SonicWall® SonicOS 6.5 セキュリティ設定

管理

SONICWALL®

目次

第 1 部 セキュリティ設定 | ファイアウォール設定

ファイアウォールの詳細設定 8
ファイアウォール設定 > 詳細 9
侵入検知と防止 10
動的ポート機能への対応 10
ソース ルーティング パケット 13
内部 VLAN 13
接続数 14
動的接続サイジング 16
アクセス ルール サービス オプション 16
IP および UDP チェックサム強制 17
ジャンボ フレーム 18
IPv6 の詳細設定 18
制御プレーン フラッド防御 20

帯域幅管理の設定 21
帯域幅管理とは 21
ファイアウォール設定 > 帯域幅管理 24
グローバル帯域幅管理の設定 27
詳細帯域幅管理 35
詳細帯域幅管理の設定 39

フラッド防御の設定 50
ファイアウォール設定 > フラッド防御 51

ファイアウォール マルチキャストの設定 70
ファイアウォール設定 > マルチキャスト 70
マルチキャスト設定 71
マルチキャスト ポリシー 71
IGMP 状態テーブル 73
マルチキャストの有効化 73

サービス品質の管理 78
ファイアウォール設定 > サービス品質の割付 78
分類 78
級割 79
制限 80
802.1p と DSCP QoS 81
帯域幅管理 93
用語集 93

SSL 制御の設定 97
SSL 制御について 97
ファイアウォール設定 > SSL 制御 105
SSL 制御の設定 105
ゾーンでの SSL 制御の有効化 109
SSL 制御のイベント 110

暗号制御の設定 112
暗号制御について 112
ファイアウォール設定 > 暗号制御 112

第 2 部 セキュリティ設定 | セキュリティ サービス

SonicWall セキュリティ サービスの管理 121
SonicWall セキュリティ サービスについて 121
セキュリティ サービスの設定 122

コンテンツ フィルタ サービスの設定 126
セキュリティ サービス > コンテンツ フィルタ: SonicWall CFS 127
セキュリティ サービス > コンテンツ フィルタ: Websense Enterprise 140

DPI-SSL 強制 146
DPI-SSL 強制について 146
DPI-SSL 強制の管理 147

SonicWall クライアント アンチウイルスの有効化 150
セキュリティ サービス > クライアント AV 強制 150
クライアント アンチウイルス サービスの設定 151

クライアント CF 強制の設定 158
セキュリティ サービス > クライアント CF 強制 158
ネットワーク ゾーンでクライアント CFS を有効化する 160

SonicWall ゲートウェイ アンチウイルス サービスの管理 162
ゲートウェイ アンチウイルス サービスSonicWall について 162
SonicWall ゲートウェイ アンチウイルス保護のセットアップ 167
SonicWall GAV シグネチャの表示 178

侵入防御サービスの有効化 181
侵入防御サービスについて 181
侵入防御サービスの設定 183

キャプチャ ATP の設定 192
セキュリティ サービス > キャプチャ ATP 193
キャプチャ ATP について 193
キャプチャ ATP の有効化 196
「セキュリティ サービス > キャプチャ ATP」ページについて 196

キャプチャ ATP の設定 201
GAV またはクラウド アンチウイルスの無効化 203

アンチスパイウェア サービスの有効化 205
アンチスパイウェアについて 205
セキュリティ サービス > アンチスパイウェア 206
アンチスパイウェア ポリシーの設定 211

SonicWall リアルタイム ブラックリストの設定 214
セキュリティ サービス > RBL フィルタ 214
リアルタイム ブラックリスト フィルタについて 215
RBL フィルタの設定 215

地域 IP フィルタの設定 220
セキュリティ サービス > 地域 IP フィルタ 220
地域 IP フィルタの設定 221
ユーザ定義国リストの作成 224
ウェブ遮断ページの設定のカスタマイズ 228
地域 IP フィルタ診断の使用 230

ボットネット フィルタの設定 234
セキュリティ サービス > ボットネット フィルタ 234
ボットネット フィルタの設定 235
ユーザ定義ボットネット リストの作成 236
動的 HTTP 認証の設定 240
ウェブ遮断ページの設定のカスタマイズ 242
ボットネット フィルタ診断の使用 243
ボットネット機能およびデータベースの状況表示 246

第 3 部 セキュリティ設定 | 復号化サービス

DPI-SSL について 248
DPI-SSL について 248
配備方針 251
DPI SSL のカスタマイズ 252
装置モデル別の接続 252

DPI-SSL/TLS クライアントの設定 254
復号化サービス > DPI-SSL/TLS クライアント 254
DPI-SSL 状況の表示 255
DPI-SSL/TLS クライアントの設定 255

DPI-SSL/TLS サーバの設定 272
復号化サービス > DPI-SSL/TLS サーバ 272
DPI-SSL/TLS サーバの設定 273

DPI-SSH の設定 276
DPI-SSH について 276
DPI-SSH ライセンスの有効化 278
DPI-SSH の設定 278

第 4 部 セキュリティ設定 | アンチスパム

アンチスパムについて 284
アンチスパムについて 284
アンチスパム サービスの仕組み 285
アンチスパム ライセンスの購入 290

アンチスパムの有効化とアクティブ化 292
アンチスパム > 基本設定 293
アンチスパムのアクティブ化 293
ジャンク ストアのインストール 295
電子メール脅威種別の設定 296
アクセス リストの設定 298
詳細オプションの設定 300

アンチスパム ログの設定 303
アンチスパム > 詳細 303
システム ファイル/ログ ファイルのダウンロード 304

RBL フィルタの設定 308
アンチスパム > リアルタイム ブラックリスト フィルタ 309
RBL リストについて 309
RBL フィルタの有効化 310
RBL サービスの管理 311
ユーザ定義 SMTP サーバ リスト 315
リアルタイム ブラック リストのテスト 317

中継ドメインの指定 318
アンチスパム > 中継ドメイン 318
オープン リレーについて 319
許可された中継ドメインのリスト作成 319

ジャンク ボックス設定の構成 320
アンチスパム > ジャンク ボックス設定 320

ジャンク サマリの管理 322
アンチスパム > ジャンクボックス サマリ 322
ジャンク サマリの管理 323
既定値に戻す 326

ジャンク ボックスの表示の設定 327

アンチスパム > ジャンク ボックス 327
ジャンク ボックス タブについて 328
メッセージの検索 329
ジャンク ストア内のメッセージの管理 332

ユーザに表示される設定の構成 334
アンチスパム > ユーザ画面セットアップ 334
ユーザ画面セットアップの構成 335
既定の設定に戻す 335

企業の許可および遮断リストの設定 336
アンチスパム > アドレス帳 336
タブについて 337
許可または遮断リストへの項目の追加 338
許可または遮断リストからの項目の削除 339
アドレス帳エントリのインポート 339
アドレス帳エントリのエクスポート 340
許可および遮断リストの検索 340

ユーザの管理 341
アンチスパム > ユーザ管理 341
ユーザ テーブルの更新 342
LDAP 以外のユーザ認証の有効化 342
ユーザの表示 343
ユーザの追加 345
ユーザとしてのサインイン 347

LDAP サーバの設定 348
アンチスパム > LDAP 構成 348
利用可能な LDAP サーバ 349
LDAP サーバの追加 349
LDAP クエリの設定 353
LDAP マッピングの追加 356
グローバル LDAP 設定の構成 357
LDAP サーバ設定の編集 358
LDAP サーバの削除 359

Anti-Spam Desktop ボタンのダウンロード 360
アンチスパム > ダウンロード 360

第 5 部 セキュリティ設定 | 付録

SonicWall サポート 362
このドキュメントについて 363

第 1 部

セキュリティ 設定 | ファイアウォール 設定

- ファイアウォールの詳細設定
- 帯域幅管理の設定
- フラッド防御の設定
- ファイアウォール マルチキャストの設定
- サービス品質の管理
- SSL 制御の設定
- 暗号制御の設定

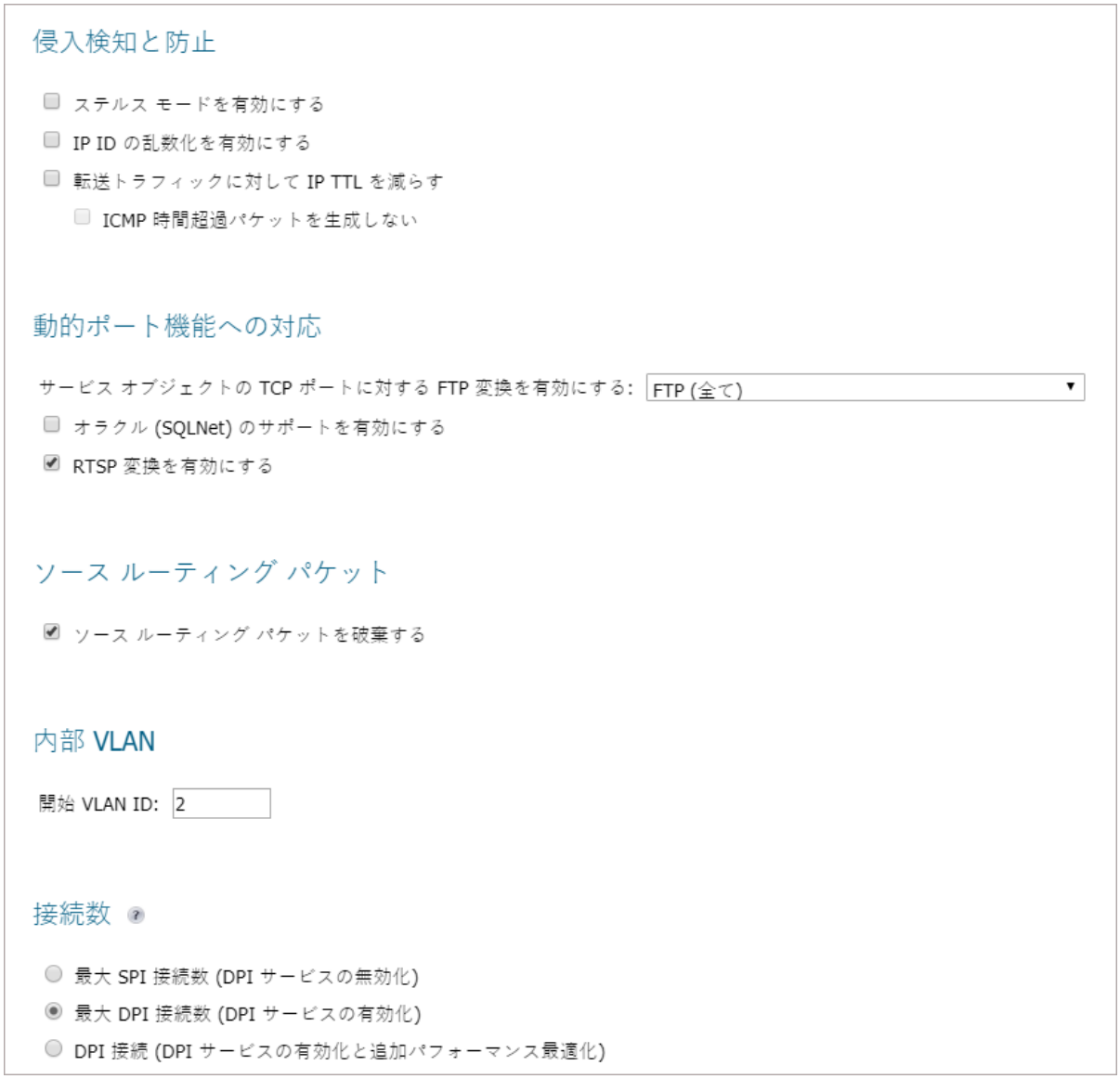
1

ファイアウォールの詳細設定

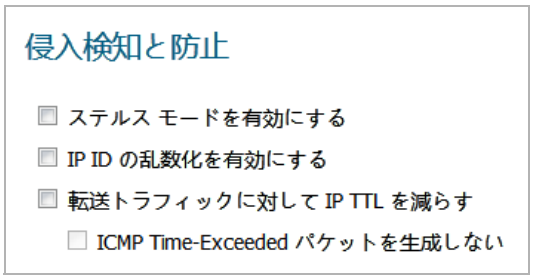
- ファイアウォール設定 > 詳細 (9 ページ)
- 侵入検知と防止 (10 ページ)
- 動的ポート機能への対応 (10 ページ)
- ソース ルーティング パケット (13 ページ)
- 内部 VLAN (13 ページ)
- 接続数 (14 ページ)
- 動的接続サイジング (16 ページ)
- アクセス ルール サービス オプション (16 ページ)
- IP および UDP チェックサム強制 (17 ページ)
- ジャンボ フレーム (18 ページ)
- IPv6 の詳細設定 (18 ページ)
- 制御プレーン フラッド防御 (20 ページ)

