、レガシー NTLM、LDAP、RADIUS) を設定する時に使用します。
- ◆ **[Data Security]** は、Data Security Management Server に登録し、ローカルの Data Security ポリシー エンジンを有効化するために使用します。
- ◆ **[SOCKS]** は、SOCKS ファイアウォールを使用するように Content Gateway を構成する時に使用します。[SOCKS] ボタンは、「**Configure**」>「**My Proxy**」>「**Basic**」>「**General**」の [Features] テーブルで [SOCKS] を有効化した場合だけ表示されます。



ご注意

SOCKS サーバーは、Content Gateway が Websense V - シリーズ アプライアンスにインストールされている場合に Content Gateway と統合されます。

Content Gateway がソフトウェアとして別のサーバーにインストールされている場合、統合された SOCKS サーバーは表示されません。SOCKS を使用するために、別個の SOCKS サーバーが必要です。

Subsystems (サブシステム)

- ◆ **[Cache (キャッシュ)]** は、キャッシュ ピンニングを有効化または無効化する時、RAM キャッシュ サイズを設定する時、キャッシュに入力できるオブジェクトの最大サイズを指定する時、およびプロトコルおよびオリジン サーバーに従ってキャッシュをパーティションに分割する時に使用します。
- ◆ **[Logging (ログ記録)]** は、イベント ロギングを有効化または無効化する時、およびロギング設定オプションを設定する時に使用します。

Networking (ネットワーク)

- ◆ **[Connection Management (接続管理)]** は下記の値を指定する時に使用します。
 - プロキシが受け入れることができる接続の最大数。
 - 透過的プロキシ キャッシングの場合、許可されるクライアント接続の最大数を指定します。この数を超えるとプロキシは要求を直接にオリジン サーバーに転送しはじめます。
 - クライアント同時接続の最大数と、制限から除外されるクライアント。
- ◆ **[ARM]** は、着信パケットを透過的モードでアドレス変更する方法を指定するリダイレクト ルールを設定する時に使用します。また、動的および静的バイパス ルールも設定できます。
- ◆ **[WCCP]** は、WCCP 構成の設定値を設定する時に使用します。[WCCP] ボタンは、「**Configure**」>「**My Proxy**」>「**Basic**」>「**General**」タブの [Features] テーブルで [WCCP] を有効化した場合だけ表示されます。
- ◆ **[DNS Proxy (DNS プロキシ)]** は、DNS プロキシポートを指定する時に使用します。[DNS Proxy] ボタンは、「**Configure**」>「**My Proxy**」>「**Basic**」>

「General」タブの [Features] テーブルで [DNS Proxy] オプションを有効化した場合だけ表示されます。

- ◆ [DNS Resolver (DNS リゾルバ)] は、ローカルドメイン拡張を有効化または無効化する時、ホストデータベースのタイムアウトを微調整する時、および Split DNS のオプションを設定する時に使用します。
- ◆ [Virtual IP (仮想 IP)] は、仮想 IP フェールオーバーを有効化または無効化する時、および Content Gateway ノードによって管理される仮想 IP アドレスを指定する時に使用します。[Virtual IP] ボタンは、「Configure」>「My Proxy」>「Basic」>「General」の [Features] テーブルで、Virtual IP を有効化した場合だけ表示されます。

SSL

- ◆ [Certificates (証明書)] は、認証機関ツリーを表示する時に使用します。その証明書の詳細情報を表示するには、該当するエントリをクリックします。
- ◆ [Decryption/Encryption (復号化/暗号化)] は、SSL Manager がインバウンドとアウトバウンドのトラフィックを処理する方法を設定する時に使用します。インバウンドトラフィックはブラウザから SSL Manager に転送され、そこでコンテンツが復号化され、検査されます。アウトバウンドトラフィックは SSL Manager から宛先 Web サーバーに転送されます。SSL Manager は、サイト証明書の取り消しステータスをチェックしてから、再暗号化したデータをサイトに転送します。
- ◆ [Validation (確認)] は、証明書の確認を設定する時、証明書が無効である場合に行う動作を指定する時、確認バイパスを設定する時、および証明書取り消しリストの処理を設定する時に使用します。
- ◆ [Incidents (インシデント)] は、クライアントがアクセス拒否メッセージを受け取った事象のレポートを表示するため、および許可する URL、ブラックリストに入れる URL、またはトンネリングする URL を指定するために使用します。
- ◆ [Client Certificates (クライアント証明書)] は、SSL Manager がクライアント証明書の要求を処理する方法を設定する時に使用します。
- ◆ [Logging (ログ記録)] は、SSL ログインレベル、ログインの詳細情報、ログファイル名、およびログファイル処理を選択する時に使用します。
- ◆ [Customization (カスタム化)] は、証明書確認の失敗メッセージをカスタム化するために使用します。
- ◆ [Internal Root CA (内部ルート CA)] は、内部ルート認証機関をインポート、作成、またはバックアップする時に使用します。

コマンドライン インターフェース

Content Gateway Manager の代わりに、コマンドライン インターフェースを使用して、Content Gateway の構成を表示および変更できます。

1. Content Gateway ノードに root としてログオンし、次に、ディレクトリ変更 ('cd') して Content Gateway bin ディレクトリ (/opt/WCG/bin) に移動します。
2. 構成の設定値を表示するには、下記のコマンドを入力します。

```
content_line -r var
```

ここで、*var* は、設定オプションに関連する変数です（変数のリストについては、[設定変数, 398 ページ](#)を参照）。

3. 構成の設定値を変更するために、下記のコマンドを入力します。

```
content_line -s var -v value
```

ここで、*var* は、設定オプションに関連する変数であり、また *value* は、使用する値です。

たとえば、FTP 非アクティブ タイムアウト オプションを 200 秒に変更するには、プロンプトに対して下記のコマンドを入力し、[Return (戻る)] を押します。

```
content_line -s
proxy.config.ftp.control_connection_timeout -v 200
```



ご注意

Content Gateway bin ディレクトリがパスにない場合、コマンドの先頭に ./ が付きます。/

例：

```
./content_line -r variable
```

設定ファイル

/opt/WCG/config にある records.config ファイルの特定の変数を編集することによって、Content Gateway の設定オプションを変更できます。テキストエディタ (vi、emacs など) でファイルを開き、変数の値を変更します。



ご注意

records.config ファイルを変更した後、Content Gateway は設定ファイルを再読み込みする必要があります。それには、Content Gateway bin ディレクトリ (/opt/WCG/bin) から下記のコマンドを入力します。

```
content_line -x
```

場合によっては、プロキシを再起動し、変更を適用する必要があります。

下記の数字は、**records.config** ファイルのサンプルの部分を示しています。

```
#Id: records.config.v 1.617.2.27 2008/09/16 22:06:35 brilee Exp #
#
# Process Records Config File
#
# <RECORD-TYPE> <NAME> <TYPE> <VALUE (till end of line)>
#
# RECORD-TYPE: CONFIG, LOCAL
# NAME: name of variable
# TYPE: INT, STRING, FLOAT
# VALUE: Initial value for record
#
#####
#
# System Variables
#
#####
CONFIG proxy.config.proxy_name STRING ibid
CONFIG proxy.config.bin_path STRING bin
CONFIG proxy.config.proxy_binary STRING traffic_server
CONFIG proxy.config.proxy_binary_opts STRING -M
CONFIG proxy.config.manager_binary STRING traffic_manager
CONFIG proxy.config.cli_binary STRING traffic_line
CONFIG proxy.config.watch_script STRING traffic_cop
CONFIG proxy.config.env_prep STRING example_prep.sh
CONFIG proxy.config.config_dir STRING config
CONFIG proxy.config.temp_dir STRING /tmp
CONFIG proxy.config.alarm_email STRING inktomi
```

変数名

変数タイプ：整数 (INT)、
文字列 (STRING)、または
浮動小数点 (FLOAT)

編集できる変数値

Content Gateway は、特定の機能を設定するために使用するその他の設定ファイルを提供します。すべて設定ファイルは [設定ファイル, 116 ページ](#) で説明しています。

構成の保存と復元

構成スナップショット機能を使用して、現在のすべての構成の設定値を保存し、必要に応じてそれらを復元できます。Content Gateway は、構成のスナップショットをそれらが撮られるノード、FTP サーバー、およびポータブルメディア上に保存できます。Content Gateway は、クラスタ内のすべてのノード上で構成のスナップショットを復元します。



ご注意

構成のスナップショットを撮ってから、システム保守を実行したり、システムパフォーマンスを微調整することを推奨します。構成のスナップショットを撮るにはほんの数秒ですみます。

このセクションでは、下記のタスクを実行する方法について説明しています。

- ◆ 現在の構成のスナップショットを撮る。[構成のスナップショットを撮る, 118 ページ](#) を参照してください。

- ◆ 以前に撮った構成のスナップショットを復元する。[構成のスナップショットの復元, 118 ページ](#) を参照してください。
- ◆ Content Gateway ノード上に保存されている構成のスナップショットを削除する。[構成のスナップショットの削除, 119 ページ](#) を参照してください。

構成のスナップショットを撮る

現在のすべての構成の設定値を Content Gateway Manager を通じて Content Gateway システムに保存できます。

構成のスナップショットを撮り、それをローカル システムに保存するには、下記の手順を実行します。

1. 「Configure」>「Snapshots (スナップショット)」>「File System (ファイルシステム)」に移動します。
2. [Change Snapshot Directory (スナップショット ディレクトリを変更)] フィールドに、Content Gateway が構成のスナップショットを保存するディレクトリの名前が表示されます。デフォルトの場所は、Content Gateway `config/snapshots` ディレクトリです。ディレクトリを変更するには、[Change Snapshot Directory] フィールドに絶対パスを入力します。絶対パスを入力した場合は、Content Gateway は、そのディレクトリが `config` ディレクトリにあると想定します。
3. [Save Snapshot] フィールドに現在の構成に使用する名前を入力します。
4. [Apply] をクリックします。

構成のスナップショットを撮り、それを FTP サーバーに保存するには、下記の手順を実行します。

1. 「Configure」>「Snapshots」>「FTP Server (FTP サーバー)」に移動します。
2. 表示されたフィールドに、FTP サーバー名、ログイン およびパスワード、および FTP サーバーが構成のスナップショットを保存するリモートディレクトリを入力します。
3. [Apply] をクリックします。
FTP サーバーに正常にログオンした後、「FTP Server」ページに追加のフィールドが表示されます。
4. [Save Snapshot to FTP Server (FTP サーバーにスナップショットを保存)] フィールドに、撮る構成のスナップショットの名前を入力します。
5. [Apply] をクリックします。

構成のスナップショットの復元

Content Gateway サーバーのクラスタを実行している場合、構成はそのクラスタ内のすべてのノードに復元されます。

ローカルノード上に保存されている構成のスナップショットを復元するには、下記の手順を実行します。

1. 「Configure」>「Snapshots」>「File System」タブに移動します。
2. [Restore (復元)]>[Delete Snapshot (スナップショットを削除)] ドロップダウン リストから、復元する構成のスナップショットを選択します。
3. [Restore Snapshot from “directory_name” Directory ('directory_name' ディレクトリからスナップショットを復元)] ボックスをクリックします。
4. [Apply] をクリックします。
Content Gateway システムまたはクラスタは、復元された構成を使用します。

FTP サーバーから構成のスナップショットを復元するには、下記の手順を実行します。

1. 「Configure」>「Snapshots」>「FTP Server」に移動します。
2. 表示されたフィールドに、FTP サーバー名、ログイン およびパスワード、および FTP サーバーが構成のスナップショットを保存するリモートディレクトリを入力します。
3. [Apply] をクリックします。
FTP サーバーに正常にログインした後、「FTP Server」タブに追加のフィールドが表示されます。
4. [Delete Snapshot (スナップショットを削除)] ドロップダウン リストで、復元する構成のスナップショットを選択します。
5. [Apply] をクリックします。
Content Gateway システムまたはクラスタは、復元された構成を使用します。

構成のスナップショットの削除

1. 「Configure」>「Snapshots」>「File System」に移動します。
2. [Restore]>[Delete Snapshot] ドロップダウン リストから、削除する構成のスナップショットを選択します。
3. [Delete Snapshot from “directory_name” Directory ('directory_name' ディレクトリからスナップショットを削除)] ボックスをクリックします。
4. [Apply] をクリックします。
構成のスナップショットが削除されます。

11

トラフィックのモニタリング

Websense Content Gateway は、システム パフォーマンスをモニタし、ネットワーク トラフィックを分析するために下記のツールを提供します。

- ◆ Content Gateway のパフォーマンスとネットワーク トラフィック情報を示す統計。[統計の表示, 121 ページ](#) を参照してください。コマンドライン インターフェイスは、この情報を表示するための代替の方法を提供します。[コマンドラインからの統計の表示, 124 ページ](#) を参照してください。
- ◆ 検出したエラー条件を知らせるアラーム。[アラームの処理, 125 ページ](#) を参照してください。
- ◆ Content Gateway のパフォーマンスとネットワーク トラフィックの履歴情報を示すパフォーマンス グラフ。[パフォーマンス グラフの使用, 127 ページ](#) を参照してください。
- ◆ 認証機関およびインシデントのステータスを確認するために SSL Manager を通じて生成されたレポート。[SSL Manager によるレポートの作成, 128 ページ](#) を参照してください。

統計の表示

Content Gateway のパフォーマンスおよび Web トラフィックに関する統計を収集し、解釈するために、Content Gateway Manager を使用します。モニタモードを使用して統計を表示します。

Content Gateway Manager へのログ オンの手順については、[Content Gateway Manager へのアクセス, 11 ページ](#) を参照してください。

モニタ モードの使用

モニタ モードの場合、Content Gateway Manager は、ディスプレイの左側に一連のボタンを表示します。統計を表示するには、ボタンをクリックします。

モニタ モードで表示されるすべての統計の詳細については、[統計, 259 ページ](#) を参照してください。

My Proxy (マイプロキシ)

Content Gateway に関する統計を表示するには、**[My Proxy (マイ プロキシ)]** をクリックします。

- ◆ Content Gateway システムの簡潔なビューを表示するには、**[Summary (要約)]** をクリックします。ページの上部は、有効期限を含む、Websense Web Security Gateway サブスクリプションの機能に関する情報を表示します。ページの間部分には、使用中のスキャンエンジンとそれに関連するデータ ファイルに関する情報を表示します。ページの下部は、プロキシ ノードに関する統計を含み、名前別にすべてのクラスタ ノードを表示し、各ノードの必須の統計を追跡します。クラスタ内の特定のノードに関する詳細情報を表示する場合、[Summary] テーブルでノードの名前をクリックし、次に **[Monitor (モニタ)]** タブ上の別のいずれかのボタンをクリックします。
- ◆ 選択したノードに関する情報を表示するには、**[Node (ノード)]** をクリックします。ノードがアクティブか非アクティブかを確認でき、また **content_gateway** プロセスが開始された日付および時刻、キャッシュのパフォーマンス情報 (ドキュメント ヒット率、帯域幅の節約量、現在のキャッシュの空き容量の割合 (%))、現在開いているクライアントとサーバーの接続の数、および現在進捗中の転送の数を確認できます。また、ホスト データベースのヒット率および秒あたりの DNS ルックアップの数など、名前解決情報を確認できます。



ご注意

ノードがクラスタの一部である場合は、次の 2 組の統計が表示されます。シングル ノードに関する情報とクラスタ内のすべてのノードの平均値を示す情報です。グラフ形式で情報を表示するには、統計の名前をクリックします。

- ◆ **[Node (ノード)]** ページに表示される同じ統計 (キャッシュのパフォーマンス、現在の接続および転送、ネットワーク、および名前解決) をグラフ形式で表示するには、**[Graphs (グラフ)]** をクリックします。1 つのグラフに複数の統計を表示できます。
特定の統計をグラフ形式で表示するには、グラフの名前の隣のボックスをクリックし、次に **[Graph]** をクリックします。1 つのグラフに複数の統計を表示するには、表示する各グラフの名前の隣のボックスをクリックし、次に **[Graph]** をクリックします。
- ◆ Content Gateway が生成したアラームを表示するには、**[Alarms (アラーム)]** をクリックします。[アラームの処理, 125 ページ](#) を参照してください。

Protocols (プロトコル)

Protocols ボタンは、HTTP および FTP のトランザクションに関する情報を提供します。

- ◆ HTTP のトランザクションおよび速度 (キャッシュ ミス、キャッシュ ヒット、接続エラー、中断されたトランザクションなど) に関する情報、およびクライアントとサーバーの接続情報を確認するには、**[HTTP]** をク

リックします。また、開いている FTP サーバー接続の数、成功および失敗した PASV と PORT 接続の数、キャッシュのルックアップ、ヒット、およびミスの数など HTTP クライアントからの FTP 要求に関する情報を確認できます。

- ◆ FTP クライアントからの FTP 要求に関する情報を確認するには、[FTP] をクリックします。



ご注意

「Configure」>「My Proxy」>「Basic」タブの [Features] テーブルで FTP 処理を有効化している場合だけ、[FTP] ボタンが表示されます。

Security (セキュリティ)

Security ボタンは、下記に示すようにプロキシ認証、および SOCKS サーバー接続に関する情報を提供します。

- ◆ LDAP キャッシュ ヒットおよびミスの数、および LDAP 認証サーバー エラーの数と失敗した認証の試行回数を確認するには、[LDAP] をクリックします。[LDAP] ボタンは、「Configure」>「My Proxy」>「Basic」>「General」タブの [Features] テーブルで [LDAP] オプションを有効化した場合だけ表示されます。
- ◆ NTLM キャッシュ ヒットおよびミスの数、および NTLM 認証サーバー エラーの数と失敗した認証の試行回数を確認するには、[NTLM] をクリックします。[NTLM] ボタンは、「Configure」>「My Proxy」>「Basic」>「General」タブの [Features] テーブルで [NTLM] オプションを有効化した場合だけ表示されます。
- ◆ 折衝済み要求のカウンタ、HTLM 要求カウンタ、および基本認証要求カウンタを確認するには、「Integrated Windows Authentication (統合 Windows 認証)」(IWA) をクリックします。「IWA」タブは、「Configure」>「My Proxy」>「Basic」>「General」タブの [Features] テーブルで [IWA] オプションを有効化した場合だけ表示されます。
- ◆ SOCKS サーバーへの接続の成功回数と失敗回数、および現在進捗中の接続の数を確認するには [SOCKS] をクリックします。[SOCKS] ボタンは、「Configure」>「My Proxy」>「Basic」>「General」タブの [Features] テーブルで [SOCKS] オプションを有効化した場合だけ表示されます。

Subsystems (サブシステム)

Subsystems ボタンは、下記のようなプロキシ キャッシュ、クラスタ、イベント ログイングに関する情報を提供します。

- ◆ プロキシ キャッシュに関する情報を確認するには、[Cache (キャッシュ)] をクリックします。現在使用中のキャッシュの空き容量、キャッシュのギガバイト単位の合計サイズ、RAM キャッシュのバイト単位の合計サイズ、RAM キャッシュのヒットおよびミスの数、キャッシュルックアップ、オブジェクトの読み込み、書き込み、更新、および削除の数を示します。

- ◆ クラスタ内のノードの数、クラスタ操作の合計の数、クラスタ内のすべてのノードへのバイト読み取りおよび読み込みの数、およびクラスタ内のオープン接続の現在の数を確認するには、[Clustering] をクリックします。
- ◆ 現在開いているログ ファイルの数、ログ ファイルに現在使用中のスペースの量、ログされたアクセス イベントとエラー イベントの数、スキップされたアクセス イベントの数を確認するには、[Logging (ログ記録)] をクリックします。

Networking (ネットワーク)

Networking ボタンは、システム ネットワーク構成、ARM ルーター、WCCP ルーター、DNS プロキシ、ドメイン名解決、仮想 IP アドレス指定に関する情報を提供します。

- ◆ プロキシ コンピュータおよびデフォルト ゲートウェイに割り当てられたホスト名、検索ドメイン、プロキシ コンピュータが使用する DNS サーバーを含むシステム ネットワーク構成を確認するには、[System (システム)] をクリックします。
- ◆ Network Address Translation (ネットワーク アドレス変換) および動的バイパスに関する情報を確認するには、[ARM] をクリックします。
- ◆ WCCP v2 フラグメント化の統計、Content Gateway ノードで有効にされている各 WCCP サービス グループの構成を確認するには、[WCCP] をクリックします。[WCCP] ボタンは、「Configure」> 「My Proxy」> 「Basic」> 「General」 タブの [Features] テーブルで WCCP を有効化した場合だけ表示されます。
- ◆ Content Gateway によって処理された DNS 要求の合計数、およびキャッシュのヒットとミスを確認するには、[DNS Prox (DNS プロキシ)] をクリックします。[DNS Proxy] ボタンは、「Configure」> 「My Proxy」> 「Basic」> 「General」 タブの [Features] テーブルで [DNS Proxy] オプションを有効化している場合だけ表示されます。
- ◆ ホスト データベース内のルックアップとヒットの合計数、および DNS サーバーでの平均ルックアップ時間、ルックアップの合計数、成功したルックアップの数を確認するには、[DNS Resolver (DNS リゾルバ)] をクリックします。
- ◆ 現在の仮想 IP アドレス マッピングを確認するには、[Virtual IP Address (仮想 IP アドレス)] をクリックします。[Virtual IP Address] ボタンは、「Configure」> 「My Proxy」> 「Basic」> 「General」 の [Features] テーブルで [Virtual IP] オプションを有効化した場合にだけ表示されます。

Performance (パフォーマンス)

Performance ボタンは、パフォーマンスの履歴的グラフを表示します。[パフォーマンス グラフの使用, 127 ページ](#) を参照してください。

コマンドラインからの統計の表示

コマンドライン インターフェースを使用して Content Gateway のパフォーマンスおよび Web トラフィックに関する統計を表示できます。

またコマンドラインから Content Gateway を構成、停止、再起動することもできます。[コマンドライン インターフェース, 115 ページ](#) および [Websense Content Gateway 変数, 285 ページ](#) を参照してください。

Content Gateway のノードまたはクラスタに関する特定の情報を表示するには、下記の手順を実行し、表示対象の統計に対応する変数を指定します。

1. root に移動します。

```
su
```

2. Content Gateway にログオンします。
3. Content Gateway bin ディレクトリ (/opt/WCG/bin) から、下記のコマンドを入力します。

```
content_line -r variable
```

ここで *variable* は、表示対象の情報を表す変数です。指定できる変数のリストについては、[Websense Content Gateway 変数, 285 ページ](#) を参照してください。

たとえば、下記のコマンドは、ノードのドキュメント ヒット率を表示します。

```
content_line -r proxy.node.http.cache_hit_ratio
```



ご注意

Content Gateway bin ディレクトリがパスにない場合、コマンドの先頭に ./ が付きます。./

例：

```
./content_line -r variable
```

アラームの処理

Content Gateway は、問題を検出したとき、例えばイベント ログに割り当てられたスペースがいっぱいになった場合、または設定ファイルに書き込みできない場合に、アラームを生成します。

すべてのアラームが重要というわけではありません。一部のアラームは、一時的な状況を報告します。たとえば、**license download failed:4** アラームがインターネット接続での一時的な中断によって生成されることがあります。

下記に示すような現在のアラームのリストを表示するには、「Monitor (モニタ)」>「My Proxy」>「Alarms (アラーム)」に移動します。

Alarm! (保留中) バーは、アラームがある場合にディスプレイの上部に表示されます。



ご注意

Content Gateway はまた、いくつかのアラームを TRITON - Web Security に送信します。そこではそれらはアラートと呼ばれます。要約アラートメッセージが TRITON - Web Security 「Status (ステータス)」>「Today (本日)」ページに表示されます。Web Security 管理者は、Content Gateway がどのような状態でアラートメッセージを生成するか、およびどのような方法でアラートを送信するか (電子メールまたは SNMP) を、「Sttomgs」>「Alerts」ページで設定できます。

アラームの解除

アラームメッセージを読み取った後、アラームを除去するには、アラームメッセージウィンドウの [Clear (クリア)] をクリックします。[アラームメッセージ, 471 ページ](#) に、Content Gateway が生成するいくつかのアラームメッセージの説明を示しています。



重要

[Clear] をクリックするとアラームメッセージを除去するだけです。アラームの原因を解決しません。

同じアラーム状況が 2 度発生した場合、最初のアラームが解除されなかった場合は 2 度目のアラームはログされません。

アラームを電子メール送信するように Content Gateway を構成する

1. 「Configure」 > 「My Proxy」 > 「Basic」 > 「General」 タブの順に選択します。
2. [Alarm eMail (アラーム電子メール)] フィールドに、アラームの送信先の電子メールアドレスを入力します。下記の例のような @ 記号を含む完全な電子メール アドレスを必ず使用してください。
receivername@example.com
3. [Apply] をクリックします。

アラームのスクリプト ファイルの使用

アラーム メッセージは、Content Gateway に組み込まれています。それらを変更できません。しかし、アラームが生成されたとき特定のアクションを実行するようにスクリプト ファイルに書き込むことができます。

`example_alarm_bin.sh` という名前のサンプルのスクリプト ファイルが `/opt/WCG/bin` にあります。このファイルを変更できます。

パフォーマンス グラフの使用

パフォーマンス グラフ表示ツール (Multi Router Traffic Grapher) を使って Content Gateway のパフォーマンスをモニタし、ネットワークトラフィックを分析できます。パフォーマンス グラフは、仮想メモリ使用量、クライアント接続、キャッシュのヒット率およびミス率などに関する情報を示します。表示された情報は、Content Gateway が起動した時刻から記録されます。統計は、5 分間隔で収集されます。

パフォーマンス グラフにアクセスするには、[Monitor] > [Performance] を順に選択します。



重要

Multi Router Traffic Grapher (パフォーマンス グラフ表示ツール) を実行するには、Content Gateway システム上に Perl バージョン 5.005 以上をインストールしている必要があります。

1. Content Gateway ノードがクラスタに含まれている場合は、「Monitor」 > 「My Proxy」 > 「Summary (要約)」 ディスプレイから表示する統計のノードを選択します。
2. [Monitor] タブで [Performance (パフォーマンス)] をクリックします。
3. 利用可能なグラフのサブセットを表示するには、[Overview (概要)] をクリックします。

本日の統計を表示するには、[Daily (毎日)] をクリックします。

今週の統計を表示するには、[Weekly (毎週)] をクリックします。

今月の統計を表示するには、[Monthly (毎月)] をクリックします。

今年の統計を表示するには、[Yearly (毎年)] をクリックします。

4. Content Gateway の起動の後、少なくとも 15 分間待機してからグラフを見ます。ツールは 5 分間のサンプルをいくつか処理してから統計を初期化します。

Multi Router Traffic Grapher (MRTG) を構成していない場合、システムは、それが利用できないことを示すメッセージを表示します。ツールを構成するには、以下の手順を行います。

1. システムに Perl 5.005 がインストールされていることを確認します。
2. コマンド プロンプトで下記のように入力します。

```
perl ./pathfix.pl `which perl`
```

 これによって perl バイナリが PATH にあることを確認します。
3. Content Gateway の bin ディレクトリ (/opt/WCG/bin) に変更します。
4. コマンド プロンプトで下記のように入力して MRTG 更新の間隔を変更します。

```
./update_mrtg;sleep 5;./update_mrtg;sleep 5;
```

 デフォルトでは MRTG 更新の間隔は 15 分に設定されています。このコマンドは、更新を 5 分に設定します。
5. 下記のコマンドを入力して MRTG cron 更新を開始します。

```
./mrtgcron start
```
6. 約 15 分間待ってから、Content Gateway Manager からパフォーマンス グラフにアクセスします。



ご注意

MRTG cron 更新を停止するには、下記のコマンドを入力します。

```
./mrtgcron stop.
```

SSL Manager によるレポートの作成

認証機関のステータスを詳述するレポート ([認証機関](#), 129 ページ を参照)、またはインシデントのリストを示すレポート ([Incidents \(インシデント\)](#), 130 ページ を参照) を要求できます。レポートは、HTML 形式か、カンマ区切り形式にできます。カンマ区切りのレポートは、SSL Manager では Excel スプレッドシートとして表示されます。

認証機関

1. 「Monitor」> 「SSL」> 「Reports (レポート)」> 「Certificate Authorities (認証機関)」タブを順に選択します。
2. レポートの形式を選択します。
 - a. HTML
 - b. Comma-separated values (CSV)
 CSV を選択した場合、レポートは Excel スプレッドシートとして作成されます。
3. レポートが対象とする期間を指定します。
 - a. 日数
 - b. 現在に及ぶ開始日
 - c. ログ内のすべてのレコード
4. レポートのソート順序を指定します。
 - a. 日付別に機関をリストする
 - b. OCSP 適切な応答を最初にリストする
 - c. OCSP 不良な応答を最初にリストする

最新の取り消し情報を保持する, 169 ページを参照してください。
5. レポートを生成するには、[Generate Report (レポートを生成)] をクリックします。

HTML 出力は下記のように示されます。

Certificate Authorities		Incidents			
Validation Reports					
HTML Report of EVA - Certificate Authorities					
Profile: default_default					
Certificate Authority	Count good	Percentage	Count bad	Percentage	Last Access Date
Class 3 Public Primary Certification Authority	167	13.47 %	0	0.00 %	2008-02-12 12:07:17
www.verisign.com/CPS Incorporation by Reference: LIABILITY LIMITED BY THE TERMS OF USE OF THE VERISIGN CERTIFICATE AUTHORITY	88	7.10 %	0	0.00 %	2008-02-12 12:07:17
VeriSign Class 3 Secure Server CA	75	6.05 %	0	0.00 %	2008-02-12 12:07:17
Equifax Secure Certificate Authority	535	43.15 %	0	0.00 %	2008-02-12 10:30:06
Microsoft Internet Authority	112	9.03 %	0	0.00 %	2008-02-11 19:41:58

カンマ区切りの形式の同じレポートは、下記のように表示されます。

Certificate Authorities		Incidents					
Validation Reports							
A1		CSV Report of EVA - Certificate Authorities					
	A	B	C	D	E	F	G
1	CSV Report of EVA - Certificate Authorities						
2							
3	Profile: default_default						
4							
5	Certificate	Count good	Percentage	Count bad	Percentage	Last Access Date	
6	Class 3 Pu	167	13.47%	0	0.00%	#####	
7	www.verisi	88	7.10%	0	0.00%	#####	
8	VeriSign C	75	6.05%	0	0.00%	#####	
9	Equifax Se	535	43.15%	0	0.00%	#####	
10	Microsoft I	112	9.03%	0	0.00%	#####	



ご注意

収集した SSL ログ データを削除するには、[Reset all collected data (収集したすべてのデータをリセット)] をクリックします。

Incidents (インシデント)

1. 「Monitor」> 「SSL」> 「Reports」> 「Incidents (インシデント)」タブを順に選択します。
2. HTML 形式、またはカンマ区切り形式を選択します。カンマ区切り形式を選択場合、レポートは Excel スプレッドシートとして作成されます。
3. レポートが対象とする期間を指定します。下記のいずれかを指定できます。
 - a. 日数
 - b. 日付範囲
 - c. SSL Manager が配備されて以降の期間
4. レポートのソート順序を指定します。
 - a. 日付別にインシデントをリストする
 - b. URL 別にインシデントをリストする
 - c. 各インシデントが発生した回数をリストする

[Web HTTPS サイト アクセスの管理, 171 ページ](#) を参照してください。
5. レポートを生成するには、[Generate Report] をクリックします。

HTML 出力は下記のように示されます。

Hostname	Count	Percentage	last modification
data.coremetrics.com:443	12	7.84 %	2008-02-12 12:07:17
tc.bankofamerica.com	2	1.31 %	2008-02-12 11:55:16
*.coremetrics.com	2	1.31 %	2008-02-12 11:55:16
egov.ins.usdoj.gov	4	2.61 %	2008-02-11 19:41:58
egov.immigration.gov:443	2	1.31 %	2008-02-11 19:41:58
*.usps.com	2	1.31 %	2008-02-11 19:31:57
urs.microsoft.com	19	12.42 %	2008-02-11 19:30:57
revoked.microdasys.net	9	5.88 %	2008-02-11 19:23:56
revoked.microdasys.net:443	11	7.19 %	2008-02-11 19:23:56
www.microdasys.net	3	1.96 %	2008-02-11 19:23:56

カンマ区切りの形式の同じレポートは、下記のように表示されます。

	A	B	C	D	E
1	CSV Report of EVA - Incidents				
2					
3	Profile: default_default				
4					
5	Hostname	Count	Percentage	last modification	
6	data.coreme	12	7.84%	#####	
7	tc.bankofa	2	1.31%	#####	
8	*.coremetr	2	1.31%	#####	
9	egov.ins.us	4	2.61%	#####	
10	egov.immig	2	1.31%	#####	
11	*.usps.con	2	1.31%	#####	
12	urs.micros	19	12.42%	#####	
13	revoked.mi	9	5.88%	#####	
14	revoked.mi	11	7.19%	#####	
15	www.micr	3	1.96%	#####	



ご注意

収集した SSL ログ データを削除するには、[Reset all collected data] をクリックします。

12

Websense Data Security の使用

関連トピック：

- ◆ [Data Security の登録と構成, 135 ページ](#)
- ◆ [ICAP クライアントの構成, 139 ページ](#)

Websense Content Gateway は、Websense Data Security コンポーネントと共に、下記の機能をサポートします。

- ◆ Threats ダッシュボード (Web Security Gateway)
- ◆ Web データ 損失防止 (DLP) および Threats ダッシュボード (Web Security Gateway Anywhere、または Web Security Gateway およびフル Data Security サブスクリプション)

Web Security Gateway での Threats ダッシュボード

Content Gateway と Web Security Gateway を合わせて配備している場合、Content Gateway および TRITON 管理サーバー上にいくつかの Data Security コンポーネントがインストールされ、Web Security Threats ダッシュボードをサポートします (TRITON - Web Security Help を参照)。これらのコンポーネントには、Data Security Policy Engine (Content Gateway コンピュータ上)、および TRITON 管理サーバー上の Data Security Forensics Repository が含まれます。

Content Gateway は最初に構成されたときこれらのコンポーネントに登録し、それ以降は、再起動時に登録ステータスをチェックし、必要に応じて自動的に再登録します。

Websense Web Security Gateway Anywhere を使用する 場合の WebDLP および Threats ダッシュボード

Content Gateway が Web Security Gateway Anywhere (または Web Security Gateway およびフル Data Security サブスクリプション) と合わせて配備されているとき、Threats ダッシュボード内のフォレンジック データ、および

HTTPS, FTP、FTP over HTTP などの Web チャンネル上でのデータ損失防止 (DLP) などの機能がサポートされます。(フル Data Security 環境は、Web DLP がモバイル デバイス、リムーバブル メディア、プリンタなどのチャンネルを含むように拡張できます。Websense Data Security の詳細については、www.websense.com の Data Security 製品のページを参照してください。

WebDLP、および拡張 Data Security 構成では、TRITON – Data Security と他の Data Security のコンポーネントを別々にインストールする必要があります。Content Gateway を Data Security と合わせて使用するよう構成する場合、[Websense Technical Library](#) で提供している配備およびインストール情報を参照してください。

Content Gateway を Data Security と合わせて使用する 2 つの方法があります。

- ◆ Data Security コンポーネントを Content Gateway と同じコンピュータにオンボックス インストールして使用する
- ◆ ICAP 上で、別のホストに置かれている Data Security のコンポーネントを使用する (Data Security Suite の 7.1 以前のバージョンで使用)

1 度に使用できる方法は 1 つだけです

WebDLP の仕組み

1. プロキシは、アウトバウンド コンテンツを傍受し、そのコンテンツを Data Security に提供します。
2. Data Security は、そのコンテンツを分析して、Web 転送または FTP アップロードを許可するか、またはブロックするかを決定します。
 - この決定は、Data Security ポリシーに基づいて行われます。
 - ディスポジションは、プロキシに伝達されます。
 - Data Security は、トランザクションをログに記録します。
3. プロキシは、Data Security の決定に影響を与えます。
 - a. コンテンツがブロックされた場合、そのコンテンツはリモート ホストに送信されず、Data Security は送信者にブロック ページを返します。
 - b. コンテンツが許可された場合、コンテンツはその宛先に転送されます。



ご注意

要求がブロックされ、DLP サーバーが応答でブロック ページを送信するとき、下記の事柄が行われます。

- ◆ Content Gateway は、ブロック ページを 403 Forbidden メッセージの形式で送信者に転送します。
 - ◆ ブロック ページは 512 キロバイト以上であるか、または一部のユーザー エージェント (例、Internet Explorer) は一般的なエラー メッセージに置き換えます。
-

HTTP、HTTPS、FTP、および FTP over HTTP を使用するトランザクションが検査されることがあります。

トランザクションの詳細情報は、Data Security によってその構成ごとにログに記録されます。

Content Gateway と共にインストールされた Data Security コンポーネント

Content Gateway をインストールした場合、いくつかの Data Security コンポーネントが同じコンピュータにインストールされます。Content Gateway は最初に構成されたときこれらのコンポーネントに登録し、次に再起動時に常に登録ステータスをチェックし、必要に応じて自動的に再登録します。Data Security の登録の詳細については、[Data Security の登録と構成, 135 ページ](#) を参照してください。

Data Security ポリシーが作成され、配備された後、Content Gateway は、分析およびポリシーの実施のために、転送やアップロードなどのコンテンツを Data Security に送信します。

Content Gateway は、以下のような Data Security のトランザクションの統計を収集し、表示します。

- ◆ 転送の合計数
- ◆ 分析した転送の合計数
- ◆ 分析した FTP アップロードの数
- ◆ ブロックした要求の数
- ◆ 等々

これらの統計を Content Gateway Manager で表示するには、「Monitor」> 「Security」> 「Data Security」を順に選択します。統計の完全なリストについては、[Data Security, 269 ページ](#) を参照してください。

ICAP を使用する Data Security

Data Security ポリシー エンジンが別のホストにあるとき、Content Gateway は、ICAP v1.0 準拠の Data Security と通信できます。構成の詳細については [ICAP クライアントの構成, 139 ページ](#) を参照してください。

Data Security の登録と構成

関連トピック：

- ◆ [ICAP クライアントの構成, 139 ページ](#)

Websense Data Security の概要については、[Websense Data Security の使用, 133 ページ](#) を参照してください。

登録と構成の要約：

- ◆ コンピュータにインストールされている Data Security コンポーネントへの登録は自動的に行われます。構成は不要です。
Threat ダッシュボードのフォレンジック データは、Websense Web Security によって自動的に収集されます。
登録が失敗した場合、アラームが表示されます。
- ◆ オフボックス Data Security Management Server への登録は、「**Configure**」>「**My Proxy**」>「**Basic**」>「**Data Security**」>「**Integrated on-box (コンピュータに統合済み)**」が有効化され、Content Gateway が再起動した後自動的に行われます。
Content Gateway は、Data Security Management Server の存在を TRITON コンソールに問い合わせます。
Content Gateway と Data Security Management Server のシステム時刻は、数分間以内に同期化する必要があります。
Content Gateway が起動されるたびに、登録が検査され、必要に応じて再登録されます。
自動登録が失敗した場合、アラームが表示されます。



重要

Data Security と Content Gateway は、下記のように複数のポートを通じて通信します。IPTable が Content Gateway ホストシステムに構成されている場合、これらのポートを IPTables で開く必要があります。『Content Gateway インストールガイド』または Technical Library の「Configuring IPTables for Websense Content Gateway」というタイトルの記事を参照してください。

- ◆ Web DLP ポリシーは、**System Modules** セクションの TRITON - Data Security で構成されます。Data Security ポリシーを有効にするために、これらのポリシーを**配備**する必要があります。詳細については、TRITON - Data Security Help を参照してください。
- ◆ **[More Detail (詳細)]** をクリックし、「**Subscription Details (サブスクリプションの詳細)**」セクションの下部のリストをチェックすることによって、「**Monitor**」>「**Summary**」ページで Content Gateway Manager で登録ステータスを表示します。
- ◆ 登録の成功および失敗の情報は下記のファイルにログ記録されます。/
opt/WCG/logs/dss_registration.log

登録と構成の詳細

Web Security Gateway を配備する場合でも Web Security Gateway Anywhere を配備する場合でも、Forensics Repository への登録は自動的に行われます。追加の構成はありません。

Web DLP を使用するために Web Security Gateway Anywhere を配備する場合は、Content Gateway Manager で Data Security の統合を有効にする必要があります。

- ◆ 「Configure」> 「My Proxy」> 「Basic」を順に選択し、[Data Security > Integrated on-box (コンピュータに統合された Data Security)] を有効にします。このオプションが有効にされなかった場合、登録は Forensics Repository にのみ行われます。



ご注意

[Data Security > Integrated on-box] を有効化する前に、Content Gateway コンピュータと Data Security Management Server コンピュータが実行しておりアクセス可能であること、またそれらのシステムクロックが数分以内で同期化していることを確認します。

[Data Security > Integrated on-box] が有効化された後、Data Security Management Server への登録は自動的に行われ、Content Gateway が起動するたびに必要に応じて実行されます。登録を実行するために、Content Gateway は、IP アドレスやクラスタ ID を含む必要な情報について Websense Web Security Policy Broker に問い合わせます。

[More Detail] をクリックし、「Subscription Details」セクションの下部のリストをチェックすることによって、「Monitor」> 「Summary」ページで Content Gateway Manager で登録ステータスを表示できます。

登録が完了した後、Content Gateway は、マルウェア検出のために Web DLP ポリシー エンジンを使用します。TRITON - Data Security) に移動し、Web DLP のポリシーを構成し、配備します。TRITON - Data Security で Web DLP を配備する必要があります。

自動登録が失敗した場合、アラームが表示されます。

手動登録

[Data Security > Integrated on-box] を有効にした後、Content Gateway を再起動した場合、「Configure」> 「Security」> 「Data Security」を順に選択することによって手動登録を行うことができます（下記を参照）。

Content Gateway の再起動によって常に登録ステータスがチェックされ、必要に応じて、自動-再登録が開始されます。

登録の成功および失敗の情報は下記のファイルにログ記録されます。/opt/WCG/logs/dss_registration.log



重要

Content Gateway が V シリーズ アプライアンス上でない場合、登録のために Content Gateway ホストシステムが eth0 ネットワーク インターフェースに割り当てられた IPv4 アドレスを取得していることを必要とします。登録の後、IP アドレスはシステム上の他のネットワーク インターフェースに移動してもかまいません。しかし、その IP アドレスは Data Security の構成配備に使用され、2 つのモジュールが登録されている間は利用可能でなければなりません。

Data Security Management Server への手動登録：

1. Content Gateway システムと Data Security Management Server システムが実行しておりアクセス可能であること、またそれらのシステム クロックが数分以内で同期化していることを確認します。
2. [Data Security > Integrated on-box] が有効化されていることを確認します。Content Gateway Manager で、「Configure」>「Basic」>「General」を順に選択します。Networking にある [Features (フィーチャ)] のリストで、[Data Security] を見つけ、[On (オン)] を選択し、次に [Integrated on-box (コンピュータに統合済み)] を選択します。
3. [Not registered (未登録)] リンクをクリックします。それによって、「Configure」>「Security」>「Data Security」登録画面が開きます。
4. [Data Security Management Server] の IP アドレスを入力します。
5. Data Security Manager にログ オンするためにユーザー名およびパスワードを入力します。これは、Data Security ポリシーが構成される管理インターフェースです。ユーザーは、配備設定の権限をもつ Data Security 管理者である必要があります。
6. [Register (登録)] をクリックします。登録が成功した場合、結果を確認するメッセージが示され、Content Gateway を再起動するように要求されます。登録が失敗した場合、失敗の原因を示すエラー メッセージが表示されます。問題を訂正し、登録プロセスをもう一度実行します。

設定のオプション

登録が成功したとき、「Configure」>「Security」>「Data Security」ページで下記の設定を行います。

1. **Analyze FTP Uploads (FTP アップロードを分析)**：分析とポリシーの実施のために、FTP アップロードを Data Security に送信するには、このオプションを選択します。

2. **Analyze HTTPS Content (HTTPS コンテンツを分析)**: 分析とポリシーの実施のために、復号化した HTTPS ポストを Data Security に送信するには、このオプションを選択します。SSL Manager を Content Gateway で有効化する必要があります。[暗号化データの使用, 145 ページ](#) を参照してください。

**ご注意**

これらのオプションを有効にするために、Content Gateway をプロキシ FTP および HTTPS トラフィックに構成する必要があります。

3. **[Apply]** をクリックして設定を保存し、次に Content Gateway を再起動します。
4. TRITON – Data Security に移動し、Data Security Content Gateway モジュールを構成します。『*Websense Web Security Gateway Anywhere Getting Started*』ガイドの「Deploying the Content Gateway module」というタイトルのセクションを参照してください。

Data Security と Content Gateway は、下記のように複数のポートを通じて通信します。IPTable が Content Gateway ホスト システムに構成されている場合、これらのポートを IPTables で開く必要があります。『*Content Gateway インストール ガイド*』または Technical Library の「Configuring IPTables for Websense Content Gateway」というタイトルの記事を参照してください。

**ご注意**

Content Gateway Manager のアラームは、下記の場合に生成されます。

- ◆ コンピュータにインストールされている Data Security が有効化されているが、登録されていない
- ◆ コンピュータにインストールされている Data Security が有効化され登録されているが、Data Security Manager に構成されていない

ICAP クライアントの構成

ICAP は、Websense Data Security のすべてのバージョンと共に使用できますが、しかし、ポリシー エンジンが Content Gateway と同じコンピュータにインストールされている場合は、ダイレクト インターフェースを使用することを推奨します。[Data Security の登録と構成, 135 ページ](#) を参照してください。

Data Security Suite バージョン 7.1 以前と相互運用する場合は、ICAP を使用する必要があります。



ご注意

プライマリ サーバーが故障した場合のフェールオーバー サーバーとして、セカンダリ ICAP サーバーを指定できます。

プライマリ サーバーとセカンダリ サーバーをロード バランシングを実行するように構成できます。

下記の [ICAP フェールオーバーとロード バランシング](#) を参照。

ICP との統合を構成するには、Content Gateway Manager にログ オンし、「Configure」> 「My Proxy」> 「Basic」> 「General」 ページを順に選択します。

1. [Features] テーブルの [Networking] セクションで、Data Security の [On (オン)] を選択します。
2. [Apply] をクリックし、次に [Restart (再起動)] をクリックします。
3. 「Configure」> 「Networking」> 「ICAP」> 「General」を順に選択します。
4. [ICAP Service URI ([ICAP サービス URI]) フィールドに、一次 ICAP サービスの Uniform Resource Identifier (URI) を入力し、次にカンマ (スペースなし) を入力し、二次 ICAP サービスの URI を入力します。セカンダリ ICAP サービスは任意です。

URI は URL と似ていますが、URI は、ページではなくディレクトリで終了します。Websense Data Security Suite 管理者から識別子を取得してください。URI を下記の形式で入力します。

```
icap://hostname:port/path
```

hostname として、Websense Data Security Suite Protector アプライアンスの IP アドレスまたはホスト名を入力します。

デフォルトの ICAP ポートは 1344 です。

Path は、ホスト コンピュータ上の ICAP サービスのパスです。

例 :

```
icap://ICAP_machine:1344/REQMOD
```

デフォルトの ICAP ポート 1344 を使用している場合はポートを指定する必要はありません。たとえば、デフォルト ポートでなくても上記の URI を入力できます。

```
icap://ICAP_machine/REQMOD
```

5. [Analyze HTTPS Content (HTTPS コンテンツを分析)] で、復号化したトラフィックを分析のために Websense Data Security Suite に送信するか、または宛先の直接に送信するかを指定します。Websense Data Security Suite にトラフィックを送信するために、SSL Manager を実行する必要があります。[暗号化データの使用, 145 ページ](#) を参照してください。

6. U[**Analyze FTP Uploads (FTP アップロードを分析)**] で、FTP アップロード要求を分析のために Websense Data Security Suite に送信するかどうかを指定します。FTP トラフィックを Websense Data Security Suite に送信するには、FTP プロキシ機能を有効化する必要があります。[FTP, 314 ページ](#) を参照してください。
7. **[Action for Communication Errors (通信エラーの場合の処置)]** で、Websense Data Security Suite との通信中に Content Gateway にエラーが発生した場合に、トラフィックを許可するか、またはブロック ページを送信するかを選択します。
8. Under **[Action for Large Files (大きなファイルの場合の処置)]** で、Websense Data Security Suite で指定されたサイズの上限より大きいファイルを送信する場合に、トラフィックを許可するか、またはブロック ページを送信するかを選択します。Data Security Suite バージョン 7.0 以前のデフォルトのサイズの上限は、12 MB です。
9. **[Apply]** をクリックします。



ご注意

URI を変更した場合、Content Gateway を再起動する必要があります。他の変更では、再起動は不要です。

ICAP フェールオーバーとロード バランシング

アクティブな ICAP サーバーが障害を起こした場合、バックアップ ICAP サーバーにフェールオーバーするように Content Gateway を構成できます。プロキシは、エラー条件を検出し、トラフィックをセカンダリ サーバーに送信します。セカンダリ サーバーが応答しなくなった場合、プロキシはプライマリ サーバーを使用します。どちらの ICAP サーバーも利用できない場合、プロキシはフェールオープンします。

2 つの ICAP サーバー間のロード バランシングも任意です。

フェールオーバーまでの時間

Content Gateway では、実際に故障が発生した時からプロキシが障害を起こしたサーバーを「故障」とマークする時までの間に、一時的に要求と処理の間の遅延が発生する場合があります。障害を起こしたサーバーが「故障」とマークされた後、新しい要求はすべて、セカンダリ ICAP サーバーに送信されます。フェールオーバーまでの時間は、主に接続タイムアウトの設定によって制限されています。

フェールオーバーの原因になるエラー条件

- ◆ レイヤー 3 の障害によって ICAP 要求が失敗した (同じ要求に対して 2 回)
- ◆ 指定された時間内にポートに接続できなかった
- ◆ 要求を送信できなかった (サーバーによる接続のリセットなど)

除外される失敗条件

Content Gateway は、応答がない、無効、または遅いことを失敗とはみなしません。

しかし、Content Gateway は、ICAP OPTIONS 要求への応答を検証することによって ICAP サーバーが起動時に有効であったことを確認します。

復旧の条件

障害を起こしたサーバーが「故障」とマークされた後、新しい要求はセカンダリサーバーに送信されます。下記の復旧条件に基づいて、サーバーが再びアクティブであることが検出されるまで、障害を起こしたサーバーには新しい ICAP 要求は送信されません。

Content Gateway は、指定された間隔で、故障した各 ICAP サーバーの復旧条件についてテストします。ロード バランシングが無効化されている場合は、プライマリ ICAP サーバーがオンラインに復帰するまで、要求は引き続きセカンダリ ICAP サーバーに送信されます。ロード バランシングが有効化されている場合は、Content Gateway は、サーバー（ラウンドロビン）が「稼働中」とマークされるとすぐに、そのサーバーに要求の送信を開始します。

- ◆ TCP 接続が成功した
- ◆ OPTIONS 要求が正常に送信された
- ◆ OPTIONS 要求への有効な応答が正常に受信された

復旧の処置

サーバーの復旧時（サーバーがオンラインに復帰し、「稼働中」とマークされる）

- ◆ ロード バランシングがオンのとき：要求は、新しく稼働中になったサーバー（ラウンドロビン）に配信され始めます。
- ◆ ロード バランシングがオフのとき：プライマリサーバーが復旧した場合は、すべての要求はプライマリサーバーに送信され始めます。セカンダリサーバーが復旧した場合は、プライマリサーバーがダウンするまで、トラフィックは引き続きプライマリサーバーに送信されます。

フェイル オープン

すべての ICAP サーバーが停止した場合は、構成オプションによってフェール オープンまたはフェール クローズの動作が可能になります。すべての ICAP サーバーが停止した場合、バックグラウンド スレッドは、引き続き各サーバーとの新しい接続の再確立を試みます。

構成の設定

下記の ICAP フェールオーバー パラメータは、*records.config* ファイルで設定されています（デフォルト値を示しています）。

構成変数	データタイプ	デフォルト値	説明
proxy.config.icap.ICAPUri	STRING	(empty)	ICAP URI のカンマ区切り形式のリスト。例： icap://1.2.3.4:1344/reqmod, icap://4.3.2.1:1344/reqmod
proxy.config.icap.ActiveTimeout	INT	5	読み込み / 応答タイムアウト（秒単位）タイムアウトを超過した場合、アクティビティは失敗と見なされます
proxy.config.icap.RetryTime	INT	5	停止したサーバーが普及したかどうかをテストするための復旧時間（秒）
proxy.config.icap.FailOpen	INT	1	設定： <ul style="list-style-type: none"> ICAP サーバーがダウン状態にあるとき、トラフィックを許可する場合は 1 に設定 サーバーがダウン状態にあるとき、ブロック ページを送信する場合は 0 に設定
proxy.config.icap.LoadBalance	INT	1	設定： <ul style="list-style-type: none"> すべての利用可能なサーバーに要求を配信する場合は 1 に設定 プライマリ サーバーにだけ要求を配信する場合は、0 に設定

13

暗号化データの使用

関連トピック：

- ◆ [明示的プロキシ モードでの実行](#), 147 ページ
- ◆ [タスク](#), 150 ページ
- ◆ [SSL Manager の有効化](#), 149 ページ
- ◆ [証明書](#), 150 ページ
- ◆ [内部ルート CA](#), 151 ページ
- ◆ [証明書の管理](#), 159 ページ
- ◆ [インバウンドトラフィックの場合の SSL Manager の構成](#), 162 ページ
- ◆ [アウトバウンドトラフィックの場合の SSL Manager の構成](#), 163 ページ
- ◆ [証明書の検証](#), 164 ページ
- ◆ [Web HTTPS サイト アクセスの管理](#), 171 ページ
- ◆ [クライアント証明書](#), 175 ページ
- ◆ [SSL Manager ロギングの構成](#), 177 ページ
- ◆ [SSL 接続エラー メッセージのカスタム化](#), 180 ページ

SSL (Secure Sockets Layer) は、インターネット上のセキュアなデータ転送のための業界標準です。これは、データ暗号化と、認証機関により発行されクライアントおよびサーバーにより承認されている「信頼される証明書」のシステムをベースとしています。

SSL 接続を確立するために、クライアントはサーバーに SSL 接続要求を送信します。サーバーが同意した場合、クライアントとサーバーは、標準ハンドシェイクを使用して SSL 接続を折衝します。

SSL Manager が有効化されている場合は、SSL トラフィックが復号化され、検査され、再-暗号化されてから、その宛先に送信されます。



重要

SSL Manager が有効化されておらず、HTTPS が復号化されていないときでも、Content Gateway は HTTPS URL フィルタリングを実行します。つまり、各 HTTPS 要求に対して、URL ルックアップが実行され、ポリシーが適用されます。

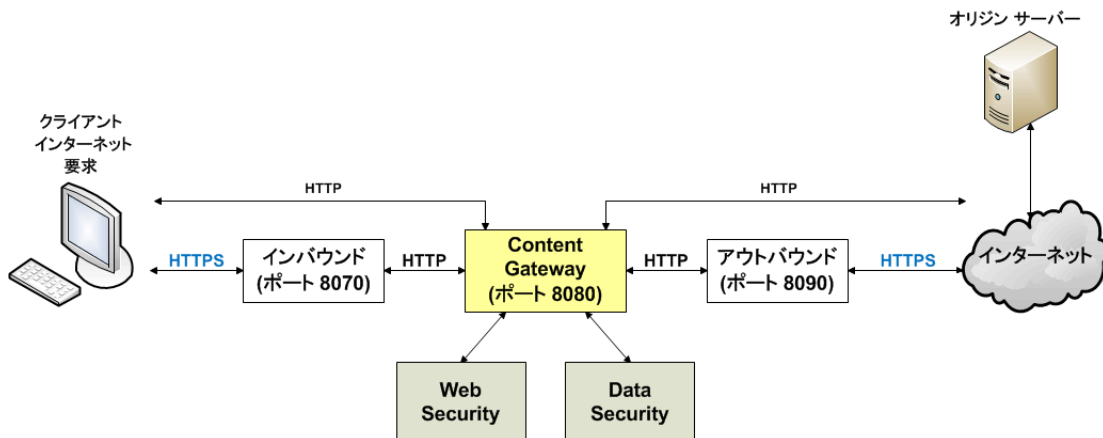
明示的プロキシモードでは、SSL がオフにされたとき、Content Gateway は要求内のホスト名に基づき URL フィルタリングを実行します。サイトがブロックされている場合、Content Gateway はブロックページを提供します。一部のブラウザは、ブロックページの表示をサポートしません。この機能を無効にするには、クライアントがプロキシに HTTPS 要求を送信しないように設定します。

透過的プロキシモードでは、SSL がオフにされたとき、Content Gateway は、宛先サーバーによって提出された認証の中の共通名に基づき URL フィルタリングを実行します。サイトがブロックされている場合、クライアントとの接続が失われます。ブロックページは提供されません。WCCP と共に使用しているときこの機能を無効にするには、HTTPS のサービスグループを作成しないでください。

SSL ベースの各要求は、2 つの個別のセッションで構成されています。

- ◆ 1 つはクライアントブラウザから SSL Manager へのセッションです。これは、インバウンド SSL トラフィックを対象としています。
- ◆ もうひとつは、SSL Manager からセキュアなデータを受信する Web サーバーへのセッションです。これは、アウトバウンド SSL トラフィックを対象としています。

これらのセッションのために種々の証明書が必要です。



**ご注意**

Content Gateway は HTTPS コンテンツをキャッシュしません。

SSL および SSL 証明書の詳細については、インターネットで検索するか、または市販の入手可能な書籍を参照してください。

システムの準備の詳細については、[Websense Technical Library](#) から入手できるの配備とインストールに関するマニュアルを参照してください。

明示的プロキシモードでの実行

既存の PAC ファイルがある場合は、Content Gateway **config** ディレクトリ（デフォルトの場所は `/opt/WCG/config`）にある **proxy.pac** を既存のファイルに置き換えます。PAC ファイルがない場合は、コピーできるスクリプトについて下記のステップ 4 を参照してください。

1. 「Configure (設定)」> 「My Proxy (マイ プロキシ)」> 「Basic (基本)」> 「General (一般)」タブで、HTTPS が有効化されていることを確認します。無効化されている場合は、HTTPS を [On (オン)] に設定し、[Apply (適用)] をクリックし、Content Gateway の [Restart (再起動)] をクリックします。
2. 「Configure」> 「Content Routing (コンテンツ ルーティング)」> 「Browser Auto-Config (ブラウザ自動設定)」> 「PAC」タブに移動します。
3. [Auto-Configuration Port (ポートの自動設定)] フィールドで、プロキシが PAC ファイルを提供するために使用するポートを指定します。デフォルトポートは 8083 です。
4. [PAC Settings (PAC 設定)] 領域に **proxy.pac** ファイルが表示されます。
 - 既存の PAC ファイルを Content Gateway の **config** ディレクトリにコピーした場合、**proxy.pac** ファイルは、ユーザーのプロキシの設定を含みます。設定値を確認し、必要な場合変更を行います。
 - 既存の PAC ファイルを Content Gateway の **config** ディレクトリにコピーしていない場合は、**proxy.pac** ファイルは空です。PAC の設定として下記のスクリプトをコピー & ペーストします。プロキシドメイン名または IP アドレスを入力する必要があります。このテンプレートは、基本的なテストのみを目的としています。組織のすべてのニーズに対応するようにこのファイルをさらに変更してください。

```
function FindProxyForURL(url, host)
{
    url = url.toLowerCase();
    host = host.toLowerCase();
    if(url.substring(0, 5) == "http:"){
        return "PROXY WCG_DOMAIN_NAME_or_IP_Address:8080";
    }
    else if(url.substring(0, 4) == "ftp:"){
```

```
        return "PROXY WCG_DOMAIN_NAME_or_IP_Address:2121";
    }
    else if(url.substring(0, 6) == "https:"){
        return "PROXY WCG_DOMAIN_NAME_or_IP_Address:8080";
    }
    else{
        return "DIRECT";
    }
}
```

5. **[Apply]** をクリックします。
6. **[Configure]** > **[My Proxy]** > **[Basic]** > **[General]** で **[Restart]** をクリックします。

新しい PAC 情報を配置した後、ユーザーにブラウザで PAC ファイルを設定するよう指示しなければなりません。たとえば、PAC ファイルが置かれているプロキシサーバーのホスト名が **proxy1** であり、Content Gateway がデフォルトポート 8083 を使用してファイルを提供する場合、ユーザーはプロキシ設定で下記の URL を指定する必要があります。

```
http://proxy1.company.com:8083/proxy.pac
```

PAC ファイルの場所の指定の手順はブラウザによって異なります。

Microsoft Internet Explorer バージョン 7.0 以上の場合：

1. 「Tools (ツール)」 > 「Internet Options (インターネット オプション)」 > 「Connections (接続)」 > 「LAN Settings (LAN の設定)」 を順に選択します。
2. **[Use automatic configuration script (自動構成スクリプトを使用)]** フィールドを選択し、**[Address]** フィールドに下記の URL を入力します。

```
http://WCG_Domain_Name_or_IP_Address:8083/proxy.pac
```

3. **[OK]** をクリックします。

Mozilla Firefox 2.0 以上の場合：

1. 「Tools」 > 「Options (オプション)」 > 「Advanced (詳細設定)」 > 「Network (ネットワーク)」 > 「Connection (接続)」 > 「Settings (設定)」 を順に選択します。
2. **[Automatic proxy configuration URL (自動プロキシ構成 URL)]** フィールドを選択し、下記の URL を入力します。

```
http://WCG_Domain_Name_or_IP_Address:8083/proxy.pac
```

3. **[Reload (再ロード)]** をクリックし、**[OK]** をクリックします。

詳細についてはご使用のブラウザのマニュアルを参照してください。

SSL Manager の有効化

1. 「Configure」> 「My Proxy」> 「Basic」> 「General」を順に選択し、HTTPS の [On] をクリックします。



ご注意

HTTPS トラフィックを検査する他の Websense の製品、たとえば、Websense Data Security Suite などと共に実行している場合は、ここで HTTPS の有効化を選択しなければなりません。

2. [Apply] をクリックし、次に [Restart] をクリックします。
3. 「Configure」> 「My Proxy」> 「UI Setup (UI の設定)」> 「General」を順に選択し、SSL Manager インターフェースのポートを指定します。デフォルトは 8071 です。このポートは、Content Gateway Manager インターフェースのポート（デフォルト 8081）とは別のポート番号にしなければなりません。
4. SSL 証明書ファイルの名前を入力します。[下位 CA の作成, 153 ページ](#) を参照してください。

「Configure (設定)」> 「Protocols (プロトコル)」> 「HTTPS」ページを使用して、ポート情報を入力し、Skype トンネリング を有効にします。

1. [HTTPS Proxy Server Port (HTTPS プロキシ サーバー ポート)] フィールドに、インバウンド（クライアントから SSL Manager へ）の HTTP トラフィックポートのポートを入力します。デフォルトは 8070 です。
2. [SSL Outbound Port (SSL アウトバウンド ポート)] フィールドに、SSL Manager が SSL Manager から宛先サーバーへのアウトバウンド HTTPS トラフィックに使用するポートを入力します。デフォルトは 8090 です。
3. Content Gateway が明示的プロキシであり、Skype トラフィックを許可する場合は、[Tunnel Skype (Skype をトンネリング)] オプションを有効化します。このオプションが必要です。なぜなら、Skype は SSL ハンドシェイクを提示しますが、Skype のデータ フローは SSL 標準に準拠しないからです。トラフィックがトンネリングされない限り、接続が失われます。

構成を完了するには、TRITON - Web Security で Skype のユーザーに適用するフィルタリング ポリシーが「インターネット電話」を許可することを確認します。SSL Manager を有効化するか否かを指定することは、Skype のユーザーにとって必須です。

また、禁止されなかった場合、最初のハンドシェイクの後、Skype は非 HTTP ポートを使ってトラフィックをルーティングします。Content

Gateway を経由するように Skype を強制するには、[『Skype IT Administrators Guide』](#) に記載されている通り、GPO を使用します。



重要

SSL Manager が有効化されていない場合は、このオプションを設定する必要はありません。

このオプションは Content Gateway が透過的プロキシである場合は、有効ではなく、無効です。

タスク

インバウンド（クライアントから SSL Manager へ）トラフィックの場合、SSL Manager の配備を準備するために下記の手順を実行します。

1. 内部ルート CA（認証機関）を作成します。SSL トラフィックにサインするために、SSL Manager は、SSL 証明書を署名する能力をもつ内部 SSL Certificate Authority を必要とします。これは、ブラウザと SSL Manager の間のトラフィックを対象としています。[内部ルート CA, 151 ページ](#) を参照してください。
2. この CA を証明書ツリーに追加します。宛先サーバーなどのサーバーは、このツリーをチェックして、ユーザーがここにリストされている機関からの証明書があるのでそれらのサーバーがユーザーを信用できることを確認します。証明書ツリーにリストされている証明書は、個別の Web サイトの妥当性を検証する権限（信用）を与える認証機関です。証明書ツリー内の認証機関によって署名されていて、「許可」ステータスをもつすべての Web サイトは、SSL Manager を通過することを許可されます。[証明書の管理, 159 ページ](#) を参照してください。
3. ブラウザのユーザーが閲覧するページをカスタマイズします。[SSL 接続エラーメッセージのカスタム化, 180 ページ](#) を参照してください。カスタマイズできるページは、接続失敗および証明書検証失敗ページです。

証明書

セキュリティでは、証明書が中心的な役割を果たします。SSL Manager の 1 つの役割は、証明書の有効性を確認することです。証明書は、下記の 3 つの基準を満たさなければなりません。

- ◆ 現在の証明書であること（有効期限切れになっていたり、取り消されていないこと）。[証明書の検証, 164 ページ](#) を参照してください。
- ◆ 信頼のある CA（認証機関）によって発行されていること。[証明書の管理, 159 ページ](#) を参照してください。
- ◆ URL と証明書の所有者が一致すること。[検証設定値の構成, 165 ページ](#) を参照してください。

クライアント ブラウザから SSL Manager へのトラフィックは、内部ルート認証機関によって発行された証明書を必要とします。[内部ルート CA, 151 ページ](#) を参照してください。

SSL Manager から宛先サーバーへのトラフィックは、「Configure」>「SSL」>「Certificates (証明書)」>「Certificate Authorities (認証機関)」タブの Certificate Authority Tree (認証機関ツリー) にリストされている機関の 1 つによって発行された証明書を必要とします。[証明書の管理, 159 ページ](#) を参照してください。

内部ルート CA

内部ルート CA は、クライアント ブラウザと SSL Manager の間で使用されるすべての証明書を動的に生成します。

- ◆ インバウンド トラフィックを SSL Manager に移動するために、内部ルート CA を持つ必要があります。
- ◆ CA をインポートするか、または作成できます。
- ◆ 内部ルート CA は、`/opt/WCG/sxsuite/conf/CA_default/PCA` に保存されます。
- ◆ CA の名前は、`PCAcert.pem` です。



重要

既存の内部ルート CA のバックアップを作成してから、新しい内部ルート CA をインポートまたは作成してください。それによって、必要な場合に証明書の以前のバージョンに戻ることができるようになります。詳細については、[内部ルート CA のバックアップの作成, 158 ページ](#) を参照してください。

同時に 1 つの内部ルート CA だけをアクティブにできます。



重要

SSL Manager に含まれているデフォルトの内部ルート CA は一意的な内部ルート CA ではありませんから、製造環境では使用しないでください。

デフォルトのルート CA を組織のルート CA に置き換えるかまたは新しいルート CA を作成します。後の項を参照してください。

内部ルート CA を作成するための下記の 3 つのオプションがあります。

- ◆ 既存の企業 CA を活用し、それを SSL Manager にインポートする。[ルート CA のインポート, 152 ページ](#) を参照してください。
- ◆ 新しい CA をプロキシとして作成し、その CA をブラウザが利用できるようにする。[新しいルート CA の作成, 152 ページ](#) を参照してください。

- ◆ 下位 CA を作成する。これは企業 CA を活用します。しかし企業 CA によって取り消すこともできます。[下位 CA の作成, 153 ページ](#) を参照してください。

ルート CA のインポート

組織がルート認証機関を所有している場合は、それをインポートできます。この証明書は、組織内のすべてのブラウザによって信頼を得なければなりません。インポートした新しい内部ルート CA のバックアップを必ず作成してください。詳細については、[内部ルート CA のバックアップの作成, 158 ページ](#) を参照してください。

1. 「Configure」> 「SSL」> 「Internal Root CA」> 「Import Root CA (ルート CA をインポート)」を順に選択します。
2. 参照して証明書を選択します。証明書は、X.509 の形式で、base64 のエンコード方式でなければなりません。
3. 参照してプライベート キーを選択します。プライベート キーは、ステップ 2 で選択した証明書と一致しなければなりません。
4. パスフレーズを入力し、確認します。
5. 「Import Root CA (ルート CA をインポート)」をクリックします。インポートされた CA は、`/opt/WCG/sxsuite/conf/CA_default/PCA` に保存されます。

新しいルート CA の作成

関連項目：

- ◆ [下位 CA の作成, 153 ページ](#)

またルート CA がない場合は、このタブのフィールドに記入して、ルート CA を作成します。作成した新しい内部ルート CA のバックアップを必ず作成してください。詳細については、[内部ルート CA のバックアップの作成, 158 ページ](#) を参照してください。

このページのアスタリスク(*)は、必須のフィールドを示しています。

1. 「Configure」> 「SSL」> 「Internal Root CA」を順に選択し、次に「Create Root CA (ルート CA を作成)」を選択します。
2. 要求された情報、特に下記の情報をフィールドに入力します。
 - フィールド [Organization (組織)、Organizational Unit (組織単位)] (このフィールドはオプションです)、および [Common Name (共通名)] が 1 つの識別名で構成されています。
 - ・ [Organization] に、自社名を入力します。
 - ・ [Common Name] に、自社内認証機関の名前を入力します。

- コメントは証明書の一部になります。入力する最初の行はエンドユーザーが閲覧できます。
 - パスフレーズを入力し、確認します（パスフレーズはパスワードに似ています。しかし通常は、より大きなセキュリティを実現するためにパスフレーズのほうが長いです）。数字、文字、および大文字と小文字の組み合せた、強いパスフレーズを使用することを推奨します。
3. **[Generate and Deploy Certificate (証明書 を生成し 配備)]** をクリックして、証明書を Content Gateway サーバーに配備します。

下位 CA の作成

下位認証機関（下位 CA）を作成することによって、ルート CA の既存のすべての情報を利用することができます。しかし、ルート CA はいつでも下位 CA を取り消すことができます。

OpenSSL および Microsoft Windows の認証サービスを使用して下位 CA を作成するには、下記の手順を実行します。

準備

- ◆ 企業ドメイン管理者でない場合は、その管理者と協力して下位 CA を作成するための正しいドメイン許可を得る必要があります。
- ◆ Windows コンピュータまたは Linux コンピュータに **OpenSSL 0.9.8(x)** ツールキット (www.openssl.org) をインストールします。

証明書署名要求 (CSR) の作成

1. OpenSSL を使用して CSR を作成します。

Windows Command Prompt 画面でまたは Linux コマンドラインで、下記の **openssl** コマンドを使って CSR を作成します。

```
openssl req -new -newkey rsa:2048 -keyout wcg.key -out  
wcg.csr
```

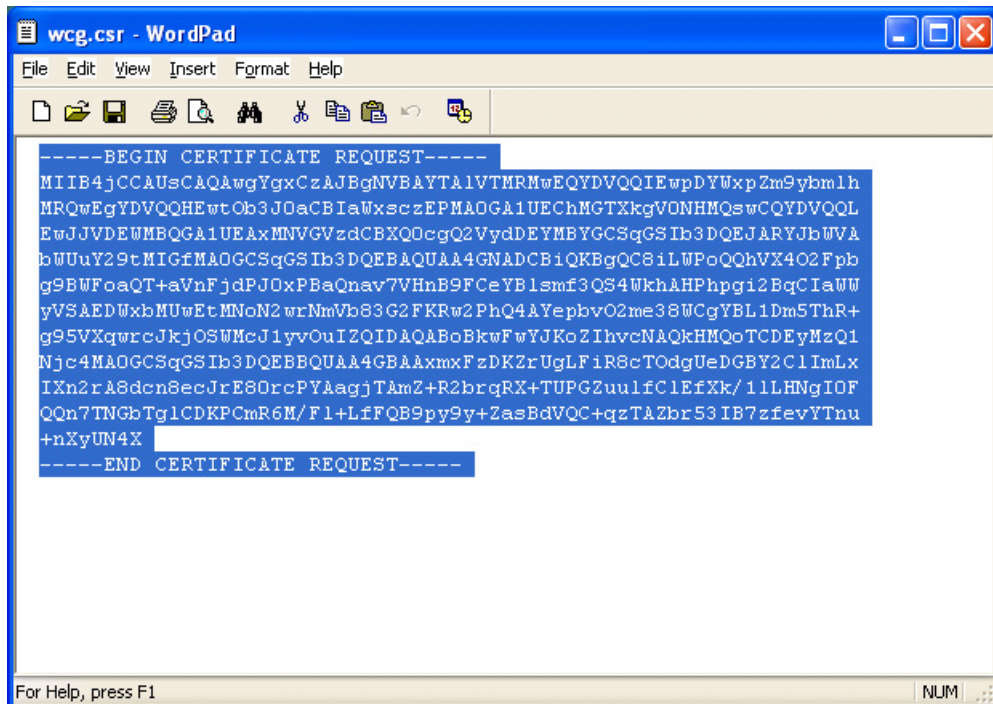
```
[root@JS-WCG ~]# openssl req -new -newkey rsa:2048 -keyout wcg.key -out wcg.csr  
Generating a 2048 bit RSA private key  
.....+++  
.....+++  
writing new private key to 'wcg.key'  
Enter PEM pass phrase:  
Verifying - Enter PEM pass phrase:  
-----  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
Country Name (2 letter code) [GB]:US  
State or Province Name (full name) [Berkshire]:California  
Locality Name (eg, city) [Newbury]:San Diego  
Organization Name (eg, company) [My Company Ltd]:Websense, INC.  
Organizational Unit Name (eg, section) []:Technical Support  
Common Name (eg, your name or your server's hostname) []:10.212.4.164  
Email Address []:  
  
Please enter the following 'extra' attributes  
to be sent with your certificate request  
A challenge password []:  
An optional company name []:  
[root@JS-WCG ~]# █
```

- 一連の質問があります。各質問に回答し、チャレンジパスワードをメモします。これは後のプロセスで必要になります。
openssl コマンドは下記の2つのファイルを生成します。
 - ・ **wcg.csr** -- 最終の証明書を作成するため認証機関によって署名される CSR
 - ・ **wcg.key** -- プライベートキー
- Linux システムで CSR を作成した場合は、WinSCP または他のファイル転送ユーティリティを使用して作成した CSR を Windows ホストにコピーします。

要求の署名

要求を Microsoft Certificate Services を使用して署名する必要があります。

1. **Wordpad** で **wcg.csr** を開き (フォーマットを保持するため)、コンテンツをクリップボードにコピーします ([Edit (編集)] > [Select all (すべて選択)];、[Edit] > [Copy (コピー)])。

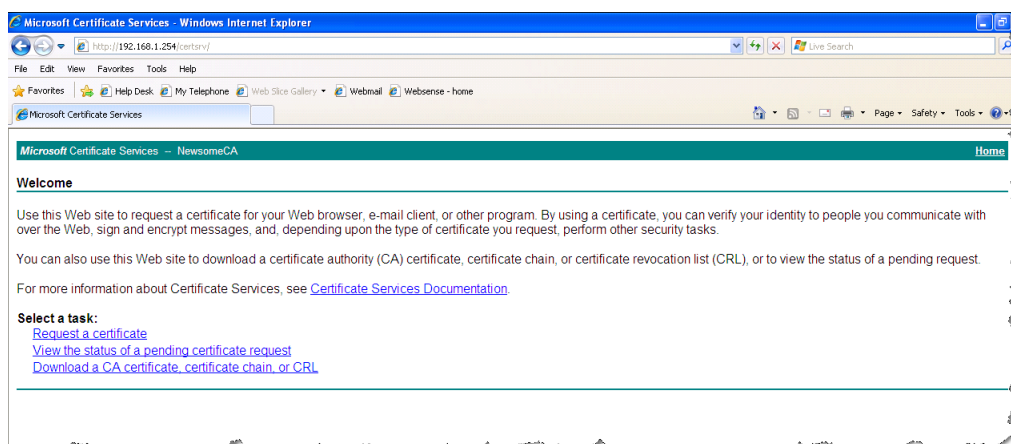


2. **Internet Explorer** で、**Microsoft CA server (Microsoft CA サーバー)** に移動します。

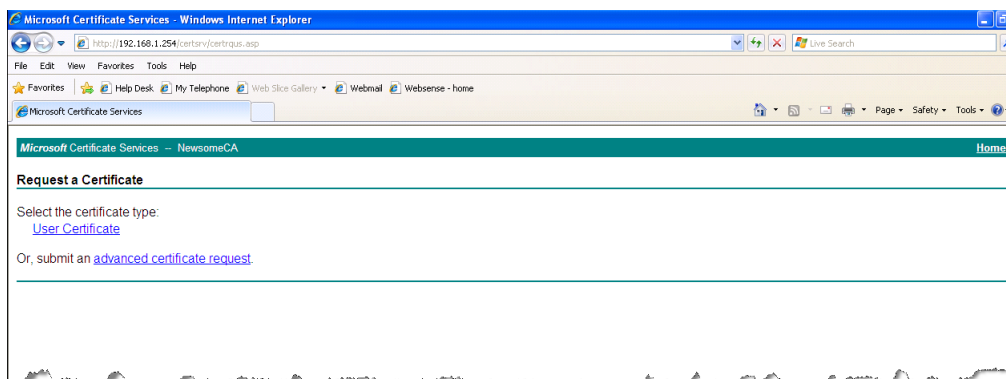
下記の URL を入力します。

`http://<CA_server_IP_address>/certsrv`

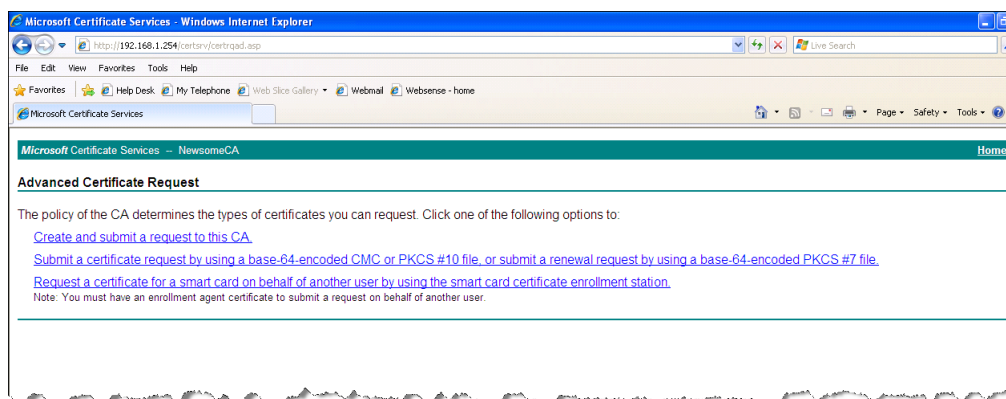
Certificate Services (認証サービス) アプレット が起動します。



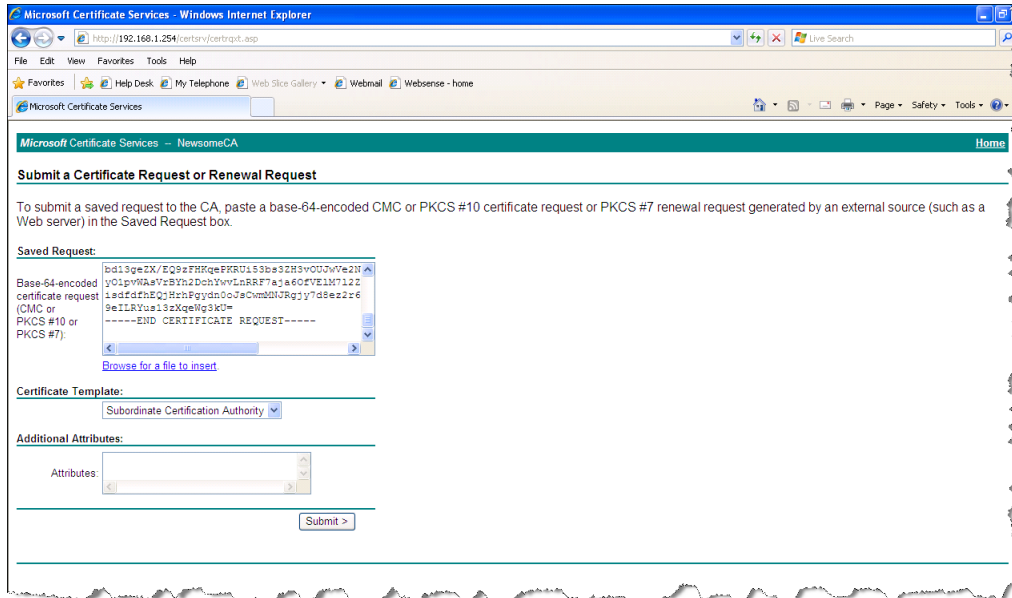
3. [Welcome (ようこそ)] 画面の見出し [Select a task (タスクを選択)] の下から [Request a certificate (証明書を要求)] を選択します。[Request a certificate (証明書を要求)] ページが表示されます。



4. advanced certificate request (最新の証明書要求) を送信するように選択します。

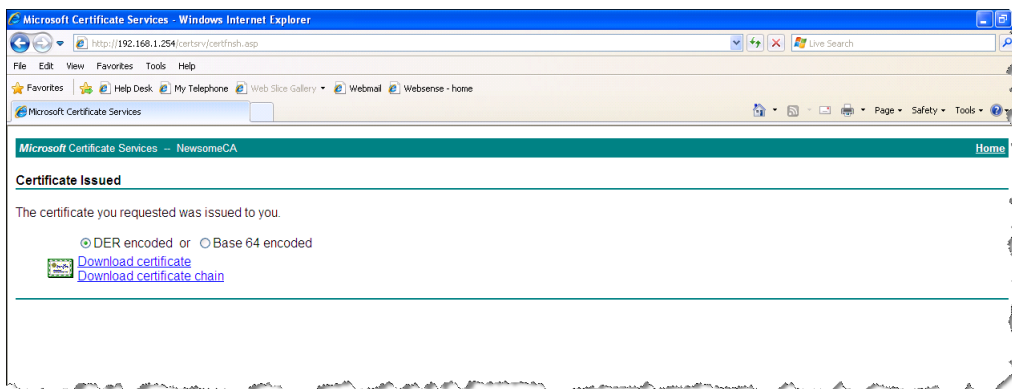


5. [Advanced Certificate Request (拡張証明書要求)] 画面で、[Submit a certificate request by using a base-64-encoded CMC (base64 エンコード CMC) を使用して証明書要求を送信] を選択します。[Submit a Certificate Request or Renewal Request (証明書要求または更新要求を送信)] 画面が表示されます。



6. [Submit a Certificate Request or Renewal Request] 画面で、[Certificate Template (証明書テンプレート)] ドロップダウンウィンドウに `wcg.csr` ファイル (前にクリップボードに置かれていた) のコンテンツを張付け、[Submit (送信)] をクリックします。

証明書が発行され、[Certificate Issued (証明書発行済み)] 画面が表示されます。代わりに、[Certificate Pending (証明書保留中)] 画面が表示される場合は、下位 CA を作成するための十分な権限がないことを表します。企業ドメイン管理者に問い合わせ、証明書作成プロセスを完了してから、次にステップ 7 に進んでください。



7. **[Base 64 encoded (Base 64 エンコード方式)]** ラジオ ボタンを選択し、次に **[Download certificate (証明書をダウンロード)]** を選択します。証明書をデスクトップに保存します。後で、その証明書を Content Gateway にインポートします。

デスクトップ上の base 64 エンコード方式の証明書は、CSR 生成プロセス中に作成されたプライベート キーと共に Content Gateway SSL Manager にインポートできる状態になっています。

下位 CA を SSL Manager にインポート

1. Content Gateway Manager を開き、「Configure」> 「SSL」> 「Internal Root CA」> 「Import Root CA (ルート CA をインポート)」を順に選択します。

2. 参照して証明書を選択します。証明書は、X.509 の形式で、base64 のエンコード方式でなければなりません。
3. 参照してプライベート キーを選択します。プライベート キーは、ステップ 2 で選択した証明書と一致しなければなりません。
4. パスフレーズを入力し、確認します
5. **[Import Root CA]** をクリックします。
6. Content Gateway の再起動

内部ルート CA のバックアップの作成

常に、内部ルート CA のパブリック キーとプライベート キーのバックアップを作成してから、新しい内部ルート CA をインポートまたは作成してください。それによって、必要な場合に証明書の以前のバージョンに戻ることが

できるようになります。さらにインポートしたまたは作成した新しいルート CA のバックアップを作成します。

1. 「Configure」> 「SSL」> 「Internal Root CA」> 「Backup Root CA (ルート CA のバックアップを作成)」を順に選択します。
2. [Save Public CA Key (パブリック CA キーを保存)] をクリックして、パブリック CA キーを確認するか、または保存します。このパブリック キーは、ユーザーの Web ブラウザによって信頼を得なければなりません。このキーがない場合は、ネットワーク管理者に問い合わせてください。
3. [Save Private CA Key (プライベート CA キーを保存)] をクリックして、プライベート CA キーを確認するか、または保存します。このキーがない場合は、ネットワーク管理者に問い合わせてください。

証明書の管理

関連項目：

- ◆ [新しい認証機関の追加, 160 ページ](#)
- ◆ [証明書のバックアップを作成, 161 ページ](#)
- ◆ [証明書の復元, 161 ページ](#)

Internet Explorer 7 によって信頼されているすべての認証機関が、「Configure」> 「SSL」> 「Certificates」> 「Certificate Authorities」タブにリストされています。宛先サーバー (SSL Manager からのアウトバウンド トラフィック) は、これらの証明書をもつ Web サーバーを信頼することができます。CRL (証明書取り消しリスト) または OCSP (オンライン証明書ステータス プロトコル) を通じて検証された一部の証明書の名前の前に、小文字の「i」が示されることがあります。これらの証明書には、URL が示されており、それによってそれらの取り消しステータスを確認できます。証明書の取り消しステータスのチェックの方法については、[最新の取り消し情報を保持する, 169 ページ](#) を参照してください。SSL Manager は、インバウンド トラフィックとアウトバウンド トラフィックの両方の証明書の取り消しステータスをチェックします。

下記の動作を実行するために、証明書の名前をクリックします。

- ◆ [証明書を確認, 159 ページ](#)
- ◆ [証明書を削除, 160 ページ](#)
- ◆ [証明書の許可 / 拒否ステータスの変更, 160 ページ](#)

証明書を確認

1. 「Configure」> 「SSL」> 「Certificates」> 「Certificate Authorities」を順に選択します。

2. 確認するステータスの機関の名前を選択します。
3. ポップアップ ウィンドウで、[Click to view certificate (クリックして証明書を確認)] を選択します。
4. Opening (オープニング) ウィンドウの指示に従い、ファイルを開くか、保存します。

証明書を削除

1. 「Configure」> 「SSL」> 「Certificates」> 「Certificate Authorities」を順に選択します。
2. 削除する認証機関の名前を入力します。
3. ポップアップ ウィンドウで、[Click to delete certificate (クリックして証明書を削除)] を選択します。
4. 証明書を削除することを確認するか、または否定します。
5. 証明書を削除することを確認した場合は、「Configure」> 「SSL」> 「Certificates」> 「Certificate Authorities」を順に選択し、証明書がリストされていないことを確認します。

証明書の許可 / 拒否ステータスの変更

1. 「Configure」> 「SSL」> 「Certificates」> 「Certificate Authorities」を順に選択します。
2. 変更するステータスの機関の名前を選択します。
3. ポップアップ ウィンドウで、[Click to change status to (クリックしてステータスを変更)] を選択します。証明書のステータスに応じて、[allow (許可)] または [deny (拒否)] を選択します。ステータスを拒否に変更した場合は、認証機関ツリーの認証機関の名前の隣に赤い X が表示されます。ステータスを許可に変更した場合は、認証機関の名前の隣に緑の円が表示されます。

新しい認証機関の追加

関連項目：

- ◆ [証明書のバックアップを作成](#), 161 ページ
- ◆ [証明書の復元](#), 161 ページ

手動で追加の認証機関をインポートするには、「Configure」> 「SSL」> 「Certificates」> 「Add Root CA (ルート CA を追加)」のページを順に選択しま

す。手動でインポートする証明書は、デフォルトのステータス **allow** にされています。



重要

現在の証明書のバックアップを作成してから、証明書の追加や削除などの変更を行うことを推奨します。[証明書のバックアップを作成](#), 161 ページ を参照してください。Content Gateway の構成全体のバックアップを作成する場合は、[構成の保存と復元](#), 117 ページ を参照してください。

1. **[Browse (参照)]** をクリックし、ディレクトリ構造を検索して、証明書を見つけます。「.cer」拡張子のあるファイルを探します。証明書は、X.509 の形式で、base64 のエンコード方式でなければなりません。
2. **[Add Certificate Authority (認証機関を追加)]** をクリックします。
3. インポートが正常に完了した場合は、「**Configure**」>「**SSL**」>「**Certificates**」>「**Certificate Authorities**」を順に選択し、そこに新しい証明書がリストされていることを確認します。

新しい CA は、ユーザーがその認証機関によって署名されたサイトを閲覧したときにも追加されます。これらの証明書を許可または拒否できます。情報は、[証明書の許可 / 拒否ステータスの変更](#), 160 ページ を参照してください。

証明書のバックアップを作成

用心のために、証明書の追加や削除などの変更を行う場合は常に、CA 証明書を含んでいるデータベースのバックアップを作成することを推奨します。そうすることによって、それらのデータベースを後日復元できます。

証明書のバックアップを作成すると、SSL Manager の設定のバックアップも作成されます。

証明書および SSL Manager の設定のバックアップを作成するには、「**Configure**」>「**SSL**」>「**Certificates**」>「**Backup Certificates (証明書のバックアップを作成)**」ページを順に選択します。

- **[Back Up Configuration to Database (構成のバックアップをデータベースに作成)]** をクリックします。

証明書だけでなく、Content Gateway の構成全体のバックアップを作成するには、[構成の保存と復元](#), 117 ページ を参照してください。

証明書の復元

証明書を復元すると、構成データベースも復元します。しかし、取り消しリストは定期的の更新されるので、それらのリストはこのプロセスの一部として復元されません。証明書取り消しリストの更新の詳細については、[最新の取り消し情報を保持する](#), 169 ページ を参照してください。

証明書および SSL Manager の設定を含む構成データベースを復元するには、「Configure」>「SSL」>「Certificates」>「Restore Certificates (証明書を復元)」ページを順に選択します。

1. **[Browse]** をクリックして、バックアップ証明書データベースの場所に移動します。
2. **[Restore (復元)]** をクリックします。復元が正常に完了したことを伝え、以前の証明書データベースのバックアップが作成された場所を示すメッセージを受け取ります。

複数のプロキシを実行している場合、この復元機能を使用して、すべてのプロキシが同じ構成にされていることを確認します。

復号化と暗号化

[インバウンドトラフィックの場合の SSL Manager の構成, 162 ページ](#)