ファイアウォール設定 > 詳細

このセクションでは、侵入検知と防止、動的ポート、ソース ルーティング パケット、接続の選択、アクセス ルール オプションなどの詳細なファイアウォール設定を示します。詳細なアクセス ルールに関するオプションを設定するには、「**管理 | セキュリティ設定 > ファイアウォール設定 > 詳細設定**」を選択します。



侵入検知と防止



侵入検知と防止を有効にするには:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 詳細設定**」に移動します。

2 「**侵入検知と防止**」までスクロールします。

3 既定では、セキュリティ装置は着信接続要求を "遮断" または "オープン" として扱います。遮断された着信接続要求にセキュリティ装置が応答しないようにするには、「**ステルス モードを有効にする**」を選択します。ステルス モードでは、セキュリティ装置は基本的にハッカーから見えなくなります。このオプションは、既定では選択されていません。

4 さまざまな検出ツールを利用するハッカーによってセキュリティ装置の存在が検出されないようにするには、「**IP ID の乱数化を有効にする**」を選択します。このオプションを有効にすると、乱数化された IP ID が IP パケットに割り当てられるようになるので、ハッカーがセキュリティ装置の“特徴"を検出するのが困難になります。このオプションは、既定では選択されていません。

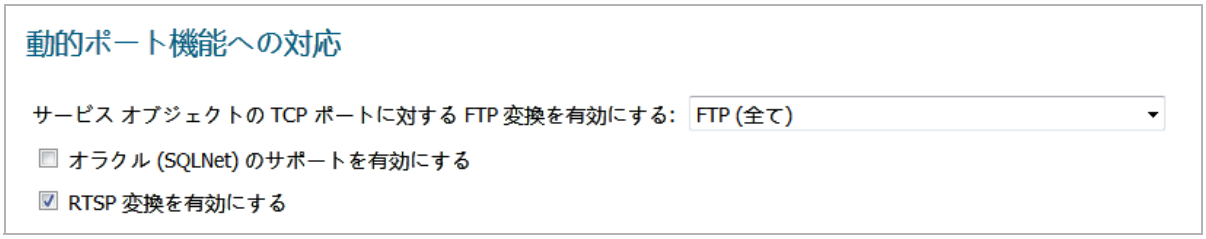
5 Time-to-live (TTL) は、パケットがネットワーク上に長い時間存在しているので破棄するかどうかを、ネットワーク ルータに指示する IP パケットの値です。転送済みで既にネットワーク上に一定の時間存在しているパケットの TTL 値を減らすには、「**転送トラフィックに対して IP TTL を減らす**」を選択します。 このオプションは、既定では選択されていません。

このオプションを選択すると、次のオプションが使用可能になります。

6 ファイアウォールは、TTL 値がゼロに減少したためにパケットが破棄されたことを報告する Time-Exceeded パケットを生成します。これらの報告パケットがファイアウォールで生成されないようにするには、「**ICMP Time-Exceeded パケットを生成しない**」を選択します。このオプションは、既定では選択されていません。

7 「**適用**」を選択します。

動的ポート機能への対応



動的ポートを設定するには:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 詳細設定**」に移動します。

2 「**動的ポート機能への対応**」までスクロールします。

3 「**サービス オブジェクトの TCP ポートに対する FTP 変換を有効にする**」から、サービス グループを選択して特定のサービス オブジェクトの FTP 変換を有効にします。既定で、サービス グループは「**FTP (全て)**」が選択されています。

FTP は TCP ポート (ポート 20 および 21) 上で動作します。ポート 21 は制御ポート、ポート 20 はデータ ポートです。しかし、標準でないポート (2020、2121 など) を使用している場合は、SonicWall はそれを FTP として認識できないため、既定でパケットを破棄します。「**サービス オブジェクトの TCP ポートに対する FTP 変換を有効にする**」オプションを使用すると、サービス オブジェクトを選択して、FTP トラフィックの個別制御ポートを指定できます。

この機能の動作を説明するために、FTP サーバが、ポート 2121 でリッスンしている SonicWall の背後にある次の例を考えます。

a 「**管理 |ポリシー > オブジェクト > アドレス オブジェクト**」ページで、次の値を使用して FTP サーバのプライベート IP アドレスに対する**アドレス オブジェクト**を作成します。

- **名前**: FTP Server Private
- **ゾーン**: LAN
- **種別**: ホスト
- **IP アドレス**: 192.168.168.2

b 「**管理 |ポリシー | オブジェクト > サービス オブジェクト**」ページで、次の値を使用して FTP サーバ用のユーザ定義サービスを作成します。

- **名前**: FTP Custom Port Control
- **プロトコル**: TCP(6)
- **ポート範囲**: 2121 - 2121

c 「**管理 |ポリシー >ルール > NAT ポリシー**」ページで、この NAT ポリシーを作成します:

d 「**管理 |ポリシー > ルール > アクセス ルール**」ページで、このアクセス ルールを作成します:

e 最後に、「**管理 | セキュリティ設定 > ファイアウォール設定 > 詳細設定** 」ページの「**サービス オブジェクトの TCP ポートに対する FTP 変換を有効にする**」で、**FTP Custom Port Control** サービス オブジェクトを選択します。

メモ：サービス グループとサービス オブジェクトの設定の詳細については、*SonicWall SonicOS 6.5 システム セットアップ*を参照してください。

4 ネットワーク上に Oracle9i 以前のアプリケーションがある場合、「**オラクル (SQLNet) のサポートを有効にする**」を選択します。このオプションは、既定では選択されていません。

重要：Oracle10g 以降のアプリケーションに対しては、このオプションを選択しないことを推奨します。

Oracle9i 以前のアプリケーションでは、データ チャネル ポートが制御接続ポートと異なります。このオプションを有効にした場合、SQLNet 制御接続に対して、ネゴシエーションされたデータ チャネルのスキャンが行われます。ネゴシエーションが検出されると、データ チャネルの接続エントリが動的に作成され、必要に応じて NAT が適用されます。SonicOS 内では、SQLNet とデータ チャネルは互いに関連付けられ、1 つのセッションとして処理されます。

Oracle10g 以降のアプリケーションでは、これら 2 つのポートは同一であるため、データ チャネル ポートを別個に追跡する必要はありません。したがって、このオプションを有効にする必要はありません。

5 オーディオとビデオなど、リアルタイム データのオンデマンド提供をサポートするには、「**RTSP 変換を有効にする**」を選択します。RTSP (Real Time Streaming Protocol) は、リアルタイムのプロ

パティを持つデータの提供を制御するための、アプリケーションレベルのプロトコルです。このオプションは、既定では選択されています。

6 「**適用**」を選択します。

ソース ルーティング パケット

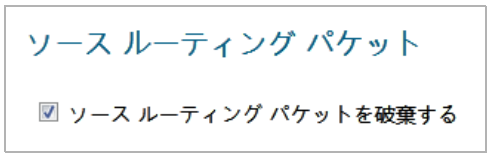
IP ソース ルーティングは、パケットの送信元が、送信先に到達するまでにパケットが使用するべきルータの一部またはすべてを指定できる、IP の標準オプションです。

この IP オプションは、通常は使用が禁止されています。A から B までルータ C を介してパケットを送信するというオプションを挿入することによって、傍受者がパケットを受信するために使用するおそれがあるためです。ルーティング テーブルは、パケットが経由するパスを制御し、送信元や下流のルータによってオーバーライドされないようにする必要があります。

ソース ルーティング パケットを設定するには:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 詳細設定**」に移動します。

2 「**ソース ルーティング パケット**」までスクロールします。



3 「**ソース ルーティング パケットを破棄する**」オプションが選択されていることを確認します。このオプションは、既定では選択されています。

> **ヒント**：2 台の指定ホスト間のトラフィックのテストを行い、かつソース ルーティングを使用する場合は、このオプションの選択を解除します。

4 「**適用**」を選択します。

内部 VLAN

「内部 VLAN」セクションで、開始 VLAN ID を指定できます。

内部 VLAN ID を変更するには:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 詳細設定**」に移動します。

2 「**内部 VLAN**」セクションまでスクロールします。

3 「**開始 VLAN ID**」フィールドに VLAN ID を入力します。既定の ID は **2** です。

4 「**適用**」を選択します。

接続数

重要：「**接続数**」設定を変更した場合は、変更を実施するために SonicWall セキュリティ装置を再起動する必要があります。

「**接続数**」セクションでは、ファイアウォールを調整して、最適なスループットを優先するのか、精密パケット検査 (DPI) サービスの検査対象となる同時接続数を増やすことを優先するのかを指定できます。接続数 テーブルを参照してください。

ヒント：ハードウェア プラットフォームが違えば使用可能なメモリの量も異なり、それに応じて接続数も変化します。最大 DPI-SSL 接続数については、装置モデル別の接続 (252 ページ) を参照してください。

接続数

プラットフォーム	SPI 接続数	DPI	
		最大接続数	パフォーマンスを最適化
NS*a* 9650	12,500,000	5,000,000	4,750,000
NS*a* 9450	10,000,000	4000000	3,750,000
NS*a* 9250	7,500,000	3000000	2,750,000
NS*a* 6650	5,000,000	2,000,000	1,750,000
NS*a* 5650	4000000	1,500,000	1,250,000
NS*a* 4650	3000000	1,000,000	750,000
NS*a* 3650	2,000,000	750,000	500,000
NS*a* 2650	1,000,000	500,000	500,000
SuperMassive 9600	10,000,000	2,000,000	1,750,000
SuperMassive 9400	7,500,000	1,500,000	1,250,000
SuperMassive 9200	5,000,000	1,500,000	1,250,000
NSA 6600	2,000,000	1,000,000	750,000
NSA 5600	2,000,000	1,000,000	750,000
NSA 4600	1,000,000	500,000	375,000
NSA 3600	750,000	375,000	250,000
NSA 2600	500,000	250,000	125,000
TZ600/TZ600P	150,000	125,000	125,000
TZ500/TZ500 W	125,000	100,000	100,000
TZ400/TZ400 W	100,000	90,000	90,000
TZ300/TZ300P/TZ300 W	50,000	50,000	50,000
SOHO W	10,000	10,000	10,000

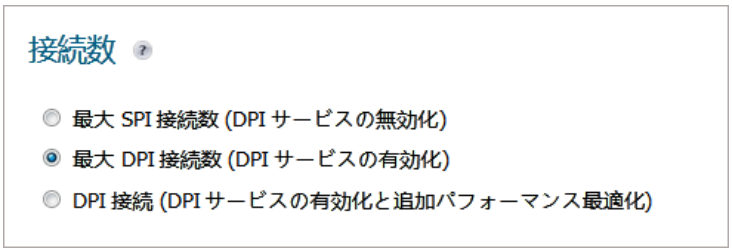
最大接続数は SonicWall セキュリティ装置の特定モデルの物理的な能力によって異なります (接続数 テーブルを参照)。NS*a* シリーズ、NSA シリーズ、および SuperMassive シリーズのファイアウォールでは、フロー報告のために接続数が減ることはありません。

「**接続数**」見出しの横にある「**情報**」アイコンをマウスでポイントすると、特定の SonicWall セキュリティ装置におけるさまざまな設定の組み合わせに対する接続の最大数を示すポップアップ テーブルが表示されます。このポップアップ テーブルには、現在の設定のテーブル エントリが示されます。

接続サービスを設定するには:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 詳細設定**」に移動します。

2 「**ソース ルーティング パケット**」までスクロールします。



3 ファイアウォールの接続数を表示するには、「**情報**」アイコンを選択します。

4 有効/無効にするサービスの種別を選択します。DPI 接続設定によって提供されるセキュリティ保護のレベルに変化はありません。

- **最大 SPI 接続数 (DPI サービスの無効化)** - このオプション (ステートフル パケット検査) は、SonicWall DPI セキュリティ サービス保護を提供せずに、ステートフル パケット検査のみを有効にして接続数が最大になるようにファイアウォールを最適化します。このオプションは、ステートフル パケット検査**のみ**を必要とするネットワークで使用してください。SonicWall ネットワーク セキュリティ装置を配備する場合は通常お勧めしません。
- **最大 DPI 接続数 (DPI サービスの有効化)** - これは、ほとんどのSonicWall ネットワーク セキュリティ装置の配備で推奨される設定です。このオプションは、既定では選択されています。
- **DPI 接続 (DPI サービスの有効化と追加パフォーマンス最適化)** - このオプションは、パフォーマンスがクリティカルな配備を意図しています。このオプションはファイアウォールの DPI 検査のスループットを増大する代わりに、最大 DPI 接続数を妥協します。