[アウトバウンドトラフィックの場合の SSL Manager の構成, 163 ページ](#)

インバウンドトラフィックの場合の SSL Manager の構成

関連項目：

- ◆ [アウトバウンドトラフィックの場合の SSL Manager の構成, 163 ページ](#)

SSL Manager がインバウンドトラフィックを処理する方法を構成するには、「Configure」>「SSL」>「Decryption / Encryption (復号化 / 暗号化)」>「Inbound (インバウンド)」ページを順に選択します。インバウンドトラフィックはブラウザから SSL Manager に転送され、そこでコンテンツが復号化され、検査されます。

1. 次のプロキシに認証資格情報を転送するために **[IP Address (IP アドレス)]** を選択します。
2. HTTP ヘッダーに、通過するプロキシチェーントラフィックを記述する特別のヘッダーを追加するには、**[Send VIA-Header (VIA ヘッダーを送信)]** を選択します。この情報は、トラブルシューティングに役立ちます。VIA-Header を含めない場合は、このボックスを選択しないでください。
3. **[Protocol Settings (プロトコルの設定)]** で、SSL Manager がサポートするプロトコルを指定します。サポートされているプロトコルは、SSLv2、SSLv3、および TLS v1 です。企業ブラウザがサポートするプロトコルを選択します。すくなくとも 1 つのプロトコルを選択しなければなりません。デフォルトは SSLv2 です。これらの設定は、ユーザーのブラウザでのプロトコルの設定を上書きします。
アウトバウンドトラフィックとは異なるプロトコルを選択できます。

4. 暗号リストは、利用可能なアルゴリズムと、クライアントと SSL Manager の間の暗号化のレベルを示します。デフォルトの設定は、eNULL および ADH Suite を除く利用可能なすべての暗号を使用するように指示します。最強の暗号（高レベルの暗号化を提供）が最初に適用されます。アウトバウンド トラフィックとは異なるレベルの暗号化に設定できません。インバウンド トラフィックの暗号化を高レベルに設定すると、システムの整合性およびセキュリティを確保するのに役立ちます。追加の暗号の設定は下記の通りです。
 - **High（高）**暗号化暗号セット：128 ビットより長いキーを持つ暗号セット、および 128 ビットのキーをもつ一部の暗号セット。
 - **Medium（中）**暗号化暗号セット：128 ビット暗号化を使用する暗号セット
 - **Low（低）**暗号化暗号セット：64 ビットまたは 56 ビットの暗号化アルゴリズムを使用するが、エクスポート暗号セットを除く暗号セット。インバウンド要求（組織内のクライアント ブラウザから SSL Manager への要求）の場合、パフォーマンスを向上させるために Low 暗号化を使用することを検討してください。暗号の詳細については、www.openssl.org/docs を参照してください。
5. [Apply] をクリックします。
6. [Configure] > [My Proxy] > [Basic] > [General] で [Restart] をクリックします。

アウトバウンド トラフィックの場合の SSL Manager の構成

SSL Manager がアウトバウンド トラフィックを処理する方法を構成するには、「Configure」>「SSL」>「Decryption / Encryption（復号化 / 暗号化）」>「Outbound（アウトバウンド）」ページを順に選択します。アウトバウンド トラフィックは SSL Manager から 宛先 Web サーバーに転送されます。SSL Manager は、サイト証明書の取り消しステータスをチェックしてから、再暗号化したデータをサイトに転送します。

1. SSL Manager と宛先ホストの間に複数のプロキシがある場合、あるプロキシから次のプロキシに認証資格情報を転送するために [IP Address (IP アドレス)] を選択します。
2. HTTP ヘッダーに、通過するプロキシ チェーン トラフィックを記述する特別のヘッダーを追加するには、[Send VIA-Header (VIA ヘッダーを送信)] を選択します。この情報は、トラブルシューティングに役立ちます。VIA-Header を含めない場合は、このボックスを選択しないでください。
3. [Protocol Settings (プロトコルの設定)] で、SSL Manager がサポートするプロトコルを指定します。サポートされているプロトコルは、SSLv2、SSLv3、および TLS v1 です。企業ブラウザがサポートするプロトコルを選択します。すくなくとも 1 つのプロトコルを選択しなければなりません。デフォルトは SSLv2 です。これらの設定は、ユーザーのブラウザでのプロトコルの設定を上書きします。インバウンド トラフィックの場合、種々のプロトコルを選択できます。

4. [Session Cache Timeout (セッション キャッシュ タイムアウト)] で指定した時間が経過するまで、キーをキャッシュする場合は、[Session Cache (セッション キャッシュ)] を選択します。これによって、パフォーマンスを改善できます。キーがキャッシュされなかった場合、各要求はもう一度折衝されます。
5. キーがキャッシュに保持される時間 (単位、秒) を指定します。デフォルトは 300 秒 (5 分) です。
6. 暗号リストは、利用可能なアルゴリズムと、クライアントと SSL Manager の間の暗号化のレベルを示します。デフォルトの設定は、eNULL および ADH Suite を除く利用可能なすべての暗号を使用するように指示します。最強の暗号 (高レベルの暗号化を提供) が最初に適用されます。インバウンド トラフィックとは異なるレベルの暗号化に設定できます。アウトバウンド トラフィックの暗号化を高レベルに設定すると、システムの整合性およびセキュリティを確保するのに役立ちます。
追加の暗号の設定は下記の通りです。
 - **High (高)** 暗号化暗号セット: 128 ビットより長いキーを持つ暗号セット、および 128 ビットのキーをもつ一部の暗号セット。
 - **Medium (中)** 暗号化暗号セット: 128 ビット暗号化を使用する暗号セット
 - **Low (低)** 暗号化暗号セット: 64 ビットまたは 56 ビットの暗号化アルゴリズムを使用するが、エクスポート暗号セットを除く暗号セット。アウトバウンド要求 (SSL Manager から暗号化データを受け取る宛先サーバーへの要求) の場合、セキュリティを向上させるために、より高度な暗号化レベルを使用することを検討してください。
暗号の詳細については、www.openssl.org/docs を参照してください。
7. [Apply] をクリックします。
8. [Configure] > [My Proxy] > [Basic] > [General] で [Restart] をクリックします。

証明書の検証

関連項目:

- ◆ [検証のバイパス, 168 ページ](#)
- ◆ [最新の取り消し情報を保持する, 169 ページ](#)

SSL 証明書の検証は、SSL セキュリティの重要な構成要素の 1 つです。クライアント (この場合は、Content Gateway SSL Manager) とオリジン サーバーは、証明書の交換と検証を通じて、相互の身元を確認します。

SSL Manager では、このタスクは、証明書検証エンジンによって実行されます。

Certificate Verification Engine (CVE) を有効化し、構成するには、「**Configure**」>「**My Proxy**」>「**SSL**」>「**Validation (検証)**」を順に選択し、タブを使用します。

検証が失敗したが、そのサイトを信用する場合のオプションの詳細については、[検証のバイパス, 168 ページ](#) を参照してください。

CVE の使用法および最善の方法の包括的な説明については、[『SSL Manager Certificate Verification Engine v7.7』](#) を参照してください。

検証設定値の構成

1. 「**Configure**」>「**SSL**」>「**Validation**」>「**General**」ページを順に選択します。
2. **Enable the certificate verification engine (証明書検証エンジンを有効化)**: このオプションは、証明書検証エンジンを有効化および無効化します。
デフォルトでは、証明書検証は無効化されています。それによって、HTTP が（「**Configuration**」>「**My Proxy**」>「**Basics**」ページで）最初に有効化されたとき、証明書検証の結果によって、Content Gateway 管理者およびネットワーク ユーザーが不意をつかれないようにします。
このオプションを選択しなかった場合は、証明書検証はおこなわれません。



重要

証明書検証エンジンを無効化した場合、下記のページのみに関する情報を入力する必要があります。

- Configure > SSL > Decryption / Encryption > Inbound
- Configure > SSL > Decryption / Encryption > Outbound
- Configure > SSL > Logging pages
- Configure > SSL > Customization > Connection Error

3. **Deny certificates where the common name does not match the URL (共通名が URL と一致しない場合に証明書を拒否する)**: このオプションを有効化した場合、下記の 2 つのチェックが行われます。
 - 最初に、証明書の共通名について宛先 URL と正確に一致しているかチェックします。
 - 最初のチェックが失敗した場合、証明書の Subject Alternative Name (SAN) リストをチェックして、宛先 URL と正確に一致する名前がないか調べます。

チェックは、大文字と小文字を区別します。

正確な一致が要求されるため、共通名に些細な違いがあったり、SAN で一致するバリエーションがないときに、ブロックされる場合があります。

たとえば、「https://cia.gov」を使用して「https://www.cia.gov」にアクセスしようとする、ブロックされてしまうことがあります。さらに、IP

アドレスを使って Web サイトにアクセス使用としたときもブロックされることがあります。

4. **Allow wildcard certificates (ワイルドカードの証明書を許可)**: これは、**When Deny Certificates where the common name does not match the URL (共通名が URL と一致しない場合に証明書を拒否する)** のサブオプションです。このオプションを有効化したとき、それによって、名前に「*」(ワイルドカード) 文字を含む共通名との一致を許可します。

一部の HTTPS サーバーは、共通名にワイルドカードを使用しますから、それによって単一の証明書がドメイン全体を対象とすることができます。例: 「*.example.com」は、「email.example.com」と「stream.example.com」などを対象とします。

ワイルドカードの使用は、ドメイン内部の個々のサーバーが検証されないことを意味します。それらはワイルドカードの結果として含まれます。

ワイルドカードの証明書を許可することは、共通名の一致が必要とされるとき厳格なマッチングの負担を軽減します。また、google.com や yahoo.com などの複数のサブドメインをもつドメインの場合に役立ちます。またドメインの詐欺的なまたは望ましくないバリエーションがブロックされずまかり通るというある種のリスクをもたらします。

5. **No expired or not yet valid certificates (期限切れまたはまだ有効でない証明書なし)**: このオプションを有効化したとき、期限切れの証明書またはまだ有効でない証明書を提供するサイトへのアクセスを拒否します。これは重要な基本のチェックです。なぜなら多くの不正なサイトが期限切れ証明書を使って運営しているからです。このオプションを選択しなかった場合、これらのサイトへのアクセスが許可されます。



ご注意

自己署名証明 (公的認証機関の発行でない証明書) は、無効と見なされ、このカテゴリに属します。

6. **Verify entire certificate chain (証明書チェーン全体を検証)**: このオプションを有効化したとき、サイト証明書と証明書の証明書パスでルートとして指定されたルート認証機関との間のすべての証明書の期限切れステータスと取り消しステータスを検証します。これは、重量なチェックです。

7. **Check certificate revocation by CRL (CRL による証明書取り消しをチェック)**: 証明書取り消しリスト (CRL) は、証明書の取り消しステータスをチェックするために使用されます。CRL は、CA によって発行され、その後取り消された証明書をリストします。

取り消しステータスの検証は、非常に重要な基本チェックです。なぜなら、証明書は、CA によって、それらが不適切に発効された、信用できなかった、偽の ID を持っている、またはポリシー違反と指定されたとき、通常は取り消されるからです。

8. **Check certificate revocation by OCSP (OCSP による証明書取り消しをチェック)**: Online Certificate Status Protocol (OCSP) は、証明書の取り消しステータスをチェックするもう一つの方法です。OCSP は役立ちます

が、CRL ほど広範に使用されておらず、したがってそれほど信頼できません。また、これはリアルタイムのインターネットがホストするチェックであり、要求処理の遅延をもたらすことがあります。



ご注意

CRL の代わりではなく、CRL に加えて OCSP を使用することを推奨します。CRL と OCSP の詳細については、[最新の取り消し情報を保持する, 169 ページ](#) を参照してください。

9. **Block certificates with Unknown OCSP state (未知の OCSP 状態がある証明書をブロック)**: OCSP 取り消しチェックを有効にしたとき、「Unknown (未知)」ステータスを返す証明書をブロックするためにこのオプションを有効化します。
10. **Preferred method for revocation check (取り消しチェックの優先する方法)**: CRL と OCSP の両方の取り消しチェックを有効にしたとき、最初にとの方法を適用するか指示するためにこのオプションを使用します。デフォルト設定は CRL です。
11. **Block certificates with no CRL URI and with no OCSP URI (CRL URI がない証明書、および OCSP URI がない証明書をブロック)**: CRL チェック、OCSP チェック、または両方のチェックを有効にしたとき、想定した関連する URI がない証明書をブロックするには、このオプションを使用します。たとえば、CRL チェックだけを有効化し、証明書に CRL URI がない場合、このオプションが有効化された場合は、接続がブロックされます。CRL と OCSP の両方のチェックを有効化した場合、CRL と OCSP の両方に URI がない場合だけ、接続がブロックされます。
ブラウザで証明書を確認することを選択した場合、証明書内の URI 情報を確認できます。詳細については、[証明書を確認, 159 ページ](#) を参照してください。
多くの証明書は、CRL 情報や OCSP 情報を含んでいませんから、このオプションを使用すると検証失敗の数が増える可能性があります。多くの場合、失敗は、「Unknown revocation state (未知の取り消し状態)」エラーとして報告されます。
これは、多くのアクセス拒否がある高い制限付きポリシーになる可能性があります。
すべての検証の失敗と同様に、インシデント リストを使用して例外を許可できます。[Web HTTPS サイト アクセスの管理, 171 ページ](#) を参照してください。
12. **Run external program on incidents (インシデント時に外部プログラムを実行)**: トラブルシューティングのために、インシデント時に外部プログラムを実行できます。インシデントは、クライアントがアクセス拒否メッセージを受け取ったときは常にログに記録されます。インシデントの詳細については、[Web HTTPS サイト アクセスの管理, 171 ページ](#) を参照してください。このフィールドにスクリプトのパスを入力します。
このスクリプトを実行するための最小限の許可は下記のようになります。

```
chmod 700 /opt/WCG/sxsuite/bin/script.sh
chown root /opt/WCG/sxsuite/bin/script.sh
chgrp root /opt/WCG/sxsuite/bin/script.sh
```

トラブルシューティングに役立てるために、下記のスクリプトをコピー & ペーストすることを推奨します。それに y って下記の情報を捕捉し、それらをファイルに書き込みます。

- インシデントを作成したアカウント
- クライアント IP アドレス、またはクライアント IP アドレスが転送されなかった場合は以前のプロキシの IP アドレス
- インシデント リストに示される通りのインシデントの ID
- インシデントの原因に関する詳細メッセージ
- インシデントを起こしたアカウント内のプロファイル
- インシデントを引き起こした URL のホスト セクション

```
#!/bin/sh
```

```
OUTFILE=/root/WCG/incidents.log
```

```
date >> $OUTFILE
```

```
echo "Account: $SCIP_INCIDENT_ACCOUNT" >> $OUTFILE
```

```
echo "Client-IP: $SCIP_INCIDENT_CLIENTIP" >> $OUTFILE
```

```
echo "Incident-ID: $SCIP_INCIDENT_ID" >> $OUTFILE
```

```
echo "Detailed Message: $SCIP_INCIDENT_MESSAGE" >> $OUTFILE
```

```
echo "Profile: $SCIP_INCIDENT_PROFILE" >> $OUTFILE
```

```
echo "Destination Host URL: $SCIP_INCIDENT_REMOTEHOST" >>
```

```
$OUTFILE
```

```
echo "User: $SCIP_INCIDENT_USER" >> $OUTFILE
```

```
echo >> $OUTFILE
```



重要

このフィールドで `opt/WCG/sxsuite/bin/` ディレクトリに他のコマンドを入力しないことを推奨します。またここに示したスクリプト以外のスクリプトを入力する場合は、注意してください。

検証のバイパス

証明書の検証が失敗したときにユーザーがサイトを閲覧するのを許可するには「**Configure**」>「**SSL**」>「**Validation**」>「**Verification Bypass (検証のバイパス)**」ページを使用します。

1. ユーザにサイトが無効の証明書があることを知らされた後、ユーザーがサイトに進むことができるようにするには、**[Permit users to visit sites with certificate failure after confirmation (証明書の認証が失敗した場合に、ユーザーに対して、確認後にサイトの閲覧を許可する)]**を選択します。このチェックボックスを選択していなかった場合は、ユーザーにはサイトを参照するオプションがありません。

- バイパスした証明書に関する情報をキャッシュに保存し、切速を再利用するには、[**Enable the SSL session cache for bypassed certificates (バイパスした証明書の SSL セッション キャッシュを有効化)**] を選択します。
 - このオプションを選択した場合は、パフォーマンスは向上しますが、一部のユーザーには検証に失敗したサイトにアクセスしようとしていることが通知されません。
 - このオプションを選択しなかった場合は、すべてのユーザーは、有効な証明書がないサイトについて通知されますが、パフォーマンスはそれほど向上しません。
- [**Timeout (タイムアウト)**] では、このサイトをバイパスしユーザーにサイトに無効の証明書があることを通知する間にかかる非アクティブの時間を指定します。デフォルトは 6 分 (360 秒) です。

最初にバイパス検証を有効化しておくことを推奨します。次にインシデントレートの変更のように、インシデント リストを使用してポリシーを適用できます。[Web HTTPS サイト アクセスの管理, 171 ページ](#) を参照してください。

最新の取り消し情報を保持する

サイトが証明書を受け入れる前に、証明書が取り消されていないことを確認するために証明書のステータスをチェックすることを推奨します。このチェックを行うための下記の 2 つの方法があります。CRL を通じて ([証明書取り消しのリスト, 169 ページ](#) を参照) と OCSP を通じて ([Online certification status protocol \(オンライン証明書ステータス プロトコル\) \(OCSP\), 170 ページ](#) を参照)。


証明書取り消しのリスト

SSL Manager が最新の取り消し情報を保持する方法を構成するには、「**Configure**」>「**SSL**」>「**Validation**」>「**Revocation Settings (取り消しの設定)**」ページを順に選択します。デフォルトでは、SSL Manager は毎日 CRL をダウンロードします。

- CRL を毎日ダウンロードするには、[**Download the CRL at (指定時に CRL をダウンロード)**] を選択し、CRL ダウンロードを行う時刻を選択します。
- [**Apply**] をクリックします。

すぐに CRL を更新する必要がある場合もこのページを使用します。

1. 指定した時刻以外の時刻に CRL をダウンロードするには、[**Update CRL Now (CRL をすぐにダウンロード)**] をクリックします。たとえば、サブスクリプションに SSL Manager を含んでいる場合は、このプログラムをインストールした後、CRL をダウンロードします。

 **ご注意**

CRL ファイルは、たくさんの証明書を含むことがあり、そのため CRL のダウンロードには時間がかかり、CPU リソースを消費することがあります。システム上のインターネットトラフィックの量が少ない時に、CRL をダウンロードすることを推奨します。

2. 更新のステータスを確認するには、[**View CRL Update Progress (CRL 更新の進捗状況を表示)**] をクリックします。

証明書取り消しリストの詳細については、RFC 3280 を参照してください。

Online certification status protocol (オンライン証明書ステータス プロトコル) (OCSP)

OCSP は、要求 / 応答に基づき機能するプロトコルです。つまり、サイトが証明書の取り消しステータスを確認するために待機しているとき、サイトは CA に証明書のステータスに関する要求を送信します。それによって CA が応答し、証明書の有効性（または取り消し）を確認します。

CRL をダウンロードするのではなく、OCSP を使用すると、要求を処理するので、パフォーマンスの向上が実現できます。しかし、一部の CA は応答を提供せず、そのため CRL を使用する方がより多くの証明書のステータスに関する情報を得ることができます。

SSL Manager は、証明書の取り消しステータスに関する OCSP 情報をキャッシュできるようにします。応答のキャッシュ処理は、SSL トラフィック量が多く、帯域幅の節約が重要な環境では便利なことがあります。

SSL Manager が最新の取り消し情報を保持する方法を構成するには、**「Configure」** > **「SSL」** > **「Validation」** > **「Revocation Settings」** ページを順に選択します。

1. OCSP データがキャッシュされる期間（日数）を指定します。OCSP データをキャッシュしない場合は、**「0」** と入力します。最大の日数は 1000 日です。
2. **「Apply」** をクリックします。

OCSP の詳細については、RFC 2560 を参照してください。

Web HTTPS サイト アクセスの管理

関連トピック：

- ◆ [インシデントの表示](#), 171 ページ
- ◆ [インシデントのステータスの変更](#), 173 ページ
- ◆ [インシデントの削除](#), 173 ページ
- ◆ [メッセージのテキストの変更](#), 173 ページ
- ◆ [インシデントの詳細の表示](#), 174 ページ
- ◆ [インシデント リストへの Web サイトの追加](#), 174 ページ

一連のタブは、Web サイトへのアクセスを管理するのに役立ち、またアクセス問題のトラブルシューティングの際にヘルプ デスクを支援します。このページに行った入力および変更は、SSL Manager データベースに保存されます。

Web サイトがセキュリティ ポリシーに準拠しなかったのでクライアントがアクセス拒否メッセージを受け取った場合、SSL Manager は、[インシデント](#)を生成します。[インシデントの表示](#), 171 ページ を参照してください。

SSL Manager が特定のサイトを処理する方法を指定する場合、そのことをインシデント リストにも追加できます。[インシデント リストへの Web サイトの追加](#), 174 ページ を参照してください。

トラブルシューティングの追加情報については、[SSL Manager Certificate Verification Engine v7.7](#) を参照してください。

インシデントの表示

クライアントがアクセス拒否メッセージを受け取った事象のレポートを表示するには、「Configure」>「SSL」>「Incidents (インシデント)」>「Incident List (インシデント リスト)」ページを順に選択します。このレポートのフィールドを使用して、今後 SSL Manager がサイトへ要求されたアクセスを処理する方法を決定することができます。

- ◆ 特定のインシデントを表示するには、ID 番号を入力し、[Search (検索)] をクリックします。
- ◆ 完全なリストを表示するには、[Show All (すべて表示)] をクリックします。

インシデント レポート

列見出しの隣の小さな三角形をクリックしてどの列でもソートできます。

インシデント レポートは、下記のフィールドを含んでいます。

フィールド	説明
ID	<p>システムにより割り当てられます。これはインシデント ID 番号であり、Ticket ID (チケット ID) とも言います。ヘルプデスクはエラー メッセージでユーザーに Ticket ID を尋ね、それを URL インシデント リストからすばやく取得します。</p> <p>エンド ユーザーには、Ticket ID と拒否メッセージが表示されます。</p>
Status (ステータス)	<p>今後 SSL Manager がこの Web サイトを処理する方法を決定します。下記の 4 つの条件が可能です。</p> <ul style="list-style-type: none"> • Allow (許可) ユーザは証明書が有効でない場合でもそのサイトにアクセスできます。トラフィックが復号化され、証明書チェック機能が無効にされます。 • Blacklisted (ブラックリストに載せる) そのサイトは完全にブロックされます。Verification Bypass (検証のバイパス) が設定されている場合でも、ユーザーはこのサイトにアクセスできません。 • Block (ブロック) 証明書検証が失敗した場合、Verification Bypass が設定されていない限り その Web サイトへのアクセスはブロックされます。Verification Bypass が設定されている場合は、ブロック ページに [Visit site anyway (それでもサイトを閲覧する)] ボタンが表示されます。検証のバイパス, 168 ページを参照してください。 • Tunnel (トンネル) このサイトはトネリングされます。トラフィックは復号化されず、SSL Manager は証明書をチェックしません。トネリングは、信用のあるサイトの検査のバイパスとパフォーマンスの向上のために使用します。 ご注意 : Tunnel by URL (URL に基づくトンネル) は、明示的プロキシトラフィックでのみサポートされています。 <p>[Action (アクション)] 列のドロップダウン ボックスから Web サイトのステータスを変更できます。</p>
Type (タイプ)	<p>サイトがその URL またはその証明書のどちらに基づいて追加されたかを指定します。サイトを証明書に基づくインシデント リストに追加することを推奨します。インシデント リストへの Web サイトの追加, 174 ページを参照してください。</p>
URL	<p>証明書が有効でなかったサイトの URL。</p>

フィールド	説明
Message (メッセージ)	エラーメッセージの編集を有効化します。エラーメッセージのカスタム化の詳細については、 メッセージのテキストの変更, 173 ページ を参照してください。ペンシルと虫メガネは、それぞれリンクを表します。これらのリンクの詳細については、 インシデントの詳細の表示, 174 ページ を参照してください。
Action (アクション)	インシデントのステータスの変更を有効化します。またインシデントを削除できるようにします。 インシデントの削除, 173 ページ を参照してください。

インシデントのステータスの変更

インシデントのステータスを変更するとき、SSL Manager が今後リストされている URL を処理する方法を変更します。

1. 「Configure」>「SSL」>「Incidents」>「Incident List」を順に選択します。
2. [Action] 列のドロップダウン リストから下記のいずれかのオプションを選択します。これらのオプションの詳細については、[インシデントレポート, 171 ページ](#) を参照してください。
 - Tunnel
 - Block
 - Blacklist
 - Allow
3. [Go(実行)] をクリックします。[Status(ステータス)] 列のアイコンは新しいステータスを反映するようになります。

インシデントの削除

1. 「Configure」>「SSL」>「Incidents」>「Incident List」を順に選択します。
2. 削除するインシデントを選択します。インシデントが表示されない場合、ID を使って検索できます。[インシデントの表示, 171 ページ](#) を参照してください。
3. [Action] 列のドロップダウン リストから [Delete(削除)] を選択し、次に [Go] をクリックします。

メッセージのテキストの変更

1. 「Configure」>「SSL」>「Incidents」>「Incident List」を順に選択します。
2. さらに詳しく検査するインシデントを見つけます。[インシデントの表示, 171 ページ](#) を参照してください。

3. ペンシルをクリックしてウィンドウを開き、そこでこのエラーメッセージのテキストを変更します。たとえば、ヘルプデスクは、エラーメッセージにより詳細な情報を追加できます。
4. 新しいテキストを記入したときは、[Submit (送信)] をクリックし、変更を行わない場合は、[Close Window (ウィンドウを閉じる)] をクリックします。

インシデントの詳細の表示

1. 「Configure」> 「SSL」> 「Incidents」> 「Incident List」を順に選択します。
2. さらに詳しく検査するインシデントを見つけます。[インシデントの表示, 171 ページ](#) を参照してください。
3. 虫メガネをクリックし、下記のようなインシデントに関する追加の詳細情報を確認します。
 - 説明 (これはインシデント リストに表示されるメッセージです)
 - インシデントが作成された時刻
 - インシデントが変更された時刻
 - インシデント カウント (ユーザーがこのサイトにアクセスを試みた回数)

インシデント リストへの Web サイトの追加

許可する、ブラックリストに載せる、またはトネリングするサイトを指定するには、「Configure」> 「SSL」> 「Incidents」> 「Add Website (Web サイトを追加)」ページを順に選択します。手動で追加されたサイトには、時系列順の Ticket ID が割り当てられます。これらのサイトは、インシデント リストに表示されます。[インシデントの表示, 171 ページ](#) を参照してください。

1. インシデント リストに追加するサイトの URL を入力します。



ご注意

IPv6 アドレスを指定する場合は、アドレスを角括弧 () で囲んではいけません。

2. [By Certificate (証明書に基づく)] または [By URL (URL に基づく)] を選択します。
 - [By Certificate] は、より高度のセキュリティを提供します。証明書に基づき Web サイトを追加した場合、クライアントは、URL ではなく IP アドレスを使うことによってポリシーをバイパスすることはできません。[By Certificate] を選択した場合、SSL Manager はサーバー証明書を取得し、サイトをインシデント リストに追加します。[インシデントの表示, 171 ページ](#) を参照してください。

サイトが証明書によってブロックされている場合、ワイルドカードの証明書は、共通名が認識されている場合でも受け入れられません。

- サイトをトネリングする、許可する、またはブラックリストに載せるには、[By URL] を選択します。
3. [Action] ドロップダウン リストでサイトを [Tunnel]、[Allow]、または [Blacklist] のどのステータスで追加するかを指定します。詳細については、[インシデント レポート, 171 ページ](#) を参照してください。
- **Tunnel** : ([By URL] の場合のみ有効) このサイトはトネリングされます。トラフィックは復号化されず、SSL Manager は証明書をチェックしません。



ご注意

Tunnel by URL (URL に基づくトンネル) は、明示的プロキシトラフィックでのみ有効です。透過的プロキシトラフィックをトネリングするには、ARM [静的バイパス ルール](#) を使用します。

- **Allow** : ユーザは証明書が有効でない場合でもそのサイトにアクセスできます。トラフィックが復号化され、証明書チェック機能が無効にされます。
 - **Blacklist** ; そのサイトは完全にブロックされます。Verification Bypass (検証のバイパス) が設定されている場合でも、ユーザーはこのサイトにアクセスできません。
4. [Apply] をクリックします。

証明書検証エンジンを無効にし一定の時間ネットワークトラフィックをモニタした後、サイトを手動でインシデントリストに追加することを推奨します。([検証設定値の構成, 165 ページ](#) を参照してください。) それにより、信頼のあるサイトをトネリングし、アクセスすべきでない分かっているサイトをブロックすることによって、パフォーマンスを向上させます。トネリングなどステータスをサイトおよびインシデントに割り当てる方法については、[インシデント レポート, 171 ページ](#) を参照してください。

クライアント証明書

セキュリティのために、宛先サーバーはクライアント証明書を要求することがあります。

関連トピック :

- ◆ [クライアント証明書のインポート, 176 ページ](#)
- ◆ [クライアント証明書が常に要求された場合 : ホスト, 176 ページ](#)
- ◆ [クライアント証明書の削除, 177 ページ](#)

クライアント証明書が要求された場合

1. 「Configure」> 「SSL」> 「Client Certificates (クライアント証明書)」> 「General」を順に選択します。
2. SSL Manager がその証明書およびサイトを処理する方法を指定するには、[Tunnel] または [Create incident (インシデントを作成)] を選択します。トンネル以外の処理 (ホワイト リストに入れる) を使用する場合は、[Create incident] を選択しなければなりません。ホワイト リスト機能は、常にサーバーに証明書を提供します。可能な処理のリストについては、[インシデント レポート, 171 ページ](#) を参照してください。
3. [Apply] をクリックします。

クライアント証明書のインポート

クライアントが代表する組織から証明書をインポートするには、「Configure」> 「SSL」> 「Client Certificates」> 「Import (インポート)」ページを順に選択します。



重要

必ず、X.509 の形式の、base64 エンコード方式の証明書を使用してください。

1. クライアント証明書の名前を入力します。
2. 証明書のパブリック キーを入力します。キーについてネットワーク管理者に問い合わせる必要があります。
3. 証明書のプライベート キーを入力します。キーについてネットワーク管理者に問い合わせる必要があります。
4. パスフレーズを入力し、確認します。数字、文字、および大文字と小文字の組み合せた、強いパスフレーズを使用することを推奨します。パスフレーズについてネットワーク管理者に問い合わせる必要があります。
5. [Import (インポート)] をクリックします。

クライアント証明書が常に要求された場合：ホスト

クライアント証明書が常に要求される宛先サーバーをリストするには、「Configure」> 「SSL」> 「Client Certificates」> 「Hostlist (ホストリスト)」ページを順に選択します。必ず、証明書をインポートしてから、それをホストリストに追加してください。[クライアント証明書のインポート, 176 ページ](#) を参照してください。

1. クライアント証明書を必要とする宛先サーバーの URL を入力します。
2. [Client Certificate (クライアント証明書)] ドロップダウン リストからクライアント証明書の名前を選択します。このリストには、インポート済みの証明書だけが表示されます。

3. **[Add]** をクリックします。

クライアント証明書の削除

インポートしたクライアント証明書を削除するには、「**Configure**」>「**SSL**」>「**Client Certificates**」>「**Manage Certificates (クライアントを管理)**」ページを順に選択します。

1. 削除するクライアントを選択します。
2. **[Delete]** をクリックします。

SSL Manager ロギングの構成

関連トピック：

- ◆ [SSL ログが保持される時間, 178 ページ](#)
- ◆ [SSL ログ ファイル サイズの制限, 178 ページ](#)
- ◆ [SSL アクセス ログファイルに表示するフィールド, 179 ページ](#)

SSL Manager は、下記の 2 種類のログ ファイルを作成します。

- ◆ アクティビティ ログ。これらのログは、SSL Manager のアクティビティをモニタし、ユーザー インターフェイスで指定されたレベルでメッセージをログ記録します。
- ◆ アクセス ログ

You can log activity for both インバウンド (クライアントから SSL Manager へ) とアウトバウンド (SSL Manager からサーバーへ) の両方のトラフィックのアクティビティをログ記録できます。システム ログ (syslog) またはファイルにデータをログ記録するオプションがあります。

ログ ファイルの名前と場所を指定するには、「**Configure**」>「**SSL**」>「**Logging (ログ記録)**」>「**General**」ページを順に選択します。

1. インバウンドトラフィックの場合、保持するログ ファイルのタイプを選択します。アクティビティ ログの場合、ログ内で詳細のレベルを指定します。
2. ログ記録する詳細のレベルを指定するために、1 ~ 7 の数値を入力します。各レベルは詳細な情報を提供します。レベル 7 は最も詳細です。ロギングおよび詳細度のレベルは、下記の通りです。

1 (アラート)	システム ファイルが壊れたなど、すぐに修正する必要があるログの状態
2 (重大)	デバイスの障害などのログの状態

3 (ノーマル)	ログのエラー
4 (警告)	ログの警告
5 (注意)	エラー状態ではないが、注意が必要であるログの状態
6 (情報)	ログ情報のメッセージ
7 (デバッグ)	ログのデバッグ情報。レベル 7 は、大部分のログ アウトプットを含みます。

3. ログ データを syslog に記録するのか、ファイルに記録するのかを指定します。
4. アクセス ログ ファイルの場合は、[Step 2](#) と [Step 3](#) を繰り返します。
5. アウトバウンドトラフィックの場合は、[Step 2](#) から [Step 4](#) までを繰り返します。
6. **[Apply]** をクリックします。

ログは、`/opt/WCG/sxsuite/log` に書き込まれます。

SSL ログが保持される時間

24 時間ごとに新しいログ ファイルのセットが作成されます。デフォルトでは、これは午前 0 時に行われます。この交換は、ログ ファイルのサイズに関係なく行われます。さらに、ログファイルがスケジュールされた交換の前に最大サイズになった場合、そのログ ファイルは交換されます。その場合でも、午前 0 時にスケジュールされた交換が行われます。最大ログ サイズの指定の詳細については、[SSL ログ ファイル サイズの制限, 178 ページ](#) を参照してください。

ログ ファイルを保持する時間を指定するには、「**Configure**」>「**SSL**」>「**Logging**」>「**Options**」ページを順に選択します。

1. ファイルを保持する期間 (日数) を指定します。デフォルトは 3 です。
2. このページで追加のオプションを設定し、**[Apply]** をクリックします。

SSL ログ ファイル サイズの制限

ログ ファイルは毎日午前 0 時に交換されます。しかし、ファイルが指定した最大サイズになった場合、スケジュールした毎日の交換の前であっても、新しいログ ファイルが開始されます。ログ ファイルのサイズは 1 分ごとにチェックされますから、一時的にログ ファイルがその最大サイズよりも大きくなる場合があります。

ログ ファイルがその最大サイズになったとき、そのファイルは拡張子「 x 」(ここで x は、1、2、または 3 など) を付けて保存され、新しいファイルが開始されます。これを 24 時間内に複数回行う場合は、保持するファイルの数 (世代) を指定しなければなりません。ログ交換の詳細については、[SSL ログが保持される時間, 178 ページ](#) を参照してください。

ログ ファイルの最大サイズを指定するには、「**Configure**」>「**SSL**」>「**Logging**」>「**Options**」ページを順に選択します。

1. ログ ファイルの最大サイズを単位 KB で指定します。デフォルトは 50,000 KB です。
2. 世代については、ファイルが毎日の交換の前に複数回最大サイズになる場合に保持するログ ファイルの数を指定します。この数になると、新しいログ ファイルが作成され、最も古いログ ファイルが削除されます。デフォルトは 3 世代です。
3. このページで追加のオプションを設定し、**[Apply]** をクリックします。

SSL アクセス ログファイルに表示するフィールド

ログ ファイルを追加または削除するには、「**Configure**」>「**SSL**」>「**Logging**」>「**Options**」ページを順に選択します。

1. [Access log file customization (ログ ファイル アクセスのカスタム化)] ボックスでフィールドを削除または追加します。下記のフィールドがあります。

time_stamp	[YYYY.MM.DD HH:MM:SS] の形式のタイムスタンプ
time_of_day	raw 形式のタイムスタンプ: Sec.mSec starting from 1st Jan 1970 UTC
src_ip	クライアントの IP アドレス
auth_user	認証されたユーザー
account	ユーザーが属すアカウント
profile	ユーザーのプロファイル
req_line	下記のフォーマットの要求: "method path protocol/version.subversion"。例: GET / HTTP/1.1
status_code	Web サーバーによって送信された HTTP ステータス応答コード
user_agent	クライアントブラウザの名前
referer	URL のホスト セクション
content_type	コンテンツ (HTML、テキスト、イメージなど)
content_length	単位 バイト
server_host	Web サーバーの IP アドレス
bytes_from_client	クライアントから SSL Manager に転送されたバイト数
bytes_to_client	SSL Manager からクライアントに転送されたバイト数
bytes_from_server	Web サーバーから SSL Manager に転送されたバイト数
bytes_to_server	SSL Manager から Web サーバーに転送されたバイト数

2. **[Apply]** をクリックします。

SSL 接続エラー メッセージのカスタム化

下記の場合に、ユーザーが受け取るメッセージをカスタマイズできます。

- ◆ ユーザーが無効の証明書があるサイトに接続しようとしている。[証明書検証フィールド](#), [180 ページ](#) を参照してください。
- ◆ 接続エラーがある。[SSL 接続エラー](#), [181 ページ](#) を参照してください。

メッセージ テンプレートの中で下記の変数を利用できます。

%P	プロトコル (HTTP または HTTPS)
%h	メッセージを生成したプロキシのホストの IP アドレスおよびポート
%o	メッセージを生成したプロキシのホストの IP アドレス
%H	要求のリモート ホスト名
%t	時刻
%s	SSL Manager サーバーの名前
%u	完全な URL
\$\$DETAILS	詳細なエラー メッセージ
\$\$TICKET_ID	インシデントの ID 番号

証明書検証フィールド

証明書検証が失敗したときにユーザーが受け取るメッセージをカスタマイズするには、「**Configure**」>「**SSL**」>「**Customization**」>「**Certificate Failure (証明書エラー)**」ページを順に選択します。



ご注意

[Preview (プレビュー)] をクリックすると、デフォルトのメッセージがどのように表示されるか確認できます。

1. ウィンドウの HTML コードを編集してメッセージを反映させるようにします。メッセージで利用できる変数のリストについては、[SSL 接続エラー メッセージのカスタム化](#), [180 ページ](#) を参照してください。
2. **[Preview]** をクリックして変更を確認します。
3. メッセージが適切に表示されるまで、ステップ 1 と 2 を繰り返します。
4. 編集を確認するには、**[Apply]** をクリックし、また元のメッセージに戻るには **[Cancel (キャンセル)]** をクリックします。

SSL 接続エラー

SSL Manager が宛先 Web サーバーに接続できなかったときに、ユーザーが受け取るメッセージをカスタマイズするには、「**Configure**」>「**SSL**」>「**Customization**」>「**Connect Error (接続エラー)**」ページを順にクリックします。



ご注意

[Preview] をクリックすると、デフォルトのメッセージがどのように表示されるか確認できます。

1. ウィンドウのテキストを編集してメッセージを反映させるようにします。メッセージで利用できる変数のリストについては、[SSL 接続エラーメッセージのカスタム化, 180 ページ](#) を参照してください。
2. **[Preview]** をクリックして変更を確認します。
3. メッセージが適切に表示されるまで、ステップ 1 と 2 を繰り返します。
4. 編集を確認するには、**[Apply]** をクリックし、また元のメッセージに戻るには **[Cancel]** をクリックします。

14

セキュリティ

Websense Content Gateway によって、プロキシとネットワーク上の他のコンピュータの間のセキュアな通信を確立できます。以下のことが可能です。

- ◆ プロキシへのクライアント アクセスを制御する。[プロキシへのクライアント アクセスの制御](#), 183 ページ を参照してください。
- ◆ 下記のどちらかの方法で Content Gateway Manager へのアクセスを制御する。
 - 管理者アカウント ([管理者 ID およびパスワードの設定](#), 185 ページ および [ユーザー アカウントのリストの作成](#), 185 ページ を参照)。
 - 暗号化され、認証されたアクセスの場合の SSL (Secure Sockets Layer) 保護 ([セキュアな管理のための SSL の使用](#), 186 ページ を参照)。
- ◆ インターネットへのアクセスを制御し、特別の認証要件を指定し、プロキシを経由する他のトラフィックを制御するフィルタリングルールを作成する。[フィルタリングルール](#), 188 ページ を参照してください。
- ◆ Content Gateway をユーザーのファイアウォールに統合し、1 つ以上の SOCKS サーバーを通じてトラフィックを制御する。[SOCKS ファイアウォール統合の設定](#), 192 ページ を参照してください。
- ◆ Content Gateway がサイトのセキュリティ設定に対応するために複数の DNS サーバーを使用するように構成する。[Split DNS オプションの使用](#), 196 ページ を参照してください。
- ◆ Content Gateway がユーザー認証を実行するように設定する。プロキシは、統合 Windows 認証 (Kerberos を使用)、レガシー NTLM (NTLMSSP)、LDAP、および RADIUS ユーザー認証をサポートします。このほかに、複数の認証領域で複数の認証方法をサポートします。[プロキシユーザー認証](#), 197 ページ を参照してください。

プロキシへのクライアント アクセスの制御

Content Gateway が特定のクライアントにだけプロキシの使用を許可するように設定できます。

アクセスを許可するには、`ip_allow.config` でクライアントの IP アドレスと IP アドレス範囲を指定します。

アクセスを拒否するには、そのクライアントの IP アドレスをこのファイルに含めないようにします。

1. 「Configure (設定)」>「Security (セキュリティ)」>「Connection Control (接続の制御)」>「Proxy Access (プロキシ アクセス)」 ページへ移動します。
2. [Edit File (ファイルの編集)] をクリックして、ip_allow.config ファイルの編集のための設定ファイル エディタを開きます。
3. 表示される下記のフィールドに情報を入力し、[Add (追加)] をクリックします。各フィールドについては [設定のオプション](#) で説明しています。
4. [Apply (適用)] をクリックして情報を保存し、次に [Close (閉じる)] をクリックします。



ご注意

許可されていないクライアントが Content Gateway へのアクセスを試みた場合、要求されたコンテンツを取得できないことを知らせるメッセージがブラウザに表示されます。

Content Gateway Manager へのアクセスの制御

Content Gateway Manager へのアクセスを制限して、許可されているユーザーだけが設定オプションを変更し、パフォーマンスおよびネットワークトラフィック統計を表示できるようにできます。

以下のことが可能です。

- ◆ 管理者 ID およびパスワードを設定する。管理者 ID で Content Gateway Manager にログオンしたユーザーは、Content Gateway Manager のすべてのアクティビティにアクセスできます。[管理者 ID およびパスワードの設定, 185 ページ](#) を参照してください。
- ◆ Content Gateway Manager にログオンできるユーザーと、そのユーザーが実行できるアクティビティを決定するユーザー アカウントのリストを作成し、保守する。[ユーザー アカウントのリストの作成, 185 ページ](#) を参照してください。
- ◆ どのコンピューターが Content Gateway Manager にアクセスできるかを定義する IP アドレス アクセス制御リストを作成する。[Content Gateway Manager へのホスト アクセスの制御, 186 ページ](#) を参照してください。
- ◆ セキュアな管理のために SSL を使用する。[セキュアな管理のための SSL の使用, 186 ページ](#) を参照してください。
- ◆ 管理者に二要素認証を使用して、または使用せずに TRITON Unified Security Center にログオンし、次に、「TRITON – Web Security Content Gateway access (TRITON – Web Security Content Gateway アクセス)」ページを使用して Content Gateway Manager にログオンすることを要求する。[Content Gateway Manager へのアクセス, 11 ページ](#) を参照してください。

管理者 ID およびパスワードの設定

インストール時に、Content Gateway Manager への管理アクセスを制御するパスワードを割り当てます。正しい ID とパスワードを使用して Content Gateway Manager にログオンしたユーザーは、「Monitor (モニター)」タブのすべての統計を表示でき、また、「Configure (設定)」タブの任意の設定オプションを変更できます。

管理者 ID とパスワードは随時変更できます。

1. 「Configure」> 「My Proxy」> 「UI Setup (UI の設定)」> 「Login (ログイン)」タブに移動します。
2. [Basic Authentication (基本認証)] が有効になっていることを確認します。
Basic Authentication が無効化されている場合は、アクセスを拒否する IP アドレスのリスト ([Content Gateway Manager へのホストアクセスの制御, 186 ページ](#) を参照) をセットアップしていない限り、すべてのユーザーが Content Gateway Manager にアクセスできます。
3. 現在の管理者 ID を変更するには、[Administrator (管理者)] セクションの [Login (ログイン)] フィールドに新しい ID を入力します。
4. 現在のパスワードを変更するには、[Old Password (古いパスワード)] フィールドに現在のパスワードを入力します。[New Password] フィールドに新しいパスワードを入力し、次に [New Password (Retype) (新しいパスワード (再入力))] フィールドに新しいパスワードを再入力します。
現在の管理者パスワードを忘れた場合、[マスタ管理者パスワードを忘れた場合に Content Gateway Manager にどのようにアクセスしますか, 482 ページ](#) をご覧ください。
5. [Apply (適用)] をクリックします。

ユーザー アカウントのリストの作成

Content Gateway Manager のために 1 つの管理者 ID とパスワードを設定するだけではニーズに対応する十分なセキュリティを確保できない場合、Content Gateway Manager にアクセスできるユーザーと、そのユーザーが実行できるアクティビティを定義するユーザー アカウントのリストを作成することができます。

1. 「Configure」> 「My Proxy」> 「UI Setup」> 「Login (ログイン)」に移動します。
2. Content Gateway Manager へのアクセスを許可するユーザーの名前を入力します。
3. そのユーザーのパスワードを入力し、次に [New Password (Retype)] フィールドにそのパスワードを再入力します。
4. [Apply] をクリックします。
5. ユーザー テーブルの [Access (アクセス)] ドロップダウン リストで、ユーザーが実行できる Content Gateway Manager アクティビティを選択します。

- ユーザーによる Content Gateway Manager へのアクセスを無効化するには、**[No Access (アクセス禁止)]** を選択します。
 - ユーザーに「Monitor」タブでの統計の表示のみを許可する場合は **[Monitor Only (モニターのみ)]** を選択します。
 - ユーザーに「Monitor」タブでの統計の表示と「Configure」タブでの設定オプションの表示を許可する場合は **[Monitor and View Configuration (モニターおよび設定の表示)]** を選択します。
 - ユーザーに「Monitor」タブでの統計の表示と「Configure」タブでの設定オプションの変更を許可する場合は **[Monitor and Modify Configuration (モニターおよび設定の変更)]** を選択します。
6. **[Apply]** をクリックします。
 7. Content Gateway Manager へのアクセスを許可する各ユーザーについて、[Step 2 ~ Step 6](#) の手順を繰り返します。
 8. **[Basic Authentication]** が有効になっていることを確認します。
Content Gateway は、このオプションが有効化されている場合にのみ、ユーザー名とパスワードをチェックします。

Content Gateway Manager へのホスト アクセスの制御

管理者 ID とユーザー アカウントの使用のほかに、どのホストが Content Gateway Manager にアクセスできるかを管理することができます。

1. 「Configure」>「My Proxy」>「UI Setup Access (UI 設定 アクセス)」へ移動します。
2. **[Access Control (アクセス制御)]** 領域で、**[Edit File]** をクリックして、**mgmt_allow.config** ファイルの編集のための設定ファイル エディタを開きます。
3. 表示される下記のフィールドに情報を入力し、**[Add]** をクリックします。すべてのフィールドは [UI Setup \(UI の設定\), 297 ページ](#) で説明しています。
4. **[Apply]** をクリックし、次に **[Close]** をクリックします。

セキュアな管理のための SSL の使用

Websense は、Content Gateway Manager によるリモート管理モニタリングおよび設定を保護するために Secure Sockets Layer protocol (SSL) をサポートします。SSL セキュリティは、証明書を使用してネットワーク接続の両端の認証を提供し、暗号化を使用してプライバシーを提供します。

SSL を使用するには、以下の準備が必要です。

- ◆ SSL 証明書を取得する
- ◆ Content Gateway Manager SSL オプションを有効化する

SSL 証明書の取得

SSL 証明書は、承認された認証機関から取得できます（例、VeriSign）。証明書を Content Gateway の `config` ディレクトリ（`/opt/WCG/bin`）にインストールします。証明書ファイルの名前をデフォルトのファイル名 `private_key.pem` に変更するか、または Content Gateway Manager を使用して証明書の名前を指定します（[SSL の有効化](#), 187 ページ の手順に従います）。

SSL の有効化

SSL 証明書を取得した後、SSL を有効化することができます。

1. 「**Configure**」 > 「**My Proxy**」 > 「**UI Setup**」 > 「**General**」 タブに移動します。
2. **HTTPS** オプションを有効化します。
3. [Certificate File (証明書ファイル)] フィールドで、SSL 証明書のファイル名を指定します。
ファイル名の変更が必要になるのは、証明書ファイルがデフォルトの名前 `private_key.pem` を使用しない場合だけです。
4. [**Apply**] をクリックします。

FIPS 140-2 モード

FIPS (Federal Information Processing Standard) 140-2 は、米国政府のハードウェアおよびソフトウェア暗号化モジュールに関するセキュリティ標準です。この標準に基づいて認証されているモジュールは、政府および他のユーザーに対して、システムで使用する暗号が厳格な基準に適合していることを保証します。

Content Gateway バージョン 7.7 で使用している暗号ライブラリは、FIPS 140-2 認証の申請中です。詳細については、[Cryptographic Module Validation Program \(CMVP\) 確認ページ](#)を参照してください。

デフォルトでは、FIPS 140-2 は SSL 接続には適用されません。

Content Gateway が HTTPS 接続に FIPS 140-2 を適用するように設定することによって、HTTPS 接続が TLSv1 および FIPS 140-2 によって承認されたアルゴリズムを使用することを保証することができます。ただし、このオプションを一度有効化すると、Content Gateway を完全に再インストールしない限り無効化できません。Content Gateway がアプライアンス上にある場合、アプライアンスを再構成しなければなりません。

HTTPS 接続上で FIPS 140-2 を有効化するには、以下の手順を実行します。

1. Content Gateway Manager で、「**Configure**」 > 「**Security**」 > 「**FIPS Security (FIPS セキュリティ)**」に進みます。
2. 警告を確認し、[**Enabled**] を選択し、[**Apply**] をクリックします。
3. FIPS を有効化する場合は、Content Gateway を再起動します。

4. FIPS を有効化しない場合は、[Disable] を選択して、[Apply] をクリックします。

フィルタリング ルール

Content Gateway は、要求のいくつかのパラメータを検査して、条件に一致する場合に指定した処置を提供するためのルールを作成する機能をサポートします。以下のようなルールを作成できます。

- ◆ URL 要求を拒否または許可する
- ◆ カスタム ヘッダを挿入する
- ◆ 指定したアプリケーション、または指定した Web サイトの要求が認証をバイパスすることを許可する
- ◆ クライアント要求のヘッダ情報を保持または削除する
- ◆ 指定したアプリケーションがプロキシを通過することを禁止する



ご注意

NTLM および LDAP 認証のルールを作成する方法については、[複数レールの認証, 216 ページ](#)を参照してください。Content Gateway 認証オプションの使用を開始する方法については、[プロキシ ユーザー認証, 197 ページ](#)を参照してください。

フィルタリング ルールの作成および変更は、「Configure」> 「Security」> 「Access Control」> 「Filtering」タブ上で行います。ルールは `filter.config` ファイルに保存されます。

ルールはリストの上から順に適用されます。最初に条件に一致したルールだけが適用されます。条件に一致するルールがない場合、要求は処理されます。

二次指定子は任意です。ルールの中で2つ以上の二次指定子を使用できます。ただし、1つの二次指定子を繰り返すことはできません。

ルールを追加、削除または変更した後、Content Gateway を再起動します。

保存されているルールの構成に関する詳細は、[filter.config](#) を参照してください。

フィルタリング ルールの作成

1. 「Configure」> 「Security」> 「Access Control」> 「Filtering」タブに移動し、[Edit File] をクリックして、ファイル エディタで `filter.config` を開きます。
2. ドロップダウンリストから [Rule Type (ルール タイプ)] を選択します。ルール タイプは、ルールが適用する処置を指定します。下記のオプションがサポートされています。

「allow (許可)」-- 特定の URL 要求が認証をバイパスすることを許可します。プロキシは要求されたコンテンツをキャッシュに入れ、提供します。

「deny (拒否)」-- 特定の宛先からのオブジェクトの要求を拒否します。要求が拒否されたとき、クライアントはアクセス拒否メッセージを受け取ります。

「keep_hdr」-- どのクライアント要求ヘッダ情報を保持するかを指定します。

「strip_hdr」-- どのクライアント要求ヘッダ情報を削除するかを指定します。

「add_hdr」-- カスタムのヘッダと値のペアを挿入します。カスタムヘッダとヘッダ値が指定されている必要があります。特定のヘッダと値のペアを要求する宛先ポストをサポートします。具体例を下の [Google enterprise gmail を許可する add_hdr ルールの作成](#) に示しています。



ご注意

「radius」ルールタイプはサポートされていません。

3. [Primary Destination Type (一次宛先タイプ)] を選択し、次に [Primary Destination Value (一次宛先値)] フィールドに対応する値を入力します。一次宛先タイプには、下記のタイプが含まれます。
 - dest_domain -- 要求されたドメイン名。対応する値はドメイン名です。
 - dest_host -- 要求されたホスト名。対応する値はホスト名です。
 - dest_ip -- 要求された IP アドレス。対応する値は IP アドレスです。
 - url_regex -- URL に含まれる正規表現。対応する値は正規表現です。
4. 一次宛先タイプが keep_hdr または strip_hdr である場合、[Header Type (ヘッダタイプ)] ドロップダウンリストから保持または削除する情報のタイプを選択します。以下のオプションがあります。
 - date (日付)
 - host (ホスト)
 - Cookie (クッキー)
 - client_ip
5. ルールが特定のポート上のインバウンドトラフィックにのみ適用される場合、プロキシポートの値を入力します。
6. ルールタイプが add_hdr である場合、カスタムヘッダおよびヘッダ値を指定します。カスタムヘッダとヘッダ値は、宛先ホストが想定している値でなければなりません。下の Google Business Gmail の例を参照してください。
7. 要求または想定されている二次指定子の値を提供します。以下の二次指定子があります。
 - Time (時間) -- 時間範囲 (例、08:00-14:00) を指定します。
 - Prefix (接頭辞) -- URL のパス部分の接頭辞を指定します。
 - Suffix (接尾辞) -- URL のファイル接尾辞を指定します。
 - Source IP address (ソース IP アドレス) -- 1 つのクライアント IP アドレス、またはクライアントの IP アドレスの範囲を指定します。

Port (ポート)— 要求された URL 中のポートを指定します。

Method (メソッド)— 要求された URL メソッドを指定します。

- ・ get
- ・ post
- ・ put
- ・ trace

Scheme (スキーム)— 要求された URL のプロトコルを指定します。以下のオプションがあります。

- ・ HTTP
- ・ HTTPS
- ・ FTP (FTP over HTTP の場合のみ)

User-Agent (ユーザーエージェント)— 要求ヘッダのユーザーエージェントの値を指定します。これは正規表現 (regex) です。

[User-Agent] フィールドを使用して、下記のような処置を行うアプリケーション フィルタリング ルールを作成できます。

- ・ 認証の要求を適切に処理しないアプリケーションが認証をバイパスすることを許可する
- ・ 特定のクライアントベースのアプリケーションからのインターネットのアクセスを禁止する

より詳しい説明といくつかの例が、Websense Knowledge Base の『When authentication prevents devices, browsers, and custom applications from working with the proxy』というタイトルの記事に収録されています。

8. ルールの定義が完了したとき、[Add] をクリックしてルールを追加し、次に、[Apply] をクリックしてルールを保存します。
9. ルールの追加が完了したとき、[Apply] をクリックしてすべての変更を保存し、次に、[Close] をクリックして編集ウィンドウを閉じます。
10. 新しいルールを有効にするには、[Content Gateway Manager] ウィンドウを選択し、Content Gateway を再起動します。

ルールの編集

1. 「Configure」> 「Security」> 「Access Control」> 「Filtering」に進み、[Edit File] をクリックしてファイル エディタで *filter.config* を開きます。
2. リストの中の変更するルールを選択し、希望する値に変更します。
3. [Set (設定)] をクリックしてルールを更新し、[Apply] をクリックしてルールを保存します。
4. [Close] をクリックして編集ウィンドウを閉じます。
5. 変更を有効にするには、[Content Gateway Manager] ウィンドウを選択し、Content Gateway を再起動します。

Google enterprise gmail を許可する add_hdr ルールの作成

Google は要求の中のカスタム ヘッダの形で、Google が enterprise gmail および他の Google Apps for Business へのアクセスを認識し、許可またはブロックするメカニズムを提供しています。

Google のソリューションが TRITON – Web Security および Content Gateway と共に使用して enterprise gmail を処理できるようにするには、以下の手順を実行します。

1. TRITON – Web Security で、Web Security カテゴリ「**Internet Communication**」>「**General Email**」を許可します。
2. Content Gateway Manager で HTTPS (SSL 暗号化) を有効化します。サイトでまだ SSL Manager を使って HTTPS を管理していない場合は、この機能をよく理解してから有効化してください。
3. Content Gateway Manager の「**Configure**」>「**Security**」>「**Access Control**」ページで `filter.config` を開き、`add_hdr` ルールを作成します。



ご注意

`add_hdr` ルール タイプは、カスタム ヘッダ-値のペアを使用して特殊な処理を実施する任意のサイトに使用できます。

- a. `add_hdr` を選択します。
- b. [Primary Destination Type] には `dest_domain` を選択します。
- c. [Primary Destination Value] には、“`mail.google.com`” を指定します。
- d. [Custom Header] フィールドで、“`X-GoogApps-Allowed-Domains`” を指定します。
- e. [Header Value] フィールドで、自分のドメイン、またはドメインのリスト（カンマで区切る）を指定します。例：
`www.example1.com,www.example2.com`
- f. [Add] をクリックしてルールを追加します。
- g. [Apply] をクリックしてすべての変更を保存し、次に、[Close] をクリックして編集ウィンドウを閉じます。
- h. 新しいルールを有効にするために、Content Gateway を再起動します。

ユーザーが許可されていないアカウントから Google サービスにアクセスしようとしたとき、Google は下のようなブロック ページを表示します。



This service is not available

Gmail is not available for bob@gmail.com within this network. Gmail is only available for accounts in the following domains:

- [example1.com](#)
- [example2.com](#)

Please talk to your network administrator for more information.

Did you use this product with a different Google Account? [Sign out](#) of your current Google Account and then sign in to the account you want.

©2011 Google - [Google Home](#) - [Terms of Service](#) - [Privacy Policy](#) - [Help](#)

Google Business Apps と Websense Web Security Gateway および Web Security Gateway Anywhere を合わせて使用する方法的詳細については [\[link to KBA\]](#) を参照してください。Google のフィルタリング ソリューションについての Google による説明は、『[Block access to consumer accounts and services while allowing access to Google Apps for your organization](#)』に掲載されています。

SOCKS ファイアウォール統合の設定

関連項目：

- ◆ [SOCKS サーバーの設定, 193 ページ](#)
- ◆ [SOCKS プロキシ オプションの設定, 195 ページ](#)
- ◆ [SOCKS サーバー バイパスの設定, 195 ページ](#)

SOCKS はネットワーク ファイアウォールとしてよく使われており、SOCKS サーバーの後方のホストがインターネットへの完全なアクセスを取得することを許可し、同時に、インターネットからファイアウォールの内側のホストへの無許可のアクセスを禁止します。

Content Gateway はキャッシュに保存されていないコンテンツへの要求を受け取ったとき、オリジン サーバーにそのコンテンツを要求しなければなりません。SOCKS 設定では、プロキシはオリジン サーバーに直接にアクセスする代わりに、SOCKS サーバーを経由してアクセスします。SOCKS サーバーはプロキシとオリジン サーバーの間の通信を許可し、データをオリジン サーバーに中継します。次に、オリジン サーバーは SOCKS サーバーを経由してプロキシにコンテンツを返送します。キャッシュが有効化されている場合、Content Gateway はコンテンツをキャッシュに入れてからクライアントに送信します。

- ◆ Content Gateway は SOCKS クライアントとして動作でき、SOCKS クライアントとして HTTP または FTP 要求を通常通りに受信および提供します。
- ◆ Content Gateway は SOCKS プロキシとして動作でき、SOCKS サーバーとの間での要求のやりとり（通常はポート 1080 上）を中継します。
- ◆ Content Gateway は、V- シリーズ アプライアンス上にインストールされている時、SOCKS サーバーとして動作でき、SOCKS サーバーのすべてのサービスを提供します。（Content Gateway は、アプライアンス上にインストールされていない時、SOCKS サーバーとして動作できません）。

SOCKS サーバーの設定

Content Gateway は、ネットワーク内の 1 つ以上の SOCKS サーバーを処理するように設定できます。Content Gateway が V- シリーズ アプライアンス上にインストールされている時、SOCKS サーバーはそのモジュールに含まれています。



ご注意

Content Gateway が V- シリーズ アプライアンス上にインストールされていない時、Content Gateway に SOCKS サーバーは提供されません。

SOCKS サーバーを設定するには、下記の手順を実行します。

1. SOCKS 機能を有効化します。
 - a. [Configure] > [My Proxy] > [Basic] > [General] の順に選択します。
 - b. [Features (フィーチャ)] テーブルの [Security] セクションで、[SOCKS On] をクリックし、次に、[Apply] をクリックします。
 - c. Content Gateway の再起動
2. SOCKS のバージョンを指定します。
 - a. [Configure] > [Security] > [SOCKS] > [General] の順に選択します。
 - b. SOCKS サーバー上で実行している SOCKS のバージョンを選択し、[Apply] をクリックします。
3. アプライアンス上の V- シリーズ SOCKS を設定するには、以下の手順を実行します。
 - a. 「Server (サーバー)」 タブを選択します。
 - b. [On- Appliance SOCKS Server (アプライアンス上の SOCKS サーバー)] 領域で、[Enabled (有効)] を選択し、[Apply] をクリックします。
socks_server.config ファイルにサーバーのエントリが作成されます。
 - c. デフォルト エントリを変更するには、[SOCKS Server] 領域で [Edit File] を選択します。エディタで 「On- Appliance- SOCKS- Server」 ルールを選択します。

ポートを変更することができ、それがデフォルトの SOCKS サーバーであるかどうか、およびサーバー認証が適用されるかどうかの設定を変更できます。

サーバー名または IP アドレスは変更できません。これは常にループバックアドレスです。

必要な変更を行った後、[Set] をクリックします。

4. ネットワーク内での他の SOCKS サーバーの使用を設定するには、以下の手順を実行します。
 - a. 「**Server**」タブを選択し、[SOCKS Server] 領域で [Edit File] をクリックします。
 - b. SOCKS サーバー名を入力します。
 - c. SOCKS サーバーの IP アドレス、またはネットワーク内の DNS サーバーによって解決できるドメイン名を入力します。
 - d. これをデフォルトの SOCKS サーバーとして指定するかどうかを選択します。
 - e. 認証を使用する場合、SOCKS ユーザー名とパスワードを指定します。
 - f. [Set] をクリックして、サーバーをリストに追加します。

いつでもエディタに戻って、ルールを選択し、変更を行い、[Set] をクリックしてそれを保存することができます。
5. 複数の SOCKS サーバーがある場合、それらを追加した後、または追加中に、それらを優先順に編成することができます。そのためには、エントリを選択して上向きおよび下向き矢印を使って、リスト内でそのエントリを上または下に移動します。
6. [Apply] をクリックしてすべての変更を確認し、次に、[Close] をクリックしてエディタを閉じます。
7. [SOCKS Server Rules (SOCKS サーバー ルール)] 領域で、宛先 IP アドレスによって特定のルーティングまたはバイパスを指定するルールを作成できます。[SOCKS サーバー バイパスの設定, 195 ページ](#) を参照してください。
8. すべての SOCKS サーバーに適用する設定オプションを検討するには、「Options」タブを選択します。
 - a. [Server Connection Timeout (サーバー接続タイムアウト)] の値を検討し、調整します。これは Content Gateway が SOCKS サーバーへの接続を試みて待機する時間(秒)を指定します。この時間を過ぎるとタイムアウトになります。
 - b. [Connection Attempts Per Server (サーバーあたりの接続試行回数)] の値を検討し、調整します。これは Content Gateway が特定の SOCKS サーバーへの接続を試みる回数を指定します。この回数を超えると、サーバーに「接続不能」というマークが付けられます。
 - c. [Server Pool Connection Attempts (サーバー プール接続試行回数)] の値を検討し、調整します。これは Content Gateway がプール内の特定の SOCKS サーバーへの接続を試みる回数を指定します。この回数を超えると、試行を中止します。

9. SOCKS サーバー設定が完了したとき、**[Apply]** をクリックし、次に、**[Configure]** > **[My Proxy]** > **[General]** を選択して Content Gateway を再起動します。

リストからサーバーを削除するには、以下の手順を実行します。

1. **[SOCKS Server]** 領域で **[Edit File]** をクリックします。
2. リストの中で、削除するエントリを選択し、リストの左側の **X** をクリックします。
3. **[Apply]** をクリックし、次に、エディタを終了する準備ができたとき、**[Close]** をクリックします。
4. 設定が完了したとき、**[Configure]** > **[My Proxy]** > **[General]** を選択して Content Gateway を再起動します。

SOCKS プロキシ オプションの設定

Content Gateway を SOCKS プロキシとして設定するには、SOCKS プロキシ オプションを有効化し、Content Gateway が SOCKS クライアントからの SOCKS トラフィックを受け付けるポートを指定します。

SOCKS プロキシとして、Content Gateway はクライアントからの SOCKS パケットを受信し（通常はポート 1080 上で）、要求を SOCKS サーバーへ直接に転送することができます。



ご注意

SOCKS オプションを有効化し、[SOCKS サーバーの設定, 193 ページ](#) に示している SOCKS サーバー情報を指定するだけでなく、SOCKS プロキシ オプションを設定しなければなりません。

1. **[Configure]** > **[Security]** > **[SOCKS]** > **[Proxy]** の順に選択します。
2. **SOCKS プロキシ** を有効化します。
3. Content Gateway が SOCKS トラフィックを受け入れるポートを指定します。デフォルト ポートは 1080 です。
4. **[Apply]** をクリックします。
5. **[Configure]** > **[My Proxy]** > **[Basic]** > **[General]** で **[Restart]** をクリックします。

SOCKS サーバー バイパスの設定

Content Gateway が SOCKS サーバーをバイパスし、特定のオリジン サーバーに直接にアクセスするように設定することができます。

1. [Configure] > [Security] > [SOCKS] > [Server] の順にクリックします。
[SOCKS Server Rules (SOCKS Server ルール)] 領域で、[Edit File] を選択して socks.config を開きます。
2. 既存のルールを変更するには、リストからルールを選択し、変更を行い、[Set] をクリックします。
3. 新しいルールを作成するには、パラメータを指定して [Add (追加)] をクリックします。
 - a. ルールタイプを選択します。
SOCKS サーバーを通過する
SOCKS サーバーを通過しない
 - b. 宛先 IP アドレスまたはアドレスの範囲を指定します。「すべてのネットワークブロードキャストアドレス」(255.255.255.255) を指定してはいけません。
 - c. トラフィックに使用する SOCKS サーバーを選択します。
 - d. トラフィックを指定された SOCKS サーバーにラウンドロビン方式で配分するかどうかを指定します。
 - e. [Add] をクリックしてルールを追加します。
4. [Apply] をクリックし、次に [Close] をクリックします。
5. [Configure] > [My Proxy] > [Basic] > [General] で [Restart] をクリックします。

Split DNS オプションの使用

セキュリティ要件に応じて、Content Gateway が複数の DNS サーバーを使用するように設定できます。たとえば、Content Gateway が 1 つの DNS サーバーのセットを使って社内ネットワーク上のホスト名を解決し、ファイアウォールの外側の DNS サーバーがインターネット上のホストを解決するように設定することができます。これによってイントラネットのセキュリティを維持し、同時に組織外のサイトへの直接のアクセスを提供します。

[Split DNS (分割 DNS)] を設定するためには、次のタスクを実行しなければなりません。

- ◆ 宛先ドメイン、宛先ホスト、または URL 正規表現を基に DNS サーバー選択を実行するためにルールを指定します。
- ◆ [Split DNS] オプションを有効化する。

Content Gateway Manager で以下の手順を実行します。

1. 「Configure」 > 「Networking」 > 「DNS Resolver」 > 「Split DNS」 タブを選択します。
2. [Split DNS] オプションを有効化する。

3. [Default Domain (デフォルト ドメイン)] フィールドで、分割 DNS 要求のデフォルト ドメインを入力します。Content Gateway は、自動的にこの値を、使用する DNS サーバーを決定する前の、ドメインを含まないホスト名に付加します。
4. [DNS Servers Specification (DNS サーバー指定)] 領域で、[Edit File] をクリックして、*splitdns.config* ファイルの編集のための設定ファイル エディタを開きます。
5. 表示される下記のフィールドに情報を入力し、[Add] をクリックします。すべてのフィールドは *splitdns.config* で説明しています。
6. [Apply] をクリックし、次に [Close] をクリックします。
7. 「Split DNS」タブで、[Apply] をクリックして設定を保存します。
8. [Configure] > [My Proxy] > [Basic] > [General] で [Restart] をクリックします。

プロキシ ユーザー 認証

関連項目：

- ◆ [ブラウザの制約, 199 ページ](#)
- ◆ [透過的プロキシ認証の設定, 200 ページ](#)
- ◆ [統合 Windows 認証, 201 ページ](#)
- ◆ [レガシー NTLM 認証, 207 ページ](#)
- ◆ [LDAP 認証, 210 ページ](#)
- ◆ [RADIUS 認証, 213 ページ](#)
- ◆ [複数レルムの認証, 216 ページ](#)

Content Gateway は、ユーザーにコンテンツへのアクセスを許可する前にユーザー認証を行うためのいくつかの方法をサポートします。これらの方法と Websense Web Security ユーザー認証エージェントを合わせて使用することによって、プロキシ ユーザー認証が利用できなくなった場合のフェールオーバーを提供できます。

明示および透過プロキシ モードの両方で、Content Gateway は、下記の方法によるユーザー認証をサポートします。

- ◆ [統合 Windows 認証, 201 ページ](#) (Kerberos による)
- ◆ [レガシー NTLM 認証, 207 ページ](#) (NTLMSSP)
- ◆ [LDAP 認証, 210 ページ](#)
- ◆ [RADIUS 認証, 213 ページ](#)

このほかに、Content Gateway は下記の認証のために [複数レルムの認証, 216 ページ](#) をサポートします。

- ◆ 特定のドメインに対する個別の IP アドレスのセットの認証
- ◆ 特定のドメインに対する特定のポート上のトラフィックの認証（明示のプロキシのみ）
- ◆ 上記の組み合わせ（明示のプロキシのみ）

それぞれのレルム（定義は下記を参照）に対して 1 つの認証メソッド（統合 Windows 認証、NTLM または LDAP）が指定されています。この機能を使用すると、複数のメソッドを使って複数のレルムのユーザーを認証できます。

複数のレルムの認証に関連する用語

- ◆ **ドメイン**は、Windows Active Directory の 1 つのドメインです。
- ◆ **レルム**は、他のドメインとの間にアウトバウンドの信頼関係がない Windows Active Directory ドメインです。したがって、レルムは、そのメンバーがドメイン内のドメイン コントローラによって認証されることを要求します。

認証モードの選択

認証モードは Content Gateway Manager の「**Configure**」>「**My Proxy**」>「**Basic**」ページの「**Authentication**」セクションで選択します。複数のレルムが存在する環境での認証の設定では、最初に「**Multiple Realm Authentication（複数レルムの認証）**」オプションを選択します。

サポートされているドメイン コントローラとディレクトリ

- ◆ Windows NT ドメイン コントローラ
- ◆ Windows 2003 および 2008 の Active Directory
- ◆ Novell eDirectory 8.7 および 8.8 (LDAP のみ)
- ◆ Oracle DSEE 11g, Sun Java 7 および 6.2 (LDAP のみ)

Windows Active Directory を使用する時の最善の方法

1 つの Active Directory ドメインがあるか、すべての Active Directory ドメインがインバウンドおよびアウトバウンドの信頼関係を共有している場合の最善の方法は、統合 Windows 認証を使用することです。

複数のレルムがあり、認証が必要である場合、複数レルム オプションを使用しなければなりません。詳細（ポリシーの適用の制限に関する説明を含む）については、[複数レルムの認証, 216 ページ](#) を参照してください。

ユーザー識別だけで十分である場合、Web Security ユーザー識別オプションの 1 つを使用することができます。『*User Identification in TRITON — Web Security Help*』というタイトルのセクションを参照してください。

透過的ユーザー認証

Content Gateway は透過的認証（シングル サインオン）と対話形式（プロンプト形式）の認証の両方をサポートします。透過的認証は統合 Windows 認証およびレガシー NTLM によってサポートされます。一部のブラウザは、限定的なサポートのみを提供します。[ブラウザの制約, 199 ページ](#) を参照してください。

Windows ネットワークで、シングル サインオンを設定している時、ユーザーは一度だけサインオンすれば、すべての許可されているネットワーク リソースに透過的にアクセスできます。したがって、ユーザーがすでに Windows ネットワークに正常にログオンしている場合、Windows ログオン時に指定された証明書がプロキシ認証に使用され、ユーザーは再びユーザー名とパスワードの入力を求められることはありません。

対話形式の認証は、シングル サインオンに設定されていないネットワークで、また、シングル サインオンをサポートしないブラウザで使用するためにサポートされます。対話形式の認証では、ユーザーは Content Gateway を通じてコンテンツにアクセスできるようになる前に、資格情報の入力を要求されます。

バックアップ ドメイン コントローラ

統合 Windows 認証およびレガシー NTLM に対して、Content Gateway はフェールオーバー用のバックアップ ドメイン コントローラの指定をサポートします。プライマリ ドメイン コントローラがプロキシ要求に応答しない場合、Content Gateway はリストの中の次のドメイン コントローラ（バックアップ ドメイン コントローラ）にコンタクトします。次の要求に対して、プロキシは再びプライマリ ドメイン コントローラへのコンタクトを試み、接続が失敗した場合、バックアップ ドメイン コントローラにコンタクトします。

ブラウザの制約

すべての Web ブラウザが透過的ユーザー認証をサポートするわけではありません。



ご注意

最も完全で最新の情報については、[『version 7.7 Content Gateway Release Notes』](#)を参照してください。

下のテーブルは、統合 Windows 認証 (IWA) が構成されている時に、ブラウザが認証要求に対応する方法を示しています。

ブラウザ / OS	Internet Explorer (v8 & 9 でテスト済み)	Firefox (v11 でテスト済み)	Chrome (v17 & 18 でテスト済み)	Opera (v10 が Windows 上で、v11 が Red Hat 上でテスト済み)	Safari (v5 でテスト済み)
Windows	透過的認証を実行	透過的認証を実行	透過的認証を実行	NTLM にフォールバックして資格情報を要求	NTLM にフォールバックして資格情報を要求

ブラウザ / OS	Internet Explorer (v8 & 9 でテスト済み)	Firefox (v11 でテスト済み)	Chrome (v17 & 18 でテスト済み)	Opera (v10 が Windows 上で、v11 が Red Hat 上でテスト済み)	Safari (v5 でテスト済み)
Mac OS X	対応しない	透過的認証を実行	ブラウザの問題により IWA が機能しない	テスト未実行	透過的認証を実行
Red Hat Enterprise Linux, update 6	対応しない	透過的認証を実行	ブラウザの問題により IWA が機能しない	どの形式のプロキシ認証もサポートしない	対応しない



ご注意

資格情報を要求された時に、ユーザーがドメイン名を入力しない場合、セッション タイムアウト エラーが発生するか、ユーザーが再び入力を要求されます。

透過的プロキシ認証の設定

Content Gateway がユーザー認証も実行する透過的プロキシである場合、いくつかの特別な認証関連の設定オプションを設定する必要があります。

Content Gateway Manager で「**Configuration**」>「**Security**」>

「**Access**」「**Control**」>「**Transparent Proxy Authentication**」タブを選択します。

- ◆ **[Redirect Hostname (リダイレクト ホスト名)]** (任意) は、プロキシの代替ホスト名を指定します。統合 Windows 認証 (IWA) ではリダイレクト ホスト名は不必要であり、使用されません。

デフォルトでは、認証を行っているクライアントは、Content Gateway コンピュータのホスト名へリダイレクトされます。クライアントが DNS によってそのホスト名を解決できない場合、またはプロキシに代替の DNS 名が定義されている場合、**[Redirect Hostname]** フィールドでそのホスト名を指定できます。



ご注意

透過的プロキシ ユーザーの認証が透過的に (つまり、ユーザーに資格情報を要求することなしに) 行われるようにするには、リダイレクト ホスト名がブラウザのイントラネットゾーンに含まれるようにブラウザを設定しなければなりません。そのためには、一般的には、リダイレクト ホスト名がブラウザを実行しているコンピュータと同じドメインに含まれるようにします。たとえば、クライアントが **workstation.example.com** で、リダイレクト ホスト名が **proxyhostname.example.com** である場合、ブラウザは認証が透過的に行われる (ユーザーに認証を要求しない) ことを許可します。ご使用のブラウザのマニュアルを参照してください。

- ◆ **[Authentication Mode (認証モード)]** は、透過的認証モードを指定します。Content Gateway は下記のいずれかのモードに設定しなければなりません。
 - **[IP mode (IP モード)]** [IP mode] (デフォルト) では、セッションの認証時に、クライアントの IP アドレスは 1 つのユーザー名に関連付けられます。その IP アドレスからの要求は、**セッション TTL** (セッション継続時間、デフォルト = 15 分) に達すまで、再び認証されることはありません。セッション継続時間内にその IP アドレスから生成された要求は、その IP アドレスに関連付けられているユーザーによって生成されたものとみなされます。
 - **[Cookie Mode (クッキー モード)]** [Cookie Mode] は、1 つの IP アドレス - たとえば 1 つの端末サーバー環境内、またはプロキシ チェイニング環境内、もしくはネットワーク アドレス変換 (NAT) が行われる環境の中の IP アドレス - を共有する複数のユーザーを一意に識別するために使用します。
- ◆ **[Session TTL (セッション継続時間)]** - ユーザーのセッションが認証された後、そのセッションは **[Session TTL]** (継続時間、デフォルト = 15 分) で指定されている時間の間有効です。有効な値の範囲は 5 - 65535 分です。

これらのフィールドのいずれかを変更した時は、必ず **[Apply]** をクリックして変更を保存し、次にプロキシを再起動して、変更を有効化してください。



ご注意

Content Gateway は WCCP ロード バランシングを使用して、プロキシ クラスタでの透過的認証をサポートします。ただし、割り当てメソッドの配分属性はソース IP でなければなりません。詳細については、[WCCP の負荷配分, 57 ページ](#) を参照してください。

統合 Windows 認証

統合 Windows 認証 (IWA) は、共有の、信頼関係がある Windows ドメイン (1 つまたは複数) に属している複数のユーザーを認証するための非常に安全で堅牢な手段を提供します。

統合 Windows 認証の特徴は以下の通りです。

- ◆ Kerberos を使用する
- ◆ Windows Active Directory 2003 および 2008 をサポートする
- ◆ 明示および透過的プロキシ モードで NTLM をサポートする
- ◆ NTLMv2 with Session Security および NTLMv1 with Session Security をサポートする
- ◆ Internet Explorer 7 以上、Firefox 4 以上、Google Chrome 6 以上、Windows Safari 4 以上、iPad iOS4 上の Safari 4 以上、Opera 10 以上をサポートする
- ◆ UTF-8 形式のユーザー名をサポートする
- ◆ 対話形式の認証 (プロンプト形式) へのフォールバックをサポートする
- ◆ Multiple Realm Authentication オプションと合わせて使用できる

- ◆ クライアントが信頼できるドメインに結合されることを必要とする
- ◆ クライアントのブラウザが Content Gateway の完全修飾ドメイン名 (FQDN) をイントラネット サイトまたは信頼できるサイトとして指定することを必要とする
- ◆ 明示的プロキシ環境では、ブラウザは Content Gateway の FQDN を指定しなければならない

統合 Windows 認証 : 設定のまとめ

以下の手順に従って統合 Windows 認証 (IWA) を設定します。

- ◆ Content Gateway Manager の「**Configure**」>「**My Proxy**」>「**Basic**」ページで IWA を有効化します。**[Apply]** をクリックします。
- ◆ Content Gateway を Windows ドメインに結合します。要求される条件のリストは、[統合 Windows 認証の設定](#)に掲載しています。
- ◆ Content Gateway が透過的プロキシである場合、[透過的プロキシ認証の設定](#)を設定します。
- ◆ **グローバル認証オプション**を設定します。これらのオプションは、IWA が NTLM を折衝するとき、または NTLM にフォールバックする時の NTLM 認証に適用されます。

統合 Windows 認証の設定

1. 「**Configure**」>「**My Proxy**」>「**Basic**」>「**General**」に移動します。
2. **[Authentication (認証)]** セクションで **[Integrated Windows Authentication]** をクリックして **[On]** にして、**[Apply]** をクリックします。
3. **[Authentication]** セクションで **[Configure]** リンクをクリックして「**Configure**」>「**Security**」>「**Access Control (アクセス制御)**」へ移動します。
4. Windows ドメインを結合します。
ドメインを結合するには、以下の条件が満たされていなければなりません。
 - Content Gateway がドメイン名を解決できなければなりません。
 - Content Gateway のシステム時刻がドメイン コントローラの時刻と 1 分以内の誤差で同期化されていなければなりません。
 - 正しいドメイン管理者名とパスワードを指定しなければなりません。
 - ドメイン コントローラ (ポート 88, 389, 445) に対する TCP/UDP 接続が確立されていなければなりません。

- バックアップ ドメイン コントローラが設定されている場合、それらのドメイン コントローラとその Kerberos Distribution Center (KDC) サービスがネットワーク上で Content Gateway からアクセス可能でなければなりません。

**重要**

すべてのクライアントがドメインに結合されていなければなりません。

ブラウザと他のプロキシクライアントが Content Gateway の FQDN をイントラネット サイトまたは信頼できるサイトとして指定するように設定されていなければなりません。

- a. **[Domain Name (ドメイン名)]** フィールドに完全修飾名を入力します。
- b. **[Administrator Name (管理者名)]** フィールドに Windows Administrator のユーザー名を入力します。
- c. **[Administrator Password (管理者パスワード)]** フィールドに Windows Administrator のパスワードを入力します。
名前とパスワードは結合時にのみ使用し、保存されません。
- d. ドメイン コントローラを見つける方法を選択します。
 - ・ **DNS による自動検出**
 - ・ **DC 名と IP アドレス**
ドメイン コントローラが名前または IP アドレスによって指定されている場合、カンマ区切り形式 (スペースは使用しない) のリストでバックアップ ドメイン コントローラも指定できます。
- e. **[Content Gateway Hostname (Content Gateway ホスト名)]** フィールドで、ホスト名が正しいホスト名で、15 文字以内 (V- シリーズ アプライアンスでは 11 文字以内) であることを確認します。文字数がそれより多ければ、IWA を使用する場合は短くしなければなりません。長さの制限は、NetBIOS ホスト名の長さの制限 (15 文字) によるものです。

**警告**

ドメインを結合した後でホスト名を変更してはいけません。変更した場合、IWA はただちに作業を中止し、ドメインの結合を解除して、新しいホスト名で再結合するまで機能しません。

- f. **[Join Domain (ドメインを結合)]** をクリックします。エラーがある場合、上記の条件が満たされていることを確認してから、[ドメインを結合できない](#)を参照してください。
5. Content Gateway が透過プロキシとして配備されている場合、[透過的プロキシ認証の設定](#)を設定し、次のステップに進みます。

6. NTLM グローバル設定を設定します。「Configure」>「Security」>「Access Control」>「Global Authentication Options (グローバル認証オプション)」タブに移動します。

**ご注意**

これらの設定は、IWA が NTLM を折衝するとき、または NTLM にフォールバックする時に適用されます。

- a. **[Fail Open (フェイル オープン)]** は、デフォルトでは有効化されます。**[Fail Open]** が設定されている場合、認証が下記の理由で失敗した場合に、要求の処理を続行することが許可されます。
 - ・ ドメイン コントローラからの応答がない
 - ・ クライアントからのメッセージの形式が正しくない
 - ・ SMB 応答が不適切**[Fail Open]** が設定されていて、プロキシで Web フィルタリングを使用していて、XID エージェントが設定されている時、IWA 認証が失敗したときでも要求者は XID エージェントによって識別でき、適切なポリシーを適用できます。
上記の理由による認証の失敗が起こった時に、要求がインターネットに送信されるのを防止したい場合は、**[Fail Open]** を無効化します。
- b. **[Credential Caching (資格情報キャッシュ)]** は、デフォルトでは有効化されます。資格情報キャッシュは、Content Gateway が明示のプロキシとして配備されている時にのみ適用されます。資格情報は、認証が成功した時にのみキャッシュされます。資格情報キャッシュを無効化するには、**[Disable (無効化)]** を選択します。
- c. **[Caching TTL (キャッシュ継続時間)]** は、資格情報キャッシュのエントリの継続時間を設定します。TTL のデフォルト値は 900 秒 (15 分) です。TTL を変更するには、入力フィールドに新しい値を入力します。サポートされる値の範囲は 300 - 86400 秒です。
- d. 端末サーバーを使ってプロキシを通じてインターネットにアクセスするユーザーがいる場合 (例、Citrix サーバーを使用する)、**[Multi-user IP Exclusions (複数ユーザー IP 除外)]** フィールドにそれらのサーバーのリストを作成しなければなりません。そのようなユーザーの資格情報はキャッシュされません。IP アドレスおよび IP アドレス範囲のカンマ区切りリストを入力します。

これで設定が完了しました。Content Gateway を再起動し、プロキシを通じていくつかのテスト トラフィックを実行して、認証が想定通りに機能していることを確認します。問題がある場合は、[統合 Windows 認証のトラブルシューティング](#)を参照してください。

現在のドメインの結合を解除し、新しいドメインを結合するには

1. 「Configure」>「Security」>「Access Control」>「Integrated Windows Authentication」タブに移動し、**[Unjoin (結合を解除)]** をクリックします。

2. 新しいドメインを結合するには、[Domain Name] フィールドに完全修飾ドメイン名を入力します。
3. [Administrator Name] フィールドに Windows Administrator のユーザー名を入力します。
4. [Administrator Password] フィールドに Windows Administrator のパスワードを入力します。名前とパスワードは結合時にのみ使用し、保存されません。
5. ドメイン コントローラを見つける方法を選択します。
 - DNS による自動検出
 - DC 名と IP アドレス
ドメイン コントローラが名前または IP アドレスによって指定されている場合、カンマ区切り形式（スペースは使用しない）のリストでバックアップ ドメイン コントローラも指定できます。
6. [Join Domain] をクリックします。

ドメイン コントローラを見つける方法を変更するには

1. 「Configure」> 「Security」> 「Access Control」> 「Integrated Windows Authentication」 タブに移動します。
2. [Domain Controller] のセクションで、ドメイン コントローラを見つける方法を選択します。
 - DNS による自動検出
 - DC 名と IP アドレス
ドメイン コントローラが名前または IP アドレスによって指定されている場合、カンマ区切り形式（スペースは使用しない）のリストでバックアップ ドメイン コントローラも指定できます。
3. [Apply] をクリックします。

統合 Windows 認証のトラブルシューティング

この項では、よく起こる 2 つの問題を説明しています。

- ◆ [ドメインを結合できない](#)
- ◆ [クライアントを認証できない](#)

ドメインを結合できない

Content Gateway がドメインを結合するには、以下の条件が必要です。

- ◆ Content Gateway がドメイン名を解決できなければなりません。
- ◆ Content Gateway のシステム時刻がドメイン コントローラの時刻と ±1 分以内の誤差で同期化されていなければなりません。
- ◆ 正しいドメイン管理者名とパスワードを指定しなければなりません。
- ◆ ドメイン コントローラ（ポート 88, 389, 445）に対する TCP/UDP 接続が確立されていなければなりません。

- ◆ バックアップ ドメイン コントローラが設定されている場合、それらのドメイン コントローラとその Kerberos Distribution Center (KDC) サービスがネットワーク上で Content Gateway からアクセス可能でなければなりません。

トラブルシューティング

- ◆ 結合処理中に発生したエラーは画面の上部 (「Integrated Windows Authentication」タブ) に報告されます。
- ◆ 通常、エラー メッセージには、詳細情報が記載されている障害ログへのリンクが含まれています。
- ◆ 結合の障害は `/opt/WCG/logs/smbadmin.join.log` に記録されます。
- ◆ ほとんどの場合、ログ内の障害メッセージは標準 Samba および Kerberos エラー メッセージであり、インターネット検索によって容易に参照できます。

クライアントを認証できない

クライアントを認証するには、以下の条件が必要です。

- ◆ Content Gateway クライアントは、Content Gateway によって結合されるクライアントと同じドメインのメンバーでなければなりません。
- ◆ クライアント のシステム時刻がドメイン コントローラおよび Content Gateway の時刻と 1 分以内の誤差で同期化されていなければなりません。
- ◆ 明示のプロキシ クライアントが Content Gateway の IP アドレスに要求を送信するように**設定されていない**こと。クライアントは Content Gateway の完全修飾ドメイン名 (FQDN) を使用しなければなりません。IP アドレスを使用している場合、常に NTLM 認証が実行されます。
- ◆ Content Gateway FQDN が DNS の中にあり、すべてのプロキシ クライアントがそれを解決できなければなりません。
- ◆ ブラウザとプロキシ クライアントが Content Gateway の FQDN をイントラネット サイトまたは信頼できるサイトとして指定しなければなりません。

トラブルシューティング

Content Gateway Manager の「Monitor」> 「Security」> 「Integrated Windows Authentication」タブで [Diagnostic Test (診断テスト)] 機能を選択します。このモニター ページは認証要求の統計を表示し、診断テスト機能を提供します。

診断テスト 機能は、接続性および認証テストを実行し、エラーを報告します。また、ドメイン コントローラの TCP ポートの接続性および遅延を示します。

エラーおよびメッセージは、下記のファイルにログ記録されます。

- ◆ `/var/log/messages`
- ◆ `content_gateway.out`
- ◆ `/opt/WCG/logs/smbadmin.log`
- ◆ `/opt/WCG/logs/smbadmin.join.log`

パフォーマンスの問題

- ◆ **IWA (Kerberos):** 認証のパフォーマンスは CPU によって制約されます。Kerberos 認証では、ドメイン コントローラとの通信は行われません。
- ◆ **NTLM および基本:** ドメイン コントローラの応答性がパフォーマンスに影響を及ぼします。「**Monitor**」>「**Security**」>「**Integrated Windows Authentication**」ページは、平均応答時間を示します。

レガシー NTLM 認証

Content Gateway は、Windows ネットワークのユーザーがインターネットへのアクセスを許可される前に認証されることを保証する方法として、NTLM (NT LAN Manager) 認証プロトコルをサポートしています。



重要

この NTLM サポートの実装 (レガシー NTLM) は NTLMSSP プロトコルのみを使用します。これは本セクションに記載されている通りに信頼できるパフォーマンスを提供しますが、この方式の代わりに [統合 Windows 認証](#) モードを使用することを強く推奨します。後者は NTLM に対する、より堅牢で、安全なサポートを提供します。

レガシー NTLM オプションが有効化されている時、プロキシはコンテンツを要求するユーザーに対して資格情報の証明を要求します。次に、プロキシはユーザーの資格情報の証明を直接に Windows ドメイン コントローラに送信して確認を求めます。資格情報が有効であれば、プロキシは要求されている内容を提供し、その資格情報を将来の使用のために NTLM キャッシュに保存します。資格情報が有効でない場合、プロキシは *authentication failed* (認証失敗) メッセージを送信します。

制約

1. **WINS 解決**はサポートされていません。ドメイン コントローラのホスト名は DNS サーバーが解決できる名前であればなりません。
2. **拡張セキュリティ**はサポートされておらず、ドメイン コントローラ上で有効化できません。
3. **NTLM2 セッション セキュリティ**はサポートされておらず、クライアント上で有効化できません。Windows OS の [Security Settings (セキュリティ設定)] の領域で、[**Network Security: Minimum session security (ネットワーク セキュリティ: 最小限のセッション セキュリティ)**] の設定を調べます。
4. **NTLMv2** は Active Directory 2008 ではサポートされていません。要求される [Network Security: LAN Manager Authentication (ネットワーク セキュリティ: LAN マネージャ認証)] の設定については、下の「[NTLM プロキシ認証の設定](#)」のステップ 5 で示しています。
5. すべてのブラウザが透過的 NTLM 認証をサポートするわけではありません。[ブラウザの制約, 199 ページ](#) を参照してください。

6. NTLM 資格情報キャッシュは、明示モードで認証が成功した時に実行されます。透過的プロキシ認証キャッシュは別途に処理され、「Configuration」>「Security」>「Access」「Control」>「Transparent Proxy Authentication (透過的プロキシ認証)」タブで設定されます。

レガシー NTLM 認証の設定

1. 「Configure」>「My Proxy」>「Basic」>「General」タブに移動します。
2. [Authentication] セクションで、[Legacy NTLM] をクリックして [On] にして、[Apply] をクリックします。
3. 「Configure」>「Security」>「Access Control」>「Legacy NTLM」へ移動します。
4. [Domain Controller Hostnames] フィールドにプライマリ ドメイン コントローラのホスト名を入力し、次に、任意に、バックアップ ドメイン コントローラのカンマ区切り形式のリストを入力します。ホスト名の形式は下記のいずれかでなければなりません。

```
host_name[:port][%netbios_name]
```

または

```
IP_address[:port][%netbios_name]
```



ご注意

Active Directory 2008 を使用している場合、netbios_name を含めるか、SMB ポート 445 を使用しなければなりません。ポート 445 を使用しない場合、Active Directory サーバー上で Windows Network File Sharing サービスが実行していることを確認しなければなりません。詳細についてはご使用の Windows Server 2008 のマニュアルを参照してください。



ご注意

Active Directory 2008 を使用している場合、Windows の [Network Security (ネットワーク セキュリティ)] 設定で、[LAN Manager Authentication level (LAN マネージャ認証レベル)] を [Send NTLM response only (NTLM 応答の送信のみ)] に設定しなければなりません。詳細についてはご使用の Windows Server 2008 のマニュアルを参照してください。

- 複数のドメイン コントローラに認証要求を送信するときにプロキシがロードバランスを利用するには、[Load Balancing (ロード バランス)] を有効化します。



ご注意

複数のドメイン コントローラが指定されている時には、ロード バランスが無効化されている場合でも、プライマリドメイン コントローラの負荷が許可されている最大の接続数に達したとき、一時的なフェールオーバーの方法として、新しい要求はセカンダリドメイン コントローラに送信されます。これはプライマリドメイン コントローラが新しい接続を受け入れられるようになるまで継続されます。

- [Fail Open (フェイル オープン)] は、デフォルトでは有効化されます。[Fail Open] が設定されている場合、認証が下記の理由で失敗した場合に、要求の処理を続行することが許可されます。
 - ドメイン コントローラからの応答がない
 - クライアントからのメッセージの形式が正しくない
 - SMB 応答が不適切[Fail Open] が設定されていて、プロキシで Web フィルタリングを使用していて、XID エージェントが設定されている時、NTLM 認証が失敗したときでも要求者は XID エージェントによって識別でき、適切なポリシーを適用できます。

上記の理由による認証の失敗が起こった時に、要求がインターネットに送信されるのを防止したい場合は、[Fail Open] を無効化します。
- [Credential Caching (資格情報キャッシュ)] は、デフォルトでは有効化されます。資格情報キャッシュは、Content Gateway が明示のプロキシとして配備されている時にのみ適用されます。資格情報は、認証が成功した時にのみキャッシュされます。資格情報キャッシュを無効化するには、[Disable (無効化)] を選択します。
- [Caching TTL (キャッシュ継続時間)] は、資格情報キャッシュのエントリから継続時間を設定します。TTL のデフォルト値は 900 秒 (15 分) です。TTL を変更するには、入力フィールドに新しい値を入力します。サポートされる値の範囲は 300 - 86400 秒です。
- 端末サーバーを使ってプロキシを通じてインターネットにアクセスするユーザーがいる場合 (例、Citrix サーバーを使用する)、[Multi-user IP Exclusions (複数ユーザー IP 除外)] フィールドにそれらのサーバーのリストを作成しなければなりません。そのようなユーザーの資格情報はキャッシュされません。IP アドレスおよび IP アドレス範囲のカンマ区切りリストを入力します。
- [Apply] をクリックします。
- [Configure] > [My Proxy] > [Basic] > [General] で [Restart] をクリックします。

任意に、次のことが可能です。

- ◆ Content Gateway が特定のクライアントに対して、NTLM サーバーによる認証を求められることなしにインターネット上の特定のサイトにアクセスすることを許可するように設定する ([Access Control \(アクセス制御\), 323 ページ](#) を参照)。
- ◆ 認証のために代替の Content Gateway ホスト名を設定し、認証モード ([IP Mode] または [Cookie Mode]) を設定し、セッション継続時間を設定する ([透過的プロキシ認証の設定, 200 ページ](#) を参照)。

LDAP 認証

Content Gateway は LDAP オプションをサポートします。このオプションは、ユーザーがプロキシを通じてコンテンツにアクセスする前に LDAP サーバーによって認証されることを保証します。



重要

複数のレルム (信頼関係を共有していないドメイン) がある環境では、[複数レルムの認証](#) オプションで LDAP 認証を設定します。


LDAP オプションが有効化されている時、プロキシは LDAP クライアントとして機能し、コンテンツを要求するユーザーに直接にユーザー名およびパスワードを要求します。ユーザー名とパスワードを受け取った後、プロキシは LDAP サーバーにコンタクトして、その資格情報が正しいかどうかを確認します。LDAP サーバーがそのユーザー名とパスワードを受け入れた場合、プロキシは要求されたコンテンツをクライアントに提供し、そのユーザー名とパスワードを Content Gateway LDAP キャッシュに保存します。そのユーザーに関する将来のすべての認証要求は、キャッシュ エントリが時間切れになるまで、LDAP キャッシュから処理されます。LDAP サーバーがそのユーザー名とパスワードを拒否した場合、ユーザーのブラウザは認証が失敗したことを知らせるメッセージを表示し、再びユーザー名とパスワードの入力を要求します。

LDAP 認証は単純バインドと匿名バインドの両方をサポートします。

Content Gateway が LDAP クライアントとして機能するように設定する

1. 「Configure」 > 「My Proxy」 > 「Basic」 > 「General」 タブに移動します。
2. [Authentication] セクションで、[LDAP] をクリックして [On] にして、[Apply] をクリックします。
3. 「Configure」 > 「Security」 > 「Access Control」 > 「LDAP」へ移動します。
4. [Purge Cache on Authentication Failure (認証失敗時にキャッシュをページ)] を有効化し、認証が失敗した時にプロキシが認証エントリを削除するように設定します。
5. LDAP サーバーのホスト名を入力します。

- Content Gateway が LDAP サーバーとの通信に使用するポートを入力します。デフォルトポートは 389 です。

 **ご注意**

LDAP ディレクトリ サービスが Active Directory である時、グローバル カタログのベース ドメインの外のユーザーからの要求は認証に失敗します。これは LDAP のデフォルトポートが 389 であり、389 へ送信された要求がグローバル カタログのベース ドメイン内でのみオブジェクトを検索するからです。ベース ドメインの外のユーザーを認証するには、LDAP ポートを 3268 に変更します。3268 へ送信された要求は、フォレスト全体でオブジェクトを検索します。

- プロキシが LDAP サーバーとの間でセキュアな通信を使用するには、Secure LDAP を有効化します。セキュアな通信はポート 636 または 3269 上で実行されます。必要に応じて、前のフィールドでポートの値を変更できます。
- 検索のためのフィルタを設定するために、ディレクトリ サービスのタイプを選択します。Active Directory ではデフォルトは **sAMAccountName** です。eDirectory またはその他のディレクトリ サービスでは、**uid** を選択します。
- LDAP ベースのディレクトリ サービスのユーザーの完全識別名（完全修飾名）を入力します。例：
CN=John Smith,CN=USERS,DC=MYCOMPANY,DC=COM
このフィールドには最大 128 文字まで入力できます。
このフィールドで値を指定しない場合、プロキシは匿名のバインドを試みます。
- 前のステップで指定したユーザーのパスワードを入力します。
- ベース識別名 (DN) を入力します。この値は LDAP 管理者から取得します。
- [Apply] をクリックします。
- [Configure] > [My Proxy] > [Basic] > [General] で [Restart] をクリックします。

任意に、以下の手順を実行できます。

- ◆ LDAP キャッシュ オプションを変更します。[LDAP キャッシュ オプションの設定, 212 ページ](#) を参照してください。
- ◆ Content Gateway が特定のクライアントに対して、LDAP サーバーによる認証を求められることなしにインターネット上の特定のサイトにアクセスすることを許可するように設定する。[Access Control \(アクセス制御\), 323 ページ](#) を参照してください。
- ◆ 認証のために代替の Content Gateway ホスト名を設定し、認証モード ([IP Mode] または [Cookie Mode]) を設定し、セッション継続時間を設定する。[透過的プロキシ認証の設定, 200 ページ](#) を参照してください。

LDAP キャッシュ オプションの設定

デフォルトでは、LDAP キャッシュは 5000 個のエントリを保存するように設定されており、各エントリは 3000 分の間、最新であると想定されます。これらのオプションを変更するには `records.config` ファイルを編集します。

1. Content Gateway の `config` ディレクトリ (`/opt/WCG/config`) の `records.config` ファイルを開きます。
2. 下記の変数を編集します。

変数	説明
<code>proxy.config.ldap.cache.size</code>	LDAP キャッシュに保存できるエントリの数を指定します。 デフォルト値は 5000 で、最小値は 256 です。
<code>proxy.config.ldap.auth.ttl_value</code>	Content Gateway がユーザー名およびパスワード エントリを LDAP キャッシュに保存できる期間(分)を指定します。
<code>proxy.config.ldap.cache.storage_size</code>	LDAP キャッシュが使用できるディスクスペースの量(バイト数)の最大値を指定します。 この値を変更する時、それに比例して <code>proxy.config.ldap.cache.size</code> の値も更新しなければなりません。たとえば、ストレージのサイズを 2 倍にした場合は、キャッシュ サイズも 2 倍にします。 この変数を変更して <code>proxy.config.ldap.cache.size</code> を変更しなかった場合、LDAP サブシステムは機能停止します。

3. ファイルを保存して、閉じます。
4. Content Gateway の `bin` ディレクトリ (`/opt/WCG/bin`) から、`content_line -L` を実行してローカル ノード上でプロキシを再起動するか、または `content_line -M` を実行してクラスタ内のすべてのノード上でプロキシを再起動します。

セキュアな LDAP の設定

デフォルトでは、LDAP トラフィックはセキュアでない状態で送信されます。Secure Sockets Layer (SSL) / Transport Layer Security (TLS) テクノロジーを使用して LDAP トラフィックを機密のセキュアな通信にすることができます。LDAP over SSL (LDAPS) を有効化するには、Microsoft 認証機関 (CA) または Microsoft 以外の CA から適切な形式の証明書をインストールします。

Content Gateway で LDAPS を使用するには、以下の手順を実行します。

1. Content Gateway の **config** ディレクトリ (`/opt/WCG/config`) の **records.config** ファイルを開きます。
2. **records.config** に下記のエントリを追加します。

```
CONFIG proxy.config.ldap.secure.bind.enabled INT 1
```
3. 「Configure」> 「Security」> 「Access Control」> 「LDAP」へ移動し、ポートを 3269 に変更します。



ご注意

Directory Service は LDAPS 認証をサポートするように設定されていなければなりません。その方法については、ディレクトリ サービスのプロバイダによって提供されるマニュアルを参照してください。

RADIUS 認証

Content Gateway は RADIUS オプションをサポートします。このオプションは、ユーザーがプロキシを通じてコンテンツにアクセスする前に RADIUS サーバーによって認証されることを保証します。

RADIUS オプションが有効化されている時、Content Gateway は RADIUS クライアントとして機能し、コンテンツを要求するユーザーに直接にユーザー名およびパスワードを要求します。ユーザー名とパスワードを受け取った後、Content Gateway は RADIUS サーバーにコンタクトして、その資格情報が正しいかどうかを確認します。RADIUS サーバーがそのユーザー名とパスワードを受け入れた場合、プロキシは要求されたコンテンツをクライアントに提供し、そのユーザー名とパスワードを RADIUS キャッシュに保存します。そのユーザーに関する将来のすべての認証要求は、そのエントリが時間切れになるまで、RADIUS キャッシュから処理されます。RADIUS サーバーがそのユーザー名とパスワードを拒否した場合、ユーザーのブラウザは認証が失敗したことを知らせるメッセージを表示し、再びユーザー名とパスワードの入力を要求します。

Content Gateway は、フェールオーバー用にプライマリ RADIUS サーバーとセカンダリ RADIUS サーバーをサポートします。プライマリ サーバーが指定した時間（デフォルトでは 60 秒）内にプロキシ要求に応答しない場合、Content Gateway は再びユーザー名とパスワードのチェックを試みます。最大再試行回数（デフォルトでは 10 回）までにプライマリ RADIUS サーバーからの応答がない場合、プロキシはセカンダリ RADIUS サーバーにコンタクトします。Content Gateway がセカンダリ RADIUS サーバーにコンタクトできない場合、ユーザーは再びユーザー名とパスワードの入力を要求されます。

RADIUS のキャッシュはメモリに保持され、ディスク上に保存されます。Content Gateway はディスク上のデータを 60 秒ごとに更新します。また、Content Gateway は RADIUS のキャッシュのユーザー名およびパスワード エントリを 60 秒ごとに保存します。RADIUS キャッシュ内のパスワードおよびユーザー名エントリが期限切れになっている場合、Content Gateway はユーザー名およびパスワードを承認または拒否するために RADIUS サーバーにコンタクトします。

Content Gateway が RADIUS クライアントとして機能するように設定するには、以下の手順を実行します。

- ◆ RADIUS オプションを有効化します。
- ◆ プライマリおよびセカンダリ（任意）RADIUS サーバーのホスト名または IP アドレスと、Content Gateway が RADIUS サーバーと通信するために使用するポートおよび共有キーを指定します。

Content Gateway が RADIUS クライアントとして機能するように設定する、[214 ページ](#) を参照してください。

Content Gateway が RADIUS クライアントとして機能するように設定する

1. 「Configure」> 「My Proxy」> 「Basic」> 「General」 タブに移動します。
2. [Authentication] セクションで、[Radius] をクリックして [On] にして、[Apply] をクリックします。
3. 「Configure」> 「Security」> 「Access Control」> 「Radius」 へ移動します。
4. プライマリ RADIUS サーバーのホスト名を入力します。
5. Content Gateway がプライマリ RADIUS サーバーとの通信に使用するポートの番号を入力します。
6. 暗号化に使用するキーを入力します。
7. セカンダリ RADIUS サーバーを使用している場合、[Secondary Radius Server (Optional)] 領域の該当するフィールドにホスト名、ポート、共有キーを入力します。
8. [Apply] をクリックします。
9. [Configure] > [My Proxy] > [Basic] > [General] で [Restart] をクリックします。



ご注意

これらの手順を実行するほかに、Content Gateway コンピュータをプライマリおよびセカンダリ RADIUS サーバー上の信頼できるクライアントとして追加し、Content Gateway コンピュータに使用する共有キーを指定しなければなりません（共有キーは下記の手順で使用するものと同じでなければなりません）。RADIUS サーバーのマニュアルを参照してください。

RADIUS キャッシュおよびサーバー タイムアウト オプションの設定

デフォルトでは、RADIUS キャッシュおよび RADIUS サーバー タイムアウト オプションは下記のように設定されます。

- ◆ RADIUS キャッシュは 1,000 個のエントリを保存するように設定されており、各エントリは 60 分の間、最新であると想定されます。

- ◆ 接続が 10 秒間アイドル状態である場合、Content Gateway は RADIUS サーバーへの接続の再確立を試みることができ、接続の再試行は 10 回まで可能です。

これらのデフォルト値を変更するには `records.config` ファイルを編集します。

1. Content Gateway の `config` ディレクトリ (`/opt/WCG/config`) の `records.config` ファイルを開きます。
2. 下記の変数を編集します。

変数	説明
<code>proxy.config.radius.auth.min_timeout</code>	Content Gateway から RADIUS サーバーへの接続がアイドル状態に維持される時間を指定します。この時間を過ぎると Content Gateway の接続が失われます。
<code>proxy.config.radius.auth.max_retries</code>	Content Gateway が RADIUS サーバーへの接続を試みる最大回数を指定します。
<code>proxy.config.radius.cache.size</code>	RADIUS キャッシュに保存できるエントリの数を指定します。最小値は 256 です。256 より小さい値を入力した場合、Content Gateway は SEGV を生成します。
<code>proxy.config.radius.auth.ttl_value</code>	Content Gateway がユーザー名およびパスワード エントリを RADIUS キャッシュに保存できる期間(分)を指定します。
<code>proxy.config.radius.cache.storage_size</code>	RADIUS キャッシュが使用できるディスクスペースの量の最大値を指定します。 この値はエントリの数の 100 倍以上でなければなりません。可能な最大量のディスクスペースを割り当てることを推奨します。

3. ファイルを保存して、閉じます。
4. Content Gateway の `bin` ディレクトリ (`/opt/WCG/bin`) から `content_line -L` を実行してローカル ノード上で Content Gateway を再起動するか、`content_line -M` を実行してクラスタ内のすべてのノード上で WCG を再起動します。

複数レルムの認証

関連項目：

- ◆ [透過的プロキシ認証の設定](#), 200 ページ
- ◆ [グローバル認証オプション](#), 220 ページ
- ◆ [複数レルムの認証 ドメイン](#), 219 ページ
- ◆ [統合 Windows 認証のレルム ルールの作成](#), 221 ページ
- ◆ [LDAP 認証のレルム ルールの作成](#), 224 ページ
- ◆ [認証レルム ルールの使用](#), 226 ページ
- ◆ [複数レルム認証の使用例](#), 227 ページ
- ◆ [複数レルムの認証のトラブルシューティング](#), 230 ページ

複数レルムの認証は、相互のインバウンドおよびアウトバウンドの信頼関係がないためにユーザー認証の観点からは基本的に隔離されている複数のドメインがある環境に対応しています。したがって、これらのドメインの中のユーザーは、そのユーザーのドメイン内のドメイン コントローラによって認証されなければなりません。この機能との関係で、これらのドメインはレルムと呼ばれます。



ご注意

ネットワーク内のすべてのユーザーが、信頼関係を共有しているドメイン コントローラによって認証できる場合、複数認証レルムのためのルールを作成する必要はありません。この場合に、最善の方法は、使用しているディレクトリ サービスに最も適した認証方法を使用することです。

複数レルムの認証によって、各ドメインに対して個別の認証ルールを作成することが可能になり、それによって複数の認証方法 (IWA、レガシー NTLM、LDAP) の同時使用がサポートされます。たとえば、RealmA は Active Directory ドメインで、このドメインに対してはユーザー認証に IWA を使用します。RealmB は LDAP ドメインで、このドメインに対してはユーザー認証に LDAP を使用しなければなりません。複数レルムの認証では、このような設定が簡単にできます。[複数レルム認証の使用例](#), 227 ページ に 3 つの仮定上のシナリオを示しています。

明示のプロキシ環境では、特定のポートへのインバウンドトラフィックに対する認証ルールを作成することができます。これによってプロキシ ポート、

ソース IP アドレス、認証方法、レルムを指定する認証ルールが可能になります。



重要

複数レルムの環境では、Content Gateway は Web Security に知られていない (User Services プライマリ ドメインの外の) ユーザーを認証することがあります。この場合に Content Gateway が Web Security に知られている “別名” のユーザー名を送信するように設定できます。デフォルト ポリシーを適用する、つまり名前を送信しないように設定することもできます。この選択は、定義した各ルールの Advanced Options (拡張オプション)で行います。

詳細については、下の [未知のユーザーと “別名” オプション](#) を参照してください。

複数レルムの認証のサポートの仕組み

複数のレルムがあるネットワークでは、IP アドレスのセット、または特定のポート上のトラフィックを個別のドメイン コントローラへ転送するルールが定義されます。これらのルールは 「Configure」 > 「Security」 > 「Access」「Control」 > 「Authentication Realms (認証レルム)」 タブ上で定義されます。ルールは `auth.config` ファイルに保存されます。

- ◆ 複数レルムの認証ルールは、IWA、レガシー NTLM、および LDAP ソースに対して定義できます。
- ◆ 各レルムに対して 1 つ以上の認証ルールを定義できます。
- ◆ レルム ルールのタイプ (IWA、レガシー NTLM、LDAP) によって、使用する指定子が異なります。
- ◆ ルールはリストの上から順にチェックされ、最初に条件に一致するルールが適用されます。IP アドレスの条件に一致するルールがない場合、認証は試みられません。
- ◆ トランザクションは、Filtering Service で使用する名前を使ってログに記録されます。
- ◆ プロキシの認証統計が収集され、認証方法別に報告されます。[Security \(セキュリティ\), 266 ページ](#) (「統計」のセクション) を参照してください。



重要

Content Gateway には、各レルムについて IWA 認証で使用する Content Gateway の完全修飾ドメイン名 (FQDN) を解決できる DNS サーバーが組み込まれていなければなりません。そうでない場合、IWA ルールは機能しません。DNS サーバーの設定方法はネットワーク管理者が決定します。1 つのオプションとして、Content Gateway のプライマリ DNS サーバーと各認証レルムの DNS サーバーの間に DNS トランスファー ゾーン (サブゾーン) を構成するという方法があります。

未知のユーザーと“別名”オプション

複数レルムの環境では、Content Gateway が認証したユーザーが、Web Security に転送された時に、その名前が User Services ディレクトリにないために認識されないことがあります。認証されたユーザー名が Web Security に転送され、Web Security 側に一致するユーザー名がない場合、デフォルトポリシーが適用されます。この問題を解決するには、いくつかの方法があります。

- ◆ Web Security User Services の設定を変更し、その名前を確認して、そのディレクトリに追加する。
- ◆ 認識されない名前を Web Security のプライマリドメインに追加する。名前は正確に一致しなければなりません。新しい名前に対するポリシーを定義します。
- ◆ 特定のレルムルールに一致するユーザーについて、別名を Web Security に転送し、別名を Web Security のプライマリドメインに追加する。名前は正確に一致しなければなりません。別名に対するポリシーを定義します。
- ◆ 既存の Web Security のデフォルトポリシーで十分な場合は、何もしないか、または特定のレルムルールに一致する各ユーザーに対して、そのレルムルールの中で空白の別名を使用することを選択します。

[複数レルム認証の使用例](#) にいくつかの具体例を示しています。

複数レルムの認証の設定のまとめ

- ◆ IWA ルールで使用するすべての Windows ドメインを結合します(ドメインを後で追加または削除できますが、結合されていないドメインに対してはルールを作成できません)。[複数レルムの認証ドメイン](#), 219 ページを参照してください。
- ◆ Content Gateway が明示のプロキシで、複数ポート上でトラフィックを受信したい場合、「Configure」>「Protocol」>「HTTP」タブでポートを指定します。

ご注意

- ◆ また、クライアントが正しいポートを使用するように設定しなければなりません。

- ◆ Content Gateway が透過的プロキシである場合、[透過的プロキシ認証の設定](#), 200 ページ を設定します。
- ◆ [グローバル認証オプション](#), 220 ページ の設定
- ◆ 認証ルールの作成
 - [統合 Windows 認証のレルムルールの作成](#), 221 ページ
 - [レガシー NTLM 認証のレルムルールの作成](#), 222 ページ
 - [LDAP 認証のレルムルールの作成](#), 224 ページ

複数レルムの認証 ドメイン

IWA レルム ルールを作成する前に、各レルムのドメインを結合しなければなりません。



重要

特定のドメインの中で認証するすべてのクライアントがそのドメインに結合されていなければなりません。

ドメインに結合するには、以下の条件が満たされていなければなりません。

- Content Gateway がドメイン名を解決できなければなりません。
- Content Gateway のシステム時刻がドメイン コントローラの時刻と =|1 分以内の誤差で同期化されていなければなりません。
- 正しいドメイン管理者名とパスワードを指定しなければなりません。
- ドメイン コントローラ (ポート 88, 389, 445) に対する TCP/UDP 接続が確立されていなければなりません。
- バックアップ ドメイン コントローラが設定されている場合、それらのドメイン コントローラとその Kerberos Distribution Center (KDC) サービスがネットワーク上で Content Gateway からアクセス可能でなければなりません。

ドメインを結合するには、以下の手順を実行します。

1. 「Configure」> 「Security」> 「Access Control」> 「Integrated Windows Authentication」 タブに移動します。
2. [Domain Name (ドメイン名)] フィールドに完全修飾名を入力します。
3. [Administrator Name] フィールドに Windows Administrator のユーザー名を入力します。
4. [Administrator Password] フィールドに Windows Administrator のパスワードを入力します。
名前とパスワードは結合時にのみ使用し、保存されません。
5. ドメイン コントローラを見つける方法を選択します。
 - DNS による自動検出
 - DC 名と IP アドレス
ドメイン コントローラが名前または IP アドレスによって指定されている場合、カンマ区切り形式 (スペースは使用しない) のリストでバックアップ ドメイン コントローラも指定できます。
6. [Join Domain] をクリックします。

[Joined Domains (結合済みのドメイン)] のセクションは、結合済みのドメインのリストと、結合解除およびドメイン コントローラを見つける方法の変更のためのコントロールを表示します。

トラブルシューティングのヒントは **ドメインを結合できない** に示しています。

ドメインの結合を解除するには、以下の手順を実行します。

[**Joined Domains**] セクションで、結合解除するドメインを選択し、[**Unjoin Domain (ドメインの結合解除)**] を選択します。

ドメイン コントローラを見つける方法を変更するには、以下の手順を実行します。

1. [**Joined Domains**] のセクションで、ドメイン コントローラを見つける方法を選択します。
 - **DNS による自動検出**
 - **DC 名と IP アドレス**

ドメイン コントローラが名前または IP アドレスによって指定されている場合、カンマ区切り形式（スペースは使用しない）のリストでバックアップ ドメイン コントローラも指定できます。
2. [**Apply**] をクリックします。

グローバル認証オプション

これらの設定は、IWA が NTLM を折衝する時、NTLM にフォールバックする時、またはレガシー NTLM を使用している時に適用されます。

1. 「**Configure**」 > 「**Security**」 > 「**Access Control**」 > 「**Global Authentication Options (グローバル認証オプション)**」 タブに移動します。
2. [**Fail Open (フェイル オープン)**] は、デフォルトでは有効化されます。[**Fail Open**] が設定されている場合、認証が下記の理由で失敗した場合に、要求の処理を続行することが許可されます。
 - ドメイン コントローラからの応答がない
 - クライアントからのメッセージの形式が正しくない
 - SMB 応答が不適切

[**Fail Open**] が設定されていて、プロキシで Web フィルタリングを使用していて、XID エージェントが設定されている時、NTLM 認証が失敗したときでも要求者は XID エージェントによって識別でき、適切なポリシーを適用できます。

上記の理由による認証の失敗が起こった時に、要求がインターネットに送信されるのを防止したい場合は、[**Fail Open**] を無効化します。

3. [**Credential Caching (資格情報キャッシュ)**] は、デフォルトでは有効化されます。資格情報キャッシュは、Content Gateway が明示のプロキシとして配備されている時にのみ適用されます。資格情報は、認証が成功した時にのみキャッシュされます。資格情報キャッシュを無効化するには、[**Disable (無効化)**] を選択します。

4. **[Caching TTL (キャッシュ継続時間)]** は、資格情報キャッシュのエントリの継続時間を設定します。TTL のデフォルト値は 900 秒 (15 分) です。TTL を変更するには、入力フィールドに新しい値を入力します。サポートされる値の範囲は 300 - 86400 秒です。
5. 端末サーバーを使ってプロキシを通じてインターネットにアクセスするユーザーがいる場合 (例、Citrix サーバーを使用する)、**[Multi-user IP Exclusions (複数ユーザー IP 除外)]** フィールドにそれらのサーバーのリストを作成しなければなりません。そのようなユーザーの資格情報はキャッシュされません。IP アドレスおよび IP アドレス範囲のカンマ区切りリストを入力します。



ご注意

Content Gateway は WCCP ロード バランシングを使用して、プロキシ クラスタでの透過的認証をサポートします。ただし、割り当てメソッドの配分属性はソース IP でなければなりません。詳細については、[Content Gateway Manager でのサービスグループの設定, 66 ページ](#) を参照してください。

統合 Windows 認証のレルム ルールの作成

IWA を通じてアクセスするレルムのためのルールを作成する前に、ドメインを結合する必要があります。また、下記の情報が必要です。

- ◆ ルールを適用するドメインの名前
- ◆ 認証するクライアントからのソース IP アドレスのセット。これは個別の IP アドレスと IP アドレスの範囲の混合でもかまいません。
- ◆ またはインバウンドトラフィックが着信するポートの一意的なポート番号 (明示のプロキシのみ)
- ◆ または上記の組み合わせ (明示のプロキシのみ)



ご注意

すべての指定子を入力した後、必ず **[Add]** をクリックしてから **[Apply]** をクリックします。先に **[Apply]** をクリックした場合や、編集ウィンドウが閉じている場合は、すべてのエントリ フィールドが消去されます。

1. Content Gateway Manager で、**[Configure] > [Security] > [Access] [Control]** を順に選択して **[Domain (ドメイン)]**、**[Global Authentication Options (グローバル認証オプション)]**、および (必要に応じて) **[Transparent Proxy Authentication (透過的プロキシ認証)]** の設定を表示または指定します。
2. 必要なら、「Domains」タブで新しいドメイン (レルム) を追加します。
3. 「Configure」>「Security」>「Access Control」>「Authentication Realms (認証レルム)」タブに移動します。既存のすべての認証レルム ルールのリストがページ上部に表示されます。
4. **[Edit file]** をクリックしてルール エディタを開きます。

5. **[Rule Type]** ドロップダウン リストから **[Integrated Windows Authentication]** を選択します。
6. ルール定義プロセスが完了した時(下のステップ 12 と 14 でルールが追加され、プロキシが再起動したとき)にルールがアクティブになるようにするには、**[Enable]** を選択します。
7. ルールに一意な**ルール名**を指定します。具体的で説明的な名前を指定すると、ルールの識別と管理が容易になります。
8. ルールを特定の IP アドレスに適用する場合は、**[Source IP (ソース IP)]** フィールドに個別の IP アドレスと IP アドレス範囲のカンマ区切り形式のリストを入力します。スペースは使用できません。例：
10.4.1.1,10.12.1.1-10.12.254.254
ソース IP アドレスの範囲に重なりがあってもかまいません。範囲の重なりは、大きなプールの中のサブグループをすばやく識別する手段として便利です。
範囲の重なりの中では、最初的一致だけが使用されます。
9. ルールを特定のポート上に着信するトラフィックに適用する場合、ドロップダウン リストからその**プロキシ ポート**を選択します(明示のプロキシにのみ有効)。
10. Filtering Service に送信する別名を指定するには、**[Advanced Settings]** を開き、**[Aliasing (別名の指定)]** をクリックします。このフィールドで、使用する名前を選択します。名前が指定されていない(入力フィールドが空白のままになっている)場合、Web Security はユーザー名を含まない要求に対応する時の(設定されている)動作を行います。別名の詳細については、**未知のユーザーと“別名”オプション**を参照してください。
11. **[Integrated Windows Authentication Specifiers (統合 Windows 認証指定子)]** のセクションの **[Domain/Realm (ドメイン/レルム)]** ドロップダウン リストでルールを適用するレルムを選択します。
12. **[Add]** をクリックしてルールを追加します。
13. ページ上部で、ルール リストの中でのそのルールの位置をチェックし、調整します。最初に条件に一致したルールが適用されます。
14. **Apply** をクリックしてから、ルールを有効にするために Content Gateway を再起動します。

**警告**

ルールに無効な値がある場合、無効なルールを示した警告メッセージが表示されます。

レガシー NTLM 認証のレルム ルールの作成

NTLM 認証レルムのルールを作成する前に、下記の情報が必要です。

- ◆ 認証するクライアントからのソース IP アドレスのセット。これは個別の IP アドレスと IP アドレスの範囲の混合でもかまいません。

- ◆ またはインバウンド トラフィックが着信するポートの一意的なポート番号（明示のプロキシのみ）
- ◆ または上記の組み合わせ（明示のプロキシのみ）
- ◆ プライマリ ドメイン コントローラと、ロード バランスまたはフェールオーバーのために使用するすべてのセカンダリ ドメイン コントローラの名前または IP アドレスとポート番号。



ご注意

すべての指定子を入力した後、必ず **[Add]** をクリックしてから **[Apply]** をクリックします。先に **[Apply]** をクリックした場合や、編集ウィンドウが閉じている場合は、すべてのエントリ フィールドが消去されます。

1. Content Gateway Manager で、**[Configure]** > **[Security]** > **[Access]** **[Control]** を順に選択して **[Domain (ドメイン)]**、**[Global Authentication Options (グローバル認証オプション)]**、および（必要に応じて）**[Transparent Proxy Authentication (透過的プロキシ認証)]** の設定を表示または指定します。
2. 「**Configure**」 > 「**Security**」 > 「**Access Control**」 > 「**Authentication Realms**」 タブに移動します。既存のすべての認証レルム ルールのリストがページ上部に表示されます。
3. **[Edit file]** をクリックしてルール エディタを開きます。
4. **[Rule Type]** ドロップダウン リストから **[NTLM]** を選択します。
5. ルール定義プロセスが完了した時（下のステップ 12 と 14 でルールが追加され、プロキシが再起動したとき）にルールがアクティブになるようにするには、**[Enable]** を選択します。
6. ルールに一意的なルール名を指定します。具体的で説明的な名前を指定すると、ルールの識別と管理が容易になります。
7. ルールを特定の IP アドレスに適用する場合は、**[Source IP (ソース IP)]** フィールドに個別の IP アドレスと IP アドレス範囲のカンマ区切り形式のリストを入力します。スペースは使用できません。例：
10.4.1.1,10.12.1.1-10.12.254.254
ソース IP アドレスの範囲に重なりがあってもかまいません。範囲の重なりは、大きなプールの中のサブグループをすばやく識別する手段として便利です。
範囲の重なりの中では、最初的一致だけが使用されます。
8. ルールを特定のポート上に着信するトラフィックに適用する場合、ドロップダウン リストからその**プロキシ ポート**を選択します。
9. Filtering Service に送信する別名を指定するには、**[Advanced Settings]** を開き、**[Aliasing (別名の指定)]** をクリックします。このフィールドで、使用する名前を選択します。名前が指定されていない（入力フィールドが空白のままになっている）場合、Web Security はユーザー名を含まない要求に対応する時の（設定されている）動作を行います。別名の詳細については、[未知のユーザーと“別名”オプション](#)を参照してください。

10. **[DC List (DC リスト)]** で、プライマリ ドメイン コントローラの IP アドレスとポート番号を入力します。ポートが指定されていない場合、Content Gateway はポート 139 を使用します。

カンマ区切り形式のリストでセカンダリ ドメイン コントローラを指定できます。下記の形式がサポートされています。

host_name[:port][%netbios_name]

IP_address[:port][%netbios_name]

netbios_name は Active Directory 2008 では必須です。

11. ドメイン コントローラ間のロード バランスを有効化するには、**[DC Load Balance (DC ロード バランス)]** を選択します。



ご注意

複数のドメイン コントローラが指定されている時には、ロード バランスが無効化されている場合でも、プライマリ ドメイン コントローラの負荷が許可されている最大の接続数に達したとき、一時的なフェールオーバーの方法として、新しい要求はセカンダリ ドメイン コントローラに送信されます。これはプライマリ ドメイン コントローラが新しい接続を受け入れられるようになるまで継続されます。

12. **[Add]** をクリックしてルールを追加します。
13. ページ上部で、ルール リストの中でのそのルールの位置をチェックし、調整します。最初に条件に一致したルールが適用されます。
14. **Apply** をクリックしてから、ルールを有効にするために Content Gateway を再起動します。



警告

ルールに無効な値がある場合、無効なルールを示した警告メッセージが表示されます。

LDAP 認証のレルム ルールの作成

LDAP 認証レルムのルールを作成する前に、下記の情報が必要です。

- ◆ LDAP サーバーに送信するソース IP アドレスのセット。これは個別の IP アドレスと IP アドレスの範囲の混合でもかまいません。
- ◆ またはインバウンド トラフィックが着信するポートの一意的なポート番号 (明示のプロキシのみ)
- ◆ または上記の組み合わせ (明示のプロキシのみ)
- ◆ LDAP サーバーの名前とポート番号。
- ◆ LDAP ベース識別名。
- ◆ LDAP バインド識別名およびパスワード。

- ◆ 任意に、LDAP 属性名と値。



ご注意

すべての指定子を入力した後、必ず **[Add]** をクリックしてから **[Apply]** をクリックします。先に **[Apply]** をクリックした場合や、編集ウィンドウが閉じている場合は、すべてのエントリフィールドが消去されます。

1. Content Gateway Manager で、**[Configure]** > **[Security]** > **[Access]** **[Control]** を順に選択して **[Domain (ドメイン)]**、**[Global Authentication Options (グローバル認証オプション)]**、および (必要に応じて) **[Transparent Proxy Authentication (透過的プロキシ認証)]** の設定を表示または指定します。
2. 「**Configure**」 > 「**Security**」 > 「**Access Control**」 > 「**Authentication Realms**」 タブに移動します。既存のすべての認証レール ルールのリストがページ上部に表示されます。
3. **[Edit file]** をクリックしてルール エディタを開きます。
4. **[Rule Type]** ドロップダウン リストから **[LDAP]** を選択します。
5. ルール定義プロセスが完了した時 (下のステップ 19 と 21 でルールが追加され、プロキシが再起動したとき) にルールがアクティブになるようにするには、**[Enable]** を選択します。
6. ルールに一意なルール名を指定します。具体的で説明的な名前を指定すると、ルールの識別と管理が容易になります。
7. ルールを特定の IP アドレスに適用する場合は、**[Source IP (ソース IP)]** フィールドに個別の IP アドレスと IP アドレス範囲のカンマ区切り形式のリストを入力します。スペースは使用できません。例：
10.4.1.1,10.12.1.1-10.12.254.254
ソース IP アドレスの範囲に重なりがあってもかまいません。範囲の重なりは、大きなプールの中のサブグループをすばやく識別する手段として便利です。
範囲の重なりの中では、最初的一致だけが使用されます。
8. ルールを特定のポート上に着信するトラフィックに適用する場合、ドロップダウン リストからその**プロキシ ポート**を選択します。
9. Filtering Service に送信する別名を指定するには、**[Advanced Settings]** を開き、**[Aliasing (別名の指定)]** をクリックします。このフィールドで、使用する名前を選択します。名前が指定されていない (入力フィールドが空白のままになっている) 場合、Web Security はユーザー名を含まない要求に対応する時の (設定されている) 動作を行います。別名の詳細については、[未知のユーザーと "別名" オプション](#)を参照してください。
10. **[LDAP Server Name (LDAP サーバー名)]** フィールドに LDAP サーバーの完全修飾ドメイン名とポート番号、または IP アドレスを入力します。
11. LDAP サーバー ポートがデフォルト (389) 以外のポートである場合、**[LDAP Server Port (LDAP サーバー ポート)]** フィールドに LDAP サーバーポートを入力します。

12. **LDAP ベース識別名**を入力します。この値は LDAP 管理者から取得します。
13. 任意に、LDAP UID フィルタを入力します。サーバー タイプが「LDAP」タブで指定されているサーバー タイプ（デフォルト値）と異なる場合、このフィールドを使ってサーバー タイプを指定します。Active Directory の場合は **sAMAccountName** を入力し、他のサービスの場合は **uid** を指定します。
14. **Bind DN** フィールドで、バインド識別名を入力します。これは LDAP ディレクトリ サービスのユーザーの完全識別名でなければなりません。例：
CN=John Smith,CN=USERS,DC=MYCOMPANY,DC=COM
15. **[Bind Password (バインド パスワード)]** フィールドに **[Bind DN]** フィールドで指定した名前に対応するパスワードを入力します。
16. Content Gateway が LDAP サーバーとの間でセキュアな通信を使用するようになるには、**[Secure LDAP]** をチェックします。
17. 任意に、LDAP 属性名を入力します。
18. 任意に、LDAP 属性値を入力します。
19. **[Add]** をクリックしてルールを追加します。
20. ページ上部で、ルール リストの中でのそのルールの位置をチェックし、調整します。最初に条件に一致したルールが適用されます。
21. **Apply** をクリックしてから、ルールを有効にするために Content Gateway を再起動します。

**警告**

ルールに無効な値がある場合、無効なルールを示した警告メッセージが表示されます。

認証レルム ルールの使用

ルールの編集

1. 「**Configure**」 > 「**Security**」 > 「**Access Control**」 > 「**Authentication Realms**」タブで、**[Edit File]** をクリックします。
2. ルールのテーブルで、変更するルールをクリックします。その値が定義領域のフィールドに入力されます。
3. 変更を行った後、**[Set]** をクリックし、次に **[Apply]** をクリックします。
4. **[Close]** をクリックして「**Authentication Realms (認証レルム)**」タブに戻ります。
5. 変更を有効にするために、Content Gateway を再起動します。

ルールのリストの順序変更

認証レルム ルールはリストの中の上から順に適用されます。

1. 「Configure」> 「Security」> 「Access Control」> 「Authentication Realms」タブで、[Edit File] をクリックします。
2. ルールのテーブルで、リストの中での位置を変更するルールをクリックし、次に左側の下向きまたは上向き矢印をクリックすることによってこのルールの位置を変更します。
3. ルールが希望する位置に置かれたとき、[Apply] をクリックします。
4. [Close] をクリックして「Authentication Realms (認証レルム)」タブに戻ります。
5. 変更を有効にするために、Content Gateway を再起動します。

ルールの削除

1. 「Configure」> 「Security」> 「Access Control」> 「Authentication Realms」タブで、[Edit File] をクリックします。
2. ルールのテーブルで、削除するルールをクリックして、左側の“X” ボタンをクリックします。
3. ルールの削除を完了したとき、[Apply] をクリックします。
4. [Close] をクリックして「Authentication Realms (認証レルム)」タブに戻ります。
5. 変更を有効にするために、Content Gateway を再起動します。

複数レルム認証の使用例

使用例 1:

この例では、既存の単一ドメイン環境にもう 1 つのドメインが追加されます。Content Gateway は明示のプロキシで、クライアントは PAC ファイルを使用します。

ある組織 - “Quality Corp” という名前であると仮定します - は Content Gateway のソフトウェア インストールを使用しています。この組織には 1 つのドメイン (QCORP) と 1 つのドメイン コントローラがあります。この組織は NTLM を使用してユーザーを認証します。

Quality Corp は New Corp を取得しました。New Corp は独自のドメイン (NCORP) とドメイン コントローラを持っています。New Corp は LDAP を使用してユーザーを認証します。

Quality Corp は両者の従業員を 1 つのドメインで管理したいと考えていますが、インフラストラクチャーの変更を行う用意はありません。その用意が整うまで、New Corp ユーザーには別の使用ポリシーを適用する (つまり、QCORP ドメインの “デフォルト” ユーザーを使用しない) ことを希望しています。

複数レルム認証機能によってそれが可能になります。

この解決策を設定するために、Quality Corp は次のことを行います。

1. 複数レルムの認証を有効化します。

2. 2 番目の、デフォルト以外の HTTP ポートを追加します ([Configure] > [Protocols] > [HTTP])。このポートは NCORP のすべてのメンバーが使用します。
3. NCORP のメンバーが新しい、2 番目のポートを通じて Content Gateway に接続するようにする PAC ファイルを作成します。
4. 複数レルムの認証のルールを、QCORP ドメインと NCORP ドメインのそれぞれのために 1 つずつ作成します。
 - a. 2 番目のポートへの接続のための NCORP ルールを定義します。
[Advanced Settings] 領域で、ポリシーの決定に使用するユーザーが固定文字列 "NCorpUser" であることを指定します。
 - b. 他のすべての接続を処理する QCORP ルールを定義します。
5. QCORP ドメインに "NCorpUser" を有効なユーザーとして追加し、TRITON - Web Security でそのユーザーのためのポリシーを作成します。

これによって、NCORP から Content Gateway に接続するすべてのユーザーが NCORP ドメイン コントローラに対して認証され、NCorpUser に関連付けられているグループ ポリシーを適用されます。このシナリオでは、個別ユーザーベースのポリシーまたは機能（例、割り当て時間）は処理できません。トランザクションは NCorpUser としてログ記録されます。これはすべて、QCORP ドメインのユーザーの認証、ポリシー、ログ記録にはどんな影響も及ぼしません。

使用例 2:

この例では、既存の単一ドメイン環境にもう 1 つのドメインが追加されます。Content Gateway は明示のプロキシで、クライアントは PAC ファイルを使用します。

ある組織 - "BigStars" という名前であると仮定します - は Content Gateway のソフトウェア インストールを使用しています。この組織には 1 つのドメイン (BIG) と 1 つのドメイン コントローラがあります。この組織は NTLM を使用してユーザーを認証します。

会社内の 1 つのグループが Apple コンピュータに切り替えますが、Apple コンピュータは NTLM では認証できません。IT グループは LDAP サーバーをインストールし、Apple ユーザーのために新しいドメイン "BIGAPL" を作成します。

このユーザーのグループは以前に存在しており、プライマリ ドメイン (BIG) 上で管理されていましたから、IT 部では、ユーザーベースのポリシーとログ記録の両方が依然として適用されると想定しています。

複数レルム認証機能によってそれが可能になります。

この解決策を設定するために、BigStars は次のことを行います。

1. BIGAPL のすべてのユーザーが BIG にも存在し、正確に同じユーザー名を割り当てられていることを確認します。
2. 複数レルムの認証を有効化します。

3. 2 番目の、デフォルト以外の HTTP ポートを追加します ([Configure] > [Protocols] > [HTTP])。このポートは BIGAPL のすべてのメンバーが使用します。
4. BIGAPL のメンバーが新しい、2 番目のポートを通じて Content Gateway に接続するようにする PAC ファイルを作成します。
5. 複数レルムの認証のルールを、BIGAPL ドメインと BIG ドメインのそれぞれのために 1 つずつ作成します。
 - a. 2 番目のポートへの接続のための BIGAPL ルールを定義します。
 - b. 他のすべての接続を処理する BIG ルールを定義します。

これによって、BIGAPL のすべてのメンバーは LDAP によって認証されますが、それらの既存の NTLM ID によって指定されている個別のポリシーが引き続き適用されます。ログおよびレポートもその同じユーザーを参照します。

使用例 3:

この例では、既存の単一ドメイン環境にもう 1 つの、特別の目的を持つドメインが追加されます。Content Gateway は WCCP v2 を使用する透過的プロキシです。

ある組織 – “Creative Corp” という名前であると仮定します – は Content Gateway のソフトウェア インストールを使用しています。この組織には 1 つのドメイン (CCORP) と 1 つのドメイン コントローラがあります。この組織は NTLM を使用してユーザーを認証します。

Creative Corp は、新製品を発売し、躍進を遂げたいと考えています。この会社はキオスク、デモンストレーション、プレゼンターを揃えたオープン ハウスを設立することを決定しました。キオスクは、新製品の適切なデモンストレーションのために、デフォルトのインターネット ポリシーのみを必要としています。IT マネージャはキオスク ネットワークを可能な限り社内イントラネットから隔離したいと考えています。このシナリオでは、個別ユーザーのログ記録は必須要件ではありません。

複数レルム認証機能によってそれが可能になります。

この解決策を設定するために、Creative Corp は次のことを行います。

1. 独自のドメイン コントローラを備えた新しい、一時的なネットワークを構築します。これを “CTEMP” ドメインと名付けます。
2. CTEMP に 1 人または複数のユーザーを追加します。これらのユーザーはプライマリ ドメイン上の既存のユーザーと 1 対 1 で対応させるか、または、プレゼンターが使用する 1 つ以上の一般ユーザーとして指定することができます。
3. CTEMP 上のトラフィックを WCCP v2 が使用されている Content Gateway へリダイレクトします。
4. 複数レルムの認証を有効化します。
5. 複数レルムの認証のルールを、CTEMP ドメインと CCORP ドメインのそれぞれのために 1 つずつ作成します。

- a. CTEMP ドメインに割り当てられている IP アドレス範囲から着信するすべての接続に適用する CTEMP ルールを定義します。[Advanced Settings] 領域で [Aliasing] を指定し、このフィールドを空白にしておきます。これによってデフォルト ポリシーが CTEMP のすべてのユーザーに適用されます。
- b. 他のすべての接続を処理する CCORP ルールを定義します。

これによって、いずれかのキオスク上でインターネットを使用しているユーザーは CTEMP ネットワークに対して認証され、要求に対してデフォルト ポリシーが適用されます。

複数レルムの認証のトラブルシューティング

複数レルムの認証では、下記のような問題がしばしば発生します。

- ◆ ユーザーに対して認証を要求するべき時に、認証が *要求されない*。
- ◆ ユーザーに対して認証を要求する必要がない時に、認証が *要求される*。
- ◆ ユーザー認証が間違っただメインに対して行われる。

これらの問題は、ユーザー認証プロセスの下記のいずれかの段階において発生します。

- ◆ 一般的なユーザー認証ロジック（下記を参照）
- ◆ レルム ルールの定義と照合
- ◆ ユーザー認証プロトコル処理 (IWA、NTLM、LDAP; IWA のトラブルシューティングについては [統合 Windows 認証のトラブルシューティング](#)を参照)

複数レルムの認証のロジック

複数レルムの認証は常に、以下のロジックに適用します。

1. **filter.config** 内のルールがチェックされ、適用されます。このアクションは、すべてのタイプの Content Gateway ユーザー認証の最初のステップとして行われます。適合するフィルタリング ルールが見つかった場合、そのルールが適用され、ユーザー認証プロセスは終了します。[フィルタリングルール, 188 ページ](#) を参照してください。
2. 適合するフィルタリング ルールが見つからない場合、レルム ルールの照合が実行されます。要求の IP アドレスが、ルール セットに対して、上から順に照合されます。IP アドレスに適合するルールが見つかった場合、ソース ポートがチェックされます（ルールの中でソース ポートが定義されている場合）。最初に条件に一致したルールが適用されます。**条件に一致するルールがない場合、認証要求は行われません。**
3. 適合するルールが見つかった場合、指定されたドメインに対して指定された認証プロトコルが適用されます。すべてのルール設定の詳細が適用されます。
4. ユーザーが認証された場合、要求は処理されるか、または Web Security ポリシーによって拒否されます。
5. このトランザクションはログに記録されます。

ロジックが実行環境にどのように適用されるかを調べるために、一時的にユーザー認証デバッグ出力を有効化することができます。デバッグ出力は、特に、ルールの解析と照合の詳細を示します。[ユーザー認証デバッグ出力の有効化と無効化](#)を参照してください。

トラブルシューティング

複数レルムの認証が所期の結果をもたらさない場合、以下の順序でトラブルシューティングを実行することを推奨します。

1. ネットワーク アドレス変換 (NAT) をチェックする

想定外の IP アドレスの NAT が行われていないことを確認します。ネットワーク アドレス変換を行うと、ユーザー認証が実行される前に元のソース IP アドレスが別のアドレスに変更されます。Content Gateway Manager で **[Configure]** > **[Networking]** > **[ARM]** > **[General]** を選択し、`ipnat.config` の中のルールを調べます。

2. filter.config 内のルールのチェック

想定外の `filter.config` ルールとの一致がないことを確認します。`filter.config` ルールは、特に、ユーザー認証を迂回するために使用することができます。[フィルタリング ルール](#)を参照してください。

3. レルム ルールの一致のチェック

想定に反して認証が要求された、または認証が要求されなかったユーザーの IP アドレスを使用して、各レルム ルールを上から順に調べ、その設定が条件に一致している最初のものを見つけます。この分析は、細部まで慎重に行ってください。よくある問題は、その IP アドレスを含む IP アドレス範囲が広すぎることです。

ルールが別名を使用している場合、その別名がプライマリ ドメイン コントローラの User Service の中にあることを確認します。

特定のポートにトラフィックを送信するように設定されている明示のクライアントについては、クライアントのブラウザのルールと設定の両方をチェックします。

4. ドメインのチェック

想定している一致するドメインが見つかった場合、そのドメインがアクセス可能であり、そのユーザーがそのドメインのメンバーであることを確認します。それが確認された場合、認証プロトコル レベルの問題のトラブルシューティングを行います。IWA については [統合 Windows 認証のトラブルシューティング](#)を参照してください。

5. Content Gateway がプロキシ チェーンの中にある場合

Content Gateway がプロキシ チェーンのメンバーである場合、「X-Forwarded-For」ヘッダーがダウンストリーム プロキシによって送信され、Content Gateway によって読み取られることを確認します。

- パケット スニファーを使ってダウンストリームのプロキシからのインバウンド パケットを検査します。適切な形式の「X-Forwarded-For」ヘッダーを探します。

- Content Gateway Manager で、[Configure] > [My Proxy] > [Basic] を選択し、ページの最下部までスクロールし、[Read authentication from child proxy (子プロキシからの認証の読み取り)] を有効化します。有効化されていない場合は [On] を選択し、[Apply] をクリックし、次に Content Gateway を再起動します。

ユーザー認証デバッグ出力の有効化と無効化



警告

デバッグ出力を有効化したままにはしてはいけません。デバッグ出力はプロキシのパフォーマンスを低下させ、ファイルシステムをログ出力でいっぱいにしてしまいます。

デバッグ ログ情報は下記のファイルに書き込まれます。`/opt/WCG/logs/content_gateway.out`

ユーザー認証デバッグ情報を有効化するには、下記のファイルを編集します。`/opt/WCG/config/records.config`

```
(root)# vi /opt/WCG/config/records.config
```

以下のパラメータを見つけ、変更して、下記のように値を割り当てます。

```
CONFIG proxy.config.debug.enabled INT 1
CONFIG proxy.config.debug.tags STRING
auth_* | winauth.* | ldap.* | ntlm.*
```

ファイルを保存して、閉じます。下記のコマンドによって、Content Gateway がファイルを再読み込みするように指示します。

```
(root)# /opt/WCG/bin/content_line -x
```

`tail -f` コマンドによってデバッグ情報のフローを追跡します。

```
(root)# tail -f /opt/WCG/logs/content_gateway.out
```

`Ctrl+C` を使用してコマンドを終了します。

必要なデバッグ出力の収集が完了したとき (1 つ以上のユーザー認証プロセスを完了した後)、`records.config` を編集して、パラメータ値を下記のように変更することによってデバッグ出力を無効化します。

```
(root)# CONFIG proxy.config.debug.enabled INT 0
```

ファイルを保存して、閉じます。下記のコマンドによって、Content Gateway がファイルを再読み込みするように指示します。

```
(root)# /opt/WCG/bin/content_line -x
```

15

ログ ファイルの使用

関連項目：

- ◆ [イベント ログ ファイル, 234 ページ](#)
- ◆ [イベント ログ ファイルの管理, 235 ページ](#)
- ◆ [イベント ログ ファイルのフォーマット, 237 ページ](#)
- ◆ [イベント ログ ファイルの取り込み, 244 ページ](#)
- ◆ [イベント ログ ファイルの分割, 247 ページ](#)
- ◆ [イベント ログ ファイルの照合, 249 ページ](#)
- ◆ [ログ記録統計情報の表示, 253 ページ](#)
- ◆ [ログ ファイルの表示, 254 ページ](#)
- ◆ [イベント ログ ファイル エントリの例, 255 ページ](#)

Websense Content Gateway には 3 種類のログ ファイルがあります：

- ◆ システム ログ ファイルはシステム情報を記録しますが、これは Content Gateway の状態に関するメッセージと Content Gateway によって出されたエラーや警告を含んでいます。この情報には、イベント ログ ファイルが取り込まれたというメッセージ、クラスタ通信がタイムアウトになったという警告、および Content Gateway が再起動されたことを示すエラーが含まれます。(Content Gateway は、エラー状態を知らせるアラームを Content Gateway Manager 上で出します。詳細については、[アラームの処理, 125 ページ](#) を参照してください。)

すべてのシステム情報メッセージは、デーモン機能のもとでシステム全体のログ機能 **syslog** によってログ記録されます。**syslog.conf** 設定ファイル (/etc directory に保存されています) で、これらのメッセージがログ記録される場所が指定されます。通常の場合は **/var/log/messages** です。

syslog プロセスはシステム全体を対象にして動作するので、このプロセスはすべての Content Gateway プロセス (これは **content_gateway**、**content_manager**、および **content_cop** を含みます) によるメッセージを記録する単一のレポジトリになっています。

ログ中の各ログ エントリは、エラーがログ記録された日時、エラーをレポートしたプロキシ サーバーのホストネーム、およびエラーまたは警告の説明についての情報を保持しています。

Content Gateway によってログ記録されるシステム情報メッセージのリストについては、[Websense Content Gateway のエラー メッセージ, 469 ページ](#) を参照してください。

- ◆ エラー ログ ファイルは、トランザクションがエラーになった理由に関する情報も記録します。
- ◆ イベント ログ ファイル(アクセス ログ ファイルともいいます)は、Content Gateway が処理した各トランザクションの状態に関する情報を記録します。

Content Gateway はエラーおよびイベントの両ログ ファイルを作成し、システム情報をシステム ログ ファイルに記録します。イベント ログ記録とエラー ログ記録の両方またはいずれか一方を無効にすることができます。ピーク時にはエラーのログ記録だけにするか、またはログ記録を無効にすることをお勧めします。

- [Configure (設定)] > [Subsystems (サブシステム)] > [Logging (ログ記録)] タブで、次のようなオプションのいずれかを選択します: [Log Transactions and Errors (トランザクションとエラーのログ記録)], [Log Transactions Only (トランザクションだけのログ記録)], [Log Errors Only (エラーだけのログ記録)], または [Disabled (無効)]。

イベント ログ ファイル

イベント ログ ファイルは、Websense Content Gateway が処理するあらゆる要求についての情報を記録します。ログ ファイルを分析することによって、プロキシを利用しているユーザーの数、各ユーザーが要求している情報量、非常に人気があるページ、等々について調べることができます。

Content Gateway はいくつかの標準ログ ファイル フォーマット(例、Squid、Netscape)とユーザー定義カスタム フォーマットをサポートしています。標準フォーマットのログ ファイルは、既製の分析パッケージによって分析することができます。ログ ファイルを分割し、各ファイルがプロトコルまたはホスト固有の情報を含むようにしておくこと、ログ ファイルの分析が容易になります。また、ログ ファイルを特定の時間間隔で自動的に取り出すように Content Gateway を構成することもできます。

以下の各セクションでログ ファイルの取り扱いについて説明しています:

- ◆ イベント ログ ファイルの管理
 - ログ ファイルを保存する集中的場所、ログ ファイルのためのディスクスペース、およびログ ファイルを取り出す回数と時刻について設定することができます。[イベント ログ ファイルの管理, 235 ページ](#) を参照してください。
- ◆ 種々のイベント ログ ファイル フォーマットの選択

トラフィック分析で使用する標準ログ ファイル フォーマットを選択できません (例、Squid、Netscape)。あるいは、XML ベースの Content Gateway カスタム フォーマットを使用すると、ログ ファイルで記録する情報の種類をより細かに管理することができます。[イベント ログ ファイルのフォーマット, 237 ページ](#) を参照してください。

- ◆ イベント ログ ファイルの自動的な取り出し
1 日のうち特定の時間間隔でイベント ログ ファイルを自動的に取り出すように Content Gateway を構成することができます、これによってアクティブでないログ ファイルを取り扱えるようになります。[イベント ログ ファイルの取り込み, 244 ページ](#) を参照してください。
- ◆ ホストごとの個別のログ ファイル
異なるプロトコルの個別のログ ファイルをホスト ベースに作成するようにプロキシを構成することができます。[イベント ログ ファイルの分割, 247 ページ](#) を参照してください。
- ◆ 異なるノードのログ ファイルの照合
ネットワーク上の 1 つ以上のノードをログ照合サーバーとして機能するように指定することができます。これらのサーバーはスタンドアロンまたは Content Gateway の一部のどちらでもよく、照合サーバーによってすべてのログ記録情報を適切に定義された場所で保存することができます。[イベント ログ ファイルの照合, 249 ページ](#) を参照してください。
- ◆ ログ記録システムに関する統計情報の表示
Content Gateway はログ記録システムに関する統計情報を提供します。Content Gateway Manager または コマンドライン インターフェースにより、この統計情報にアクセスします。[ログ記録統計情報の表示, 253 ページ](#) を参照してください。
- ◆ ログ ファイルの表示
Content Gateway が作成するシステム、イベント、およびエラーの各ログ ファイルを表示できます。ログ ファイル全体、ログ ファイル末尾からの指定行数、または指定の文字列を含むすべての行を表示できます。
- ◆ 標準ログ ファイル フォーマットのログ ファイル エントリの解釈。See [イベント ログ ファイル エントリの例, 255 ページ](#)。

イベント ログ ファイルの管理

イベント ログ ファイルを管理し、ログ ファイルの保存場所、ログ ファイルが使用できるスペースの容量、およびログ記録ディレクトリのディスク スペースが小さくなったときの対応について設定することができます。

ログ記録ディレクトリの選択

デフォルトにより、Content Gateway はすべてのイベント ログ ファイルを `logs` ディレクトリに書き込みますが、これは Content Gateway がインストー

ルされているディレクトリにあります。別のディレクトリを使用する場合は、[ログ ファイル管理オプションの設定, 236 ページ](#) を参照してください。

ログ記録スペースの管理

ログ記録ディレクトリが使用できるディスク スペースの大きさを管理することができます。これにより、システムは指定のスペースの枠内で長期にわたってスムーズに作動することができます。

スペース限界が設定されたら、Content Gateway はログ記録ディレクトリのスペースを継続してモニタします。空きスペースが減少してヘッドルーム限界に近づくと ([ログ ファイル管理オプションの設定, 236 ページ](#) 参照)、Content Gateway は小スペース状態になり、以下のような処置を行います：

- ◆ 自動削除オプション ([イベント ログ ファイルの取り込み, 244 ページ](#) 参照) が有効であると、Content Gateway は以前に取り込まれたログ ファイル (.old 拡張子のログ ファイル) を特定し、それらを古いものから削除しはじめ、小スペース状態から抜け出すまで続けます。Content Gateway は、それが削除するすべてのファイルの記録をシステム エラー ログ中に残します。
- ◆ 自動削除オプションが無効であるか、またはシステムが小スペース状態から抜け出すのに十分な古いログ ファイルがない場合は、Content Gateway は警告を出し、スペースがなくなるまでログ記録を継続します。小スペース状態から抜け出すのに十分なスペースが利用できるようになると、Content Gateway はイベント ログ記録を再開します。ログ記録ディレクトリからファイルを消去するか、またはログ記録スペース限界を増大することによって、利用可能なスペースをつくることができます。

cron スクリプトを Content Gateway と連携して実行させることによって、Content Gateway が小スペース状態になる前にログ記録ディレクトリから古いファイルを自動的に除去し、それらを一時パーティションに移すことができます。古いファイルを移動したら、これらのファイルについてログ分析スクリプトを実行することができ、次にこれらを圧縮してアーカイブ場所に移すか、または削除することができます。

ログ ファイル管理オプションの設定

1. [Configure (構成)] > [Subsystems (サブシステム)] > [Logging (ログ記録)] に移ります。

2. **[Log Directory (ログ ディレクトリ)]** フィールドで、イベント ログ ファイルを保存しようとするディレクトリのパスを入力します。これは絶対パスでもよいし、または Content Gateway がインストールされているディレクトリに対する相対パスでも結構です。デフォルトのディレクトリは、Content Gateway インストール ディレクトリ中の **logs** です。

**ご注意**

指定されるディレクトリはすでに存在していません。

Websense ユーザーは、ログ ファイルを保存するディレクトリについて読み取り / 書き込み許可を保持していなければなりません。

3. **[Log Space (ログ スペース)]** エリアの **[Limit (限界)]** フィールドで、ログ記録ディレクトリに割り当てるスペースの最大容量を入力します。

Content Gateway が V シリーズ アプライアンス上である場合は、そのサイズは 5120 (5 GB) に設定され、これを変更することはできません。

Content Gateway がスタンドアロン サーバーにインストールされている場合は、デフォルトのサイズは 20480 (20 GB) であり、このサイズは設定可能です。

**ご注意**

ログ記録ディレクトリ中のすべてのファイルは、ログファイルでないものも含めて、なんらかのスペースを使用します。

4. **[Headroom (ヘッドルーム)]** フィールドで、ログ記録スペース限界の許容値を入力します。デフォルト値は 100 MB です。

[Log Rolling (ログ 取り込み)] セクションで **[Auto-Delete Rolled Files (取り込みファイルの自動削除)]** オプションが有効になっている場合、ログ記録ディレクトリで利用できる空きスペースがヘッドルームより小さくなると、自動削除がトリガされます。ログ ファイルの取り込みについては、[イベント ログ ファイルの取り込み, 244 ページ](#) を参照してください。

5. **[Apply]** をクリックします。

イベント ログ ファイルのフォーマット

Websense Content Gateway は下記のログ ファイル フォーマットをサポートします：

- ◆ **標準フォーマット**: Squid や Netscape など ([標準フォーマットの使用, 238 ページ](#) を参照してください)

- ◆ Content Gateway カスタム フォーマット ([カスタム フォーマット, 239 ページ](#) を参照してください)

標準およびカスタム ログ ファイル フォーマットのほかに、ログ ファイルをバイナリまたは ASCII のどちらで保存するかについて選択しなければなりません。[バイナリまたは ASCII の選択, 242 ページ](#) を参照してください。



重要

イベント ログ ファイルは大量のディスク スペースを消費します。同時に複数のフォーマットでログ エントリを作成すると、ディスク リソースを速やかに消費し、プロキシ パフォーマンスに影響することがあります。



重要

IPv6 が有効であると、イベント ログのエントリが IPv6 フォーマットに標準化されます。

例えば、“10.10.41.200” は、“::ffff:10.10.41.200” とログ記録されます。

カスタム ログ中で“10.10.41.200” のクライアントをフィルタリングするには、下記のフィルタが必要です。

```
<LogFilter>
  <Name = "IPv6_Test_Machine"/>
  <Condition =
    "chi MATCH ::ffff:10.10.41.200"/>
  <Action = "ACCEPT"/>
</LogFilter>
```

標準フォーマットの使用

標準ログ ファイル フォーマットには、Squid、Netscape Common、Netscape Extended、および Netscape Extended-2 があります。

標準ログ ファイル フォーマットは、各種の既製分析パッケージによって分析することができます。標準フォーマットで対応できない情報を必要としないかぎり、いずれかの標準イベント ログ フォーマットを使用すべきです。[カスタム フォーマット, 239 ページ](#) を参照してください。

デフォルトでは、Content Gateway は Netscape Extended ログ ファイル フォーマットだけを使用するように構成されています。

標準ログ ファイル フォーマット オプションの設定

1. [Configure] > [Subsystems] > [Logging] > [Formats (フォーマット)] に移りません。
2. 使用するフォーマットを有効にします。
3. ログ ファイルの種類 (ASCII またはバイナリ) を選択します。

4. [Filename (ファイルネーム)] フィールドで、イベント ログ ファイルで使用する名前を入力します。
5. [Header (ヘッダー)] フィールドで、イベント ログ ファイルの最上部で表示されるテキスト ヘッダーを入力します。テキスト ヘッダーを使用しない場合は、このフィールドを空白のままにします。
6. [Apply] をクリックします。
7. [Configure (構成)] > [My Proxy (マイ プロキシ)] > [Basic (基本)] > [General (一般)] で [Restart (再起動)] をクリックします。

カスタム フォーマット

XML ベースのカスタム ログ フォーマットは標準ログ ファイル フォーマットよりも柔軟であり、ログ ファイル中の情報の種類をよりよく管理できるようになります。標準フォーマットで対応できないデータ分析を必要とする場合は、カスタム ログ フォーマットを作成します。各 Content Gateway トランザクションで記録すべき情報を確定し、ログ記録すべきトランザクションを定義するフィルタを作成します。

カスタム ログ記録機能の中心は XML ベースのログ記録構成ファイル (`logs.xml.config`) であり、これによりログ記録オブジェクトのモジュラ記述を作成することができます。`logs.xml.config` ファイルは、カスタム ログ ファイルを作成するために下記の 3 種類のオブジェクトを使用します：

- ◆ **LogFormat** は、printf スタイル フォーマットの文字列によってログ ファイルのコンテンツを定義します。
- ◆ **LogFilter** は、ログファイルに特定の情報を含めたり、そこから特定の情報を除外したりするフィルタを定義します。
- ◆ **LogObject** は、ログ ファイルの生成のために必要なすべての情報を指定します。例：
 - ログ ファイルの名前 (必須)。
 - 使用するフォーマット (必須)。これは、標準フォーマット (Squid あるいは Netscape) または事前に定義されているカスタム フォーマット (事前定義の **LogFormat** オブジェクト) のどちらかです。
 - ファイル モード (ASCII、Binary (バイナリ)、または ASCII_PIPE)。デフォルトは ASCII です。

ASCII_PIPE モードは、UNIX 名前付きパイプ（メモリ中のバッファ）にログ エントリを書き込みます。これによって、他のプロセスが標準 I/O 機能によりデータを読めるようになります。このオプションの利点は、Content Gateway によるハードディスク書き込みが不要になり、ディスク スペースと帯域幅が他のタスクのために解放されることです。



ご注意

バッファが一杯であると、Content Gateway はログ エントリをドロップし、抜け落ちたエントリの数を明示するエラー メッセージを出します。Content Gateway は完全なログ エントリだけをパイプに書き込むので、抜け落ちるのは完全なレコードだけです。

- 使用する任意のフィルタ（事前定義の **LogFilter** オブジェクト）。
- ログ ファイルを受け取る照合サーバー。
- ログ記録しようとするプロトコル（プロトコル タグが使用されていると、Content Gateway はリストされているプロトコルからのトランザクションだけをログ記録します。そうでない場合は、すべてのプロトコルについてすべてのトランザクションがログ記録されます）。
- ログ記録しようとするオリジン サーバー（サーバー タグが使用されていると、Content Gateway はリストされているオリジン サーバーのトランザクションだけをログ記録します。そうでない場合は、すべてのオリジン サーバーについてすべてのトランザクションがログ記録されます）。
- ログ ファイルに含めるヘッダ テキスト。ヘッダ テキストは、ログ ファイルの冒頭で最初のレコードの直前に表示されます。
- ログ ファイル取り込みオプション。



ご注意

カスタム ログ フォーマットを生成するには、少なくとも 1 つの **LogObject** 定義を指定しなければなりません。各 **LogObject** 定義ごとに 1 つのログ ファイルがつくられます。カスタム ログ フォーマットを作成するには、Content Gateway Manager を使用するか、または構成 ファイルを編集します。

1. **[Configure]** > **[Subsystems]** > **[Logging]** > **[Custom (カスタム)]** で、**[Custom Logging (カスタム ログ記録)]** オプションを有効にします。
2. **[Custom Log File Definitions (カスタム ログ ファイル定義)]** エリアで **logs_xml.config** ファイルが表示されます。「**LogFormat**」、「**LogFilter**」、および「**LogObject**」定義を構成ファイルに追加します。
logs_xml.config ファイルおよび関連するオブジェクト定義の詳細については、[logs_xml.config, 385 ページ](#) を参照してください。
3. **[Apply]** をクリックします。

要約ログ ファイルの作成

Content Gateway は、毎秒、数百のオペレーションを実行するので、イベント ログ ファイルは非常に大きくなります。SQL 式の集計演算子を使用して、特定の期間にわたるログ エントリのセットをまとめた要約ログ ファイルを作成するように Content Gateway を構成することができます。このことによって、生成されるログ ファイルのサイズを縮小することができます。

XML ベースのログ記録構成ファイル (`logs_xml.config`) で `LogFormat` オブジェクトを作成することによって要約ログ ファイルを生成するには、下記の SQL 式集計演算子を利用します：

- ◆ COUNT
- ◆ SUM
- ◆ AVERAGE
- ◆ FIRST
- ◆ LAST

これらの演算子をそれぞれ特定のフィールドに適用し、指定間隔にわたって作動するように要求することができます。

要約ログ ファイルは利便性と情報の精細性とのトレードオフを表しています。ただ 1 つのレコードが生成される時間間隔を指定しなければならないので、これにより情報が失われるかもしれません。要約ログの利便性と通常のログ ファイルの詳細性の両方を必要とする場合は、2 種類のカスタム ログ フォーマットの作成と運用を検討してください。一方のログ フォーマットでは集計演算子を利用し、他方のログ フォーマットでは集計演算子を利用しないのです。

要約ログ ファイル フォーマットを作成するには、下記の手順に従います：

1. **[Configure]** > **[Subsystems]** > **[Logging]** > **[Custom]** に移り、`logs_xml.config` ファイルを表示します。
2. 下記に従ってログ ファイルのフォーマットを定義します：

```
<LogFormat>
  <Name = "summary"/>
  <Format = "%<operator(field)> : %<operator(field)>"/>
  <Interval = "n"/>
</Format>
```

ここで：

`operator` は、5 つの演算子 (**COUNT**、**SUM**、**AVERAGE**、**FIRST**、**LAST**) の 1 つです。フォーマット行で 2 つ以上の演算子を指定できません。

`field` は、集計しようとするログ記録フィールドです。

`n` は、要約ログ エントリ間の秒単位の間隔です。

詳細については、[logs_xml.config, 385 ページ](#) を参照してください。

例えば、下記のフォーマットは 10 秒ごとに 1 つのエントリを生成し、各エントリでは当該エントリの最新のエントリのタイム スタンプ、10 秒間

隔内に認められたエントリ数のカウント、およびクライアントに送信されたすべてのバイト数の合計が要約されます：

```
<LogFormat>
  <Name = "summary"/>
  <Format = "%<LAST(cqts)> : %<COUNT(*)> :
    %<SUM(psql)>"/>
  <Interval = "10"/>
</Format>
```



重要

集計演算子と標準フィールドの両方を含むフォーマット定義を作成することはできません。例えば、下記の定義を無効です：

```
<Format = "%<LAST(cqts)> : %<COUNT(*)> :
  %<SUM(psql)> : %<cqu>"/>
```

3. このフォーマットを使用する **LogObject** を定義します。
4. **[Apply]** をクリックします。

バイナリまたは ASCII の選択

下記のどちらかのイベント ログ ファイルを作成する Content Gateway を構成することができます：

- ◆ **ASCII:** この種類のファイルは、既製の標準的分析ツールによって処理できます。しかし、Content Gateway は ASCII でファイルを作成するために追加的処理を実行しなければならず、その結果、オーバーヘッドが大きくなります。また ASCII ファイルは、同等なバイナリ ファイルよりも大きくなりがちです。ASCII ログ ファイルの拡張子はデフォルトで **.log** となります。
- ◆ **Binary (バイナリ):** この種類のファイルはシステムにとってオーバーヘッドが小さく、また、ログ記録される情報のタイプにもよりますが、一般にディスクの使用スペースが少なくてすみます。しかし、標準ツールによってこの種のファイルを読んだり、分析する前に、変換アプリケーションを使用しなければなりません。バイナリ ログ ファイルの拡張子はデフォルトで **.blog** となります。

バイナリ ログ ファイルでは、ディスクスペースの使用は一般に少なくなるのですが、常でそうであるとはいえません。例えば、0 (ゼロ) 値は、ASCII で保存する場合は 1 バイトにすぎませんが、バイナリ整数として保存する場合は 4 バイトになります。IP アドレスをログ記録するカスタム フォーマットを定義するとき、バイナリ ログ ファイルでは 32 ビット アドレスごとに 4 バイトの記憶容量を必要とするにすぎません。しかし、同じ IP アドレスをドット表記法で保存すると、ASCII ログ ファイルでは約 15 文字 (バイト) が必要になります。

標準ログ フォーマットでは、Content Gateway Manager の **[Configure] > [Subsystems] > [Logging] > [Formats]** タブで **[Binary]** または **[ASCII]** を選択し

ます。 [標準ログ ファイル フォーマット オプションの設定, 238 ページ](#) を参照してください。カスタム ログ フォーマットでは、**LogObject** で ASCII または Binary モードを指定します。 [カスタム フォーマット, 239 ページ](#) を参照してください。



ご注意

カスタム ログ ファイルでは、ASCII および Binary オプションの他に、UNIX 名前付きパイプ（メモリ中のバッファ）にログ エントリを書き込むことができます。これによって、他のプロセスが標準 I/O 機能によりデータを読めるようになります。このオプションの利点は、Content Gateway によるハードディスク書き込みが不要になり、ディスクスペースと帯域幅が他のタスクのために解放されることです。また、UNIX 名前付きパイプはディスクスペースを使用しないので、ログ記録スペースが使い尽くされても、パイプへの書き込みは中断しません。ASCII_PIPE オプションの詳細については、 [logs_xml.config, 385 ページ](#) を参照してください。

ログ ファイルで ASCII またはバイナリ モードを選択する前に、ログ記録するデータのタイプについて検討してください。別々の日にそれぞれ ASCII およびバイナリ モードでログ記録をとってみてください。両日の要求数がほぼ同じであるものとする、大ざっぱに両フォーマットを数量的に比較することができます。

logcat によるバイナリ ログから ASCII ログへの変換

バイナリ ログ ファイルを ASCII ファイルに変換して、標準ツールで分析できるようにしなければなりません。

1. バイナリ ログ ファイルを保存しているディレクトリに移ります。
2. **logcat** ユーティリティのパスが有効であることを確認してください。
3. 次のコマンドを入力します：

```
logcat options input_filename...
```

下記の表はコマンド行オプションについての説明です。

オプション	説明
<code>-o output_file</code>	コマンドの出力先を指定します。
<code>-a</code>	入力ファイル名に基づいて出力ファイル名を自動的に生成します。入力が <code>stdin</code> からであると、このオプションは無視されます。 例： <code>logcat -a squid-1.blog squid-2.blog squid-3.blog</code> により、下記のファイルが生成されます： <code>squid-1.log squid-2.log squid-3.log</code>
<code>-S</code>	可能であれば、入力を Squid フォーマットに変換しようとします。
<code>-C</code>	可能であれば、入力を Netscape Common フォーマットに変換しようとします。
<code>-E</code>	可能であれば、入力を Netscape Extended フォーマットに変換しようとします。
<code>-2</code>	可能であれば、入力を Netscape Extended-2 フォーマットに変換しようとします。



ご注意

下記のオプションのうち、どれか 1 つだけを使用するようにしてください：`-S`、`-C`、`-E`、または `-2`。

入力ファイルが指定されていないと、`logcat` は標準入力 (`stdin`) から読み込みます。出力ファイルが指定されていないと、`logcat` は標準出力 (`stdout`) に書き出します。

例えば、バイナリ ログ ファイルを ASCII ファイルに変換するには、下記のオプションどちらかで `logcat` コマンドを使用します。

```
logcat binary_file > ascii_file
logcat -o ascii_file binary_file
```

バイナリ ログ ファイルは、このコマンドによって変更されません。

イベント ログ ファイルの取り込み

Websense Content Gateway は自動ログ ファイル取り込み機能を提供します。すなわち、Content Gateway は 1 日のうち特定の区間で現在のセットのログ ファイルを閉じ、新しいログ ファイルを開きます。

ログ ファイル取り込みには、下記のような便益があります：

- ◆ これは、ログ分析を実行できる時間間隔を定義します。

- ◆ これは単一のログ ファイルが過大になるのを防止し、指定されている限界のスペースでのログ記録システムの動作を支援します。
- ◆ これは、使用されなくなっているファイルを特定して、自動化スクリプトによるログ記録ディレクトリのクリーンアップとログ分析プログラムの実行を容易にします。

1 日に数回、ログ ファイルを取り込むべきです。6 時間ごの取り込みが好ましいガイドラインになるでしょう。

取り込みログ ファイルネーム フォーマット

Websense Content Gateway は、取り込まれたログ ファイルの特定を容易にする統合的なネーム フォーマットを提供します。

Content Gateway がログ ファイルを取り込むとき、古いファイルを保存して閉じ、新しいファイルを開始します。Content Gateway は古いファイルをリネームして、下記の情報を含めます：

- ◆ ファイルのフォーマット（例、**squid.log**）。
- ◆ ログ ファイルを生成した Content Gateway サーバーのホストネーム。
- ◆ ハイフン (-) で区切られた 2 つのタイムスタンプ。最初のタイムスタンプは、ログ ファイル中の最初のレコードのタイムスタンプの下限です。この下限は、ログ レコードのために新しいバッファが作成されるときの時刻です。低負荷のもとでは、ファイルネーム中の最初のタイムスタンプは最初のエントリのタイムスタンプと異なることがあります。標準負荷のもとでは、ファイルネーム中の最初のタイムスタンプと最初のエントリのタイムスタンプは近似します。
二番目のタイムスタンプは、ログ ファイル中の最後のレコードのタイムスタンプの上限です（これは、通常、取り込み時刻です）。
- ◆ 接尾辞の **.old** - これは自動化スクリプトによる取り込みログ ファイルの検出を容易にします。

タイムスタンプは次のようなフォーマットになっています：

```
%Y%M%D.%Hh%Mm%Ss-%Y%M%D.%Hh%Mm%Ss
```

以下の表でフォーマットについて説明しています：

コード	定義	例
%Y	4 桁表記の年	2000
%M	2 桁表記の月、01-12	07
%D	2 桁表記の日、01-31	19
%H	2 桁表記の時、00-23	21
%M	2 桁表記の分、00-59	52
%S	2 桁表記の秒、00-59	36

下記は取り込みログ ファイルネームの例です：

```
squid.log.mymachine.20000912.12h00m00s-  
20000913.12h00m00s.old
```

この例では、ファイルは squid ログ フォーマットであり、そのホスト コンピュータは mymachine です。最初のタイムスタンプは、2000 年、9 月、12 日、正午 12 時 00 分という日時を示しています。二番目のタイムスタンプは、2000 年、9 月、13 日、正午 12 時 00 分という日時を示しています。ファイルネームの終りに接尾辞の .old があります。

ログ記録システムは、ログ レコードをディスクに書き込む前に、それらをバッファします。ログ ファイルが取り込まれるとき、ログ バッファはかなり一杯になっているかもしれません。そのような場合、新しいログ ファイルの最初のエントリのタイムスタンプは取り込み時刻よりも前になるでしょう。新しいログ ファイルが取り込まれると、その最初のタイムスタンプが最初のエントリのタイムスタンプの下限になります。例えば、ログ記録が 3 時間毎に取り込まれるものとし、最初の取り込みログ ファイルが下記のものであるとします：

```
squid.log.mymachine.19980912.12h00m00s-  
19980912.03h00m00s.old
```

3:00:00 の時点のログ バッファの最初のエントリの下限が 2:59:47 であると、次のログ ファイルが取り込まれると、そのタイムスタンプは下記のようになります：

```
squid.log.mymachine.19980912.02h59m47s-  
19980912.06h00m00s.old
```

ログ ファイルのコンテンツは、常に、これら 2 つのタイムスタンプの間のもので、連続するタイムスタンプが重複しているようであっても、ログ ファイルには重複するエントリはありません。

取り込み間隔

ログ ファイルは、1 日の所定時刻を基準として特定の間隔で取り込まれます。下記の 2 つのオプションによって、ログ ファイルが取り込まれる時点が管理されます：

- ◆ オフセット時刻 – これは 0 時（真夜中）から 23 時までのいずれかの正時です。
- ◆ 取り込み間隔

オフセット時刻と取り込み間隔の両方によって、ログ ファイルの取り込みが始まる時点が決まります。取り込みは、取り込み間隔毎およびオフセット時刻に行われます。

例えば、取り込み間隔が 6 時間で、オフセット時刻が 0（真夜中）であると、ログ記録の取り込みは、毎日、真夜中 (00:00)、06:00、12:00、および 18:00 に行われます。取り込み間隔が 12 時間で、オフセット時刻が 3 であると、ログ記録の取り込みは、毎日、03:00 および 15:00 に行われます。

ログ ファイル取り込みオプションの設定

1. [Configure] > [Subsystems] > [Logging] > [General] へ移ります。.
2. [Log Rolling (ログ取り込み)] セクションで [Log Rolling] オプションが有効になっていることを確かめます (デフォルトは有効です)。
3. [Offset Hour (オフセット時刻)] フィールドで、毎日、ログ ファイル取り込みが行われるべき時刻を入力します。Content Gateway は、毎日、オフセット時刻にログ ファイルの取り込みを行わせませす。
0 (真夜中) から 23 までの任意の正時を入力できます。
4. [Interval (間隔)] フィールドで、次の取り込みまで Content Gateway がログ ファイルにデータを書き込む時間の長さを入力します。
最小値は 300 秒 (5 分) です。最大値は 86400 秒 (1 日) です。



ご注意

次の取り込み時刻の数分以内に Content Gateway を起動すると、ログ ファイル取り込みはその次の取り込み時刻からになるでしょう。

5. [Auto-Delete Rolled Files (取り込みファイルの自動削除)] オプションが有効であることを確かめてください (デフォルトは有効です)。これにより、ログ ディレクトリで利用できるスペースが少なくなると、取り込みログ ファイルが自動的に削除されます。
ログ ディレクトリで利用できる空きスペースがヘッドルーム未満になると、自動削除がトリガされます。
6. [Apply] をクリックします。



ご注意

logs.xml.config ファイルの LogObject 定義でカスタム ログ ファイルの取り込み設定を微調整することができます。カスタム ログ ファイルはその LogObject を取り込み設定として使用しますが、これは Content Gateway Manager または前述の records.config ファイルで指定されているデフォルト設定よりも優先します。

イベント ログ ファイルの分割

デフォルトで、Websense Content Gateway は標準ログ フォーマットを使用し、同じファイルに HTTP および FTP トランザクションを含むログ ファイルを生成します。しかし、異なるオリジン サーバーのトランザクションを個別のログ ファイルにログ記録することが望ましい場合、ホスト ログ分割を有効にすることができます。

HTTP ホスト ログ分割

HTTP ホスト ログ分割によって、異なるオリジン サーバーの HTTP および FTP トランザクションを個別のログ ファイルに記録することができます。HTTP ホスト ログ分割が有効であると、Content Gateway は `log_hosts.config` ファイルにリストされている各オリジン サーバーごとに個別のログ ファイルを作成します ([log_hosts.config ファイルの編集](#), 248 ページ を参照してください)。

HTTP ホスト ログ分割が有効であるとき、Content Gateway は HTTP/FTP トランザクションについて、オリジン サーバー別のログ ファイルを作成します。

例えば、`log_hosts.config` ファイルが 2 つのオリジン サーバー - `uni.edu` と `company.com` - を含んでいて、かつ Squid フォーマットが有効であると、Content Gateway は下記のようなログ ファイルを生成します：

ログ ファイルネーム	説明
<code>squid-uni.edu.log</code>	<code>uni.edu</code> のすべての HTTP および FTP トランザクション
<code>squid-company.com.log</code>	<code>company.com</code> のすべての HTTP および FTP トランザクション
<code>squid.log</code>	他のホストのすべての HTTP および FTP トランザクション

Content Gateway では、プロトコルおよびホスト名に基づいてログ ファイルの生成を詳細に管理することを可能にする XML ベースのログ フォーマットを作成することもできます。[カスタム フォーマット](#), 239 ページ を参照してください。

ログ分割オプションの設定

1. **[Configure]** > **[Subsystems]** > **[Logging]** > **[Splitting (分割)]** へ移ります。
2. **[Split Host Logs (ホスト ログの分割)]** オプションを有効にして、`log_hosts.config` ファイルにリストされている各オリジン サーバーのすべての HTTP および FTP トランザクションをそれぞれ個別のログ ファイルに記録します。**[Split Host Logs (ホスト ログの分割)]** オプションを無効にして、`log_hosts.config` ファイルにリストされている各オリジン サーバーのすべての HTTP および FTP トランザクションを同一のログ ファイルに記録します。
3. **[Apply]** をクリックします。

log_hosts.config ファイルの編集

デフォルトの `log_hosts.config` ファイルは `/opt/WCG/config` にあります。異なるオリジン サーバーの HTTP および FTP トランザクションを個別のログ

ファイルに記録するには、`log_hosts.config` ファイルの個別の行で各オリジンサーバーのホスト名前を指定しなければなりません。



ご注意

`log_hosts.config` ファイルでキーワードを指定し、そのキーワードをホスト名に含むオリジンサーバーのすべてのトランザクションを別個のログファイルに記録することができます。例えば、キーワードとして `sports` を指定すると、Content Gateway は `sports.yahoo.com` および `www.foxsports.com` からのすべての HTTP および FTP トランザクションを `squid-sports.log` というログファイルに記録します (Squid フォーマットが有効である場合)。



ご注意

Content Gateway がクラスタ化されていて、ログファイル照合が有効である場合は、クラスタ中のあらゆるノードで同じ `log_hosts.config` ファイルを使用すべきでしょう。

1. `/opt/WCG/config` にある `log_hosts.config` ファイルを開きます。
2. このファイルで、各オリジンサーバーのホスト名前をそれぞれ別個の行に入力します。例：

```
webserver1
webserver2
webserver3
```

3. ファイルを保存して、閉じます。
4. 変更を適用するには、Content Gateway の `bin` ディレクトリ (`/opt/WCG/bin`) から下記のコマンドを実行します：

```
./content_line -x
```

イベント ログ ファイルの照合

ログファイル照合機能を使用して、ログ記録されたすべての情報を一箇所で保存することができます。このことにより、個別のノードとしてではなく、全体としての Content Gateway を分析し、クラスタ中の特定のノードに存在している大容量ディスクを利用することができます。

Content Gateway は、1 つ以上のノードをログ照合サーバにし、他のすべてのノードをログ照合クライアントにして、ログファイルの照合を行います。ノードがイベント ログ エントリのバッファを生成するとき、そのノードは自らが照合サーバーと照合クライアントのどちらであるかについて判断します。照合サーバーノードは、あたかもログ照合が有効になっていないかのように、すべてのログバッファをそのローカルディスクに書き込みます。