メモ：上記のどちらかの DPI 接続オプションを選択した場合、DPI 接続数が 250,000 より大きいとき、ファイアウォールに DPI 接続および DPI-SSL 接続数を動的に調整させることができます。詳細については、動的接続サイジング (16 ページ) を参照してください。

動的接続サイジング

メモ：動的接続サイジングは、NS*a* シリーズ、NSA 3600 (およびそれ以降)、および SuperMassive シリーズのネットワーク セキュリティ装置でサポートされています。

ヒント：プラットフォームごとの DPI-SSL 接続の最大数については、装置モデル別の接続 (252 ページ) を参照してください。

「**接続数**」で「**最大 DPI 接続数 (DPI サービスの有効化)**」または「**DPI 接続 (DPI サービスの有効化と追加パフォーマンス最適化)**」を選択した場合、DPI 接続数が 250,000 より大きいとき「**動的接続サイジング**」セクションが表示されます。このオプションの設定により、ファイアウォールは DPI 接続数を 1,250,000 刻みで動的に減らして DPI-SSL 接続数を 750 刻みで増やすことができます。

動的接続サイジングを設定するには:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 詳細設定**」に移動します。

2 「**動的接続サイジング**」までスクロールします。

3 次のいずれかを行います。

ヒント：1 つのオプションで接続数を変更すると、他のオプションの値も自動的に変更されます。

- 「**DPI 接続**」から DPI 接続の最大数 (125,000 刻み) を選択します。
- 「**DPI-SSL 接続**」から DPI-SSL 接続の最大数 (750 刻み) を選択します。

例えば、「**DPI 接続**」で選択した DPI 接続数が **1250000** の場合、「**DPI-SSL 接続**」の DPI-SSL 接続数は **165000** です。「**DPI 接続数**」から **1000000** を選択すると、DPI-SSL 接続数は **18000** に変化します。「**DPI-SSL 接続**」から **12000** を選択すると、DPI 接続数は **2000000** に変化します。

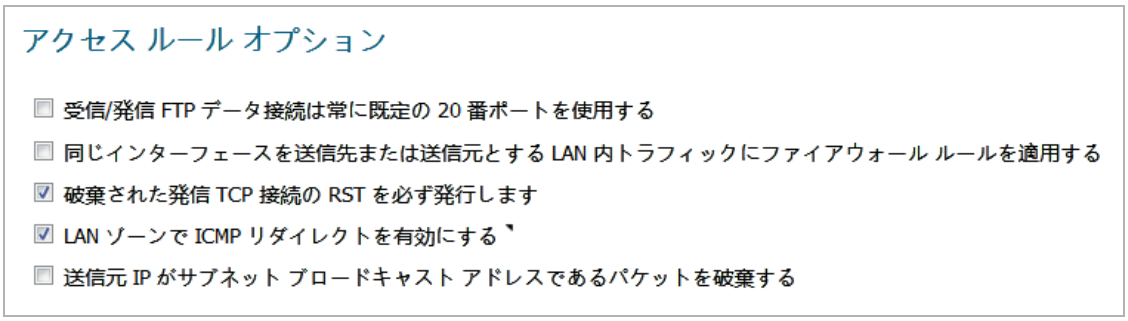
4 「**適用**」を選択します。

アクセス ルール サービス オプション

アクセス ルール オプションを設定するには:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 詳細設定**」に移動します。

2 「**アクセス ルール オプション**」までスクロールします。



3 既定の設定では、20 番ポートからの FTP 接続が許可されますが、発信トラフィックは 1024 などのポートに再割り付けされます。セキュリティ装置経由の FTP データ接続を強制するにはポート 20 で接続する必要があり、そうでなければ接続は破棄されます。「**受信/発信 FTP データ接続は常に既定の 20 番ポートを使用する**」を選択します。このオプションが選択されている場合、このイベントは、セキュリティ装置でログ イベントとして記録されます。 このオプションは、既定では選択されていません。

4 LAN インターフェースで受信した、その LAN インターフェース宛てのファイアウォール ルールを適用するには、「**同じインターフェースを送信先または送信元とする LAN 内トラフィックにファイアウォール ルールを適用する**」を選択します。通常、これはセカンダリの LAN サブネットが設定されている場合にのみ必要です。 このオプションは、既定では選択されていません。

5 破棄された発信 TCP 接続に対して、接続を削除するために RST (リセット) パケットを送信するには、「**破棄された発信 TCP 接続の RST を必ず発行します**」を選択します。 このオプションは、既定では選択されています。

6 LAN ゾーン インターフェースで、ICMP パケットをリダイレクトするには、「**LAN ゾーンで ICMP リダイレクトを有効にする**」を選択します。このオプションは、既定では選択されています。

7 検出された IP アドレスがサブネットによるアドレスとして認識されたときパケットを破棄するには、「**送信元 IP がサブネット ブロードキャスト アドレスであるパケットを破棄する**」を選択します。 このオプションは、既定では選択されていません。

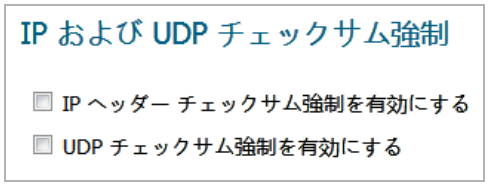
8 「**適用**」を選択します。

IP および UDP チェックサム強制

IP および UDP チェックサム強制を設定するには:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 詳細設定**」に移動します。

2 「**IP および UDP チェックサム強制**」までスクロールします。



3 IP ヘッダー チェックサムを強制して IP ヘッダーのチェックサムが正しくないパケットを破棄するには、「**IP ヘッダー チェックサム強制を有効にする**」を選択します。 このオプションは、既定では選択されていません。

4 UDP ヘッダー チェックサムを強制して UDP ヘッダーのチェックサムが正しくないパケットを破棄するには、「**UDP チェックサム強制を有効にする**」を選択します。 このオプションは、既定では選択されていません。

5 「**適用**」を選択します。

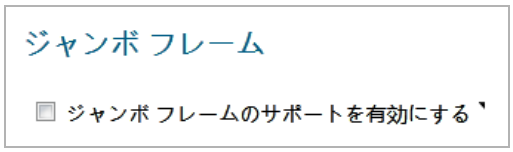
ジャンボ フレーム

メモ：ジャンボ フレームは、NSA 3600 以降の装置でサポートされています。

ジャンボ フレーム サポートを設定するには:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 詳細設定**」に移動します。

2 「**ジャンボ フレーム**」までスクロールします。



3 ジャンボ フレームのサポートを有効にするには、「**ジャンボ フレームのサポートを有効にする**」を選択します。 このオプションは、既定では選択されていません。

このオプションを有効にすると、スループットが向上し、処理するイーサネット フレームの数が減少します。スループットの向上が見られない場合もありますが、パケットのサイズが非常に大きい場合は一定の効果があります。

メモ：ジャンボ フレーム パケットはサイズが 9000 キロバイトで、メモリ要件は 4 倍に増加します。ジャンボ フレームのサポートを有効にした後に、*SonicWall SonicOS 6.5 システム セットアップ*に記載されているようにインターフェース MTU を 9000 バイトに変更する必要があります。

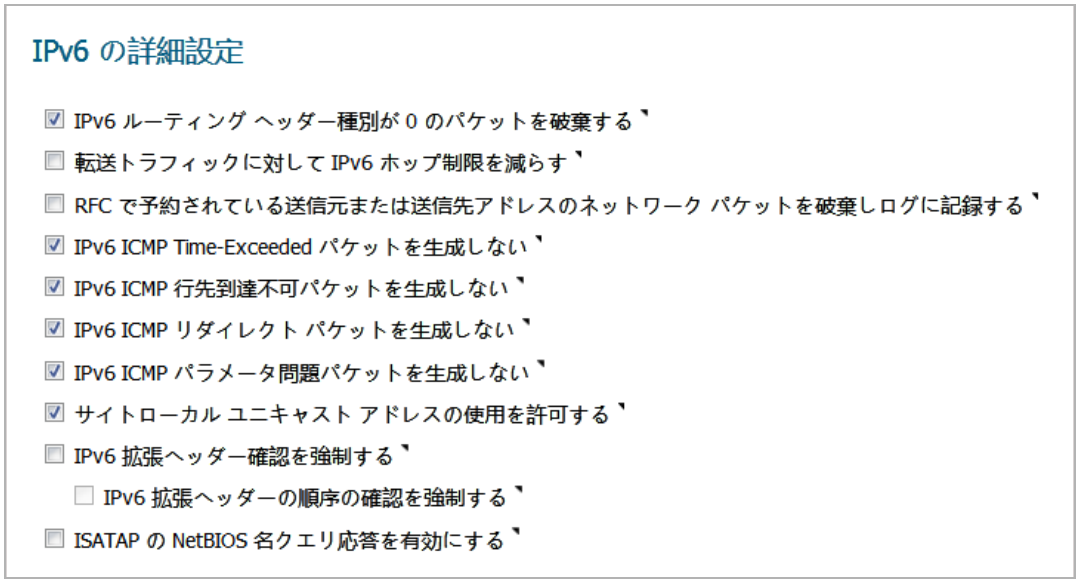
4 「**適用**」を選択します。

IPv6 の詳細設定

IPv6 の詳細設定を行うには:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 詳細設定**」に移動します。

2 「**IPv6 の詳細設定**」までスクロールします。



3 ファイアウォールで IPv6 を完全に無効にするには、「**このファイアウォールですべての IPv6 トラフィック処理を無効にする**」を選択します。有効にすると、このオプションはこのセクションの他の IPv6 オプションよりも優先されます。 このオプションは、既定では選択されていません。

4 IPv6 ルーティング ヘッダー種別が 0 (RH0) のパケットを悪用する潜在的な DoS 攻撃を防ぐには、「**IPv6 ルーティング ヘッダー種別が 0 のパケットを破棄する**」を選択します。この設定が有効になっている場合、RH0 パケットは、送信先が SonicWall セキュリティ装置で、残セグメント (Segments Left) の値が 0 の場合を除き、破棄されます。残セグメントは、最終的な送信先に到達するまでの残りルート セグメントの数を表します。このオプションは、既定では選択されています。詳細については、http://tools.ietf.org/html/rfc5095 を参照してください。

5 ホップ制限が 0 までデクリメントされたときにパケットを破棄するには、「**転送トラフィックに対して IPv6 ホップ制限を減らす**」を選択します。これは IPv4 TTL に似ていますこのオプションは、既定では選択されていません。

6 IPv6 に対する RFC 4921 において、将来の定義と使用のための予約アドレスとして定義されているネットワーク パケットの送信元または送信先アドレスを持つネットワーク パケットを破棄し、ログに記録するには、「**RFC で予約されている送信元または送信先アドレスのネットワーク パケットを破棄しログに記録する**」を選択します。 このオプションは、既定では選択されていません。

7 既定では、SonicWall 装置は IPv6 ICMP Time-Exceeded パケットを生成して、ホップ制限が 0 まで減少したためにパケットが装置によって破棄されたことを報告します。SonicWall 装置がこれらのパケットを生成しないようにこの機能を無効にするには、「**IPv6 ICMP Time-Exceeded パケットを生成しない**」を選択します。このオプションは、既定では選択されています。

8 既定では、SonicWall 装置は IPv6 ICMP 行先到達不可パケットを生成します。この機能を無効にして SonicWall 装置がこれらのパケットを生成しないようにするには、「**IPv6 ICMP 行先到達不可パケットを生成しない**」を選択します。 このオプションは、既定では選択されています。

9 既定では、SonicWall 装置はリダイレクト パケットを生成します。この機能を無効にして SonicWall 装置がリダイレクト パケットを生成しないようにするには、「**IPv6 ICMP リダイレクト パケットを生成しない**」を選択します。 このオプションは、既定では選択されています。

10 既定では、SonicWall 装置は IPv6 ICMP パラメータ問題パケットを生成します。この機能を無効にして SonicWall 装置がこれらのパケットを生成しないようにするには、「**IPv6 ICMP パラメータ問題パケットを生成しない**」を選択します。 このオプションは、既定では選択されています。

11 既定の SonicWall 装置の動作であるサイトローカル ユニキャスト (SLU) アドレスを許可するには、「**サイトローカル ユニキャスト アドレスの使用を許可する**」を選択します。 このオプションは、既定では選択されています。

現在の定義では、SLU アドレスにあいまいさがあり、複数のサイトを表している可能性があります。SLU アドレスを使用すると、漏洩、あいまいさ、および誤ったルートでの送信により、ネットワーク セキュリティに悪影響を与えることがあります。この問題を回避するには、このオプションの選択を解除して、装置による SLU アドレスの使用を防止します。