照合クライアント ノードは、そのログ バッファをネットワークを介する転送に向けて準備し、それらのバッファをログ照合サーバーに送ります。ログ照合サーバーがログ バッファをクライアントから受け取ると、サーバー ノードはそのバッファをあたかもローカルに生成されたものであるかのように自己のログ ファイルに書き込みます。ログ クライアントがそのログ照合サーバーと通信できない場合、クライアント ノードはそのログ バッファを自己のローカル ディスクで *orphan* (オーファン) ログ ファイルに書き込みます。オーファン ログ ファイルは、手動による照合を必要とします。ログ照合サーバーはスタンドアローンでもよいし、または Content Gateway を作動させているノードの一部であってもかまいません。



ご注意

ログ照合はネットワークのパフォーマンスに影響することがあります。なぜならば、すべてのノードがそれぞれログ データを単一の照合サーバーに転送するので、ネットワーク中の単一のノードに送られるデータの量がそのノードによる迅速なデータ処理能力を上まわり、ボトルネックがネットワークで発生するかもしれないのである。



ご注意

照合ログ ファイルは各エントリのタイムスタンプ情報を含んでいますが、ファイル中のエントリは厳密に時系列順になっているわけではありません。分析する前に照合ログ ファイルをソートすることができます。

照合サーバーにするための Content Gateway の構成

1. [Configure] > [Subsystems] > [Logging] > [Collation (照合)] へ移ります。
2. [Collation Mode (照合モード)] セクションで、[Be A Collation Server (照合サーバーになる)] オプションを有効にします。
3. [Log Collation Port (ログ照合ポート)] フィールドで、照合クライアントとの通信で使用されるポート番号を入力します。デフォルトのポート番号は 8085 です。
4. [Log Collation Secret (ログ照合秘密)] フィールドで、ログ記録データを検証し、恣意的情報の交換を防止するために使用されるパスワードを入力します。



ご注意

すべての照合クライアントは、この同じ秘密を使用しなければなりません。

5. [Apply] をクリックします。

**重要**

照合サーバーと照合クライアントとの接続が確立した後で照合ポートまたは秘密を変更した場合、Content Gateway を再起動しなければなりません。

照合クライアントにするための Content Gateway の構成

1. [Configure] > [Subsystems] > [Logging] > [Collation] へ移ります。
2. [Collation Mode] セクションで、[Be a Collation Client (照合クライアントになる)] オプションを有効にして、Content Gateway ノードを照合クライアントに設定し、アクティブな標準フォーマット ログ エントリ (Squid や Netscape など) をログ照合サーバーに送ります。

**ご注意**

XML ベース フォーマットの ログ エントリを照合サーバーに送るためには、`logs_xml.config` ファイルにログ オブジェクト定義を追加しなければなりません。[カスタム フォーマット](#), [239 ページ](#) を参照してください。

3. [To Collation Server (宛先照合サーバー)] フィールドで、照合サーバーのホスト名を入力します。これは、Content Gateway 照合サーバーまたはスタンドアロン照合サーバーのどちらでもかまいません。
4. [Log Collation Port (ログ照合ポート)] フィールドで、照合サーバーとの通信で使用されるポート番号を入力します。デフォルトのポート番号は 8085 です。
5. [Log Collation Secret (ログ照合秘密)] フィールドで、ログ記録データを検証し、恣意的情報の交換を防止するために使用されるパスワードを入力します。これは、照合サーバーで設定されるのと同じ秘密でなければなりません。
6. 照合ログ ファイルでログ エントリのオリジンを維持する場合は、[Log Collation Host Tagged (照合ホストをタグ付きでログ記録する)] オプションを有効にします。
7. [Log Collation Orphan Space (ログ照合オーファン スペース)] フィールドで、照合クライアントのログ記録ディレクトリでオーファン ログ ファイルを保存するために割り当てるスペースの最大容量 (メガバイト単位) を入力します。(ログ照合サーバーと通信できない場合、オーファン ログ ファイルが作成されます。) デフォルト値は 25 MB です。

8. [Apply] をクリックします。



重要

照合サーバーと照合クライアントとの接続が確立した後で照合ポートまたは秘密を変更した場合、Content Gateway を再起動しなければなりません。

スタンドアロン照合サーバー

ログ照合サーバーを Content Gateway ノードにしたいくない場合は、ログ ファイルの収集、処理、および書き込みにほぼ集中するスタンドアロン照合サーバー (SAC) をインストールおよび構成することができます。



ご注意

スタンドアロン照合サーバーを利用できるのは、現在、Linux プラットフォームだけです。

1. Content Gateway ノードをログ照合クライアントとして構成します。[照合クライアントにするための Content Gateway の構成, 251 ページ](#) を参照してください。
2. **sac** バイナリを Content Gateway の **bin** ディレクトリ (`/opt/WCG/bin`) からスタンドアロン照合サーバーになるコンピュータにコピーします。
3. **sac** バイナリを保持するディレクトリ中に **config** というディレクトリを作成します。
4. **Step 3** 作成した **config** ディレクトリ中に **internal** というディレクトリを作成します。このディレクトリは、スタンドアロン照合サーバーによってロック ファイルを保存するために内部的に使用されます。
5. ログ照合クライアントとして構成されている Content Gateway ノードから **records.config** ファイル (`/opt/WCG/config`) を **Step 3** スタンドアロン照合サーバー上で作成されている **config** ディレクトリにコピーします。
records.config ファイルは、照合クライアントになるノードの構成時に指定されたログ照合秘密およびポートを含んでいます。照合ポートおよび秘密はすべての照合クライアントおよびサーバーで同一でなければなりません。

6. スタンドアロン照合サーバー上で **records.config** ファイルを開き、下記の変数を編集します：

変数	説明
<code>proxy.config.log2.logfile_dir</code>	<p>ログ ファイルを保存すべきディレクトリを指定します。このディレクトリへの絶対パスをしてもよいし、または sac バイナリが実行されるディレクトリとの相対パスでもかまいません。</p> <p>注意：このディレクトリは、スタンドアロン照合サーバーになるコンピュータ上ですでに存在していなければなりません。</p>

7. ファイルを保存して、閉じます。
8. 次のコマンドを入力します：

```
sac -c config
```

ログ記録統計情報の表示

Content Gateway は、下記のような情報の確認を支援するログ記録システム統計情報を生成します：

- ◆ 現在、書き込まれているログ ファイル（フォーマット）の数。
- ◆ すべてのイベントおよびエラー ログを保持するログ記録ディレクトリによって使用されている現在のスペースの容量。
- ◆ Content Gateway インストール以降、ログ ファイルに書き込まれたアクセス イベントの数。このカウンタは 1 つのファイルで 1 つのエントリになります。複数のフォーマットが書き込まれると、単一のイベントによって複数のイベント ログ エントリが作成されます。
- ◆ Content Gateway インストール以降、フィルタリングによって撥ねられたためにスキップされたアクセス イベントの数。
- ◆ Content Gateway インストール以降、イベント エラー ログに書き込まれたアクセス イベントの数。

Content Gateway Manager の [Monitor (モニタ)] タブからこの統計情報を表示でき、またコマンドライン インターフェースによりこの統計情報を取得することもできます。[トラフィックのモニタリング, 121 ページ](#) を参照してください。

ログ ファイルの表示

関連項目：

- ◆ [Squid フォーマット, 256 ページ](#)
- ◆ [Netscape の例, 257 ページ](#)

Content Gateway が作成するシステム、イベント、およびエラーのログ ファイルを Content Gateway Manager で表示することができます。ログ ファイルの全体、ログ ファイル末尾の指定行数、または指定文字列を含むすべての行を表示することができます。

またログ ファイルを削除したり、それをローカル システムへコピーすることもできます。



ご注意

ログ ファイルのコピーと削除には、正しいユーザー許可が必要です。



ご注意

Content Gateway はログ ファイルの最初の 1 MB だけを表示します。1 MB を超えるログ ファイルが選択されると、Content Gateway はファイルを切り詰め、ファイルが大きすぎるという警告メッセージを表示します。

Content Gateway Manager によりログ ファイルにアクセスできるようになりました。

1. **[Configure]** > **[My Proxy (マイ プロキシ)]** > **[Logs]** > **[System]** に移ります。
2. システム ログ ファイルを表示、コピー、または削除する場合は、[Step 3](#) へ進みます。

イベントまたはエラー ログ ファイルを表示、コピー、または削除するには、**[Access (アクセス)]** タブを選択します。

3. **[Log File]** ドロップダウン リストで、表示、コピー、または削除するログ ファイルを選択します。

Content Gateway は、システム全体のログ記録機能である **syslog** がデーモン機能のもとで記録したシステム ログ ファイル をリストアップします。

Content Gateway はイベント ログ ファイルをリストアップしますが、これらのファイルは **[Configure]** > **[Subsystems]** > **[Logging]** > **[General]** タブの **[Logging Directory]** フィールドで指定されているか、または **records.config** ファイルの **proxy.config.log2.logfile_dir** 構成変数によって指定

されているディレクトリに保存されています。デフォルトのディレクトリは、Content Gateway インストール ディレクトリの `logs` です。

4. **[Action (アクション)]** エリアで、下記のオプションのどれかを選択します：
 - **Display the selected log file (選択ログ ファイルの表示)** – ログ ファイル全体を表示します。ファイルが 1 MB 超であると、最初の 1MB のデータだけが表示されます。
 - **Display last lines of the selected file (選択ファイルの末尾部分の表示)** – ログ ファイルの末尾部分を表示します。表示させる行数を用意されているフィールドで指定します。
 - **Display lines that match in the selected log file (選択ログ ファイル中の一致する行の表示)** – ログ ファイル中で特定の文字列と一致する行を表示します。文字列を用意されているフィールドで入力します。
 - **Remove the selected log file (選択ログ ファイルの削除)** – 選択されているログ ファイルを Content Gateway システムから削除します。
 - **Save the selected log file in local filesystem (選択ログ ファイルをローカル ファイルシステムへ保存)** – 選択されているログ ファイルのコピーをローカル システム上で保存します。
5. **[Apply]** をクリックします。

ログ ファイルの表示を選択していると、Content Gateway はファイルをページの最後で表示します。

ログ ファイルの削除を選択していると、Content Gateway はファイルを削除します。削除の確認は求められません。

ログ ファイルの保存を選択していると、ローカル システム上でファイルを保存すべき場所の指定を求められます。

イベント ログ ファイル エントリの例

このセクションでは、Content Gateway でサポートされている各標準ログフォーマットのログ ファイル エントリの例を紹介します：

- ◆ [Squid フォーマット, 256 ページ](#)
- ◆ [Netscape の例, 257 ページ](#)
- ◆ [Netscape Extended フォーマット, 257 ページ](#)
- ◆ [Netscape Extended-2 フォーマット, 257 ページ](#)

Squid フォーマット

次の図は、**squid.log** ファイルのログ エントリのサンプルを示しています。下記の表では、各フィールドについて説明しています。

```

1      2      3      4      5      6      7
987548934.123 19 209.131.54.138 TCP_HIT/200 4771 GET http://europe.cnn.com/
EUROPE/potd/2001/04/17/tz.pullitzer.ap.jpg - NONE/- image/jpeg
7 cont'd      8      9      10

```

フィールド	説明
1	Squid フォーマットのクライアント要求タイムスタンプ; 1970 年 1 月 1 日 (UTC) からの秒数で示されるクライアント要求の時刻 (精度: ミリ秒)。
2	プロキシがクライアントの要求の処理で費やした時間; クライアントがプロキシとの接続を確立した時点からプロキシがその応答の最後のバイトをクライアントに送り返した時点までのミリ秒数。
3	クライアントのホスト コンピュータの IP アドレス。
4	キャッシュ戻り値; 要求に対するキャッシュの応答を示します: HIT (ヒット)、MISS (ミス)、等々。Cache 戻り値については、 Squid 形式および Netscape 形式のログ ファイルのキャッシュ戻り値は何を意味しますか , 484 ページで説明しています。 プロキシ ステータス コード (Content Gateway からクライアントへの HTTP 応答ステータス コード)。
5	クライアントに対する Content Gateway の応答の長さ (バイト数) で、これはヘッダとコンテンツを含みます。
6	クライアント要求方式: GET、POST、等々。
7	クライアント要求の標準 URL; ログ分析ツールで解析できないブランクやその他の特殊文字はエスケープ シーケンスによって置き換えられます。エスケープ シーケンスは、パーセント記号とそれに後続する置換された文字の ASCII コード番号 (16 進表記) です。
8	認証されたクライアントのユーザー名。ハイフン (-) は、認証が不要であったことを示しています。
9	プロキシ階層ルート; Content Gateway がオブジェクトの取得のために使用したルート。プロキシ要求サーバー名; 要求を実現したサーバーの名前。要求がキャッシュ ヒットであった場合、このフィールドにはハイフン (-) があります。
10	プロキシ応答のコンテンツ タイプ; Content Gateway 応答 ヘッダから取られたオブジェクト コンテンツ タイプ。

Netscape の例

Netscape Common フォーマット

次の図は、**common.log** ファイルのログ エントリのサンプルを示しています。表では、各フィールドについて説明しています。

```

1      2 3      4      5
209.131.54.138 - - [17/Apr/2001:16:20:28 -0700] "GET http://europe.cnn.com/
EUROPE/potd/2001/04/17/tz.pullitzer.ap.jpg HTTP/1.0" 200 4473
                    5 cont'd                      6 7
  
```

Netscape Extended フォーマット

次の図は、**extended.log** ファイルのログ エントリのサンプルを示しています。表では、各フィールドについて説明しています。

```

1      2 3      4      5
209.131.54.138 - - [17/Apr/2001:16:20:28 -0700] "GET http://europe.cnn.com/EUROPE/potd/2001/
04/17/tz.pullitzer.ap.jpg HTTP/1.0" 200 4473 000 0 0 0 458 297 0 0 0
                    5 cont'd                      6 7 8 9 10 11 12 13 14 15 16
  
```

Netscape Extended-2 フォーマット

次の図は、**extended2.log** ファイルのログ エントリのサンプルを示しています。表では、各フィールドについて説明しています。

```

1      2 3      4      5
209.131.54.138 - - [17/Apr/2001:16:20:28 -0700] "GET http://europe.cnn.com/EUROPE/potd/2001/04/
17/tz.pullitzer.ap.jpg HTTP/1.0" 200 4473 000 0 0 0 458 297 0 0 0 NONE FIN FIN TCP_MEM
                    5 cont'd                      6 7 8 9 10 11 12 13 14 15 16 17 18 19 20
  
```

フィールド	説明
Netscape Common	
1	クライアントのホスト コンピュータの IP アドレス。
2	Netscape ログ エントリでは、このハイフン (-) は常に存在します。
3	認証されたクライアントのユーザー名。ハイフン (-) は、認証が不要であったことを示しています。
4	クライアントの要求の日付と時刻 - 括弧で囲まれています。
5	要求行 - 引用符で囲まれています。

フィールド	説明
6	プロキシ応答ステータス コード (HTTP 応答コード)。
7	クライアントに対する Content Gateway 応答の長さ (バイト数)。
	Netscape Extended
8	オリジン サーバーの応答ステータス コード。
9	サーバー応答転送の長さ; プロキシに対するオリジン サーバー応答本文の長さ (バイト数)。
10	クライアント要求転送の長さ; プロキシに対するクライアントの要求本文の長さ (バイト数)。
11	プロキシ要求転送の長さ; オリジン サーバーに対するプロキシ要求本文の長さ。
12	クライアント要求ヘッダの長さ; プロキシに対するクライアントの要求ヘッダの長さ。
13	プロキシ応答ヘッダの長さ; クライアントに対するプロキシ応答ヘッダの長さ。
14	プロキシ要求ヘッダの長さ; オリジン サーバーに対するプロキシ要求ヘッダの長さ。
15	サーバー応答ヘッダの長さ; プロキシに対するオリジン サーバー応答ヘッダの長さ。
16	Content Gateway がクライアントの要求の処理で費やした時間; クライアントがプロキシとの接続を確立した時点からプロキシがその応答の最後のバイトをクライアントに送り返した時点までの秒数。
	Netscape Extended-2
17	プロキシ階層ルート; Content Gateway がオブジェクトの取得のために使用したルート。
18	クライアント終了ステータス コード: FIN (クライアント要求が正常に完了した場合) または INTR (クライアント要求が中断された場合)。
19	プロキシ終了ステータス コード: FIN (オリジン サーバーに対する Content Gateway 要求が正常に完了した場合) または INTR (その要求が中断された場合)。
20	キャッシュ戻り値; 要求に対する Content Gateway キャッシュの応答: HIT (ヒット)、MISS (ミス)、等々。Cache 戻り値については、 Squid 形式および Netscape 形式のログ ファイルのキャッシュ戻り値は何を意味しますか, 484 ページ で説明しています。

A

統計

本付録では、Content Gateway Manager の Monitor タブの下記の統計について説明しています。

- ◆ [My Proxy \(マイ プロキシ\)](#), 259 ページ
- ◆ [Protocols \(プロトコル\)](#), 263 ページ
- ◆ [Security \(セキュリティ\)](#), 266 ページ
- ◆ [Subsystems \(サブシステム\)](#), 270 ページ
- ◆ [Networking \(ネットワーク\)](#), 272 ページ
- ◆ [Performance \(パフォーマンス\)](#), 277 ページ
- ◆ [SSL Key Data \(SSL キー データ\)](#), 280 ページ

My Proxy (マイ プロキシ)

My Proxy 統計は次のカテゴリに分けられます。

- ◆ [Summary \(要約\)](#), 259 ページ
- ◆ [Node \(ノード\)](#), 261 ページ
- ◆ [Graphs \(グラフ\)](#), 262 ページ
- ◆ [Alarms \(アラーム\)](#), 262 ページ

Summary (要約)

統計 / フィールド	説明
	Subscription Details (サブスクリプション詳細)
Feature (機能)	SSL Manager、スキャン オプションなどの購入された機能が表示します。SSL Manager およびスキャン オプションによるコンテンツの分析についての詳細は、TRITON - Web Security オンライン ヘルプの 暗号化データの使用 , 145 ページを参照してください。

統計 / フィールド	説明
Purchased Status (購入ステータス)	機能が購入されたかどうかを示します。
Expiration Date (有効期限)	機能が購入されている場合、サブスクリプションの有効期限を表示します。
	More Detail (より詳細)
Subscription key (サブスクリプションキー)	サブスクリプション キーを表示します。 サブスクリプション キーの入力, 15 ページ を参照してください。
Last successful subscription download time (最終サブスクリプションダウンロード成功時間)	サブスクリプション キーの最終確認時間を表示します。このチェックは 1 日に 1 回行われます。
Connection status (接続ステータス)	Content Gateway の Policy Server、Policy Broker、および Filtering Service への接続状態を表示します。
Registration status (登録ステータス)	Forensics Repository の Content Gateway 登録ステータスを表示します。
	Scanning Data Files (スキャンニング データ ファイル)
Engine Name (エンジン名)	各スキャンニング エンジン名を表示します。
Engine Version (エンジンバージョン)	スキャンニング エンジンのバージョン番号を表示します。
Data File Version (データファイルバージョン)	スキャンニング エンジンで現在使用されているデータ ファイルのバージョン番号を表示します。
Content Classification Analytics library version (Content Classification Analytic ライブラリバージョン)	Content Classification Analytic ライブラリのバージョン番号を表示します。
Last update (最終更新)	Content Gateway が、分析データ ファイル、設定、およびポリシーを最後にロードした日時を表示します。
Last time Content Gateway loaded data (Content Gateway 最終データ ロード時間)	Content Gateway が、分析データファイル、設定、およびポリシーを最後にロードした日時を表示します。
Last time Content Gateway checked for updates (Content Gateway 最終更新確認時間)	Content Gateway が、データ ファイルの更新を確認するために、Websense ダウンロード サーバーと最後に通信した日時を表示します。
	Node Details (ノード詳細)
Node (ノード)	Content Gateway ノードまたはクラスタ名
On/Off (オン / オフ)	プロキシ (プロキシおよびマネージャー サービス) が実行中かどうかを示します。
Objects Served (処理されたオブジェクト)	Content Gateway ノードによって処理されたオブジェクトの合計 総数。

統計 / フィールド	説明
Ops/Sec (処理数 / 秒)	Content Gateway ノードによって処理された 1 秒あたりの処理数。
Hit Rate (ヒット率)	キャッシュから処理された HTTP 要求パーセンテージ (過去 10 秒間の平均)。
Throughput (Mbit/sec) (スループット)	Content Gateway ノード (およびクラスタ) を通過した数 (Mbit/sec)。
HTTP Hit (ms) (HTTP ヒット)	キャッシュ内に最新のものが存在する HTTP オブジェクトをクライアントに出力するために要した時間。
HTTP Miss (ms) (HTTP ミス)	キャッシュ内に存在しないまたは陳腐化した HTTP オブジェクトをクライアントに出力するために要した時間。
SSL Manager Configuration Server	クラスタ内に複数の Content Gateway ノードが配備され、SSL 管理クラスタ化が有効な場合に、このフィールドは SSL Manager Configuration Server の IP アドレスを表示します。アドレスがリンクの場合、現在のシステムはサーバー ではない ことを示しています。SSL Manager Configuration Server にログオンするには、リンクをクリックします。
More Detail (より詳細)	
cache hit rate (キャッシュ ヒット率)	キャッシュから処理された HTTP 要求パーセンテージ (過去 10 秒間の平均)。この値は 10 秒毎に更新されます。
errors (エラー率)	障害により終了した要求のパーセンテージ。
aborts (中断率)	中断され要求のパーセンテージ。
active clients (アクティブなクライアント)	クライアント接続の現在のオープン数。
active servers (アクティブなサーバー)	オリジン サーバー接続の現在のオープン数。
node IP address (ノード IP アドレス)	ノードに割り当てられた IP アドレス。仮想 IP アドレス指定が有効化されている場合、複数の仮想 IP アドレスをこのノードに割り当てることができます。
cache free space (キャッシュ空容量)	キャッシュの空き容量。
HostDB hit rate (HostDB ヒット率)	Host データベース ルックアップの合計に対する Host データベース ヒットの比率 (10 秒間の平均)。

Node (ノード)

統計	説明
Node Summary (ノード要約)	
Status (ステータス)	Content Gateway がこのノード上で実行しているかを示します (active または inactive)。
Up Since (起動日時)	Content Gateway が起動した日時。

統計	説明
Clustering (クラスタ化)	このノード上でのクラスタ化のオン / オフ状態を示します。
Cache (キャッシュ)	
Document Hit Rate (ドキュメント ヒット率)	全キャッシュ要求に対するキャッシュ ヒットの割合 (10 秒間の平均値)。This value is refreshed every 10 seconds.
Bandwidth Savings (帯域幅の節約)	全要求バイトに対するキャッシュから提供されたバイト数の割合 (10 秒間の平均値)。
Cache Percent Free (キャッシュの空き容量の割合)	全キャッシュ容量に対するキャッシュ空き容量の割合。
In Progress (処理中)	
Open Server Connections (サーバー接続のオープン数)	オリジン サーバー接続の現在のオープン数。
Open Client Connections (クライアント接続のオープン数)	クライアント接続の現在のオープン数。
Cache Transfers in Progress (処理中のキャッシュ転送)	処理中のキャッシュ転送 (キャッシュ読み込み / 書き込み) 数。
Network (ネットワーク)	
Client Throughput (Mbit/Sec) (クライアントスループット)	ノード (およびクラスタ) の通過量 (Mbit/sec)。
Transactions per Second (秒当たりのトランザクション)	秒当たりの HTTP トランザクション数。
Name Resolution (名前解決)	
Host Database Hit Rate (ホストデータベースのヒット率)	ホスト データベース ルックアップの合計に対するホスト データベース ヒットの割合 (10 秒間の平均値)。This value is refreshed every 10 seconds.
DNS Lookups per Second (秒当たりの DNS ルックアップ)	秒当たりの DNS ルックアップ数。

Graphs (グラフ)

グラフページには、[Node \(ノード\)](#) ページと同じ統計 (キャッシュ パフォーマンス、現在の接続と転送量、ネットワーク、およびネーム レゾリューション) がグラフィック形式で表示されます。グラフに表示する統計を選択することができます。[統計の表示, 121 ページ](#) を参照してください。

Alarms (アラーム)

Websense Content Gateway が問題 (たとえば、イベント ログに割り当てられた容量が満杯の場合や、Content Gateway が設定ファイルに書き込めない場合) を検出した時、アラームを発生させ、アラーム メッセージ ウィンドウに

アラームの説明を表示します。さらに、Content Gateway Manager 上部の **Alarm! [pending]** バーに、アラームがいつ検出されたか、存在するアラームの数を表示します。

アラームメッセージを読んだ後、アラームメッセージ ウィンドウ内の **[Clear (クリア)]** をクリックすると、アラームは削除されます。**[Clear (クリア)]** をクリックすると、アラームメッセージは削除されますが、実際にアラームの問題が解決されるわけではありません。

アラームに関する情報は、[アラームの処理, 125 ページ](#)を参照してください。

Protocols (プロトコル)

プロトコル 統計は次のカテゴリに分けられます。

- ◆ [HTTP, 263 ページ](#)
- ◆ [FTP, 265 ページ](#)

HTTP

統計	説明
	General (一般)
Client (クライアント)	
Total Document Bytes (ドキュメントの合計バイト)	インストール以降クライアントに提供された HTTP データの合計数。
Total Header Bytes (ヘッダーの合計バイト)	インストール以降クライアントに提供された HTTP ヘッダーの合計数。
Total Connections (接続の合計)	インストール以降の HTTP クライアント接続の合計数。
Current Connections (現在の接続)	HTTP クライアント接続の現在の数。
Transactions in Progress (処理中のトランザクション)	処理中の HTTP クライアント トランザクションの数。
Server (サーバー)	
Total Document Bytes (ドキュメントの合計バイト)	インストール以降のオリジン サーバーから受信した HTTP データの合計数。
Total Header Bytes (ヘッダー の合計バイト)	インストール以降のオリジン サーバーから受信した HTTP ヘッダー データの合計数。
Total Connections (接続の合計)	インストール以降の HTTP サーバー接続の合計数。

統計	説明
Current Connections (現在の接続)	HTTP サーバー接続の現在の数。
Transactions in Progress (処理中のトランザクション)	処理中の HTTP サーバー接続の合計数。
	Transaction (トランザクション)
Hits (ヒット数)	
Fresh (最新性)	最新性ヒットのパーセンテージと平均処理時間。
Stale Revalidated (再確認され陳腐化)	陳腐化し、再確認され、最新となり、提供されているヒットのパーセンテージと平均処理時間。
Misses (ミス数)	
Now Cached (現在キャッシュ)	キャッシュ内に存在しなかった(現在は存在)ドキュメント要求のパーセンテージとその平均処理時間。
Server No Cache (サーバー キャッシュなし)	キャッシュ内に存在しないが、サーバーの no-cache ヘッダー(キャッシュ不可)を含む HTTP オブジェクト要求のパーセンテージとその平均処理時間。
Stale Reloaded (再ロードされ陳腐化)	再確認され、変更され、再ロードされて処理されたミスのパーセンテージとその平均処理時間。
Client No Cache (クライアントキャッシュなし)	クライアント no-cache ヘッダーを含むミスのパーセンテージとその平均処理時間。
Errors (エラー)	
Connection Failures (接続エラー)	接続エラーのパーセンテージとその平均処理時間。
Other Errors (その他のエラー)	その他のエラーのパーセンテージとその平均処理時間。
Aborted Transactions (トランザクション中断)	
Client Aborts (クライアントによる中断)	クライアントによる中断処理のパーセンテージとその平均処理時間。
Questionable Client Aborts (クライアントによると思われる中断)	クライアントが中断した可能性がある処理のパーセンテージとその平均処理時間。
Partial Request Hangups (部分要求ハングアップ)	部分要求後の初期ハングアップのパーセンテージとその平均処理時間。
Pre-Request Hangups (要求前ハングアップ)	Pre-Request ハングアップのパーセンテージとその平均処理時間。
Pre-Connect Hangups (接続前ハングアップ)	Pre-Connect ハングアップのパーセンテージとその平均処理時間。

統計	説明
Other Transactions (その他のトランザクション)	
Unclassified (未分類)	未分類処理のパーセンテージとその平均処理時間。
	FTP over HTTP
Connections (接続)	
Open Server Connections (サーバー接続のオープン数)	FTP サーバー接続をオープンした回数。
Successful PASV Connections (PASV 接続の成功数)	インストール以降 PASV 接続に成功した回数。
Failed PASV Connections (PASV 接続の失敗数)	インストール以降 PASV 接続に失敗した回数。
Successful PORT Connections (PORT 接続の成功数)	インストール以降 PORT 接続に成功した回数。
Failed PORT Connections (PORT 接続の失敗数)	インストール以降 PORT 接続に失敗した回数。
Cache Statistics (キャッシュ統計)	
Hits (ヒット数)	キャッシュから提供された FTP オブジェクトの HTTP 要求数。
Misses (ミス数)	オブジェクトがキャッシュ内に存在しないか無効のために、オリジン サーバーに直接転送された FTP オブジェクトの HTTP 要求の数。
Lookups (ルックアップ)	Content Gateway が、キャッシュ内の FTP オブジェクトの HTTP 要求をルックアップした回数。

FTP

統計	説明
	Client (クライアント)
Open Connections (接続オープン数)	現在オープンされているクライアント接続の数。
Bytes Read (読み込みバイト数)	インストール以降、読み込まれたクライアント要求のバイト数。
Bytes Written (書き込みバイト数)	インストール以降、書き込まれたクライアント要求のバイト数。
	Server (サーバー)
Open Connections (接続オープン数)	現在オープンされている FTP サーバー接続の数。

統計	説明
Bytes Read (読み込みバイト数)	インストール以降、FTP サーバーから読み込まれたバイト数。
Bytes Written (書き込みバイト数)	インストール以降、キャッシュに書き込まれたバイト数。

Security (セキュリティ)

セキュリティ 統計は次のカテゴリに分けられます。

- ◆ [Integrated Windows Authentication \(統合 Windows 認証\), 266 ページ](#)
- ◆ [LDAP, 268 ページ](#)
- ◆ [Legacy NTLM \(レガシー NTLM\), 268 ページ](#)
- ◆ [SOCKS, 269 ページ](#)
- ◆ [Data Security, 269 ページ](#)



ご注意

複数の認証ルールを使用している場合でも、Content Gateway は、各認証方法 (IWA、LDAP、Legacy NTLM) の認証統計を個別にレポートします。

Integrated Windows Authentication (統合 Windows 認証)

統計	説明
	Diagnostic Test (診断テスト) この機能は、選択されたドメインに対してケルベロス接続を行う場合に診断テストを実行します。結果は、画面上と /opt/WCG/logs/content_gateway.out および /opt/WCG/logs/smbadmin.log に書き込まれます。
Domain ドロップダウン ボックス	接続されているドメインを選択します。複数レールの認証が設定されていない限り、接続されているドメインは1つのみです。
Run Test ボタン	クリックするとテストを開始します。
	Kerberos request counters (Kerberos 要求カウンタ)
Total Kerberos requests (Kerberos 要求の合計数)	Kerberos 認証要求の合計数。
Authentication succeeded (認証成功数)	認証に成功した Kerberos 認証要求の数。

統計	説明
Authentication failed (認証失敗数)	認証に失敗した Kerberos 認証要求の数。
Kerberos errors (Kerberos エラー数)	Kerberos プロセス エラーの数。
NTLM request counters (NTLM 要求カウンタ)	
Total NTLM requests (NTLM 要求の合計数)	NTLM 認証要求の合計数。
Authentication succeeded (認証成功数)	認証に成功した NTLM 認証要求の数。
Authentication failed (認証失敗数)	認証に失敗した NTLM 認証要求の数。
NTLM request errors (NTLM 要求エラーの数)	NTLM プロセス エラーの数。
NTLM within negotiate requests (ネゴシエーション要求内の NTLM 要求)	ネゴシエーション要求内にカプセル化された NTLM 要求の数。
Basic authentication request counters (Basic 認証要求カウンタ)	
Total basic authentication requests (Basic 認証要求の合計数)	Basic 認証要求の合計数。
Authentication succeeded (認証成功数)	認証に成功した Basic 認証要求の数。
Authentication failed (認証失敗数)	認証に失敗した Basic 認証要求の数。
Basic authentication request errors (Basic 認証要求エラー)	Basic 認証処理エラーの数。
Performance counters (パフォーマンス カウンタ)	
Kerberos - Average time per transaction (Kerberos トランザクション平均 時間)	Kerberos トランザクションを完了するまでの平均 時間(単位ミリ秒)。
NTLM - Average time per transaction (NTLM トランザクション平均時 間)	NTLM トランザクションを完了するまでの平均 時間(ミリ秒単位)。
Basic - Average time per transaction (Basic トランザクション平均時 間)	Basic トランザクションを完了するまでの平均 時間(ミリ秒単位)。
Average helper latency per transaction (ヘルパー遅延トランザクシ ョン平均時間)	Samba の認証要求を処理する平均時間。

統計	説明
Time authentication spent offline (認証オフライン時間)	サービスまたは接続性の障害のために、Content Gateway が NTLM 認証を実行できなかった時間(秒単位)。(DC と通信する必要がないため、この測定は Kerberos に適用されません。) Global Fail Open オプションが有効な場合、プロキシ要求は認証なしに続行されます。 障害の後、接続が再確立した時に、カウンタは増加します。
Number of times authentication servers or services went offline (認証サーバーまたはサービスがオフラインになった回数)	認証サーバーまたはサービスとの接続性が失われた回数。

LDAP

統計	説明
	Cache (キャッシュ)
Hits (ヒット数)	LDAP キャッシュのヒット回数。
Misses (ミス数)	LDAP キャッシュのミス回数。
	Errors (エラー)
Server (サーバー)	LDAP サーバーエラーの回数。
	Unsuccessful Authentications (認証失敗回数)
Authorization Denied (認証拒否回数)	LDAP サーバーが認証を拒否した回数。
Authorization Timeouts (認証タイムアウト回数)	認証がタイムアウトになった回数。
Authentication Cancelled (認証キャンセル回数)	LDAP 認証を開始し完了する前に、終了してしまった回数。 ご注意: クライアントが資格情報を要求するダイアログボックス内の "Cancel" クリックして、認証をキャンセルした場合はカウントされません。

Legacy NTLM (レガシー NTLM)

統計	説明
	Cache (キャッシュ)
Hits (ヒット数)	NTLM キャッシュのヒット回数。
Misses (ミス数)	NTLM キャッシュのミス回数。

統計	説明
	Errors (エラー)
Server (サーバー)	NTLM サーバーエラーの回数。
	Unsuccessful Authentications (認証失敗回数)
Authorization Denied (認証拒否回数)	NTLM サーバーが認証を拒否した回数。
Authentication Cancelled (認証キャンセル回数)	認証がキャンセルされた回数。
Authentication Rejected (認証リジェクト回数)	キューが満杯のために認証が失敗した回数。
	Queue Size (キュー サイズ)
Authentication Queued (キューに入っている認証数)	すべてのドメイン コントローラがビジーのため、現在キューに入れられている要求の数。

SOCKS

統計	説明
On-Appliance SOCKS Server (V シリーズ アプライアンス上に Content Gateway が存在する場合)	アプライアンス上の SOCKS サーバーがオン(有効)かオフ(無効)かを示します。
Unsuccessful Connections (接続失敗回数)	Content Gateway を起動して以降、SOCKS サーバーとの接続に失敗した回数。
Successful Connections (接続成功回数)	Content Gateway を起動して以降、SOCKS サーバーとの接続に成功した回数。
Connections in Progress (現在の接続数)	現在の SOCKS サーバー接続の数。

Data Security

統計	説明
Total Posts (転送の合計数)	Data Security への転送の合計数。
Total Analyzed (分析の合計数)	Data Security で分析した転送の合計数。
FTP Analyzed (FTP 分析の合計数)	Data Security で分析した FTP 要求の合計数。
Blocked Requests (ブロックされた要求数)	分析およびポリシーの実施後に、ブロックされた要求の合計数。
Allowed Requests (許可された要求数)	分析およびポリシーの実施後に、許可された要求の合計数。

統計	説明
Failed Requests (失敗した要求数)	Data Security へ送信され、タイムアウトまたはその他の原因で完了しなかった転送の合計数。
Huge Requests (超過要求数)	最大 トランザクション サイズを超過した要求の合計数。
Tiny Requests (不足要求数)	最小トランザクション サイズより小さい要求の合計数。
Decrypted Requests (復号化要求数)	復号化され、Data Security に送信された SSL 要求の合計数。
Total Bytes Scanned (スキャン合計バイト数)	Data Security でスキャンされた合計バイト数。
Average Response Time (平均応答時間)	Content Gateway が最後に起動して以降の、Data Security がスキャンを完了するまでに必要とした平均時間。

Subsystems (サブシステム)

サブシステム統計は次のカテゴリに分けられます。

- ◆ [Cache \(キャッシュ\), 270 ページ](#)
- ◆ [Clustering \(クラスタ化\), 272 ページ](#)
- ◆ [Logging \(ログ記録\), 272 ページ](#)

Cache (キャッシュ)



ご注意

Content Gateway に送信されたすべてのコンテンツがキャッシュ不可の場合でも、キャッシュ統計はゼロではない場合があります。クライアントが no-cache ヘッダーを送信した場合でも、Content Gateway はキャッシュ読み込みを実行します。

統計	説明
	General (一般)
Bytes Used (使用バイト数)	現在キャッシュに使用されているバイト数。
Cache Size (キャッシュ サイズ)	キャッシュに割り当てられているバイト数。

統計	説明
	Ram Cache (RAM キャッシュ)
Bytes (バイト数)	RAM キャッシュの合計サイズ(バイト単位)。
Hits (ヒット数)	RAM キャッシュにヒットしたドキュメント数。
Misses (ミス数)	RAM キャッシュにヒットしなかったドキュメント数。ドキュメントはキャッシュ ディスクにヒットすることがあります。
	Reads (読み込み)
In Progress (処理中)	現在読み込み中のキャッシュの数(HTTP および FTP)。
Hits (ヒット数)	Content Gateway が起動して以降、キャッシュ読み込みを完了した回数(HTTP および FTP)。
Misses (ミス数)	Content Gateway が起動して以降、キャッシュ読み込みをミスした回数(HTTP および FTP)。
	Writes (書き込み)
In Progress (処理中)	現在書き込み中のキャッシュ数(HTTP および FTP)。
Successes (成功回数)	Content Gateway が起動して以降のキャッシュ書き込み成功回数(HTTP および FTP)。
Failures (失敗回数)	Content Gateway が起動して以降のキャッシュ書き込み失敗回数(HTTP および FTP)。
	Updates (更新)
In Progress (処理中)	現在更新中の HTTP ドキュメントの数。Content Gateway がオブジェクトを再確認し、最新であることを検出し、オブジェクト ヘッダーを更新した時に、更新が発生します。
Successes (成功回数)	Content Gateway が起動して以降、HTTP キャッシュ更新に成功した回数。
Failures (失敗回数)	Content Gateway が起動して以降、HTTP キャッシュ更新に失敗した回数。
	Removes (削除)
In Progress (処理中)	現在削除中のドキュメントの数。Content Gateway がドキュメントを再確認し、オリジン サーバー上で削除するドキュメントを発見し、キャッシュ から削除(HTTP および FTP を含む)した時に、削除が発生します。
Successes (成功回数)	Content Gateway が起動して以降、キャッシュの削除に成功した回数。
Failures (失敗回数)	Content Gateway が起動して以降、キャッシュの削除に失敗した回数(HTTP および FTP を含む)。

Clustering (クラスタ化)

統計	説明
Clustering Nodes (クラスタリング ノード数)	クラスタリング ノードの数。

Logging (ログ記録)

統計	説明
Currently Open Log Files (現在オープン中のログ ファイル数)	現在書き込み中の event log ファイル(フォーマット)の数。
Space Used for Log Files (ログ ファイル使用容量)	ログ記録ディレクトリ(すべてのイベント、およびエラー ログを保持)に使用されている現在の容量。
Number of Access Events Logged (アクセス イベントのログ数)	Content Gateway インストール以降、ログ ファイルに書き込まれたアクセス イベントの数。このカウンタは 1つのファイルに 1つのエントリを表します。複数のフォーマットが書き込まれると、単一のイベントによって複数のイベント ログ エントリが作成されます。
Number of Access Events Skipped (アクセス イベントのスキップ数)	Content Gateway インストール以降、(フィルタリングによって撥ねられたために)スキップされたアクセス イベントの数。
Number of Error Events Logged (イベント エラーのログ数)	Content Gateway インストール以降、イベント エラー ログに書き込まれたアクセス イベントの数。

Networking (ネットワーク)

ネットワーク統計は 次のカテゴリに分けられます。

- ◆ [System \(システム\), 273 ページ](#)
- ◆ [ARM, 273 ページ](#)
- ◆ [ICAP, 275 ページ](#)
- ◆ [WCCP, 275 ページ](#)
- ◆ [DNS Resolver \(DNS リゾルバ\), 277 ページ](#)
- ◆ [Virtual IP \(仮想 IP\), 277 ページ](#)

System (システム)

統計 / フィールド	説明
	General (一般)
Hostname (ホスト名)	Content Gateway コンピュータに割り当てられたホスト名。
Search Domain (検索ドメイン)	Content Gateway コンピュータ使用する検索ドメイン。
IPv4 または IPv6	
Default Gateway (デフォルト ゲートウェイ)	Content Gateway コンピュータから、他のネットワークまたはサブネットに、パケット転送を行うために使用するデフォルト ゲートウェイの IP アドレス。
Primary DNS (一次 DNS)	Content Gateway コンピュータが、ホスト名の解決に使用する一次 DNS サーバーの IP アドレス。
Secondary DNS (二次 DNS)	Content Gateway コンピュータが、ホスト名の解決に使用する二次 DNS サーバーの IP アドレス。
Tertiary DNS (三次 DNS)	Content Gateway コンピュータが、ホスト名の解決に使用する三次 DNS サーバーの IP アドレス。
	NIC < インターフェイス名 >
Status (ステータス)	NIC が動作中か停止中かを示します。
Start on Boot (起動時開始)	NIC が起動時に開始するよう設定されているかを示します。
IPv4 または IPv6	
IP address (IP アドレス)	NIC に割り当てられた IP アドレス。
Netmask (ネットマスク)	IP アドレスのネットマスク。
Gateway (ゲートウェイ)	NIC に設定されたデフォルト ゲートウェイの IP アドレス。

ARM

統計	説明
	Network Address Translation (NAT) Statistics (NAT 統計)
Client Connections Natted (変換された接続数)	ARM によって透過的にリダイレクトされたクライアント接続の数。
Client Connections in Progress (処理中の接続数)	ARM によって現在処理中のクライアント接続数。

統計	説明
Total Packets Natted (変換されたパケットの合計数)	ARM によって変換されたパケットの数。
DNS Packets Natted (変換された DNS パケットの合計数)	ARM によって変換された DNS パケットの数。
Bypass Statistics (バイパス統計)	
Total Connections Bypassed (バイパスされた接続の合計数)	ARM によってバイパスされた接続の合計数。
Connections Dynamically Bypassed (動的にバイパスされた接続の合計数)	動的にバイパスされた接続の合計数。 動的バイパスルール, 74 ページ を参照してください。
DNS Packets Bypassed (バイパスされた DNS パケットの合計数)	ARM によってバイパスされた DNS パケットの数。
Connections Shed (破棄された接続の合計数)	破棄された接続の合計数。 接続負荷の軽減, 77 ページ を参照してください。
HTTP Bypass Statistics (HTTP バイパス統計)	
Bypass on Bad Client Request (不正クライアント要求によるバイパス)	Content Gateway がポート 80 上で非 HTTP トラフィックを検出したために、直接オリジンサーバーに転送された要求の数。
Bypass on 400	オリジンサーバーが 400 エラーを返したために、オリジンサーバーに直接転送された要求の数。
Bypass on 401	オリジンサーバーが 401 エラーを返したために、オリジンサーバーに直接転送された要求の数。
Bypass on 403	オリジンサーバーが 403 エラーを返したために、オリジンサーバーに直接転送された要求の数。
Bypass on 405	オリジンサーバーが 405 エラーを返したために、オリジンサーバーに直接転送された要求の数。
Bypass on 406	オリジンサーバーが 406 エラーを返したために、オリジンサーバーに直接転送された要求の数。
Bypass on 408	オリジンサーバーが 408 エラーを返したために、オリジンサーバーに直接転送された要求の数。
Bypass on 500	オリジンサーバーが 500 エラーを返したために、オリジンサーバーに直接転送された要求の数。

ICAP

統計	説明
Total Posts (転送の合計数)	Data Security への転送の合計数。
Total Analyzed (分析の合計数)	Data Security で分析した転送の合計数。
FTP Analyzed (FTP 分析の合計数)	Data Security で分析した FTP 要求の合計数。
Blocked Requests (ブロックされた要求数)	分析およびポリシーの実施後に、ブロックされた要求の合計数。
Allowed Requests (許可された要求数)	分析およびポリシーの実施後に、許可された要求の合計数。
Failed Requests (失敗した要求数)	Data Security へ送信され、タイムアウトまたはその他の原因で完了しなかった転送の合計数。
Huge Requests (超過要求数)	最大 トランザクション サイズを超過した要求の合計数。
Decrypted Requests (復号化要求数)	復号化され、Data Security に送信された SSL 要求の合計数。

WCCP

WCCP WCCP バージョン v2 が有効化されている場合にのみ、WCCP v2 統計は表示されます。

統計 / フィールド	説明
	WCCP v2.0 Statistics (WCCP v2.0 統計)
WCCP Fragmentation (WCCP フラグメント)	
Total Fragments (フラグメントの合計数)	WCCP フラグメントの合計数。
Fragmentation Table Entries (フラグメント テーブルのエントリー数)	フラグメント テーブル内のエントリー数。
Out of Order Fragments (順番に並んでいないフラグメントの数)	順番に並んでいないフラグメントの数。
Matches (フラグメント一致数)	フラグメント テーブル内のフラグメントと一致しているフラグメントの数。
Service group name (サービス グループの名前)	
Service Group ID (サービス グループの ID)	サービスが提供されているプロトコルのサービス グループの ID

統計 / フィールド	説明
Configured mode (設定モード)	転送、返送、割り当ての設定。
IP Address (IP アドレス)	ルーターがトラフィックを送信している IP アドレス。
Leaderfs IP Address (リーダー IP アドレス)	WCCP キャッシュ ファームのリーダーの IP アドレス。
Number of Buckets Assigned (割り当てられたバケット数)	Content Gateway ノードに割り当てられているバケット数。Weight 値と現在のアクティブ ノードによって決定されます。
Number of Caches (キャッシュ数)	WCCP キャッシュ ファームに存在するキャッシュの数。
Number of Routers (ルーター数)	Content Gateway ノードにトラフィックを送信しているルーターの数。
Router IP Address (IP アドレス)	Content Gateway ノードにトラフィックを送信している WCCP ルーターの IP アドレス。 ご注意: WCCP ルーターに複数の IP アドレスが設定されている場合 - たとえばルーターが複数の VLAN をサポートするように設定されている時 - [Monitor] > [Networking] > [WCCP] の統計で報告される IP アドレスが、ここで設定される IP アドレスを異なる場合があります。これは、ルーターが常に最も高いアクティブ IP アドレスにおけるトラフィックを報告するからです。 ルーターが常に同じ IP アドレスを報告するようにする 1 つの方法は、ルーターのループバックアドレスをルーターの最も高い IP アドレスよりも高い値に設定することです。それによってループバックアドレスが常にルーターの IP アドレスとして報告されるようになります。この設定を使用することを推奨します。
Router ID Received (ルーター ID 受信回数)	Content Gateway が、ルーターから WCCP プロトコル メッセージを受信した回数。
Router Negotiated mode (ルーター ネゴシエーションモード)	ルーターとネゴシエーションされた転送、返送、割り当てモード。

DNS Proxy (DNS プロキシ)

統計	説明
Total Requests (要求の合計数)	クライアントから受信した DNS 要求の合計数。
Hits (ヒット数)	DNS キャッシュ ヒットの数。
Misses (ミス数)	DNS キャッシュ ミスの数。

DNS Resolver (DNS リゾルバ)

統計	説明
	DNS Resolver (DNS リゾルバ)
Total Lookups (ルックアップの合計数)	インストール以降の DNS ルックアップ (DNS ネーム サーバーへのクエリー) の合計数。
Successes (成功回数)	インストール以降の DNS ルックアップ成功の合計回数。
Average Lookup Time (ms) (平均ルックアップ時間)	DNS ルックアップの平均時間。
	Host Database (ホスト データベース)
Total Lookups (ルックアップの合計数)	インストール以降、Content Gateway ホスト データベースをルックアップした合計回数。
Total Hits (ヒット合計回数)	インストール以降、ホスト データベースにヒットした合計回数。
Average TTL (min) (平均 TTL)	平均継続時間 (分単位)。

Virtual IP (仮想 IP)

仮想 IP テーブルは、クラスタ内のプロキシによって管理されている仮想 IP アドレスを表示します。

Performance (パフォーマンス)

パフォーマンス グラフによって、Websense Content Gateway のパフォーマンスをモニタし、ネットワーク トラフィックを分析することができます。また、パフォーマンス グラフは、仮想メモリ使用量、クライアント接続、ドキュメント ヒット率などに関する情報を示します。パフォーマンス グラフは、Multi Router Traffic Grapher ツール (MRTG) によって作成されます。MRTG は、5 分間隔で 統計情報を累積します。

パフォーマンス グラフは、次の情報を提供します。

統計	説明
Overview (概要)	利用可能なグラフのサブセットを表示します。
Daily (毎日)	現在の日付の履歴情報を示すグラフを表示します。
Weekly (毎週)	現在の週の履歴情報を示すグラフを表示します。
Monthly (毎月)	現在の月の履歴情報を示すグラフを表示します。
Yearly (毎年)	現在の年の履歴情報を示すグラフを表示します。



重要

Multi Router Traffic Grapher (パフォーマンス グラフ表示ツール) を実行するには、Content Gateway システム上に Perl バージョン 5.005 以上をインストールする必要があります。

グラフの横に説明が表示されます。1つの画面で、毎日、毎週、毎月、毎年を表示するには、グラフをクリックします。

これらのグラフはアルファベット順に並べられます。

- Active Client Connections
- Active Native FTP Client Connections
- Active Origin Server Connections
- Active Parent Proxy Connections
- Bandwidth Savings (帯域幅の節約)
- Cache Read
- Cache Reads Per Second
- Cache Writes
- Cache Writes Per Second
- Client Transactions Per Second
- Content Gateway Manager Memory Usage
- Content Gateway Uptime
- CPU Available
- CPU Busy
- Data Security Module Memory Usage
- Disk Cache Usage
- DNS Cache Usage
- HTTP Abort Latency
- HTTP and HTTPS Transactions Per Second

- HTTP Cache Hit Latency
- HTTP Cache Miss Latency
- HTTP Connection Errors & Aborts (回数)
- HTTP Connection Errors & Aborts (パーセンテージ)
- HTTP Document Hit Rate
- HTTP Error Latency
- HTTP Hits & Misses (回数)
- HTTP Hits & Misses (パーセンテージ)
- HTTP POST and FTP PUT Transactions Per Second
- Microsoft Internet Explorer Browser Requests (パーセンテージ)
- MRTG Runtime
- Network Reads
- Network Writes
- RAM Cache Read I/O Hit Rate
- RAM Cache Usage
- SSL Manager Memory Usage
- TCP CLOSE_WAIT Connections
- TCP Connect Rate
- TCP ESTABLISHED Connections
- TCP FIN_WAIT_1 Connections
- TCP FIN_WAIT_2 Connections
- TCP LAST_ACK Connections
- TCP Segments Transmitted
- TCP Throughput
- TCP TIME_WAIT Connections
- Transaction Buffer Memory Usage
- WCCP Exceptional Input Fragments
- WCCP Fragment Table Size
- WCCP Input Fragments
- Web Security Scanned Transactions (Percentage)
- Web Security Slow Scanned Transactions
- Web Security Slow Transactions
- Websense Content Gateway Memory Usage

SSL

以下のタブは SSL Manager によってサポートされています：

[SSL Key Data \(SSL キー データ\), 280 ページ](#)

[CRL Statistics \(CRL 統計\), 281 ページ](#)

[Reports \(レポート\), 281 ページ](#)

SSL Key Data (SSL キー データ)

これらのフィールドは、クライアントと SSL Manager、および SSL Manager と宛先サーバー間の SSL 接続の状態とアクティビティについての情報を提供しています。

統計 / フィールド	説明
	SSL Inbound Key Data (SSL インバウンド キー データ)
Is alive (動作中)	Online は SSL Manager が有効なことを示しています。
Current SSL connections (現在の SSL 接続数)	アクティブなインバウンド SSL 要求数 (ブラウザから SSL Manager)。
Total SSL server connections (SSL サーバー接続の合計数)	ブラウザ要求の数。
Total finished SSL server connections (完了した SSL サーバー接続の合計数)	復号化のために、SSL Manager に送られたブラウザ要求の数。
Total SSL server renegotiation requests (SSL サーバー ネゴシエーションの合計数)	ブラウザと SSL Manager 間のハンドシェイクが失敗、または証明書が無効のために、再ネゴシエーションされたブラウザ要求の数。
	SSL Outbound Key Data (SSL アウトバウンド キー データ)
Is alive (動作中)	Online は SSL Manager が有効なことを示しています。
Current SSL connections (現在の SSL 接続数)	アクティブなアウトバウンド SSL 要求の数 (SSL Manager から宛先サーバー)。
Total SSL client connections (SSL クライアント接続の合計数)	ブラウザ要求の数。
Total finished SSL client connections (完了した SSL クライアント接続の合計数)	SSL Manager から宛先サーバーに送信されたデータの要求数。

統計 / フィールド	説明
Total SSL client renegotiation requests (SSL クライアント ネゴシエーションの合計数)	SSL Manager と宛先サーバー間のハンドシェークが失敗、または証明書が無効のために、再ネゴシエーションされた要求の数。
Total SSL session cache hits (SSL セッション キャッシュ ヒット回数)	セッション キャッシュ内のキーによって、要求が検証された回数。
Total SSL session cache misses (SSL セッション キャッシュ ミス回数)	セッション キャッシュ内のキーによって、要求が検証できなかった回数。
Total SSL session cache misses (SSL セッション タイムアウト回数)	タイムアウト時間が切れたために、セッション キャッシュから削除されたキーの数。

CRL Statistics (CRL 統計)

フィールドは、証明書のステータスについての情報を提供します。

統計 / フィールド	説明
	CRL Statistics (CRL 統計)
CRL list count (CRL リスト数)	証明書取り消しのリストの証明書の数。このリストは毎晩ダウンロードされます。 最新の取り消し情報を保持する, 169 ページ を参照してください。
	OCSP Statistics (OCSP 統計)
OCSP good count (OCSP 有効数)	証明書が有効である応答の数。
OCSP unknown count (OCSP 未知数)	証明書が認証されなかった OCSP 応答の数。
OCSP revoked count (OCSP 取り消し数)	取り消された証明書の数 (CRL & OCSP)。

Reports (レポート)

認証機関またはインシデントのレポートを作成するための情報は、[SSL Manager によるレポートの作成, 128 ページ](#)を参照してください。

B

コマンドと変数

Websense Content Gateway のコマンド

個別のコマンドを実行するか、シェルの中に複数のコマンドを記述するときに、コマンドラインを使用します。

コマンドを実行するために、root に移動します：

```
su
```

Content Gateway bin ディレクトリから、Content Gateway のコマンドを実行します。



ご注意

Content Gateway bin ディレクトリがパスにない場合、コマンドの先頭に次を追加します：

```
./
```

例：

```
./content_line -p
```

コマンド	説明
WCGAdmin start	Content Gateway サービスを起動します。
./WCGAdmin stop	Content Gateway サービスを停止します。
./WCGAdmin restart	Content Gateway サービスを停止し、その後再起動します。
./WCGAdmin status	次の Content Gateway サービスのステータス（実行中または停止中）を表示します：Content Gateway、Content Gateway Manager、および content_cop 。
WCGAdmin help	WCGAdmin コマンドのリストを表示します。
content_line -p socket_path	Content Gateway コマンドラインと Content Gateway Manager 通信で使用するファイルの位置（ディレクトリとパス）を指定します。デフォルトパスは install_dir/config/cli です。

コマンド	説明
<code>content_line -r variable</code>	パフォーマンス統計の指定 または 現在の設定値を表示します。指定できる変数のリストについては、 Websense Content Gateway 変数, 285 ページ を参照してください。
<code>content_line -s variable -v value</code>	<i>variable</i> は、変更する設定変数名であり、 <i>value</i> は設定する値です。指定できる設定変数のリストについては、 Websense Content Gateway 変数, 285 ページ を参照してください。
<code>content_line -h</code>	Content Gateway コマンドのリストを表示します。
<code>content_line -x</code>	Content Gateway 設定ファイルの再読みを開始します。このコマンドを実行することは、Content Gateway Manager の [Apply (適用)] をクリックすることと同じです。
<code>content_line -M</code>	クラスタ内のすべてのノード上の content_manager プロセスと content_gateway プロセスを再起動します。
<code>content_line -L</code>	ローカルノード上の content_manager プロセスと content_gateway プロセスを再起動します。
<code>content_line -S</code>	ローカルノード上の Content Gateway を停止します。
<code>content_line -U</code>	ローカルノード上の Content Gateway を起動します。
<code>content_line -B</code>	クラスタ全体に渡って Content Gateway を再起動します。ノード毎に Content Gateway を停止し即座にプロキシを再起動します。
<code>content_line -b</code>	ローカルノード上の Content Gateway を再起動します。ローカルノード上で Content Gateway を停止し即座にプロキシを再起動します。

Websense Content Gateway 変数

`content_line -s` コマンドを使用して、コマンドライン上で指定の構成変数の値を変更することができます。設定できる変数については、[records.config, 397 ページ](#)を参照してください。

`content_line -r` コマンドを使用して、コマンドライン上で指定の変数に関連する統計を表示することができます。変数のリストは 下記を参照してください。

また、[コマンドラインからの統計の表示, 124 ページ](#)および [コマンドラインインターフェース, 115 ページ](#)を参照してください。

統計情報

次の表は、個々の統計を表示させるために、コマンドライン上で指定できる変数をリストしています。情報は、[統計, 259 ページ](#)を参照してください。

統計を表示させるためには、プロンプトで次のように入力します：

```
content_line -r variable
```

統計	Variable (変数)
	Summary (要約)
Node name (ノード名)	<i>proxy.node.hostname</i>
Objects served (処理されたオブジェクト)	<i>proxy.node.user_agents_total_documents_served</i>
Transactions per second (秒当たりのトランザクション)	<i>proxy.node.user_agent_xacts_per_second</i>
	Node (ノード)
Document hit rate (ドキュメント ヒット率)	<i>proxy.node.cache_hit_ratio_avg_10s</i> <i>proxy.cluster.cache_hit_ratio_avg_10s</i>
Bandwidth savings (帯域幅の節約)	<i>proxy.node.bandwidth_hit_ratio_avg_10s</i> <i>proxy.cluster.bandwidth_hit_ratio_avg_10s</i>
Cache percent free (キャッシュの空き容量の割合)	<i>proxy.node.cache.percent_free</i> <i>proxy.cluster.cache.percent_free</i>
Open origin server connections (オリジン サーバー接続のオープン数)	<i>proxy.node.current_server_connections</i> <i>proxy.cluster.current_server_connections</i>
Open client connections (クライアント接続のオープン数)	<i>proxy.node.current_client_connections</i> <i>proxy.cluster.current_client_connections</i>
Cache transfers in progress (進行中のキャッシュ転送)	<i>proxy.node.current_cache_connections</i> <i>proxy.cluster.current_cache_connections</i>
Client throughput (Mbits/sec) (クライアントスループット)	<i>proxy.node.client_throughput_out</i> <i>proxy.cluster.client_throughput_out</i>

統計	Variable (変数)
Transactions per second (秒当たりのトランザクション)	<i>proxy.node.http.user_agent_xacts_per_second</i> <i>proxy.cluster.http.user_agent_xacts_per_second</i>
DNS lookups per second (秒当たりのDNSルックアップ)	<i>proxy.node.dns.lookups_per_second</i> <i>proxy.cluster.dns.lookups_per_second</i>
Host database hit rate (ホストデータベースのヒット率)	<i>proxy.node.hostdb.hit_ratio_avg_10s</i> <i>proxy.cluster.hostdb.hit_ratio_avg_10s</i>
	HTTP
Total document bytes from client (クライアントからのドキュメントの合計バイト)	<i>proxy.process.http.user_agent_response_document_total_size</i>
Total document bytes from client (クライアントからのヘッダーの合計バイト)	<i>proxy.process.http.user_agent_response_header_total_size</i>
Total response header bytes to client from cache (キャッシュからクライアントへのヘッダーの合計バイト)	<i>proxy.process.http.user_agent_response_from_cache_header_total_size</i>
Total response header bytes to client from cache (キャッシュからクライアントへの応答ヘッダーの合計バイト)	<i>proxy.process.http.user_agent_response_from_cache_document_total_size</i>
Total connections to client (クライアントへの接続の合計)	<i>proxy.process.http.current_client_connections</i>
Current unique clients connected (現在接続中のユニークなクライアント)	<i>proxy.process.http.client.unique_clients.active</i>
Total unique clients that have connected (接続が完了したユニークなクライアント)	<i>proxy.process.http.client.unique_clients.total</i>
Total clients that exceeded limit (限界数を超過したクライアントの合計)	<i>proxy.process.http.client.exceeding_limit</i>
Total clients for which connections were closed (接続が閉じたクライアントの合計)	<i>proxy.process.http.client.closed_connections</i>
Open HTTP client connections (HTTPクライアント接続のオープン数)	<i>proxy.process.http.current_active_http_client_connections</i>
Open HTTPS client connections (HTTPSクライアント接続のオープン数)	<i>proxy.node.process.http.current_active_https_client_connections</i>
Client Requests (IPv4 +IPv6) (クライアント要求 (IPv4 +IPv6))	<i>proxy.process.http.real_client_requests</i>

統計	Variable (変数)
Client IPv6 Requests (クライアント IPv6 要求)	<code>proxy.process.http.real_client_ipv6_requests</code>
Client transactions in progress (処理中のクライアント トランザクション)	<code>proxy.process.http.current_client_transactions</code>
Total document bytes from origin server (オリジン サーバーからのドキュメントの合計バイト)	<code>proxy.process.http. origin_server_response_document_total_size</code>
Total document bytes from origin server (オリジン サーバーからのヘッダーの合計バイト)	<code>proxy.process.http. origin_server_response_header_total_size</code>
Total connections to origin server (オリジン サーバーとの接続の合計)	<code>proxy.process.http.current_server_connections</code>
Origin server transactions in progress (進行中のオリジン サーバートランザクション)	<code>proxy.process.http.current_server_transactions</code>
	FTP
Currently open FTP connections (FTP 接続の現在のオープン数)	<code>proxy.process.ftp.connections_currently_open</code>
Successful PASV connections (PASV 接続の成功数)	<code>proxy.process.ftp.connections_successful_pasv</code>
Unsuccessful PASV connections (PASV 接続の失敗数)	<code>proxy.process.ftp.connections_failed_pasv</code>
Successful PORT connections (ポート接続の成功数)	<code>proxy.process.ftp.connections_successful_port</code>
Unsuccessful PORT connections (ポート接続の失敗数)	<code>proxy.process.ftp.connections_failed_port</code>
	WCCP
Enabled (有効化)	<code>proxy.config.wccp.enabled</code>
WCCP interface (WCCP インターフェイス)	<code>proxy.local.wccp2.ethernet_interface</code>
	Cache (キャッシュ)
Bytes used	<code>proxy.process.cache.bytes_used</code>
Cache size (キャッシュ サイズ)	<code>proxy.process.cache.bytes_total</code>
Lookups in progress (ルックアップ中)	<code>proxy.process.cache.lookup.active</code>

統計	Variable (変数)
Lookups completed (ルックアップ完了)	<i>proxy.process.cache.lookup.success</i>
Lookup misses (ルックアップミス)	<i>proxy.process.cache.lookup.failure</i>
Reads in progress (読み込み中)	<i>proxy.process.cache.read.active</i>
Reads completed (読み込み完了)	<i>proxy.process.cache.read.success</i>
Read misses (読み込みミス)	<i>proxy.process.cache.read.failure</i>
Writes in progress (書き込み中)	<i>proxy.process.cache.write.active</i>
Writes completed (書き込み完了)	<i>proxy.process.cache.write.success</i>
Write failures (書き込み失敗)	<i>proxy.process.cache.write.failure</i>
Updates in progress (更新中)	<i>proxy.process.cache.update.active</i>
Updates completed (更新完了)	<i>proxy.process.cache.update.success</i>
Update failures (更新失敗)	<i>proxy.process.cache.update.failure</i>
Removes in progress (削除中)	<i>proxy.process.cache.remove.active</i>
Remove successes (削除成功)	<i>proxy.process.cache.remove.success</i>
Remove failures (削除失敗)	<i>proxy.process.cache.remove.failure</i>
Host DB (ホストデータベース)	
Total lookups (ルックアップ合計)	<i>proxy.process.hostdb.total_lookups</i>
Total hits	<i>proxy.process.hostdb.total_hits</i>
Time TTL (分) (TTL 時間)	<i>proxy.process.hostdb.ttl</i>
DNS	
DNS total lookups (DNS ルックアップ合計)	<i>proxy.process.dns.total_dns_lookups</i>
Average lookup time (ミリ秒) (平均ルックアップ時間)	<i>proxy.process.dns.lookup_avg_time</i>
DNS successes (DNS ルックアップ成功)	<i>proxy.process.dns.lookup_successes</i>
Cluster	

統計	Variable (変数)
Bytes Read (読み込みバイト数)	<i>proxy.process.cluster.read_bytes</i>
Bytes written (書き込みバイト数)	<i>proxy.process.cluster.write_bytes</i>
Connections open (接続オープン数)	<i>proxy.process.cluster.connections_open</i>
Total operations (処理合計数)	<i>proxy.process.cluster.connections_opened</i>
Network backups (ネットワークバックアップ)	<i>proxy.process.cluster.net_backup</i>
Clustering nodes (クラスタリング ノード)	<i>proxy.process.cluster.nodes</i>
	SOCKS
Unsuccessful connections (接続失敗)	<i>proxy.process.socks.connections_unsuccessful</i>
Successful connections (接続成功)	<i>proxy.process.socks.connections_successful</i>
Connections in progress (接続中)	<i>proxy.process.socks.connections_currently_open</i>
	Logging (ログ記録)
Currently open log files (現在開いているログファイル)	<i>proxy.process.log2.log_files_open</i>
Space used for log files (ログ ファイルの容量)	<i>proxy.process.log2.log_files_space_used</i>
Number of access events logged (ログされたアクセス イベントの数)	<i>proxy.process.log2.event_log_access</i>
Number of access events skipped (スキップされたアクセス イベントの数)	<i>proxy.process.log2.event_log_access_skip</i>
Number of error events logged (ログされたエラー イベントの数)	<i>proxy.process.log2.event_log_error</i>

C

設定のオプション

オプションは、設定ペインの左側に次のように分類されています。

[My Proxy \(マイ プロキシ\)](#), 291 ページ

[Protocols \(プロトコル\)](#), 302 ページ

[Content Routing \(コンテンツ ルーティング\)](#), 315 ページ

[Security \(セキュリティ\)](#), 320 ページ

[Subsystems \(サブシステム\)](#), 337 ページ

[Networking \(ネットワーク\)](#), 343 ページ

My Proxy (マイ プロキシ)

My Proxy オプションは、次のように分類されています：

[Basic \(基本\)](#), 292 ページ

[Subscription \(サブスクリプション\)](#), 296 ページ

[UI Setup \(UI の設定\)](#), 297 ページ

[Snapshots \(スナップショット\)](#), 299 ページ

[Logs \(ログ\)](#), 301 ページ

Basic (基本)

オプション	説明
	General (一般)
Restart (再起動)	<p>プロキシおよびマネージャー サービス (<code>content_gateway</code> および <code>content_manager</code> プロセス) を再起動します。一部の設定オプションを変更した場合、プロキシおよびマネージャー サービスを再起動する必要があります。</p> <p>クラスタ構成の場合、[Restart] ボタンは クラスタ内のすべてのノード上のプロキシおよびマネージャー サービスを再起動します。</p>
Proxy Name (プロキシ)	<p>Content Gateway ノードの名前を指定します。デフォルトは、Content Gateway を実行しているコンピュータのホスト名です。</p> <p>ノードがクラスタの一部である場合は、このオプションで、Content Gateway クラスタの名前を指定します。Content Gateway クラスタでは、すべてのノードは同じノード名を共有する必要があります。</p>
Alarm email (アラーム電子メール)	Content Gateway が、アラーム通知を送信する電子メールアドレスを指定します。
	Features (機能)
Protocols: FTP	<p>このオプションを有効にした場合、Content Gateway は、FTP クライアントからの FTP 要求を受け入れます。このオプションを変更した場合、Content Gateway を再起動する必要があります。</p>
Protocols: HTTPS	<p>SSL Manager の HTTPS 要求 (暗号化データ) 処理を有効化 / 無効化します。HTTPS On を選択した場合、「Configure」 > 「Protocols」 > HTTPS ページ、および 「Configure」 > 「SSL」 ページで、追加情報を入力する必要があります。暗号化データの使用, 145 ページ を参照してください。</p>
Networking: WCCP	<p>このオプションを有効にした場合、Content Gateway への透過的なリダイレクトのために、WCCP v2- 対応のルーターを使用します。WCCP v1 は、サポートされていません。</p> <p>WCCP v2 デバイスによる透過的遮断, 55 ページ を参照してください。</p> <p>このオプションを変更した場合、Content Gateway を再起動する必要があります。</p>
Networking: DNS Proxy	<p>このオプションを有効にした場合、Content Gateway は、クライアントに代わって、DNS 要求を解決します。このオプションによって、リモート DNS サーバーの負荷が軽減され、DNS ルックアップの応答時間が短くなります。DNS プロキシキャッシング, 107 ページ を参照してください。</p>

オプション	説明
Networking: Virtual IP	このオプションを有効にした場合、Content Gateway は必要に応じてクラスタ内のノードに割り当てる仮想 IP アドレスのプールを維持します。 仮想 IP フェールオーバー, 89 ページ を参照してください。
Networking: IPv6	このオプションを有効にした場合、Content Gateway は、IPv6 に対する限定的なサポートを提供します。サポートは、明示的プロキシのみ提供されます。IPv6 アドレスは、クライアントおよび（または）インターネットトラフィックを処理する、すべてのデュアルスタックイーサネットインタフェースで使用することができます。すべての TRITON コンポーネントとの通信には、IPv4 アドレスを使用する必要があります。 Content Gateway バージョン 7.7.0 による IPv6 のサポート, 48 ページ を参照してください。
Networking: Data Security	Websense Data Security との接続を有効化します。次の 2 つのオプションがあります： <ul style="list-style-type: none"> • Data Security Management Server への自動登録（バージョン 7.7 が必要）。 • リモート Data Security Suite との ICAP 通信（バージョン 7.1、またはそれ以前）。 Websense Data Security の使用, 133 ページ を参照してください。このオプションを変更した場合、Content Gateway を再起動する必要があります。
Networking: Data Security: Integrated on-box	インストールされている Data Security コンポーネントと Data Security Management Server への登録を有効にします。 Data Security の登録と構成, 135 ページ を参照してください。
Networking: Data Security: ICAP	Data Security Suite で ICAP を有効にします。 ICAP クライアントの構成, 139 ページ を参照してください。
Security: SOCKS	SOCKS を有効にした場合、Content Gateway は SOCKS サーバーと通信します。 SOCKS ファイアウォール統合の設定, 192 ページ を参照してください。このオプションを変更した場合、Content Gateway を再起動する必要があります。
Authentication: None	Content Gateway は、ユーザー認証のいくつかのタイプをサポートしています。このオプションを選択した場合、プロキシはユーザー認証を実行しません。これは、デフォルト設定です。
Authentication: Integrated Windows Authentication	統合 Windows 認証 (IWA) を有効にした場合、ユーザーがコンテンツへのアクセスを許可される前に、ユーザーは IWA によって認証されます。 統合 Windows 認証, 201 ページ を参照してください。このオプションを変更した場合、Content Gateway を再起動する必要があります。

オプション	説明
Authentication: LDAP	<p>LDAP を有効した場合、コンテンツへのアクセスを許可される前に、ユーザーは LDAP によって認証されます。LDAP 認証, 210 ページを参照してください。</p> <p>このオプションを変更した場合、Content Gateway を再起動する必要があります。</p>
Authentication: Radius	<p>RADIUS を有効した場合、コンテンツへのアクセスを許可される前に、ユーザーは RADIUS によって認証されます。RADIUS 認証, 213 ページを参照してください。</p> <p>このオプションを変更した場合、Content Gateway を再起動する必要があります。</p>
Authentication: Legacy NTLM	<p>レガシー NTLM (NTLMSSP) を有効した場合、Windows ネットワーク内のユーザーは、コンテンツへのアクセスを許可される前に、ドメイン コントローラによって認証されます。</p> <p>レガシー NTLM 認証, 207 ページを参照してください。</p> <p>このオプションを変更した場合、Content Gateway を再起動する必要があります。</p>
Authentication: Multiple Realm Authentication	<p>複数レルムの認証を有効化または無効化します。複数レルムの認証は、信頼関係を共有していない複数のドメイン環境、従って、特定のドメイン コントローラによって、特定のユーザーが認証される必要がある環境をサポートしています。</p> <p>複数レルムの認証, 216 ページを参照してください。</p> <p>このオプションを変更した場合、Content Gateway を再起動する必要があります。</p>
Authentication: Read authentication from child proxy	<p>着信要求内の X-Authenticated-User、および X-Forwarded-For ヘッダー値の読み込みを有効化または無効化します。このオプションはデフォルトで無効です。</p> <p>Content Gateway がチェーンの中の親(アップストリーム)プロキシであり、子(ダウンストリーム)プロキシが認証のために、X-Authenticated-User、および X-Forwarded-For ヘッダーを送信する場合に、このオプションを有効にします。</p>
Authentication: Send authentication to parent proxy	<p>送信要求内に、X-Authenticated-User ヘッダー値を挿入するかどうか指定します。このオプションはデフォルトで無効です。</p> <p>Content Gateway がチェーンの中の子(ダウンストリーム)プロキシであり、親(アップストリーム)プロキシが認証のために、X-Authenticated-User ヘッダーを必要とする場合に、このオプションを有効にします。</p>

オプション	説明
Cluster: Type	<p>Clustering (クラスタ化)</p> <p>クラスタ モードを指定します。</p> <p>Content Gateway サーバーを単一モードで実行する場合、[Single Node] を選択します。このノードは、クラスタの一部ではなくなります。</p> <p>管理クラスタ化モードアクティブにするには、[Management Clustering] を選択します。クラスタ内のノードは設定情報を共有しており、同時にすべてのノードを管理できます。</p> <p>クラスタ化の詳細については、クラスタ, 83 ページを参照してください。</p> <p>このオプションを変更した場合、Content Gateway を再起動する必要があります。</p>
Cluster: Interface	<p>Content Gateway が、クラスタ内の他のノードと通信するために、どのインターフェースを使用するかを指定します。例、eth0</p> <p>専用のセカンダリー インターフェースを使用することを推奨します。</p> <p>ノード構成情報は、プレーン テキストで、同じサブネット中の他の Content Gateway ノードにマルチキャストされます。したがって、Websense は、クライアントを Content Gateway ノードから独立したサブネット上に配置することを推奨します (クラスタ化のためのマルチキャスト通信はルーティングされません)。</p> <p>V シリーズ アプライアンス上では、P1 (eth0) が推奨インターフェースです。しかし、クラスタ管理トラフィックを隔離したい場合には、P2 (eth1) を使用してもかまいません。</p> <p>クラスタ構成の変更, 86 ページを参照してください。</p> <p>このオプションを変更した場合、Content Gateway を再起動する必要があります。</p>
Cluster: Multicast Group Address	<p>Content Gateway が、クラスタ ピアと通信するためのマルチキャスト グループ アドレスを指定します。</p> <p>クラスタ構成の変更, 86 ページを参照してください。</p>
Cluster: SSL Manager Configuration Server	<p>SSL Manager Configuration Server の IP アドレスを指定します。Content Gateway が再起動した時、SSL Manager Configuration Server (プライマリ) は、クラスタのすべてのメンバーに識別されます。すべての SSL の構成の変更は、プライマリ上で行われる必要があります。SSL 管理クラスタ化, 85 ページを参照してください。</p>

Subscription (サブスクリプション)

オプション	説明
	Subscription Management (サブスクリプション管理)
Subscription Key	Websense から受け取ったサブスクリプション キーを表示します。キーは、ライセンス契約した製品を反映しています。Web Security Gateway、または Web Security Gateway Anywhere で Content Gateway を使用する場合、TRITON Web Security に入力したサブスクリプション キーです。Content Gateway が、Websense Data Security Suite のみと共に配備されている場合、このフィールドに Content Gateway のサブスクリプション キーを入力する必要があります。
	Scanning (スキャンニング)
Policy Server	
IP address	Websense Web Security Policy Server の IP アドレスを指定します。
Port	Websense Web Security Policy Server が使用するポートを指定します。
Filtering Service	
IP address	Websense Web Security Filtering Service の IP アドレスを指定します。
Port	Websense Web Security Filtering Service が使用するポートを指定します。
Communication Timeout	Policy Server および Filtering Service が応答を返す必要があるタイムアウト時間をミリ秒単位で指定します。この時間を過ぎると、通信タイムアウト条件が発生し、[Action for Communication Errors] の設定が適用されます。デフォルトのタイムアウト値は、5000 (5 秒) です。
Action for Communication Errors	
Permit traffic	Policy Server または Filtering Service との通信が失敗した場合に、すべてのページを許可します。
Block traffic	Policy Server または Filtering Service との通信が失敗した場合に、すべてのページをブロックします。

UI Setup (UI の設定)

オプション	説明
	General (一般)
UI Port	ブラウザが Content Gateway Manager と接続するポートを指定します。ポートは Content Gateway システム上にあり、Content Gateway のみが使用する必要があります。デフォルトポートは 8081 です。 この設定を変更した場合、Content Gateway を再起動する必要があります。
SSL UI Port	SSL Manager ユーザー インターフェースのポートを指定します。このインターフェースを使用して、データの復号化、および 証明書の管理を設定できます。デフォルトポートは 8071 です。 暗号化データの使用, 145 ページ を参照してください。 Content Gateway Manager インターフェースと SSL Manager インターフェースは、異なる ポートを使用する必要があります。 この設定を変更した場合、Content Gateway を再起動する必要があります。
HTTPS: Enable/Disable	Content Gateway Manager との SSL 接続を有効化または無効化します。SSL は、リモート管理モニタリングおよび設定の保護を提供します。Content Gateway Manager との接続に SSL を使用するためには、Content Gateway サーバー コンピュータに SSL 証明書をインストールする必要があります。詳細情報は、 セキュアな管理のための SSL の使用, 186 ページ を参照してください。
HTTPS: Certificate File	Content Gateway Manager にアクセスするユーザーを認証するための、SSL 証明書ファイル を指定します。
Monitor Refresh Rate	Content Gateway Manager が、「 Monitor 」ペイン上の統計を更新する頻度を指定します。デフォルト値は 30 秒です。
	Login (ログイン)
Basic Authentication	基本認証を有効化または無効化します。このオプションを有効にした場合、Content Gateway は、ユーザーが Content Gateway Manager にアクセスする度に、管理ログインとパスワード、または ユーザー名とパスワード (ユーザー アカウントが設定されている場合) をチェックします。
Administrator: Login	管理ログインを指定します。管理ログインは、Content Gateway Manager の設定モード、および モニタ モード両方にアクセスするマスター ログインです。 ご注意: 基本認証オプションが有効化されている場合のみ、Content Gateway は管理ログインをチェックします。

オプション	説明
Administrator Password	<p>Content Gateway Manager へのアクセスを制御する管理者パスワードを変更します。</p> <p>パスワードを変更するには、[Old Password] フィールドに現在のパスワードを入力し、[New Password] フィールドに新しいパスワードを入力します。[New Password (Retype)] フィールドに新しいパスワードを再入力し、[Apply] をクリックします。</p> <p>ご注意: 基本認証オプションが有効化されている場合にのみ、Content Gateway は管理ログインとパスワードをチェックします。</p> <p>インストール中に管理者パスワードを選択します。インストーラは自動的にパスワードを暗号化し、records.config ファイルに暗号を保存します。Content Gateway Manager のパスワードを変更する度に、Content Gateway は records.config ファイルを更新します。管理者パスワードを忘れてしまい、Content Gateway Manager にアクセスできない場合、マスタ管理者パスワードを忘れた場合に Content Gateway Manager にどのようにアクセスしますか, 482 ページをご覧ください。</p>
Additional Users	<p>現在のユーザー アカウントをリストし、新しいユーザー アカウントを追加できます。ユーザー アカウントは、誰が Content Gateway Manager にアクセスし、どの動作を実行できるかを決定します。1つの管理ログインとパスワードだけでは、ニーズに対応する十分なセキュリティを確保できない場合に、ユーザー アカウントのリストを作成できます。</p> <p>新しいアカウントを作成するには、[New User] フィールドにユーザーログインを入力し、[New Password] フィールドにユーザーパスワードを入力します。[New Password (Retype)] フィールドにユーザーパスワードを再入力し、[Apply] をクリックします。新しいユーザーの情報が、表内に表示されます。テーブルの [Access] ドロップダウンリストで、ユーザーが実行できるアクティビティを選択します(モニタ、モニターおよび設定の表示、モニターおよび設定の変更)。ユーザー アカウントの詳細については、ユーザー アカウントのリストの作成, 185 ページを参照してください。</p> <p>ご注意: 基本認証オプションが有効化されている場合にのみ、Content Gateway は管理ログインとパスワードをチェックします。</p>
Access (アクセス)	
Access Control	<p>Content Gateway Manager へのアクセスを許可するリモートホストを指定した mgmt_allow.config ファイル内のルールを表を表示します。このファイルのエントリは、認証されたユーザーだけが設定オプションを変更でき、パフォーマンスおよびネットワークトラフィック統計を表示できるようにします。</p> <p>ご注意: デフォルトでは、すべてのリモートホストが Content Gateway Manager へのアクセスを許可されています。</p>
Refresh	<p>mgmt_allow.config ファイルの最も最新のルールを表示するために、表を更新します。</p>

オプション	説明
Edit File	<code>mgmt_allow.config</code> ファイルを編集、およびルールを追加するために、設定ファイル エディタを開きます。
	mgmt_allow.config Configuration File Editor (mgmt_allow.config 設定ファイル エディタ)
ルール表示ボックス	<code>mgmt_allow.config</code> ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または上下に移動できます。Content Gateway は、リストの上から順にルールを適用します。
Add	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。
Set	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。
IP Action	追加できるルールのタイプをリストします。 ip_allow ルールは、[Source IP] フィールドで指定したりモートホストが、Content Gateway Manager にアクセスすることを許可します。 ip_deny ルールは、[Source IP] フィールドで指定したりモートホストが、Content Gateway Manager にアクセスすることを拒否します。
Source IP	Content Gateway Manager にアクセスすることを許可または拒否する IP アドレスを指定します。単一の IP アドレス (111.111.11.1)、または アドレスの範囲 (0.0.0.0-255.255.255.255) を入力できます。
Apply	設定の変更を適用します。
Close	設定ファイル エディタ を終了します。 [Close] をクリックする前に、[Apply] をクリックします。そうでないと、設定変更は失われます。

Snapshots (スナップショット)

オプション	説明
	File System (ファイル システム)
Change Snapshot Directory	Content Gateway ノードのスナップショットを保存するディレクトリを指定します。

オプション	説明
Snapshots: Save Snapshot	<p>撮る構成のスナップショットの名前を入力します。[Apply] をクリックして、ローカルノード上の設定を保存します。Content Gateway は、[Change Snapshot Directory] フィールドで指定されたディレクトリに、構成のスナップショットを保存します。</p> <p>スナップショットを撮ってから、システム保守を実行したり、システムパフォーマンスを微調整することを推奨します。スナップショットを撮るのはほんの数秒で、構成の間違いを修正する時間を節約できます。</p>
Snapshots: Restore/Delete Snapshot	<p>ノードに保存されているスナップショットをリストします。ドロップダウンリストから、削除、または復元したいスナップショットを選択します。</p>
Snapshots: Restore Snapshot from "directory_name" Directory	<p>[Restore/Delete Snapshot] ドロップダウン ボックスで選択されたスナップショットを復元します。</p> <p>クラスタ構成の場合、スナップショットは、クラスタ内のすべてのノード上で復元されます。</p>
Snapshots: Delete Snapshot from "directory_name" Directory	<p>[Restore/Delete Snapshot] ドロップダウン ボックスで選択されたスナップショットを削除します。</p>
FTP Server (FTP サーバー)	
FTP Server	<p>構成のスナップショットから復元、または 構成のスナップショットに保存する FTP サーバー名を指定します。</p>
Login	<p>FTP サーバーへのアクセスに必要なログイン名を指定します。</p>
Password	<p>FTP サーバーへのアクセスに必要なパスワードを指定します。</p>
Remote Directory	<p>構成スナップショットから復元、または 構成スナップショットに保存する FTP サーバーのディレクトリを指定します。</p>
Restore Snapshot	<p>復元できる FTP サーバーの構成スナップショットがリストされます。</p> <p>FTP サーバーに正常にログオンした後、このフィールドは表示されます。</p>
Save Snapshot to FTP Server	<p>撮る構成のスナップショットの名前を入力し、FTP サーバーに保存します。</p> <p>FTP サーバーに正常にログオンした後、このフィールドは表示されます。</p>

Logs (ログ)

オプション	説明
	System (システム)
Log File	表示できるシステム ログ ファイルがリストされ、削除、またはローカルシステムにコピーします。Content Gateway は、システム全体のログ記録機能である syslog がデーモン機能で記録したシステム ログ ファイル をリストアップします。
Action: Display the selected log file	このオプションを有効にした場合、Content Gateway は、 [Log File] ドロップダウン リストで選択されたシステム ログ ファイルの最初の 1MB を表示します。全体のファイルを表示するには、“Save the selected log file in local filesystem” を選択し、ローカル ビューアで ファイルを表示します。
Action: Display last lines of the selected file	このオプションを有効にした場合、Content Gateway は、選択されたシステム ログ ファイルの末尾の指定行数を表示します。
Action: Display lines that match in the selected log file	このオプションを有効にした場合、Content Gateway は、指定された文字列と一致したシステム ログ ファイルのすべての行を表示します。
Action: Remove the selected log file	このオプションを有効にした場合、Content Gateway は、選択されたログ ファイルを削除します。
Action: Save the selected log file in local filesystem	このオプションを有効にした場合、Content Gateway は、選択されたログ ファイルを、ローカル システム上の指定された場所に保存します。
	Access (アクセス)
Log File	表示できるイベントまたはエラーファイルをリストし、削除 または ローカルシステムにコピーします。Content Gateway はイベント ログ ファイルを、 [Subsystems/Logging] の [Logging Directory] フィールドで指定され、および records.config ファイルの proxy.config.log2.logfile_dir 構成変数によって指定されているディレクトリに保存します。デフォルトのディレクトリは、Content Gateway インストール ディレクトリの logs です。
Action: Display the selected log file	このオプションを有効にした場合、Content Gateway は、 [Log File] ドロップダウン リストで選択されたイベントまたはエラー ログ ファイルの最初の 1MB を表示します。全体のファイルを表示するには、“Save the selected log file in local filesystem” を選択し、ローカル ビューアで ファイルを表示します。
Action: Display last lines of the selected file	このオプションを有効にした場合、Content Gateway は、 [Log File] ドロップダウン リストで選択されたイベントまたはエラー ログ ファイルの末尾の指定行数を表示します。

オプション	説明
Action: Display lines that match in the selected log file	このオプションを有効にした場合、Content Gateway は、指定された文字列と一致したイベントまたはエラー ログ ファイルのすべての行を表示します。
Remove the selected log file	このオプションを有効にした場合、Content Gateway は、選択されたログ ファイルを削除します。
Action: Save the selected log file in local filesystem	このオプションを有効にした場合、Content Gateway は、選択されたログ ファイルを、ローカル システム上の指定された場所に保存します。

Protocols (プロトコル)

プロトコル設定オプションは、次のカテゴリに分けられます：

[HTTP, 302 ページ](#)

[HTTP Responses \(HTTP 応答\), 311 ページ](#)

[HTTP Scheduled Update \(HTTP スケジュール設定した更新\), 312 ページ](#)

[HTTPS, 313 ページ](#)

[FTP, 314 ページ](#)

HTTP

オプション	説明
	General (一般)
HTTP Proxy Server Port	Content Gateway が、HTTP トラフィックの Web プロキシ サーバーとして動作する時、または HTTP 要求を透過的に処理する時に使用するポートを指定します。デフォルトポートは 8080 です。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Secondary HTTP Proxy Server Ports	明示的プロキシ構成の場合のみ 、Content Gateway が HTTP トラフィックを受信待機する追加のポートを指定します。 透過的プロキシ構成では、すべての HTTP トラフィックをポート 8080 に送信します。

オプション	説明
Unqualified Domain Name Expansion	<p>.com 名拡張を有効化または無効化します。このオプションを有効にした場合、Content Gateway は、先頭に www. を追加し 末尾に .com を付加し、拡張したアドレスにリダイレクトすることで、不適切なホスト名を解決しようと試みます。たとえば、クライアントが <i>company</i> に要求を行うと、Content Gateway は、www.company.com に要求をリダイレクトします。</p> <p>ローカル ドメイン拡張が有効な場合 (DNS Resolver (DNS リゾルバ), 353 ページを参照)、Content Gateway は .com ドメイン拡張の前に、ローカル ドメイン拡張を試みます。Content Gateway は ローカルドメイン拡張が失敗した場合にのみ .com ドメイン拡張を試みます。</p>
Send HTTP 1.1 by Default	<p>オリジン サーバーへの最初の要求に HTTP 1.1 を送信します (デフォルト)。オリジン サーバーが HTTP 1.0 で応答した場合、Content Gateway は HTTP 1.0 に変更します (ほとんどのオリジン サーバーは HTTP 1.1 を使用します)。無効化された場合、オリジン サーバーへの最初の要求に HTTP 1.0 が使用されます。オリジン サーバーが HTTP 1.1 で応答した場合、Content Gateway は HTTP 1.1 に変更します。</p>
Reverse DNS	<p>URL に (ホスト名の代わりに) IP アドレスが含まれ、filter.config、cache.config、または parent.config にルールが存在する場合、リバース DNS ルックアップを有効化します。これは、ルールが 宛先ホスト名、および ドメイン名に基づく場合に必要です。</p>
Tunnel Ports	<p>Content Gateway が トンネリングを許可するポートを指定します。これは、スペースで区切られたリストで、ポート範囲を指定できます (例、1-65535)。</p> <p>SSL が有効化されていない場合、指定されたポート宛てのすべてのトラフィックは、オリジン サーバーへのトンネリングを許可されます。SSL が有効化されている場合、[HTTPS Ports] フィールドにリストされているすべてのポートへのトラフィックは トネリングされず、復号化され、フィルタリング ポリシーが適用されます。</p>
HTTPS Ports	<p>SSL が有効化されている場合に、トラフィックが復号化され、フィルタリング ポリシーが適用されるポートを指定します。SSL が無効化されている場合は、このポートへのトラフィックは 復号化されず、下記に基づいたフィルタリング ポリシーが適用されます：</p> <ul style="list-style-type: none"> • 明示的プロキシの場合、CONNECT 要求内のサーバーホスト名。 • 透過的モードの場合、サーバー証明書内のサーバーホスト名。
FTP over HTTP: Anonymous Password	<p>パスワードを要求する FTP サーバー接続に、Content Gateway が 使用する匿名パスワードを指定します。このオプションは、HTTP クライアントからの FTP 要求に適用されます。</p>