12 SonicWall 装置で IPv6 拡張ヘッダーの有効性をチェックするには、「**IPv6 拡張ヘッダー確認を強制する**」を選択します。 このオプションは、既定では選択されています。

このオプションを選択すると、「**IPv6 拡張ヘッダーの順序の確認を強制する**」オプションが使用可能になります。(ページの再表示が必要な場合があります)。

- SonicWall 装置による IPv6 拡張ヘッダーの順序の確認を行う場合は、「**IPv6 拡張ヘッダーの順序の確認を強制する**」を選択します。このオプションは、既定では選択されていません。

13 SonicWall 装置にブロードキャスト ISATAP クエリに対する応答として NetBIOS 名の生成を行わせる場合は、「**ISATAP の NetBIOS 名クエリ応答を有効にする**」を選択します。このオプションは、既定では選択されていません。

> **重要**：このオプションは、1 つの ISATAP トンネル インターフェースが設定されている場合にのみ選択してください。

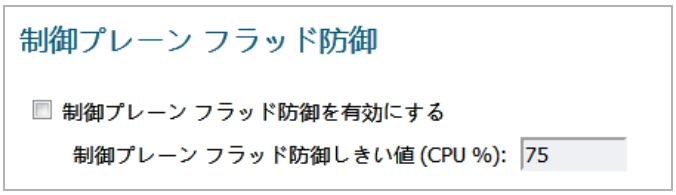
14 「**適用**」を選択します。

制御プレーン フラッド防御

制御プレーン フラッド防御を設定するには:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 詳細設定**」に移動します。

2 「**制御プレーン フラッド防御**」までスクロールします。



3 制御プレーン上のトラフィックが所定のしきい値を超えた場合、ファイアウォール宛ての制御トラフィックに限ってシステムの制御プレーン コア (コア 0) への転送をファイアウォールに行わせるには、「**制御プレーン フラッド防御を有効にする**」を選択し、新しいオプションである「**制御プレーンフラッド防御しきい値 (CPU %)**」でそのしきい値を指定します。このオプションは既定では無効になっています。

正当な制御トラフィックを優先するために、超過分のデータ トラフィックは破棄されます。この制限は、過剰なトラフィックが制御プレーン コアに到達するのを防止します。こうした状況は、システムの応答性の低下や、ネットワーク接続の切断の原因となる場合があります。制御トラフィックに対して設定された割合は保証されます。

- 「**制御プレーンフラッド防御しきい値 (CPU %)**」にフラッド防御しきい値を割合 (%) で入力します。最小値は 5 (%)、最大値は 95、既定値は **75** です。

4 「**適用**」を選択します。

2

帯域幅管理の設定

- 帯域幅管理とは (21 ページ)
- ファイアウォール設定 > 帯域幅管理 (24 ページ)
- グローバル帯域幅管理の設定 (27 ページ)
- 詳細帯域幅管理 (35 ページ)
- 詳細帯域幅管理の設定 (39 ページ)

帯域幅管理とは

帯域幅管理 (BWM) は、ネットワーク上の重要なアプリケーションに帯域幅のリソースを割り当てる手法です。

SonicOS は、発信 (送信) および着信 (受信) 帯域幅管理インターフェースを通して統合されたトラフィック調節機構を提供します。送信帯域幅管理は、信頼済みゾーンまたはパブリック ゾーンから発して非保護ゾーンまたは暗号化ゾーンに向かうトラフィックに適用できます。受信帯域幅管理は、非保護ゾーンまたは暗号化ゾーンから発して信頼済みゾーンまたはパブリック ゾーンに向かうトラフィックに適用できます。

SonicWallセキュリティ装置 は、帯域幅管理を使用して受信トラフィックと送信トラフィックを管理します。帯域幅管理により、ネットワーク管理者は管理インターフェースの「**管理 |ポリシー> ルール > アクセス ルール**」ページで作成したアクセス ルールに基づいて、最小帯域幅の保証やトラフィックの優先順位の設定を行うことができます。アプリケーションやユーザの帯域幅の量を制御することにより、利用可能な帯域幅すべてを少数のアプリケーションやユーザが消費することを防げます。異なるネットワーク トラフィックに割り当てられた帯域幅のバランスをとり、そしてトラフィックに優先順位を付けることで、ネットワークのパフォーマンスを向上できます。

メモ：帯域幅管理はサービス品質 (QoS) システムに完全に統合されますが、1 台の SonicWall 装置で等級分けと調節を実行する点で、事実上外部システムへの依存性を除去し、したがってマーキングの必要性を除去し、単一のアクセス ルール上で同時に**帯域幅管理**と **QoS** (レイヤ 2 および/または レイヤ 3 マーキング) を設定できます。これにより、外部システムでは、既にトラフィックのシェイピングを行った後でさえ、ファイアウォールで実行された分類のメリットが得られます。帯域幅管理の QoS の詳細については、サービス品質の管理 (78 ページ) を参照してください。

帯域幅管理の優先順位キュー テーブルに SonicOS の優先順位キューを示します。

帯域幅管理の優先順位キュー

0 - リアルタイム	3 - 中高	6 - 低
1 - 最高	4 - 中	7 - 最低
2 - 高	5 - 中低	

「**管理 | セキュリティ設定 > ファイアウォール設定 > 帯域幅管理**」ページでは、各種の帯域幅管理が選択できます。

帯域幅管理種別

帯域幅管理種別	説明
詳細	詳細帯域幅管理を有効にします。送信および受信帯域幅の最大制限値は、帯域幅オブジェクト、アクセス ルール、およびアプリケーション ポリシーを設定してそれらをインターフェースに付与することで、任意のインターフェースに対してインターフェース単位で設定できます。
グローバル	すべてのゾーンでサービスに対する保証帯域幅および最大帯域幅の割り当てと、トラフィックの優先順位付けが可能です。インターフェースでグローバル帯域幅管理が有効になっている場合、そのインターフェースで送受信されるすべてのトラフィックに対し、優先順位キューに応じた帯域幅管理が行われます。 以下は既定のグローバル帯域幅管理キューです。 **2** - 高 **4** - 中 **6** - 低 帯域幅管理が有効なアクセス ルールまたはアプリケーション制御ポリシーによって管理されないすべてのトラフィックに対する既定の優先順位は「**4 中**」です。キューイングのため、トラフィックが 1 Gbps を超える場合は最大帯域幅が 1 Gbps に制限され、処理するパケット数が制限されます。
なし	(既定) 帯域幅管理は無効です。

帯域幅管理種別が「**なし**」で、インターフェースを使用しているトラフィック種別が 3 つあり、インターフェースのリンク容量が 100 Mbps の場合、3 つのトラフィック種別すべての累積容量は 100 Mbps になります。

グローバル帯域幅管理がインターフェースで有効になっている場合、そのインターフェースで送受信されるすべてのトラフィックに対して帯域幅管理が行われます。使用可能な受信および送信トラフィックが 10 Mbps に設定されている場合、既定では 3 つのトラフィック種別すべてが中優先順位のキューに送信されます。中優先順位のキューは、既定では 50% の保証帯域幅と 100% の最大帯域幅を持ちます。**グローバル**帯域幅管理ポリシーが設定されていない場合、各トラフィック種別の累積リンク容量は 10 Mbps になります。

メモ：帯域幅管理ルールはそれぞれがパケット キューイングのためにメモリを消費するので、SonicOS 上でキューに入れることができるパケットおよびルールの数はプラットフォームによって制限されています (これらの値は変更されることがあります)。

「**グローバル**」では、他のキューの未使用の保証された帯域幅を使用して最大帯域幅を確保します。既定または単一のキューのトラフィックのみがあり、保証された帯域幅としてすべてのキューの合計 100% が割り当てられている場合、「**グローバル**」では他のキューの未使用のグローバル帯域幅が使用され、これによって、既定/単一キューに最大の帯域幅が確保されます。

用語集

帯域幅管理 (BWM)
トラフィックのシェイピングやポリシングを行うために使用されるさまざまなアルゴリズムや手法です。シェイピングは、送信トラフィックを管理することを表します。 ポリシングとは、受信トラフィックを管理することを表します (受付制御とも呼ばれます)。帯域幅管理には、さまざまなキューイングおよび破棄手法を含め、それぞれ独自の設計上の長所を持つ多くの異なる方式があります。SonicWall では、特定のタイプの受信トラフィックに対する破棄手法に加え、受信および送信 BWM 用にトークンベース、等級ベースのキューイング方式を採用しています。

保証帯域幅
ある等級のトラフィックに常に与えられる、インターフェース上で利用可能な合計帯域幅に対して宣言された割合です。受信 BWM と送信 BWM の両方に適用されます。すべての BWM ルールにおける保証された帯域幅の合計は、利用可能な帯域幅の合計の 100%を超過することはできません。SonicOS 5.0 以降では、帯域幅管理機能が拡張され、速度制限機能を使用できます。第 2 層、3 層、または 4 層ネットワーク トラフィックの最大速度を指定するトラフィック ポリシーを作成できます。「保証された帯域幅」は 0%に設定することもできます。

受信帯域幅管理
特定のインターフェースに入るトラフィックの速度のシェイピングを行う機能です。TCP トラフィックの場合、実際のシェイピングが行われるのは、TCP のウィンドウ調整メカニズムによって受信フローの速度が調整される場合です。UDP トラフィックの場合、UDP にはネイティブなフィードバック制御がないので、破棄手法が使用されます。

最大帯域幅
ある等級のトラフィックに許可される最大帯域幅を定義する、インターフェース上で利用可能な合計帯域幅に対して宣言された割合です。受信 BWM と送信 BWM の両方に適用されます。帯域幅の速度制限を指定する調整メカニズムとして使用されます。帯域幅管理機能が拡張され、速度制限機能が使用できます。第 2 層、3 層、または 4 層ネットワーク トラフィックの最大速度を指定するトラフィック ポリシーを作成できます。これにより、プライマリ WAN リンクから、あまり多数のトラフィックを処理できないバックアップ接続へのフェイルオーバーが生じた場合でも、帯域幅管理が行えます。「最大帯域幅」は 0% にも設定でき、この場合はあらゆるトラフィックの送受信ができなくなります。

送信帯域幅管理
インターフェースからトラフィックを送出する速度を制限することです。送信BWM では、8 つの優先順位キューを持つクレジット (またはトークン) ベースのキューイング システムを使用して、アクセス ルールによって分類される異なるタイプのトラフィックを処理します。

優先順位
トラフィックの分類で使用される追加要素です。SonicOS では、帯域幅管理に使用するキュー構造に 8 つの優先順位 (0=最高、7=最低) が使用されます。キューは、優先順位の順序で処理されます。

キューイング
リンク上の利用可能な帯域幅を効果的に使用できるようにします。キューは一般的に、トラフィックを分類した後に、並べ替えのため、および個別に管理するために使われます。

ファイアウォール設定 > 帯域幅管理

トピック:

- グローバル帯域幅管理の設定 (24 ページ)
- 動作オブジェクト (26 ページ)

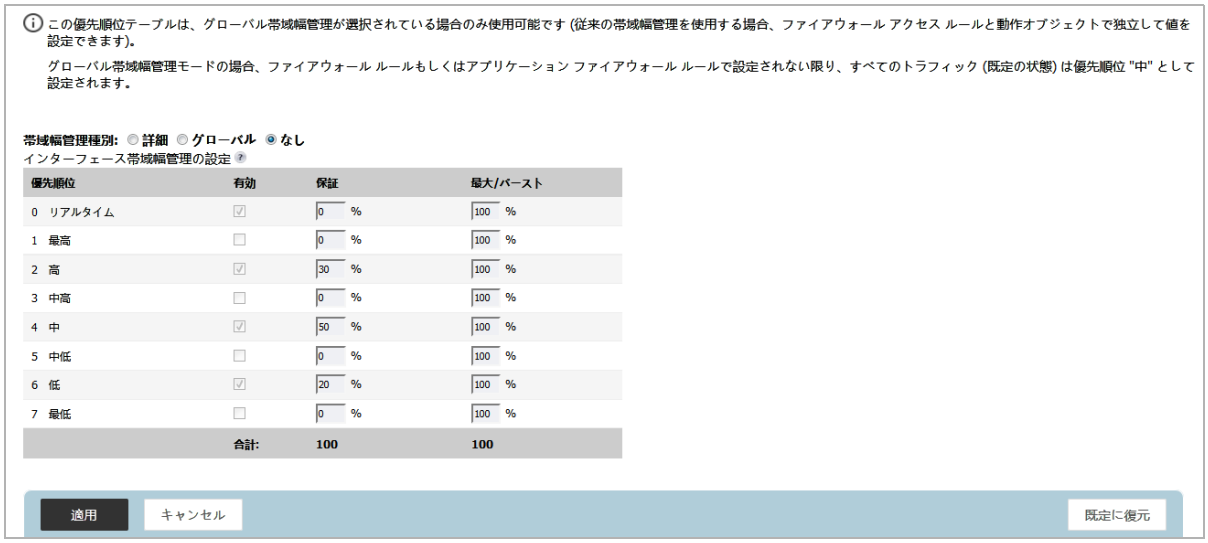
グローバル帯域幅管理の設定

帯域幅管理を実際に働かせるには、最初に「**管理 | セキュリティ設定 > ファイアウォール設定 > 帯域幅管理**」ページで帯域幅管理を有効化してインターフェース/ファイアウォール/アプリケーションルールの帯域幅管理を有効にし、その後、インターフェースの受信および送信トラフィックに対して利用可能な帯域幅を割り当てます。さらに、ネットワーク トラフィックの各クラスに対して個別の制限を設定します。ネットワーク トラフィックに優先順位を割り当てることで、Telnet のような応答性重視のアプリケーションを、FTP のような応答時間があまり重要でないトラフィックよりも優先させることができます。

帯域幅管理の設定を見るには、「**管理 | セキュリティ設定 > ファイアウォール設定 > 帯域幅管理**」ページに移動します。

メモ：このページの既定の設定は、事前定義された保証帯域と最大帯域と 3 つの優先順位で構成されています。中という優先順位は、この優先順位キューが帯域幅管理が有効なポリシーによって管理されていないすべてのトラフィックに対して既定で使われるので、最高の保証値を持ちます。

メモ：帯域幅管理が使いやすいように、SonicWall によって既定値が設定されています。具体的な帯域幅のニーズを調査して、状況に応じてこのページに値を入力することを推奨します。



- **帯域幅管理種別**オプション

  重要：「**帯域幅管理種別**」を変更した場合の影響を以下に示します。

  - 「**グローバル**」から「**詳細**」に変更すると、アプリケーション ルール ポリシーで使用されている既定の帯域幅管理動作が自動的に「**詳細帯域幅管理**」の設定に変換されます。
  - 「**詳細**」から「**グローバル**」に変更すると、既定の帯域幅管理動作が「**帯域幅管理グローバル - 中**」に変換されます。

  この**種別**を変更したり元に戻したりしても、ファイアウォールでは以前の動作優先順位レベルが保存されません。変換の内容は、「**管理 |ポリシー > ルール > アプリケーション制御**」ページで確認できます。

  - **詳細** - 任意のゾーンで保証帯域幅および最大帯域幅の割り当てと、インターフェースごとに割り当てられたトラフィックの優先順位付けが可能です。
  - **グローバル** - すべてのゾーンでサービスに対する保証帯域幅および最大帯域幅の割り当てと、トラフィックの優先順位付けが可能です。トラフィックが 1 Gbps を超える場合は最大帯域幅が 1 Gbps に制限されます。
  - **なし** - 帯域幅管理を無効にします。このオプションは既定の設定です。

- **インターフェース帯域幅管理の設定** - **疑問符**アイコンをマウスでポイントすると、各種インターフェースの受信および送信で帯域幅管理設定が無効になっているか有効になっているかを示すテーブルが表示されます。

- **グローバル優先順位** 帯域幅テーブル - 優先順位に関する以下の情報を表示します。

  メモ：このテーブルは、「**グローバル**」帯域幅管理が選択されている場合にのみ使用されます。「**詳細**」または「**なし**」が選択されていると、テーブルはグレー表示になります。

  - **優先順位** - 優先順位の番号と名前を表示します (**0 リアルタイム ～ 7 最低**)。
  - **有効** - 優先順位がオンになっている場合、該当する優先順位の優先順位キューが有効になります。
  - **保証** - 有効となっている優先順位について、保証される比率 (パーセント) を有効にします。インターフェースに設定された帯域幅は、最終的な値の計算に使われます。

    この速度を反映するには、対応する「**有効**」チェックボックスがオンになっている必要があります。既定では、次の優先順位と保証率のみが有効です。

- **2 高** 30%
- **4 中** 50%
- **6 低** 20%

ヒント： 優先順位「**4 中**」を無効にすることはできませんが、比率を変更することはできます。

保証帯域幅の比率の合計が 100% を超えてはなりません。帯域幅が 100% を超えると、**合計**の値が赤色で表示されます。また、保証帯域幅が、キューごとの最大帯域幅を超えてはなりません。

- **最大/バースト** - 有効となっている優先順位について、最大/バースト比率 (パーセント) を有効にします。この速度を反映するには、対応する「**有効**」チェックボックスがオンになっている必要があります。

動作オブジェクト

動作オブジェクトは、一致イベントに対するアプリケーション ルール ポリシーの動作を定義します。動作をカスタマイズするか、あらかじめ定義されている既定の動作のうちの 1 つを選択できます。あらかじめ定義されている動作は、アプリケーション ルール ページでポリシーを追加または編集する際にアプリケーション制御ポリシー設定ページに表示されます。

個別帯域幅管理動作は既定の帯域幅管理動作と異なる振舞いをします。個別帯域幅管理動作は、「**管理 |ポリシー > オブジェクト > 動作オブジェクト**」ページで新しい動作オブジェクトを追加して、帯域幅管理動作種別を選択することによって設定されます。個別帯域幅管理動作とそれらを使用するポリシーでは、帯域幅管理種別が「**グローバル**」から「**詳細**」に、または「**詳細**」から「**グローバル**」に変更されても優先順位レベルの設定が保持されます。

多くの帯域幅管理動作オプションも、あらかじめ定義された既定の動作リストで利用可能です。この帯域幅管理動作オプションは、「**ファイアウォール設定 > 帯域幅管理**」ページの「帯域幅管理種別」の設定によって異なります。**帯域幅管理種別**の設定の違いによる影響を以下に示します。

- 「**グローバル**」に設定されている場合は、帯域幅管理の 8 つの優先順位すべてが利用可能です。
- 「**詳細**」に設定されている場合、優先順位は設定されません。優先順位の設定は、「**管理 |ポリシー > オブジェクト > 帯域幅オブジェクト**」で帯域幅オブジェクトを設定することで行います。

ポリシーの追加: 既定の動作 テーブルに、ポリシー追加時に利用可能な事前定義済みの既定の動作のリストを示します。

ポリシーの追加: 既定の動作

帯域幅管理種別	
グローバル	**詳細**
帯域幅管理グローバル-リアルタイム	高度な帯域幅管理 - 高
帯域幅管理グローバル-最高	高度な帯域幅管理 - 中
帯域幅管理グローバル-高	高度な帯域幅管理 - 低
帯域幅管理グローバル-中高	
帯域幅管理グローバル-中	
帯域幅管理グローバル-中低	
帯域幅管理グローバル-低	
帯域幅管理グローバル-最低	

グローバル帯域幅管理の設定

重要：帯域幅管理は、「**管理 | セキュリティ設定 > ファイアウォール設定 > 帯域幅管理**」で最初に有効にする必要があります。

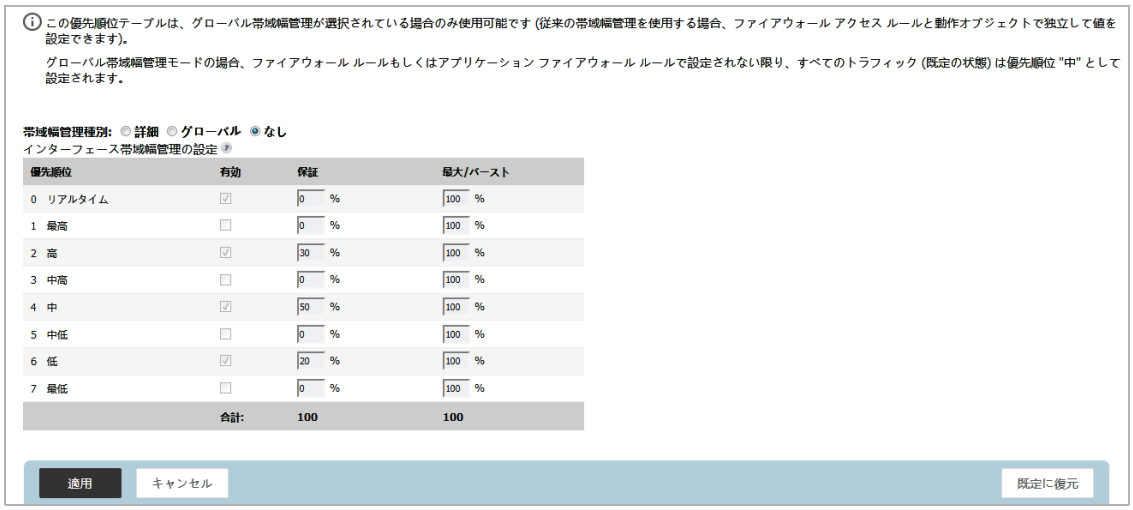
グローバル帯域幅管理は以下の方法を使って設定できます。

- グローバル帯域幅管理の設定 (27 ページ)
- インターフェースに対するグローバル帯域幅管理の設定 (28 ページ)
- アクセス ルールでのグローバル帯域幅管理の設定 (29 ページ)
- 動作オブジェクトでのグローバル帯域幅管理の設定 (30 ページ)
- アプリケーション ルールの設定 (31 ページ)
- AppFlow 監視の設定 (32 ページ)

グローバル帯域幅管理の設定

帯域幅管理種別を「グローバル」に設定するには:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 帯域幅管理**」に移動します。



2 「**帯域幅管理種別**」オプションを「**グローバル**」に設定します。

3 「**有効**」列にある適切なチェックボックスを選択して、適切な優先順位を有効にします。

メモ：アクセス ルール、アプリケーション ルール、および動作オブジェクトでこうした優先順位を設定できるようにするには、このページで該当する優先順位を有効にする必要があります。

4 選択した各優先順位に対して適切な保証帯域幅の割合を入力します。割合の合計は 100% を超えることができません。

5 選択した各優先順位に対して**最大/バースト**帯域幅の割合を入力します。

6 「**適用**」を選択します。

インターフェースに対するグローバル帯域幅管理の設定

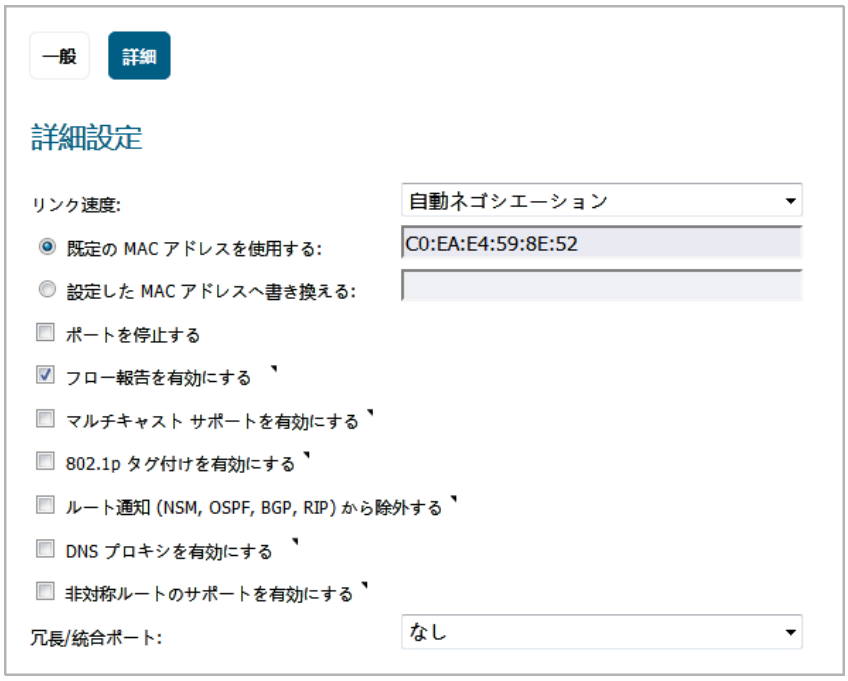
重要：グローバル帯域幅管理は、グローバル帯域幅管理の設定 (27 ページ) の説明に従って、「**ファイアウォール設定 > 帯域幅管理**」で最初に有効にする必要があります。