オプション	説明
FTP over HTTP: Data Connection Mode	<p>FTP 転送は、2 つの接続を必要とします：データ要求を FTP サーバーに通知する コントロール接続と、データを送信するデータ接続です。FTP モードは、データ接続を Content Gateway が開始するか、FTP サーバーが開始するかを決定します。</p> <p>[PASV then PORT] を選択すると、Content Gateway は、最初に PASV 接続モードを試みます。PASV モードが失敗した場合、Content Gateway は PORT モードを試み、データ接続を開始します。成功すれば、FTP サーバーはデータ接続を受け入れます。</p> <p>[PASV only] を選択すると、Content Gateway は、FTP サーバーとデータ接続を開始します。このモードは、ファイアウォールに適していますが、いくつかの FTP サーバーはサポートしていません。</p> <p>[PORT only] を選択すると、FTP サーバーは データ接続を開始し、Content Gateway は接続を受け入れます。デフォルト値は、[PASV then PORT] です。</p>
Cacheability (キャッシュ機能)	
Caching: HTTP Caching	<p>HTTP キャッシュを有効化または無効化します。このオプションを有効にした場合、Content Gateway は HTTP 要求をキャッシュから処理します。このオプションを無効にした場合、Content Gateway はプロキシサーバーとして動作し、すべての HTTP 要求を直接オリジンサーバーに転送します。</p>
Caching: FTP over HTTP Caching	<p>FTP over HTTP キャッシュを有効化または無効化します。このオプションを有効にした場合、Content Gateway は、HTTP クライアントからの FTP 要求をキャッシュから処理します。このオプションを無効にした場合、Content Gateway は、プロキシサーバーとして動作し、HTTP クライアントからのすべての FTP 要求を直接オリジンサーバーに転送します。</p>
Behavior: Required Headers	<p>HTTP オブジェクトをキャッシュするために要求される、最小限のヘッダー情報を指定します。</p> <p>Select Expires または max-age ヘッダーを含んだ HTTP オブジェクトのみキャッシュする場合、[An Explicit Lifetime Header] を選択します。</p> <p>last_modified ヘッダーを含んだ HTTP オブジェクトのみキャッシュする場合、[A Last-Modified Header] を選択します。</p> <p>Expires、max-age、または last-modified ヘッダーを含まない HTTP オブジェクトをキャッシュする場合、[No Required Headers] を選択します。これは、デフォルト オプションです。</p> <p>警告：デフォルトで、Content Gateway は すべてのオブジェクトをキャッシュします (ヘッダーのないオブジェクトを含む)。プロキシの特別の事情がない限りデフォルト設定を変更しないことを推奨します。Content Gateway が Expires または max-age ヘッダーをもつ HTTP オブジェクトのみをキャッシュするように設定されている場合、キャッシュ ヒット率が下がります (明示的な期限切れ情報があるオブジェクトはごく少数です)。</p>

オプション	説明
Behavior: When to Revalidate	<p>キャッシュ内の HTTP オブジェクトの最新性を評価する方法を指定します：</p> <p>キャッシュ内の HTTP オブジェクトをオリジン サーバーに再確認しない場合、[Never Revalidate] を選択します (Content Gateway は、すべての HTTP オブジェクトが最新であるとみなします)。</p> <p>常にキャッシュ内の HTTP オブジェクトをオリジン サーバーに再確認する場合、[Always Revalidate] を選択します (Content Gateway は、すべての HTTP オブジェクトが古くなったとみなします)。</p> <p>オブジェクトが Expires または Cache-Control ヘッダーを含まない場合に、HTTP オブジェクトの最新性をオリジン サーバーに確認する場合、[Revalidate if Heuristic Expiration] を選択します。Content Gateway は、Expires または Cache-Control ヘッダーのないすべての HTTP オブジェクトは古くなったとみなします。</p> <p>Content Gateway が、オブジェクト ヘッダー、絶対最新性限界値、および (または) cache.config ファイル内のルールに基づいて、キャッシュ内のオブジェクトが古くなった見なしたときに、HTTP オブジェクトの最新性をオリジン サーバーに確認する場合、[Use Cache Directive or Heuristic] を選択します。これは、デフォルト オプションです。</p> <p>再確認の詳細については、HTTP オブジェクトの再確認, 26 ページを参照してください。</p>
Behavior: Add “no-cache” MSIE Requests	<p>Content Gateway が、Microsoft Internet Explorer からの要求に対して no-cache ヘッダー付加する場合に、指定します。</p> <p>Microsoft Internet Explorer の一部のバージョンは、ユーザーがブラウザの [Refresh] ボタンを押した場合、透過的キャッシュからのキャッシュ再ロードを要求しません。それによって、コンテンツがオリジン サーバーから直接にロードされるのを防止します。Content Gateway が Microsoft Internet Explorer の要求をより慎重に処理するように設定できます。その場合、提供するコンテンツの最新性を向上させることができますが、キャッシュから提供できるドキュメントの数が少なくなります。</p> <p>Microsoft Internet Explorer からのすべての要求に、no-cache ヘッダー付加する場合、[To All MSIE Requests] を選択します。</p> <p>IMS (If Modified Since) を含む Microsoft Internet Explorer からの要求に no-cache ヘッダー付加する場合、[To IMS MSIE Requests] を選択します。</p> <p>Microsoft Internet Explorer からのすべての要求に、no-cache ヘッダー付加しない場合、[Not to Any MSIE Requests] を選択します。</p>

オプション	説明
Behavior: Ignore “no-cache” in Client Requests	このオプションを有効にすると、Content Gateway はクライアント要求の no-cache ヘッダーを無視し、キャッシュで要求を処理します。 このオプションを無効にすると、Content Gateway は no-cache ヘッダーの要求をキャッシュで処理せず、オリジンサーバーに転送します
Freshness: Minimum Heuristic Lifetime	HTTP オブジェクトが、キャッシュ内で最新と見なされる最小時間を指定します。
Freshness: Maximum Heuristic Lifetime	HTTP オブジェクトが、キャッシュ内で最新と見なされる最大時間を指定します。
Freshness: FTP Document Lifetime	FTP ファイルが、キャッシュ内に存在する最大時間を指定します。このオプションは、HTTP クライアントからの FTP 要求のみに適用されます。
Maximum Alternates	Content Gateway が、キャッシュするオブジェクトの代替バージョンの最大数を指定します。 警告: 0 (ゼロ) を入力した場合、キャッシュする代替バージョンの制限はありません。よくアクセスする URL に数千の代替がある場合、Content Gateway が各要求に対して数千の代替を検索し、キャッシュヒットの遅延 (処理時間) を増加させていないかを、監視する必要があります。特に、いくつかの URL は、クッキーによって、多くの数代替をもつことがあります。Content Gateway がクッキーで変化するように設定されている場合、この問題に遭遇するかもしれません。
Vary Based on Content Type: Enable/ Disable	Vary ヘッダーを含んでいない HTTP ドキュメントの代替バージョンのキャッシングを、有効化または無効化します。Vary ヘッダーが存在しなければ、Content Gateway はドキュメントコンテンツタイプに従って、下記で指定されたヘッダーを変化させます。
Vary by Default on Text	テキストドキュメントの場合に、Content Gateway が変化させるヘッダーフィールドを指定します。
Vary by Default on Images	イメージの場合に、Content Gateway が変化させるヘッダーフィールドを指定します。
Vary by Default on Other Document Types	テキストとイメージ以外の場合に、Content Gateway が変化させるヘッダーフィールドを指定します。
Dynamic Caching: Caching Documents with Dynamic URLs	このオプションを有効にした場合、Content Gateway は、ダイナミックコンテンツをキャッシュしようとします。コンテンツが疑問符 (?)、セミコロン (;)、 cgi を含むか、または .asp で終了する場合、そのコンテンツはダイナミックと見なされます。 警告: 専用のプロキシが割り当てられている場合のみ、Content Gateway がダイナミックコンテンツをキャッシュするように設定することを推奨します。

オプション	説明
Dynamic Caching: Caching Response to Cookies	<p>クッキーを含む要求に対する応答がキャッシュされる方法を指定します。</p> <p>テキスト以外のすべてコンテンツタイプを含むクッキーをキャッシュする場合、[Cache All but Text] を選択します。これはデフォルトです。</p> <p>イメージを含む場合にのみクッキーをキャッシュする場合、[Cache Only Image Types] を選択します。</p> <p>どのコンテンツタイプでもクッキーをキャッシュする場合、[Cache Any Content-Type] を選択します。</p> <p>クッキーをキャッシュしない場合、[No Cache on Cookies] を選択します。</p>
Caching Policy/Forcing Document Caching	URL の特定のグループをキャッシュするかどうかを指定する <code>cache.config</code> ファイル内のルールの表を表示します。このファイルで、指定時間、特定の URL をキャッシュするよう強制できます。
Refresh	<code>cache.config</code> ファイルの最も最新のルールを表示するために、表を更新します。設定ファイル エディタで、ルールを追加 または 編集した後は、[Refresh] をクリックします。
Edit File	<code>cache.config</code> ファイルを編集、およびルールを追加するために、設定ファイル エディタを開きます。
	cache.config Configuration File Editor (cache.config 設定ファイル エディタ)
ルール表示ボックス	<code>cache.config</code> ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または上下に移動できます。
Add	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。
Set	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。

オプション	説明
Rule Type	<p>cache.config ファイルに追加できるルールのタイプをリストします。</p> <p>[never-cache] ルールは、特定のオブジェクトをキャッシュしないように、Content Gateway を設定します。</p> <p>[ignore-no-cache] ルールは、すべての Cache-Control: no-cache ヘッダーを無視するように、Content Gateway を設定します。</p> <p>[ignore-client-no-cache] ルールは、クライアント要求の Cache-Control: no-cache ヘッダーを無視するように、Content Gateway を設定します。</p> <p>[ignore-server-no-cache] ルールは、オリジン サーバー応答の Cache-Control: no-cache ヘッダーを無視するように、Content Gateway を設定します。</p> <p>[pin-in-cache] ルールは、指定時間の間、キャッシュにオブジェクトを残しておくように、Content Gateway を設定します。</p> <p>[revalidate] ルールは、指定時間の間、キャッシュ内のオブジェクトが最新であると見なすように、Content Gateway を設定します。</p> <p>[ttl-in-cache] ルールは、HTTP 要求 および 応答ヘッダー内のキャッシング指令に関係なく、[Time Period] フィールドで指定された時間、キャッシュからの HTTP オブジェクトを処理するように、Content Gateway を設定します。</p>
Primary Destination Type	<p>一次宛先タイプをリストします：</p> <p>[dest_domain] は 要求されたドメイン名。</p> <p>[dest_host] は 要求されたホスト名。</p> <p>[dest_ip] は 要求された IP アドレス。</p> <p>[url_regex] は URL に含まれる正規表現。</p>
Primary Destination Value	<p>一次宛先タイプの値を指定します。たとえば、Primary Destination Type が [dest_ip] の場合、このフィールドに 123.456.78.9 を選択できます。</p>
Additional Specifier: Time Period	<p>[revalidate]、[pin-in-cache]、および [ttl-in-cache] ルールタイプに適用する時間を指定します。次の時間形式で入力できます：</p> <p>d：日付（例 2d）</p> <p>h：時間（例 10h）</p> <p>m：分（例 5m）</p> <p>s：秒（例 20s）</p> <p>組み合わせ（例 1h15m20s）</p>
Secondary Specifiers: Time	<p>時間範囲（例、08:00-14:00）を指定します。</p>
Secondary Specifiers: Prefix	<p>URL のパス部分の接頭辞を指定します。</p>
Secondary Specifiers: Suffix	<p>URL のファイル接尾辞を指定します。</p>

オプション	説明
Secondary Specifiers: Source IP	クライアントの IP アドレスを指定します。
Secondary Specifiers:Port	要求された URL 中のポートを指定します。
Secondary Specifiers: Method	要求された URL メソッドを指定します。
Secondary Specifiers: Scheme	要求された URL のプロトコルを指定します。
Secondary Specifiers: User-Agent	要求ヘッダーのユーザー エージェントの値を指定します。
Apply	設定の変更を適用します。
Close	設定ファイル エディタ を終了します。 [Close] をクリックする前に、[Apply] をクリックします。そうでないと、設定変更は失われます。
	Privacy (プライバシー)
Insert Headers: Client-IP	有効にすると、クライアント IP アドレスを保持するために、Content Gateway は送信要求に Client-IP ヘッダーを挿入します。
Insert Headers: Via	有効にすると、Content Gateway は送信要求に Via ヘッダーを挿入します。
Insert Headers: X-Forwarded-For	有効にすると、Content Gateway は送信要求に X-Forwarded-For ヘッダーを挿入します。
Remove Headers: Client-IP	このオプションが有効な場合、ユーザーのプライバシーを保護するために、Content Gateway は送信要求から Client-IP ヘッダーを削除します。
Remove Headers: Cookie	このオプションが有効な場合、ユーザーのプライバシーを保護するために、Content Gateway は送信要求から Cookie ヘッダーを削除します。 Cookie ヘッダーは、しばしば要求を行ったユーザーを識別します。
Remove Headers: From	このオプションが有効な場合、ユーザーのプライバシーを保護するために、Content Gateway は送信要求から From ヘッダーを削除します。 From ヘッダーは、クライアントの電子メール アドレスを識別します。
Remove Headers: Referer	このオプションが有効な場合、ユーザーのプライバシーを保護するために、Content Gateway は送信要求から Referer ヘッダーを削除します。 Referer ヘッダーは、クライアントが選択した Web リンクを識別します。
Remove Headers: User-Agent	このオプションが有効な場合、ユーザーのプライバシーを保護するために、Content Gateway は送信要求から User-Agent ヘッダーを削除します。 User-Agent ヘッダーは、要求を行ったエージェント (通常はブラウザ) を識別します。
Remove Headers: Remove Others	ユーザーのプライバシーを保護するために、送信要求から削除する、 From 、 Referer 、 User-Agent 、および Cookie 以外のヘッダーを指定します。

オプション	説明
Timeouts (タイムアウト)	
Keep-Alive Timeouts: Client	<p>トランザクション終了後、後続の要求のために、クライアントとの接続を開きつづける時間(秒単位)を指定します。クライアント要求を受け入れるために Content Gateway が接続をオープンする度に、要求を処理した後、指定されたタイムアウト時間の間、接続を続けます。タイムアウト時間前にクライアントが他の要求を行った場合、Content Gateway は接続を閉じます。クライアントが他の要求を行った場合、タイムアウト時間は再開します。</p> <p>クライアントはいつでも接続を閉じることができます。</p>
Keep-Alive Timeouts: Origin Server	<p>トランザクション終了後、後続のデータ転送のために、オリジン サーバーへの接続を開き続ける時間(秒単位)を指定します。オリジン サーバーからデータをダウンロードするために、Content Gateway が接続をオープンする度に、データをダウンロードした後、指定されたタイムアウト時間の間、接続を続けます。タイムアウト時間前に後続のデータ要求が必要ない場合は、Content Gateway は接続を閉じます。その場合、タイムアウト時間は再開します。</p> <p>オリジン サーバーはいつでも接続を閉じることができます。</p>
Inactivity Timeouts: Client	<p>トランザクションが停止した場合に、Content Gateway がクライアントとの接続を開き続ける時間を指定します。Content Gateway がデータの受信を停止した場合や、クライアントがデータの読み込みを停止した場合、Content Gateway は、このタイムアウト時間が経過した後、接続を閉じます。</p> <p>クライアントはいつでも接続を閉じることができます。</p>
Inactivity Timeouts: Origin Server	<p>トランザクションが停止した場合に、Content Gateway がオリジン サーバーとの接続を開き続ける時間を指定します。Content Gateway が、オリジン サーバーからのデータ受信を停止した場合、このタイムアウト時間が経過するまで、接続を閉じません。</p> <p>オリジン サーバーはいつでも接続を閉じることができます。</p>
Active Timeouts: Client	<p>Content Gateway が、クライアントと接続されたままになる時間を指定します。このタイムアウト時間の前に、クライアントが要求(読み込み および 書き込みデータ)を完了していない場合、Content Gateway は接続を閉じます。</p> <p>デフォルト値の 0 は タイムアウトなしです。</p> <p>クライアントはいつでも接続を閉じることができます。</p>

オプション	説明
Active Timeouts: Origin Server Request	Content Gateway がオリジン サーバーへの接続要求の完了を待つ時間を指定します。 このタイムアウト時間の前に、Content Gateway がオリジン サーバーと接続を確立できなかった場合、Content Gateway は接続を終了します。 デフォルト値の 0 は タイムアウトなしです。 オリジン サーバーは いつでも接続を閉じることができます。
Active Timeouts: Origin Server Response	Content Gateway がオリジン サーバーからの応答を待つ時間を指定します。
FTP Control Connection Timeout	Content Gateway が FTP サーバーからの応答を待つ時間を指定します。指定した時間内に FTP サーバーが応答しない場合、Content Gateway はクライアントのデータ要求を破棄します。このオプションは、HTTP クライアントからの FTP 要求のみに適用されます。 デフォルト値は 300 です。

HTTP Responses (HTTP 応答)

オプション	説明
	General (一般)
Response Suppression Mode	Content Gateway は、特定のクライアント トランザクションで HTTP の問題 (利用できないオリジン サーバー、認証要件、プロトコル エラーなど) を検出した場合に、クライアント ブラウザに HTML 応答を送信します。Content Gateway には、HTTP エラーの詳細をクライアントに説明する変更不可のデフォルトの応答ページのセットがあります。 クライアントに HTTP 応答を送信しない場合、 [Always Suppressed] を選択します。 非透過的なトラフィックのみに HTTP 応答を送信する場合、 [Intercepted Traffic Only] を選択します。(Content Gateway が透過的に実行されていて、キャッシュの存在を示したくない場合に、このオプションは有効です。) すべてのクライアントに HTTP 応答を送信する場合、 [Never Suppressed] を選択します。 このオプションを変更した場合、Content Gateway を再起動する必要があります。

オプション	説明
	Custom (カスタム)
Custom Responses	<p>Content Gateway が クライアントに送信する応答をカスタマイズすることができます。デフォルトでは、カスタマイズ可能な応答は、Content Gateway の config/body_factory/default ディレクトリにあります。</p> <p>Accept-Language ヘッダーで指定された言語で、クライアントにカスタマイズされた応答を送信する場合、[Select Enabled Language-Targeted Response] を選択します。</p> <p>Select デフォルト ディレクトリにあるカスタマイズされた応答を送信する場合、[Enabled in "default" Directory Only] を選択します。</p> <p>カスタム応答を無効にする場合、[Disabled] を選択します。[Response Suppression Mode] オプションで、[Never Suppressed] または [Intercepted Traffic Only] が選択されている場合、Content Gateway は変更不可のデフォルトの応答を送信します。</p> <p>このオプションを変更した場合、Content Gateway を再起動する必要があります。</p>
Custom Response Logging	<p>有効にした場合、カスタム応答が使用 または変更された時に、Content Gateway はエラー ログにメッセージを送信します。</p> <p>このオプションを変更した場合、Content Gateway を再起動する必要があります。</p>
Custom Response Template Directory	<p>カスタム応答の位置するディレクトリを指定します。デフォルトの場所は、Content Gateway config/body_factory ディレクトリです。</p> <p>このオプションを変更した場合、Content Gateway を再起動する必要があります。</p>

HTTP Scheduled Update (HTTP スケジュール設定した更新)

オプション	説明
	General (一般)
Scheduled Update	Scheduled Update オプションを有効化 または 無効化します。このオプションを有効化した場合、Content Gateway は、指定した時間にローカル キャッシュ内の特定のオブジェクトを自動的に更新します。
Maximum Concurrent Updates	許容する同時更新要求の最大数を指定します。スケジュール設定した更新が、ホストに過大な負荷をかけないようにするために、このオプションを有効にします。デフォルト値は 100 です。
Retry on Update Error: Count	失敗した場合に、URL のスケジュール設定した更新を再試行する回数を入力します。デフォルト値は 10 回です。
Retry on Update Error: Interval	失敗した場合に、URL のスケジュール設定した各再試行間の間隔を秒単位で入力します。デフォルト値は 2 秒です。

オプション	説明
	Update URLs (URL 更新)
Force Immediate Update	有効にした場合、Content Gateway はすべてのスケジュール設定した更新の期限切れ時刻を上書きし、25 秒毎に更新を開始します。
Scheduled Object Update	Content Gateway が、指定したローカル キャッシュ コンテンツのスケジュール設定した更新を制御する方法を指定する <code>update.config</code> ファイル内のルールの表を表示します。
Refresh	<code>update.config</code> ファイルの最も最新のルールを表示するために、表を更新します。
Edit File	<code>update.config</code> ファイルを編集、および ルールを追加するために、設定ファイル エディタを開きます。
	update.config Configuration File Editor (update.config 設定ファイル エディタ)
ルール表示ボックス	<code>update.config</code> ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または 上下に移動できます。
Add	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。
Set	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。
URL	更新する URL を指定します。
Request Headers (オプション)	各 GET 要求で渡されたヘッダー (セミコロンで区切り) のリストを指定します。HTTP 仕様に準拠する任意の要求ヘッダーを指定できます。デフォルトは 要求ヘッダーはありません。
Offset Hour	更新時間を導出するために使用する基準時間を指定します。範囲は 00-23 時です。
Interval	更新が行われる (オフセット時間からの) 間隔 (秒)。
Recursion Depth	参照されている URL が再帰的に更新される (指定した URL からの) 深さ。たとえば、再帰の深さが 1 であれば、指定した URL と、元の URL からのリンクによって直接に参照されるすべての URL が更新されます。

HTTPS

オプション	説明
	General (一般)
HTTPS Proxy Server Port	Content Gateway が、HTTPS トラフィックの Web プロキシ サーバーとして動作する時に使用するポートを指定します。SSL Inbound Port とも言います。

オプション	説明
SSL Outbound Port	宛先に送られる前に、再暗号化のために HTTPS トラフィックが送られるポートを指定します。デフォルトは 8090 です。
Tunnel Skype	<p>HTTPS(SSL Manager) が有効であり、Content Gateway が明示的プロキシである場合に、Skype トラフィックのトンネリングを有効化 / 無効化します。</p> <p>設定を完了するには、Skype の使用を許可されたすべてのユーザーが、「インターネット電話」を許可するフィルタリング ポリシーを使用していることを確認します。SSL を有効化して Skype を使用するか否かに関わらず、これは必要です。</p> <p>また、Skype が禁止されていない場合、ハンドシェイクの後、Skype は非 HTTP ポートを使ってトラフィックをルーティングします。Content Gateway を経由するように Skype を強制するには、『Skype IT Administrators Guide』に記載されている通り、GPO を使用します。</p> <p>ご注意：SSL が有効化されていない場合、このオプションは必要ありません。</p> <p>ご注意：Content Gateway が透過的プロキシの場合、このオプションは無効です。</p>

FTP



ご注意

FTP 構成オプションは、「Configure」> 「My Proxy」> 「Basic」> 「General」タブの [Features] テーブルで FTP 処理を有効化した場合だけ、「Configure」ペインに表示されます。

オプション	説明
	General (一般)
FTP Proxy Server Port	Content Gateway が、FTP 要求を受け入れるために使用するポートを指定します。デフォルト ポートは 2121 です。
Listening Port Configuration	<p>データ転送のために FTP が開くリッスン ポートを指定します。</p> <p>[Default Settings] を選択すると、オペレーティング システムが使用可能なポートを選択します。Content Gateway は 0 を送信し、リッスンが成功すれば新しいポート番号を取得します。</p> <p>[Listening Port (Max)] および [Listening Port (Min)] フィールドで指定されたポート範囲によってリッスン ポートを決定する場合、[Specify Range] を選択します。</p>

オプション	説明
Default Data Connection Method	FTP サーバーとのデータ接続設定に使用するデフォルトの方法を指定します。 [Proxy Sends PASV] を選択すると、FTP サーバーに PASV を送信し、FTP サーバーはリスン ポートを開きます。 [Proxy Sends PORT] を選択すると、Content Gateway 側に最初の接続のリスン ポートをセットアップします。
Shared Server Connections	有効にすると、サーバー コントロール接続が、複数の匿名 FTP クライアントの間で共有されます。
	Timeouts (タイムアウト)
Keep-Alive Timeout: Server Control	どの FTP クライアントも FTP サーバー コントロール接続を使用しなくなった時の、タイムアウト値を指定します。デフォルト値は 90 秒です。
Inactivity Timeouts: Client Control	FTP クライアントコントロール接続のアイドル状態の持続時間を指定します。デフォルト値は 900 秒です。
Inactivity Timeouts: Server Control	FTP サーバーコントロール接続のアイドル状態の持続時間を指定します。デフォルト値は 120 秒です。
Active Timeouts: Client Control	FTP クライアントコントロール接続のオープン状態の持続時間を指定します。デフォルト値は 14400 秒です。
Active Timeouts: Server Control	FTP サーバーコントロール接続のオープン状態の持続時間を指定します。デフォルト値は 14400 秒です。

Content Routing (コンテンツルーティング)

Content Routing 設定オプションは、次のカテゴリに分けられます：

[Hierarchies \(階層\), 315 ページ](#)

[Mapping and Redirection \(マッピングおよびリダイレクト\), 318 ページ](#)

[Browser Auto-Config \(ブラウザ自動設定\), 320 ページ](#)

Hierarchies (階層)

オプション	説明
	Parenting (親)
Parent Proxy	HTTP 親キャッシング オプションを有効化 または 無効化します。このオプションを有効にした場合、Content Gateway を HTTP キャッシュ階層を組み込むことができます。Content Gateway サーバーを、親ネットワーク キャッシュ (他の Content Gateway サーバー または 別のキャッシング製品) に接続して、クライアント要求実行中に親キャッシュに依存する子キャッシュのキャッシュ階層形成できます。 HTTP キャッシュ階層, 93 ページ を参照してください。

オプション	説明
No DNS and Just Forward to Parent	このオプションを有効にした場合、HTTP 親キャッシュが有効になり、Content Gateway は 要求されたホスト名の DNS ルックアップを行いません。 選択された要求のみが親プロキシに送られるように、 parent.config ファイルのルールが設定されている場合、Content Gateway は、親プロキシに送られる要求のみ名前解決をスキップします。親プロキシに送られない要求は、通常通りに名前解決が実行されます。親プロキシが停止して、子プロキシが直接オリジン サーバーを参照できる場合、子プロキシは名前解決を実行します。
Uncacheable Requests Bypass Parent	このオプションが有効で、親キャッシングが有効な場合、Content Gateway は キャッシュできない要求の場合、親プロキシを迂回します。
HTTPS Requests Bypass Parent	このオプションが有効にすると、Content Gateway は HTTPS 要求の場合に 親プロキシを迂回します。
Tunnel Requests Bypass Parent	このオプションが有効にすると、Content Gateway は 非 HTTPS トンネル要求の場合に 親プロキシを迂回します。
Parent Proxy Cache Rules	HTTP キャッシュ階層で使用される HTTP 親プロキシを指定し、選択された URL 要求が親プロキシを迂回するように設定された parent.config ファイルのルールの表を表示します。ルールはリストの上から順にチェックされ、最初に条件に一致するルールが適用されます。
Refresh	parent.config ファイルの最も最新のルールを表示するために、表を更新します。
Edit File	parent.config ファイルを編集、および ルールを追加するために、設定ファイル エディタを開きます。 parent.config Configuration File Editor (parent.config 設定ファイル エディタ)
ルール表示ボックス	parent.config ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または 上下に移動できます。
Add	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。
Set	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。
Primary Destination Type	一次宛先タイプをリストします： [dest_domain] は 要求されたドメイン名。 [dest_host] は 要求されたホスト名。 [dest_ip] は 要求された IP アドレス。 [url_regex] は URL に含まれる正規表現。

オプション	説明
Primary Destination Value	一次宛先タイプの値を指定します。 例： 一次宛先が <code>dest_domain</code> の場合 このフィールドの値に <code>yahoo.com</code> を選択できます。 一次宛先タイプが <code>dest_ip</code> の場合、このフィールドに <code>123.456.78.9</code> を選択できます。 一次宛先が <code>url_regex</code> の場合 このフィールドの値に <code>politics</code> を選択できます。
Parent Proxies	親プロキシの IP アドレス または ホスト名、通信に使用するポート番号を指定します。親プロキシは リスト内で指定された順序に従って問い合わせを受けます。リスト内の最後の親サーバーによって要求が処理されなかった場合、オリジンサーバーにルーティングされます。各エントリはセミコロンで区切ります。例： <code>parent1:8080;</code> <code>parent2:8080</code>
Round Robin	プロキシがクライアント IP アドレスに基づいたラウンドロビン内の親キャッシュ リストを経由する場合、 <code>[true]</code> を選択します。 プロキシが厳格に順番どおりに要求を処理するためには、 <code>[strict]</code> を選択します。たとえば、コンピュータ <code>proxy1</code> が最初の要求を処理し、 <code>proxy2</code> が 2 番目の要求を処理するなど。 ラウンド ロビン選択を発生させたくない場合、 <code>[false]</code> を選択します。
Go direct	<code>[true]</code> を選択すると、要求が親階層を迂回して、直接オリジンサーバーに向かいます。 要求が親階層を迂回することを望まない場合、 <code>[false]</code> を選択します。
Secondary Specifiers: Time	08:00-14:00 等の 24 時間クロックを使用して、時間範囲を指定します。範囲が午前 0 時をまたぐ場合、2 つのカンマ区切りの範囲を入力します。たとえば、範囲が午後 6:00 から午前 8:00 の場合、次のように入力します： <code>18:00 - 23:59, 0:00 - 8:00</code>
Secondary Specifiers: Prefix	URL のパス部分の接頭辞を指定します。
Secondary Specifiers: Suffix	<code>.htm</code> 、 <code>.gif</code> 等の URL のファイル接尾辞を指定します。
Secondary Specifiers: Source IP	クライアントの IP アドレス または IP アドレス範囲を指定します。
Secondary Specifiers:Port	要求された URL 中のポートを指定します。
Secondary Specifiers: Method	要求された URL メソッドを指定します。例： <ul style="list-style-type: none"> • <code>get</code> • <code>post</code> • <code>put</code> • <code>trace</code>

オプション	説明
Secondary Specifiers: Scheme	要求された URL のプロトコルを指定します。HTTP か FTP である必要があります。
Secondary Specifiers: User-Agent	要求ヘッダーのユーザー エージェントの値を指定します。

Mapping and Redirection (マッピングおよびリダイレクト)

オプション	説明
Serve Mapped Hosts Only	<i>remap.config</i> ファイルのマッピングのルールにリストされたオリジン サーバーへの要求のみをプロキシに処理させる場合、[Required] を選択します。要求が <i>remap.config</i> ファイルのルールに一致しない場合、ブラウザはエラーを受け取ります。このオプションは Content Gateway システムのセキュリティを強化します。
Retain Client Host Header	このオプションが有効な場合、Content Gateway は 要求内のクライアント ホスト ヘッダーを保持します (マッピング変換内のクライアント ホスト ヘッダーは含みません)。
Redirect No-Host Header to URL	Host: ヘッダーを提供しない旧バージョンのクライアントからの着信要求をリダイレクトする代替 URL を指定します。状態をユーザーに説明し、ブラウザのアップグレードを指示するか、プロキシを迂回するオリジン サーバーへの直接のリンクを提供するページを設定することが推奨されます。代わりに、Host: ヘッダーのない要求を特定のサーバーにマップするマップ ルールを指定することもできます。
URL Remapping Rules	オリジン サーバーに接続せずに、永久的または一時的に HTTP 要求をリダイレクトする <i>remap.config</i> ファイルのマッピング ルールのテーブルを表示します。 ご注意: URL を同じドメインの別の URL にマッピングする場合、[From Path Prefix] フィールドに "/" を指定する必要があります。このテーブルの後の例を参照してください。
Refresh	<i>remap.config</i> ファイルの最も最新のルールを表示するために、表を更新します。
Edit File	<i>remap.config</i> ファイルを編集、および ルールを追加するために、設定ファイル エディタを開きます。 remap.config Configuration File Editor (remap.config 設定ファイル エディタ)
ルール表示ボックス	<i>remap.config</i> ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または上下に移動できます。
Add	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。
Set	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。

オプション	説明
Rule Type	<p>remap.config ファイルに追加できるルールのタイプをリストします。</p> <p>[redirect] は、オリジン サーバーに接続せずに、永久的に HTTP 要求をリダイレクトします。永久的リダイレクトは、(HTTP ステータス コード 301 を返すことで) URL 変更をブラウザに通知しますので、ブラウザはブックマークを更新できます。</p> <p>[redirect temporary] は、オリジン サーバーに接続せずに、一時的に HTTP 要求をリダイレクトします。一時的リダイレクトは、(HTTP ステータス コード 307 を返すことで) 現在の要求のみの URL 変更をブラウザに通知します。</p>
From Scheme	<p>マッピング ルールのプロトコルを指定します。“rtsp” および “mms” はサポートされていません。</p> <p>ご注意: あるプロトコル(スキーム)の URL を別のプロトコル(スキーム)にマッピングすることは、サポートされていません。</p>
From Host	マップ元の URL のホスト名を指定します。
From Port (オプション)	マップ元の URL のポート番号を指定します。
From Path Prefix (オプション)	マップ元の URL のパス接頭辞を指定します。
To Host	マップ先の URL のホスト名を指定します。
To Port (オプション)	マップ先の URL のポート番号を指定します。
To Path Prefix (オプション)	マップ先の URL のパス接頭辞を指定します。
{undefined}	マッピング ルールのメディア プロトコル タイプを指定します。サポートされていません。

URL を同じドメインのサブ ページにリダイレクトしたい場合があります。たとえば、“www.cnn.com” を “www.cnn.com/tech” にリダイレクトする。このルールを動作させるためには、[From Path Prefix] フィールドに “/” を指定する必要があります。もし指定しなければ、再帰的にページ指定子が URL に追加されます。たとえば、“www.cnn.com/tech” は “www.cnn.com/tech/tech/tech/tech/tech/tech/tech/tech/..” になります。

Browser Auto-Config (ブラウザ自動設定)

オプション	説明
	PAC
Auto-Configuration Port	Content Gateway が、自動設定ファイルをブラウザにダウンロードするポートを指定します。このポートは他のすべてのプロセスに割り当てることはできません。デフォルトポートは 8083 です。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
PAC Settings	PAC ファイル (proxy.pac) を編集します。 PAC ファイルの使用, 42 ページ を参照してください。
	WPAD
WPAD Settings	wpad.dat ファイルを編集します。 WPAD の使用, 44 ページ を参照してください。

Security (セキュリティ)

Security 設定オプションは、次のカテゴリに分けられます：

[Connection Control \(接続の制御\), 320 ページ](#)

[FIPS Security \(FIPS セキュリティ\), 321 ページ](#)

[Data Security, 322 ページ](#)

[Access Control \(アクセス制御\), 323 ページ](#)

[SOCKS, 334 ページ](#)

Connection Control (接続の制御)

オプション	説明
	Proxy Access (プロキシ アクセス)
Access Control	どのクライアントが Content Gateway にアクセスできるかを制御する ip_allow.config ファイルのルールを表示します。 デフォルトでは、すべてのリモートホストはプロキシへのアクセスを許可されています。
Refresh	ip_allow.config ファイルの最も最新のルールを表示するために、表を更新します。
Edit File	ip_allow.config ファイルを編集するために、設定ファイル エディタを開きます。

オプション	説明
	ip_allow.config Configuration File Editor (ip_allow.config 設定ファイル エディタ)
ルール表示ボックス	<i>ip_allow.config</i> ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または上下に移動できます。
Add	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。
Set	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。
IP Action	追加できるルールのタイプをリストします。 [ip_allow] ルールは、[Source IP] フィールドにリストされたクライアントが、プロキシにアクセスすることを許可します。 [ip_deny] ルールは、[Source IP] フィールドにリストされたクライアントが、プロキシにアクセスすることを拒否します。
Source IP	クライアントの IP アドレス または IP アドレス範囲を指定します。
Apply	設定の変更を適用します。
Close	設定ファイル エディタ を終了します。 [Close] をクリックする前に、[Apply] をクリックします。そうでないと、設定変更は失われます。

FIPS Security (FIPS セキュリティ)

このオプションは HTTPS トラフィック および FIPS 140-2 暗号化標準に関連しています。

デフォルトでは、HTTPS トラフィックを処理する場合、Content Gateway は SSLv2 および SSLv3 等のプロトコルを使用して接続を受け入れます。

FIPS オプションを有効にすると、TLSv1 および FIP 140-2 によって承認されたアルゴリズムを使用する HTTPS 接続を受け入れるように、Content Gateway を制限します。



警告

一度有効にすると、Content Gateway を再インストールしないと、FIPS 140-2 モードを無効にできません。Content Gateway がアプライアンス上にある場合、アプライアンスを再構成しなければなりません。

詳細情報は、[FIPS 140-2 モード](#), 187 ページを参照してください。

オプション	説明
FIPS Enable/Disable ラジオ ボタン	<p>デフォルトでは、Content Gateway は 非 FIPS 140-2 モードでインストールされます。</p> <p>FIPS 140-2 モードに切り替えるためには、[Enabled] ラジオ ボタンを選択し、[Apply] をクリックし、Content Gateway を再起動します。</p> <p>ご注意: 一度有効にすると、Content Gateway を再インストールしないと、FIPS 140-2 モードを無効にできません。Websense アプライアンス インストールの場合、再インストールは システムの再構成を必要とします。</p>

Data Security



ご注意

Data Security 設定オプションは、次を所有している場合のみ、「Configure」ペインに表示されます：

- ◆ Web Security Gateway Anywhere サブスクリプション、およびそのキーが TRITON Web Security に入力されていること。
- ◆ 「Configure」 > 「My Proxy」 > 「Basic」 > 「General」 タブの [Data Security] を有効にし、[Features] テーブルの [Integrated on-box] を選択します。

オプション	説明
Data Security IP address	Data Security Management Server の IP アドレスを指定します。これは、Websense Data Security ポリシーの構成と管理が実行される場所です。
Analyze HTTPS Content (HTTPS コンテンツを分析)	復号化したトラフィックを分析のために、Websense Data Security に送信するか、または宛先の直接に送信するかを指定します。
Analyze FTP Uploads (FTP アップロードを分析)	FTP アップロード要求を分析のために、Websense Data Security に送信するかどうかを指定します。FTP プロキシ機能を有効化する必要があります。 FTP, 314 ページ を参照してください。

登録画面フィールド：

オプション	説明
Data Security IP address	Data Security Management Server の IP アドレスを指定します。これは、データセキュリティポリシーの構成と管理が実行される場所です。
Data Security Manager user name	Websense Data Security 管理者のアカウント名を指定します。管理者には 配備設定権限が必要です。
Data Security Manager user name	Websense Data Security 管理者のパスワードを指定します。
Register ボタン	登録を開始します。すべてのフィールドにデータが入力された後、このボタンが有効になります。

Access Control (アクセス制御)

Access Control タブを次のように使用します：

- ◆ カスタム フィルタリング ルールを作成します
- ◆ プロキシ ユーザー認証を設定します

「Access Control」 ページ上の *Filtering* タブは常に使用可能です。

Transparent Proxy Authentication タブも常に存在します。しかし、Content Gateway が 透過的プロキシとして配備された場合にのみ適用されます。

その他のタブは、「Configure」>「My Proxy」の「Authentication」セクションで選択された認証方法に基づいて、動的に変化します。

Integrated Windows Authentication (統合 Windows 認証) が選択された場合、次のタブが表示します：

- Integrated Windows Authentication
- Global Authentication Options (NTLM に適用)

LDAP が選択された場合、次のタブが表示します：

- LDAP

Radius が選択された場合、次のタブが表示します：

- Radius

Legacy NTLM が選択された場合、次のタブが表示します：

- NTLM

Multiple Realm Authentication (複数レルム認証) が選択された場合、次のタブが表示します：

- Domains
- Authentication Realms
- Global Authentication Options

下記の表は各タブの各フィールドの目的を説明しています。お探しのフィールドを見つけるために、ブラウザの検索機能を使用することをお勧めします。

Content Gateway ユーザー認証機能の詳細は、[プロキシ ユーザー認証, 197 ページ](#)を参照してください。

オプション	説明
	Filtering
Filtering	<p><i>filter.config</i> のルールをリストするテーブルを表示します。ルールはリストの上から下へ辿り、最初に条件に一致するルールが適用されます。条件に一致するルールがない場合、要求は処理されます。</p> <p>フィルタリング ルールのの目的の詳細は、フィルタリングルール, 188 ページを参照してください。</p> <p>ご注意: ルールを追加、削除または変更した後は、Content Gateway を再起動してください。</p> <p>ご注意: NTLM および LDAP 認証ルールは、「Authentication Realms」タブで定義されており、<i>auth.config</i> ファイルに保存されています(この表で後のエントリを参照)。</p>
Refresh	filter.config ファイルの最も最新のルールを表示するために、表を更新します。
Edit File	filter.config ファイルを編集するために、設定ファイル エディタを開きます。
	filter.config Configuration File Editor (filter.config 設定ファイル エディタ)
ルール表示ボックス	<i>filter.config</i> に現在保存されているルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または上下に移動できます。
Add	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。ルールを選択 または 値を入力した後、[Add] クリックします。
Set	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。

オプション	説明
Rule Type	<p>ルール タイプを指定します。</p> <p>[allow] を選択すると、特定の URL 要求が認証をバイパスすることを許可します。プロキシは要求されたコンテンツをキャッシュし、提供します。</p> <p>[deny] を選択すると、特定の宛先からのオブジェクトの要求を拒否します。要求が拒否されたとき、クライアントはアクセス拒否メッセージを受け取ります。</p> <p>どのクライアント要求ヘッダ情報を保持するかを指定するためには、[keep_hdr] を選択します。</p> <p>どのクライアント要求ヘッダ情報を削除するかを指定するためには、[strip_hdr] を選択します。</p> <p>要求にカスタム ヘッダーを追加するには、[add_hdr] を選択します。このルールタイプは、[Custom Header] および [Header Value] で定義された値を必要とします。宛先ドメインの特定の要求に対応するために、カスタムヘッダーを追加します。フィルタリングルール, 188 ページを参照してください。</p> <p>ご注意: “radius” ルールタイプはサポートされていません。</p>
Primary Destination Type	<p>一次宛先タイプをリストします:</p> <p>[dest_domain] は 要求されたドメイン名。</p> <p>[dest_host] は 要求されたホスト名。</p> <p>[dest_ip] は 要求された IP アドレス。</p> <p>[url_regex] は URL に含まれる正規表現。</p>
Primary Destination Value	<p>一次宛先タイプの値を指定します。たとえば、一次宛先タイプが [dest_ip] の場合、このフィールドに 123.456.78.9 を選択できます。</p>
Additional Specifiers: Header Type	<p>保持または削除するクライアント要求ヘッダ情報を指定します。</p> <p>このオプションは、[keep_hdr] または [strip_hdr] ルールタイプにのみ適用されます。</p>
Additional Specifiers: Realm (オプション)	<p>サポートされていません。</p>
Additional Specifiers: Proxy Port (オプション)	<p>このルールに一致するプロキシ ポートを指定します。</p>
Additional Specifiers: Custom Header (オプション)	<p>ルールタイプが [add_hdr] の場合に使用します。宛先ドメインが要求内で検索するカスタム ヘッダー名を指定します。</p>
Additional Specifiers: Header Value (オプション)	<p>ルールタイプが [add_hdr] の場合に使用します。宛先ドメインがカスタム ヘッダーと組になるカスタム ヘッダー値を指定します。</p>
Secondary Specifiers: Time	<p>時間範囲 (例、08:00-14:00) を指定します。</p>
Secondary Specifiers: Prefix	<p>URL のパス部分の接頭辞を指定します。</p>
Secondary Specifiers: Suffix	<p>URL のファイル接尾辞を指定します。</p>

オプション	説明
Secondary Specifiers: Source IP	クライアントの IP アドレスを指定します。
Secondary Specifiers:Port	要求された URL 中のポートを指定します。
Secondary Specifiers: Method	要求の URL メソッドを指定します : <ul style="list-style-type: none"> - get - post - put - trace
Secondary Specifiers: Scheme	要求された URL のプロトコルを指定します。Options are: <ul style="list-style-type: none"> - HTTP - HTTPS - FTP (FTP over HTTP のみ) ご注意: rtsp および mms は サポートされません。
Secondary Specifiers: User-Agent	要求ヘッダーのユーザー エージェントの値を指定します。 このフィールドを、次のアプリケーション フィルタリング ルールを作成するために使用します : <ul style="list-style-type: none"> • 認証の要求を適切に処理しないアプリケーションが認証をバイパスすることを許可する • 指定のクライアントベースのアプリケーションからのインターネットのアクセスを禁止する
Apply	設定の変更を適用します。
Close	設定ファイル エディタ を終了します。 [Close] をクリックする前に、 [Apply] をクリックします。 そうでないと、設定変更は失われます。
Integrated Windows Authentication (統合 Windows 認証)	
統合 Windows 認証ページは、「 Configure 」>「 My Proxy 」>「 Basic 」>「 General 」タブの [Features] テーブルで IWA を有効化した場合だけ表示されます。 Windows ドメインと結合するか、または 結合を解除するために、このページを使用します。ドメインが結合されている場合、このページにはドメイン属性の要約と [Unjoin] ボタンが表示されます。 統合 Windows 認証, 201 ページ を参照してください。	
Domain Name	完全修飾 Windows ドメイン名を指定します。
Administrator Name	Windows Administrator のユーザー名を指定します。
Administrator Password	Windows Administrator のパスワード指定します。 ご注意: 名前とパスワードは結合時のみ使用し、保存されません。

オプション	説明
Domain Controller	<p>ドメイン コントローラを見つける方法を指定します。</p> <ul style="list-style-type: none"> • DNS による自動検出 • DC 名と IP アドレス <p>ドメイン コントローラが名前 または IP アドレスによって指定されている場合、カンマ区切り形式のリストでバックアップ ドメイン コントローラも指定できます。</p>
Content Gateway Hostname	<p>Content Gateway のホスト名を指定します。</p> <p>IWA は、Kerberos に登録する時に ホスト名を NetBIOS 名として使用するため、ホスト名長は 15 文字を超えることができません (NetBIOS の制限)。また、V-Series はモジュール (Dom) 間で一意的であることを保障するために、ホスト名に 4 文字付加します。V-Series アプライアンス上では、ホスト名は 11 文字を超えることができません。</p> <p>重要: 一度ホスト名と結合されたドメインは変更できません。もしそうした場合、ドメインの結合を解除して、新しいホスト名と再結合するまで、IWA は 即座に動作を停止します。</p>
Join Domain	ドメインを結合するには、[Join Domain] をクリックします。
	<p>Global Authentication Options (グローバル認証オプション)</p> <p>Integrated Windows Authentication が NTLM 認証を実行するときに適用されるオプション設定するために、このページを使用します。</p>
Fail Open	<p>有効に設定されている場合、認証が下記の理由で失敗した場合に、要求の処理を続行することが許可されます：</p> <ul style="list-style-type: none"> • ドメイン コントローラからの応答がない • クライアントからのメッセージの形式が正しくない • SMB 応答が不適切 <p>ご注意: パスワード認証が失敗した場合は、続行されません。</p>
NTLM Credential Caching	NTLM 認証後の ユーザー証明書のキャッシングを有効化または 無効化します。Content Gateway が明示的プロキシの場合にのみ適用されます。
Caching TTL	キャッシュ内のエントリの継続時間 (TTL) を指定します。デフォルトは 900 秒 (15 分) です。
Multi-user IP Exclusions	端末サーバー等の複数のユーザーをホストするネットワークシステムの IP アドレス、および IP アドレス範囲をカンマ区切りのリストで指定します。

オプション	説明
	<p>Transparent Proxy Authentication</p> <p>Content Gateway が透過的プロキシの場合、このページを使用します。詳細情報は、透過的プロキシ認証の設定、200 ページを参照してください。</p>
Redirect Hostname (オプション)	<p>DSN によりネットワーク上のすべてのクライアントを解決できるプロキシの代替ホスト名を指定します。</p> <p>ご注意 統合 Windows 認証 (IWA) ではリダイレクトホスト名は不必要であり、適用されません。</p>
Authentication Mode	<p>透過的プロキシ認証が設定されている場合、Content Gateway は認証モードを設定する必要があります。</p> <ul style="list-style-type: none"> • [IP mode] (デフォルト) では、セッションが認証された時に、クライアント IP アドレスとユーザー名を関連付けます。その IP アドレスからの要求は、[Session TTL] の期限まで再認証されません。デフォルトは 15 分です。 • [Cookie Mode] は、1 つの IP アドレス - たとえばプロキシチェイニング環境内、もしくはネットワークアドレス変換 (NAT) が行われる環境 - を共有する複数のユーザーを一意に識別するために使用します。
Session TTL	<p>クライアントが再認証を必要とするまでの時間を分単位で指定します。IP モード および Cookie モード両方で必要です。デフォルトは 15 分です。有効な値の範囲は 5 - 65535 分です。</p>
	<p>LDAP</p> <p>LDAP 構成オプションは、「Configure」 > 「My Proxy」 > 「Basic」 > 「General」 タブの [Features] テーブルで LDAP を有効化した場合だけ、「Configure」ペインに表示されます。</p> <p>LDAP の設定の詳細は、LDAP 認証、210 ページを参照してください。</p>
Purge Cache on Authentication Failure	<p>このオプションを有効にした場合、Content Gateway は認証が失敗した時に LDAP キャッシュ内の認証エントリを削除します。</p>
LDAP Server: Hostname	<p>LDAP サーバーのホスト名を指定します。</p> <p>このオプションを変更した場合、Content Gateway を再起動する必要があります。</p>
LDAP Server:Port	<p>LDAP 通信に使用するポートを入力します。デフォルトのポート番号は 389 です。</p> <p>このオプションを変更した場合、Content Gateway を再起動する必要があります。</p>
LDAP Server: Secure LDAP	<p>Content Gateway が、LDAP サーバーとの通信にセキュアな通信を使用するかどうかを指定します。有効にすると、LDAP の [Port] フィールド (上記) が 636 または 3269 (セキュア LDAP ポート) に設定されます。</p>
LDAP Server: Server Type	<p>検索フィルタを指定します。Active Directory または他のディレクトリサービスを指定します。</p>

オプション	説明
LDAP Server: Bind Distinguished Name	LDAP ベースのディレクトリ サービスのユーザーの完全識別名 (完全修飾名) を指定します。例: CN=John Smith,CN=USERS,DC=MYCOMPANY, DC=COM このフィールドには最大 128 文字まで入力できます。 このフィールドで値を指定しない場合、プロキシは匿名のバインドを試みます。
LDAP Server: Password	[Bind_DN] フィールドに識別されるユーザーのパスワードを指定します。
LDAP Server: Base Distinguished Name	ベース識別名 (DN) を指定します。この値は LDAP 管理者から取得します。 正しいベース識別名 (DN) を指定する必要があります。 そうでない場合は、LDAP 認証は機能しません。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Radius	
Radius 構成オプションは、「 Configure 」>「 My Proxy 」>「 Basic 」>「 General 」タブの [Features] テーブルで Radius を有効化した場合だけ、「Configure」ペインに表示されます。 Radius の設定の詳細は、 RADIUS 認証, 213 ページ を参照してください。	
Primary Radius Server: Hostname	プライマリ RADIUS 認証サーバーのホスト名 または IP アドレスを指定します。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Primary Radius Server:Port	Content Gateway がプライマリ RADIUS 認証サーバーとの通信に使用するポートの番号を指定します。デフォルトポートは 1812 です。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Primary Radius Server: Shared Key	暗号化に使用するキーを指定します。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Secondary Radius Server (optional): Hostname	セカンダリ RADIUS 認証サーバーのホスト名または IP アドレスを指定します。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Secondary Radius Server (オプション):Port	Content Gateway がセカンダリ RADIUS 認証サーバーとの通信に使用するポートの番号を指定します。デフォルトポートは 1812 です。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Secondary Radius Server (オプション): Shared Key	暗号化に使用するキーを指定します。 このオプションを変更した場合、Content Gateway を再起動する必要があります。

オプション	説明
	<p>Legacy NTLM</p> <p>NTLM 構成オプションは、「Configure」>「My Proxy」>「Basic」>「General」タブの [Features] テーブルで NTLM を有効化した場合だけ、「Configure」ペインに表示されます。</p> <p>NTLM の設定の詳細は、レガシー NTLM 認証, 207 ページを参照してください。</p>
<p>Domain Controller Hostnames</p>	<p>カンマ区切り形式のリストで ドメイン コントローラの ホスト名を指定できます。形式は下記の通りです。</p> <p>host_name[:port][%netbios_name]</p> <p>または</p> <p>IP_address[:port][%netbios_name]</p> <p>Active Directory 2008 を使用している場合、netbios_name を含めるか、SMB ポート 445 を使用しなければなりません。</p> <p>このオプションを変更した場合、Content Gateway を再起動する必要があります。</p>
<p>Load Balancing</p>	<p>ロード バランシングを有効化または無効化します。有効にすると、Content Gateway は、ドメイン コントローラに認証要求を送信するときに、ロード バランシングを処理します。</p> <p>ご注意: 複数のドメイン コントローラが指定されている時には、ロード バランスが無効化されている場合でも、プライマリドメイン コントローラの負荷が許可されている最大の接続数に達したとき、一時的なフェールオーバーの方法として、新しい要求はセカンダリドメイン コントローラに送信されます。これはプライマリドメイン コントローラが新しい接続を受け入れられるようになるまで継続されます。</p> <p>このオプションを変更した場合、Content Gateway を再起動する必要があります。</p>
<p>Fail Open</p>	<p>有効に設定されている場合、認証が下記の理由で失敗した場合に、要求の処理を続行することが許可されます:</p> <ul style="list-style-type: none"> • ドメイン コントローラからの応答がない • クライアントからのメッセージの形式が正しくない • SMB 応答が不適切 <p>ご注意: パスワード認証が失敗した場合は、続行されません。</p>
<p>IP Credentials: Credential caching</p>	<p>NTLM 資格情報キャッシュを有効化 または 無効化します。Content Gateway が明示的プロキシの場合にのみ適用されます。</p>
<p>IP Credentials: Caching TTL</p>	<p>NTLM 資格情報キャッシュの継続時間(秒単位)を指定します。デフォルトは 900 秒(15 分)です。サポートする範囲は、300 から 86400 秒です。</p>
<p>IP Credentials: Multi-user IP Exclusions</p>	<p>端末サーバー、NAT ファイアウォール等のマルチユーザーの IP アドレス、および IP アドレス範囲をカンマ区切りのリストで指定します。</p> <p>このようなユーザーの資格情報はキャッシュされません。</p>
	<p>Domains (ドメイン)</p>

オプション	説明
	<p>「Configure」>「My Proxy」>「Basic」>「General」タブの [Features] テーブルで [Multiple Realm Authentication] を有効化した場合だけ、アクセス制御リストに「Domains」ページが表示されます。</p> <p>認証ルールの作成するドメインを結合するために、このタブを使用します。</p> <p>複数レルムの認証の詳細は、複数レルムの認証, 216 ページを参照してください。</p>
Domain Name	完全修飾 Windows ドメイン名を指定します。
Administrator Name	Windows Administrator のユーザー名を指定します。
Administrator Password	Windows Administrator のパスワード指定します。 ご注意: 名前とパスワードは結合時にのみ使用し、保存されません。
Domain Controller	<p>ドメイン コントローラを見つける方法を指定します。</p> <ul style="list-style-type: none"> • DNS による自動検出 • DC 名と IP アドレス <p>ドメイン コントローラが名前 または IP アドレスによって指定されている場合、カンマ区切り形式のリストでバックアップ ドメイン コントローラも指定できます。</p>
Content Gateway Hostname	<p>Content Gateway のホスト名を指定します。</p> <p>IWA は、Kerberos に登録する時に ホスト名を NetBIOS 名として使用するため、ホスト名長は 15 文字を超えることができません (NetBIOS の制限)。また、V-Series はモジュール (Dom) 間で一意であることを保障するために、ホスト名に 4 文字付加します。V-Series アプリアンス上では、ホスト名は 11 文字を超えることができません。</p> <p>重要: 一度ホスト名と結合されたドメインは変更できません。もしそうした場合、ドメインの結合を解除して、新しいホスト名と再結合するまで、IWA は 即座に動作を停止します。</p>
Join Domain	ドメインを結合するには、[Join Domain] をクリックします。
Joined Domains list	結合されたドメインのリストを表示します。
Unjoin Domain ボタン	ドメインの結合を解除するには、ドメインを選択し ボタンをクリックします。
Realm Name	結合ドメイン リストで選択されたドメインの名前を表示します。
Fully Qualified Domain Name	結合ドメイン リストで選択されたドメインの FQDN を表示します。
Content Gateway Hostname	Integrated Windows Authentication(Kerberos) が設定されている場合に、ブラウザ プロキシ設定セクションで指定されている、クライアントブラウザが使用するホスト名を表示します。

オプション	説明
Domain Controller	<p>選択されたドメイン コントローラを見つける方法を指定します。</p> <ul style="list-style-type: none"> • DNS による自動検出 • DC 名と IP アドレス <p>ドメイン コントローラが名前または IP アドレスによって指定されている場合、カンマ区切り形式のリストでバックアップ ドメイン コントローラも指定できます。</p>
Multiple Realm Authentication (複数レルム認証)	
<p>複数のレルム (ドメインは相互に信頼関係接続共有していない) のネットワークでは、指定のドメイン コントローラへ転送する IP アドレスのセットのルールを定義できます。</p> <p>詳細情報は、複数レルムの認証, 216 ページを参照してください。</p>	
Authentication	<p>認証のために、指定の IP アドレスを特定のドメイン コントローラへ転送する <code>auth.config</code> ファイルのルールを表示します。明示のプロキシ設定では、特定のポートへのインバウンド トラフィックに対するルールを作成することができます。</p> <p>IWA、LDAP および NTLM のルールを設定できます。</p>
Refresh	<p><code>auth.config</code> ファイルの現在のルールを表示するために、表を更新します。</p>
Edit File	<p><code>auth.config</code> ファイルを編集するために、設定ファイル エディタを開きます。</p>
auth.config Configuration File Editor (auth.config 設定ファイル エディタ)	
ルール表示ボックス	<p><code>auth.config</code> ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または上下に移動できます。</p>
Add	<p>設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。</p>
Set	<p>設定ファイル エディタ ページの上部のルール表示ボックスを更新します。</p>
Rule Type	<p>ルール タイプを指定します。</p> <p>Kerberos にルールを適用する場合、[Integrated Windows Authentication] を選択します。</p> <p>NTLMSSP に適用するルールを指定する場合、[Legacy NTLM] を選択します。</p> <p>LDAP で使用するルールを指定する場合、[LDAP] を選択します。</p>
Status	<p>ルールを保存し Content Gateway が再起動された後、ルールを有効にするか、無効にするかを指定します。</p>
Rule Name	<p>ルールのわかりやすい名前を指定します (一意でなければなりません)。</p>

オプション	説明
Source IP	このルールの IP アドレス、または IP アドレス範囲を指定します (スペースを含めないでください)。 例: 10.1.1.1 または 0.0.0.0-255.255.255.255 または 10.1.1.1,20.2.2.2,3.0.0.0-3.255.255.255
Proxy Port	Content Gateway が明示のプロキシとして配備されている時のトラフィックのインバウンドポートを指定します。
Advanced Settings: Aliasing	このルールに一致したすべてのユーザーを Filtering Service に送信する別名を指定します。別名は静的である必要があります。空白 (ブランク) にすることができません。別名はプライマリドメインコントローラに存在している必要があります (DC はフィルタリング サービスから認識される)。
IWA Specifiers: Domain/Realm	ルールを適用するドメイン (レルム) を指定します。
NTLM Specifiers: DC List	プライマリドメインコントローラの IP アドレスとポート番号を指定します (ポート番号を指定しない場合、Content Gateway はポート 139 を使用します)。続けて、カンマ区切り形式のリストで、ロードバランシングおよびフェールオーバーに使用するセカンダリドメインコントローラを指定します。
NTLM Specifiers: DC Load Balance	ロードバランシングを使用するかどうかを指定します: <ul style="list-style-type: none"> • 0 = 無効 • 1 = 有効 ご注意: 複数のドメインコントローラが指定されている時には、ロードバランスが無効化されている場合でも、プライマリドメインコントローラの負荷が許可されている最大の接続数に達したとき、一時的なフェールオーバーの方法として、新しい要求はセカンダリドメインコントローラに送信されます。これはプライマリドメインコントローラが新しい接続を受け入れられるようになるまで継続されます。
LDAP Specifiers: LDAP Server Name	LDAP サーバー名を指定します。 このオプションは、ldap ルールタイプにのみ適用されます。
LDAP Specifiers: LDAP Server Port	LDAP サーバーポートを指定します (オプション - デフォルト 389)。
LDAP Specifiers: LDAP Base Distinguished Name	LDAP ベース識別名を指定します。 このオプションは、ldap ルールタイプにのみ適用されます。
LDAP Specifiers: Server Type	Active Directory の場合、検索フィルタを "sAMAccountName" に指定します。その他のディレクトリサービスでは、"uid" を指定します。
LDAP Specifiers: Bind DN	LDAP バインドアカウント識別名を指定します。
LDAP Specifiers: Bind Password	LDAP バインドアカウントパスワードを指定します。

オプション	説明
LDAP Specifiers: Secure LDAP	Content Gateway が、LDAP サーバーとの通信にセキュアな通信を使用するかどうかを指定します。 有効にした場合、LDAP ポートにセキュアポートの1つを設定する必要があります: 636 または 3269。
LDAP Specifiers: LDAP Attribute Name (オプション)	LDAP 属性名を指定します。
LDAP Specifiers: LDAP Attribute Value (オプション)	LDAP 属性のペアを指定します。
Apply	設定の変更を適用します。
Close	設定ファイル エディタ を終了します。 [Close] をクリックする前に、[Apply] をクリックします。 そうでないと、設定変更は失われます。

SOCKS

Content Gateway による SOCKS サポートの詳細については、[SOCKS ファイアウォール統合の設定, 192 ページ](#) を参照してください。



ご注意

SOCKS 構成オプションは、「Configure」>「My Proxy」>「Basic」>「General」タブの [Features] テーブルで SOCKS を有効化した場合だけ、「Configure」ペインに表示されます。

オプション	説明
	General (一般)
SOCKS Version	SOCKS サーバーに使用する SOCKS のバージョンを指定します。Content Gateway は SOCKS バージョン 4 とバージョン 5 をサポートしています。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
	Proxy (プロキシ)
SOCKS Proxy	SOCKS Proxy オプションを有効化または無効化します。 SOCKS プロキシとして、Content Gateway はクライアントからの SOCKS パケットを受信し (通常はポート 1080 上で)、要求を SOCKS サーバーへ直接に転送することができます。 SOCKS Proxy オプションの詳細については、 SOCKS ファイアウォール統合の設定, 192 ページ を参照してください。 このオプションを変更した場合、Content Gateway を再起動する必要があります。

オプション	説明
SOCKS Proxy Port	Content Gateway が SOCKS トラフィックを受け入れるポートを指定します。通常これはポート 1080 です。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
	Server (サーバー)
On-Appliance SOCKS server	Content Gateway が、V- シリーズ アプライアンス上にある場合に表示されます。 アプライアンス上の SOCKS サーバーを有効化または無効化します。 クライアント要求が SOCKS サーバーを経由するためには、SOCKS プロキシ オプションを有効にする必要があります。 socks_server.config を編集して、ネットワーク内の他の SOCKS サーバーの使用するように、Content Gateway を設定できます。下のエントリを参照してください。
Socks Server テーブル	設定された SOCKS サーバーのテーブルを表示します。 SOCKS サーバーの追加 および 設定については SOCKS サーバーの設定, 193 ページ を参照してください。
Refresh	socks_server.config ファイルの現在のエントリを表示するために、表を更新します。
Edit File	socks_server.config ファイルを編集するために、設定ファイルエディタを開きます。
	socks_server.config Configuration File Editor (socks_server.config 設定ファイル エディタ)
エントリ表示ボックス	Content Gateway で使用するために設定された SOCKS サーバーをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したエントリを削除、または上下に移動できます。
Add	サーバーのリストにエントリを追加します。
Set	選択されたエントリを更新します。リストからサーバーを選択し、設定を修正し、 [Set] をクリックしてエントリを更新します。
Clear Fields	選択されたサーバーのすべてのフィールドをクリアします。
SOCKS Server Name	他の SOCKS サーバーと、この SOCKS サーバーを区別するための名前を指定します。
SOCKS Server Host	SOCKS サーバーの IP アドレス、または内部 DNS サーバーによって解決できるホスト名を指定します。
SOCKS Port	SOCKS サーバーがリッスンするポートを指定します。
Default SOCKS Server	この SOCKS サーバーをデフォルトの SOCKS サーバーとして指定する場合、オプションを選択します。
SOCKS User Name	SOCKS 認証が使用される場合に、認証される SOCKS ユーザー名を指定します。
SOCKS Password	SOCKS 認証が使用される場合に、指定したユーザーのパスワードを指定します。
Apply	設定の変更を適用します。

オプション	説明
Close	設定ファイル エディタ を終了します。 [Close] をクリックする前に、[Apply] をクリックします。そうでないと、設定変更は失われます。
Socks Server Rules	Content Gateway が指定したオリジン サーバーにアクセスするために経由しなければならない SOCKS サーバー、および Content Gateway が経由する SOCKS サーバーリストの順序を指定した <code>socks.config</code> ファイルのルールを表示します。 また、SOCKS サーバーを経由せずに、プロキシが直接アクセスするオリジン サーバーを指定することもできます。
Refresh	<code>socks.config</code> ファイルの現在のルールを表示するために、表を更新します。
Edit File	<code>socks.config</code> ファイルを編集するために、設定ファイル エディタを開きます。
	socks.config Configuration File Editor (socks.config 設定ファイル エディタ)
ルール表示ボックス	<code>socks.config</code> ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または上下に移動できます。
Add	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。
Set	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。
Rule Type	プロキシに SOCKS サーバーを経由されるオリジン サーバーを指定するには、[Route through SOCKS server] を選択します。 プロキシが SOCKS サーバーを迂回して、直接アクセスするオリジン サーバーを指定するには、[Do not route through SOCKS server] を選択します。
Destination IP	[Route through SOCKS server] を選択した場合、下記の [SOCKS Servers] フィールドで指定された Content Gateway が使用する SOCKS サーバーに、オリジン サーバーの 1 つの IP アドレス または IP アドレスの範囲を指定します。 [Do not route through SOCKS server] を選択した場合、(SOCKS サーバーを経由せずに) プロキシに直接アクセスさせるオリジン サーバーの IP アドレスを指定します。1 つの IP アドレス、IP アドレスの範囲、または IP アドレスのリストを入力できます。リストの各エントリをコンマで区切ります。「すべてのネットワークブロードキャストアドレス」を指定してはいけません : 255.255.255.255
SOCKS Server	[Route through SOCKS server] を選択した場合、要求を通過させる SOCKS サーバー を選択します。
Round Robin	Content Gateway が厳格にラウンドロビン方式を使用するかどうかを指定します。[strict] または [false] を選択できます。
Apply	設定の変更を適用します。
Close	設定ファイル エディタ を終了します。 [Close] をクリックする前に、[Apply] をクリックします。そうでないと、設定変更は失われます。

オプション	説明
	Options (オプション)
Server Connection Timeout	Content Gateway が SOCKS サーバーへの接続を試みて待機する時間(秒)を指定します。この時間を過ぎるとタイムアウトになります。
Connection Attempts Per Server	Content Gateway が特定の SOCKS サーバーへの接続を試みる回数を指定します。この回数を超えると、サーバーに「接続不能」というマークが付けられます。
Server Pool Connection Attempts	Content Gateway がプール内の特定の SOCKS サーバーへの接続を試みる回数を指定します。この回数を超えると、試行を中止します。

Subsystems (サブシステム)

Subsystem 設定オプションは、次のカテゴリに分けられます：

[Cache \(キャッシュ\), 337 ページ](#)

[Logging \(ログ記録\), 339 ページ](#)

[Forensics Repository, 343 ページ](#)

Cache (キャッシュ)

オプション	説明
	General (一般)
Allow Pinning	指定時間の間、キャッシュにオブジェクトを残しておく キャッシュピンニング オプションを有効化または無効化し ます。 cache.config ファイルでキャッシュピンニングル ールを設定します。
Ram Cache Size	RAM キャッシュのサイズをバイト単位で指定します。デ フォルトのサイズは 104857600 (100 MB) です。 値を“-1”にすると、Content Gateway は RAM キャッシュの サイズをディスク キャッシュ 1 GB につき約 1 MB にしま す。 このオプションを変更した場合、Content Gateway を再起動 する必要があります。
Maximum Object Size	キャッシュで許容されるオブジェクトの最大サイズのを指 定します。 0 (ゼロ) は、サイズ制限がないことを意味します。
	Partition (パーティション)
Cache Partition	キャッシュのパーティション区分を制御する partition.config ファイルのルールを表示します。

オプション	説明
Refresh	partition.config ファイルの最も最新のルールを表示するために、表を更新します。設定ファイル エディタで、ルールを追加 または 編集した後は、このボタンをクリックします。
Edit File	partition.config ファイルを編集、および ルールを追加するために、設定ファイル エディタを開きます。
	partition.config Configuration File Editor (partition.config 設定ファイル エディタ)
ルール表示ボックス	partition.config ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または 上下に移動できます。
Add	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。このボタンをクリックする前に、表示されるフィールドに情報を入力します。
Set	このページ上部のルール表示ボックスを更新します。このボタンをクリックする前に、ルールを選択しプロパティを変更します。
Partition Number	1 から 255 までのパーティション番号を指定します。
Scheme	パーティションに保存されるコンテンツ タイプを指定します。HTTP のみサポートされています。
Partition Size	パーティションに割り当てられるキャッシュ容量を指定します。このサイズは、全キャッシュ容量に対するパーセンテージか、MB 単位の絶対値を指定できます。
Partition Size Format	パーティション サイズの形式を指定します：パーセンテージまたは絶対値。
Apply	設定の変更を適用します。
Close	設定ファイル エディタ を終了します。 [Close] をクリックする前に、[Apply] をクリックします。そうでないと、設定変更は失われます。
	Hosting (ホスティング)
Cache Hosting	指定のオリジン サーバー、および ドメインのキャッシュパーティションへの割り当てを制御する hosting.config ファイルのルールの表を表示します。
Refresh	hosting.config ファイルの最も最新のルールを表示するために、表を更新します。
Edit File	hosting.config ファイルを編集するために、設定ファイル エディタを開きます。 設定ファイル エディタ ページについては後述します。
	hosting.config Configuration File Editor (hosting.config 設定ファイル エディタ)
ルール表示ボックス	hosting.config ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または 上下に移動できます。
Add	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。

オプション	説明
Set	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。
Primary Destination Type	一次宛先タイプを指定します： ドメインに基づいてキャッシュのパーティション区分を行う場合、 [domain] を選択します。 ホスト名に基づいてキャッシュのパーティション区分を行う場合、 [hostname] を選択します。
Primary Destination Value	特定のパーティションに保存するコンテンツのドメイン、またはオリジン サーバー ホスト名を指定します。
Partitions	指定したオリジン サーバー または ドメインに属するコンテンツを保存するパーティションを指定します。各パーティションをコンマで区切ります。 ご注意： パーティションが、既に partition.config ファイルに作成されている必要があります。パーティション作成については、 キャッシュのパーティション区分, 101 ページ を参照してください。
Partitions	指定したオリジン サーバー、または ドメインに属するコンテンツを保存するパーティションのカンマ区切り形式のリストを指定します。
Apply	設定の変更を適用します。
Close	設定ファイル エディタ を終了します。 [Close] をクリックする前に、 [Apply] をクリックします。そうでないと、設定変更は失われます。

Logging (ログ記録)

オプション	説明
	General (一般)
Logging	トランザクションをイベント ログ ファイル および / または エラー ログ ファイルに記録する、イベントログ記録を有効化 または 無効化します。 トランザクションを選択したイベント ログ ファイルに、エラーをエラー ログファイルに記録する場合、 [Log Transactions and Errors] を選択します。 トランザクションのみを選択したイベント ログ ファイルに記録する場合、 [Log Transactions Only] を選択します。 Content Gateway は エラー ログファイルにエラーを記録しません。 エラーのみをエラー ログファイルに記録する場合、 [Log Errors Only] を選択します。Content Gateway は トランザクションを選択したイベント ログ ファイルに記録しません。 ログ記録を停止する場合、 [Disabled] を選択します。

オプション	説明
Log Directory	Content Gateway がイベント ログを保存するディレクトリのパスを指定します。ディレクトリのパスは、Content Gateway クラスタのフェイルオーバー グループ内の各ノードで同じである必要があります。デフォルトは /opt/WCG/logs です。
Log Space: Limit	<p>ログ ファイルのログ記録ディレクトリに割り当てられる最大容量 (メガバイト単位) を指定します。</p> <p>Content Gateway が V シリーズ アプライアンス上である場合は、そのサイズは 5120 (5GB) に設定され、これを変更することはできません。</p> <p>Content Gateway がスタンドアロン サーバーにインストールされている場合は、デフォルトのサイズは 20480 (20 GB) であり、このサイズは設定可能です。</p> <p>ご注意: トランザクション ログは大量のディスク スペースを消費します。この制限が、ログ記録ディレクトリを含むパーティションの使用可能な実容量より、小さいことを確認してください。</p>
Log Space: Headroom	ログ記録容量限界の許容値を指定します。[Auto-Delete Rolled Files (取り込みファイルの自動削除)] オプションが有効になっている場合、ログ記録ディレクトリで利用できる空きスペースがヘッドルームより小さくなると、自動削除がトリガされます。
Log Rolling: Enable/Disable	ログ ファイル取り込みを有効化または無効化します。ログ ファイルを処理しやすいサイズに維持するために、定期的に取り出すことができます。 イベント ログ ファイルの取り込み, 244 ページ を参照してください。
Log Rolling: Offset Hour	ログ ファイル取り込みが行われる時間を指定します。例えば、オフセット時刻が 0 (真夜中) で、取り込み間隔が 6 時間であると、ログ記録の取り込みは、真夜中 (00:00)、06:00、12:00、および 18:00 に行われます。
Log Rolling: Interval	.old ファイルへの取り込みまでに、Content Gateway がログファイルにデータを書き込む時間の長さを指定します。最小値は 300 秒 (5 分) です。デフォルトのタイムアウト値は、21600 秒 (6 時間) です。最大値は 86400 (1 日) です。
Log Rolling: Auto-Delete Rolled Files	ログ ディレクトリで利用できるスペースが少なくなった時の、取り込みログ ファイルの自動的削除を有効にします。ログ ディレクトリの空き容量が [Log Space Headroom] 未満になると、自動削除がトリガされます。
Formats (フォーマット)	
Squid Format: Enable/Disable	Squid ログ フォーマットを有効化または無効化します。
Squid Format: ASCII/Binary	作成されるログ ファイルの種類 (ASCII または Binary) を選択します。
Squid Format: Filename	Squid ログ ファイルの名前を指定します。デフォルトのファイル名は squid.log です。
Squid Format: Header	Squid ログ ファイルに含めるテキストヘッダーを指定します。

オプション	説明
Netscape Common Format: Enable/Disable	Netscape Common ログ フォーマットを有効化または無効化します。
Netscape Common Format: ASCII/ Binary	作成されるログ ファイルの種類 (ASCII または Binary) を選択します。
Netscape Common Format: Filename	Netscape Common ログ ファイルの名前を指定します。デフォルトのファイル名は common.log です。
Netscape Common Format: Header	Netscape Common ログ ファイルに含めるテキストヘッダーを指定します。
Netscape Extended Format: Enable/Disable	Netscape Extended フォーマットを有効化または無効化します。
Netscape Extended Format: ASCII/ Binary	作成されるログ ファイルの種類 (ASCII または Binary) を選択します。
Netscape Extended Format: Filename	Netscape Extended ログ ファイルの名前を指定します。デフォルトのファイル名は extended.log です。
Netscape Extended Format: Header	Netscape Extended ログ ファイルに含めるテキストヘッダーを指定します。
Netscape Extended 2 Format: Enable/Disable	Netscape Extended-2 ログ フォーマットを有効化または無効化します。
Netscape Extended 2 Format: ASCII/Binary	作成されるログ ファイルの種類 (ASCII または Binary) を選択します。
Netscape Extended 2 Format: Filename	Netscape Extended-2 ログ ファイルの名前を指定します。デフォルトのファイル名は extended2.log です。
Netscape Extended 2 Format: Header	Netscape Extended-2 ログ ファイルに含めるテキストヘッダーを指定します。

オプション	説明
	Collation (照合)
Collation Mode	<p>Content Gateway ノードのログ照合モードを指定します。ログ ファイル照合機能を使用して、ログ記録されたすべての情報を一箇所で保存することができます。ログファイル照合については、イベント ログ ファイルの照合, 249 ページ を参照してください。</p> <p>Content Gateway ノードのログ照合を無効化するには、[Collation Disabled] を選択します。</p> <p>Content Gateway ノードを照合サーバーにするには、[Be a Collation Server] を選択します。</p> <p>Content Gateway ノードを照合クライアントにするには、[Be a Collation Client] を選択します。照合クライアントと設定された Content Gateway は、Squid、Netscape Common 等の アクティブな標準ログファイルのみを照合サーバーに送信します。このオプションを選択した場合、[Log Collation Server] フィールドに、クラスタの照合サーバーのホスト名を指定します。</p> <p>ご注意: [Log collation host tagged] オプション(後述)を有効にしない限り、ログが照合されるときにログエントリのソース-オリジンのノード-は失われます。</p> <p>ログ照合は、1つのノードにすべてのログエントリ送信する際に、クラスタの帯域幅を消費します。従って、クラスタのパフォーマンスに影響を及ぼします。</p> <p>照合クライアントの Content Gateway に、カスタム(XMLベース)ログ ファイルを送信させるためには、logs_xml.config ファイルに LogObject を指定する必要があります。</p>
Log Collation Server	ログ ファイルを送信するログ照合サーバーのホスト名を指定します。
Log Collation Port	<p>照合サーバーとクライアントが、通信に使用するポートを指定します。ログ照合がアクティブな場合は、どの場合でも、ポート番号を指定する必要があります。デフォルトのポート番号は 8085 です。</p> <p>ご注意: 他のサービスが既に使用しているポートと競合しない限り、ポート番号を変更しないでください。</p>
Log Collation Secret	クラスタ内のログ照合サーバーと他のノードとのパスワードを指定します。このパスワードは、ログ記録データを検証し、恣意的情報の交換を防止するために使用されます。
Log Collation Host Tagged	このオプションを有効にした場合、Content Gateway は、照合ログ ファイルの最後にログエントリを作成したノードのホスト名を追加します。
Log Collation Orphan Space	Content Gateway ノード上で、オーファン ログ ファイルを保存するためのログ記録ディレクトリに割り当てられる最大容量(メガバイト単位)を指定します。Content Gateway は、ログ照合サーバーと接続できない場合にオーファン ログ エントリを作成します。

オプション	説明
	Custom (カスタム)
Custom Logging	カスタム ログ記録を有効化または無効化します。
Custom Log File Definitions	カスタム (XML ベース) ログ記録オプションを設定するために、 logs.xml.config ファイルを表示します。

Forensics Repository

オプション	説明
Registration status	Forensics Repository における Content Gateway の現在の状態が表示されます。
Forensics Repository IP address	Forensics Repository の場所 (IP アドレス) を表示します。
Unregister ボタン	Forensics Repository から登録削除します。 ご注意: Content Gateway は、起動時に毎回 Forensics Repository の登録状態をチェックし、必要に応じて、自動登録が開始されます。

Networking (ネットワーク)

ネットワーク設定オプションは、次のカテゴリに分けられます:

[Connection Management \(接続管理 \), 344 ページ](#)

[ARM, 345 ページ](#)

[WCCP, 349 ページ](#)

[DNS Proxy \(DNS プロキシ\), 353 ページ](#)

[DNS Resolver \(DNS リゾルバ\), 353 ページ](#)

[ICAP, 355 ページ](#)

[Virtual IP \(仮想 IP \), 356 ページ](#)

Connection Management (接続管理)

オプション	説明
	Throttling (スロットリング)
Throttling Net Connections	Content Gateway が、受け入れるネットワーク接続の最大数を指定します。 Content Gateway のスロットル制限は、ボトルネックの発生時のシステムの過負荷防止に役立ちます。ネットワーク接続がこの値に達した場合、Content Gateway は、既存の接続が閉じるまで新しい接続を順番待ちさせます。 この変数を 100 の最小値以下にしないでください。
	Load Shedding (負荷軽減)
Maximum Connections	ARM が着信要求を直接オリジン サーバーに転送を開始する前に、許可されるクライアント接続の最大数を指定します。デフォルト値は、100 万接続です。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
	Client Connection Control (クライアント接続制御) 次を指定します： <ul style="list-style-type: none"> • クライアント同時接続制限 • クライアント接続率の制限 • 制限超過時のプロキシ応答 • 制限から除外されるクライアントのリスト
Concurrent Connection Limit: Maximum concurrent connections	クライアントに許可される同時 HTTP/HTTPS 接続数の最大値を指定します。デフォルトは 1000 です。次の値の範囲が有効です：1 - 45000
Concurrent Connection Limit: Alert when limit exceeded	有効にすると、クライアントが最大同時接続制限を超過した場合に、Content Gateway にアラートを発生させます。 Content Gateway Manager にアラートを表示する他に、 <code>/var/log/messages</code> および <code>content_gateway.out</code> にログ記録します。
Concurrent Connection Limit: Close excessive connections when limit exceeded	有効にすると、制限を超過した場合に Content Gateway に過剰な接続を閉じさせます。
Connection Rate Limit: Maximum connection rate	クライアントが接続可能な秒当たりの最大接続数 (1 分間の平均) を指定します。デフォルトは 100 です。サポートされる範囲は、1 - 1000 です。
Connection Rate Limit: Alert when limit exceeded	有効にすると、クライアントが最大接続率制限を超過した場合に、Content Gateway にアラートを発生させます。 Content Gateway Manager にアラートを表示する他に、 <code>/var/log/messages</code> および <code>content_gateway.out</code> にログ記録します。

オプション	説明
Connection Rate Limit: Close excessive connections when limit exceeded	有効にすると、制限を超過した場合に Content Gateway に過剰な接続を閉じさせます。
Exceptions	接続制限を適用しない IP アドレス または IP アドレス範囲を指定します。IP アドレスは、IPv4 または IPv6 (IPv6 サポートを有効にする必要があります) を指定できます。カンマ区切り形式のリストで、複数の IP アドレス または IP アドレス範囲を指定できます。
	Low Memory Mode ホストシステムがメモリ不足の場合に、Content Gateway が Web トラフィックのスキャンを中断するかどうかを指定します。 ご注意： この状態で、URL フィルタリングは通常通りに適用されます。
Low Memory Mode: Enabled/Disabled	メモリ不足の間スキャンを中断する場合、[Enabled] を選択します。
Low Memory Mode Duration	スキャンが中断される時間の長さを分単位で指定します。タイマーが切れる前にメモリ不足状態が解決された場合、スキャンを再開し メモリ不足モードトリガーをリセットします。 タイマーが切れた場合、スキャンを再開し メモリ不足モードトリガーをリセットしません。

ARM

Adaptive Redirection Module (ARM) は、クラスタ通信インターフェース フェールオーバーのデバイス通知を送信する機能、および IP レイヤーが着信パケットを受け取る前に検査し、パケットを Content Gateway で処理するようにアドレス変更する機能を含むいくつかの重要な機能を実行します。

ARM は常にアクティブです。詳細情報は、[ARM, 52 ページ](#)を参照してください。

オプション	説明
	General (一般)
IP spoofing	IP スプーフィング オプションを有効化または無効化します。IP スプーフィング オプションは、Content Gateway の IP アドレスの代わりにクライアント IP アドレスを使用して、オリジン サーバーとの接続を確立するように、Content Gateway を設定します。詳細情報は、 IP スプーフィング, 78 ページ を参照してください。 警告： IP スプーフィングは、ネットワーク上のルーティングパスを正確に制御する必要があり、TCP ポート 80 および 443 上で実行する通常のルーティング プロセスを無効にする必要があります。

オプション	説明
Network Address Translation (NAT)	プロキシが透過的にトラフィックを処理する時に、着信パケットをどのようにアドレス変更するかを指定した <i>ipnat.conf</i> ファイルのリダイレクトのルールを表示します。Content Gateway はインストール中にリダイレクトのルールを作成します。このルールは変更できます。
Refresh	ipnat.config ファイルの最も最新のルールを表示するために、表を更新します。
Edit File	ipnat.config ファイルを編集するために、設定ファイル エディタを開きます。
	ipnat.conf Configuration File Editor (ipnat.conf 設定ファイル エディタ)
ルール表示ボックス	<i>ipnat.conf</i> ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または上下に移動できます。
Add	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。
Set	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。
Ethernet Interface	Content Gateway コンピュータへアクセスするトラフィックが使用するイーサネット インタフェースを指定します：例 <code>eth0</code> (Linux)
Connection Type	ルールに適用する接続タイプを指定します：TCP または UDP。
Original Destination IP	トラフィックの送信 IP アドレスを指定します。0.0.0.0 は すべての IP アドレスにマッチします。
Original Destination CIDR	1.1.1.0/24 等の CIDR (Classless Inter-Domain Routing) 形式の IP アドレスを指定します。このフィールドへの入力はおプションです。
Original Destination Port	トラフィックの宛先ポートを指定します：例 HTTP トラフィックの場合 80
Local Client IP	Content Gateway サーバーの IP アドレスを指定します。
Local Port	プロキシポートを指定します：例 HTTP トラフィックの場合 8080
User Protocol (オプション)	[dns] を選択した場合、ARM は DNS トラフィックを Content Gateway にリダイレクトします。そうでない場合は、DNS トラフィックはバイパスされます。
Apply	設定の変更を適用します。
Close	設定ファイル エディタ を終了します。 [Close] をクリックする前に、[Apply] をクリックします。そうでないと、設定変更は破棄されます。

オプション	説明
	Static Bypass (静的バイパス)
Static Bypass	静的透過バイパス ルールを指定した bypass.config ファイルのルールをリストします。透過が有効な場合、プロキシは着信クライアント要求をバイパスするか、透過的に処理しようとするかを決定するために、このルールを使用します。
Refresh	bypass.config ファイルの最も最新のルールを表示するために、表を更新します。
Edit File	bypass.config ファイルを編集するために、設定ファイル エディタを開きます。
	bypass.config Configuration File Editor (bypass.config 設定ファイル エディタ)
ルール表示ボックス	bypass.config ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または上下に移動できます。
Add	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。
Set	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。
Rule Type	ルール タイプを指定します。 [bypass] ルールは 指定された着信要求をバイパスします。 [deny_dyn_bypass] ルールは、指定された着信クライアント要求がプロキシをバイパスすることを禁止します (バイパス禁止ルールは、Content Gateway 自身をバイパスすることを禁止できます)。
Source IP	プロキシをバイパスするか、または バイパスを禁止する着信要求の送信元 IP アドレスを指定します。IP アドレスは、次のいずれかの表記が可能です： 123.45.67.8 等の単一の IP アドレス 1.1.1.0/24 等の CIDR (Classless Inter-Domain Routing) 形式 1.1.1.1-2.2.2.2 等のダッシュで区切られた IP アドレス範囲 1.1.1.0/24, 25.25.25.25, 123.1.23.1-123.1.23.123 等のカンマで区切られた上記の組み合わせ
Destination IP	プロキシをバイパスするか、または バイパスを禁止する着信要求の宛先 IP アドレスを指定します。IP アドレスは、次のいずれかの表記が可能です： 123.45.67.8 等の単一の IP アドレス 1.1.1.0/24 等の CIDR (Classless Inter-Domain Routing) 形式 1.1.1.1-2.2.2.2 等のダッシュで区切られた IP アドレス範囲 1.1.1.0/24, 25.25.25.25, 123.1.23.1-123.1.23.123 等のカンマで区切られた上記の組み合わせ
Apply	設定の変更を適用します。
Close	設定ファイル エディタ を終了します。 [Close] をクリックする前に、[Apply] をクリックします。そうでないと、設定変更は失われます。

オプション	説明
	Dynamic Bypass (動的バイパス)
Dynamic Bypass	クライアントまたはサーバーに問題が発生した場合に、プロキシをバイパスし直接オリジンサーバーに向かう動的バイパスオプションを有効化または無効化します。Content Gateway を停止した場合、動的バイパスルールは削除されます。
Behavior: Non-HTTP, Port 80	<p>Content Gateway がポート 80 上で非 HTTP トラフィックを検出した時に、動的バイパスを有効にするには、[Enabled] を選択します。</p> <p>Content Gateway がポート 80 上で非 HTTP トラフィックを検出した時に、動的バイパスを無効にするには、[Disabled] を選択します。</p> <p>Content Gateway がポート 80 上で非 HTTP トラフィックを検出した時に、動的送信元バイパス / 動的宛先バイパスを有効にするには、[Source-Destination] を選択します。</p> <p>Content Gateway がポート 80 上で非 HTTP トラフィックを検出した時に、動的宛先バイパスのみを有効にするには、[Destination Only] を選択します。</p>
Behavior: HTTP 400	<p>オリジンサーバーが 400 エラーを返した時に、動的バイパスを有効にするには、[Enabled] を選択します。</p> <p>オリジンサーバーが 400 エラーを返した時に、動的バイパスを無効にするには、[Disabled] を選択します。</p> <p>オリジンサーバーが 400 エラーを返した時に、動的送信元バイパス / 動的宛先バイパスを有効にするには、[Source-Destination] を選択します。</p> <p>オリジンサーバーが 400 エラーを返した時に、動的宛先バイパスのみを有効にするには、[Destination Only] を選択します。</p>
Behavior: HTTP 401	<p>オリジンサーバーが 401 エラーを返した時に、動的バイパスを有効にするには、[Enabled] を選択します。</p> <p>オリジンサーバーが 401 エラーを返した時に、動的バイパスを無効にするには、[Disabled] を選択します。</p> <p>オリジンサーバーが 401 エラーを返した時に、動的送信元バイパス / 動的宛先バイパスを有効にするには、[Source-Destination] を選択します。</p> <p>オリジンサーバーが 401 エラーを返した時に、動的宛先バイパスのみを有効にするには、[Destination Only] を選択します。</p>
Behavior: HTTP 403	<p>オリジンサーバーが 403 エラーを返した時に、動的バイパスを有効にするには、[Enabled] を選択します。</p> <p>オリジンサーバーが 403 エラーを返した時に、動的バイパスを無効にするには、[Disabled] を選択します。</p> <p>オリジンサーバーが 403 エラーを返した時に、動的送信元バイパス / 動的宛先バイパスを有効にするには、[Source-Destination] を選択します。</p> <p>オリジンサーバーが 403 エラーを返した時に、動的宛先バイパスのみを有効にするには、[Destination Only] を選択します。</p>

オプション	説明
Behavior: HTTP 405	<p>オリジン サーバーが 405 エラーを返した時に、動的バイパスを有効にするには、[Enabled] を選択します。</p> <p>オリジン サーバーが 405 エラーを返した時に、動的バイパスを無効にするには、[Disabled] を選択します。</p> <p>オリジン サーバーが 405 エラーを返した時に、動的送信元バイパス / 動的宛先バイパスを有効にするには、[Source-Destination] を選択します。</p> <p>オリジン サーバーが 405 エラーを返した時に、動的宛先バイパスのみを有効にするには、[Destination Only] を選択します。</p>
Behavior: HTTP 406	<p>オリジン サーバーが 406 エラーを返した時に、動的バイパスを有効にするには、[Enabled] を選択します。</p> <p>オリジン サーバーが 406 エラーを返した時に、動的バイパスを無効にするには、[Disabled] を選択します。</p> <p>オリジン サーバーが 406 エラーを返した時に、動的送信元バイパス / 動的宛先バイパスを有効にするには、[Source-Destination] を選択します。</p> <p>オリジン サーバーが 406 エラーを返した時に、動的宛先バイパスのみを有効にするには、[Destination Only] を選択します。</p>
Behavior: HTTP 408	<p>オリジン サーバーが 408 エラーを返した時に、動的バイパスを有効にするには、[Enabled] を選択します。</p> <p>オリジン サーバーが 408 エラーを返した時に、動的バイパスを無効にするには、[Disabled] を選択します。</p> <p>オリジン サーバーが 408 エラーを返した時に、動的送信元バイパス / 動的宛先バイパスを有効にするには、[Source-Destination] を選択します。</p> <p>オリジン サーバーが 408 エラーを返した時に、動的宛先バイパスのみを有効にするには、[Destination Only] を選択します。</p>
Behavior: HTTP 500	<p>オリジン サーバーが 500 エラーを返した時に、動的バイパスを有効にするには、[Enabled] を選択します。</p> <p>オリジン サーバーが 500 エラーを返した時に、動的バイパスを無効にするには、[Disabled] を選択します。</p> <p>オリジン サーバーが 500 エラーを返した時に、動的送信元バイパス / 動的宛先バイパスを有効にするには、[Source-Destination] を選択します。</p> <p>オリジン サーバーが 500 エラーを返した時に、動的宛先バイパスのみを有効にするには、[Destination Only] を選択します。</p>

WCCP



ご注意

WCCP 構成オプションは、「**Configure**」 > 「**My Proxy**」 > 「**Basic**」 > 「**General**」 タブの [Features] テーブルで WCCP を有効化した場合だけ、「Configure」 ペインに表示されます。

このオプションは、Content Gateway での WCCP の使用を制御する `wccp.config` 設定ファイルに定義されています。エントリは、「Configure」>「Networking」>「WCCP」で提供されているエディタを使用して、定義および保守されるべきです。

管理者は、WCCP に関する実用的知識を持っていることが必要になります。

WCCP v2 のみサポートされています。

WCCP v2 の構成と処理能力に関する情報について、マニュアルおよび製造者のサポート サイトを参照することを強く推奨します。大部分のデバイスを、ハードウェア ベースのリダイレクトを最大限に活用するように構成する必要があります。Cisco デバイスでは、通常は IOS の最新バージョンが最も適切です。

アクティブな WCCP サービス グループは、それぞれに対応する ARM NAT ルールが必要です。[ARM, 345 ページ](#)を参照してください。

クラスタ内に複数のプロキシサーバーが構成されている時、[Service Group Enabled/Disabled]、[Network Interface]、および [Weight] を除くすべての設定は、クラスタ全体には適用されます。

Content Gateway の WCCP v2 サポートの詳細は、[WCCP v2 デバイスによる透過的遮断, 55 ページ](#)を参照してください。

オプション	説明
WCCP Service Groups	<code>wccp.config</code> ファイルで定義されているサービス グループの表を表示します。WCCP サービス グループ設定は WCCP の動作を定義します。列フィールドは下記の設定エディタ エントリで説明されています。
Refresh	<code>wccp.config</code> ファイルの現在の定義を表示するために、テーブルをリフレッシュします。
Edit File	設定ファイル エディタで、 <code>wccp.config</code> ファイルを開きます。
	wccp.config Configuration File Editor (wccp.config 設定ファイル エディタ)
サービス グループ表示ボックス	WCCP サービス グループの定義をリストします。 リスト内で編集するエントリを選択します。 “X” ボタンは 選択を削除するために使用します。 リストの順序に意味はありません。そのため、上 / 下矢印ボタンは無視されます。
Add	新しいサービス グループの定義を追加します。[Add] をクリックすると、ページの上部のボックス内に新しい定義が表示されます。
Set	選択したサービス グループの定義の変更を適用し、ページの上部のボックス内に新しい値を表示します。

オプション	説明
	Service Group Information (サービスグループの情報)
Service Group Status	サービスグループを有効化または無効化します。 この設定はクラスタ全体には適用されません。選択されたメンバーのサービスグループのみアクティブにします。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
Service Group Name	固有のサービスグループ名を指定します。これは管理に役立ちます。
Service Group ID	0 から 255 までのサービスグループ ID を指定します。この ID は、ルーター上でも設定しなければなりません。 既に使用中の番号を指定した場合、[Add] または [Set] がクリックされた時にエラーを表示します。
Protocol	このサービスグループに適用するプロトコル (TCP または UDP) を指定します。
Ports	カンマ区切り形式のリストで最大 8 つのポートを指定します。
Network Interface	このサービスグループに使用する Content Gateway ホストシステム上のネットワークインターフェースを指定します。
	Mode Negotiation (モードのネゴシエーション)
Packet Forward Method	遮断されたトラフィックをプロキシに送信するために、WCCP ルーターによって使用される優先されるカプセル化方法を指定します。ルーターが GRE および L2 をサポートしている場合、ここで指定された方法を使用します。 重要: GRE と Multicast は互換ではありません。
Packet Return Method	遮断されたトラフィックを WCCP ルーターに返信するために使用される、優先されるパケットカプセル化方法を指定します。 ご注意 Content Gateway がルーターによってサポートされていない Forward/Return 方法を使用するように設定されている場合、プロキシはルーターによってサポートされている方法を使用しようと試みます。 ご注意 L2 を選択するには、ルーターとスイッチが Content Gateway と Layer 2-adjacent (同じサブセットにある) であることが必要です。
	Advanced Settings (拡張設定)
Assignment Method	遮断されたトラフィックを複数のプロキシサーバーに配分するために使用する方法を指定します。[HASH] および [MASK] を選択できます。 MASK 値は最大 6 つの有効ビットまで適用されます (1 つのクラスタで、合計 64 個の bucket が作成されます)。 割り当て方法の詳細については WCCP のマニュアルを参照してください。ご使用のデバイスに、製造業者のマニュアルで推奨されている値を使用してください。

オプション	説明
Distribution attribute(s)	<p>どの要求がどのプロキシサーバーに配信されるかを決定するために、割り当て方法が使用する属性を指定します。</p> <p>割り当て方法が [HASH] の場合、1 つ以上の配分属性を選択します。</p> <p>割り当て方法が [MASK] の場合、1 つの配分属性を選択します。</p>
Weight	<p>比例重み付けによる要求のサーバーへの配分を指定します。トラフィックの全フローに対する希望する割合を指定します。</p> <p>すべてのクラスタメンバーが 0(デフォルト)に設定された場合、均等に配分されます。いずれかのメンバーが 0 以外に設定されている時、他のメンバーの値に対する相対的で、比例的に分配されます。0 の値のままのメンバーはトラフィックを受け取りません。</p>
Reverse Service Group ID	<p>IP スプーフィングが有効な場合にのみ使用します。</p> <p>IP スプーフィングが有効化されている時、プロキシはそれぞれの有効化されている WCCP フォワード サービスグループに対して、リバース サービスグループを公告します。リバース サービスグループは、プロキシへのオリジンサーバー応答のリターンパスに適用されなければなりません。</p>
Router Information (ルーター情報)	
Security (オプション)	<p>ルーターと Content Gateway との相互認証を有効化または無効化します。</p> <p>Content Gateway のセキュリティを有効化した場合、ルーターのセキュリティも有効化する必要があります。ルーターのマニュアルを参照してください。</p> <p>このオプションを変更した場合、Content Gateway を再起動する必要があります。</p>
Security:Password	<p>認証に使用されるパスワードを指定します。パスワードは、ルーターに設定されたパスワードと同じ必要があります。最大 8 文字まで入力できます。</p> <p>このオプションを変更した場合、Content Gateway を再起動する必要があります。</p>
Multicast (オプション)	<p>WCCP マルチキャストモードを有効化または無効化します。</p> <p>重要: GRE パケットの Forward/Return メソッドでは使用できません。</p> <p>このオプションを変更した場合、Content Gateway を再起動する必要があります。</p>

オプション	説明
Multicast: IP Address	マルチキャスト IP アドレスを指定します。 このオプションを変更した場合、Content Gateway を再起動する必要があります。
WCCP Routers	最大 10 個の WCCP v2-対応ルーターの IP アドレスを指定します。 GRE が Packet Forward Method または Packet Return Method に選択されている場合は、各ルーターの仮想 IP アドレスと、ゲートウェイの IP アドレスも指定します。仮想 IP アドレスは一意でなければなりません。 マルチキャストが有効でない場合、ネットワーク内のルーターは自動的に検出されません。 このオプションを変更した場合、Content Gateway を再起動する必要があります。

DNS Proxy (DNS プロキシ)



ご注意

DNS Proxy 構成オプションは、「Configure」>「My Proxy」>「Basic」>「General」タブの [Features] テーブルで DNS Proxy を有効化した場合だけ、「Configure」ペインに表示されます。

オプション	説明
DNS Proxy Port	Content Gateway が DNS トラフィックに使用するポートを指定します。デフォルトポートは 5353 です。

DNS Resolver (DNS リゾルバ)

オプション	説明
	Resolver (リゾルバ)
Local Domain Expansion	ローカルドメインを拡張することで、不適切なホスト名を解決しようと試みるローカルドメイン拡張を有効化または無効化します。たとえば、クライアントが不適切なホスト名 <code>hostx</code> を要求した時、WCG ローカルドメインが <code>y.com</code> である場合、Content Gateway はホスト名を <code>hostx.y.com</code> に拡張します。
	Host Database (ホスト データベース)
DNS Lookup Timeout	プロキシがドメイン名サーバーからのルックアップ応答を待つ最大時間を秒単位で指定します。

オプション	説明
Foreground Timeout	DNS エントリをデータベース内に保持する時間を指定します。この時間を過ぎるとオブジェクトは古くなっているとみなされます。 たとえば、このタイムアウトが 24 時間で、データベース内に 24 時間以上存在するエントリをクライアントが要求した場合、プロキシはエントリを処理する前にリフレッシュします。 警告：フォアグラウンド タイムアウトが小さすぎると、応答時間が遅くなります。設定が高すぎると、誤った情報を蓄積する危険性があります。
Failed DNS Timeout	ホスト名が DNS ルックアップ失敗キャッシュに保存される時間を秒単位で指定します。タイムアウト時間が経過すると、ホスト名はキャッシュから削除され、そのホスト名への次の要求は DNS サーバーへ送信されます。
Split DNS (分割 DNS)	
Split DNS	分割 DNS オプションを有効化 または 無効化します。有効にすると、セキュリティ要件に応じて、Content Gateway が複数の DNS サーバーを使用できます。たとえば、プロキシが 1 つの DNS サーバーのセットを使って社内ネットワーク上のホスト名を解決し、ファイアウォールの外側の DNS サーバーがインターネット上のホストを解決するように設定することができます。分割 DNS の使用の詳細については、 Split DNS オプションの使用, 196 ページ を参照してください。
Default Domain	DNS 要求を分割するために使用するデフォルト ドメインを指定します。ホスト名がドメインを含まない場合、Content Gateway は、使用する DNS サーバーを選択する前に、ホスト名にデフォルト ドメインを付加します。
DNS Servers Specification	特定の条件のもとで、プロキシがホストを解決するために使用する DNS サーバーを制御する splitdns.config ファイルのルールを表示します。
Refresh	splitdns.config ファイルの最新のルールを表示するために、表を更新します。設定ファイル エディタで、ルールを追加 または 編集した後は、このボタンをクリックします。
Edit File	splitdns.config ファイルを編集、および ルールを追加するために、設定ファイル エディタを開きます。設定ファイル エディタ ページについては後述します。
splitdns.config Configuration File Editor (splitdns.config 設定ファイル エディタ)	
ルール表示ボックス	splitdns.config ファイルのルールをリストします。編集するルールを選択します。ボックスの左側のボタンで、選択したルールを削除、または 上下に移動できます。
Add	設定ファイル エディタ ページ上部のルール表示ボックスに、新しいルールを追加します。このボタンをクリックする前に、表示されるフィールドに情報を入力します。

オプション	説明
Set	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。このボタンをクリックする前に、ルールを選択しプロパティを変更します。
Primary Destination Type	DNS サーバーが、宛先ドメイン (<code>dest_domain</code>)、宛先ホスト (<code>dest_host</code>)、または 正規表現 (<code>url_regex</code>) のいずれかに基づいて選択されるかを指定します。
Primary Destination Value	一次宛先の値を指定します。NOT 論理演算子を指定するには、値の最初に記号 "!" を置きます。
DNS Server IP	一次宛先指定子に使用する DNS サーバーを指定します。コロン (:) を使用してポートを指定することができます。ポートを指定しない場合、53 が使用されます。スペース または セミコロン (;) で区切ることで、複数の DNS サーバーを指定できます。
Default Domain Name (オプション)	ホストの解決に使用するデフォルト ドメイン名を指定します。許可されるのは 1 つだけです。デフォルト ドメインを指定していない場合、システムは <code>/etc/resolv.conf</code> からその値を決定します。
Domain Search List (オプション)	ドメイン検索の順序を指定します。スペース または セミコロン (;) で区切ることで、複数のドメインを指定できます。検索リストを指定していない場合、システムは <code>/etc/resolv.conf</code> からその値を決定します。
Apply	設定の変更を適用します。
Close	設定ファイル エディタ を終了します。 [Close] をクリックする前に、[Apply] をクリックします。そうでないと、設定変更は失われます。

ICAP



ご注意

ICAP 構成オプションは、「Configure」 > 「My Proxy」 > 「Basic」 > 「General」 タブの [Features] テーブルで ICAP を有効化した場合だけ、「Configure」 ペインに表示されます。

ICAP は、Websense Data Security および ICAP 対応のその他のデータ セキュリティ サービスに、代替インターフェースを提供します。プライマリおよびバックアップ URI を指定でき、フェールオーバーおよびロード バランシングを設定できます。 [ICAP クライアントの構成, 139 ページ](#) および [ICAP フェー](#)

[ルオーバーとロード バランシング, 141 ページ](#)のサブセクションを参照してください。

オプション	説明
ICAP Service URI	ICAP サービスの URI(Uniform Resource Identifier) を指定します。形式は下記の通りです。 <code>icap://hostname:port/path</code> 例: <code>icap://ICAP_machine:1344/REQMOD</code> デフォルトの ICAP ポートは 1344 です。デフォルトのポートを使用している場合、URI にポートを指定する必要はありません。 オプションの第 2URI サービスは、最初のサービスのすぐ後に、コンマと第 2 サービスをスペースなして付加することで指定できます。
Analyze HTTPS Content	復号化したトラフィックを分析のために、Data Security Suite に送信するか、または直接宛先に送信するかを指定します。
Analyze FTP Uploads	FTP アップロード要求を分析のために、Data Security Suite に送信するかどうかを指定します。FTP プロキシ機能を有効化する必要があります。 FTP, 314 ページ を参照してください。
Action for Communication Errors	Content Gateway が Websense Data Security Suite との通信中にエラーを受信した場合に、トラフィックを許可するか、ブロック ページを送信するかを指定します。
Action for Large files	DSS 内で指定されたサイズ制限より大きなファイルが送られた場合に、トラフィックを許可するか、ブロック ページを送信するかを指定します。DSS のサイズの制限は 12MB です。

Virtual IP (仮想 IP)



ご注意

Virtual IP 構成オプションは、「**Configure**」>「**My Proxy**」>「**Basic**」>「**General**」タブの [Features] テーブルで Virtual IP を有効化した場合だけ、「Configure」ペインに表示されます。

オプション	説明
Virtual IP Addresses	Content Gateway によって管理される仮想 IP アドレスの表を表示します。
Refresh	最新の仮想 IP アドレスを表示するために、表を更新します。設定ファイル エディタで、仮想 IP アドレスを追加または編集した後は、このボタンをクリックします。

オプション	説明
Edit File	仮想 IP アドレスのリストを編集、および追加するために、設定ファイル エディタを開きます。
	vaddrs.config Configuration File Editor (vaddrs.config 設定ファイル エディタ)
ルール表示ボックス	仮想 IP アドレスをリストします。編集する仮想 IP アドレスを選択します。ボックスの左側のボタンで、選択した仮想 IP アドレスを削除、または上下に移動できます。
Add	設定ファイル エディタ ページ上部のルール表示ボックスに、新しい仮想 IP アドレスを追加します。
Set	設定ファイル エディタ ページの上部のルール表示ボックスを更新します。
Virtual IP Address	Content Gateway によって管理される仮想 IP アドレスを指定します。
Ethernet Interface	仮想 IP アドレスに割り当てられたネットワーク インターフェイスを指定します。
Sub-Interface	サブインターフェイス ID を指定します。これは、インターフェイスがアドレスとして使用する 1 から 255 までの番号です。
Apply	設定の変更を適用します。
Close	設定ファイル エディタ を終了します。 [Close] をクリックする前に、[Apply] をクリックします。そうでないと、設定変更は失われます。

SSL

SSL 設定オプションは、次のカテゴリに分けられます：

- ◆ 証明書 ([証明書の管理](#), 159 ページを参照)
- ◆ 復号化/暗号化 ([インバウンド トラフィックの場合の SSL Manager の構成](#), 162 ページおよび [アウトバウンド トラフィックの場合の SSL Manager の構成](#), 163 ページを参照)
- ◆ 検証 ([証明書の検証](#), 164 ページを参照)
- ◆ インシデント ([Web HTTPS サイト アクセスの管理](#), 171 ページを参照)
- ◆ クライアント証明書 ([クライアント証明書](#), 175 ページを参照)
- ◆ ログ記録 ([SSL Manager ロギングの構成](#), 177 ページを参照)
- ◆ カスタム化 ([SSL 接続エラー メッセージのカスタム化](#), 180 ページを参照)
- ◆ 内部ルート CA ([内部ルート CA](#), 151 ページを参照)

D

イベントログ記録フォーマット

カスタム ログ記録フィールド

関連項目:

- ◆ [ログ記録フォーマット相互参照, 362 ページ](#)

%<field symbol>	説明
{ <i>HTTP header field name</i> }cqh	クライアント要求 HTTP ヘッダーの要求されたフィールドの情報をログ記録します。たとえば、%<{Accept-Language}cqh> はクライアント要求ヘッダー内の Accept-Language: フィールドをログ記録します。 このフィールドは カスタム ログ フィルタでは使用できません。
{ <i>HTTP header field name</i> }cqhua	クライアント要求 HTTP ヘッダーの要求されたフィールドの情報をログ記録します。たとえば、%<{User-Agent}cqhua> はクライアント要求ヘッダー内の User-Agent: フィールドをログ記録します。
{ <i>HTTP header field name</i> }pqh	プロキシ要求 HTTP ヘッダーの要求されたフィールドの情報をログ記録します。たとえば、%<{Authorization}pqh> はプロキシ要求ヘッダー内の Authorization: フィールドをログ記録します。 このフィールドは カスタム ログ フィルタでは使用できません。
{ <i>HTTP header field name</i> }psh	プロキシ応答 HTTP ヘッダーの要求されたフィールドの情報をログ記録します。たとえば、%<{Retry-After}psh> はプロキシ応答ヘッダー内の Retry-After: フィールドをログ記録します。 このフィールドは カスタム ログ フィルタでは使用できません。

%<field symbol>	説明
{HTTP header field name}ssh	サーバー応答 HTTP ヘッダーの要求されたフィールドの情報をログ記録します。たとえば、%<{Age}ssh> はサーバー応答ヘッダー内の Age: フィールドをログ記録します。 このフィールドはカスタム ログ フィルタでは使用できません。
caun	認証されたクライアントのユーザー名。 クライアントのユーザー名の RFC931/ident ルックアップの結果。
cfsc	クライアント終了ステータス コード。プロキシへのクライアント要求が成功 (FIN) したか、中断 (INTR) したかを示します。
chi	クライアント ホスト IP。クライアントのホストコンピュータの IP アドレス。
cqbl	クライアント要求転送長。Content Gateway に対するクライアントの要求本文の長さ (バイト数)。
cqhl	クライアント要求ヘッダー長。Content Gateway に対するクライアント要求ヘッダーの長さ。
cqhm	Content Gateway に対するクライアント要求の HTTP メソッド: GET、POST 等 (cctx のサブセット)。
cqhv	クライアントの要求の HTTP バージョン。
cqtd	クライアント要求のタイムスタンプ。yyyy-mm-dd の形式のクライアントの要求の日付。ここで、yyyy は 4 桁の年、mm は 2 桁の月、dd は 2 桁日です。
cqtn	クライアント要求のタイムスタンプ。クライアントの要求の日付と時間 (Netscape タイムスタンプ形式)。
cqtg	クライアントの要求のミリ秒精度のタイムスタンプ。
cqts	Squid フォーマットのクライアント要求タイムスタンプ。1970 年 1 月 1 日からの秒数で示されるクライアント要求の時刻。
cqtt	クライアント要求のタイムスタンプ。hh:mm:ss の形式のクライアントの要求の時間。ここで、hh は 24 時間形式の 2 桁の時刻、mm は 2 桁の分、ss は 2-桁の秒です。例: 16:01:19
cctx	ヘッダーを除いた完全な HTTP クライアント要求テキスト。例: GET http://www.company.com HTTP/1.0
cqu	クライアント要求 URI。クライアントから Content Gateway への要求の URI(cctx のサブセット)。
cquc	クライアント要求の標準 URL。cqu との違いは、ブランク (および、ログ分析ツールで解析できないその他の特殊文字) が、エスケープ シーケンスによって置き換えられていること。エスケープ シーケンスは、パーセント記号とそれに後続する 16 進表記の ASCII コード番号です。

%<field symbol>	説明
cqup	クライアント要求の URL パス。URL の引数部分 (ホストの後のすべて)。たとえば、URL が http://www.company.com/images/x.gif の場合、このフィールドは /images/x.gif と表示します。
cqus	クライアント要求の URL スキーム (HTTP、FTP など)。
crc	キャッシュ戻り値。要求に対するキャッシュの応答を示します (HIT、MISS 等)。
pfsc	プロキシ終了ステータス コード。Content Gateway のオリジン サーバーへの要求が、正常に完了したか (FIN)、中断された (INTR) かどうかを示します。
phn	照合ログ ファイルにログ エントリを生成した Content Gateway サーバーのホストネーム。
phr	プロキシ階層ルート。Content Gateway がオブジェクトの取得のために使用したルート。
pqbl	プロキシ要求転送の長さ。オリジン サーバーに対する Content Gateway 要求本文の長さ。
pqhl	プロキシ要求ヘッダーの長さ。オリジン サーバーに対する Content Gateway 要求ヘッダーの長さ。
pqsi	プロキシ要求サーバーの IP アドレス (0 はキャッシュ ヒット、親プロキシへの要求は 親 IP アドレス)。
pqsn	プロキシ要求サーバー名。要求を実行したサーバーの名前。
pscl	プロキシ応答転送の長さ。クライアントに対する Content Gateway 応答の長さ (バイト数)。
psct	プロキシ応答のコンテンツ タイプ。サーバー応答ヘッダー内のドキュメント (例: <code>img/gif</code>) のコンテンツ タイプ。
pshl	プロキシ応答ヘッダーの長さ。クライアントに対する Content Gateway 応答ヘッダーの長さ。
psql	Squid フォーマットのプロキシ応答転送の長さ (ヘッダーとコンテンツの長さを含む)。
pssc	プロキシ応答ステータス コード (Content Gateway からクライアントへの HTTP 応答ステータス コード)。
shi	<p>要求内のホストの DNS 名ルックアップで解決された IP アドレス。複数の IP アドレスをもつホストでは、このフィールドは特定の DNS 名ルックアップで解決された IP アドレスを記録します。これは、キャッシュドキュメントのためにミスリードされることがあります。</p> <p>たとえば、サーバー S の最初の要求はキャッシュ ミスで IP1 から取得し、サーバー S の 2 回目の要求が IP2 と解決され、キャッシュから取得した場合、2 回目の要求のログ エントリは IP2 と表示します。</p>
shn	オリジン サーバーのホスト名。

%<field symbol>	説明
sscl	サーバー応答転送の長さ。Content Gateway に対するオリジン サーバーから応答の長さ (バイト数)。
sshl	サーバー応答ヘッダーの長さ。Content Gateway に対するオリジン サーバーから応答ヘッダーの長さ (バイト数)。
sshv	サーバー応答の HTTP バージョン (1.0、1.1 等)。
sssc	サーバー応答ステータス コード。オリジン サーバーから Content Gateway への HTTP 応答ステータス コード。
ttms	Content Gateway がクライアントの要求の処理で費やした時間。クライアントが Content Gateway との接続を確立した時点から Content Gateway がその応答の最後のバイトをクライアントに送り返した時点までのミリ秒。
ttmsf	Content Gateway がクライアントの要求の処理で費やした時間 (秒の分数)。ミリ秒精度の時間を示しますが、整数形式 (<i>ttms</i>) の出力の代わりに、秒の分数を表す浮動小数点形式で表示します。たとえば、時間が 1500 ミリ秒の場合、このフィールドは 1.5 と表示されますが、 <i>ttms</i> フィールドでは 1500 と表示され、 <i>tts</i> フィールドでは 1 と表示されます。
tts	Content Gateway がクライアントの要求の処理で費やした時間; クライアントがプロキシとの接続を確立した時点からプロキシがその応答の最後のバイトをクライアントに送り返した時点までの秒数。
wc	スキャンされるデータの URL の事前定義カテゴリまたはカスタム カテゴリ。例: "News and Media"
wct	Web ページのコンテンツ タイプ。例: "text/html; charset=UTF-8"
wsds	CATEGORY_BLOCKED、PERMIT_ALL、FILTERED_AND_PASSED 等のフィルタの種類 of 文字列。
wsr	スキャン推奨ビット ("true" または "false")。URL データベースで、さらに分析すべきデータを識別し、推奨します。使用されているポリシーに依存して、データは更に分析される場合もあり、分析されない場合もあります。
wstms	ダウンロードしたファイルまたはページのスキャンに費やしたスキャン時間 (単位ミリ秒)。
wui	クライアント要求のデータをスキャンするポリシーを選択するために使用する認証されたユーザー ID。

ログ記録フォーマット相互参照

以下のセクションでは、Content Gateway のログ記録フィールドと、Squid および Netscape フォーマットの標準ログ記録フィールドの対応を示しています。

Squid ログ記録フォーマット

Squid	Content Gateway フィールドの記号
time	cqts
elapsed	ttms
client	chi
action/code	crc/pssc
size	psql
method	cqhm
url	cquc
ident	caun
hierarchy/from	phr/pqsn
content	psct

たとえば、最初の 3 つの Squid フィールドを基にして、`short_sq` という名前のカスタム フォーマットを作成する場合、`logs.config` ファイルの次の行を入力します：

```
format:enabled:1:short_sq:%<cqts> %<ttms>
%<chi>:short_sq:ASCII:none
```

カスタム ログ ファイルの定義の詳細については、[カスタム フォーマット](#)、[239 ページ](#) を参照してください。

Netscape Common ログ記録フォーマット

Netscape Common	Content Gateway フィールドの記号
host	chi
usr	caun
[time]	[cqtn]
“req”	“cqtX”
s1	pssc
c1	pscl

Netscape Extended ログ記録フォーマット

Netscape Extended	Content Gateway フィールドの記号
host	chi
usr	caun
[time]	[cqtn]
“req”	“cqtX”
s1	pssc
c1	pscl
s2	sssc
c2	sscl
b1	cqbl
b2	pqbl
h1	cqhl
h2	pshl
h3	pqhl
h4	sshl
xt	tts

Netscape Extended-2 ログ記録フォーマット

Netscape Extended-2	Content Gateway フィールドの記号
host	chi
usr	caun
[time]	[cqtn]
“req”	“cqtX”
s1	pssc
c1	pscl
s2	sssc
c2	sscl
b1	cqbl
b2	pqbl
h1	cqhl
h2	pshl

Netscape Extended-2	Content Gateway フィールドの記号
h3	pqhl
h4	sshl
xt	tts
route	phr
pfs	cfsc
ss	pfsc
crc	crc

E

設定ファイル

Websense Content Gateway には、下記の設定ファイルを含まれ、プロキシをカスタマイズするために編集することができます。

- ◆ [auth.config, 369 ページ](#)
- ◆ [bypass.config, 372 ページ](#)
- ◆ [cache.config, 374 ページ](#)
- ◆ [filter.config, 377 ページ](#)
- ◆ [hosting.config, 380 ページ](#)
- ◆ [ip_allow.config, 382 ページ](#)
- ◆ [ipnat.conf, 383 ページ](#)
- ◆ [log_hosts.config, 383 ページ](#)
- ◆ [logs_xml.config, 385 ページ](#)
- ◆ [mgmt_allow.config, 392 ページ](#)
- ◆ [parent.config, 393 ページ](#)
- ◆ [partition.config, 396 ページ](#)
- ◆ [records.config, 397 ページ](#)
- ◆ [remap.config, 458 ページ](#)
- ◆ [socks.config, 460 ページ](#)
- ◆ [socks_server.config, 461 ページ](#)
- ◆ [splitdns.config, 462 ページ](#)
- ◆ [storage.config, 464 ページ](#)
- ◆ [update.config, 465 ページ](#)
- ◆ [wccp.config, 467 ページ](#)

URL 正規表現の指定 (url_regex)

照会を実行するために正規表現を使用する設定ファイル内の url_regex タイプのエントリ。

下記の表は、有効な `url_regex` を作成する方法を示す例を提供しています。

値	説明
<code>x</code>	文字 <code>x</code> に一致。
<code>.</code>	すべての文字に一致。
<code>^</code>	行の先頭を指定。
<code>\$</code>	行の最後を指定。
<code>[xyz]</code>	文字クラス。この場合、パターンは <code>x</code> 、 <code>y</code> 、または <code>z</code> のいずれかに一致します。
<code>[abj-oZ]</code>	範囲の文字クラス。このパターンは <code>a</code> 、 <code>b</code> 、 <code>j</code> から <code>o</code> までのいずれかの文字、または <code>Z</code> に一致します。
<code>[^A-Z]</code>	否定文字クラス。このパターンは クラスの中の文字以外のすべての文字に一致します。
<code>r*</code>	<code>r</code> の 0 回以上の繰り返しに一致します。ここで、 <code>r</code> はすべての正規表現です。
<code>r+</code>	<code>r</code> の 1 回以上の繰り返しに一致します。ここで、 <code>r</code> はすべての正規表現です。
<code>r?</code>	<code>r</code> の 0 回または 1 回に一致します。ここで、 <code>r</code> はすべての正規表現です。
<code>r{2,5}</code>	<code>r</code> の 2 回から 5 回までの繰り返しに一致します。ここで、 <code>r</code> はすべての正規表現です。
<code>r{2,}</code>	<code>r</code> の 2 回以上の繰り返しに一致します。ここで、 <code>r</code> はすべての正規表現です。
<code>r{4}</code>	<code>r</code> の 4 回丁度の繰り返しに一致します。ここで、 <code>r</code> はすべての正規表現です。
<code>"[xyz]¥"images</code>	リテラルの文字列 <code>[xyz]¥"images</code>
<code>¥X</code>	<code>X</code> が <code>a</code> 、 <code>b</code> 、 <code>f</code> 、 <code>n</code> 、 <code>r</code> 、 <code>t</code> 、or <code>v</code> の場合、 <code>¥x</code> の ANSI-C インタープリテーション。そうでない場合は、リテラルの文字 <code>X</code> 。これは、 <code>*</code> 等のエスケープ演算子に使用されます。
<code>¥0</code>	NULL 文字。
<code>¥123</code>	8 進数の値 <code>123</code> の文字。
<code>¥x2a</code>	16 進数の値 <code>2a</code> の文字。
<code>(r)</code>	<code>r</code> に一致します。ここで、 <code>r</code> はすべての正規表現です。優先順位をオーバーライドするために、括弧を使用できます。
<code>rs</code>	正規表現 <code>r</code> の後に正規表現 <code>s</code> が続く。
<code>r s</code>	<code>r</code> または <code>s</code> のいずれかに一致します。
<code>#<n>#</code>	到達した時に正規表現マッチングを停止させる <i>エンド</i> ノードを挿入。値 <code>n</code> が返されます。

例

mydomain.com 内のすべてのホストに一致させるには、
`dest_domain=mydomain.com` を指定します。同様に、すべての要求に一致されるには、`dest_domain=.` を指定します。

auth.config

auth.config ファイルは、指定された IP アドレスと IP アドレス範囲、および（または）特定のドメイン コントローラに対する着信ポート（明示的プロキシのみ）上のトラフィックを管理するルール保存します。この機能は、[複数レルムの認証, 216 ページ](#)と呼ばれます。認証レルム ルールは、「**Configure**」>「**Security**」>「**Access Control**」>「**Authentication Realms (認証レルム)**」タブ上で定義されます。

- ◆ 複数レルムの認証は、統合 Windows(IWA)、レガシー NTLM、および LDAP 認証のみをサポートしています。
- ◆ 各認証ルールは、ソース IP アドレス、および / または 着信ポート（明示的プロキシのみ）、認証方法、ドメイン、および その他の関連するオプションを指定します。
- ◆ 複数のルールを同時にアクティブにすることができます。この方法では、複数の認証方法を同時に使用することができます。
- ◆ IWA、LDAP、および NTLM ルールによって使用される指定子が異なります。
- ◆ ルールはリストの上から順にチェックされ、最初に条件に一致するルールのみが適用されます。IP アドレスの条件に一致するルールがない場合、認証は試みられません。



ご注意

ネットワーク内のすべてのクライアントが、信頼関係を共有している認証サーバーによって認証される場合、複数認証レルムのためのルールを作成する必要はありません。

フォーマット

auth.config の各行は、一連のタグとそれに続く値で構成されます。認証ルールは次の形式になります：

```
type=<auth_type> name=<profile_name> src_ip=<IP addresses> <additional tags>
```

下記の表は、すべてのルールで共通のタグをリストしています。

一般タグ	使用できる値
type	ルール タイプを示す文字列：winauth、ntlm、ldap
enabled	ルールがアクティブかどうかを指定： <ul style="list-style-type: none"> • 0 = 無効 • 1 = 有効
name	ログ記録に使用する解り易い一意な名前。
src_ip	IP アドレスおよび IP アドレス範囲のカンマ区切りリスト。
proxy_port (オプション)	ポート番号。
use_alias	認証が成功した場合にフィルタリング サービスに送信するユーザ名を指定。 <ul style="list-style-type: none"> • 0 = 実際に認証されたユーザ名を送信 (デフォルト) • 1 = 空白のユーザ名を送信 • 2 = auth_name_string で指定された文字列を送信
auth_name_string	use_alias=2 の場合にのみ有効。このルールを使用して認証に成功したすべてのユーザーのユーザー名として送信される静的文字列。

下記の表は、統合 Windows 認証のルールで使用される追加タグをリストしています。

IWA タグ	使用できる値
winauth_realm	ルールで使用する結合 Windows ドメインを指定。Content Gateway は、このドメイン内で結合されアクティブにされる必要があります。

下記の表は、NTLM ルールで使用される追加タグをリストしています。

一般タグ	使用できる値
dc_list	プライマリ ドメイン コントローラの IP アドレスとポート番号を指定 (ポートが指定されていない場合、Content Gateway はポート 139 を使用)、続けてカンマ区切り形式のリストで、ロード バランシングとフェールオーバーに使用するとセカンダリ ドメイン コントローラを指定。
dc_load_balance (オプション)	ロード バランシングを使用するかどうかを指定： <ul style="list-style-type: none"> • 0 = 無効 • 1 = 有効 <p>ご注意： 複数のドメイン コントローラが指定されている時には、ロード バランスが無効化されている場合でも、プライマリ ドメイン コントローラの負荷が許可されている最大の接続数に達したとき、一時的なフェールオーバーの方法として、新しい要求はセカンダリ ドメイン コントローラに送信されます。これはプライマリ ドメイン コントローラが新しい接続を受け入れられるようになるまで継続されます。</p>

下記の表は、LDAP ルールで使用される追加タグをリストしています。

LDAP タグ	使用できる値
server_name	LDAP サーバーの完全修飾ドメイン名を指定。
server_port (オプション)	LDAP サーバーのポートを指定。デフォルト値は 389 です。 Secure LDAP が有効な場合、ポート 636 または 3269 (セキュア LDAP ポート) を指定。
base_dn (オプション)	LDAP ベース識別名を指定。
uid_filter (オプション)	LDAP タブの設定と異なる場合に、サービス タイプを指定。Active Directory の場合は sAMAccountName を入力し、他のサービスの場合は uid を指定します。
bind_dn (オプション)	バインド識別名を指定。これは LDAP ディレクトリ サービスのユーザーの完全識別名でなければなりません。例： CN=John Smith,CN=USERS,DC=MYCOMPANY,DC=COM
bind_pwd (オプション)	バインド識別名のパスワードを指定。
sec_bind	Content Gateway が LDAP サーバーとセキュア通信を行うかどうかを指定。 <ul style="list-style-type: none"> • 0 = 無効 • 1 = 有効 <p>有効にした場合、LDAP ポードは 636 または 3269 (セキュア LDAP ポート) に設定されます。</p>

LDAP タグ	使用できる値
attr	LDAP 属性名を指定。
attr_value	LDAP 属性値を指定。

例

統合 Windows 認証:

```
type=winauth name=CorpHQ src_ip=10.1.1.1,10.10.0.0-10.100.254.254 proxy_port=0 status=1 domain=BigCorp.com
```

NTLM:

```
type=ntlm name=CorpHQ src_ip=10.1.1.1,12.13.0.0-12.13.0.128 dc_list=HQdc1.BigCorp.com,HQdc2.BigCorp.com
```

LDAP:

```
type=ldap name=CorpHQ src_ip=10.1.1.1,12.13.0.0-12.13.0.128 server_name=HQldap1.BigCorp.com server_port=389
```



ご注意

リストされた順序で最初に一致したルールが適用されます。

bypass.config

bypass.config ファイルには、Content Gateway が透過プロキシ モードで使用する **静的バイパス** ルールが含まれます。静的バイパス ルールは、Content Gateway に特定の着信クライアント要求をバイパスし、オリジン サーバーによって処理されるよう指示します。

また、**bypass.config** ファイルは **動的バイパス拒否ルール** に対応しています。[動的バイパス拒否ルール, 373 ページ](#) を参照してください。

3 つのタイプの静的バイパス ルールを設定できます。

- ◆ **送信元バイパスルール**は、特定の送信元IPアドレスまたはIPアドレスの範囲を迂回するようプロキシを設定します。たとえば、キャッシュを使用させたくないクライアントを迂回させることができます。
- ◆ **宛先バイパスルール**は、特定の宛先元IPアドレスまたはIPアドレスの範囲を迂回するようプロキシを設定します。たとえば、クライアントの実際のIPアドレスを基にIP認証を使用するオリジンサーバーを迂回できます。



重要

宛先バイパス ルールは、プロキシがサイト全体をキャッシュすることを防止します。迂回したサイトが人気のあるサイトである場合、ヒット率への影響が顕著に表れます。

- ◆ **送信元／宛先ペアバイパスルール**は、指定の送信元から指定の宛先へ発信する要求を迂回するようプロキシを設定します。たとえば、IP 認証が破られた、またはキャッシュ時に帯域外の HTTP トラフィックの問題があるクライアント／サーバー ペアを迂回することができます。送信元／宛先バイパスルールは、宛先サーバーを、問題が発生したユーザーに対してのみブロックしますから、宛先バイパスルールよりも適切です。

フォーマット

バイパスルールは次の形式になります：

```
bypass src ipaddress | dst ipaddress | src ipaddress AND dst
ipaddress
```

オプション	説明
<code>src <i>ipaddress</i></code>	<p>プロキシが迂回するべき着信要求内の送信元(クライアント)IP アドレスを指定。</p> <p><i>ipaddress</i> は 以下のいずれかになります：</p> <p>123.45.67.8 等の単一 IP アドレス</p> <ul style="list-style-type: none"> • 1.1.1.0/24 等の CIDR(Classless Inter-Domain Routing) 形式 • 1.1.1.1-2.2.2.2 等のダッシュで区切られたアドレス範囲 • 1.1.1.0/24, 25.25.25.25, 123.1.23.1-123.1.23.123等のコンマで区切られた上記の組み合わせ。
<code>dst <i>ipaddress</i></code>	<p>プロキシが迂回するべき着信要求内の宛先(オリジンサーバー)IP アドレスを指定。</p> <p><i>ipaddress</i> は 以下のいずれかになります：</p> <p>123.45.67.8 等の単一 IP アドレス</p> <ul style="list-style-type: none"> • 1.1.1.0/24 等の CIDR(Classless Inter-Domain Routing) 形式 • 1.1.1.1-2.2.2.2 等のダッシュで区切られたアドレス範囲 • 1.1.1.0/24, 25.25.25.25, 123.1.23.1-123.1.23.123等のコンマで区切られた上記の組み合わせ。
<code>src <i>ipaddress</i> および dst <i>ipaddress</i></code>	<p>プロキシが迂回するべき送信元／宛先 IP アドレスのペアを指定。</p> <p><i>ipaddress</i> は 123.45.67.8 等の単一 IP アドレスである必要があります。</p>

動的バイパス拒否ルール

静的バイパスルールに加えて、`bypass.config` ファイルは**動的バイパス拒否**ルールに対応しています。

バイパス拒否ルールは、プロキシに特定の着信クライアント要求が迂回することを動的に禁止させます(バイパス拒否ルールは、プロキシが自分を迂回することを禁止できます)。動的バイパス拒否ルールは、送信元、宛先、送信元／宛先を指定でき、次の形式になります：

```
deny_dyn_bypass src ipaddress | dst ipaddress | src  
ipaddress AND dst ipaddress
```

オプションの説明は、[フォーマット, 373 ページ](#)の表を参照してください。



ご注意

動的バイパス拒否ルールを動作させるには、Content Gateway Manager で **[Dynamic Bypass]** オプションを有効にするか、**records.config** ファイルで、
`proxy.config.arm.bypass_dynamic_enabled` 変数を 1 に設定する必要があります。



重要

静的バイパス ルールは 動的バイパス拒否ルールを上書きします。従って、静的バイパス ルールと動的バイパス拒否ルールが同じ IP アドレスを含む場合、動的バイパス拒否ルールは無視されます。

例

下記の例は、送信元、宛先、送信元 / 宛先のバイパスルールを示しています：

```
bypass src 1.1.1.0/24, 25.25.25.25, 128.252.11.11-  
128.252.11.255  
bypass dst 24.24.24.0/24  
bypass src 25.25.25.25 AND dst 24.24.24.0
```

下記の例は、送信元、宛先、送信元 / 宛先の動的バイパス拒否ルールを示しています：

```
deny_dyn_bypass src 128.252.11.11-128.252.11.255  
deny_dyn_bypass dst 111.111.11.1  
deny_dyn_bypass src 111.11.11.1 AND dst 111.11.1.1
```

cache.config

cache.config ファイルは プロキシが Web オブジェクトをキャッシュする方法を指定します。下記の設定を指定することで、キャッシング ルールを追加できます：

- ◆ 特定の IP アドレスのオブジェクトのキャッシュを否定
- ◆ 特定のオブジェクトをキャッシュ内に留める時間を指定
- ◆ キャッシュされたオブジェクトが最新であると見なされる時間を指定

- ◆ サーバーからの no-cache 指示を無視するかどうか



重要

このファイルを変更した後は、変更を適用するために、Content Gateway の bin ディレクトリ (/opt/WCG/bin) で `content_line -x` を実行してください。クラスタ内の1つのノードに変更を適用した場合、Content Gateway はクラスタ内のすべてのノードに変更を適用します。

フォーマット

`cache.config` ファイルの各行には、キャッシュルールが含まれます。Content Gateway は 3 つのスペース区切りのタグを認識します：

```
primary_destination=value secondary_specifier=value
action=value
```

下記の表は、使用可能な一次宛先とその値をリストしています。

一次宛先	使用できる値
dest_domain	要求されたドメイン名。
dest_host	要求されたホスト名。
dest_ip	要求された IP アドレス。
url_regex	URL に含まれる正規表現。

`cache.config` ファイルで二次指定子は任意です。下記の表は、使用可能な二次指定子とその値をリストしています。



ご注意

ルールの中で 1 つ以上の二次指定子を使用できます。ただし、1 つの二次指定子を繰り返すことはできません。

二次指定子	使用できる値
port	要求された URL のポート。
scheme	要求 URL のプロトコル。次の内の 1 つ： <ul style="list-style-type: none"> • HTTP • FTP
prefix	URL のパス部分の接頭辞。
suffix	URL のファイル接尾辞。

二次指定子	使用できる値
method	要求 URL のメソッド。次の内の 1 つ： <ul style="list-style-type: none"> • get • put • trace
time	時間範囲（例、08:00–14:00）。
src_ip	クライアント IP アドレス。
user_agent	要求ヘッダーのユーザー エージェントの値。

下記の表は、使用可能なアクションとその値をリストしています。

アクション	値
action	次の値の内の 1 つ： <ul style="list-style-type: none"> • never-cache は、プロキシが指定したオブジェクトをキャッシュしないよう設定します。 • ignore-no-cache は、プロキシがすべての Cache-Control: no-cache ヘッダーを無視するように設定します。 • ignore-client-no-cache は、プロキシがクライアント要求の Cache-Control: no-cache ヘッダーを無視するように設定します。 • ignore-server-no-cache は、プロキシがオリジン サーバー応答の Cache-Control: no-cache ヘッダーを無視するように設定します。
pin-in-cache	オブジェクトがキャッシュ内に留まる時間。次の時間形式で入力できます： <ul style="list-style-type: none"> • <i>d</i> 日付（例 2d） • <i>h</i> 時間（例 10h） • <i>m</i> 分（例 5m） • <i>s</i> 秒（例 20s） • 組み合わせ（例 1h15m20s）
revalidate	オブジェクトが、キャッシュ内で最新と見なされる時間。pin-in-cache と同じ時間形式を使用します。
ttl-in-cache	Cache-Control 応答ヘッダーに関係なく、キャッシュ内にオブジェクトを保持する時間。pin-in-cache および revalidate と同じ時間形式を使用します。

例

下記の例は、IP アドレス 112.12.12.12 から要求された FTP ドキュメントをキャッシュしないようにプロキシを設定します。

```
dest_ip=112.12.12.12 scheme=ftp action=never-cache
```

下記の例は、正規表現 `politics` とパス `prefix/viewpoint` を含む URL のドキュメントを 12 時間の間キャッシュ内に保持するように、プロキシを設定します。

```
url_regex=politics prefix=/viewpoint pin-in-cache=12h
```

下記の例は、`mydomain.com` 内の `gif` および `jpeg` オブジェクトを 6 時間毎に再確認し、`mydomain.com` 内のその他のオブジェクトを 1 時間毎に再確認するように、プロキシを設定します。

```
dest_domain=mydomain.com suffix=gif revalidate=6h
dest_domain=mydomain.com suffix=jpeg revalidate=6h
dest_domain=mydomain.com revalidate=1h
```



ご注意

ルールはリストされた順に適用されます。

filter.config

`filter.config` に保存されたフィルタリング ルールで次のことができます：

- ◆ URL 要求を拒否または許可する
- ◆ クライアント要求のヘッダー情報を保持または削除する
- ◆ カスタム ヘッダーを挿入する
- ◆ 指定したアプリケーション、または指定した Web サイトの要求が認証をバイパスすることを許可する
- ◆ 指定したアプリケーションがプロキシを通過することを禁止する

フィルタリング ルールは、Content Gateway Manager 内の「**Configure**」>「**Security**」>「**Access Control**」>「**Filtering**」タブ上で定義されます。[フィルタリング ルールの作成, 188 ページ](#)を参照してください。



ご注意

NTLM および LDAP のフィルタリング ルールは、「**Access Control**」>「**Authentication Realms**」タブで定義され、[auth.config](#) ファイルに保存されます。



重要

このファイルを変更した後は、変更を適用するために、Content Gateway の `bin` ディレクトリ (`/opt/WCG/bin`) で `content_line -x` を実行してください。クラスタ内の 1 つのノードに変更を適用した場合、Content Gateway はクラスタ内のすべてのノードに変更を適用します。

フォーマット

`filter.config` の各行がフィルタリングルールです。Content Gateway は、ファイルの上位から開始し、リストされた順にルールを適用します。条件に一致するルールがない場合、要求は処理されます。

Content Gateway は 3 つのスペース区切りのタグを認識します：

```
primary_destination=value secondary_specifier=value action=value
```

下記の表は、使用可能な一次宛先タイプをリストしています。

一次宛先タイプ	使用できる値
dest_domain	要求されたドメイン名。
dest_host	要求されたホスト名。
dest_ip	要求された IP アドレス。
url_regex	URL に含まれる正規表現。

二次指定子は任意です。下記の表は、使用可能な二次指定子とその用途をリストしています。



ご注意

ルールの中で 1 つ以上の二次指定子を使用できます。ただし、1 つの二次指定子を繰り返すことはできません。

二次指定子	使用できる値
time	時間範囲 (例、08:00–14:00)。
prefix	URL のパス部分の接頭辞。
suffix	URL のファイル接尾辞。
src_ip	単一のクライアント IP アドレス、またはクライアント IP アドレスの範囲。
port	要求された URL のポート。
method	要求 URL のメソッド。次の内の 1 つ： <ul style="list-style-type: none"> • get • post • put • trace

二次指定子	使用できる値
scheme	要求 URL のプロトコル。以下のいずれかを指定できます： <ul style="list-style-type: none"> • HTTP • HTTPS • FTP (FTP over HTTP のみ)
user_agent	要求ヘッダーのユーザー エージェントの値。

下記の表は、使用可能なアクションとその値をリストしています。

アクション	使用できる値
action	次の内の 1 つを指定します： <ul style="list-style-type: none"> • [allow] – 特定の URL 要求が認証をバイパスすることを許可します。プロキシは要求されたコンテンツをキャッシュに入れ、提供します。 • [deny] – 特定の宛先からの HTTP または FTP オブジェクトの要求を拒否します。要求が拒否されたとき、クライアントはアクセス拒否メッセージを受け取ります。 • [radius] – サポートされていません。
keep_hdr	保持するクライアント要求ヘッダー情報。以下のオプションを指定できます： <ul style="list-style-type: none"> • date • host • cookie • client_ip
strip_hdr	削除するクライアント要求ヘッダー情報。 keep_hdr と同じオプションを指定できます。
add_hdr	追加するカスタム ヘッダー値。カスタム ヘッダーとヘッダー値が指定されている必要があります。例： <pre>add_hdr="header_name:header_value"</pre>

例

下記の例は、IP アドレス 112.12.12.12 に対するすべての FTP ドキュメント要求を拒否するように、Content Gateway を設定します：

```
dest_ip=112.12.12.12 scheme=ftp action=deny
```

下記の例は、正規表現 `politics` とパス接頭辞 `/viewpoint` を含む URL 要求のクライアント IP アドレス ヘッダーを保持するように、Content Gateway を設定します：

```
url_regex=politics prefix=/viewpoint keep_hdr=client_ip
```

下記の例は、オリジン サーバー `www.server1.com` 宛てのクライアント要求のすべてのクッキーを削除するように、Content Gateway を設定します：

```
dest_host=www.server1.com strip_hdr=cookie
```

下記の例は、オリジン サーバー **www.server2.com** への **put** を非許可にするように、Content Gateway を設定します：

```
dest_host=www.server2.com method=put action=deny
```

Content Gateway は、ファイルにリストされた順にルールを適用します。たとえば、下記のサンプル **filter.config** ファイルは、次の動作をさせるように Content Gateway を設定します：

- ◆ server1.com へのアクセスをすべてのユーザーに許可 (internal.com へのアクセス試行を除く)
- ◆ notthatsite.com へのアクセスをすべてのユーザーに拒否

```
dest_host=server1.com action=allow
```

```
dest_host=notthatsite.com action=deny
```

hosting.config

hosting.config ファイルを利用して、キャッシュ パーティションを特定のオリジン サーバーとドメインに割り当てることで、キャッシュ スペースをより効率的に管理し、ディスクの使用を制限することができます。

オリジン サーバーとドメイン別のキャッシュのパーティショニングの順を追った使用手順は、[オリジン サーバーまたはドメインに基づくキャッシュのパーティション区分, 102 ページ](#)を参照してください。



ご注意

特定のオリジン サーバーとドメインにキャッシュ パーティションを割り当てる前に、**partition.config** ファイルで、サイズとプロトコルに基づいてキャッシュを分割する必要があります。キャッシュ パーティションに関する情報は、[キャッシュのパーティション区分, 101 ページ](#)を参照してください。**partition.config** ファイルの説明は、[partition.config, 396 ページ](#)を参照してください。

hosting.config ファイルを変更した後は、変更を適用するために、Content Gateway の **bin** ディレクトリで **content_line -x** を実行してください。クラスタ内の1つのノードに変更を適用した場合、Content Gateway は自動的にクラスタ内のすべてのノードに変更を適用します。



重要

パーティション構成は、クラスタ中のすべてのノードで同一でなければなりません。

フォーマット

`hosting.config` ファイルの各行は、下記の形式のいずれかである必要があります：

```
hostname=hostname partition=partition_numbers
domain=domain_name partition=partition_numbers
```

ここで：

hostname は、コンテンツを特定のパーティションに保存させるオリジンサーバーの完全修飾ホスト名です（例 `www.myhost.com`）。

domain_name は、コンテンツを特定のパーティション保存させるドメイン名です（例 `mydomain.com`）。

partition_numbers は、リストされたオリジンサーバーまたはドメインのコンテンツを保存させるパーティションのカンマ区切り形式のリストです。パーティション番号は、`partition.config` ファイルにリストされた有効な番号でなければなりません（[partition.config, 396 ページ](#)を参照）。



ご注意

オリジンサーバーまたはドメインに1つ以上のパーティションを割り当てる場合、1行にカンマ区切り形式のリストでパーティションを入力します。`hosting.config` ファイルに、同じオリジンサーバーまたはドメインの複数のエントリを含めることはできません。

汎用パーティション

`hosting.config` ファイルの設定時に、どのオリジンサーバーまたはドメインにも属さないコンテンツのために使用する汎用パーティションを割り当てる必要があります。特定のオリジンサーバーのためのすべてのパーティションが破損した場合、Content Gateway はオリジンサーバーのコンテンツを保存するために汎用パーティションを使用します。

汎用パーティションは次の形式である必要があります：

```
hostname=* partition=partition_numbers
```

ここで、**partition_numbers** は汎用パーティションのカンマ区切り形式のリストです。

例

下記の例は、ドメイン `mydomain.com` のコンテンツをパーティション 1 に、ドメイン `www.myhost.com` のコンテンツをパーティション 2 に保存するようにプロキシを設定します。プロキシはすべてのオリジンサーバーのコンテンツをパーティション 3 と 4 に保存します。

```
domain=mydomain.com partition=1
hostname=www.myhost.com partition=2
hostname=* partition=3,4
```

ip_allow.config

ip_allow.config ファイルは プロキシに対するクライアントのアクセスを制御します。Content Gateway を使用することを許可する IP アドレスの範囲を指定できます。



重要

このファイルを変更した後は、変更を適用するために、Content Gateway の **bin** ディレクトリ (`/opt/WCG/bin`) で `content_line -x` を実行してください。クラスタ内の1つのノードに変更を適用した場合、Content Gateway は クラスタ内のすべてのノードに変更を適用します。

フォーマット

ip_allow.config ファイルの各行は 次の形式である必要があります：

```
src_ip=ipaddress action=ip_allow | ip_deny
```

ここで、*ipaddress* は プロキシへのアクセスを許可するクライアントの IP アドレスまたは IP アドレス範囲です。

アクション `ip_allow` は 指定したクライアントがプロキシへアクセスすることを許可します。

アクション `ip_deny` は 指定したクライアントがプロキシへアクセスすることを拒否します。

デフォルトでは、**ip_allow.config** ファイルは 次の行を含み、すべてのクライアントにプロキシへアクセスすることを許可します。アクセス制限のルールを追加する前に、この行をコメントアウトするか、削除してください。

```
src_ip=0.0.0.0-255.255.255.255 action=ip_allow
```

例

下記の例は、すべてのクライアントにプロキシへアクセスすることを許可します。

```
src_ip=0.0.0.0-255.255.255.255 action=ip_allow
```

下記の例は、特定のサブネット上のすべてのクライアントにプロキシへアクセスすることを許可します。

```
src_ip=123.12.3.000-123.12.3.123 action=ip_allow
```

下記の例は、特定のサブネット上のすべてのクライアントにプロキシへアクセスすることを拒否します。

```
src_ip=123.45.6.0-123.45.6.123 action=ip_deny
```

ipnat.conf

ipnat.conf ファイルには、プロキシが透過的にトラフィックを処理するとき、着信パケットのアドレスを変更する方法を指定するリダイレクト ルールが含まれます。Content Gateway はインストール時にリダイレクト ルールを作成します。これらのルールを変更できます。



重要

このファイルを変更したらコンピュータを再起動する必要があります。

フォーマット

ipnat.conf ファイルの各行は 次の形式である必要があります：

```
rdr interface 0.0.0.0/0 port dest -> ipaddress port proxy  
tcp|udp
```

ここで：

interface は、トラフィックが Content Gateway コンピュータにアクセスするために使用するイーサネット インタフェースです（例 Linux 上の場合 *eth0*）。

dest は トラフィックの宛先ポートです（例 HTTP トラフィックの場合 80）。

ipaddress は Content Gateway サーバーの IP アドレス。

proxy は Content Gateway のプロキシ ポート（HTTP トラフィックの場合、通常 8080）。

例

下記の例は、すべての着信 HTTP トラフィックを、Content Gateway の IP アドレス (111.111.11.1) の Content Gateway のプロキシ ポート (8080) へアドレス変更するように、ARM を設定します：

```
rdr hme0 0.0.0.0/0 port 80 -> 111.111.11.1 port 8080 tcp
```

log_hosts.config

異なるオリジン サーバーの HTTP/FTP トランザクションを個別のログ ファイルに記録するには、**log_hosts.config** ファイルに各オリジン サーバーのホス

ト名をリストしなければなりません。さらに、HTTP ホスト分割オプションを有効にする必要があります ([HTTP ホスト ログ分割, 248 ページ](#)を参照)。



ご注意

クラスタ内の各 Content Gateway ノードで、同じ `log_hosts.config` ファイルを使用することが推奨されます。



重要

このファイルを変更した後は、変更を適用するために、Content Gateway の `bin` ディレクトリ (`/opt/WCG/bin`) で `content_line -x` を実行してください。クラスタ内の 1 つのノードに変更を適用した場合、Content Gateway はクラスタ内のすべてのノードに変更を適用します。

フォーマット

`log_hosts.config` ファイルの各行は 次の形式である必要があります：

```
hostname
```

ここで、`hostname` は オリジン サーバーのホスト名です。



ご注意

`log_hosts.config` ファイルでキーワードを指定し、そのキーワードをホスト名に含むオリジン サーバーのすべてのトランザクションを別個のログ ファイルに記録することができます。下記の例を参照してください。

例

下記の例は、オリジン サーバー `webserver1`、`webserver2`、および `webserver3` のすべての HTTP/FTP トランザクションを含む別個のログ ファイルを作成するように、Content Gateway を設定します：

```
webserver1  
webserver2  
webserver3
```

下記の例は、名前に `sports` を含むオリジン サーバー (例 `sports.yahoo.com` および `www.foxsports.com`) からのすべての HTTP および FTP ランザクションを、`squid-sport.log` (Squid フォーマットが有効な場合) という名前のログ ファイルに保存します：

```
sports
```

logs_xml.config

logs_xml.config ファイルは、カスタム ログ ファイル フォーマット、フィルタ、および 処理オプションを定義します。このファイルのフォーマットは、XML(Extensible Markup Language) モデルです。

フォーマット

logs_xml.config ファイルには下記の定義が含まれます：

- ◆ LogFormat は、各プロトコル イベント アクセスから収集されるフィールドを指定します。[LogFormat, 385 ページ](#)を参照してください。
- ◆ LogFilter は、エントリ内の値を基にログ記録される特定のエントリを含める または 除外するために使用するフィルタを指定します。[LogFilter, 387 ページ](#)を参照してください。
- ◆ LogObject は、特定のフォーマット、ローカル ファイル名、フィルタ、および 照合サーバーを含むオブジェクトを指定します。[LogObject, 388 ページ](#)を参照してください。



ご注意

logs_xml.config ファイルは 余分な空白、空白の行、およびすべてのコメントを無視します。

LogFormat

下記の表は LogFormat の定義をリストしています。

フィールド	使用できる入力値
<code><Name = "valid_format_name"/></code>	必須。使用できるフォーマットの名前は、squid、common、extended、extended2(事前定義されているフォーマット名)を除くすべての名前です。このタグのデフォルト設定はありません。

フィールド	使用できる入力値
<pre data-bbox="351 247 786 300"><Format = "valid_format_specification"/></pre>	<p data-bbox="817 247 1330 485">必須。使用できるフォーマットの定義は、ASCII 形式出力時に各ログ エントリを表す printf スタイルの文字列です。有効なフィールド名のプレースホルダとして、'<code>%(field)</code>' を使用します。詳細情報は、カスタム ログ記録フィールド, 359 ページを参照してください。指定フィールドは 2 つの型を使用できます：</p> <p data-bbox="817 491 1071 522">単純な型：例 <code>%(cqu)</code></p> <p data-bbox="817 529 1330 644">HTTP ヘッダーまたは Content Gateway 統計等のコンテナ内のフィールド。この型のフィールドは 次の書式です： <code>'%(field)container'</code>。</p>
<pre data-bbox="351 663 740 716"><Interval = "aggregate_interval_secs"/></pre>	<p data-bbox="817 663 1330 716">フォーマットに集計演算子が含まれる場合にこのタグを使用します。</p> <p data-bbox="817 722 1330 837">"<code>aggregate_interval_secs</code>" は、個々の集計値が作成される秒単位の間隔を表しています。使用できる集計演算子のセットを次に示します：</p> <ul data-bbox="817 844 940 1026" style="list-style-type: none"> • COUNT • SUM • AVG • FIRST • LAST

LogFilter

下記の表は LogFilter の定義をリストしています。

フィールド	使用できる入力値
<code><Name = "valid_filter_name"/></code>	必須。すべてのフィルタは 固有の名前をもつ必要があります。
<code><Condition = "valid_log_field valid_operator valid_comparison_value"/></code>	<p>必須。このフィールドには次の要素が含まれます：</p> <p><code>valid_log_field</code> - 指定された値に対して比較されるフィールド。詳細情報は、ログ記録フォーマット相互参照, 362 ページを参照してください。</p> <p><code>valid_operator</code> - 次のいずれかになります：<code>MATCH</code>、<code>CASE_INSENSITIVE_MATCH</code>、<code>CONTAIN</code>、<code>CASE_INSENSITIVE_CONTAIN</code>。<code>MATCH</code> フィールドと値が同じ場合に true になります（大文字と小文字を区別）。<code>CASE_INSENSITIVE_MATCH</code> 大文字と小文字を区別しない以外は <code>MATCH</code> と同じ。<code>CONTAIN</code> フィールドが値を含む場合に true になります（値はフィールドの部分文字列になります）。<code>CASE_INSENSITIVE_CONTAIN</code> は <code>CONTAIN</code> の大文字と小文字を区別しないバージョンです。</p> <p><code>valid_comparison_value</code> - フィールドタイプに一致する整数または文字列。整数値の場合、演算子はすべて等価演算子で、フィールドが指定された値と等しくなければならないことを意味します。</p> <p>ご注意： 否定比較演算子は存在しません。否定条件を指定したい場合、Action フィールドに <code>REJECT</code> を使用します。</p>
<code><Action = "valid_action_field"/></code>	必須。 <code>ACCEPT</code> または <code>REJECT</code> 。これは、フィルタの条件を満足するレコードを受け入れるか、拒否するかを Content Gateway に指示します。

LogObject

下記の表は LogObject の定義をリストしています。

フィールド	使用できる入力値
<Format = "valid_format_name"/>	必須。使用できるフォーマットの名前は、事前定義された次のログ記録フォーマットです：事前定義されたカスタム ログフォーマットと squid、common、extended、extended2。このタグのデフォルト設定はありません。
<Filename = "file_name"/>	必須。ローカル システムまたはリモート照会サーバー上で書き込まれるログ ファイルのファイル名。このタグを指定し損なった場合、ローカル ログ ファイルは作成されません。すべてのファイル名は、デフォルトログ記録ディレクトリからの相対位置になります。 名前に特定の拡張子（例 squid）が含まれない場合、ASCII 形式のログには 拡張子 .log が、バイナリ形式のログには .blog が自動的に付加されます。（後述の <Mode = "valid_logging_mode"/> を参照）拡張子を付加したくない場合は、ファイル名の最後をドット（.）で終わります：例 squid。

フィールド	使用できる入力値
<code><Mode = "valid_logging_mode"/></code>	<p>使用できるログ記録モードは、<code>ascii</code>、<code>binary</code>、および <code>ascii_pipe</code> です。デフォルトは <code>ascii</code> です。</p> <p>人が読みとれる形式（プレーン ASCII）のイベント ログ ファイルを作成するには、<code>ascii</code> を使用します。</p> <p>バイナリ形式のイベント ログ ファイルを作成するには、<code>binary</code> を使用します。バイナリ形式のログ ファイルは、システム オーバヘッドが小さく、ディスクスペースが少なくてすみずみ（ログ記録される情報に依存します）。バイナリ形式のログ ファイルを ASCII 形式に変換するためには、<code>logcat</code> ユーティリティを使用する必要があります。</p> <p>UNIX 名前付きパイプ（メモリ中のバッファ）にログ エントリを書き込むには、<code>ascii_pipe</code> を使用します。他のプロセスが標準 I/O 機能によりデータを読めるようになります。Content Gateway によるハードディスク書き込みが不要になり、ディスクスペースと帯域幅が他のタスクのために解放されます。また、UNIX 名前付きパイプはディスクスペースを使用しないので、ログ記録スペースが使い尽くされても、パイプへの書き込みは中断しません。</p> <p>ご注意：照合サーバーを使用している場合、ログは照合サーバー上のパイプに書き込まれます。トランザクションが処理される前でも、ローカルパイプは作成されます。従って、Content Gateway 起動直後にパイプを参照できます。ただし、照合サーバー上のパイプは Content Gateway が起動した時に作成されず。</p>
<code><Filters = "list_of_valid_filter_names"/></code>	<p>前に定義されたログ フィルタ名のカンマ区切り形式のリスト。1つ以上のフィルタが指定されている場合、レコードがログ記録されるためには、すべてのフィルタがレコードを受け入れる必要があります。</p>
<code><Protocols = "list_of_valid_protocols"/></code>	<p>ログ記録されるべきオブジェクトのプロトコルのカンマ区切り形式のリスト。使用できるプロトコル名は <code>HTTP</code> です。</p>
<code><ServerHosts = "list_of_valid_servers"/></code>	<p>ホスト名のカンマ区切り形式のリスト。このタグは、ファイルに含まれる名前付のサーバーのエントリのみを示します。</p>
<code><CollationHosts = "list_of_valid_hostnames"/></code>	<p>（このオブジェクトの）すべてのログ エントリが転送される照合サーバーのカンマ区切り形式のリスト。照合サーバーは、名前または IP アドレスで指定できます。名前の後のコロンで照合ポートを指定します（例 <code>host:port</code>）。</p>

フィールド	使用できる入力値
<code><Header = "header"/></code>	ログ ファイルに含めるヘッダー テキスト。ヘッダ テキストは、ログ ファイルの冒頭で最初のレコードの直前に表示されます。
<code><RollingEnabled = "truth value"/></code>	<i>LogObject</i> のログ ファイル取り込みを有効化または無効化します。この設定は、Content Gateway Manager の設定 [Log Rolling: Enabled/Disabled]、または <code>records.config</code> ファイルの <code>proxy.config.log2.rolling_enabled</code> を上書きします。 取り込みを有効にするには、“truth value” を 1 または true に設定します。この特定の <i>LogObject</i> の取り込みを無効にするには、0 または false に設定します。
<code><RollingIntervalSec = "seconds"/></code>	<i>LogObject</i> のログ ファイル取り込みの秒単位の間隔を指定します。この設定は、Content Gateway Manager の設定 [Log Rolling: Interval]、または <code>records.config</code> ファイルの <code>proxy.config.log2.rolling_interval_sec</code> を上書きします。このオプションで、異なる <i>LogObjects</i> に異なる取り込み間隔を指定できます。
<code><RollingOffsetHr = "hour"/></code>	取り込み “整列” させる時間 (0 から 23) を指定します。その時間より前に取り込みが開始されることがありますが、取り込みファイルはその時間に作成されます。取り込み間隔が 1 時間より大きい場合に、この設定の影響が重要になります。この設定は、Content Gateway Manager の設定 [Log Rolling: Offset Hour]、または <code>records.config</code> ファイルの <code>proxy.config.log2.rolling_offset_hr</code> を上書きします。

例

下記は、3 つのカンマ フィールドを使用して情報収集する `LogFormat` の定義の例です：

```
<LogFormat>
  <Name = "minimal"/>
  <Format = "%<chi> : %<cqu> : %<pssc>"/>
</LogFormat>
```

下記は、集計演算子を使用した `LogFormat` の定義の例です：

```
<LogFormat>
  <Name = "summary"/>
  <Format = "%<LAST(cqts)> : %<COUNT(*)> : %<SUM(psql)>"/>
```

```
<Interval = "10"/>
</LogFormat>
```

下記は、REFRESH_HIT エントリのみによりログ記録する LogFilter の定義の例です：

```
<LogFilter>
<Name = "only_refresh_hits"/>
<Action = "ACCEPT"/>
<Condition = "%<pssc> MATCH REFRESH_HIT"/>
</LogFilter>
```



ご注意

フィルタ条件フィールドを指定する時に、%< を省略することができます。これは、下記のフィルタが上記同じであることを意味します。

```
<LogFilter>
  <Name = "only_refresh_hits"/>
  <Action = "ACCEPT"/>
  <Condition = "pssc MATCH REFRESH_HIT"/>
</LogFilter>
```

下記は、前に定義した最小限の形式でローカル ログ ファイルを作成する LogObject の定義の例です：これは ASCII ログ ファイル（デフォルト）なので、ログ ファイル名は **minimal.log** になります。

```
<LogObject>
<Format = "minimal"/>
<Filename = "minimal"/>
</LogObject>
```

下記は、ドメイン **company.com** のホスト、または 指定のサーバー **server.somewhere.com** で処理される HTTP 要求のみを含める LogObject の定義の例です：ログ エントリは、照合ホスト **logs.company.com** のポート 4000 と、照合ホスト **209.131.52.129** のポート 5000 に送信されます。

```
<LogObject>
<Format = "minimal"/>
<Filename = "minimal"/>
<ServerHosts = "company.com,server.somewhere.com"/>
<Protocols = "http"/>
<CollationHosts =
"logs.company.com:4000,209.131.52.129:5000"/>
</LogObject>
```

WELF (WebTrends Enhanced Log Format)

Content Gateway は、WELF(WebTrends Enhanced Log Format) をサポートしており、WebTrend レポートツールを使用して、Content Gateway のログ ファイルを分析することができます。WELF 互換の定義済みの <LogFormat> は、**logs.config** ファイルの最後に指定されます（下記参照）。WELF 形式の

ログ ファイルを作成するためには、この定義済みフォーマットを使用する `<LogObject>` を作成します。

```
<LogFormat>
<Name = "welf"/>
<Format = "id=firewall time=\"%<cqtd> %<cqtt>\\" fw=%<phn>
pri=6 proto=%<cqus> duration=%<ttmsf> sent=%<psql>
rcvd=%<cqhl> src=%<chi> dst=%<shi> dstname=%<shn>
user=%<caun> op=%<cqhm> arg=\"%<cqup>\\" result=%<pssc>
ref=\"%<{Referer}cqhq>\\" agent=\"%<{user-agent}cqhq>\\"
cache=%<crc>"/>
</LogFormat>
```

mgmt_allow.config

`mgmt_allow.config` ファイルは、Content Gateway Manager へのアクセスを許可または拒否するリモート ホストの IP アドレスを指定します。



重要

このファイルを変更した後は、変更を適用するために、Content Gateway の `bin` ディレクトリ (`/opt/WCG/bin`) で `content_line -x` を実行してください。クラスタ内の 1 つのノードに変更を適用した場合、Content Gateway は クラスタ内のすべてのノードに変更を適用します。

フォーマット

`mgmt_allow.config` ファイルの各行は 次の形式である必要があります：

```
src_ip=ipaddress action=ip_allow|ip_deny
```

ここで、`ipaddress` は、Content Gateway Manager へのアクセスを許可される IP アドレスまたは IP アドレス範囲です。

`action` は、Content Gateway Manager へのアクセスを許可するためには `ip_allow` を、アクセスを拒否するためには `ip_deny` を指定します。

デフォルトでは、`mgmt_allow.config` は下記の行を含み、すべてのリモート ホストが Content Gateway Manager にアクセスすることを許可します。アクセス制限のルールを追加する前に、この行をコメントアウトするか、削除してください。

```
src_ip=0.0.0.0-255.255.255.255 action=ip_allow
```

例

下記の例は、Content Gateway Manager へのアクセスを一人のユーザーのみに許可するように、Content Gateway を設定します：

```
src_ip=123.12.3.123 action=ip_allow
```

下記の例は、特定の IP アドレス範囲が Content Gateway Manager へのアクセスを許可するように、Content Gateway を設定します：

```
src_ip=123.12.3.000-123.12.3.123 action=ip_allow
```

下記の例は、IP アドレス 123.45.67.8 が Content Gateway Manager へのアクセスを拒否するように、Content Gateway を設定します：

```
src_ip=123.45.67.8 action=ip_deny
```

parent.config

parent.config ファイルは、HTTP キャッシュ階層の中で使用される HTTP 親プロキシを指定します。下記の設定を実行するために、このファイルを使用します。

- ◆ 複数の親および親フェールオーバーの親キャッシュ階層を設定
- ◆ 親プロキシを迂回する URL 要求を設定

ルールはリストの上から順にチェックされ、最初に条件に一致するルールが適用されます。通常、バイパスルールは親プロキシ指定ルールの上位に位置します。

HTTP 親キャッシュ オプションが有効な場合にのみ、Content Gateway は **parent.config** ファイルを使用します。[HTTP 親キャッシュを使用する Content Gateway の構成, 94 ページ](#)を参照してください。



重要

このファイルを変更した後は、変更を適用するために、Content Gateway の **bin** ディレクトリ (`/opt/WCG/bin`) で `content_line -x` を実行してください。クラスタ内の1つのノードに変更を適用した場合、Content Gateway はクラスタ内のすべてのノードに変更を適用します。

フォーマット

parent.config ファイルの各行は親キャッシュのルールを含む必要があります。Content Gateway は 3 つのスペース区切りのタグを認識します：

```
primary_destination=value secondary_specifier=value  
action=value
```

下記の表は、使用可能な一次宛先とその値をリストしています。

一次宛先	使用できる値
dest_domain	要求されたドメイン名。
dest_host	要求されたホスト名。
dest_ip	要求された IP アドレスまたはのダッシュ (-) で区切られた IP アドレス範囲。
url_regex	URL に含まれる正規表現。

parent.config ファイルで二次指定子は任意です。下記の表は、使用可能な二次指定子とその値をリストしています。

二次指定子	使用できる値
time	08:00-14:00等の親キャッシュ要求を処理する時間範囲。
prefix	URL のパス部分の接頭辞。
suffix	URL のファイル接尾辞。
src_ip	クライアント IP アドレス。
port	要求された URL のポート。
scheme	要求 URL のプロトコル。次の内の 1 つ： <ul style="list-style-type: none">• HTTP• FTP
method	要求 URL のメソッド。次の内の 1 つ： <ul style="list-style-type: none">• get• post• put• trace
user_agent	要求ヘッダーのユーザー エージェントの値。

下記の表は、使用可能なアクションとその値をリストしています。

アクション	使用できる値
parent	親サーバーの順序立てられたリスト内の最後の親サーバーによって要求が処理されなかった場合、オリジンサーバーにルーティングされます。ホスト名または IP アドレスを指定できます。ポート番号を指定する必要があります。
round_robin	次の値の内の 1 つ： <ul style="list-style-type: none"> • true - Content Gateway はクライアント IP アドレスに基づいたラウンドロビン内の親キャッシュ リストを経由します。 • strict - Content Gateway コンピュータは厳格に順番どおりに要求を処理します。たとえば、コンピュータ proxy1 が最初の要求を処理し、proxy2 が 2 番目の要求を処理するなど。 • false - ラウンド ロビン選択を発生させません。
go_direct	次の値の内の 1 つ： <ul style="list-style-type: none"> • true - 要求は親階層を迂回して、直接オリジンサーバーに向かいます。 • false - 要求は親階層を迂回しません。

例

下記のルールは、Content Gateway (子) と 2 つの親 p1.x.com および p2.x.com で構成される親キャッシュは階層を設定します。round_robin=true であるため、プロキシは処理できない要求を親サーバー p1.x.com および p2.x.com ラウンドロビン方式で転送します。

```
dest_domain=. method=get parent="p1.x.com:8080;
p2.y.com:8080" round_robin=true
```

下記のルールは、正規表現 politics とパス /viewpoint を含むすべての要求を、(親階層を迂回して) 直接オリジンサーバーに送信するように、Content Gateway を設定します：

```
url_regex=politics prefix=/viewpoint go_direct=true
```

下記のルールは、標準的な宛先バイパス ルールです：

```
dest_domain=example.com go_direct=true
```



重要

parent.config ファイルの各行は、parent= または go_direct= ディレクティブの **いずれか** を含む必要があります。

parent= **および** go_direct=true を含むバイパス ルールでは、指定された dest_domain は親に送信され、(通常意図されたアクションとは反対に) その他のすべてのドメインはバイパスされます。

partition.config

partition.config ファイルを使用して、異なるサイズのキャッシュパーティションを作成することで、キャッシュスペースをより効果的に管理できます。**hosting.config** ファイルで、特定のオリジンサーバーおよびドメインからのデータをこれらのパーティションに保存するように設定することができます。これは、コンテンツが稀にしか変更されない頻繁に訪問するサイトのキャッシングに活用できます。



重要

パーティション構成は、クラスタ中のすべてのノードで同一でなければなりません。

キャッシュパーティションサイズを変更する前に、Content Gateway を停止しなければなりません。

フォーマット

作成する各パーティションのために、下記の形式で行を入力します：

```
partition=partition_number scheme=protocol_type
size=partition_size
```

ここで：

partition_number は 1 から 255 までの数字です（パーティションの最大数は 255 です）。

protocol_type は **http** です。



ご注意

現時点では、HTTP のみがサポートされています。ストリーミングメディアコンテンツ **-mixt-** はサポートされていません。

partition_size はパーティションに割り当てられるキャッシュ容量です。値は、全キャッシュ容量に対するパーセンテージか、絶対値のいずれかを指定できます。絶対値は 128 MB の倍数である必要があります。ここで、128 MB は最小値です。パーセンテージを指定した場合、サイズは最も近い 128 MB の倍数のに丸められます。各パーティションは、パラレル I/O を実行するために複数のディスクに分割されます。たとえば、4 つの

ディスクがある場合、1 GB のパーティションは、各ディスク上に 256 MB になります（各ディスクが十分な空き容量をもつ場合）。



ご注意

キャッシュにすべてのディスクを割り当てない場合、追加ディスクスペースは使用できません。既存のパーティションを削除/クリアすることなしに、後で新しいパーティションを作成するために、追加スペースを使用できます。

例

下記の例は、キャッシュを均等にパーティション化します。

```
partition=1 scheme=http size=50%
partition=2 scheme=http size=50%
```

records.config

records.config ファイルは、Content Gateway で使用される設定変数のリストです。

ほとんどの値は、Content Gateway Manager 内のコントロールを使用して設定されます。いくつかのオプションは、**records.config** ファイル内の変数を編集ことでのみ設定できます。



警告

確信がない場合、**records.config** の変数を変更しないでください。多くの変数は組になっており、それらは他の変数に影響します。個別に単一の変数を変更することは、Content Gateway に障害を発生させる原因になります。**可能な限り、Content Gateway の設定には Content Gateway Manager を使用してください。**



重要

このファイルを変更した後は、変更を適用するために、Content Gateway の **bin** ディレクトリ (**/opt/WCG/bin**) で `content_line -x` を実行してください。

クラスタ内の 1 つのノードに変更を適用した場合、Content Gateway は クラスタ内のすべてのノードに変更を適用します。

フォーマット

各変数は次の形式になります：

```
CONFIG variable_name DATATYPE variable_value
```

ここで、*DATATYPE* は INT(整数)、STRING(文字列)、FLOAT(浮動小数点)。

例

下記の例で、変数 `proxy.config.proxy_name` はデータタイプ **文字列** であり、その値が `contentserver1` です。これは、Content Gateway プロキシの名前が `contentserver1` であることを意味します。

```
CONFIG proxy.config.proxy_name STRING contentserver1
```

下記の例で、変数 `proxy.config.winauth.enabled` は、“はい” または “いいえ” のフラグです。0 (ゼロ) は オプションを無効にします。1 (ゼロ) は オプションを有効にします。

```
CONFIG proxy.config.winauth.enabled INT 0
```

下記の例では、クラスタ スタートアップ タイムアウトを 10 秒に設定します。

```
CONFIG proxy.config.cluster.startup_timeout INT 10
```

設定変数

下記の表は、`records.config` ファイル内にリストされた設定変数を説明しています。

[システム変数](#)

[ローカル マネージャー](#)

[仮想 IP マネージャー](#)

[アラーム設定](#)

[ARM](#)

[負荷軽減設定 \(ARM\)](#)

[認証基本レールム](#)

[LDAP](#)

[RADIUS 認証](#)

[NTLM](#)

[統合 Windows 認証](#)

[透過的認証](#)

[HTTP エンジン](#)

親プロキシ設定

キャッシュ コントロール

ヒューリスティック期限

ダイナミック コンテンツおよびコンテンツ ネゴシエーション

匿名 FTP パスワード

キャッシュされた FTP ドキュメントのライフタイム

FTP 転送モード

FTP エンジン

カスタムユーザー応答ページ

SOCKS プロセッサ

ネット サブシステム

クラスタ サブシステム

キャッシュ

DNS

DNS プロキシ

HostDB

ログ記録設定

URL リマップ ルール

スケジュール更新設定

WCCP の設定

SSL 復号化

ICAP

接続性、分析、および境界条件

システム変数

設定変数 データタイプ	データ タイプ	デフォルト値	説明
proxy.config.proxy_name	STRING		Content Gateway ノードの名前を指定します。
proxy.config.bin_path	STRING	bin	Content Gateway の bin ディレクトリの位置を指定します。 これは、インストーラによって Content Gateway のバイナリファイルが配置されるディレクトリです。
proxy.config.proxy_binary	STRING	content_gateway	content_gateway プロセスを実行する実行ファイルの名前を指定します。
proxy.config.proxy_binary_opts	STRING	-M	content_gateway 起動時のコマンドライン オプションを指定します。
proxy.config.manager_binary	STRING	content_manager	content_manager プロセスを実行する実行ファイルの名前を指定します。
proxy.config.cli_binary	STRING	content_line	content_line インターフェースを実行する実行ファイルの名前を指定します。
proxy.config.watch_script	STRING	content_cop	content_cop プロセスを実行する実行ファイルの名前を指定します。
proxy.config.env_prep	STRING	example_prep.sh	content_manager プロセスが content_gateway プロセスを発行する前に、実行されるスクリプトを指定します。
proxy.config.config_dir	STRING	config	Content Gateway 設定ファイルが含まれるディレクトリ(上記の bin_path からの相対)を指定します。
proxy.config.temp_dir	STRING	/tmp	Content Gateway 一時ファイルに使用するディレクトリを指定します。
proxy.config.alarm_email	STRING	websense	Content Gateway が、アラームメッセージを送信する電子メールアドレスを指定します。 インストール中に電子メールアドレスを指定できません。そうでない場合は、Content Gateway は、デフォルト値として Content Gateway ユーザー アカウント名を使用します。

設定変数 データタイプ	データ タイプ	デフォルト値	説明
proxy.config.syslog_ facility	STRING	LOG_DAEMON	システム ログ ファイルを記録するために使用する機能を指定します。 ログ ファイルの使用, 233 ページ を参照してください。
proxy.config.cop.core_ signal	INT	3	content_cop が管理するプロセス content_manager および content_gateway に、それらを停止するために送信するシグナルを指定します。 ご注意： この変数の値を変更しないでください。
proxy.config.cop.sleep_ time	INT	45	content_manager および content_gateway プロセスの状態をテストするために、 content_cop によって実行されるハートビート テストの間隔を秒単位で指定します。 ご注意： この変数の値を変更しないでください。
proxy.config.cop.linux_ min_swapfree_kb	INT	10240	この変数は使用されていません。
proxy.config.cop.linux_ min_memfree_kb	INT	10240	この変数は使用されていません。
proxy.config.output. logfile	STRING	content_gateway .out	Content Gateway プロセスで作成される警告、ステータス、メッセージ、および エラーメッセージを保存するファイルの名前と場所を指定します。 パスが指定されない場合、Content Gateway は このファイルをログ記録ディレクトリに作成します。
proxy.config. snapshot_dir	STRING	snapshots	Content Gateway が 構成のスナップショットを保存するローカルシステム上のディレクトリを指定します。絶対パスを指定しない場合、このディレクトリは Content Gateway config ディレクトリになります。

設定変数 データタイプ	データ タイプ	デフォルト値	説明
proxy.config. attach_debugger_script	STRING	attach_debugger	この変数は、Websense テクニカル サポートからの指示があった場合にのみ使用されるべきです。 セットすると、 content_gateway プロセス再起動時に、デバッグ スクリプト (in /opt/WCG/bin) を実行します。
proxy.config.diags.debug .clients_ips	STRING	NULL	

ローカル マネージャー

設定変数	データ タイプ	デフォルト値	説明
proxy.config.lm.sem_id	INT	11452	ローカル マネージャーのセマフォ ID を指定します。 ご注意： この変数の値を変更しないでください。
proxy.local.cluster.type	INT	3	クラスタ モードを指定します。 <ul style="list-style-type: none"> • 2 = 管理専用モード • 3 = クラスタ化しない
proxy.config.cluster. rsport	INT	8087	信頼できるサービス ポートを指定します。信頼できるサービス ポートはクラスタ内のノード間で設定情報を送信するために使用します。クラスタ内のすべてのノードは同じ信頼できるサービス ポートを使用しなければなりません。
proxy.config.cluster. mcport	INT	8088	マルチキャスト ポートを指定します。マルチキャスト ポートは、ノードの識別のために使用します。クラスタ内のすべてのノードは同じマルチキャスト ポートを使用しなければなりません。
proxy.config.cluster. mc_group_addr	STRING	224.0.1.37	クラスタ通信のためのマルチキャスト アドレスを指定します。クラスタ内のすべてのノードは同じマルチキャスト アドレスを使用しなければなりません。

設定変数	データタイプ	デフォルト値	説明
proxy.config.cluster.mc_ttl	INT	1	クラスタ通信のためのマルチキャスト Time-To-Live を指定します。
proxy.config.cluster.log_bogus_mc_msgs	INT	1	無効なマルチキャストメッセージのログ記録を有効化 (1) または 無効化 (0) します。
proxy.config.admin.html_doc_root	STRING	ui	Content Gateway Manager のドキュメント ルートを指定します。
proxy.config.admin.web_interface_port	INT	8081	Content Gateway Manager ポートを指定します。
proxy.config.admin.autoconf_port	INT	8083	自動構成ポートを指定します。
proxy.config.admin.overseer_port	INT	-1	統計および設定変数を取得 / 設定するポートを指定します。このポートはデフォルトで無効です。
proxy.config.admin.admin_user	STRING	admin	Content Gateway Manager へのアクセスを制御する管理者 ID を設定します。
proxy.config.admin.admin_password	STRING		Content Gateway Manager へのアクセスを制御する管理者パスワードを設定します。パスワードを編集することはできません。しかし、パスワードをクリアするために NULL を指定することはできます。 <i>マスタ管理者パスワードを忘れた場合に Content Gateway Manager にどのようにアクセスしますか</i> , 482 ページを参照してください。
proxy.config.admin.basic_auth	INT	1	Content Gateway Manager へのアクセスを制御する基本ユーザー認証を有効化 (1) または無効化 (0) します。 ご注意: 基本認証が有効でない場合、Content Gateway をモニターおよび設定するために、すべてのユーザーが Content Gateway Manager にアクセスできます。
proxy.config.admin.use_ssl	INT	1	リモートホストと Content Gateway Manager 間でセキュア通信を行うために、Content Gateway Manager SSL オプションを有効にします。

設定変数	データタイプ	デフォルト値	説明
proxy.config.admin.ssl_cert_file	STRING	server.pem	リモートホストと Content Gateway Manager 間でセキュア通信を行うために、Content Gateway システムにインストールされた SSL 証明書の名前を指定します。
proxy.config.admin.number_config_bak	INT	3	保持する取り込み設定ファイルのコピーの最大数を指定します。
proxy.config.admin.user_id	STRING	root	Content Gateway に指定される非特権ユーザー アカウントを指定します。
proxy.config.admin.ui_refresh_rate	INT	30	Content Gateway Manager の Monitor ページ内の統計表示の更新頻度を指定します。
proxy.config.admin.log_mgmt_access	INT	0	すべての Content Gateway Manager トランザクションを lm.log ファイルにログ記録することを、有効化 (1) または無効化 (0) します。
proxy.config.admin.log_resolve_hostname	INT	1	有効 (1) にすると、Content Gateway Manager に接続しているクライアントのホスト名が、 lm.log ファイルに記録されます。 無効 (0) にすると、Content Gateway Manager に接続しているクライアントの IP アドレスが、 lm.log ファイルに記録されます。
proxy.config.admin.subscription	STRING	NULL	未使用。
proxy.config.admin.supported_cipher_list	STRING	AES128-SHA, DHE-RSA-AES128-SHA, DHE-DSS-AES128-SHA, DES-CBC3-SHA, EDH-RSA-DES-CBC3-SHA, EDH-DSS-DES-CBC3-SHA	ブラウザが Content Gateway Manager とのセキュア接続を確立するときに、許可される暗号のカンマ区切り形式のリスト (空白を含まず)。 文字列の検証は行われません。最初の正しい値が使用されます。正しい値でない場合、ブラウザはマネージャーとの接続を許可せず、エラーを返します。
proxy.config.lm.display_reset_alarm	INT	0	有効 (1) な場合、Content Gateway がリセットされた時はいつでも、電子メールが管理者 (proxy.config.alarm_email) に送信されます。 デフォルトは 0 です。