帯域幅管理をインターフェースに対して設定するには、以下の手順に従います。

1 「**管理 | システム セットアップ > ネットワーク > インターフェース**」に移動します。

2 目的のインターフェースの「**編集**」ボタンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

3 「**詳細設定**」を選択します。



メモ：表示されるオプションは、インターフェースの設定状況によって異なることがあります。

4 「**帯域幅管理**」までスクロールします。

5 「**送信帯域幅管理を有効にする**」および「**受信帯域幅管理を有効にする**」のどちらかまたは両方をオンにします。これらのオプションは、既定ではオフになっています。

これらのどちらかまたは両方のオプションがオンの場合、対応するアクセス ルールまたはアプリケーション ルールが存在しなければ、そのインターフェースでの送信/受信トラフィックの合計は、「**利用可能なインターフェース送信/受信帯域幅 (kbps)**」フィールドで指定されている量までに制限されます。

両方のオプションがオフの場合、帯域幅の制限はインターフェース レベルでは設定されませんが、送信トラフィックはその他のオプションを使用して調整できます。

6 「**利用可能なインターフェース送信/受信帯域幅 (Kbps)**」フィールドに、すべての送信/受信トラフィックで利用可能な合計帯域幅を Kbps 単位で入力します。既定値は **384.000000** Kbps です。

7 「**OK**」を選択します。

アクセス ルールでのグローバル帯域幅管理の設定

重要：**グローバル**帯域幅管理は、グローバル帯域幅管理の設定 (27 ページ) の説明に従って、「**ファイアウォール設定 > 帯域幅管理**」で最初に有効にする必要があります。

それぞれのアクセス ルールで帯域幅管理を設定できます。この方法は、帯域幅管理を適用する方向を設定して、優先順位キューを設定します。

重要：アクセス ルールで優先順位を設定する前に、まず「**ファイアウォール設定 > 帯域幅管理**」ページで、使用する優先順位を有効にする必要があります。このページを参照して、有効になっている優先順位を確認してください。「**ファイアウォール設定 > 帯域幅管理**」ページで有効になっていない帯域幅優先順位を選択した場合、トラフィックは自動的に優先順位 **4 (中)** に割り付けられます。グローバル帯域幅管理の設定 (27 ページ) を参照してください。

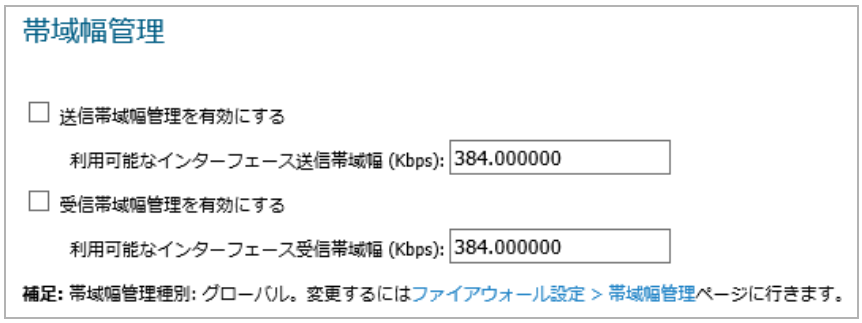
優先順位は「**アクセス ルール**」ダイアログの「**帯域幅優先順位**」テーブルに表示されます。帯域幅管理の優先順位キュー テーブルを参照してください。

アクセス ルールでグローバル帯域幅管理を設定するには、以下の手順に従います。

1 「**管理 |ポリシー > ルール > アクセス ルール**」ページに移動します。

2 編集するルールの**編集**アイコンを選択します。「**ルールの編集**」ダイアログが表示されます。

3 「**BWM**」をクリックします。



4 「**送信帯域幅管理を有効にする**」および「**受信帯域幅管理を有効にする**」のどちらかまたは両方をオンにします。これらのオプションは、既定ではオフになっています。

   a 適切な「**利用可能なインターフェース送信/受信帯域幅 (Kbps)**」フィールドに、すべての送信/受信トラフィックで利用可能な総帯域幅を Kbps 単位で入力します。既定値は **384.000000** Kbps です。

5 「**OK**」を選択します。

動作オブジェクトでのグローバル帯域幅管理の設定

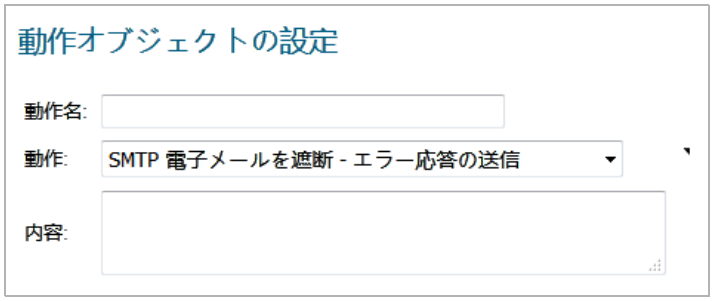
重要：グローバル帯域幅管理は、グローバル帯域幅管理の設定の説明に従って、「**管理 | セキュリティ設定 > ファイアウォール設定 > 帯域幅管理**」で最初に有効にする必要があります。

あらかじめ定義されているグローバル帯域幅管理動作やポリシーを使いたくない場合は、要求に合致する新しいものを作成できます。

新しいグローバル帯域幅管理動作オブジェクトを作成するには:

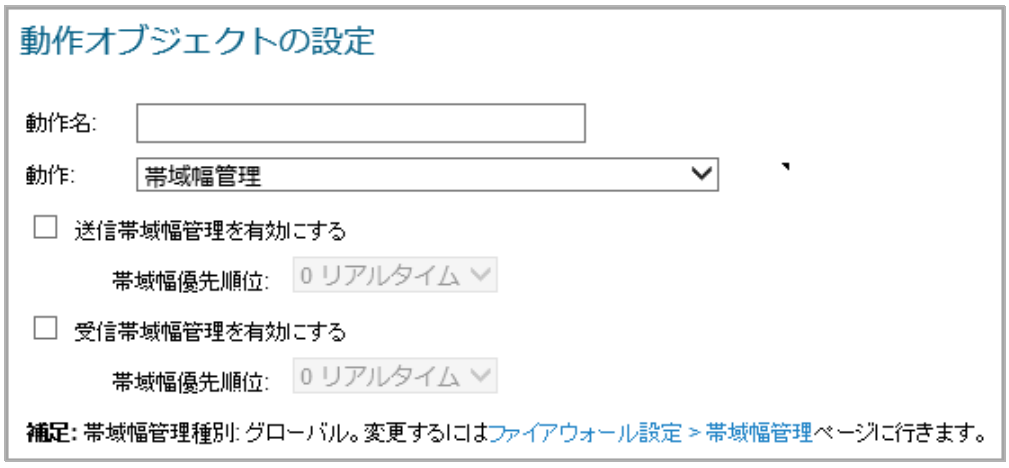
1 「**管理 |ポリシー > オブジェクト > 動作オブジェクト**」ページに移動します。

2 「**動作オブジェクト**」テーブルの上部にある「**追加**」アイコンを選択します。「**動作オブジェクトの追加/編集**」ダイアログが表示されます。



3 「**動作名**」フィールドに動作オブジェクトの名前を入力します。

4 「**動作**」ドロップダウン メニューから、アプリケーションレベルの帯域幅使用状況の制御と監視を行うための「**帯域幅管理**」を選択します。ダイアログ上のオプションが変化します。



5 優先順位に基づく帯域幅管理を指定するには、「**送信帯域幅管理を有効にする**」および「**受信帯域幅管理を有効にする**」のどちらかまたは両方をオンにします。これらのオプションは、既定ではオフになっています。

6 「**帯域幅優先順位**」ドロップダウン メニューから目的の帯域幅優先順位を選択します。最高の優先順位は「**0 リアルタイム**」で、これが既定値です。最低の優先順位は「**7 最低**」です。

7 「**OK**」を選択します。

アプリケーション ルールの設定

アプリケーション ルールで帯域幅管理 (BWM) を設定すると、プロトコル内の特定のファイル種別については帯域幅の消費を制限する一方で、その他のファイル種別については帯域幅の無制限な使用を許可するポリシーを作成できます。これにより、同じプロトコル内で好ましいトラフィックと好ましくないトラフィックを区別できます。

アプリケーション ルールによる帯域幅管理では、次の「**ポリシー種別**」をサポートしています。

- SMTP クライアント
- HTTP クライアント
- HTTP サーバ
- FTP クライアント
- FTP クライアント ファイル アップロード
- FTP クライアント ファイル ダウンロード
- FTP データ転送
- POP3 クライアント
- POP3サーバ
- 個別ポリシー
- IPS コンテンツ
- アプリケーション制御コンテンツ
- CFS

メモ：アプリケーション ルールで帯域幅管理を設定する前に、まず帯域幅管理を有効にする必要があります。

アプリケーション ルールで帯域幅管理を設定する前に:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 帯域幅管理**」で使用する優先順位を有効にします。グローバル帯域幅管理の設定 (27 ページ) を参照してください。

2 **動作オブジェクト**で帯域幅管理を有効にします。動作オブジェクトでのグローバル帯域幅管理の設定 (30 ページ) を参照してください。

3 **インターフェース**で帯域幅管理を設定します。インターフェースに対するグローバル帯域幅管理の設定 (28 ページ) を参照してください。

アプリケーション ルールで帯域幅管理を設定するには:

1 「**管理 |ポリシー > ルール > アプリケーション ルール**」ページに移動します。

2 **追加**アイコンを選択します。「**アプリケーション制御ポリシーの設定**」ダイアログが表示されます。

3 「**アプリケーション制御ポリシーの設定**」の下で、「**ポリシー名**」フィールドに意味のある名前を入力します。

4 「**動作オブジェクト**」から、目的の帯域幅管理動作オブジェクトを選択します。

5 必要に応じて残りの項目を設定します (*SonicWall SonicOS 6.5 ポリシー*を参照)。

6 「**OK**」を選択します。

AppFlow 監視の設定

帯域幅管理は、「**ログ > AppFlow ログ**」ページからも設定できます。そのためには、サービス種別アプリケーションまたはシグネチャ種別アプリケーションを選択してから「**ルールの作成**」ボタンを選択します。利用可能な帯域幅管理オプションは、「**ファイアウォール設定 > 帯域幅管理**」ページのグローバル優先順位キュー テーブル内の有効な優先順位レベルに依存します。既定で有効になっている優先順位レベルは、高、中、低です。

メモ：進める前に、SonicWall アプリケーション可視化を有効にしておく必要があります。

AppFlow 監視を使って帯域幅管理を設定するには:

1 「**調査**」ビューを選択します。

2 「**ログ > AppFlow ログ**」ページに移動します。

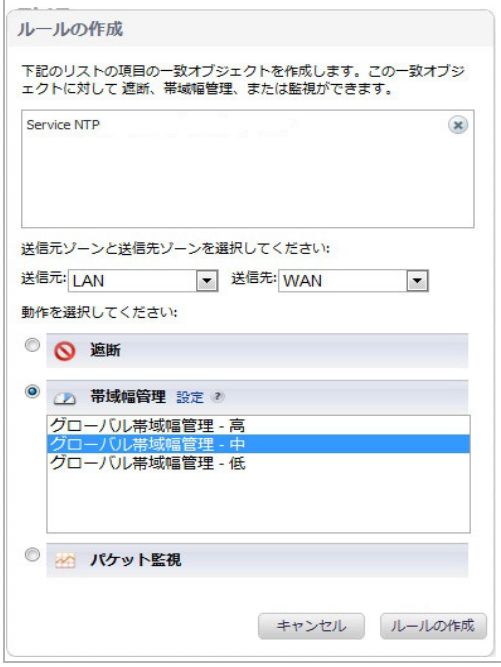
3 グローバル帯域幅管理を適用したい、サービス ベースのアプリケーションまたはシグネチャ ベースのアプリケーションをチェックします。

メモ：標準アプリケーションは選択できません。サービス種別アプリケーションとシグネチャ種別アプリケーションは、単一ルール内に混在できません。

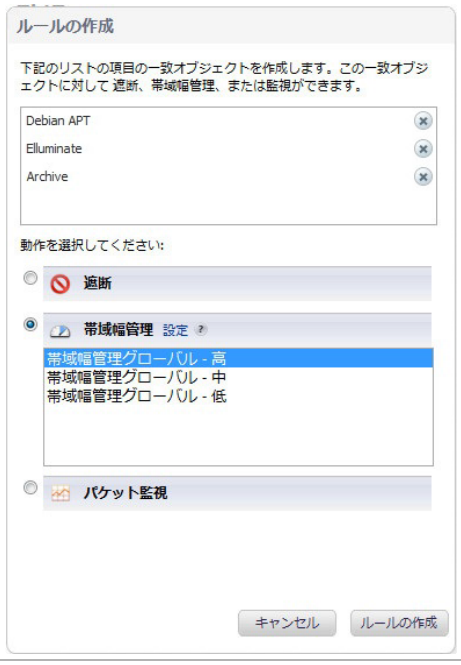
メモ：サービス ベースのアプリケーションに対してルールを作成すると、ファイアウォール アクセス ルールが作成され、シグネチャ ベースのアプリケーションに対してルールを作成すると、アプリケーション制御ポリシーが作成されます。