プロセス マネージャー

設定変数	データ タイプ	デフォルト値	説明
<code>proxy.config.process_ manager.mgmt_port</code>	INT	8084	content_manager プロセスと content_gateway プロセス間の 内部通信に使用するポートを 指定します。

仮想 IP マネージャー

設定変数	Data Type	Default Value	説明
<code>proxy.config.vmap. enabled</code>	INT	0	仮想 IP オプションを有効化 または 無効化します。

アラーム設定

設定変数	データ タイプ	デフォルト値	説明
<code>proxy.config.alarm.bin</code>	STRING	<code>example_alarm_ bin.sh</code>	アラームが発生した時に特定 の動作をさせるスクリプトの 名前を指定します。デフォルト ファイルは、 bin ディレク トリにある example_alarm_bin.sh という名 前のサンプル スクリプトで す。必要に応じてスクリプト を編集する必要があります。
<code>proxy.config.alarm.abs_ path</code>	STRING	NULL	proxy.config.alarm.bin (前のエ ントリ)で指定されたスクリ プト ファイルの絶対パスを 指定します。

ARM

設定変数	データタイプ	デフォルト値	説明
proxy.config.arm.ignore_ifp	INT	1	NAT ルールが適用されている場合に、トリガされた NAT ルールのものでなく、パケットのクライアントへの返信時に利用可能インタフェースのどれかを使用するように、Content Gateway を設定します。
proxy.config.arm.always_query_dest	INT	0	<p>有効 (1) にした場合、Content Gateway は常に着信要求の元の宛先 IP アドレスを ARM に問い合わせます。これは、要求のホスト名 DNS ルックアップの代わりに行われます。</p> <p>有効にした場合、ドメイン名の代わりに IP アドレスがログ記録されます。</p> <p>無効にした場合、ドメイン名がログ記録されます。情報は、DNS ルックアップの削減, 77 ページを参照してください。</p> <p>Content Gateway が明示的プロキシおよび透過的プロキシモードの両方で動作している場合、この変数を有効にしないことが推奨されます。明示的プロキシモードでは、クライアントは、オリジンサーバーのホスト名の DNS ルックアップを実行しません。そのため、Content Gateway がそれを行う必要があります。</p>
proxy.config.http.outgoing_ip_spoofing_enabled	INT	0	<p>Content Gateway の IP アドレスの代わりにクライアントの IP アドレスを使用して、オリジンサーバーとの接続を確立することを、Content Gateway に許可する IP スプーフィング オプションを有効化 (1) または無効化 (0) します。</p> <p>IP スプーフィング, 78 ページを参照してください。</p>

設定変数	データタイプ	デフォルト値	説明
<code>proxy.config.arm.bypass_dynamic_enabled</code>	INT	0	クライアントまたはサーバーに問題が発生した場合に、プロキシを迂回して直接オリジンサーバーに送信する適応型バイパスオプションを有効化(1)または無効化(0)します。 動的バイパスルール , 74 ページ を参照してください。
<code>proxy.config.arm.bypass_use_and_rules_bad_client_request</code>	INT	0	ポート 80 上で非 HTTP トラフィックの発生時の動的送信元 / 宛先バイパスを有効化(1)または無効化(0)します。 ご注意: このオプションが動作するためには、 proxy.config.arm.bypass_on_bad_client_request も有効にする必要があります。
<code>proxy.config.arm.bypass_use_and_rules_400</code>	INT	0	オリジンサーバーが 400 エラーを返した場合の送信元 / 宛先バイパスルールの動的作成を有効化(1)または無効化(0)します。 ご注意: このオプションが動作するためには、 proxy.config.arm.bypass_on_400 も有効にする必要があります。
<code>proxy.config.arm.bypass_use_and_rules_401</code>	INT	0	オリジンサーバーが 401 エラーを返した場合の送信元 / 宛先バイパスルールの動的作成を有効化(1)または無効化(0)します。 ご注意: このオプションが動作するためには、 proxy.config.arm.bypass_on_401 も有効にする必要があります。
<code>proxy.config.arm.bypass_use_and_rules_403</code>	INT	0	オリジンサーバーが 403 エラーを返した場合の送信元 / 宛先バイパスルールの動的作成を有効化(1)または無効化(0)します。 ご注意: このオプションが動作するためには、 proxy.config.arm.bypass_on_403 も有効にする必要があります。

設定変数	データタイプ	デフォルト値	説明
proxy.config.arm.bypass_use_and_rules_405	INT	0	オリジン サーバーが 405 エラーを返した場合の送信元 / 宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。 ご注意: このオプションが動作するためには、 proxy.config.arm.bypass_on_405 も有効にする必要があります。
proxy.config.arm.bypass_use_and_rules_406	INT	0	オリジン サーバーが 406 エラーを返した場合の送信元 / 宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。 ご注意: このオプションが動作するためには、 proxy.config.arm.bypass_on_406 も有効にする必要があります。
proxy.config.arm.bypass_use_and_rules_408	INT	0	オリジン サーバーが 408 エラーを返した場合の送信元 / 宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。 ご注意: このオプションが動作するためには、 proxy.config.arm.bypass_on_408 も有効にする必要があります。
proxy.config.arm.bypass_use_and_rules_500	INT	0	オリジン サーバーが 500 エラーを返した場合の送信元 / 宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。 ご注意: このオプションが動作するためには、 proxy.config.arm.bypass_on_500 も有効にする必要があります。
proxy.config.arm.bypass_on_bad_client_request	INT	0	ポート 80 上で非 HTTP トラフィック発生時に、動的宛先バイパスを有効化 (1) または無効化 (0) します。
proxy.config.arm.bypass_on_400	INT	0	オリジン サーバーが 400 エラーを返した場合に、宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.arm.bypass_on_401	INT	0	オリジン サーバーが 401 エラーを返した場合に、宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。
proxy.config.arm.bypass_on_403	INT	0	オリジン サーバーが 403 エラーを返した場合に、宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。
proxy.config.arm.bypass_on_405	INT	0	オリジン サーバーが 405 エラーを返した場合に、宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。
proxy.config.arm.bypass_on_406	INT	0	オリジン サーバーが 406 エラーを返した場合に、宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。
proxy.config.arm.bypass_on_408	INT	0	オリジン サーバーが 408 エラーを返した場合に、宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。
proxy.config.arm.bypass_on_500	INT	0	オリジン サーバーが 500 エラーを返した場合に、宛先バイパス ルールの動的作成を有効化 (1) または無効化 (0) します。

負荷軽減設定 (ARM)

設定変数	データタイプ	デフォルト値	説明
proxy.config.arm.loadshedding.max_connections	INT	1000000	許可されるクライアント接続の最大数を指定します。この数を超えるとプロキシは要求を直接にオリジン サーバーに転送しはじめます。
proxy.config.http.client.connection_control.enabled	INT	1	1 つのコンピュータからの接続数を制限する機能を有効化 (1) または無効化 (0) します。
proxy.config.http.client.concurrent_connection_control.close.enabled	INT	1	同時接続制限に達した場合に接続を閉じる機能を有効化 (1) または無効化 (0) します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.client.concurrent_connection_control.alert.enabled	INT	0	同時接続違反の警告を有効化 (1) または無効化 (0) します。
proxy.config.http.client.concurrent_connection_control.max_connections	INT	1000	1つのクライアントIPアドレスに許可される同時接続数の最大値を指定します。
proxy.config.http.client.connection_rate_control.close.enabled	INT	0	接続率制限に達した場合に接続を閉じる機能を有効化 (1) または無効化 (0) します。
proxy.config.http.client.connection_rate_control.alert.enabled	INT	1	接続率制限超過時の警告を有効化 (1) または無効化 (0) します。
proxy.config.http.client.connection_rate_control.second	INT	100	1つのクライアントIPアドレスに許可される1秒当たりの最大接続数を指定します。
proxy.config.http.client.connection_control.exceptions	STRING	NULL	接続制限を適用しないIPアドレスをカンマ区切りリストで指定します。

認証基本レルム

設定変数	データタイプ	デフォルト値	説明
proxy.config.proxy.authenticate.basic.realm	STRING	NULL	認証レルムの名前を指定します。デフォルト値 NULL を指定すると、 Content Gateway が使用されます。
proxy.config.auth_type	INT	0	クライアント認証のタイプを指定します。 <ul style="list-style-type: none"> 0 = None 1 = LDAP 2 = RADIUS 3 = レガシー NTLM 4 = 統合 Windows 認証 (Integrated Window Authentication) 5 = 複数レルムの認証
proxy.config.multiauth.enabled	INT	0	複数レルムの認証を有効化 (1) または無効化 (0) します。Content Gateway が、複数レルムの認証のために auth.config を使用するようになります。

LDAP

設定変数	データタイプ	デフォルト値	説明
proxy.config.ldap.auth.enabled	INT	0	LDAP プロキシ認証を有効化 (1) または 無効化 (0) します。 LDAP 認証, 210 ページ を参照してください。
proxy.config.ldap.cache.size	INT	5000	LDAP キャッシュに許可されるエントリの最大数を指定します。 この値を変更する時、それに比例して proxy.config.ldap.cache.size の値も更新しなければなりません。 たとえば、キャッシュ サイズを 2 倍にした場合は、 キャッシュ ストレージ サイズも 2 倍にします。
proxy.config.ldap.cache.storage_size	INT	24582912	LDAP キャッシュのサイズをバイト単位で指定します。これは、直接 キャッシュ内のエントリ数に関連します。 この値を変更する時、それに比例して proxy.config.ldap.cache.size の値も更新しなければなりません。 たとえば、キャッシュ サイズを 2 倍にした場合は、 キャッシュ ストレージ サイズも 2 倍にします。 proxy.config.ldap.cache.size を修正せずにこの変数を修正した場合、LDAP サブシステムの機能停止の原因になることがあります。
proxy.config.ldap.auth.ttl_value	INT	3000	エントリがキャッシュ内で有効である時間を分単位で指定します。
proxy.config.ldap.auth.purge_cache_on_auth_fail	INT	1	有効 (1) にすると、認証が失敗した時に LDAP キャッシュ内のクライアントの認証エントリを削除します。
proxy.config.ldap.proc.ldap.server.name	STRING	NULL	LDAP サーバー名を指定します。
proxy.config.ldap.proc.ldap.server.port	INT	389	LDAP サーバーのポートを指定。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ldap.proc.ldap.base.dn	STRING	NULL	LDAP ベース識別名 (DN) を指定します。この値は LDAP 管理者から取得します。
proxy.config.ldap.proc.ldap.uid_filter	STRING	sAMAccountName	LDAP ログイン名 /ID を指定します。これは、完全 DN データベースを検索するためのフィルタとして使用します。 eDirectory またはその他のディレクトリ サービスでは、このフィールドに uid を入力します。
proxy.config.ldap.secure.bind.enabled	INT	0	有効 (1) にすると、プロキシが LDAP サーバーとの通信にセキュア LDAP(LDAPS) を使用するように設定します。通常セキュア通信はポート 636 または 3269 上で実行されません。
proxy.config.ldap.proc.ldap.server.bind_dn	STRING	NULL	LDAP ベースのディレクトリサービスのユーザーの完全識別名 (完全修飾名) を指定します。例： CN=John Smith,CN=USERS,DC=MYCOMPANY,DC=COM このフィールドには最大 128 文字まで入力できます。 このフィールドで値を指定しない場合、プロキシは匿名のバインドを試みます。
proxy.config.ldap.proc.ldap.server.bind_pwd	STRING	NULL	proxy.config.ldap.proc.ldap.server.bind_dn 変数によって識別されるユーザーのパスワードを指定します。

RADIUS 認証

設定変数	データタイプ	デフォルト値	説明
proxy.config.radius.auth.enabled	INT	0	RADIUS プロキシ認証を有効化 (1) または無効化 (0) します。
proxy.config.radius.proc.radius.primary_server.name	STRING	NULL	プライマリ RADIUS 認証サーバーのホスト名または IP アドレスを入力します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.radius. proc.radius. primary_server. auth_port	INT	1812	Content Gateway が RADIUS サーバーとの通信で使用する RADIUS サーバー ポートを指定します。
proxy.config.radius. proc.radius. primary_server. shared_key	STRING	NULL	プライマリ RADIUS 認証サーバーで暗号化に使用するキーを指定します。
proxy.config.radius. proc.radius. secondary_server. name	STRING	NULL	セカンダリ RADIUS 認証サーバーのホスト名または IP アドレスを入力します。
proxy.config.radius. proc.radius. secondary_server. auth_port	INT	1812	プロキシがセカンダリ RADIUS 認証サーバーとの通信に使用するポートを指定します。
proxy.config.radius. proc.radius. secondary_server. shared_key	STRING	NULL	セカンダリ RADIUS 認証サーバーで暗号化に使用するキーを指定します。
proxy.config.radius. auth.min_timeout	INT	10	RADIUS サーバーとの接続がアイドル状態を維持する時間を指定します。この時間を過ぎると Content Gateway は接続を閉じます。
proxy.config.radius. auth.max_retries	INT	10	Content Gateway が RADIUS サーバーへの接続を試みる最大回数を指定します。
proxy.config.radius. cache.size	INT	1000	RADIUS キャッシュに保存できるエントリの数を指定します。最小値は 256 です。
proxy.config.radius. cache.storage_size	INT	15728640	RADIUS キャッシュが使用できるディスクスペースの量の最大値を指定します。 この値はエントリの数の 100 倍以上でなければなりません。可能な最大量のディスクスペースを割り当てることを推奨します。
proxy.config.radius. auth.ttl_value	INT	60	Content Gateway がユーザー名およびパスワード エントリを RADIUS キャッシュに保存できる期間(分)を指定します。

NTLM

設定変数	データ タイプ	デフォルト値	説明
proxy.config.ntlm.auth.enabled	INT	0	NTLM プロキシ認証を有効化 (1) または無効化 (0) します。
proxy.config.ntlm.dc.list	STRING	NULL	ドメイン コントローラのホスト名を指定します。各エントリをカンマで区切る必要があります。形式は下記の通りです。 host_name[:port] [%netbios_name] または IP_address[:port] [%netbios_name] Active Directory 2008 を使用している場合、 netbios_name を含めるか、SMB ポート 445 を使用しなければなりません。
proxy.config.ntlm.dc.load_balance	INT	0	ロード バランシングを有効化 (1) または無効化 (0) します。有効にすると、Content Gateway はドメイン コントローラに認証要求を送信するときにロードバランスを行います。 ご注意： 複数のドメイン コントローラが指定されている時には、ロード バランスが無効化されている場合でも、プライマリドメイン コントローラの負荷が許可されている最大の接続数に達したとき、一時的なフェールオーバーの方法として、新しい要求はセカンダリドメイン コントローラに送信されます。これはプライマリドメイン コントローラが新しい接続を受け入れられるようになるまで継続されます。
proxy.config.ntlm.dc.max_connections	INT	10	Content Gateway がドメイン コントローラをオープンすることができる接続の最大数を指定します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ntlm.cache.enabled	INT	1	NTLM キャッシュを有効化(1)または無効化(0)します。Content Gateway が明示的のプロキシの時にのみ適用します。有効(1)にした場合、Content Gateway は 今後の使用に備えて NTLM キャッシュに資格情報を保存することはありません。Content Gateway は 常に確認のためにドメイン サーバーに資格情報を送信します。
proxy.config.ntlm.cache.ttl_value	INT	900	Content Gateway が NTLM キャッシュにエントリを保存する時間(秒)を指定します。サポートされる値の範囲は 300 - 86400 秒です。
proxy.config.ntlm.cache.size	INT	5000	NTLM キャッシュに保存できるエントリの数を指定します。
proxy.config.ntlm.cache.storage_size	INT	15728640	NTLM キャッシュが使用できるディスク スペースの量の最大値を指定します。この値は、NTLM キャッシュ内のエントリ数に比例する必要があります。たとえば、NTLM キャッシュ内の各エントリが約 128 バイトで、NTLM キャッシュに許可されるエントリの数が 5000 の場合、キャッシュストレージサイズは少なくとも 64000 バイト必要です。
proxy.config.ntlm.cache_exception.list	STRING	NULL	キャッシュされない IP アドレスおよび IP アドレス範囲のリストを保持します。この変数は、Content Gateway Manager の NTLM Multi-Host の IP アドレス フィールドから値を取得します。
proxy.config.ntlm.fail_open	INT	1	認証が下記の理由で失敗した場合に、要求の処理を続行することを許可(1)するか許可しないか(0)を指定します。 <ul style="list-style-type: none"> ドメイン コントローラからの応答がない クライアントからのメッセージの形式が正しくない SMB 応答が不適切 ご注意: パスワード認証が失敗した場合は、続行されません。

統合 Windows 認証

設定変数	データタイプ	デフォルト値	説明
proxy.config.winauth.enabled	INT	0	統合 Windows 認証 (ケルベロス) を有効化 (1) または 無効化 (0) します。
proxy.config.winauth.realm	STRING	NULL	Windows Active Directory ドメインの名前を指定します。 “*”を入力することで、DNS SRV レコード内で発見されたすべてのドメイン コントローラを使用できます。
proxy.config.winauth.log_denied_requests	INT	1	拒否された認証要求のログ記録を有効化 (1) または無効化 (0) します。

透過的認証

設定変数	データ タイプ	デフォルト値	説明
proxy.config.http.transparent_auth_hostname	STRING	NULL	<p>DSN を介してすべてのクライアントが解決できるプロキシの代替ホスト名を指定します。Content Gateway コンピュータの正規ホスト名が、DSN を介してすべてのユーザーに解決されない場合に、これが必要になります。</p> <p>詳細情報は、透過的プロキシ認証の設定, 200 ページを参照してください。</p>
proxy.config.http.transparent_auth_type	INT	1	<p>次を指定します：</p> <ul style="list-style-type: none"> • 0 を指定すると、ユーザーセッションが認証された後、セッション ID とユーザー名を関連付けます。プロキシチェイニングまたはネットワークアドレス変換等で1つの IP アドレスを共有するユーザーを、一意に識別するためにこの設定が必要になります。 • 1 を指定すると、ユーザーセッションが認証された後、クライアント IP アドレスとユーザー名を関連付けます。 <p>いずれのモードでも、クライアントが再認証する必要のある時間の長さは、proxy.config.http.transparent_auth_session_time の値によって決定されません。</p>
proxy.config.http.transparent_auth_session_time	INT	15	<p>ブラウザが再認証を必要とするまでの時間(分)の長さを指定します。IP およびクッキー モード両方で、この値が使用されます。</p>

HTTP エンジン

設定変数	データ タイプ	デフォルト値	説明
proxy.config.http. server_port	INT	8080	Content Gateway が、Web トラフィックの Web プロキシ サーバーとして動作する時、または Web トラフィックを透過的に処理する時に使用するポートを指定します。
proxy.config.http. server_port_attr	STRING	X	サーバーのポート オプションを指定します。以下のいずれかを指定できます： <ul style="list-style-type: none"> • C=SERVER_PORT_COMPRESSED • X=SERVER_PORT_DEFAULT • T=SERVER_PORT_BLIND_TUNNEL
proxy.config.http. server_other_ports	STRING	NULL	変数 proxy.config.http.server_port で指定されたポート以外で、着信 HTTP 要求とバインドするポートを指定します。
proxy.config.http. ssl_ports	STRING	443 563 8081 8071 9443 9444	トンネリングに使用するポートを指定します。これは、スペースで区切られたリストで、1 から 65535 までのポート範囲を指定できます。 Content Gateway は指定されたポートのみトンネリングを許可します。
proxy.config.http. insert_request_via_str	INT	1	次の内の 1 つを指定します： <ul style="list-style-type: none"> • 0 = 文字列に追加情報を付加しない。 • 1 = すべての追加情報を付加。 • 2 = 一部の追加情報を付加。
proxy.config.http. insert_response_via_str	INT	1	次の内の 1 つを指定します： <ul style="list-style-type: none"> • 0 = 文字列に追加情報を付加しない。 • 1 = すべての追加情報を付加。 • 2 = 一部の追加情報を付加。

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.enable_url_expandomatic	INT	1	.com ドメイン拡張を有効化 (1) または無効化 (0) します。これは、先頭に www. を追加し 末尾に .com を付加し、拡張したアドレスにリダイレクトすることで、不適切なホスト名を解決するよう Content Gateway を設定します。たとえば、クライアントが host に対して要求を行った場合、Content Gateway は www.host.com に要求をリダイレクトします。
proxy.config.http.no_dns_just_forward_to_parent	INT	0	有効 (1) にした場合、Content Gateway は HTTP 親キャッシュが有効な時に要求されたホスト名の DNS ルックアップを行いません。
proxy.config.http.uncacheable_requests_bypass_parent	INT	0	有効 (1) にした場合、Content Gateway は キャッシュ不可能な要求を親プロキシに迂回します。
proxy.config.http.keep_alive_enabled	INT	1	オリジン サーバーまたはクライアントとのキープアライブ接続を有効化 (1) または無効化 (0) します。
proxy.config.http.chunking_enabled	INT	1	Content Gateway がチャンクレスポンスを作成するかどうかを指定します。 <ul style="list-style-type: none"> • 0 = しない • 1 = 常に行う

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.send_http11_requests	INT	3	<p>Content Gateway が オリジン サーバーとの通信時に、HTTP バージョン 1.1 を使用するかを指定します。以下の値いずれかを指定できます：</p> <ul style="list-style-type: none"> • 0 = オリジン サーバーとの通信に HTTP 1.1 を使用しない。 • 1 = 常にオリジン サーバーとの通信に HTTP 1.1 を使用する。 • 2 = これまで、オリジン サーバーが HTTP 1.1 を使用していた場合は、HTTP 1.1 を使用する。 • 3 = クライアント要求が HTTP 1.1 で、これまで、オリジン サーバーが HTTP 1.1 を使用していた場合は、HTTP 1.1 を使用する。 <p>ご注意： HTTP 1.1 を使用した場合、Content Gateway は オリジン サーバーに対してパイプライン処理を行う キープアライブ接続を使用できます。HTTP 0.9 を使用した場合、Content Gateway は オリジン サーバーに対してキープアライブ接続を使用できません。HTTP 1.0 を使用した場合、Content Gateway は オリジン サーバーに対してパイプライン処理なしの キープアライブ接続を使用できます。</p>
proxy.config.http.send_http11_asfirstrequest	INT	1	<p>有効 (1) にした場合、サーバーへの最初の要求に HTTP 1.1 を送信するように指定します。そうでない場合は、proxy.config.http.send_http11_requests で指定されたデフォルト動作になります。</p>
proxy.config.http.share_server_sessions	INT	1	<p>サーバー セッションの再利用を有効化 (1) または無効化 (0) します。</p> <p>ご注意： IP スプーフィングが有効な場合、Content Gateway は自動的にこの変数を無効にします。</p>

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.ftp_enabled	INT	1	HTTP で送信された FTP 要求を Content Gateway Manager が処理することを有効化 (1) または無効化 (0) します。
proxy.config.http.record_heartbeat	INT	0	content_cop ハートビートのログ記録を有効化 (1) または無効化 (0) します。
proxy.config.http.large_file_support	INT	1	有効 (1) にした場合、Content Gateway は 2GB 以上ファイルのダウンロードをサポートします。

親プロキシ設定

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.parent_proxy_routing_enable	INT	0	HTTP 親キャッシング オプションを有効化 (1) または無効化 (0) します。 階層キャッシング, 93 ページ を参照してください。
proxy.config.http.parent_proxy.retry_time	INT	300	利用できない親キャッシュに対する再試行接続間隔を指定します。
proxy.config.http.parent_proxy.fail_threshold	INT	10	親キャッシュに対して接続を失敗できる回数を指定します。この回数を過ぎると Content Gateway は親キャッシュが利用不可とみなします。
proxy.config.http.parent_proxy.total_connect_attempts	INT	4	親キャッシュに対して接続を試みることができる合計回数を指定します。この回数を過ぎると Content Gateway は親キャッシュを迂回するか、要求に失敗します (bypass.config ファイルの go_direct オプションに依存します)。
proxy.config.http.parent_proxy.per_parent_connect_attempts	INT	2	複数の親を使用している場合に、親単位で接続を試みることができる合計回数を指定します。
proxy.config.http.parent_proxy.connect_attempts_timeout	INT	30	親キャッシュ接続試行のタイムアウト値を秒単位で指定します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.forward.proxy_auth_to_parent	INT	0	有効にすると、親プロキシに送信される要求から Proxy- Authorization ヘッダーが削除されません。 Content Gateway が子プロキシで親プロキシが認証を実行する場合に、これを有効にします。
proxy.config.http.child_proxy.read_auth_from_header	INT	0	Content Gateway が親プロキシの場合に、X-Authenticated-User および X-Forwarded-For フィールドを読み込みます。 1 = 有効 0 = 無効
proxy.local.http.parent_proxy.disable_ssl_connect_tunneling	INT	0	有効 (1) にした場合、HTTPS 要求は親プロキシを迂回します。
proxy.local.http.parent_proxy.disable_unknown_connect_tunneling	INT	0	有効 (1) にした場合、非 HTTPS トンネル要求は親プロキシを迂回します。

HTTP 接続タイムアウト (秒単位)

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.keep_alive_no_activity_timeout_in	INT	60	トランザクション終了後、後続の要求のために、クライアントとの接続を開き続ける時間を指定します。
proxy.config.http.keep_alive_no_activity_timeout_out	INT	60	トランザクション終了後、後続のデータ転送のために、オリジンサーバーへの接続を開き続ける時間を指定します。
proxy.config.http.transaction_no_activity_timeout_in	INT	120	トランザクションが停止した場合に、Content Gateway がクライアントとの接続を開き続ける時間を指定します。
proxy.config.http.transaction_no_activity_timeout_out	INT	120	トランザクションが停止した場合に、Content Gateway がオリジンサーバーとの接続を開き続ける時間を指定します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.transaction_active_timeout_in	INT	0	Content Gateway が、クライアントと接続されたままになる時間を指定します。タイムアウト時間前にクライアントへの転送が完了しない場合、Content Gateway は接続を閉じます。 デフォルト値の 0 は タイムアウトなしです。
proxy.config.http.transaction_active_timeout_out	INT	0	Content Gateway がオリジンサーバーへの接続要求の完了を待つ時間を指定します。このタイムアウト時間の前に、Content Gateway がオリジンサーバーへの転送を完了しない場合、接続要求は終了させられます。 デフォルト値の 0 は タイムアウトなしです。
proxy.config.http.accept_no_activity_timeout	INT	120	秒単位でタイムアウト間隔を指定します。この時間を過ぎると、Content Gateway はアクティビティのない接続を閉じます。
proxy.config.http.background_fill_active_timeout	INT	60	Content Gateway が バックグラウンド読み込みを継続する時間を指定します。この時間を過ぎると、オリジンサーバー接続を放棄し切断します。
proxy.config.http.background_fill_completed_threshold	FLOAT	0.50000	プロキシが、オリジンサーバーからキャッシュに入れるドキュメントの取得（バックグラウンド読み込み）を継続中に、クライアントが中断した時に、既に転送された全ドキュメントサイズの割合を指定します。

オリジン サーバー接続試行

設定変数	データ タイプ	デフォルト値	説明
proxy.config.http. connect_attempts_max_ retries	INT	6	オリジン サーバーからの応答がない時に、Content Gateway が接続を再試行する最大回数を指定します。
proxy.config.http. connect_attempts_max_ retries_dead_server	INT	2	オリジン サーバーが利用不可の時に、Content Gateway が接続を再試行する最大回数を指定します。
proxy.config.http. connect_attempts_rr_ retries	INT	2	接続試行に失敗できる最大回数を指定します。この回数を過ぎると、サーバーがラウンドロビン DNS エントリを使用している場合、ラウンドロビン エントリはダウンとマークされます。
proxy.config.http. connect_attempts_timeout	INT	60	オリジン サーバー接続のタイムアウト値を秒単位で指定します。
proxy.config.http. streaming_connect_ attempts_timeout	INT	1800	ストリーミング コンテンツ接続のタイムアウト値を秒単位で指定します。
proxy.config.http. down_server.cache_time	INT	30	Content Gateway が到達できなかったオリジン サーバーを記憶する時間を秒単位で指定します。
proxy.config.http. down_server. abort_threshold	INT	10	オリジン サーバーの応答ヘッダーの送信が遅すぎるために、クライアントが接続を破棄した時に Content Gateway がオリジン サーバーを利用不可とマークするまでの秒数を指定します。

否定応答キャッシング

設定変数	データ タイプ	デフォルト値	説明
proxy.config.http.negative_caching_enabled	INT	0	<p>有効(1)にした場合、Content Gateway は否定応答をキャッシュします(要求されたページが存在しない場合の <i>404 Not Found</i> 等)。次回クライアントが同じページを要求した場合、Content Gateway はキャッシュからの否定応答を提供します。</p> <p>Content Gateway は下記の否定応答をキャッシュします:</p> <ul style="list-style-type: none"> 204 No Content 305 Use Proxy 400 Bad Request 403 Forbidden 404 Not Found 405 Method Not Allowed 500 Internal Server Error 501 Not Implemented 502 Bad Gateway 503 Service Unavailable 504 Gateway Timeout
proxy.config.http.negative_caching_lifetime	INT	1800	Content Gateway が 否定応答をキャッシュ内に保持する時間を指定します。

プロキシ ユーザー変数

設定変数	データ タイプ	デフォルト値	説明
proxy.config.http.anonymize_remove_from	INT	0	有効(1)にすると、ユーザーのプライバシーを保護するために、Content Gateway はトランザクションを伴う From ヘッダーを削除します。
proxy.config.http.anonymize_remove_referer	INT	0	有効(1)にすると、サイトおよびユーザーのプライバシーを保護するために、Content Gateway はトランザクションを伴う Referer ヘッダーを削除します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.anonymize_remove_user_agent	INT	0	有効(1)にすると、サイトおよびユーザーのプライバシーを保護するために、Content Gateway は トランザクションを伴う User-agent ヘッダーを削除します。
proxy.config.http.anonymize_remove_cookie	INT	0	有効(1)にすると、サイトおよびユーザーのプライバシーを保護するために、Content Gateway は トランザクションを伴う Cookie ヘッダーを削除します。
proxy.config.http.anonymize_remove_client_ip	INT	1	有効(1)にすると、プライバシーを強化するために、Content Gateway は トランザクションを伴う Client-IP ヘッダーを削除します。
proxy.config.http.anonymize_insert_client_ip	INT	0	有効(1)にすると、クライアント IP アドレスを保持するために、Content Gateway は Client-IP ヘッダーを挿入します。
proxy.config.http.append_xforwards_header	INT	0	有効(1)にすると、Content Gateway は送信要求に X-Forwards ヘッダーを付加します。
proxy.config.http.anonymize_other_header_list	STRING	NULL	Content Gateway が、送信要求から削除するヘッダーを指定します。
proxy.config.http.snarf_username_from_authorization	INT	0	有効(1)にすると、認証スキームが <i>Basic</i> の場合に LDAP の認証ヘッダーからユーザ名とパスワードを削除します。
proxy.config.http.insert_squid_x_forwarded_for	INT	0	有効(1)にすると、Content Gateway は X-Forwarded-For ヘッダーにクライアント IP アドレスを追加します。
proxy.config.http.insert_x_authenticated_user	INT	0	有効(1)にすると、Content Gateway は プロキシ認証ユーザーを公表するために X-Authenticated-User ヘッダーを挿入します。

セキュリティ

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.push_method_enabled	INT	0	有効(1)にすると、ユーザー要求なしにコンテンツを直接キャッシュにプッシュする filter.config ルールを使用できます。既知のソース IP アドレスのみが PUSH 要求をキャッシュに対して実行するようにするために、PUSH アクションのフィルタリングルールを追加する必要があります。設定ファイルエディタの Method ドロップダウンリストで PUSH を有効にする前に、この変数を有効にする必要があります。

キャッシュ コントロール

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.cache.http	INT	1	HTTP 要求のキャッシングを有効化(1)または無効化(0)します。
proxy.config.http.cache.ftp	INT	1	HTTP で送信された FTP 要求のキャッシングを有効化(1)または無効化(0)します。
proxy.config.http.cache.ignore_client_no_cache	INT	0	有効(1)にすると、Content Gateway はキャッシュをバイパスするクライアント要求を無視します。
proxy.config.http.cache.ims_on_client_no_cache	INT	0	有効(1)にすると、着信要求が no-cache ヘッダーを含む場合に Content Gateway はオリジン サーバーに条件付要求を発行します。
proxy.config.http.cache.ignore_server_no_cache	INT	0	有効(1)にすると、Content Gateway はキャッシュをバイパスするオリジン サーバー要求を無視します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.cache.cache_responses_to_cookies	INT	3	<p>クッキーがキャッシュされる方法を指定します：</p> <ul style="list-style-type: none"> • 0=クッキーに対するすべての応答をキャッシュしない • 1=すべてのコンテンツをキャッシュする • 2=イメージタイプのみキャッシュする • 3=テキストコンテンツタイプ以外すべてキャッシュする
proxy.config.http.cache.ignore_authentication	INT	0	<p>有効 (1) にすると、応答内の WWW-Authentication ヘッダーを無視します。 WWW-Authentication ヘッダーは削除され、キャッシュされません。</p>
proxy.config.http.cache.cache_urls_that_look_dynamic	INT	0	<p>動的と思われる URL のキャッシングを有効化 (1) または無効化 (0) します。</p>
proxy.config.http.cache.enable_default_vary_headers	INT	0	<p>Vary ヘッダーを含んでいない HTTP オブジェクトの代替バージョンのキャッシングを有効化 (1) または (0) 無効化します。</p>
proxy.config.http.cache.when_to_revalidate	INT	0	<p>いつコンテンツを再確認するかを指定します：</p> <ul style="list-style-type: none"> • 0=キャッシュ ディレクティブまたはヒューリスティックを使用 (デフォルト値)。 • 1=ヒューリスティックで陳腐化。 • 2=常に陳腐化 (常に再確認)。 • 3=陳腐化なし。 • 4=要求に If-Modified-Since ヘッダーがない場合 キャッシュ ディレクティブまたはヒューリスティックを使用 (0) 要求に If-Modified-Since ヘッダーが含まれる場合、Content Gateway は常にキャッシュ コンテンツを再確認し、プロキシ要求に If-Modified-Since ヘッダーを使用します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.cache.when_to_add_no_cache_to_msie_requests	INT	0	Microsoft Internet Explorer の要求に no-cache ディレクティブを追加するかを指定します。以下を指定できます： <ul style="list-style-type: none"> • 0 = 0 = no-cache を MSIE 要求に追加しない。 • 1 = 1 = no-cache を IMS MSIE 要求に追加する。 • 2 = 2 = no-cache をすべての MSIE 要求に追加する。
proxy.config.http.cache.required_headers	INT	0	要求がキャッシュ可能であるために要求内で必要なヘッダータイプを指定します。 <ul style="list-style-type: none"> • 0 = ドキュメントがキャッシュ可能のために必要なヘッダーはない。 • 1 = 少なくとも Last-Modified ヘッダーは必要。 • 2 = 明示的寿命時間が必要、Expires または Cache-Control。
proxy.config.http.cache.max_stale_age	INT	604800	陳腐化応答の許容される最大期間を指定します。この期間を過ぎるとキャッシュできません。
proxy.config.http.cache.range.lookup	INT	1	有効 (1) にすると、Content Gateway はキャッシュ内の範囲要求をルックアップします。
proxy.config.http.cache.cache_301_responses	INT	0	"301" 応答ページのキャッシングを有効化 (1) または無効化 (0) します。

ヒューリスティック期限

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.cache.heuristic_min_lifetime	INT	3600	キャッシュ内のドキュメントが最新と見なされる最小時間を指定します。
proxy.config.http.cache.heuristic_max_lifetime	INT	86400	キャッシュ内のドキュメントが最新と見なされる最大時間を指定します。
proxy.config.http.cache.heuristic_lm_factor	FLOAT	0.10000	最新性計算のためのエージング係数を指定します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.cache.fuzz.time	INT	240	プロキシがリフレッシュのためにチェックするドキュメント陳腐化時間の秒単位の間隔を指定します。
proxy.config.http.cache.fuzz.probability	FLOAT	0.00500	指定したファズ タイム中にドキュメントでリフレッシュが行われる確率を指定します。

ダイナミック コンテンツおよびコンテンツ ネゴシエーション

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.cache.vary_default_text	STRING	NULL	テキスト ドキュメントの場合に、Content Gateway が 変化するヘッダー を指定します。たとえば、 user-agent を指定した場合、プロキシは検出されたドキュメントの異なるユーザー エージェントのバージョンを キャッシュ します。
proxy.config.http.cache.vary_default_images	STRING	NULL	イメージの場合に、Content Gateway が 変化するヘッダーを指定します。
proxy.config.http.cache.vary_default_other	STRING	NULL	テキストとイメージ以外の場合に、Content Gateway が 変化するヘッダーを指定します。

匿名 FTP パスワード

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.ftp.anonymous_passwd	STRING	<i>インストール中に提供された管理者電子メールの値</i>	アクセスするためにはパスワードを要求する FTP サーバーの匿名パスワードを指定します。 Content Gateway は、この変数のデフォルト値として Content Gateway ユーザー アカウント名を使用します。

キャッシュされた FTP ドキュメントのライフタイム

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.ftp.cache.document_lifetime	INT	259200	FTP ドキュメントが、キャッシュ内に存在する最大時間を指定します。

FTP 転送モード

設定変数	データタイプ	デフォルト値	説明
proxy.config.http.ftp.binary_transfer_only	INT	0	<p>有効(1)にすると、HTTP クライアントから要求されたすべての FTP ドキュメントはバイナリモードのみで転送されます。</p> <p>無効(0)にすると、HTTP クライアントから要求されたすべての FTP ドキュメントは、ドキュメントタイプに依存して ASCII またはバイナリモードで転送されます。</p>

カスタムユーザー応答ページ

設定変数	データタイプ	デフォルト値	説明
proxy.config. body_factory. enable_customizations	INT	0	<p>カスタムユーザー応答ページを有効化するか無効化するか、どの応答ページを使用するかを指定します。</p> <ul style="list-style-type: none"> 0 = カスタムユーザー応答ページを無効化します 1 = デフォルトディレクトリ内のみのカスタムユーザー応答ページを有効化します 2 = 言語別のユーザー応答ページを有効化します
proxy.config. body_factory. enable_logging	INT	0	<p>カスタム応答ページのログ記録を有効化(1)または無効化(0)します。有効にすると、カスタム応答ページが使用または変更される毎に、Content Gateway はエラー ログにメッセージを記録します。</p>
proxy.config. body_factory. template_sets_dir	STRING	config/ body_factory	<p>カスタム応答ページのデフォルトディレクトリを指定します。</p>
proxy.config. body_factory.response_ suppression_mode	INT	0	<p>Content Gateway が作成された応答ページをいつ抑制するかを指定します：</p> <ul style="list-style-type: none"> 0 = 作成された応答ページを抑制しない 1 = 作成された応答ページを常に抑制する 2 = 遮断されたトラフィックの場合のみ抑制する

FTP エンジン

設定変数	データタイプ	デフォルト値	説明
HTTP 上の FTP			
proxy.config.ftp. data_connection_mode	INT	1	<p>FTP 接続モードを指定します：</p> <ul style="list-style-type: none"> 1 = PASV 次に PORT 2 = PORT のみ 3 = PASV のみ

設定変数	データタイプ	デフォルト値	説明
proxy.config.ftp.control_connection_timeout	INT	300	Content Gateway が FTP サーバーからの応答を待つ時間を指定します。
proxy.config.ftp.rc_to_switch_to_PORT	STRING	NULL	設定変数 proxy.config.ftp.data_connection_mode が 1 に設定されている場合に、PASV が失敗した時に Content Gateway が自動的に PORT コマンドにフェイルオーバーするときに使用する応答コードを指定します。この変数は、HTTP クライアントからの FTP 要求のみに使用されます。
FTP プロキシ			
proxy.config.ftp.ftp_enabled	INT	0	FTP クライアントからの FTP 要求処理を有効化 (1) または無効化 (0) します。
proxy.config.ftp.logging_enabled	INT	1	FTP トランザクションのログ記録を有効化 (1) または無効化 (0) します。
proxy.config.ftp.proxy_server_port	INT	2121	FTP 接続に使用するポートを指定します。
proxy.config.ftp.open_lisn_port_mode	INT	1	データ転送のために FTP が開くリッスンポートを指定します。 <ul style="list-style-type: none"> • 1 = オペレーティングシステムが使用可能なポートを選択します。Content Gateway は 0 を送信し、リッスンが成功すれば新しいポート番号を取得します。 • 2 = Content Gateway 変数 proxy.config.ftp.min_lisn_port および proxy.config.ftp.max_lisn_port(後述) で指定されたポート範囲で、リッスンポートを決定します。
proxy.config.ftp.min_lisn_port	INT	32768	FTP クライアントが PASV を送信または Content Gateway が FTP サーバーに PORT を送信する時に、データ接続のために Content Gateway によって使用されるリッスンポートの範囲の最小値を指定します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ftp.max_lisn_port	INT	65535	FTP クライアントが PASV を送信 または Content Gateway が FTP サーバーに PORT を送信する時に、データ接続のために Content Gateway によって使用されるリスンポートの範囲の最大値を指定します。
proxy.config.ftp.server_data_default_pasv	INT	1	サーバー サイドとのデータ接続設定に使用するデフォルトの方法を指定します： <ul style="list-style-type: none"> • 1 = Content Gateway は FTP サーバーに PASV を送信し、FTP サーバーはリスンポートを開きます。 • 0 = Content Gateway は最初に PORT を試みます（接続のプロキシ側にリスンポートをセットアップします）。
proxy.config.ftp.different_client_port_ip_allowed	INT	0	有効 (1) にすると、Content Gateway は、データ接続の確立を実行中の FTP クライアント以外のコンピュータに接続できます。 FTP クライアントは自分のサイドにリスンポートをセットアップするために PORT を使用します。そして、データ接続（ファイル転送に使用）を確立するために、Content Gateway がそのポートに接続することを許可します。リスンポートをセットアップする時、FTP クライアントは IP アドレスとリスンポートのポート番号を指定します。この変数が 0（ゼロ）の場合、クライアントから送信された IP アドレスと FTP クライアントを実行しているコンピュータの IP アドレスが異なる場合は、Content Gateway は FTP クライアントに接続できません。
proxy.config.ftp.try_pasv_times	INT	1024	FTP クライアントが PASV を送信した時に、Content Gateway がリスンポートのオープンを試みる回数を指定します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ftp.try_port_times	INT	1024	FTP サーバーに PORT を送信する時に、Content Gateway がリッスン ポートのオープンを試みる最大回数を指定します。
proxy.config.ftp.try_server_ctrl_connect_times	INT	6	Content Gateway が FTP サーバーのコントロール リッスン ポートへの接続を試みる最大回数を指定します。
proxy.config.ftp.try_server_data_connect_times	INT	3	Content Gateway が、FTP サーバーに PASV を送信し IP/リッスン ポート情報を受信した時に、FTP サーバーのデータ リッスン ポートへの接続を試みる最大回数を指定します。
proxy.config.ftp.try_client_data_connect_times	INT	3	FTP クライアントが IP/リッスン ポート情報を付けて PORT を送信した時に、Content Gateway が FTP クライアントのデータ リッスン ポートへの接続を試みる最大回数を指定します。
proxy.config.ftp.client_ctrl_no_activity_timeout	INT	900	FTP クライアント コントロール接続の非アクティブ タイムアウトを秒単位で指定します。
proxy.config.ftp.client_ctrl_active_timeout	INT	14400	FTP クライアント コントロール接続のアクティブ タイムアウトを秒単位で指定します。
proxy.config.ftp.server_ctrl_no_activity_timeout	INT	120	FTP サーバー コントロール接続の非アクティブ タイムアウトを秒単位で指定します。
proxy.config.ftp.server_ctrl_active_timeout	INT	14400	FTP サーバー コントロール接続のアクティブ タイムアウトを秒単位で指定します。
proxy.config.ftp.client_data_no_activity_timeout	INT	120	クライアント FTP データ転送接続がアイドル状態を維持する最大時間を秒単位で指定します。この時間を過ぎると接続は中断されます。
proxy.config.ftp.client_data_active_timeout	INT	14400	クライアントからの FTP データ転送接続の最大時間を秒単位で指定します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ftp.server_data_no_activity_timeout	INT	120	サーバー FTP データ転送接続がアイドル状態を維持する最大時間を秒単位で指定します。この時間を過ぎると接続は中断されます。
proxy.config.ftp.server_data_active_timeout	INT	14400	サーバーからの FTP データ転送接続の最大時間を秒単位で指定します。
proxy.config.ftp.pasv_accept_timeout	INT	120	Content Gateway のリスンデータ ポートのタイムアウト値を指定します (PASV、クライアント データ接続)。
proxy.config.ftp.port_accept_timeout	INT	120	Content Gateway のリスンデータ ポートのタイムアウト値を指定します (PORT、サーバー データ接続)。
proxy.config.ftp.share_ftp_server_ctrl_enabled	INT	1	複数の匿名 FTP クライアントの間でのサーバー コントロール接続の共有を有効化 (1) または無効化 (0) します。
proxy.config.ftp.share_only_after_session_end	INT	1	FTP サーバー コントロール接続が異なる FTP クライアント セッション間で共有される方法を指定します。 <ul style="list-style-type: none"> • 1 = FTP クライアント セッションが完了した時 (通常、FTP クライアントが QUIT コマンドを送信) にのみ、他のクライアント セッションが FTP サーバー コントロール接続を使用することができます。 • 0 = FTP クライアント セッションが FTP サーバー接続を能動的に使用していない場合にのみ、他のクライアント セッションが FTP サーバー コントロール接続を使用することができます。
proxy.config.ftp.server_ctrl_keep_alive_no_activity_timeout	INT	90	どの FTP クライアントも FTP サーバー コントロール接続を使用しなくなった時の、タイムアウト値を指定します。
proxy.config.ftp.reverse_ftp_enabled	INT	0	サポートされていません。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ftp.login_info_fresh_in_cache_time	INT	604800	220/230 応答 (ログイン メッセージ) をキャッシュ内で最新とする時間を指定します。
proxy.config.ftp.data_source_port_20_enabled	INT	0	有効 (1) にすると、Active モードの FTP クライアントに対する送信データ転送接続にソース ポート 20 をバインドします。

SOCKS プロセッサ

設定変数	データタイプ	デフォルト値	説明
proxy.config.socks.socks_needed	INT	0	SOCKS オプションを有効化または無効化します。 SOCKS ファイアウォール統合の設定, 192 ページ を参照してください。
proxy.config.socks.socks_version	INT	4	SOCKS バージョンを指定します。
proxy.config.socks.default_servers	STRING	s1.example.com:1080;socks2:4080	Content Gateway が通信する SOCKS サーバーの名前とポートを指定します。
proxy.config.socks.accept_enabled	INT	0	SOCKS プロキシ オプションを有効化 (1) または無効化 (0) します。SOCKS プロキシとして、Content Gateway は SOCKS トラフィックを受信し (通常はポート 1080 上で)、すべての要求を SOCKS サーバーへ直接に転送します。
proxy.config.socks.accept_port	INT	1080	Content Gateway が SOCKS トラフィックを受け入れるポートを指定します。
proxy.config.socks.socks_server_enabled	INT	0	ご注意: Content Gateway がアプライアンス上にインストールされている場合にのみ設定します。
proxy.config.socks.socks_server_port	INT	61080	ご注意: Content Gateway がアプライアンス上にインストールされている場合にのみ設定します。

ネット サブシステム

設定変数	データタイプ	デフォルト値	説明
<code>proxy.config.net.connections_throttle</code>	INT	45000	Content Gateway がハンドルできる接続の最大数を指定します。Content Gateway が追加のクライアント要求を受信した場合、それらは要求が処理されるまでキューに入れます。 この変数を 100 以下にしないでください。

クラスタ サブシステム

設定変数	データタイプ	デフォルト値 デフォルト値	説明
<code>proxy.config.cluster.cluster_port</code>	INT	8086	クラスタ通信に使用するポートを指定します。
<code>proxy.config.cluster.ethernet_interface</code>	STRING	<i>your_interface</i>	クラスタ トラフィックに使用するネットワーク インターフェイスを指定します。クラスタ内のすべてのノードは同じネットワーク インターフェイスを使用しなければなりません。

キャッシュ

設定変数	データタイプ	デフォルト値	説明
<code>proxy.config.cache.permit.pinning</code>	INT	0	キャッシュピンニングオプションを有効化(1)または無効化(0)します。このオプションで、指定時間の間、キャッシュにオブジェクトを残しておくことができます。 cache.config ファイルでキャッシュピンニングルールを設定します(cache.config, 374 ページ を参照)。
<code>proxy.config.cache.ram_cache.size</code>	INT	-1	RAM キャッシュのサイズをバイト単位で指定します。 値を -1 にすると、RAM キャッシュのサイズは自動的にディスク 1GB につき約 41MB になります。
<code>proxy.config.cache.limits.http.max_alts</code>	INT	3	Content Gateway がキャッシュできる HTTP 代替の最大数を指定します。
<code>proxy.config.cache.max_doc_size</code>	INT	0	キャッシュ内のドキュメントの最大サイズを指定します(バイト単位)。 0 = サイズ制限なし。

DNS

設定変数	データ タイプ	デフォルト値	説明
proxy.config.dns. search_default_domains	INT	1	ローカルドメイン拡張を有効化(1)または無効化(0)します。有効化すると、Content Gatewayは、ローカルドメインを拡張することで不適切なホスト名を解決しようとします。たとえば、クライアントが host_x という名前の不適切なホスト名を要求した場合、かつ Content Gateway のローカルドメインが y.com の場合、Content Gateway はホスト名を host_x.y.com に拡張します。
proxy.config.dns. splitDNS.enabled	INT	0	DNS サーバー選択を有効化(1)または無効化(0)します。有効(1)にすると、Content Gateway は選択のために splitdns.config ファイルを参照します。 Split DNS オプションの使用, 196 ページ を参照してください。
proxy.config.dns. splitdns.def_domain	STRING	NULL	分割 DNS 要求のデフォルトドメインを指定します。分割 DNS が使用する DNS サーバーを決定する前に、ホスト名がドメインを含まない場合に、この値はホスト名に自動的に付加されます。
proxy.config.dns. url_expansions	STRING	NULL	ルックアップ失敗の後、自動的にホスト名に付加されるホスト名拡張子のリストを指定します。たとえば、Content Gateway にホスト名拡張子 .org を付加させたい場合、変数の値に org を指定します (Content Gateway は自動的にドット(.)を付加します)。 ご注意：変数 proxy.config.http.enable_url_expandomatic が 1(デフォルト値)に設定されている場合、このリストに www. および .com を加える必要はありません。Content Gateway は指定した値を試みる前に自動的に www. および .com を試みます。

設定変数	データタイプ	デフォルト値	説明
proxy.config.dns.lookup_timeout	INT	20	DNS ルックアップ タイムアウト期間を秒単位で指定します。タイムアウト時間が過ぎると、ルックアップの試行を中止します。
proxy.config.dns.retries	INT	5	DNS ルックアップを試みる回数を指定します。この回数を超えると、試行を中止します。
proxy.config.dns.prefer_ipv4	INT	1	名前が IPv4 アドレスおよび IPv6 アドレス両方に解決される時、優先するアドレスタイプを指定します。
proxy.config.ipv6.ipv6_enabled	INT	0	IPv6 のサポートを有効化 (1) するか、無効化 (0) するかを指定します。

DNS プロキシ

設定変数 データタイプ	データタイプ	デフォルト値	説明
proxy.config.dns.proxy.enabled	INT	0	クライアントに代わって、DNS 要求を解決する DNS プロキシキャッシングオプションを有効化 (1) または無効化 (0) します。このオプションによって、リモート DNS サーバーの負荷が軽減され、DNS ルックアップの応答時間が短くなります。- DNS プロキシキャッシング, 107 ページ を参照してください。
proxy.config.dns.proxy_port	INT	5353	Content Gateway が DNS トラフィックに使用するポートを指定します。

HostDB

設定変数	データタイプ	デフォルト値	説明
proxy.config.hostdb.size	INT	200000	ホスト データベースに許可されるエントリの最大数を指定します。
proxy.config.hostdb.ttl_mode	INT	0	ホストデータベースの Time-To-Live モードを指定します。以下のいずれかを指定できます： <ul style="list-style-type: none"> • 0 = 従属 • 1 = 無視 • 2 = 最小 (X,ttl) • 3 = 最大 (X,ttl)
proxy.config.hostdb.timeout	INT	86400	フォアグラウンド タイムアウトを秒単位で指定します。
proxy.config.hostdb.fail.timeout	INT	60	失敗した DNS がキャッシュされる時間を秒単位で指定します。
proxy.config.hostdb.strict_round_robin	INT	0	無効 (0) にすると、オリジンサーバーが使用可能な限り、Content Gateway は 同じクライアントに同じオリジンサーバーを使用します。

ログ記録設定

設定変数	データタイプ	デフォルト値	説明
proxy.config.log2.logging_enabled	INT	1	ログ記録を有効化または無効化します： <ul style="list-style-type: none"> • 0 = ログ記録無効 • 1 = エラーのみ ログ記録 • 2 = トランザクションのみ ログ記録 • 3 = 完全ログ記録 (エラー + トランザクション) ログ ファイルの使用, 233 ページ を参照してください。
proxy.config.log2.max_secs_per_buffer	INT	5	バッファ内のデータが ディスクにフラッシュされるまでの最大時間を指定します。

設定変数	データ タイプ	デフォルト値	説明
proxy.config.log2. max_space_mb_for_logs	INT	5120 または 20480	ログ記録ディレクトリに割り当てられる容量をメガバイト単位で指定します。 Content Gateway が V シリーズ アプライアンス上である場合は、そのサイズは 5120 (5GB) に設定され、これを変更することはできません。 Content Gateway がスタンドアローン サーバーにインストールされている場合は、デフォルトのサイズは 20480 (20 GB) であり、このサイズは設定可能です。
proxy.config.log2. max_space_mb_for_orphan_logs	INT	25	ノードが照合クライアントとして動作している場合に、ログ記録ディレクトリに割り当てられる容量をメガバイト単位で指定します。
proxy.config.log2. max_space_mb_headroom	INT	100	ログ記録スペース限界の許容値をバイト単位で指定します。変数 proxy.config.log2.auto_delete_rolled_file が 1 (有効) に設定されている場合、空き容量がここで指定された値より少なくなった時にログファイルの自動削除がトリガされます。
proxy.config.log2. hostname	STRING	localhost	Content Gateway を実行しているコンピュータのホスト名を指定します。
proxy.config.log2. logfile_dir	STRING	/opt/WCG/logs	ログ記録ディレクトリの完全パスを指定します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.log2.logfile_perm	STRING	rw-r--r--	<p>ログ ファイルのアクセス許可を指定します。標準的な UNIX ファイルのアクセス許可には、owner、group、other が使用されます。有効な値は以下のとおりです：</p> <ul style="list-style-type: none"> • - = 許可なし • r = 読み込み許可 • w = 書き込許可 • x = 実行許可 <p>アクセス許可は、Content Gateway プロセスのアンマスク設定に従います。これは、設定ファイルで指定したとしても、002 のアンマスク設定が、other の書き込を許可しないことを意味します。</p> <p>設定ファイルが変更された時、既存のログ ファイルのアクセス許可は変更されません。</p> <p>Linux のみ。</p>
proxy.config.log2.custom_logs_enabled	INT	0	<p>有効 (1) にすると、logs.xml.config の定義に従ったカスタム ログ ファイルの定義および作成をサポートします。</p> <p>logs.xml.config, 385 ページを参照してください。</p>
proxy.config.log2.xml_logs_config	INT	1	<p>ログ ファイルのロールオーバーが発生するサイズをメガバイト単位で指定します。イベント ログ ファイルの取り込み, 244 ページを参照してください。</p>
proxy.config.log2.squid_log_enabled	INT	0	<p>squid ログ ファイル フォーマットを有効化 (1) または無効化 (0) します。</p>
proxy.config.log2.squid_log_is_ascii	INT	1	<p>squid ログ ファイルのタイプを指定します。</p> <ul style="list-style-type: none"> • 1 = ASCII • 0 = バイナリ
proxy.config.log2.squid_log_name	STRING	squid	<p>squid ログ ファイル名を指定します。</p>
proxy.config.log2.squid_log_header	STRING	NULL	<p>squid ログ ファイルのヘッダー テキストを指定します。</p>

設定変数	データタイプ	デフォルト値	説明
proxy.config.log2.common_log_enabled	INT	0	Netscape Common ログ ファイル フォーマットを有効化 (1) または無効化 (0) します。
proxy.config.log2.common_log_is_ascii	INT	1	Netscape Common ログ ファイルのタイプを指定します。 <ul style="list-style-type: none"> • 1 = ASCII • 0 = バイナリ
proxy.config.log2.common_log_name	STRING	common	Netscape Common ログ ファイル名を指定します。
proxy.config.log2.common_log_header	STRING	NULL	Netscape Common ログ ファイルのヘッダー テキストを指定します。
proxy.config.log2.extended_log_enabled	INT	1	Netscape Extended ログ ファイル フォーマットを有効化 (1) または無効化 (0) します。
proxy.config.log2.extended_log_is_ascii	INT	1	Netscape Extended ログ ファイルのタイプを指定します。 <ul style="list-style-type: none"> • 1 = ASCII • 0 = バイナリ
proxy.config.log2.extended_log_name	STRING	extended	Netscape Extended ログ ファイル名を指定します。
proxy.config.log2.extended_log_header	STRING	NULL	Netscape Extended ログ ファイルのヘッダー テキストを指定します。
proxy.config.log2.extended2_log_enabled	INT	0	Netscape Extended-2 ログ ファイル フォーマットを有効化 (1) または無効化 (0) します。
proxy.config.log2.extended2_log_is_ascii	INT	1	Netscape Extended-2 ログ ファイルのタイプを指定します。 <ul style="list-style-type: none"> • 1 = ASCII • 0 = binary
proxy.config.log2.extended2_log_name	STRING	extended2	Netscape Extended-2 ログ ファイル名を指定します。
proxy.config.log2.extended2_log_header	STRING	NULL	Netscape Extended-2 ログ ファイルのヘッダー テキストを指定します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.log2.separate_host_logs	INT	0	有効 (1) にすると、Content Gateway は log_hosts.config ファイルにリストされている各オリジン サーバーごとに、個別の HTTP/FTP トランザクションのログ ファイルを作成します (HTTP ホスト ログ 分割, 248 ページ を参照してください)。
proxy.local.log2.collation_mode	INT	0	ログ照合モードを指定します： <ul style="list-style-type: none"> • 0 = 照合無効。 • 1 = このホストはログ照合サーバー。 • 2 = このホストは照合クライアントで、照合サーバーに標準フォーマットを使用してエントリを送信。 ログ照合サーバーに、XML ベースのカスタム フォーマットを送信するための情報は、 logs.xml.config, 385 ページ を参照してください。
proxy.config.log2.collation_host	STRING	NULL	ログ照合サーバーのホスト名を指定します。
proxy.config.log2.collation_port	INT	8085	照合サーバーとクライアント間の通信に使用するポートを指定します。
proxy.config.log2.collation_secret	STRING	foobar	照合サーバー使用時に、無許可の情報の交換を防止し、ログ記録データを検証するために使用するパスワードを指定します。
proxy.config.log2.collation_host_tagged	INT	0	有効 (1) にすると、ログ エントリを作成した照合クライアントのホスト名を各エントリに含めるように、Content Gateway を設定します。
proxy.config.log2.collation_retry_sec	INT	5	照合サーバー接続再試行の間隔を秒単位で指定します。
proxy.config.log2.rolling_enabled	INT	1	ログ ファイル取り込みを有効化 (1) または無効化 (0) します。 イベント ログ ファイルの取り込み, 244 ページ を参照してください。
proxy.config.log2.rolling_interval_sec	INT	21600	ログ ファイル取り込み間隔を秒単位で指定します。最小値は 300(5 分) です。最大値は 86400 秒 (1 日) です。

設定変数	データタイプ	デフォルト値	説明
proxy.config.log2.rolling_offset_hr	INT	0	ファイル取り込みオフセット時刻を指定します。ログ取り込み期間の開始時刻。
proxy.config.log2.rolling_size_mb	INT	10	現在のファイルを閉じ、新しいファイルを開くサイズをメガバイト単位で指定します。
proxy.config.log2.auto_delete_rolled_files	INT	1	取り込みファイルの自動削除を有効化(1)または無効化(0)します。
proxy.config.log2.sampling_frequency	INT	1	トランザクション毎ではなく、トランザクションのサンプルのみをログ記録するように、Content Gateway を設定します。以下の値を指定できます： <ul style="list-style-type: none">• 1=1 トランザクション毎にログ記録• 2=2 トランザクション毎にログ記録• 3=3 トランザクション毎にログ記録 など ...

URL リマップ ルール

設定変数	データ タイプ	デフォルト値	説明
<code>proxy.config.url_remap. default_to_server_pac</code>	INT	0	<p>プロキシ サーバー ポート (デフォルト 8080) 上の PAC ファイルの要求が、PAC ポートにリダイレクトされることを有効 (1) または無効 (0) にします。</p> <p>このタイプのリダイレクトが動作するためには、変数 <code>proxy.config.reverse_proxy.enabled</code> が 1 に設定されている必要があります。</p>
<code>proxy.config.url_remap. default_to_server_pac_port</code>	INT	-1	<p>PAC ポートを設定します。Content Gateway プロキシ サーバー ポートへの PAC 要求は、このポートにリダイレクトされます。</p> <p>-1 を指定すると、PAC ポートは自動構成ポートに設定されます (デフォルト自動構成ポートは 8083 です)。これはデフォルト設定です。</p> <p>この変数は、異なるポートから PAC ファイルを取得するために、<code>proxy.config.url_remap.default_to_server_pac</code> 変数と一緒に使用することができます。このポートの PAC ファイルを処理するプロセスを作成し、実行する必要があります。たとえば、ポート 9000 をリッスンし、すべての要求に対する応答に PAC ファイルを書き込む Perl スクリプトを作成します。この変数を 9000 に設定した場合、ポート 8080 上でプロキシ サーバーから PAC ファイルを要求するブラウザは、Perl スクリプトによって提供された PAC ファイルを取得します。</p>

設定変数	データタイプ	デフォルト値	説明
proxy.config.url_remap.remap_required	INT	0	remap.config ファイルのマッピング ルールにリストされたオリジン サーバーからの要求のみを処理するように、Content Gateway を設定するためには、この変数を 1 に設定します。要求が一致しない場合、ブラウザはエラーを受け取ります。
proxy.config.url_remap.pristine_host_hdr	INT	0	再マッピング中に要求内のクライアント ホスト ヘッダーを保持するためには、この変数を 1 に設定します。

スケジュール更新設定

設定変数	データタイプ	デフォルト値	説明
proxy.config.update.enabled	INT	0	Scheduled Update オプションを有効化 (1) または無効化 (0) します。
proxy.config.update.force	INT	0	Force Immediate Update (直ちに更新を強制) を有効化 (1) または無効化 (0) します。有効にした場合、Content Gateway はすべてのスケジュール設定した更新のエントリを上書きし、このオプションが無効にされるまで、更新を開始し続けます。
proxy.config.update.retry_count	INT	10	失敗した場合に、URL のスケジュール設定した更新を再試行する回数を指定します。
proxy.config.update.retry_interval	INT	2	失敗した場合に、URL のスケジュール設定した各更新の再試行の間隔を秒単位で指定します。
proxy.config.update.concurrent_updates	INT	100	許容する同時更新要求の最大数を指定します。このオプションは、スケジュール設定した更新が、ホストに過大な負荷をかけることを防止します。

SNMP の設定

設定変数	データ タイプ	デフォルト値	説明
proxy.config.snmp. master_agent_enabled	INT	0	
proxy.config. snmp_encap_enabled	INT	0	

プラグイン設定

設定変数	データ タイプ	デフォルト値	説明
proxy.config.plugin. plugin_dir	STRING	config/plugins	プラグインの位置するディレクトリを指定します。

WCCP の設定

設定変数	データ タイプ	デフォルト値	説明
proxy.config.wccp. enabled	INT	0	WCCP を有効化 (1) または無効化 (0) します。

FIPS (セキュリティ設定)

設定変数	データタイプ	デフォルト値	説明
proxy.config.fips.security_enabled	INT	0	v7.5.3 FIPS から v7.7 へのカスタマーアップグレードの FIPS 設定を保存します。
proxy.config.fips.security_enabled_ui	INT	0	v7.5.3 FIPS から v7.7 へのカスタマーアップグレードの FIPS UI 設定を保存します。

SSL 復号化



ご注意

すべての SSL 復号化の設定は、Content Gateway Manager 内で行うべきです。下記の表内の変数を、records.config 内で直接編集すべきではありません。

設定変数	データタイプ	デフォルト値	説明
proxy.config.ssl_decryption.use_decryption	INT	0	Content Gateway が SSL 復号化を実行することを有効化(1)または無効化(0)します。
proxy.config.ssl_decryption_ports	INT	443	HTTPS ポートを指定します。Content Gateway は指定されたポートにのみ SSL 復号化およびポリシー ルックアップを許可します。
proxy.config.ssl_decryption.ui_enabled	INT	0	有効(1)にすると、Content Gateway Manager に SSL 設定タブが表示されます。
proxy.config.ssl_management_port	INT	8071	SSL Manager がリスンする管理ポート。
proxy.config.ssl_inbound_port	INT	8070	SSL Manager が着信(クライアント側)トラフィックをリスンするポート。
proxy.config.ssl_outbound_port	INT	8090	SSL Manager が発信(インターネット側)トラフィックに使用するポート。
proxy.config.ssl_outbound_ip	STRING	127.0.0.1	SSL Manager 着信および発信プロキシの IP アドレス。
proxy.config.ssl_forward_to_inbound	INT	1	変更しないでください。 SSL Manager が有効な時、SSL トラフィックを正しいプロキシ ポートに転送します。

設定変数	データタイプ	デフォルト値	説明
proxy.config. administrator_id	STRING	NULL	変更しないでください。 暗号化された管理者 ID を保持 します。この変数は SSL Manager で使用されます。
proxy.config. ssl_decryption. tunnel_skype	INT	0	有効 (1) にした場合、Content Gateway は Skype トラフィック を識別し、トンネリングし ます (明示的プロキシ配備の み)。ユーザー ポリシーを適切 に調整する必要があります。 設定情報は、 SSL Manager の有効化, 149 ページ を参照してく ださい。
proxy.config. ssl_decryption. master_cas	STRING	127.0.0.1	変更しないでください。UI で SSL Manager Configuration Server が指定された時、この 値は自動的に設定されます。 値 127.0.0.1 は、SSL マスター 設定サーバーが ローカルホス トに設定されていることを意 味します。

ICAP

設定変数	データタイプ	デフォルト値	説明
proxy.config.icap.enabled	INT	0	<p>Websense Data Security Suite(DSS) のサポートを有効化 (1) または無効化 (0) します。Websense Data Security の使用, 133 ページを参照してください。</p>
proxy.config.icap.ICAPUri	STRING	NULL	<p>ICAP サービスの Uniform Resource Identifier を指定します。</p> <p>カンマ区切り形式のリストでバックアップ サーバーを指定できます。</p> <p>DSS 管理者から識別子を取得します。URI を下記の形式で入力します。</p> <pre>icap://hostname:port/path</pre> <p><i>hostname</i>には、DSS Protector の IP アドレスまたはホスト名を入力します。</p> <p>デフォルトの ICAP ポートは 1344 です。</p> <p><i>Path</i> は、ホスト コンピュータ上の ICAP サービスのパスです。</p> <p>例：</p> <pre>icap:// ICAP_machine:1344/opt/ icap_services</pre> <p>デフォルトの ICAP ポート 1344 を使用している場合はポートを指定する必要はありません。</p>
proxy.config.icap.FailOpen	INT	1	<p>設定：</p> <ul style="list-style-type: none"> • 1 は、ICAP サーバーがダウンした場合 トラフィックを許可します。 • 0 は、ICAP サーバーがダウンした場合 ブロック ページを送信します。

設定変数	データタイプ	デフォルト値	説明
proxy.config.icap. BlockHugeContent	INT	0	<p>設定:</p> <ul style="list-style-type: none"> 0 に設定すると、送信されたファイルが Data Security Suite で指定されたサイズ制限より大きい場合にブロック ページを送信しません。DSS のデフォルトのサイズ制限は 12MB です。 1 に設定するとトラフィックを許可します。
proxy.config.icap. AnalyzeSecureContent	INT	1	<p>設定:</p> <ul style="list-style-type: none"> 復号化されたトラフィックを宛先に直接に送信する場合、0 を指定します。 復号化されトラフィックを分析のために Websense Data Security に送信する場合、1 を指定します。
proxy.config.icap. AnalyzeFTP	INT	1	有効 (1) にすると、ネイティブな FTP アップロード ファイル転送を分析のために ICAP サーバー に送信します。
proxy.config.icap. ActiveTimeout	INT	5	読み込み / 応答タイムアウト (秒単位)。タイムアウトを超過した場合、アクティビティは失敗と見なされます。
proxy.config.icap. RetryTime	INT	5	停止したサーバーが復旧したかどうかをテストするための復旧時間 (秒)。
proxy.config.icap. LoadBalance	INT	1	<p>ICAP サーバーが指定されている時、次を設定します:</p> <ul style="list-style-type: none"> すべての利用可能なサーバーに要求を配信する場合は 1 に設定 プライマリ サーバーにだけ要求を配信する場合は、0 に設定。

Data Security

設定変数	データタイプ	デフォルト値	説明
proxy.config.dss.enabled	INT	0	オンボックス Data Security のサポートを有効化(1)または無効化(0)します。 Websense Data Security の使用, 133 ページ を参照してください。
proxy.config.dss.AnalyzeFTP	INT	1	有効(1)にすると、ネイティブな FTP アップロード ファイル転送を分析のために、オンボックス Data Security ポリシー エンジンに送信します。
proxy.config.dss.AnalyzeSecureContent	INT	1	設定: <ul style="list-style-type: none"> 復号化されたトラフィックを宛先に直接に送信する場合、0 を指定します。 復号化されトラフィックを分析のために Websense Data Security に送信する場合、1 を指定します。
proxy.config.dss.analysis_timeout	INT	10000	1 つのファイルの分析に使用できる最大時間をミリ秒単位で指定します。この時間を過ぎると、分析は中断します。

接続性、分析、および境界条件

設定変数	データタイプ	デフォルト値	説明
wtg.config.subscription_key	STRING	NULL	Websense Security Gateway または Websense Security Gateway Anywhere のサブスクリプション キーの値を保持します。
wtg.config.download_server_ip	STRING	download.websense.com	Websense ダウンロード サーバーのホスト名または IP アドレスを保持します。
wtg.config.download_server_port	INT	80	Websense ダウンロード サーバーのポート番号を保持します。
wtg.config.policy_server_ip	STRING		Websense Policy Server の IP アドレスを保持します。
wtg.config.policy_server_port	INT	55806	Websense Policy Server のポート番号を保持します。

設定変数	データタイプ	デフォルト値	説明
wtg.config.wse_server_ip	STRING		Websense Filtering Service の IP アドレスを保持します。
wtg.config.wse_server_port	INT	15868	Websense Filtering Service WISP インターフェースのポート番号を保持します。
wtg.config.wse_server_timeout	INT	5000	Filtering Service との通信の最大時間をミリ秒単位で指定します。
wtg.config.ssl_bypassed_categories	STRING	NULL	この変数は、SSL 復号化をバイパスするカテゴリ識別子のリストです。 この変数の値を変更しないでください。これは、トラブルシューティングの支援のために含まれています。 SSL 復号化をバイパスするカテゴリを指定するためには、Web Security Manager を使用してください。
wtg.config.ssl_decryption_bypass_ip_based	INT	0	カテゴリー ルックアップ実行時に、SSL カテゴリ バイパス プロセスが、IP アドレス(ホスト名ではなく)のみを使用するよう設定します。 0 = 無効 1 = 有効
wtg.config.fail_open	INT	1	Websense Web フィルタリング (Filtering Service) が利用できない場合、Content Gateway が要求を許可するか、ブロックするかを指定します。 設定: • 0 ブロック ページを送信 • 1 要求を許可
wtg.config.fail_open_analytic_scan	INT	1	分析スキャンが機能しなくなった時の、Content Gateway の動作を指定します。 設定: • 0 トラフィックをブロック • 1 URL マスターデータベースのルックアップを実行、ポリシーを適用 ご注意: 分析スキャンが機能しなくなった時はいつでも、アラームが発生します。

設定変数	データタイプ	デフォルト値	説明
wtg.config.archive_depth	INT	5	分析がアーカイブファイル上で実行される最大の深さを指定します。
wtg.config.max_decompressions	INT	10	アーカイブファイルが解凍される最大合計数を指定します(トランザクション単位)。この値は 25 を超えてはいけません。
wtg.config.max_subsamples	INT	10000	トランザクションを分類するために、Content Gateway が解凍し、分析するアーカイブファイル内の個別のファイルの最大数を指定します。
wtg.config.zipbomb_action	INT	1	内部で使用。高圧縮ファイル爆弾の分析ステータス。 この変数の値を変更しないでください。
wtg.config.max_mem_allowed	INT	1500	消費された時に、Content Gateway がより広範なメモリモニタリングを実行するメモリの最大数をメガバイト単位で指定します。
wtg.config.lowmem_behavior	INT	0	スキップのバイパスを有効化(1)または無効化(0)します。ただし、フィルタは実行されます。
wtg.config.lowmem_timeout	INT	120	メモリ不足管理のタイムアウト値(分単位)。この時間の後、“no management” にリセットされます。
wtg.config.rdnsclients	INT	0	リバース DNS によって、ログレコード内のクライアントのホスト名をログ記録することを、有効化(1)または無効化(0)します。

設定変数	データタイプ	デフォルト値	説明
wtg.config. ip_ranges_not_to_scan	STRING	10.0.0.0- 10.255.255.255, 172.16.0.0- 172.31.255.255, 192.168.0.0- 192.168.255.255	スキャンしない内部 IP アドレス範囲を指定します。デフォルトでは、このリストは標準のプライベートなルーティング不可の IP アドレスです。各範囲はカンマで区切れ、アドレス範囲はハイフンで結ばれます。 PAC ファイルを使用せずに、スキャンから標準の内部 IP アドレスを除外する明示的のプロキシ配備で、これは特に有用です。
wtg.config. scan_ip_ranges	INT	1	wtg.config. ip_ranges_not_to_scan で指定された内部 IP アドレス範囲のバイパスを有効化(1)または無効化(0)します。上記を参照。

remap.config

remap.config ファイルには、Websense Content Gateway が オリジン サーバーに接続せずに、HTTP 要求を永久的または一時的にリダイレクトするマッピング ルールが含まれます。



重要

このファイルを変更した後は、変更を適用するために、Content Gateway の bin ディレクトリ (/opt/WCG/bin) で `content_line -x` を実行してください。クラスタ内の 1 つのノードに変更を適用した場合、Content Gateway はクラスタ内のすべてのノードに変更を適用します。

フォーマット

remap.config ファイルの各行は マッピング ルールを含む必要があります。Content Gateway は 3 つのスペース区切りのフィールドを認識します：タイ

プ、ターゲット、置換。下記の表は各フィールドのフォーマットについて説明しています。

フィールド	説明
<i>type</i>	次のうち 1 つを入力します： <ul style="list-style-type: none"> • [redirect] – オリジン サーバーに接続せずに、永久的に HTTP 要求をリダイレクトします。永久的リダイレクトは、(HTTP ステータス コード 301 を返すことで) URL 変更をブラウザに通知しますので、ブラウザはブックマークを更新できます。 • [redirect_temporary] – オリジン サーバーに接続せずに、一時的に HTTP 要求をリダイレクトします。一時的リダイレクトは、(HTTP ステータス コード 307 を返すことで) 現在の要求のみの URL 変更をブラウザに通知します。
<i>target</i>	転送元 または <i>from</i> URL を入力します。4 つまでのコンポーネントを入力できます： <pre>scheme://host:port/path_prefix</pre> <i>scheme</i> は http?https、または ftp です。
<i>replacement</i>	転送先 または <i>to</i> URL を入力します。4 つまでのコンポーネントを入力できます： <pre>scheme://host:port/path_prefix</pre> <i>scheme</i> は http、https、または ftp です。



ご注意

target と *replacement* のスキーム タイプ (HTTP、HTTPS、FTP) は一致する必要があります。

例

下記のセクションは、**remap.config** ファイルのマッピング ルールの例を示しています。

リダイレクト マッピング ルール

次のルールは、www.company.com からのすべての HTTP 要求を www.company2.com に永久的にリダイレクトします：

```
redirect http://www.company.com http://www.company2.com
```

次のルールは、www.company1.com からのすべての HTTP 要求を www.company2.com に一時的にリダイレクトします：

```
redirect_temporary http://www.company1.com http://
www.company2.com
```

socks.config

The **socks.config** ファイルは次の項目を指定します：

- ◆ プロキシが指定のオリジン サーバーにアクセスするために使用する必要がある SOCKS サーバー、およびプロキシが SOCKS サーバーリストを経由させる指令。
- ◆ SOCKS サーバーを *経由せず* に、Content Gateway が直接アクセスする Origin サーバー。



ご注意

すべての SOCKS の設定は、Content Gateway Manager 内で行うことが推奨されます。



重要

このファイルを変更したらコンピュータを再起動する必要があります。

手動で設定されたルールに一致しないトラフィックは、デフォルト ルールで処理されます。デフォルト ルールは、**Socks Servers** テーブル内で **default** オプションを有効化することで、各 SOCKS サーバーに設定されます。デフォルト ルールは、自動的に作成され、SOCKS Server ページに表示されます。デフォルト ルールは、**socks.config** ファイルに書き込まれません。宛先 IP アドレスは 'All' です。

フォーマット

プロキシが指定のオリジン サーバーに到達するために使用する SOCKS サーバーを指定するために、**socks.config** に記の形式でルールを追加します。

```
dest_ip=ipaddress socksparent="alias1" [round_robin=value]
```

ここで：

ipaddress は、- または / で区切られたオリジン サーバーの IP アドレスまたは IP アドレス範囲です。

alias1 は、**SOCKS Servers** リストで命名された SOCKS サーバーの別名です。

value は、Content Gateway が 1 つずつ SOCKS サーバーを試す場合は **strict** を指定します。ラウンド ロビン選択を発生さない場合は、**false** を選択します。

SOCKS サーバーを経由することなしに、Content Gateway が直接アクセスするオリジン サーバーを指定するためには、**socks.config** に次の形式のルールを入力します。

```
no_socks ipaddress
```

ここで、*ipaddress* は、Content Gateway が直接アクセスするオリジン サーバーに関連付けられた IP アドレスと IP アドレス範囲のカンマ区切り形式のリストです。「すべてのネットワーク ブロードキャスト アドレス」を指定してはいけません。255.255.255.255.