4 「**ルールの作成**」を選択します。「**ルールの作成**」ダイアログが表示されます。サービス ベースのアプリケーションのオプションと、シグネチャ ベースのアプリケーションのオプションで、ルールには少し違いがあります。

サービス ベースのアプリケーションのオプション



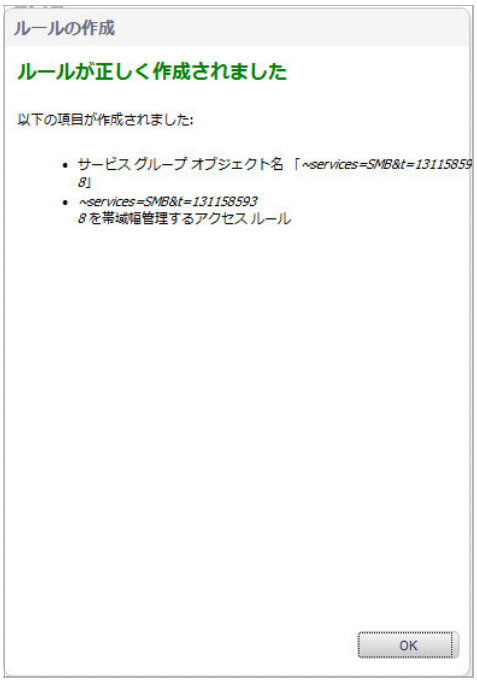
シグネチャ ベースのアプリケーションのオプション



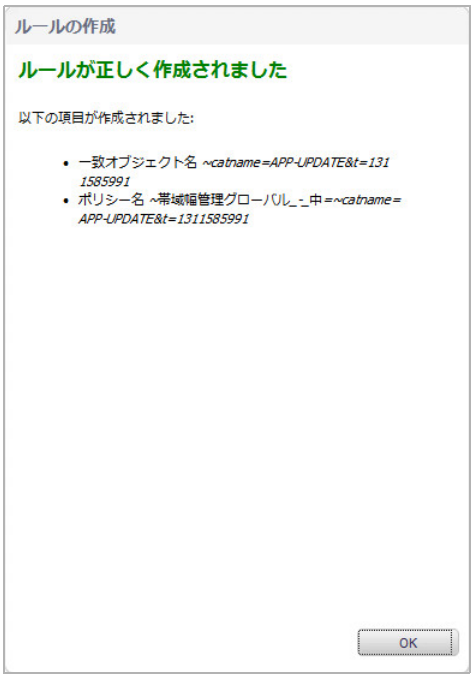
5 「**帯域幅管理**」ラジオ ボタンを選択します。

6 グローバル帯域幅管理の優先順位を選択します。

7 「**ルールの作成**」を選択します。確認ダイアログが表示されます。サービス ベースのアプリケーションのオプションと、シグネチャ ベースのアプリケーションのオプションで、作成される項目には少し違いがあります。



サービス ベースのアプリケーション成功



シグネチャ ベースのアプリケーション成功

8 「**OK**」を選択します。

9 ルールが作成されたことを確認するには、次のページに移動します。

- 「**管理 |ポリシー > ルール > アクセス ルール**」ページ (サービス ベースのアプリケーションの場合)。
- 「**管理 |ポリシー > ルール > アプリケーション制御** (シグネチャ ベースのアプリケーションの場合)。

メモ：サービス ベースのアプリケーションの場合、新しいルールは**コメント**列の**ピン** アイコンと**サービス**列の接頭辞 `~services=<サービス名>` で識別されます (例: `~services=NTP&t=1306361297`)。

シグネチャ ベースのアプリケーションの場合、新しいルールは**名前**列の接頭辞 `~BWM_グローバル-<優先順位>=~catname=<アプリケーション名>` と**オブジェクト**列の接頭辞 `~catname=<アプリケーション名>` で識別されます。

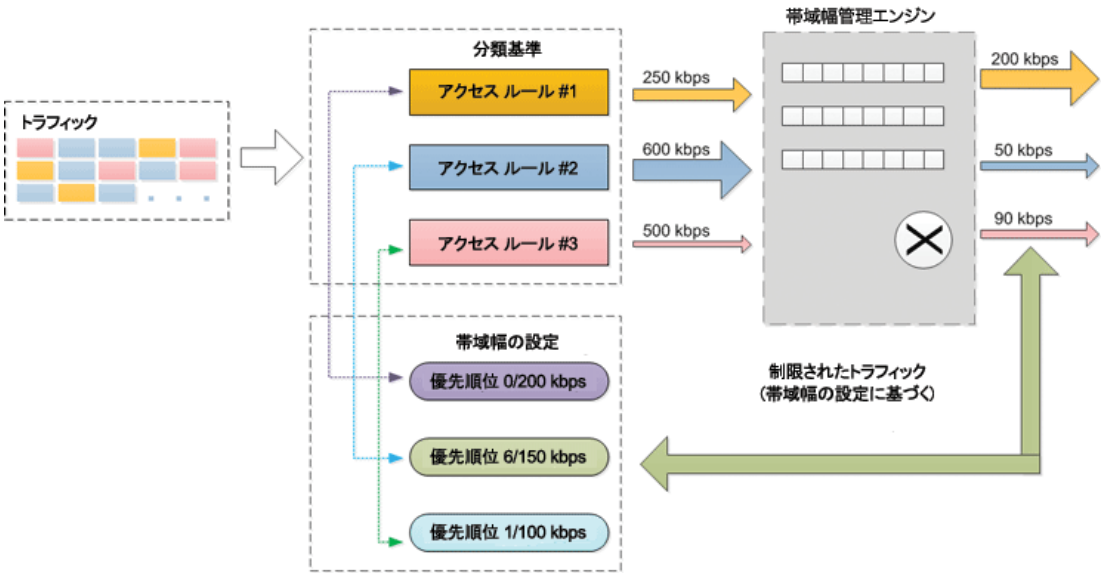
詳細帯域幅管理

詳細帯域幅管理を使用すると、特定の等級のトラフィックを優先順位と最大帯域幅の設定に基づいて管理できます。詳細帯域幅管理は、主に次の 3 つのコンポーネントで構成されています。

- **分類基準** - ファイアウォールを通過するパケットを適切なトラフィック等級に分類します。
- **エスティメータ** - あるトラフィック等級に利用可能な帯域幅があるかどうかを確認するために、そのトラフィック等級によって一定時間内に使用される帯域幅を推定および計算します。
- **スケジューラ** - エスティメータによって提供されるトラフィック等級の帯域幅の状況に基づいて転送されるトラフィックをスケジュールします。

詳細帯域幅管理: 基本概念は、詳細帯域幅管理の基本的な概念を示しています。

詳細帯域幅管理: 基本概念



帯域幅管理の設定は、トラフィック等級に対する帯域幅制限を指定するポリシーに基づいています。完全な帯域幅管理ポリシーは、分類基準と帯域幅ルールという 2 つの部分で構成されます。

帯域幅ルールは、優先順位、保証帯域幅、最大帯域幅、IP 毎帯域幅管理など、実際のパラメータを指定し、帯域幅オブジェクト内で設定されます。帯域幅ルールは、具体的な基準との照合によってパケットの識別とトラフィック等級への分類を行います。

分類基準とは、帯域幅オブジェクトが有効になっているアクセス ルールまたはアプリケーション ルールです。アクセス ルールとアプリケーション ルールは、特定のインターフェースまたはインターフェース グループに対して設定されます。

帯域幅管理での最初の手順は、SonicOS ファイアウォールを通過するすべてのパケットに分類基準 (等級タグ) が割り当てられるようにすることです。分類基準により、パケットは特定のトラフィック等級に属するものとして識別されます。次に、分類されたパケットは、ポリシングおよびシェイピングのために帯域幅管理エンジンに渡されます。SonicOS では次の 2 種類の分類基準を使用しています。

- アクセス ルール
- アプリケーション ルール

サブ要素を持つルールは、親ルールと呼ばれます。

帯域幅オブジェクトの設定: 「パラメータ」 テーブルに、帯域幅オブジェクトで設定されるパラメータを示します。

帯域幅オブジェクトの設定: 「パラメータ」

名前	説明
保証帯域幅	特定のトラフィック等級に対して提供されることが保証されている帯域幅です。
最大帯域幅	トラフィック等級で利用できる最大の帯域幅です。
トラフィック優先順位	トラフィック等級の優先順位です。 • **0** - 最高優先順位 • **7** - 最低優先順位
違反動作	トラフィックが最大帯域幅を超えたときに行われるファイアウォールの動作です。 • **遅延** - パケットはキューに登録され、送信可能になると送信されます。 • **破棄** - パケットは直ちに破棄されます。
IP 毎帯域幅管理を有効にする	音声やビデオといったタイムクリティカルなトラフィックを、ファイアウォールが効果的にサポートできるようにする基本機能です。IP 毎帯域幅管理を有効にすると、基本帯域幅の設定が、その親ルールの下の個々の IP に適用されます。

パケットに特定のトラフィック等級がタグ付けされた後、帯域幅管理エンジンは、帯域幅オブジェクトで定義され、アクセス ルールで有効化され、アプリケーション ルールに付与された帯域幅設定に基づいたポリシングとシェイピングのために、そうしたパケットを収集します。

また、分類基準により、トラフィック フローにおけるパケットの方向の識別も行われます。分類基準は送信、受信、双方向のいずれに対しても設定できます。帯域幅管理では、受信と送信という用語が次のように定義されています。

- **受信** - 特定のトラフィック フローにおける始動者から応答者へのトラフィック。
- **送信** - 特定のトラフィック フローにおける応答者から始動者へのトラフィック。

例えば、インターフェース X0 の背後にあるクライアントがインターフェース X1 の背後にあるサーバへの接続を持っているとします。トラフィックの方向 テーブルに次の項目を示します。

- クライアントとサーバに対する方向のそれぞれにおけるトラフィック フローの方向

- 各インターフェースでのトラフィックの方向
- 帯域幅管理の分類基準によって示される方向

トラフィックの方向

トラフィック フローの方向	インターフェース X0 での方向	インターフェース X1 での方向	帯域幅管理分類基準
クライアントからサーバ	送信	受信	送信
サーバからクライアント	受信	送信	受信

WAN ゾーンでの従来の帯域幅管理設定との互換性を確保するために、トラフィックの方向の定義では今なお着信および発信という用語がサポートされています。これらの用語はアクティブな WAN ゾーン インターフェースのみに適用できます。

- **発信** - WAN ゾーンに対する LAN\DMZ ゾーンからのトラフィック (送信)。
- **着信** - LAN\DMZ ゾーンに対する WAN ゾーンからのトラフィック (受信)。

トピック:

- 基本帯域幅の設定 (37 ページ)
- ゾーン不要の帯域幅管理 (38 ページ)
- 重み付け公平キューイング (38 ページ)

基本帯域幅の設定

基本帯域幅の設定では、単一の帯域幅管理ルールを、そのルールの個々の要素に適用することができます。IP 毎帯域幅管理は、帯域幅オブジェクトのサブオプションである “基本” 機能です。IP 毎帯域幅管理を有効にすると、基本帯域幅の設定が、その親ルールの下の個々の IP に適用されます。

基本帯域幅の設定機能では、帯域幅オブジェクトを親のトラフィック等級の下にある個々の要素に適用できます。「基本帯域幅の設定」は、親ルールまたはトラフィック等級である「**管理 | ポリシー > オブジェクト > 帯域幅 オブジェクト**」のサブオプションです。次の表に、基本帯域幅の設定で設定されるパラメータを示します。*SonicWall SonicOS 6.5 ポリシー*を参照してください。

基本帯域幅の設定: 「パラメータ」

名前	説明
IP 毎帯域幅管理を有効にする	これを有効にすると、最大基本帯域幅の設定が、親トラフィック等級の下の個々の IP アドレスに適用されます。これによってファイアウォールは、音声やビデオといったタイムクリティカルなトラフィックを効果的にサポートできます。
最大帯域幅	親のトラフィック等級の下にある IP アドレスに適用できる最大の基本帯域幅です。 最大の基本帯域幅は、その親の等級の最大帯域幅より大きな値にはできません。