ご注意

socks.config の各ルールは 最大 400 文字で構成されます。**socks.config** ファイル内のルールの順序は 重要ではありません。

例

下記の例は、SOCKS サーバー ‘alias1’ および ‘alias2’ を経由して、IP アドレス範囲 123.15.17.1 - 123.14.17.4 のオリジン サーバーに要求を送信するようにプロキシを設定します。オプション指定子 **round_robin** が **strict** に設定されているために、プロキシは、最初の要求を alias1 に送信し、2 番目の要求を alias2 に送信し、3 番目の要求を alias1 に送信します。

```
dest_ip=123.14.15.1 - 123.14.17.4
socksparent="alias; alias2" round_robin=strict
```

下記の例は、SOCKS サーバーを経由 *せず* に、IP アドレス 11.11.11.1 のオリジン サーバーに直接アクセスするようにプロキシを設定します。

```
no_socks 11.11.11.1
```

下記の例は、SOCKS サーバーを経由 *せず* に、IP アドレス範囲 123.14.15.1 - 123.14.17.4 と IP アドレス 113.14.18.2 のオリジン サーバーに直接アクセスするように Content Gateway を設定します。

```
no_socks 123.14.15.1 - 123.14.17.4, 113.14.18.2
```

socks_server.config

socks_server.config ファイルは、Content Gateway で利用可能な SOCKS サーバーを指定します。

フォーマット

SOCKS サーバー を指定するために、下記の形式を使用します：

```
alias=name host=IP_address|domain_name port=port_number
[username=user_name password=password] default=true|false
```

ここで：

name は SOCKS サーバーの名前です。

IP_address または *domain_name* は、貴社の DNS サービスで解決できる IP アドレスまたはドメイン名です。

port_number は、SOCKS サーバーがリッスンするポートです。

username および *password* は、SOCKS 5 認証のユーザ名とパスワードのペアです。パスワードは暗号化されます。

指定したサーバーをデフォルト SOCKS サーバーにするためには、*default* を *true* に設定します。デフォルト サーバー オプションがオンの場合、SOCKS サーバーは SOCKS ルールが一致しない場合に使用されます。

デフォルト サーバーに指定された SOCKS サーバーがない場合、ルールに一致しないトラフィックは、SOCKS サーバーを介してルーティングされません。

例：

この例は、127.0.0.1 ポート 61080 の 'default1' SOCKS サーバーを追加します。

```
alias=default1 host=127.0.0.1 port=61080 default=true
```

この例は、認証を使用する SOCKS サーバーを追加します。パスワード "465751475058" は、実際のパスワードではないことに注意してください。これは暗号化されています。

```
alias=test1 host=socks5.example.com port=1080 username=test  
password=465751475058 default=false
```

このファイルを修正した場合、Content Gateway を再起動する必要があります。



ご注意

socks_server.config の各ルールは、400 文字を超えることはできません。

splitdns.config

splitdns.config ファイルを使用して、Content Gateway が指定の条件のもとでホストを解決するために使用する DNS サーバーを指定できます。

DNS サーバーを指定するためには、ファイル内の各有効な行に次の情報を提供する必要があります：

- ◆ 一次宛先指定子（宛先ドメイン、宛先ホスト、または URL 正規表現形式）。
- ◆ サーバー指令のセット（対応するポート番号をもつ1つ以上のDSNサーバーのリスト）。

各 DNS サーバーの定義に次のオプション情報を含めることができます。

- ◆ ホスト解決のためのデフォルト ドメイン
- ◆ 複数のドメインが指定されている場合のドメイン検索順序を指定した検索リスト

詳細情報は、[Split DNS オプションの使用, 196 ページ](#)を参照してください。



重要

このファイルを変更した後は、変更を適用するために、Content Gateway の `bin` ディレクトリ (`/opt/WCG/bin`) で `content_line -x` を実行してください。クラスタ内の1つのノードに変更を適用した場合、Content Gateway はクラスタ内のすべてのノードに変更を適用します。

フォーマット

`splittedns.config` ファイルの各行は、下記のいずれかの形式を使用します：

```
dest_domain=dest_domain | dest_host | url_regex
named=dns_server
def_domain=def_domain search_list=search_list
```

下記の表は各フィールドを説明しています。

フィールド	使用できる値
<code>dest_domain</code>	有効なドメイン名。これは、宛先ドメインに基づく DNS サーバー選択を指定します。NOT 論理演算子を表す感嘆符 (!) をドメインの前に付けることができます。
<code>dest_host</code>	有効なホスト名。これは、宛先ホストに基づく DNS サーバー選択を指定します。NOT 論理演算子を表す感嘆符 (!) をホストの前に付けることができます。
<code>url_regex</code>	有効な URL 正規表現。これは、正規表現に基づく DNS サーバー選択を指定します。
<code>dns_server</code>	これは必須の指令です。これは、Content Gateway が宛先指定子に対して使用する DNS サーバーを識別します。コロン (:) を使用してポートを指定できます。指定しない場合、53 が使用されます。スペースまたはセミコロン (;) で区切ることで、複数の DNS サーバーを指定できます。 ドット表記の IP アドレスを使用して、ドメインを指定する必要があります。
<code>def_domain</code>	有効なドメイン名。このオプションの指令は、ホスト解決に使用するデフォルトドメイン名を指定します。1つのエントリのみ入力できます。デフォルトドメインを提供しない場合、システムは <code>/etc/resolv.conf</code> からその値を決定します。
<code>search_list</code>	スペースまたはセミコロン (;) で区切られたドメインのリスト。これは、ドメイン検索の順序を指定します。検索リストを提供しない場合、システムは <code>/etc/resolv.conf</code> からその値を決定します。

例

下記の DNS サーバー選択定義を見てみましょう：

```
dest_domain=internal.company.com named=255.255.255.255:212
255.255.255.254 def_domain=company.com
search_list=company.com company1.com
dest_domain=!internal.company.com named=255.255.255.253
```

下記の 2 つの要求について考えます：

- ◆ `http://minstar.internal.company.com`
この要求は、最初の行にマッチし、255.255.255.255 ポート 212 の DNS サーバーを選択します。すべての解決要求は、デフォルト ドメインとして `company.com` を使用し、最初に検索するドメインのセットとして、`company.com` および `company1.com` を使用します。
- ◆ `http://www.microsoft.com`
この要求は、2 番目の行にマッチします。従って、Content Gateway は、DNS サーバー 255.255.255.253 を選択します。`def_domain` または `search_list` が提供されなかった場合、Content Gateway は この情報を `/etc/resolv.conf` から取得します。

storage.config

`storage.config` ファイルは、キャッシュを構成するすべてのファイル、ディレクトリ、または ハードディスク パーティションをリストします。



重要

このファイルを変更したらコンピュータを再起動する必要があります。

フォーマット

`storage.config` ファイルの形式下記のとおりです：

```
pathname size
```

ここで、*pathname* は、パーティション、ディレクトリ、またはファイルの名前で、*size* は、名前の付けられたパーティション、ディレクトリ、またはファイルのバイト単位のサイズです。ディレクトリまたはファイルのサイズを指定する必要があります。Raw パーティションの場合、サイズ指定はオプションです。

いかなるサイズのいかなるパーティションでも使用できます。最高のパフォーマンスを得るために、下記のガイドラインが推奨されます：

- ◆ Raw ディスク パーティションを使用する。
- ◆ 各ディスクで、すべてのパーティションを同じサイズにする。
- ◆ 各ノードで、すべてのディスク上の同じパーティション番号を使用する。

オペレーティングシステム要件に従って、パス名を指定します。次の例を参照してください。

**重要**

storage.config ファイルで、フォーマット済み または Raw ディスクは、少なくとも 2 GB 必要です。推奨されるディスク キャッシュ サイズは、147 GB です。

update.config

update.config ファイルは、Websense Content Gateway が 指定のローカル キャッシュ コンテンツの更新のスケジュールを実行する方法を制御します。ファイルには、更新をスケジュールしたいオブジェクトを指定した URL のリストが含まれます。

スケジュール設定した更新は、指定した時刻または間隔で、オブジェクトのローカル HTTP GET を実行します。各オブジェクトに対して下記のパラメータを制御できます。

- ◆ URL
- ◆ URL 指定要求ヘッダー（デフォルトを上書き）
- ◆ 更新時刻および間隔
- ◆ 再帰の深さ

**重要**

このファイルを変更した後は、変更を適用するために、Content Gateway の **bin** ディレクトリ (`/opt/WCG/bin`) で `content_line -x` を実行してください。クラスタ内の 1 つのノードに変更を適用した場合、Content Gateway は クラスタ内のすべてのノードに変更を適用します。

再帰的 URL 更新実行時に、スケジュール設定した更新は 下記のタグ / 属性のペアをサポートしています。

- ◆ ``
- ◆ ``
- ◆ ``
- ◆ `<body background=" " >`
- ◆ `<frame src=" " >`
- ◆ `<iframe src=" " >`
- ◆ `<fig src=" " >`
- ◆ `<overlay src=" " >`
- ◆ `<applet code=" " >`

- ◆ <script src="">
- ◆ <embed src="">
- ◆ <bgsound src="">
- ◆ <area href="">
- ◆ <base href="">
- ◆ <meta content="">

スケジュール設定した更新は、数百の URL 入力からなる URL セットで動作するように設計されています（再帰的 URL が含まれる場合は数千に拡張されます）。これは、インターネット クローラで使用されるのもののような大規模な URL セットでの動作を意図したものではありません。

フォーマット

update.config ファイルの各行は 次の形式を使用します：

```
URL\request_headers\offset_hour\interval\recursion_depth\
```

下記の表は各フィールドを説明しています。

フィールド	使用できる入力値
<i>URL</i>	HTTP および FTP ベースの URL。
<i>request_headers</i>	（オプション）各 GET 要求で渡されたヘッダー（セミコロンで区切り）のリスト。HTTP 仕様に準拠する任意の要求ヘッダーを指定できます。デフォルトは 要求ヘッダーはありません。
<i>offset_hour</i>	更新時間を導出するために使用する基準時間。範囲は 00-23 時です。
<i>interval</i>	更新が行われる（オフセット時間からの）間隔（秒）。
<i>recursion_depth</i>	参照されている URL が再帰的に更新される（指定した URL からの）深さ。

例

下記の例は HTTP のスケジュール設定した更新を示します：

```
http://www.company.com\User-Agent: noname user
agent\13\3600\5\
```

この例では、URL と要求ヘッダー、オフセット時間 13（午後 1 時）、1 時間の間隔、再帰の深さ 5 を指定しています。1 日に 1 回だけ更新するようにスケジュールするためには、間隔の値に 24 時間 x 60 分 x 60 秒 = 86400 を使用します。

下記の例は FTP のスケジュール設定した更新を示します：

```
ftp://anonymous@ftp.company.com/pub/misc/  
test_file.cc\18\120\0\
```

この例は、FTP 要求、オフセット時間 18(午後 6 時)、2 分毎の間隔を指定しています。ユーザーは *anonymous* で、パスワードは **records.config** ファイルの *proxy.config.http.ftp.anonymous_passwd* 変数に指定する必要があります。

wccp.config

wccp.config ファイルは、WCCP 設定情報とサービスグループの設定を保存します。「**Configure**」>「**MyProxy**」>「**Basic**」ページで WCCP を有効化した時、WCCP サービスグループ設定は「**Configure**」>「**Networking**」>「**WCCP**」ページで設定できます。WCCP が Content Gateway への透過的なりダイレクトのために使用される場合、サービスグループを定義する必要があります。詳細情報は、[WCCP v2 デバイスによる透過的遮断, 55 ページ](#)を参照してください。

F

エラー メッセージ

Websense Content Gateway のエラー メッセージ

下の表は、システム ログ ファイルに表示されることがあるメッセージをリストしています。このリストは完全なリストではありません。発生する可能性があり、注意が必要となることがある警告メッセージを示しています。下記のリストに含まれていない警告メッセージの詳細については、www.websense.com にアクセスし、「Support & Knowledge Base」に移動してください。

処理の致命的エラー

メッセージ	説明
Accept port is not between 1 and 65535. Please check configuration.	records.config ファイルで指定されている着信 HTTP 要求を受け入れるポートは無効です。
Ftp accept port is not between 1 and 65535.	records.config ファイルで指定されている着信 FTP 要求を受け入れるポートは無効です。
Self loop is detected in parent proxy configuration.	親プロキシの名前およびポートが Content Gateway の名前およびポートと同じです。そのため、Content Gateway が親プロキシに要求を送信しようとした時、ループが作成されます。
Could not open the ARM device	ARM をロードできませんでした。この最もよくある理由は、ホスト システムのシステムカーネルの適合性の問題です。 ARM がロードされたかどうか確認するには、下記のコマンドを実行します。 /sbin/lsmmod grep arm
content_manager failed to set cluster IP address	content_manager プロセスがクラスタ IP アドレスを設定できませんでした。クラスタ IP アドレスを確認してください。この IP アドレスがネットワーク内の他のデバイスによって使用されていないことを確認してください。
Unable to initialize storage. (Re)Configuration required.	起動中にキャッシュ初期化に失敗しました。キャッシュ構成をチェックし、構成または再構成する必要があります。

警告

メッセージ	説明
<i>Logfile error: error_number</i>	一般的なログ記録エラー。
Bad cluster major version range <i>version1-version2</i> for node <i>IP address</i> connect failed	互換性のないソフトウェアバージョンが問題を起こしています。
can't open config file <i>filename</i> for reading custom formats	カスタムログ記録は有効化されていますが、Content Gateway が logs.config ファイルを見つけることができません。
connect by disallowed client <i>IP address</i> , closing connection	指定されたクライアントは、Content Gateway への接続を許可されていません。そのクライアント IP アドレスは ip_allow.config ファイルにリストされていません。
Could not rename log <i>filename</i> to <i>rolled filename</i>	取り出し中にログ ファイルの名前を変更した時のシステム エラー。
Did <i>this_amount</i> of backup still to do <i>remaining_amount</i>	混雑にさしかかっています。
Different clustering minor versions <i>version 1</i> , <i>version 2</i> for node <i>IP address</i> continuing	互換性のないソフトウェアバージョンが問題を起こしています。
log format symbol <i>symbol_name</i> not found	カスタム ログ フォーマットが存在していないフィールド シンボルを参照しています。 イベントログ記録フォーマット, 359 ページ を参照してください。
missing field for field marker	ログ バッファの読み取りエラーが発生しました。
Unable to accept cluster connections on port: <i>cluster_port_number</i>	Websense テクニカル サポート にお問い合わせください。テクニカル サポートの連絡先については、 www.websense.com/support/ を参照してください。
Unable to open log file <i>filename</i> , errno= <i>error_number</i>	ログ ファイルを開くことができません。
Error accessing disk <i>disk_name</i>	Content Gateway がキャッシュ読み取り問題を起こした可能性があります。ディスクを交換する必要があることもあります。
Too many errors accessing disk <i>disk_name</i> : declaring disk bad	Content Gateway は、エラーがあまりに多く発生したので、キャッシュ ディスクを使用できません。ディスクが破損している可能性があり、交換する必要がある場合があります。
No cache disks specified in storage.config file: cache disabled	Content Gateway storage.config ファイルにどのキャッシュ ディスクもリストされていません。Content Gateway はプロキシ専用モードで実行しています。 storage.config ファイルへのキャッシュに使用するディスクを追加する必要があります (storage.config, 464 ページ を参照)。

メッセージ	説明
All disks are bad, cache disabled	キャッシュ ディスクに問題があり、キャッシングが無効化されています。キャッシュ ディスクが稼働していて、キャッシングのために適切にフォーマットされていることを確認してください。 キャッシュの構成, 97 ページ を参照してください。
Missing DC parameter <missing_param> on auth.profile line	必須のパラメータが指定されていません。欠落しているパラメータの値を入力してください。
Bad DC parameter <bad_param> - <dc_name>	指定されている Domain Controller パラメータが無効です。上記のパラメータの有効な値を入力してください。
[ParentSelection] <error_description> for default parent proxy	子プロキシでの親プロキシの誤った構成のためにプロキシ チェーンが機能していません。子プロキシでの親プロキシの値のチェーン構成を確認してください。
WCCP2: Cannot find Interface name. Please check that the variable proxy.local.wccp2. ethernet_interface is set correctly	WCCP インターフェースの値が指定されていません。Content Gateway Manager で、「Configure (設定)」> 「Networking (ネットワーク)」> 「WCCP」> 「General (一般)」を順に選択し、確認してください。または records.config ファイルの proxy.local.wccp2.ethernet_interface に値を割り当ててください。
ARMManager: Unable to read network interface configuration	ipnat.conf にフォーマットまたは設定エラーがあります。Content Gateway Manager で、「Configure」> 「Networking」> 「ARM」> 「General」を順に選択し、[Edit File (ファイルを編集)] をクリックして ipnat.conf を表示し訂正してください。

アラーム メッセージ

下記の表は、Content Gateway Manager で表示されることがあるアラームメッセージを示しています。

メッセージ	説明 / ソリューション
The Content Gateway subscription has expired.	最寄りの Websense 顧客サービス代理店またはテクニカル サポートまでご連絡ください。
Content Gateway subscription download failed.	Content Gateway がサブスクリプション情報を確認するためダウンロード サーバーに接続することができませんでした。ダウンロード サーバーへの接続を確認してください。

メッセージ	説明 / ソリューション
After several attempts, Content Gateway failed to connect to the Websense Database Download Service. Please troubleshoot the connection.	Content Gateway がインターネットにアクセスできることを確認します。ファイアウォールおよびアップストリーム プロキシ サーバーの設定によって Content Gateway がダウンロードサーバーに接続できない可能性がないか確認してください。
After several attempts, Content Gateway failed to connect to the Policy Server. Please troubleshoot the connection.	Content Gateway と Web Security の間のネットワーク接続があることを確認してください。ファイアウォール設定によって接続がブロックされていることがあります。また、Policy Server サービスが Web Security ホストで実行していることを確認してください。
After several attempts, Content Gateway failed to connect to the Policy Broker. Please troubleshoot the connection.	Content Gateway と Web Security の間のネットワーク接続があることを確認してください。ファイアウォール設定によって接続がブロックされていることがあります。また、Policy Broker サービスが Web Security ホストで実行していることを確認してください。
After several attempts, Content Gateway failed to connect to the Filter service. Please troubleshoot the connection.	Content Gateway と Web Security の間のネットワーク接続があることを確認してください。ファイアウォール設定によって接続がブロックされていることがあります。また、Filter Service 処理が Web Security ホストで実行していることを確認してください。
Communication with the analytics engine has failed. Please restart Content Gateway.	Content Gateway を再起動してください。
SSL decryption has been disabled due to an internal error, please restart Content Gateway.	SSL Manager モジュールで致命的エラーがありました。Content Gateway を再起動してください。
[Rollback::Rollback] Config file is read-only: <i>filename</i>	Content Gateway の config ディレクトリ (デフォルトの場所は /opt/WCG/config) に移動し、指定されたファイルのアクセス権を確認し、必要な場合それらを変更してください。
[Rollback::Rollback] Unable to read or write config file <i>filename</i>	Content Gateway の config ディレクトリに移動し、指定されたファイルが存在しているを確認してください。そのファイルのアクセス権をチェックし、必要な場合はそれらを変更してください。
[Content Gateway Manager] Configuration File Update Failed <i>error_number</i>	Content Gateway の config ディレクトリに移動し、指定されたファイルのアクセス権を確認し、必要な場合はそれらを変更してください。

メッセージ	説明 / ソリューション
Access logging suspended – configured space allocation exhausted.	イベント ログ ファイルに割り当てられたファイル空間がいっぱいになりました。アクセスのログ記録を継続できるようにするには、空間を大きくするか、または一部のログ ファイルを削除する必要があります。このエラーの発生を防止するために、ログ ファイルの取り込みをより頻繁にし、自動削除機能を有効化することを検討してください。 イベント ログ ファイルの取り込み, 244 ページ を参照してください。
Access logging suspended – no more space on the logging partition.	イベント ログを含んでいるパーティション全体がいっぱいになりました。引き続きログ機能にアクセスするために、一部のログ ファイルを削除するか、移動してください。これが起こるのを防ぐために、ログ ファイルの取り込みをより頻繁にし、自動削除機能を有効化することを検討してください。 イベント ログ ファイルの取り込み, 244 ページ を参照してください。
Created zero length place holder for config file <i>filename</i>	Content Gateway の config ディレクトリに移動し、指定されたファイルを確認してください。その長さがまったくゼロである場合は、設定ファイルのバックアップ コピーを使用してください。
Content Gateway can't open <i>filename</i> for reading custom formats	records.config の変数 <i>proxy.config.log2.config_file</i> がカスタム ログ ファイル (デフォルトでは logging/logs.config) への正しいパスを含んでいることを確認してください。
Content Gateway could not open logfile <i>filename</i>	指定したファイルおよびログ記録ディレクトリのアクセス権を確認してください。
Content Gateway failed to parse line <i>line_number</i> of the logging config file <i>filename</i>	カスタム ログ設定ファイルを確認してください。構文エラーの可能性がります。正しいカスタム ログ フォーマットのフィールドについては、 カスタム ログ記録フィールド, 359 ページ を参照してください。
vip_config binary is not setuid root, manager will be unable to enable virtual ip addresses	content_manager 処理が仮想 IP アドレスを設定できませんでした。You must setuid root for the file in the Content Gateway の bin ディレクトリで vip_config のルートを設定する必要があります。
Content Gateway cannot parse the ICAP URI. Please ensure that the URI is entered correctly in Content Gateway Manager or in the <i>proxy.config.icap.ICAPUri</i> configuration variable.	Universal Resource Identifier (URI) が正しい形式ではありません。下記のとおり URI を入力してください。 <pre>icap://hostname:port/path</pre> <p>URI の形式の詳細については、Websense Data Security の使用, 133 ページ を参照してください。</p>

メッセージ	説明 / ソリューション
The specified ICAP server does not have a DNS entry. Please ensure that a valid DSS hostname is entered correctly in Content Gateway Manager or in the <i>proxy.config.icap.ICAPUri</i> configuration variable.	records.config ファイルのホスト名が DNS のどのエントリとも一致しません。有効な Websense Data Security Suite サーバーの名前が Content Gateway Manager に正しく入力されていることを確認してください。 URI の形式の詳細については、 Websense Data Security の使用, 133 ページ を参照してください。
Content Gateway is not able to communicate with the DSS server. Please try again.	Websense Data Security Suite が起動し実行していること、および変数 <i>proxy.config.icap.ICAPUri</i> で指定されているポートへの接続を受け入れることを確認してください。このメッセージが持続する場合は、Websense Data Security Suite 管理者に連絡してください。
Domain controller <i>domain_controller_name:port</i> is down.	指定された NTLM ドメイン コントローラが要求に応答せず、機能停止とマーク付けされています。ドメイン コントローラのステータスを調べてください。

クライアントに送信される HTML メッセージ

Websense Content Gateway は、ブラウザによって要求されたトランザクションで問題が発生した場合、ブラウザのクライアントに詳細なエラー メッセージを返します。これらの応答メッセージは、標準の HTTP 応答コードに対応しますが、より多くの情報を提供します。非常に頻繁に表示される HTTP 応答コードは、[標準 HTTP 応答メッセージ, 477 ページ](#) に示しています。応答メッセージをカスタマイズできます。

下記の表は、Content Gateway のハード コード化された HTTP メッセージ、それらに対応する HTTP 応答コード、およびそれらに対応するカスタマイズ可能なファイルを示しています。

タイトル	HTTP コード	説明	カスタマイズ可能なファイル名
Access Denied	403	場所 <i>URL</i> のドキュメントへのアクセスが許可されていません。	access#denied
Bad HTTP request for FTP Object	400	FTP オブジェクトの HTTP 要求が不適切です。	ftp#bad_request
Cache Read Error	500	キャッシュからの読み取り中のエラー。要求を再度実行してください。	cache#read_error

タイトル	HTTP コード	説明	カスタマイズ可能なファイル名
Connection Timed Out	504	サーバーが長時間に渡りデータを送信していませんでした。	timeout#inactivity
Content Length Required	400	Content-Length が指定されていなかったために、この要求は処理できませんでした。	request#no_content_length
Cycle Detected	400	要求は HTTP プロキシ サイクルの原因となる可能性があるため禁止されました。	request#cycle_detected
Forbidden	403	<i>port_number</i> は、SSL 接続の許可されたポートではありません (禁止されたポート番号へのセキュアな SSL 接続の要求を行いました)。	access#ssl_forbidden
FTP Authentication Required	401	要求した FTP ドキュメント <i>URL</i> にアクセスするために、正しいユーザー名およびパスワードを指定する必要があります。	ftp#auth_required
FTP Connection Failed	502	サーバー <i>server_name</i> に接続できませんでした。	connect#failed_connect
FTP Error	502	FTP サーバー <i>server_name</i> がエラーを返しました。ドキュメント <i>URL</i> へのアクセス要求が失敗しました。	ftp#error
Host Header Required	400	要求を透過的にプロキシ処理する試みが行われましたが、この試みは、ブラウザが HTTP <i>Host</i> ヘッダーを送信していなかったために失敗しました。HTTP プロキシとして <code>https://<i>proxy_name</i>;<i>proxy_port</i></code> を使用するように手動でブラウザを設定します。詳細についてはご使用のブラウザのマニュアルを参照してください。 代わりに、エンドユーザーは HTTP <i>Host</i> ヘッダー フィールドをサポートするブラウザにアップグレードできます。	interception#no_host

タイトル	HTTP コード	説明	カスタマイズ可能なファイル名
Host Header Required	400	ブラウザが <code>Host</code> HTTP ヘッダー フィールドを送信していませんでした。そのため要求される仮想ホストを判別できませんでした。この Web サイトに正しくアクセスするために、HTTP <code>Host</code> ヘッダー フィールドをサポートするブラウザにアップグレードする必要があります。	request#no_host
HTTP Version Not Supported	505	オリジン サーバー <code>server_name</code> は、HTTP プロトコルのサポートされていないバージョンを使用しています。	response#bad_version
Invalid HTTP Request	400	この <code>client_request</code> HTTP 方式での <code>URL</code> へのアクセス要求を処理できませんでした。	request#syntax_error
Invalid HTTP Response	502	ホスト <code>server_name</code> がドキュメントの <code>URL</code> を正しく返しませんでした。	response#bad_response
Malformed Server Response	502	ホスト <code>server_name</code> がドキュメントの <code>URL</code> を正しく返しませんでした。	response#bad_response
Malformed Server Response Status	502	ホスト <code>server_name</code> がドキュメントの <code>URL</code> を正しく返しませんでした。	response#bad_response
Maximum Transaction Time exceeded	504	ドキュメントの <code>URL</code> の送信に時間がかかりすぎです。	timeout#activity
No Response Header From Server	502	ホスト <code>server_name</code> がドキュメントの <code>URL</code> を正しく返しませんでした。	response#bad_response
Not Cached	504	このドキュメントはキャッシュにはなく、また、クライアントはキャッシュされたコピーのみを受け入れます。	cache#not_in_cache
Not Found on Accelerator	404	ホスト <code>server_name</code> 上で <code>URL</code> が検出されませんでした。場所を確認し、再度実行してください。	urlrouting#no_mapping
NULL	502	ホスト <code>hostname</code> がドキュメントの <code>URL</code> を返しませんでした。	response#bad_response

タイトル	HTTP コード	説明	カスタマイズ可能なファイル名
Proxy Authentication Required	407	ユーザー名とパスワードを入力してログインしてください。	access#proxy_auth_required
Server Hangup	502	トランザクションが完了する前にサーバー <i>hostname</i> が接続を中止しました。	connect#hangup
Temporarily Moved	302	要求したドキュメント <i>URL</i> は新しい場所に移動しました。新しい場所は、 <i>new_URL</i> です。	redirect#moved_temporarily
Transcoding Not Available	406	ご利用のブラウザによって要求された形式でドキュメント <i>URL</i> を提供することはできません。	transcoding#unsupported
Tunnel Connection Failed	502	サーバー <i>hostname</i> に接続できませんでした。	connect#failed_connect
Unknown Error	502	ホスト <i>hostname</i> がドキュメントの <i>URL</i> を返しませんでした。	response#bad_response
Unknown Host	500	<i>hostname</i> というサーバーを見つけることができませんでした。サーバーには、DNS エントリがありません。おそらくサーバー名に誤ったつづりがあるか、そのサーバーが存在していないかのどちらかです。名前をダブルクリックして、再度実行してください。	connect#dns_failed
Unsupported URL Scheme	400	プロトコル スキームが未知のためにドキュメント <i>URL</i> の要求を実行できません。	request#scheme_unsupported

標準 HTTP 応答メッセージ

下記の標準 HTTP 応答メッセージは情報を提供します。より完全なリストについては、*Hypertext Transfer Protocol – HTTP/1.1 Specification* を参照してください。

メッセージ	説明
200	OK
202	受け入れられた
204	コンテンツなし

メッセージ	説明
206	部分的コンテンツ
300	複数の選択肢
301	永久に移動させられた
302	検出された
303	他を参照
304	変更されていない
400	不適切な要求
401	無許可：再度実行
403	禁止
404	見つからない
405	メソッドが許可されていない
406	許容できない
408	要求の時間切れ
500	内部サーバー エラー
501	適用されない
502	不良の Gateway
504	Gateway タイムアウト

G

req_ca.cnf ファイル

req_ca.cnf ファイルを作成し、そのファイルに下記のコードをコピーしてください。**req_ca.cnf** ファイルに関する情報は、[下位 CA の作成, 153 ページ](#)を参照してください。

```
#
# Configuration file for generating a CA Request
#
HOME = .
RANDFILE = $ENV::HOME/.rnd
#
[ policy_match ]
countryName = match
stateOrProvinceName = match
organizationName = match
organizationalUnitName = optional
commonName = supplied
emailAddress = optional
#
[ policy_anything ]
countryName = optional
stateOrProvinceName = optional
localityName = optional
organizationName = optional
organizationalUnitName = optional
commonName = supplied
emailAddress = optional
#####
#
[ req ]
default_bits = 1024
default_keyfile = privkey.pem
distinguished_name = req_distinguished_name
string_mask = nombstr
req_extensions = v3_req # The extensions to add to a certificate
request
[ req_distinguished_name ]
countryName = Country Name (2 letter code)
countryName_default = US
countryName_min = 2
countryName_max = 2
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = Some-State
localityName = Locality Name (eg, city)
0.organizationName = Organization Name (eg, company)
0.organizationName_default = Internet Widgits Pty Ltd
```

```
#organizationalUnitName = Organizational Unit Name (eg, section)
#organizationalUnitName_default =
commonName = Common Name (Name of Sub-CA)
commonName_max = 64
emailAddress = Email Address
emailAddress_max = 64
[ v3_req ]
# Extensions to add to a certificate request to make it a CA
basicConstraints=CA:TRUE
nsCertType = sslCA
keyUsage = cRLSign, keyCertSign
```

H

FAQ およびトラブル シューティングのヒント

よく寄せられる質問 (FAQ)

- ◆ ディスク IO エラーはキャッシュにどのような影響を与えますか、また、キャッシュ ディスクに障害が発生した場合 Content Gateway は何をしますか、482 ページ
- ◆ Content Gateway が大きなオブジェクトをダウンロードしているときにクライアントが切断した場合、キャッシュにオブジェクトの一部が保存されますか、482 ページ
- ◆ Content Gateway は、Java アプレット、JavaScript プログラム、またはその他の VBScript などのアプリケーション ファイルをキャッシュできますか、482 ページ
- ◆ マスタ管理者パスワードを忘れた場合に Content Gateway Manager にどのようにアクセスしますか、482 ページ
- ◆ logs.xml.config ファイルへの変更をクラスタ内のすべてのノードにどのように適用しますか、483 ページ
- ◆ Squid 形式および Netscape 形式のログ ファイルのキャッシュ戻り値は何を意味しますか、484 ページ
- ◆ cctx フィールドはカスタム ログ ファイルに何を記録するのですか、485 ページ
- ◆ Content Gateway はホスト データベース内のエントリが一定期間使用されていない場合に、それらのエントリを更新しますか、485 ページ
- ◆ イメージ、動画 gif、および Java アプレットを使用してカスタム応答の外観を改善できますか、486 ページ
- ◆ Content Gateway が透過的要求のみを処理するように設定するにはどうすればよいですか、486 ページ

詳細は [トラブルシューティングのヒント](#)、488 ページ を参照してください。

ディスク IO エラーはキャッシュにどのような影響を与えますか、また、キャッシュ ディスクに障害が発生した場合 Content Gateway は何をしますか

ディスク ドライブが 5 回連続で IO 動作に失敗した場合、Content Gateway はそのドライブがアクセス不能とみなし、キャッシュからディスク全体を削除します。他のすべての Content Gateway ディスク ドライブでは正常なキャッシュ処理が続行します。

Content Gateway が大きなオブジェクトをダウンロードしているときにクライアントが切断した場合、キャッシュにオブジェクトの一部が保存されますか

HTTP または FTP 処理中にクライアントが切断した場合、Content Gateway は最大 10 秒間、オリジン サーバーからのオブジェクトのダウンロードを継続します。クライアントが切断した後 10 秒以内にオリジン サーバーからの転送が正常に完了した場合は、Content Gateway はオブジェクトをキャッシュに保存します。オリジン サーバーが 10 秒以内にダウンロードを正常に完了しなかった場合は、Content Gateway はオリジン サーバーとの接続を中止し、キャッシュからオブジェクトを削除します。Content Gateway は、部分的なドキュメントをキャッシュに保存しません。

Content Gateway は、Java アプレット、JavaScript プログラム、またはそのほかの VBScript などのアプリケーション ファイルをキャッシュできますか

Content Gateway は、Java アプレット、JavaScript プログラム、VBScripts および他の実行可能なオブジェクトを、HTTP オブジェクトの最新性およびキャッシュ可能性のルールに従って、キャッシュに保存し、そこから提供することができます。

Content Gateway は、アプレット、スクリプト、またはプログラムを実行しません。これらのオブジェクトは、要求を送信したクライアント システムがこれらのオブジェクトをロードしたときのみ実行します。

マスタ管理者パスワードを忘れた場合に Content Gateway Manager にどのようにアクセスしますか

インストール時に、管理者パスワードを指定することができます。インストーラは自動的にパスワードを暗号化し、暗号を `records.config` ファイルに保存します。Content Gateway Manager でパスワードを変更するたびに、Content Gateway は、`records.config` ファイルを更新します。

管理者パスワードを忘れ、Content Gateway Manager にアクセスできない場合、`records.config` ファイルで現在のパスワードをクリア（設定変数を NULL

に設定します)し、Content Gateway Manager で新しいパスワードを入力します。パスワードの変数にはパスワードの暗号化または値 NULL のみを含めることができますから、`records.config` ファイルでパスワードを設定できません。

1. `/opt/WCG/config` の `records.config` ファイルを開きます。
2. 変数 `proxy.config.admin.admin_password` を NULL にせ手直し、パスワードを空白のままにしておきます。



ご注意

語 NULL の後ろにスペースがないことを確認します。

3. ファイルを保存して、閉じます。
4. Content Gateway `bin` ディレクトリ (`/opt/WCG/bin`) から `content_line -x` を実行して変更を適用します。
5. Content Gateway Manager にログ オンします。ユーザー名とパスワードの入力を要求されたとき、管理者 ID を入力し、パスワードの欄は空白のままにしておきます。

`records.config` ファイルでパスワードをクリアしていた場合は、管理者としてログオンするためにパスワードは入力する必要はありません。

6. 「Configure (設定)」> 「My Proxy (マイ プロキシ)」> 「UI Setup (UI の設定)」> 「Login (ログイン)」タブを順に選択します。
7. [Administrator (管理者)] セクションで [Old Password] フィールドを空白のままにしておきます。[New Password (新しいパスワード)] フィールドに新しいパスワードを入力し、次に [New Password (Retype) (新しいパスワード (再入力))] フィールドに新しいパスワードを再入力します。
8. [Apply (適用)] をクリックします。

Content Gateway Manager に次回アクセスするとき、この新しいパスワードを使用する必要があります。

logs_xml.config ファイルへの変更をクラスタ内のすべてのノードにどのよう適用しますか

1 つの Content Gateway ノードで `logs_xml.config` ファイルを変更した後、Content Gateway `bin` ディレクトリ (`/opt/WCG/bin`) から下記のコマンドを入力します。

```
content_line -x
```

Content Gateway は、変更をクラスタ内のすべてのノードに適用します。変更はすぐに有効になります。

Squid 形式および Netscape 形式のログ ファイルのキャッシュ戻り値は何を意味しますか

下記の表は、Squid および Netscape ログ ファイルのキャッシュ戻り値を示しています。

キャッシュ戻り値	説明
TCP_HIT	要求されたオブジェクトの有効なコピーがキャッシュに入れられたこと、およびプロキシがオブジェクトをクライアントに送信したことを示します。
TCP_MISS	要求されたオブジェクトがキャッシュに入れられなかったこと、およびプロキシがオリジン サーバーまたは親プロキシからオブジェクトを取得し、それをクライアントに送信したことを示します。
TCP_REFRESH_HIT	オブジェクトがキャッシュに入れられたが、陳腐化したことを示します。Content Gateway は、 <code>if-modified-since</code> 要求をオリジン サーバーに行い、オリジン サーバーが <code>304 not-modified</code> 応答を送信したことを示します。プロキシは、キャッシュされたオブジェクトをクライアントに送信しました。
TCP_REF_FAIL_HIT	オブジェクトがキャッシュに入れられたが、陳腐化したことを示します。Content Gateway は、 <code>if-modified-since</code> 要求をオリジン サーバーに行いましたが、そのサーバーは応答しませんでした。プロキシは、キャッシュされたオブジェクトをクライアントに送信しました。
TCP_REFRESH_MISS	オブジェクトがキャッシュに入れられたが、陳腐化したことを示します。Content Gateway は、 <code>if-modified-since</code> 要求をオリジン サーバーに行い、そのサーバーは新しいオブジェクトを返しました。プロキシは、新しいオブジェクトをクライアントに送信しました。
TCP_CLIENT_REFRESH	クライアントが <code>no-cache</code> ヘッダーの付いた要求を発行したことを示します。プロキシは要求されたオブジェクトをオリジン サーバーから取得し、コピーをクライアントに送信します。Content Gateway は、キャッシュからオブジェクトの以前のすべてのコピーを削除します。
TCP_IMS_HIT	クライアントが <code>if-modified-since</code> 要求を発行し、オブジェクトがキャッシュに入っていて IMS の日付より新しいこと、またはオリジン サーバーへの <code>if-modified-since</code> でそのキャッシュ オブジェクトが新しいことが確認されたことを示します。プロキシは、キャッシュされたオブジェクトをクライアントに送信しました。

キャッシュ戻り値	説明
TCP_IMS_MISS	クライアントが if-modified-since 要求を発行したこと、およびオブジェクトがキャッシュにいれられていなか、またはキャッシュ内で陳腐化していることを示します。プロキシは、if-modified-since 要求をオリジン サーバーに行い、新しいオブジェクトを受信しました。プロキシは、更新されたオブジェクトをクライアントに送信しました。
TCP_SWAPFAIL	オブジェクトがキャッシュに入れられたが、アクセスできなかったことを示します。クライアントはオブジェクトを受信しませんでした。
ERR_CLIENT_ABORT	完全なオブジェクトが送信される前にクライアントが切断されたことを示します。
ERR_CONNECT_FAIL	Content Gateway がオリジン サーバーにアクセスできなかったことを示します。
ERR_DNS_FAIL	Domain Name Server がオリジン サーバー名を解決できなかったこと、または Domain Name Server がアクセスできなかったことを示します。
ERR_INVALID_REQ	クライアント HTTP 要求が無効であったことを示します。Content Gateway は未知の方法で要求をオリジン サーバーに転送します。
ERR_READ_TIMEOUT	タイムアウト間隔以内にオリジン サーバーが Content Gateway の要求に応答しなかったことを示します。
ERR_PROXY_DENIED	クライアント サービスがアクセス制御設定によって拒否されたことを示します。
ERR_UNKNOWN	クライアントは接続しましたが、その後要求を送信せずに切断されたことを示します。

cqtx フィールドはカスタム ログ ファイルに何を記録するのですか

cqtx フィールドは完全なクライアント要求テキスト（ヘッダーを除く）をログ ファイルに記録します。例、`get http://www.company.com HTTP/1.0`

Content Gateway はホスト データベース内のエントリが一定期間使用されていない場合に、それらのエントリを更新しますか

デフォルトでは、Content Gateway ホスト データベースは、名前サーバーによって設定された time-to-live (ttl) の値を監視します。Content Gateway を別の値に再設定できます。

1. `/opt/WCG/config` の `records.config` ファイルを開きます。

2. 下記の変数を編集します。

変数	説明
<code>proxy.config.hostdb.ttl_mode</code>	<p>設定</p> <p>0 - 名前サーバーによって設定された ttl の値に従います。</p> <p>1 - 名前サーバーによって設定された ttl の値を無視し、Content Gateway 設定変数 <code>proxy.config.hostdb.timeout</code> によって設定された値を使用します。この変数を環境に適した値に設定してください。</p> <p>2 - 2 つの値 (名前サーバーによって設定された値と Content Gateway によって設定された値) の小さい方を使用します。</p> <p>3 - 2 つの値 (名前サーバーによって設定された値と Content Gateway によって設定された値) の大きい方を使用します。</p>

3. ファイルを保存して、閉じます。
4. Content Gateway bin ディレクトリ (`/opt/WCG/bin`) から `content_line -x` を実行して設定の変更を適用します。

イメージ、動画 gif、および Java アプレットを使用してカスタム応答の外観を改善できますか

Content Gateway はクライアントへの応答にシングル テキストまたは HTML ドキュメントのみを使用できます。しかし、カスタム応答ページにイメージ、動画 gif、Java アプレットまたは Web サーバーに置かれているテキスト以外のオブジェクトへのリファレンスを提供できます。

`body_factory` テンプレート ファイルにリンクを追加する方法は、HTML ドキュメントにイメージを追加するのと同じ方法で、SRC 属性に完全な URL を指定します。

Web サーバーと Content Gateway が同じポート番号を使ってドキュメントを送信しようとするのを防止するために、これらのプログラムを同じシステムで実行しないことを推奨します。

Content Gateway が透過的要求のみを処理するように設定するにはどうすればよいですか

下記の方法で、Content Gateway が透過的要求のみを処理し、明示的プロキシ要求を処理しないように構成できます。

- ◆ プロキシを使用することを許可される IP アドレスの範囲を指定することによって、`ip_allow.config` ファイルから Content Gateway へのクライアント アクセスを制御できます。Content Gateway は、このファイルで指定さ

れた範囲にリストされていない IP アドレスから要求を受け取った場合、その要求を破棄します。[ip_allow.config, 382 ページ](#) を参照してください。

- ◆ Content Gateway へのアクセスを許可されているクライアント IP アドレスの範囲がわからない場合は、Layer 4 スイッチまたは WCCP ルータによってリダイレクトされた要求のみがプロキシポートに受信されるようにするルールを `ipnat.conf` ファイルに追加できます。透過専用の Content Gateway をサーバーを作成するには、`ipnat.conf` ファイルの通常のリダイレクトサービスのルールの前に、明示的プロキシトラフィックをリスンしているサービスがないポートにリダイレクトするルールを追加します。たとえば、Content Gateway が明示の HTTP 要求を無視するようにするには、`ipnat.conf` ファイルの通常 HTTP リダイレクトルールの前に、下記のようなルールを追加します（ここで、`ipaddress` はご使用の Content Gateway システムの IP アドレス、`port_number` はリスンしているサービスがないポート番号です）。

```
rdr hme0 ipaddress port 80 -> ipaddress port port_number tcp
rdr hme0 ipaddress port 8080 -> ipaddress port port_number tcp
rdr hme0 0.0.0.0/0 port 80 -> ipaddress port 8080 tcp
```

処理対象の各プロトコル サービス ポートまたは個別のネットワーク インターフェースについて、同様のルールを `ipnat.conf` ファイルに追加します。`ipnat.conf` ファイルに変更を行った後、プロキシを再起動する必要があります。

- ◆ Content Gateway システムに複数のネットワーク インターフェースがある場合、または Content Gateway オペレーティング システムが仮想 IP アドレスを使用するように設定する場合、Content Gateway に 2 つの IP アドレスを割り当てることができます。1 つのアドレスは、プロキシがオリジン サーバーと通信するために使用する *実際* のアドレス、もう一方のアドレスは、WCCP またはスイッチ リダイレクションに使用するプライベート IP アドレス（例、10.0.0.1）でなければなりません。IP アドレスを設定した後、`records.config` ファイルの終わりに下記の変数を追加しなければなりません。`private_ipaddress` を WCCP またはスイッチ リダイレクションに使用されるプライベート IP アドレスに置き換え `real_ipaddress` をプロキシがオリジン サーバーと通信するために使用する IP アドレスに置き換えます。

```
LOCAL proxy.local.incoming_ip_to_bind STRING
private_ipaddress
LOCAL proxy.local.outgoing_ip_to_bind STRING
real_ipaddress
```

トラブルシューティングのヒント

- ◆ [Content Gateway Manager でスループット統計が不正確, 488 ページ](#)
- ◆ [Content Gateway コマンドを実行することができません, 488 ページ](#)
- ◆ [1 つのノードがクラスタ内の他のノードからオブジェクトを取得するときに矛盾した動作が行われる, 489 ページ](#)
- ◆ [Web ブラウザがデータ欠落メッセージを示すエラー ドキュメントを表示することがある, 489 ページ](#)
- ◆ [Content Gateway がどんな Web サイトも解決しない, 490 ページ](#)
- ◆ [システム ログ ファイルでの最大ドキュメント サイズ超過メッセージ, 491 ページ](#)
- ◆ [システム ログ ファイルでの DrainIncomingChannel メッセージ, 491 ページ](#)
- ◆ [システム ログ ファイルの cop ファイル メッセージがない, 491 ページ](#)
- ◆ [vaddrs.config の編集時のシステム ログ ファイルでの警告 \(Linux\), 492 ページ](#)
- ◆ [always_query_destination を有効化した後、非透過的要求が失敗する, 492 ページ](#)
- ◆ [Content Gateway は実行しているが、ログ ファイルが作成されない, 493 ページ](#)
- ◆ [Content Gateway エラーがネットワーク接続が多すぎることを示す, 493 ページ](#)
- ◆ [低メモリの兆候, 494 ページ](#)
- ◆ [オリジン サーバーとの接続タイム アウト, 495 ページ](#)
- ◆ [IBM Web サーバーが Content Gateway で機能しない, 495 ページ](#)
- ◆ [Content Gateway が起動 \(または停止\) しない, 495 ページ](#)

Content Gateway Manager でスループット統計が不正確

Content Gateway は、オブジェクト全体を転送した後、スループット統計を更新します。サイズが大きなファイルの場合、転送の終わりの時点でバイトカウントが急に大きくなります。転送されるバイトの完全な数は、最後の 10-秒間の結果であると考えられます。ただしオブジェクトを転送するのに数分かかることがあります。

この不正確さは、負荷が小さい場合に、より顕著になります。負荷が重いほどより正確な統計を得ることができます。

Content Gateway コマンドを実行することができません

コマンドは下記の条件では実行しません。

- ◆ `content_manager` プロセスが実行していない場合。 .

下記のコマンドを入力することによって、`content_manager` プロセスが実行しているかどうか確認します。

```
ps aux | grep content_manager
```

または

```
./WCGAdmin status
```

`content_manager` プロセスが実行していない場合は、そのプロセスを開始するために Content Gateway `bin` ディレクトリ (`/opt/WCG/bin`) から下記のコマンドを入力します。

```
./content_manager
```



重要

Content Gateway を停止しなければならない場合は、`./WCGAdmin` を使用して Content Gateway を再起動することを推奨します。プロセス全体が適切に停止し開始するようにするために、`./WCGAdmin stop` を使用して停止し、`./WCGAdmin start` を使用して起動します。 [使用開始にあたって, 11 ページ](#) を参照してください。

- ◆ コマンドを `$WCGHome/bin` から実行していなかった場合。
Content Gateway `bin` ディレクトリがパスにない場合は、コマンドの先頭に `./` を付けます (例、`./content_line -h`)。
- ◆ 複数の Content Gateway をインストールしており、`/etc/content_gateway` で指定したアクティブなパスからコマンドを実行していなかった場合。
常に、下記のコマンドを発行することによって正しいディレクトリに変更します。

```
cd `cat /etc/content_gateway`/bin
```

1 つのノードがクラスタ内の他のノードからオブジェクトを取得するときに矛盾した動作が行われる

システム準備プロセスの一部として、クラスタ内のすべてのノードにあるクロックを同期化しなければなりません。モニタ時刻の違いは何も問題を起こしませんが、数分を超える違いは Content Gateway の動作に影響を与えることがあります。

`xntpd` などのクロック同期化デーモンを実行することを推奨します。下記の URL から `xntpd` の最新のバージョンを入手できます。

<http://www.ntp.org>

Web ブラウザがデータ欠落メッセージを示すエラー ドキュメントを表示することがある

Web ブラウザで下記のようなメッセージが表示されます。

```
Data Missing
```

This document resulted from a POST operation and has expired from the cache. If you wish you can repost the form data to re-create the document by pressing the reload button.

Web ブラウザはそのローカル キャッシュをクライアント システム上のメモリおよび(または)ディスクに保持します。キャッシュから有効期限切れで消去されたドキュメントに関するブラウザのメッセージは、Content Gateway キャッシュではなく、ブラウザのローカル キャッシュを参照します。Web ブラウザでこのようなメッセージが表示される原因となるような Content Gateway メッセージや条件はありません。

ブラウザ キャッシュのオプションおよび効果の詳細については、ブラウザのマニュアルを参照してください。

Content Gateway がどんな Web サイトも解決しない

ブラウザは、ホストと通信していること、その後下記のメッセージによってタイムアウトになることを示します。

The document contains no data; Try again later, or contact the server's Administrator....

システムが正しく設定されていること、および Content Gateway が名前解決ファイルを読み取ることができることを確認してください。

- ◆ nslookup コマンドを発行することによって、サーバーが DNS ルックアップを解決できるかどうか確認します。例：

```
nslookup www.myhost.com
```
- ◆ `/etc/resolv.conf` ファイルに DNS サーバーの有効な IP アドレスが含まれているかどうか確認します。
- ◆ 一部のシステムでは、`/etc/resolv.conf` ファイルが判読不能な場合、または名前サーバー エントリがない場合、オペレーティング システムは名前サーバーとして `localhost` を使用します。しかし、Content Gateway はこの規則を使用しません。`localhost` を名前サーバーとして使用する場合は、`/etc/resolv.conf` ファイルに `127.0.0.1` または `0.0.0.0` の名前サーバー エントリを追加する必要があります。
- ◆ Content Gateway ユーザー アカウントが `/etc/resolv.conf` ファイルを読み取る権限があるかどうかを確認します。ファイルのアクセス権を `rw-r--r--` (644) に変更します。



重要

`/etc/resolv.conf` の IP アドレスが変わった場合は、Content Gateway を再起動する必要があります。

システム ログ ファイルでの最大ドキュメント サイズ超過メッセージ

下記のメッセージがシステム ログ ファイルに示されます。

```
WARNING: Maximum document size exceeded
```

要求されたオブジェクトがプロキシ キャッシュで許容されている最大サイズより大きかったのです。Content Gateway は超過サイズのオブジェクトに対してプロキシ サービスを提供しましたが、それをキャッシュしていません。

キャッシュのオブジェクト サイズの限度を設定するには、「**Configure**」>「**Subsystems (サブシステム)**」>「**Cache (キャッシュ)**」>「**General (一般)**」タブを順に選択し、**[Maximum Object Size (最大オブジェクト サイズ)]** フィールドを変更します。キャッシュのオブジェクトのサイズを限定しない場合は、ドキュメント サイズを 0 (ゼロ) に設定します。

システム ログ ファイルでの DrainIncomingChannel メッセージ

下記のメッセージがシステム ログ ファイルに示されます。

```
Feb 20 23:53:40 louis content_manager[4414]: ERROR ==>
[drainIncomingChannel] Unknown message: 'GET http://
www.telechamada.pt/ HTTP/1.0'
Feb 20 23:53:46 louis last message repeated 1 time
Feb 20 23:53:58 louis content_manager[4414]: ERROR ==>
[drainIncomingChannel] Unknown message: 'GET http://
www.ip.pt/ HTTP/1.0'
```

これらのエラー メッセージは、ブラウザが Content Gateway クラスタ ポートの 1 つ、つまり `rsport` (デフォルト ポート 8087) または `mcport` (デフォルト ポート 8088) に HTTP 要求を送信していることを示します。Content Gateway は、要求を破棄します。このエラーは、Content Gateway の問題を引き起こすことはありません。正しいプロキシ ポートを使用するためにブラウザを再設定する必要があります。



ご注意

Content Gateway クラスタは、プライベート サブネット上で別のネットワーク インターフェースおよびクラスタを使用するように設定し、それによってクライアント コンピュータがクラスタ ポートへのアクセス権限を持たないようにすれば、最も効率的に機能します。

システム ログ ファイルの cop ファイル メッセージがない

下記のメッセージが繰り返しシステム ログ ファイルに示されます。

```
content_cop[16056]: encountered "config/internal/no_cop"
file...exiting
```

ファイル `config/internal/no_cop` は、管理制御として機能し、`content_cop` プロセスが `content_manager` を起動したり、何らかのヘルス チェックを実行することなく、すぐに終了するように指示します。`no_cop` ファイルは、プロキシが `./WCGAdmin stop` または `stop_content_gateway` コマンドによって停止させられたとき、自動的に開始するのを防ぎます。そのような静的制御がなくても、Content Gateway はシステムの再起動時に自動的に再起動します。`no_cop` 制御は、Content Gateway が下記のコマンドによって再起動されるまで、オフの状態にしておきます。

`./WCGAdmin start` コマンドまたは `start_content_gateway` コマンド。

The Content Gateway が自動的に起動しないようにするために Content Gateway インストール スクリプトは `no_cop` ファイルを作成します。インストールおよび設定を完了し、オペレーティング システムが再起動された後、`./WCGAdmin start` コマンドまたは `start_content_gateway` コマンドを使用して、Content Gateway を起動します。Content Gateway の起動および停止の詳細については、[使用開始にあたって, 11 ページ](#) を参照してください。

vaddrs.config の編集時のシステム ログ ファイルでの警告 (Linux)

Linux システムで非ルート ユーザーとして `vaddrs.config` ファイルを編集する場合、Content Gateway は、システム ログ ファイルで下記のような警告メッセージを発行します。

```
WARNING: interface is ignored: Operation not permitted.
```

このメッセージを無視できます。Content Gateway は設定の編集を適用します。.



重要

常に Content Gateway Manager から仮想 IP アドレスを設定することを推奨します。`vaddrs.config` ファイルを編集すると想定外の結果をもたらすことがあります。

always_query_destination を有効化した後、非透過的要求が失敗する

`records.config` ファイルに含まれている変数 `proxy.config.arm.always_query_dest` は、ホスト ヘッダーを無視し、オリジン サーバーの IP アドレスを常に要求するように Content Gateway を透過的模式で設定します。この変数を有効化したとき、Content Gateway は、既存の NAT マップリストからオリジン サーバーの IP アドレスを取得します。DNS ルックアップを使って宛先ホスト名を解決しようとはしません。そのため、ログ記録された URL は IP アドレスのみを含み、ホスト名を含みません。ドメイン名をログ記録するには、`proxy.config.arm.always_query_dest` を 0 に設定します。ただし、`proxy.config.arm.always_query_dest` を 0 に設定しても DNS ルックアップの数を減らしません。

しかし、NAT リストに一致するマップがないので、明示的要求（ポート 80 上の要求を含む非透過的要求）は失敗します。



ご注意

`always_query_destination` オプションは、プライマリ プロキシ ポートでのみ機能します。

Content Gateway は実行しているが、ログ ファイルが作成されない

Content Gateway は、記録する情報がある場合のみイベント ログ ファイルを作成します。Content Gateway がアイドル状態の場合、ログ ファイルはありません。

正しいディレクトリを調べているか確認します。デフォルトでは、Content Gateway は、ログ ファイルをその `logs` ディレクトリに作成します。

「**Configure**」>「**Subsystems**」>「**Logging (ログ記録)**」>「**General**」タブを順に選択して、**[Log Directory]** フィールドを調べて Content Gateway Manager のログ ファイルの場所を確認します。代わりに、`records.config` ファイルに含まれている変数 `proxy.config.log2.logfile_dir` の値を調べることができます。

ログ ディレクトリに Content Gateway ユーザー アカウントの読み取り / 書き込み権限があることを確認します。ログ ディレクトリに正しい権限がない場合は、`content_gateway` プロセスはログ ファイルを開けたり作成したりすることができません。

ロギングが有効化されているか確認します。Content Gateway Manager で、「**Configure**」>「**Subsystems**」>「**Logging**」>「**General**」タブを順に選択し、**[Logging (ログ記録)]** エリアを調べます。代わりに、`records.config` ファイルに含まれている変数 `proxy.config.log2.logging_enabled` の値を調べることができます。

ログ フォーマットが有効化されているか確認します。Content Gateway Manager で、「**Configure**」>「**Subsystems**」>「**Logging**」>「**Formats**」タブを順に選択し、標準フォーマットが有効化されていること、および「**Custom (カスタム)**」タブでカスタム フォーマットが有効化されていることを確認します。`records.config` ファイルの **[Logging Config (設定のロギング)]** セクションの変数を編集することによって標準フォーマットまたはカスタム フォーマットを選択します。

Content Gateway エラーがネットワーク接続が多すぎることを示す

デフォルトでは、Content Gateway は 8000 のネットワーク接続をサポートします。この半分の 4000 がクライアントの接続に割り当てられ、残りの 4000 がオリジン サーバーの接続に割り当てられます。クライアントまたはオリジン サーバーの接続が設定された制限値の半分の 90% (デフォルトでは 3600) に到達したとき、接続スロットル イベントが発生します。接続スロットルイ

イベントが発生した場合、Content Gateway は既存のすべての接続を処理し続けますが、接続カウントが制限値以下に下がるまで、新しいクライアントの接続要求を受け入れません。

接続スロットル イベントは下記の条件で発生することがあります。

- ◆ **接続スパイクがある場合** – 数千件のクライアント要求が一斉にプロキシに到達する場合。そのような事象は一般的には一時的であり、是正処理を必要としません。
- ◆ **サービスの過負荷がある場合** – クライアント要求が継続的にプロキシの処理能力を上回る速さで到達する場合。サービスの過負荷は、Content Gateway とオリジン サーバーとの間のネットワークの問題を示すことがあり、またクライアント負荷を処理するために Content Gateway がより多くのメモリ、CPU、キャッシュ ディスク、または他のリソースを必要とすることを示すことがあります。

接続スロットルの性質を判断するためにパフォーマンス グラフを調べます。特に、[Client Connections (クライアントの接続)]、[TCP Connections (TCP の接続)]、および [Client Ops Per Second (1 秒あたりのクライアントの操作数)] グラフを調べてください。またシステム ログ ファイル、エラー ログ ファイル、またはイベント ログ ファイルでエラー メッセージを調べることもできます。

必要な場合、「Configure」>「Networking (ネットワーク)」>「Connection Management (接続管理)」>「Throttling (スロットリング)」タブを使って、または `records.config` ファイルの `proxy.config.net.connections_throttle` の値を編集することによって、プロキシによってサポートされる接続の最大数をリセットできます。システムが必要なクライアント接続を処理するための十分なメモリを備えていない限り、接続スロットル制限値を大きくしてはいけません。RAM のサイズが小さいシステムでは、スロットル制限値をデフォルト値より低く設定しなければならないことがあります。



重要

この変数を最小値 100 より以下に設定しないようにしてください。

低メモリの兆候

重負荷の下では、Linux カーネルは RAM を超過して実行することがあります。低メモリ条件は、パフォーマンスの低下と種々のシステム上の問題を引き起こすことがあります。RAM の枯渇は、システムに十分な空きのスワップスペースがある場合でも生じることがあります。

過度なメモリの枯渇の兆候は、システム ログ ファイル (`/var/log/messages`) の下記のメッセージを含みます。

```
WARNING: errno 105 is ENOBUFS (low on kernel memory),
consider a memory upgrade
kernel: eth0: can't fill rx buffer (force 0)!
kernel: recvmsg bug: copied E01BA916 seq E01BAB22
```

オプションで、システムが低メモリ状態になった時、トラフィックのスキャンを一時中断するように Content Gateway を設定できます。Content Gateway Manager で、「**Configure**」>「**Networking**」>「**Connection Management**」>「**Low Memory Mode (低メモリモード)**」タブを順に選択します。[Connection Control \(接続の制御\), 320 ページ](#) を参照してください。

オリジン サーバーとの接続タイムアウト

一部のオリジン サーバーは HTTP 要求を送信するのに 30 秒以上かかり、そのためプロキシ接続がタイムアウトになります。そのような接続タイムアウトを防止するには、Content Gateway Manager で「**Configure**」>「**Protocols (プロトコル)**」>「**HTTP**」>「**Timeouts (タイムアウト)**」タブを順に選択し、**[Active Timeout (アクティブ タイムアウト)]** セクションで、**[Origin Server Response (オリジン サーバー応答)]** の値を 60 秒またはそれ以上に変更します。

IBM Web サーバーが Content Gateway で機能しない

IBM Web サーバーは、TLS (Transport Layer Security) プロトコルをサポートしません。IBM Web サーバーが Content Gateway で機能するようにするには、設定変数の値を編集する必要があります。

1. `/opt/WCG/config` の `records.config` ファイルを開きます。
2. 下記の設定変数を編集します。

変数	説明
<code>proxy.config.ssl.TLSv1</code>	この変数を 0 (ゼロ) に設定します。

3. ファイルを保存して、閉じます。
4. Content Gateway **bin** ディレクトリ (`/opt/WCG/bin`) から `content_line -x` を実行して変更を適用します。

Content Gateway が起動 (または停止) しない

Content Gateway は、インストール時に自動的に起動します。Content Gateway を停止する必要がある場合、停止および再起動には `./WCGAdmin start` コマンドと `./WCGAdmin stop` コマンドを使用することを推奨します。

Content Gateway の起動または停止

1. `root` に移動します。


```
su
```
2. Content Gateway の `bin` ディレクトリ (`/opt/WCG/bin`) に変更します。
3. プロキシを起動します。


```
./WCGAdmin start
```

下記のコマンドを入力してプロキシを停止します。

```
./WCGAdmin stop
```

用語集

代替

同じ Web オブジェクトの異なるバージョン。一部のオリジン サーバーは、種々のオブジェクトが含まれている同一の URL への要求に応答します。これらのオブジェクトのコンテンツは、サーバーが種々の言語のコンテンツを配信するか、種々のプレゼンテーション スタイルを持つ種々のブラウザを対象としているか、または時間帯によって異なるコンテンツを配信するかどうかによって異なります。

ARM

Adaptive Redirection Module (利用可能なリダイレクション モジュール)。この機能はその一環として透過的プロキシ キャッシングをサポートし、それによって ARM はオリジン サーバーを宛先とするクライアント トラフィックが中断された時にそれを Content Gateway にリダイレクトします。トラフィックは ARM によってリダイレクトされる前に、**L4 スイッチ** またはルーターによって遮断されます。

キャッシュ

頻繁にアクセスされるオブジェクトのコピーをユーザーおよびサーバーに近い場所に保存し、要求時にそれらをユーザーに送信します。**オブジェクトストア** も参照してください。

キャッシュ階層

相互に交信する複数のキャッシュのレベル。すべてのキャッシュ階層は**親キャッシュ** と **子キャッシュ** という概念を認識します。

キャッシュ ヒット

クライアントに直接に送信できるキャッシュ内のオブジェクト

キャッシュ ミス

キャッシュにないオブジェクト、またはキャッシュにはあるが有効でなくなったオブジェクト。どちらの場合もプロキシは**オリジン サーバー**からオブジェクトを取得しなければなりません。

キャッシング Web プロキシ サーバー

プロキシがオリジン サーバーの以前の応答のキャッシュされたコピーを使って、クライアントの要求をローカルに処理できるようにするローカル キャッシュ ストレージを備えた Web プロキシ サーバー。

CGI

Common Gateway Interface。オリジン サーバーと、同じコンピュータ上に置かれている他のソフトウェア (*CGI プログラム*) が通信する方法を記述する ルールのセット。

cgi-bin

オリジン サーバー上の **CGI** プログラムが保存されている最も一般的なディレクトリの名前。

子キャッシュ

Content Gateway を親とする **キャッシュ階層** にある下位のキャッシュ。親 **キャッシュ** も参照してください。

クラスタ

構成情報を共有する Content Gateway ノードのグループで、単一の大規模な仮想キャッシュとして使用できます。

設定モード

Content Gateway Manager の 2 つのモードの 1 つ。設定モードを使用して Content Gateway システムを設定できます。**モニタ モード** も参照してください。

content_cop

定期的にハートビート要求を発行して合成 Web ページを取得することによって、**content_gateway** および **content_manager** プロセスの状態をモニタする Content Gateway プロセス。

content_gateway

Content Gateway 製品のキャッシュ処理エンジンである Content Gateway プロセス。**content_gateway** は、**キャッシュ** または **オリジン サーバー** からの接続を受け入れ、要求を処理し、ドキュメントを提供する役割を持っています。

Content Gateway Manager

Content Gateway のブラウザ ベースのインターフェースで、パフォーマンスのモニタおよび構成設定値の変更のために使用する一連の Web ページから成ります。

content_manager

Content Gateway のプロセスであり、コマンドおよびコントロール機能です。**content_manager** は、**content_gateway** プロセスの起動、モニタ、および再設定を行います。また、管理者ユーザー インターフェース、プロキシ自動設定

ポート、統計インターフェース、クラスタ管理、および **仮想 IP フェールオーバー** も処理します。

クッキー

オリジン サーバーによって Web ブラウザに送信される 1 つの情報。ブラウザ ソフトウェアはこの情報を保存し、ブラウザがサーバーから追加の要求を行うとき、それをサーバーに返送します。クッキーによってオリジン サーバーがユーザーを追跡できます。

DNS

ドメイン名サービス。Content Gateway は、ホスト名の IP アドレスへの変換を簡素化する高速の、非同期 DNS リゾルバを含んでいます。

明示的プロキシ キャッシング

Content Gateway の設定オプションの 1 つで、この中でクライアント ソフトウェア（一般的にはブラウザ）が Web 要求を Content Gateway プロキシに送信するように設定する必要があります。

FTP

File Transfer Protocol。TCP/IP に基づく信頼できるファイル転送プロトコル

HTTP

Hypertext Transfer Protocol。World Wide Web のベースとなっているクライアント / サーバー プロトコル。

HTTPS

Hypertext Transfer Protocol Secure。HTTP と SSL の使用によって提供される World Wide Web 上の暗号化通信の形式。

IP

Internet Protocol。TCP/IP の下の、エンドツーエンド転送およびロング パケット フラグメント化コントロールを受け持っている最下層プロトコル。

ISP

インターネット サービス プロバイダ。インターネットへのアクセスを提供する組織。

JavaScript

Web ページにそれらを開覧するユーザーとの相互動作の能力を与えるために設計されたスクリプト言語。そのような相互動作の例として、マウスの移動またはマウスのクリックに対応して動作を実行したり、フォームに入力された内容を確認することがあります。

L4 スイッチ

Level 4 の規則を使用してネットワークトラフィックフローを管理できるイーサネットスイッチ。このスイッチは、希望するクライアントプロトコルパケットを遮断し、それらを透過的処理するようにプロキシに転送します。

管理クラスタ化

クラスタ内のすべてのノードが自動的に設定情報を共有する Content Gateway のオプション。

モニタ モード

Content Gateway Manager の 2 つのモードの 1 つ。モニタ モードを使用して、Content Gateway のパフォーマンスおよび Web トラフィックに関する統計を見ることができます。**設定モード** も参照してください。

MRTG

Multi Router Traffic Graphe。Content Gateway のパフォーマンスをモニタできるパフォーマンス グラフを作成する Content Gateway に備えられているグラフ表示ツール。

Netscape ログ フォーマット

標準アクセス ログ フォーマット。Netscape ログ フォーマットを使用すると、既製の分析ログ スクリプトによって Content Gateway のアクセス ログ ファイルを分析することができます。**Squid ログ フォーマット** も参照してください。

オブジェクトストア

Content Gateway がすべてのキャッシュされたオブジェクトを保存するカスタム高速データベース。

オリジン サーバー

要求された情報のオリジナルのコピーを含んでいる Web サーバー。

PAC ファイル

Proxy Auto-Configuration ファイル。ブラウザが要求を処理する方法を決定するために呼び出す JavaScript 関数定義です。

親キャッシュ

キャッシュ階層 の最上位のキャッシュで、プロキシがそこに要求を送信することができます。

プロキシ サーバー

Web プロキシ サーバー を参照してください。

ルータ

2 つ以上のネットワーク間の接続を処理するデバイス。ルータは、通過するパケットの宛先アドレスを調べて、それらを送信する経路を決定します。

SOCKS

プロキシで処理するのが難しいプロトコルのためのトンネリング メカニズムを提供するサーキット レベルのプロキシ プロトコル。

Squid ログ フォーマット

標準アクセス ログ フォーマット。Squid ログ フォーマットを使用すると、既製の分析ログ スクリプトによって Content Gateway のイベント ログ ファイルを分析することができます。[Netscape ログ フォーマット](#) も参照してください。

SSL

Secure Sockets Layer。インターネット全体で暗号化された認証通信を可能にするプロトコル。ほとんどの場合、オリジン サーバーと Web ブラウザの間の通信で使用されます。

syslog

UNIX システム ログ機能。

TCP

Transmission Control Protocol。インターネット標準トランスポート層プロトコル。TCP は、IP によって送信されるシーケンス化されたデータを使用することによって信頼できるエンドツーエンド通信を提供します。

透過的プロキシ キャッシング

Content Gateway がインターネット要求に対して、ユーザーにブラウザの再設定を要求することなしに遮断および応答できるようにする設定オプション。これはオリジン サーバーを宛先とするトラフィックを遮断し、そのトラフィックをプロキシ キャッシュへリダイレクトすることによって行われます。

URL

Uniform Resource Locator。Web 上のファイルまたは他のインターネット機能への経路を定義するアドレス。

仮想 IP フェールオーバー

クラスタ化された Content Gateway サーバーで利用できるオプションで、それによって WCG はクラスタのノードに割り当てる仮想 IP アドレスのプールを維持します。ノードが停止したとき、残りのノードは、障害をマスクし、停止したノードの仮想インターフェースを引き継ぎます。

WCCP

Web Cache Control Protocol。Cisco IOS ベースのルータが、透過的プロキシ キャッシング中にトラフィックをリダイレクトするために使用するプロトコル。

Web プロキシ サーバー

クライアント要求を **オリジン サーバー** に転送するプロキシ サーバー。プロキシ サーバーはフィルター ルールまたはセキュリティの制限に従って要求を拒否することがあります。

Web サーバー

インターネット上で World Wide Web サービスを提供するコンピュータ。**オリジン サーバー** も参照してください。

WPAD

Web Proxy Auto-Discovery。クライアントが自動的に Web プロキシを見つけることができるプロトコルで、明示的クライアント設定の必要なしにプロキシの活用を可能にします。

Websense® Content Gateway Online Help

©1996–2011, Yahoo, Inc., and Websense, Inc.

All rights reserved.

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

発行 1 0 4 , 2 0 1 2

アメリカ合衆国にて印刷

R033011760

本書には Yahoo, Inc および Websense, Inc の独占的情報および機密情報が含まれています。本書の内容の全部または一部を Websense, Inc の事前の書面による許可なしに第三者に開示したり、いかなる形式でも複写または複製することを禁じます。

Websense および ThreatSeeker は米国およびその他の国際市場における Websense, Inc. の登録商標です。Websense は、米国において、および国際的に、多くの他の未登録商標を所有しています。すべての他の商標は、それぞれ該当する所有者の財産です。

本ガイドの内容の正確性については万全を期しています。しかしながら、Websense, Inc. および Yahoo, Inc. は、これを一切保証するものではなく、本製品の商品性および特定の用途に対する適合性についても同じく一切保証していません。Websense Inc. は、本ガイドまたはガイドに含まれる例の提供、性能、または使用にかかわる偶発的、副次的ないかなる損害に対しても、責任を負いかねます。本書の情報は、通知なしに変更されることがあります。

Traffic Server は、Yahoo! Inc. の米国および他の国における商標または登録商標です。

Red Hat は Red Hat, Inc. の登録商標です。

Linux は Linus Torvalds の登録商標です。

Microsoft、Windows、Windows NT、および Active Directory は、Microsoft Corporation の米国およびその他の国における登録商標または商標です。

Mozilla および Firefox は、Mozilla Foundation の登録商標です。

Netscape および Netscape Navigator は Netscape Communications Corporation の米国 および その他の国における登録商標です。

UNIX は、AT&T の登録商標です。

他のすべての商標は、それぞれの所有者の財産です。

制限付きの権利について

政府機関による本書に含まれる技術データの使用、複製、または開示は、DFARS 52.227-7013 の「技術データおよびコンピュータ ソフトウェアの権利」の項目のサブ項目 (c) (1)(ii) および FAR、DOD または NASA FAR の補足文書における同様の、または後継の条項に記載されている制限の対象となります。非公開の権利は、米国の著作権法の下で留保されています。契約業者 / 製造業者は、10240 Sorrento Valley Parkway, San Diego, CA 92121 を所在地とする Websense, Inc. です。

Websense Content Gateway の一部には、ライセンス契約に基づき使用された第三者の技術が含まれています。注記およびその所有権については、下記に掲載されています。

Websense Content Gateway のいくつかの部分には下記の技術が含まれます。

OpenSSL 0.9.6

OpenSSL は、GNU (General Public License) の下でライセンス許諾されたオープン ソース ツールキットです。Copyright © 1989, 1991 Free Software Foundation, Inc. 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

このプログラムは無償でライセンスされているため、このプログラムには適用法で許容されている限りにおいて、いかなる保証もありません。別途に書面において記載されていない限り、本プログラムは、著作権保有者および(または)他の当事者によって無保証で提供されており、商品性および特定の用途に対する適合性に関する暗黙の保証を含む(ただしそれに限定されない)明示または暗黙の一切の保証は否認されています。本プログラムの品質およびパ

パフォーマンスに関する全リスクは、お客様が引き受けるものとします。本プログラムに問題が生じた場合、お客様が必要なサービス、修理、または修正のすべての費用を負うものとします。

Netscape Directory SDK 4.0 for C

Netscape Directory SDK 4.0 for C は、Netscape ONE SDK End User License Agreement (Netscape ONE SDK エンドユーザー ライセンス 契約) に基づき無償で使用できます。

各コンポーネントは、無保証で提供されており、商品性、特定の用途および著作権侵害の不存在に対する適合性を含み(ただしそれに限定されない)明示または暗黙の一切の保証を否認します。コンポーネントの品質およびパフォーマンスに関する全リスクは、お客様の負担になります。コンポーネントが不良または不正確であると判明した場合、事情に応じて、Netscape やその供給業者ではなくお客様がサービスおよび修理の全費用を引き受けることとします。さらに、コンポーネントによって実装されているセキュリティメカニズム(もしあれば)には固有の制限事項があり、またお客様は各コンポーネントがお客様の要件に十分に対応するものであることを判断する必要があります。この保証の放棄は、本契約の基本的部分を構成しています。一部の司法管轄区域は、暗黙の保証の除外を許可していません。その場合この権利放棄はお客様には適用されず、お客様は他の法律上の権利(司法管轄区域によって異なる)を有する場合があります。

Tcl 8.3

Tcl ソフトウェアは、Regents of University of California、Sun Microsystems, Inc.、Scriptics Corporation、および他の当事者が著作権を有しています。以下の条件は、個々のファイルにおいて明示的に否認されていない限り、本ソフトウェアに関連するすべてのファイルに適用します。作成者は、既存の著作権に関する注記が全てのコピーにおいて保持されること、およびこの注記がすべての配布物において逐語的に含まれていることを条件に、本ソフトウェアおよびそのマニュアルをいかなる目的においても、無償で使用、コピー、変更、配布、ライセンスすることを許諾します。承認された使用において、いかなる書面による契約、ライセンス、または使用料も要求されません。本ソフトウェアへの変更は、その作成者による著作権登録が可能であり、本契約に記載しているライセンス条件に従う必要はありませんが、但しライセンス条件を変更する場合は、それが適用される各ファイルの最初のページに新しいライセンス条件が明記される必要があります。

いかなる場合でも、作成者または販売代理店は、本ソフトウェア、そのマニュアル、またはその派生物の使用から生じたいかなる直接的、間接的、特殊的、偶発的、または結果的損害に対して、作成者がそのような損害が生じる可能性について通告を受けていた場合でも、すべての当事者に対して一切の責任を負いません。作成者および販売代理店は、特に、商品性、特定の目的に対する適合性、および著作権侵害の不存在に関する暗黙の保証を含む(ただしそれに限定されない)一切の保証を否認するものとします。本ソフトウェアは、無償で提供されており、作成者および販売代理店は、保守、サポート、更新、機能強化、変更を提供する責任はありません。

libdb

LIBDB Copyright © 1991, 1993 The Regents of the University of California. All rights reserved. 本製品には、University of California, Lawrence Berkeley Laboratory とそのコントリビューターによって開発されたソフトウェアが含まれます。

本ソフトウェアは、REGENTS およびコントリビューターによって無保証で提供されており、商品性および特定の用途に対する適合性に関する暗黙の保証を含む(ただしそれに限定されない)明示または暗黙の一切の保証は否認されています。いかなる場合でも、REGENTS またはそのコントリビューターはいかなる形においても本ソフトウェアの使用から生じたいかなる直接的、間接的、偶発的、特殊的、懲罰的、派生的損害(データまたは利益の損失、もしくは業務の中断を含むがそれに限定されない)に対しても、その原因や、責任に関する法理に関わりなく、また、契約上の保証、厳格な責任に基づく保証、不法行為(過失またはその他を含む)のいずれにも基づくものに関わりなく、また、そのような損害が生じる可能性について通告を受けていた場合でも、一切責任を負いません。

INN

Copyright © 1991, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001 The Internet Software Consortium and Rich Salz. 本コードは、Rich Salz Redistribution により Internet Software Consortium に提供されたソフトウェアから派生したものであり、以下の条件が満たされている場合は、変更の有無にかかわらず、ソース形式およびバイナリ形式での使用を許可します。1. ソース・コードの再配布においては、上記の著作権に関する注記、この条件のリスト、および以下の免責事項が保持されている。2. バイナリ形式による再配布においては、そのマニュアルおよび(または)その他の添付される資料に、上記の著作権に関する注記、この条件のリスト、および以下の免責事項が記載されている。3. 本ソフトウェアの機能または使用方法を記述するすべての広告物には、下記の献辞を表示しなければなりません: 本製品には、Internet Software Consortium とそのコントリビューターによって開発されたソフトウェアが含まれます。4. Internet Software Consortium またはそのコントリビューターの名称が、事前の特別の書面による承諾なしに本ソフトウェアから派生した製品の推奨または販売促進のために使用されない。

本ソフトウェアは、INTERNET SOFTWARE CONSORTIUM およびコントリビューターによって無保証で提供されており、商品性および特定の用途に対する適合性に関する暗黙の保証を含む(ただしそれに限定されない)明示または暗黙の一切の保証は否認されています。いかなる場合でも、INTERNET SOFTWARE CONSORTIUM またはコントリビューターはいかなる形においても本ソフトウェアの使用から生じたいかなる直接的、間接的、偶発的、特殊的、懲罰的、派生的損害(代替品またはサービスの購入、使用機会、データまたは利益の損失、もしくは業務

の中断を含むがそれに限定されない)に対しても、その原因や、責任に関する法理に関わりなく、また、契約上の保証、厳格な責任に基づく保証、不法行為(過失またはその他)のいずれに基づくものかに関わりなく、また、そのような損害が生じる可能性について通告を受けていた場合でも、一切責任を負いません。

MRTG

Multi Router Traffic Grapher (MRTG) は、GNU General Public Licenses の条件に基づき無料で利用できます。Copyright © 1989, 1991 Free Software Foundation, Inc. 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

本プログラムは無償で許諾されたものであるもので、準拠法によって許可されている範囲で、本プログラムの保証はありません。別途に書面において記載されていない限り、本プログラムは、著作権保有者および(または)他の当事者によって無保証で提供されており、商品性および特定の用途に対する適合性に関する暗黙の保証を含む(ただしそれに限定されない)明示または暗黙の一切の保証は否認されています。本プログラムの品質およびパフォーマンスに関する全リスクは、お客様が引き受けるものとします。本プログラムに問題が生じた場合、お客様が必要なサービス、修理、または修正のすべての費用を負うものとします。

Libregx

Copyright © 1992, 1993, 1994, 1997 Henry Spencer. All rights reserved. このソフトウェアは、American Telephone and Telegraph Company または Regents of the University of California のすべてのライセンスの対象ではありません。

libmagic

Copyright (c) Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995.

Software written by Ian F. Darwin and others; maintained 1994- Christos Zoulas.

このソフトウェアは、United States Department of Commerce のいかなる輸出規制の対象でもなく、すべての国または全世界に輸出できます。

以下の条件が満たされている場合は、変更の有無にかかわらず、ソースフォームおよびバイナリーフォームにより再配布および使用を許可します:

1. ソース・コードの再配布においては、上記の著作権に関する注記、この条件のリスト、および以下の免責事項が、ファイルの先頭の直後に記載されている。
2. バイナリ形式による再配布においては、そのマニュアルおよび(または)その他の添付される資料に、上記の著作権に関する注記、この条件のリスト、および以下の免責事項が記載されている。

本ソフトウェアは、著作者およびコントリビューターによって無保証で提供されており、商品性および特定の用途に対する適合性に関する暗黙の保証を含む(ただしそれに限定されない)明示または暗黙の一切の保証は否認されています。いかなる場合でも、著作者またはコントリビューターはいかなる形においても本ソフトウェアの使用から生じたいかなる直接的、間接的、偶発的、特殊的、懲罰的、派生的損害(代替品またはサービスの購入、使用機会、データまたは利益の損失、もしくは業務の中断を含むがそれに限定されない)に対しても、その原因や、責任に関する法理に関わりなく、また、契約上の保証、厳格な責任に基づく保証、不法行為(過失またはその他)のいずれに基づくものかに関わりなく、また、そのような損害が生じる可能性について通告を受けていた場合でも、一切責任を負いません。



索引

A

Adaptive Redirection Module ARM を参照。

admin, 2

analytic_server プロセス, 7

ARM, 6, 51, 76

迂回と WCCP, 53

静的バイパス ルール, 74

有効化, 52

リダイレクトのルール, 52

ASCII ログ ファイル, 242

ASCII_PIPE モード, 240, 389

auth.config ファイル, 369

B

bypass.config ファイル, 372

フォーマット, 373

例, 374

C

cache.config ファイル, 23, 374

cache-control ヘッダー, 25

Citrix, 204, 209, 221

Content Gateway Manager, 122, 186

Performance ボタン, 124

アクセスの制御, 184

アラーム, 125

アラームボタン, 262

設定モード, 12, 111

統計の表示, 121

モニタ モード, 121

モニタ モードの起動, 121

ユーザー アカウント, 185

ログオン, 12

起動, 12

Content Gateway Manager で使用するブラウザ, 11

Content Gateway Manager の起動, 12

Content Gateway Manager へのアクセス, 12, 185

Content Gateway Manager へのアクセスの制御, 184

Content Gateway Manager へのホスト アクセス, 186

Content Gateway Manager へのホスト アクセスの制御, 186

Content Gateway Manager へのログオン, 12

Content Gateway の構成, 111

content_cop プロセス, 7

content_gateway プロセス, 7

content_line -h コマンド, 18

content_manager プロセス, 7

D

Date ヘッダー, 23

DNS

プロキシ キャッシング, 107

リゾルバ, 7

DNS サーバー

指定, 196, 462

E

Expires ヘッダー, 22

F

filter.config ファイル, 377

フォーマット, 378

例, 379

FIPS 140-2, 187

force immediate update オプション, 29

FTP オブジェクト

キャッシング, 39

最新性, 27

FTP オブジェクトのキャッシング, 39

FTP クライアント アプリケーション, 46

G

Graphs ボタン

Content Gateway Manager, 122

H

hosting.config ファイル, 380

HTML エラー メッセージ, 474

HTTP

キャッシュ階層, 93, 94, 393

ホスト、個別のログ, 248

代替, 38

プロキシ キャッシング

HTTP 代替, 38
HTTP 応答メッセージ, 477
HTTP オブジェクトの最新性, 22

I

ICAP, 135
ICAP Service URI, 140
IP スプーフィング, 79
ip_allow.config ファイル, 184, 382
 フォーマット, 382
 例, 382
ipnat.conf ファイル, 383
IWA, 201
 設定, 202
 設定のまとめ, 202
 ドメイン コントローラを見つける, 205
 ドメインの変更, 204
 トラブルシューティング, 205
 ホスト名, 変更, 203
 ホスト名の長さの制限, 203
IWA でのホスト名の長さの制限, 203

J

Java, 11
JavaScript, 11

K

Kerberos, 201

L

Last-Modified ヘッダー, 23
LDAP プロキシ認証, 210
log_hosts.config ファイル, 248
logcat アプリケーション, 243
logs_xml.config ファイル, 239
LogFilter 定義, 387
LogFormat 定義, 387
LogObject 定義, 388
logs_xml.config ファイル, 239

M

manager のアラーム, 8
max-age ヘッダー, 22
mgmt_allow.config ファイル, 186

mgmt_allow.config ファイル, 392

My Proxy
 統計, 259
My Proxy ボタン
 Monitor タブ, 122

N

Netscape Common ログ記録フォーマット, 363
Netscape Extended ログ記録フォーマット, 364
Networking ボタン
 Content Gateway Manager Monitor タブ, 124
NTLM プロキシ認証, 207, 208
NTLMv2, 201

O

ログ記録
 バイナリ ファイルの ASCII への変換, 243
Online certification status protocol (オンライン
 証明書ステータス プロトコル), 170

P

PAC ファイル
 HTTPS, 148
 SSL Manager, 147
parent.config ファイル, 94
parent.config ファイル, 393
partition.config file, 101
partition.config ファイル, 396
pin-in-cache, 376
print_bypass ユーティリティ, 77
Protocols ボタン
 Content Gateway Manager Monitor タブ, 122
PUSH, 378

R

RADIUS プロキシ認証, 213, 214
RAM キャッシュ, 97, 104
Raw ディスク, 464
records.config ファイル, 23
records.config の変数の変更, 116
records.config ファイル, 397

S

SAC (スタンドアローン照合サーバー), 252

- Secure Sockets Layer, 186
- Security ボタン
 - Content Gateway Manager Monitor タブ, 123
- SOCKS, 193
 - プロキシ オプション, 195
- socks_server.config ファイル, 461
- socks.config ファイル, 460
- SOCKS サーバー
 - 指定, 460, 461
- splitdns.config ファイル, 196, 462
 - ファイル
 - splitdns.config ファイル, 462
- Squid ログ記録フォーマット, 363
- SSL, 186
 - アウトバウンド トラフィック, 163
 - インバウンド トラフィック, 162
 - 証明書, 187
 - 有効化, 187
- storage.config ファイル, 99, 464
 - フォーマット, 464
- Subsystems ボタン
 - Content Gateway Manager Monitor タブ, 123
- Super Administrator (優先管理者)
 - admin, 2
- T**
- TRITON – Web Security, 2
- U**
- update.config ファイル, 28, 465
- URL の確認, 29
- url_regix, 367
- URL 正規表現, 367
- W**
- WCCP, 55
 - サービス グループ, 64
 - 有効化, 65
 - ロード バランシング, 57
- wccp
 - wccp.config ファイル, 467
- WCCP 2.0
 - セキュリティ, 64
- WCCP 処理
 - 無効化, 64
 - 有効化, 61
- WCCP2 ルーター
 - 設定, 59
- WCGAdmin start コマンド, 18
- Web Security ユーザー認証, 197
- web サイト アクセス, 171
- web サイトのアクセス, 171
- Web ブラウザの認証サポートの制約, 199
- web プロキシ キャッシング, 3, 21
- Websense Content Gateway, 18
 - 確認, 16
- Websense Content Gateway Manager
 - グラフィックボタン, 262
 - モニタ モード, 12
- Websense Content Gateway が実行していることの確認, 16
- Websense Content Gateway の構成, 116
 - コマンドラインの使用, 115
 - 保存, 117
- Websense Content Gateway の構成の復元, 117, 118
- Websense Content Gateway のコンポーネント, 5
- Websense Content Gateway のプロセス, 7
- Websense Content Gateway の起動, 18
- Websense Content Gateway の設定, 17
- WELF, 391
- Windows 7, 13
- WWW-Authenticate ヘッダー, 35
- X**
- X-Authenticated-User, 294
- X-Forwarded-For, 294
- XML カスタムログフォーマット, 385, 239
- あ**
- アウトバウンド トラフィック
 - SSL, 163
- Content Gateway Manager
 - アクセス, 12
- アラート, 8
- アラーム, 8, 125
 - 解除, 126
 - 電子メール通知, 127
 - 表示, 126

アラーム スクリプト ファイル, 127
アラーム メッセージ, 471
アラームの解除, 126
アラームのスクリプト ファイル, 127
アラームの電子メール送信, 127
アラームの表示, 126
アラームボタン, 262
暗号化, 482

い

イベント ログ エントリ、例, 255
イベント ログ ファイル
管理, 235
照合, 249
統計情報, 253
バイナリから ASCII への変換, 243
分割, 247
要約ログ, 241
イベント ログ ファイルの照合, 249
イベント ログ ファイルの分割, 247
インシデント, 171
インバウンド トラフィック
SSL, 162

え

エージング係数
変更, 23
エージング係数の変更, 23
エラー メッセージ, 469
HTML, 474
エラー ログ ファイル, 234

お

オーファン ログ ファイル, 250
オブジェクト キャッシング、強制, 37
オブジェクト キャッシングの強制, 37
オブジェクト ストア, 97
オブジェクトの最新性
エージング係数, 23
親フェールオーバー, 94
親プロキシ
バイパス, 94, 393
親プロキシをバイパス, 393
オリジン サーバー, 21

か

階層キャッシング, 3
HTTP 階層, 93
親フェールオーバー, 94
カスタマ サポート, 10
カスタム ログ
フィールド, 359
カスタム ログ記録, 239
仮想 IP アドレス, 90
追加, 91
編集, 91
仮想 IP アドレスの追加, 91
仮想 IP アドレスの編集, 91
仮想 IP フェールオーバー, 4, 89
管理クラスタ化, 84
管理者 ID, 12
管理者 ID およびパスワードの設定, 184, 185
管理者 ID, 設定, 185
管理者 ID, 変更, 185
管理者パスワード, 185
管理者パスワード デフォルト
管理者 ID, 12
管理専用クラスタ化, 4
管理ツール, 8

き

起動, 18
Content Gateway Manager 設定モード, 111
Content Gateway Manager モニタ モード
, 121
キャッシュ統計, 262
キャッシュ統計表示, 262
キャッシュ
クリア, 104
更新のスケジュール設定, 27
コンテンツ, 99, 464
統計, 122
パーティション, 101
ヒット, 22
ミス, 22
容量の変更, 99
キャッシュ アフィニティ, 54, 56
キャッシュ コンテンツのリスト, 99
キャッシュ スペース

- 管理, 101
 - キャッシュ ピンニング, 30
 - キャッシュ期間, 22
 - キャッシュされたオブジェクト
 - FTP, 22
 - HTTP, 22
 - 最新性, 22
 - 有効期限, 22
 - キャッシュ統計の表示, 122
 - キャッシュのクリア, 104
 - キャッシュのパーティション区分, 101
 - キャッシュ要求の概要, 21
 - キャッシュ容量
 - 管理, 396
 - キャッシュ容量の削減, 100
 - キャッシュ容量の増加, 99
 - キャッシュ容量の変更, 99
 - キャッシング, 22
- く**
- クッキー。クッキーを含むコンテンツのキャッシングを参照
 - クッキーを含むコンテンツのキャッシング, 37
 - クライアント アクセス制御リスト, 74
 - クライアントの no-cache 指令, 33
 - クライアントのプロキシ キャッシュへのアクセス, 74, 183
 - クラスタ化
 - 管理, 84
 - 管理専用, 4
 - ノードの追加, 87
 - 仮想 IP フェールオーバー, 4
 - クラスタへのノードの追加, 87
 - クラスタ化
 - モード, 4
 - グラフィックボタン
 - 統計, 262
- け**
- 検証、証明書のバイパス, 168
- こ**
- 更新
 - スケジュール, 465
 - 構成情報、共有, 84
 - 構成のスナップショット
 - 削除, 119
 - 撮る, 118
 - 復元, 118
 - 構成のスナップショットの削除, 119
 - 構成のスナップショットの復元, 118
 - 構成の保存, 118
 - 子プロキシからの認証読み込み, 294
 - WCGAdmin start コマンド, 18
 - コマンド
 - content_line -h, 18
 - WCGAdmin start, 18
 - コマンドのリスト, 18
 - コマンドライン インターフェース, 17
 - コマンドラインインタフェース
 - コマンド, 283
 - 変数, 285
 - コンテンツ, 179
- さ**
- サーバーの no-cache 指令, 34
 - サービス グループ, 64
 - WCCP 処理の無効化, 64
 - WCCP 処理の有効化, 61
 - 設定のガイドライン, 60
 - サービス グループの ID 番号, 60
 - 再確認, 26
 - サイズの変更
 - RAM キャッシュ, 104
 - 再認証, 200
 - サブシステム
 - 統計, 270
 - Content Gateway Manager
 - サポートされているブラウザ, 11
- し**
- システム ステータス, 8
 - 遮断戦略, 53
 - 使用開始, 11
 - 情報漏洩、管理, 135
 - 情報漏洩の管理, 135
 - ステータスの変更, 160
 - 証明書, 150, 160
 - インポート, 152
 - 下位認証機関, 153

- 管理, 159
 - 許可, 160
 - 拒否, 160
 - 検証のバイパス, 168
 - 削除, 160
 - 生成, 151
 - 取り消しステータス, 169
 - バックアップ, 161
 - 復元, 161
 - 証明書エラー, 12
 - 証明書取り消しのリスト
 - 更新, 169
 - 証明書の確認
 - 証明書確認, 160
 - 証明書の管理, 159
 - 証明書の検証、バイパス, 168
 - 証明書の検証のバイパス, 168
 - 証明書の削除, 160
 - 証明書のステータス, 159
 - 証明書のステータスの変更, 159, 160
 - 証明書のバックアップを作成, 161
 - 証明書の復元, 161
 - 証明書を許可, 160
 - 証明書を拒否, 160
- す**
- スケジュール設定された更新, 465
 - スタンドアロン照合サーバー, 252
 - ステータス、証明書, 159
 - ステータスの変更, 160
 - スナップショット
 - 削除, 119
 - 撮る, 118
 - 復元, 118
 - スプーフィング, 79
- せ**
- 正規表現, 367
 - 制御
 - Content Gateway Manager へのアクセス, 184, 392
 - クライアントのプロキシ キャッシュへのアクセス, 183
 - 静的バイパス ルール, 76, 374
 - セキュリティ, 183
 - Content Gateway Manager
 - アクセス, 184
 - SOCKS, 192
 - オプション, 1, 183
 - セキュアな管理のための SSL, 186
 - 統計, 266
 - プロキシ ユーザー認証, 197
 - 分割 DNS, 196
 - 管理者 ID およびパスワードの設定, 184
 - セキュリティ証明書アラート, 12
 - 絶対最新性限界値, 設定, 24
 - 絶対最新性限界値の設定, 24
 - 設定
 - リモート, 186
 - 設定, 管理者パスワード, 185
 - 設定オプション, 193
 - records.config ファイルでの変更, 116
 - 設定ファイル, 116
 - filter.config, 377
 - 設定モード
 - Content Gateway Manager, 111
- そ**
- 送信するコンテンツ、検査, 135
- た**
- 代替のキャッシング, 38
 - ダイナミック コンテンツ
 - キャッシング, 36
 - ダイナミック コンテンツのキャッシング, 36
 - タイムスタンプ, 245
 - 直ちに更新, 29
 - 端末サーバー, 204, 209, 221
- て**
- ディスク使用状況
 - 限定, 101
 - ディスクの使用
 - 制限, 396
 - ディレクトリ サービス, ユーザー認証, 198
 - テクニカル サポート, 10
 - デフォルト, 12

と

- 透過的プロキシ, 21
 - 遮断戦略, 53
- 透過的プロキシ キャッシング, 51
 - L4 スイッチ, 54
 - WCCP, 55
 - ソフトウェア ソリューション, 73
 - ポリシー ベースのルーティング, 72
- 透過的プロキシ認証, 200, 328
 - セッション TTL, 200
 - 認証モード, 200
 - リダイレクト ホスト名, 200
- 統計
 - Content Gateway Manager からの表示, 121
 - Content Gateway Manager での表示, 121
 - My Proxy, 259
 - コマンドラインからの表示, 124
 - サブシステム, 270
 - ネットワーク, 272
 - プロトコル, 263
- 統計の表示
 - Content Gateway Manager から, 121
 - コマンドラインを通じて, 124
- 統合 Windows 認証, 201
- 動的バイパス ルール, 74
 - 設定, 75
 - バイパス拒否, 75, 373
- 動的バイパス ルールの上書き, 374
- 動的バイパス統計の表示, 76
- トラフィック グラフ, パフォーマンス グラフを参照, 8
- トラフィック分析オプション, 8
- トラブルシューティング
 - 統合 Windows 認証, 205
- トランザクション ロギング, 9
- 取り消しステータス, 169
- 取り消しリスト
 - 復元, 161
- 取り込み間隔, 246
- 取り込みログ ファイル, 245
- 取り込みログ ファイルの命名, 245

な

- 内部ルート CA, 151

- バックアップ, 158

に

- 認証機関
 - 追加, 159, 160
- 認証機関の追加, 159, 160

ね

- ネットワーク
 - 統計, 272

の

- ノード
 - クラスタへの追加, 87

は

- パーティション, 464
- バイナリ ログ ファイル, 242
- バイパス ルール
 - 静的, 76
 - 動的, 74
 - 表示, 77
- バイパス ルールの表示, 77
- バイパス拒否ルール, 75, 373
- バイパスルール
 - 拒否, 373
- 配備のオプション, 3
- パスフレーズ, 153
- パスワード, 12, 185
- パスワード, 設定, 管理者, 185
- 暗号化, 482
- パスワードの暗号化, 482
- バックアップ ドメイン コントローラ, 199
- パフォーマンス グラフ, 8

ふ

- ファイル
 - auth.config, 369
 - bypass.config, 372
 - cache.config, 23, 374
 - hosting.config, 380
 - ip_allow.config, 184, 382
 - ipnat.conf, 383
 - log_hosts.config, 248
 - logs_xml.config, 239
 - mgmt_allow.config, 186, 392

- parent.config, 94, 393
- partition.config, 101, 396
- records.config, 397
- socks_server.config, 461
- socks.config, 460
- splitdns.config, 196
- storage.config, 99, 464
- update.config, 465
- wccp.config, 467
- 複数レルムのユーザー認証, 216
 - IWA ルール, 221
 - LDAP ルール, 224
 - グローバル オプション, 220
 - 使用例, 227
 - 設定のまとめ, 218
 - ドメイン, 219
 - トラブルシューティング, 230
 - 認証ロジック, 230
 - 別名とログ記録, 218
 - ルールの変更, 226
 - レガシー NTLM ルール, 222
- プロキシ
 - 透過的, 21
 - 明示的, 21
- プロキシ キャッシュ
 - クライアント アクセス, 183
 - クライアントアクセスの制御, 382
- プロキシ キャッシング
 - cache-control ヘッダー, 25
 - FTP オブジェクトの最新性, 27
 - HTTP オブジェクトの再確認, 26
 - HTTP キャッシングの無効化, 36
 - HTTP 代替, 38
 - WWW-Authenticate ヘッダー, 35
 - キャッシュするか否か, 31
 - キャッシュの更新のスケジュール設定, 27
 - クッキーを含むコンテンツ, 37
 - クライアントの no-cache 指令, 33
 - サーバーの no-cache 指令, 34
 - ダイナミック コンテンツ, 36
 - ヘッダーの要件, 24
- プロキシ ユーザー認証, 197
- 親プロキシのバイパス, 94
- プロセス (Websense Content Gateway), 7
- プロトコル
 - 統計, 263
- 分割 DNS, 196
- へ
- ヘッダー
 - cache-control, 25
 - Last-Modified ヘッダー [Last-Modified], 23
 - max-age, 22
 - WWW-Authenticate, 35
 - 期限切れ, 22
- ヘッダー情報削除, 377
- ヘッダー情報を保持, 377
- ヘッダーの要件, 24
- ヘッドルーム限界, 236
- ヘルス アラート, 8
- 変更, 185
- 変数
 - records.config ファイル, 116
 - records.config ファイル, 397
- ほ
- ホスト アクセス, 186
- ホスト データベース, 6
- ホスト ログ分割, 248
- ホスト名, 変更, 203
- ま
- マルチユーザー IP 除外, 204, 209, 221
- マルチユーザー ホスト, 204, 209, 221
- む
- 無効化
 - HTTP キャッシング, 36
 - HTTP 上の FTP のキャッシング, 40
 - ログ記録, 234
- め
- 明示的プロキシ, 21
 - HTTPS PAC ファイル, 148
 - SSL, 147
- 明示的プロキシ キャッシング, 3
- メッセージ
 - 証明書検証エラー, 180
 - 接続エラー, 181

も

- モニタ
 - リモート, 186
- モニタ モード, 121

ゆ

- ユーザー アカウント, 185
- ユーザー 認証, 197
 - Kerberos, 201
 - LDAP, 210
 - NTLM, 207
 - NTLMv2, 201
 - RADIUS, 213
 - サポートされているディレクトリ, 198
 - タイムアウト時間, 200
 - 透過的, 198
 - 透過的プロキシ, 200
 - 統合 Windows, 認証のまとめ, 202
 - 統合 Windows, 201
 - バックアップ ドメイン コントローラ, 199
 - 複数レルムの認証, 216
 - IWA ルール, 221
 - LDAP ルール, 224
 - グローバル オプション, 220
 - 使用例, 227
 - 設定のまとめ, 218
 - ドメイン, 219
 - トラブルシューティング, 230
 - 認証ロジック, 230
 - 別名とログ記録, 218
 - ルールの変更, 226
 - レガシー NTLM ルール, 222
 - ブラウザの制約, 199
- ユーザー 認証の設定
 - NTLM, 208
 - RADIUS, 214
- ユーザー 認証のタイムアウト時間, 200
- 有効期限, 22

よ

- 要求のリダイレクト (ARM), 51
- 要求を許可, 377
- 要求を拒否, 377
- 要約ログ ファイル, 241

り

- リダイレクト ホスト名, 200
- リモート モニタリングおよび設定, 186

る

- ルーター
 - 設定, 59
- ルート CA
 - 内部, 151

ろ

- ログ ファイル
 - 自動削除, 236
- ログ ファイル、コンテンツ, 179
- ログ ファイルのアクセス, 179
- ログ ファイルの自動削除, 236
- ログ フォーマット, 237
- ログオン
 - Windows 7, 13
- ログ記録
 - ASCII_PIPE, 240, 389
 - Netscape Common フォーマット, 363
 - Netscape Extended-2 フォーマット, 364
 - Netscape Extended フォーマット, 364
 - Squid フォーマット, 363
 - SSL Manager, 177
 - WELF, 391
 - アクセス ログ, 177
 - アクティビティ ログ, 177
 - オフセット時刻, 246
 - カスタム ログ, 359
 - スタンドアロン照合サーバー, 252
 - タイムスタンプ, 246
 - 統計情報, 253
 - バイナリ ファイルの ASCII への変換, 243
 - ファイル分割, 247
 - ファイルを保持する時間, 178
 - ヘッドルーム限界, 236
 - 無効化, 234
 - 要約の集計, 241
 - ログ エントリの例, 255
 - ログ ファイル フォーマットの選択, 237
 - ログ ファイルの管理, 235
 - ログ ファイルのサイズ, 178
 - ログ ファイルの照合, 249

ログ記録統計情報の表示 , 253
ログ照合 , 249

ログ照合サーバー , 250