IP 毎帯域幅管理を有効にすると、親ルールの下の個々の IP に基本帯域幅の設定が適用されます。

ゾーン不要の帯域幅管理

ゾーン不要の帯域幅管理機能は、ゾーンの割り当てに関係なく、すべてのインターフェースで帯域幅管理を有効にします。これまで、帯域幅管理は以下のゾーンのみに適用されていました。

- LAN/DMZ から WAN/VPN
- WAN/VPN から LAN/DMZ

SonicOS 6.2 以上のゾーン不要の帯域幅管理は、ゾーンに関係なく、すべてのインターフェースにわたって実行できます。

ゾーン不要の帯域幅管理により、受信と送信のどちらかの方向または両方の方向で、最大帯域幅の制限を個別に設定したり、アクセス ルールやアプリケーション ルールを使用してこうした制限を任意のインターフェースに適用したりできます。

メモ：インターフェースの帯域幅制限は、物理インターフェースでのみ使用できます。フェイルオーバーや負荷分散の設定は、インターフェースの帯域幅制限には影響しません。

重み付け公平キューイング

従来、SonicOS の帯域幅管理では、パケットのトラフィック等級の優先順位に基づいて、トラフィックを 8 つのキューに分配しています。これら 8 つのキューは厳格な優先順位キューイングによって動作します。優先順位が最高のパケットは必ず最初に送信されます。

厳格な優先順位キューイングでは、優先順位の高いトラフィックがインターフェースで使用可能な帯域幅のすべてを独占し、結果として優先順位の低いトラフィックがいつまでもキューに詰め込まれたままになる可能性があります。厳格な優先順位キューイングでは、スケジューラが常に優先順位のより高いキューに優先権を与えます。その結果、優先順位のより低いキューでは帯域幅が不足する可能性があります。

重み付け公平キューイング (WFQ) は、すべてのキューが一定時間内に公平に処理されるように、各キューのパケットをラウンド ロビン方式で処理することで帯域幅不足の問題を軽減します。優先順位の高いキューに対してはより多くの処理が行われ、優先順位の低いキューほど処理量が少なくなります。優先順位が高いからといってすべての処理を獲得できるキューはなく、優先順位が低いからといってまったく処理されずに放置されるキューもありません。

例えば、トラフィック等級 A は 400 kbps の最大帯域幅で優先順位 1 に設定されているとします。トラフィック等級 B は 600 kbps の最大帯域幅で優先順位 3 に設定されています。どちらのトラフィック等級も最大帯域幅が 500 kbps しかないインターフェースに対してキューイングされます。双方のキューは、それぞれの優先順位に基づいてラウンド ロビン方式で処理されます。そのため、どちらのキューも処理されますが、トラフィック等級 A はトラフィック等級 B よりも迅速に送信されます。

連続サンプリング区間に対する調節された帯域幅 テーブルに、連続するサンプリング区間ごとの調節された帯域幅を示します。

連続サンプリング区間に対する調節された帯域幅

サンプリング間隔	トラフィック等級 A		トラフィック等級 B	
	受信帯域幅 (kbps)	調節された帯域幅 (kbps)	受信帯域幅 (kbps)	調節された帯域幅 (kbps)
1	500	380	500	120
2	500	350	500	150
3	400	300	800	200

連続サンプリング区間に対する調節された帯域幅

サンプリング間隔	トラフィック等級 A		トラフィック等級 B	
	受信帯域幅 (kbps)	調節された帯域幅 (kbps)	受信帯域幅 (kbps)	調節された帯域幅 (kbps)
4	600	400	400	100
5	200	180	600	320
6	200	200	250	250

詳細帯域幅管理の設定

トピック:

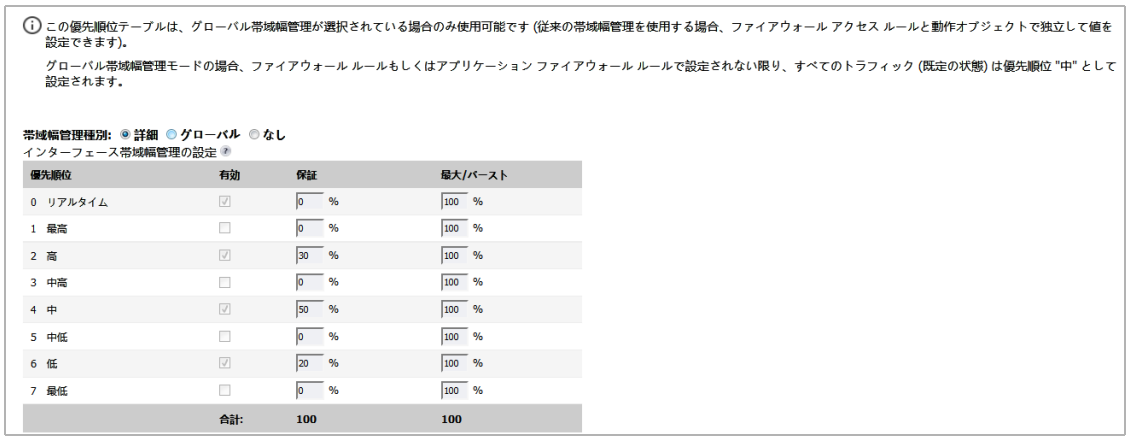
- 詳細帯域幅管理の有効化 (39 ページ)
- 帯域幅ポリシーの設定 (40 ページ)
- 詳細帯域幅管理でのインターフェース帯域幅制限の設定 (47 ページ)
- 詳細帯域幅管理でのインターフェース帯域幅制限の設定 (47 ページ)
- グローバル帯域幅管理でのインターフェース帯域幅制限の設定 (48 ページ)

詳細帯域幅管理の有効化

詳細帯域幅管理を有効にするには:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 帯域幅管理**」に移動します。

2 「**帯域幅管理種別**」オプションを「**詳細**」に設定します。



3 「**適用**」を選択します。

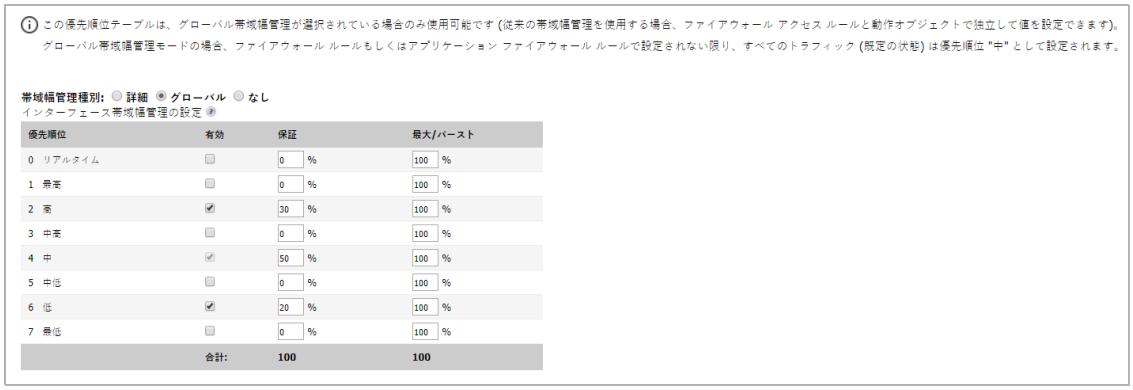
メモ：詳細帯域幅管理が選択されている場合、優先順位フィールドは無効になっていて、ここでは設定できません。詳細帯域幅管理では、優先順位が帯域幅ポリシーにおいて設定されます。帯域幅ポリシーの設定 (40 ページ) を参照してください。

グローバル帯域幅管理を有効にする

グローバル帯域幅管理を有効にするには:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 帯域幅管理**」に移動します。

2 「**帯域幅管理種別**」オプションを「**グローバル**」に設定します。



既定では、3 つの優先順位のみが設定されます。

- **2 高** - 30% 保証
- **4 中** - 50% 保証 (選択解除できませんが、割合は変更可能)
- **6 低** - 20% 保証

3 優先順位 (4 中を除く) の「有効」チェックボックスを選択して、優先順位を有効または無効にします。

4 「保証」フィールドに割合を入力して、選択した各優先順位の保証帯域幅を指定します。

> **重要**：保証帯域幅の比率の合計が 100% を超えてはなりません。帯域幅が 100% を超えると、**合計**の値が赤色で表示されます。また、保証帯域幅が、キューごとの最大帯域幅を超えてはなりません。

5 「最大/バースト」フィールドに割合を入力して、選択した各優先順位の最大 (バースト) 帯域幅を指定します。

> **ヒント**： すべての優先順位に、同じ**最大/バースト**帯域幅を持たせることができます。

6 「**適用**」を選択します。

帯域幅ポリシーの設定

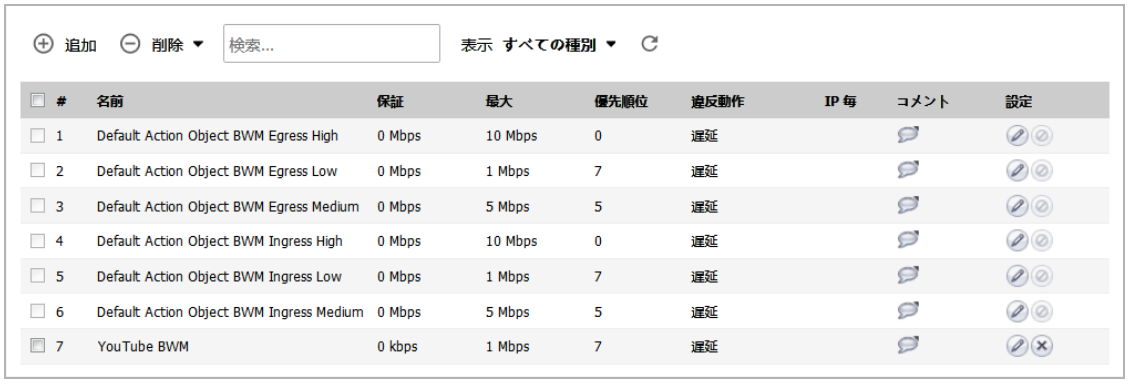
トピック:

- 帯域幅オブジェクトの設定 (41 ページ)
- 基本帯域幅管理の有効化 (42 ページ)
- アクセス ルールでの帯域幅オブジェクトの有効化 (43 ページ)
- アクセス ルールでの帯域幅優先順位の有効化 (44 ページ)
- 動作オブジェクトでの帯域幅オブジェクトの有効化 (45 ページ)
- 動作オブジェクトでの帯域幅優先順位と帯域幅オブジェクトの有効化 (46 ページ)

帯域幅オブジェクトの設定

帯域幅オブジェクトを設定するには:

1 「**管理 |ポリシー > オブジェクト > 帯域幅オブジェクト**」に移動します。



2 以下のいずれかを実行します。

- 「**追加**」アイコンを選択して、新しい帯域幅オブジェクトを作成します。
- 変更する帯域幅オブジェクトの**編集**アイコンを選択します。

「**帯域幅オブジェクトの設定**」ダイアログが表示されます。

3 「**名前**」フィールドに、帯域幅オブジェクトの名前を入力します。

4 「**保証帯域幅**」フィールドに、この帯域幅オブジェクトがあるトラフィック等級への提供を保証する帯域幅の量を (kbps または Mbps 単位で) 入力します。

a 帯域幅の単位が「**kbps**」(既定) と「**Mbps**」のどちらであるかをドロップダウン メニューから選択します。

5 「**最大帯域幅**」フィールドに、この帯域幅オブジェクトがあるトラフィック等級に提供する帯域幅の最大量を入力します。

メモ：複数のトラフィック等級が共有された帯域幅をめぐって競合している場合、実際に割り当てられる帯域幅はこの値よりも少なくなることがあります。

a 帯域幅の単位が「**kbps**」(既定) と「**Mbps**」のどちらであるかをドロップダウン メニューから選択します。

6 「**トラフィック優先順位**」フィールドに、この帯域幅オブジェクトがあるトラフィック等級に付与する優先順位を入力します。最高の優先順位は「**0 リアルタイム**」で、これが既定値です。最低の優先順位は「**7 最低**」です。

複数のトラフィック等級が共有された帯域幅をめぐって競合している場合は、優先順位が指向の等級に優先権が与えられます。

7 「**違反動作**」フィールドに、トラフィックが最大帯域幅の設定値を上回った場合にこの帯域幅オブジェクトが実施する動作を入力します。

- **遅延** - 過剰なトラフィック パケットをキューに登録し、送信可能になった時点で送信することを示します。
- **破棄** - 過剰なトラフィック パケットが直ちに破棄されることを示します。

8 「**コメント**」フィールドに、この帯域幅オブジェクトに対するコメントまたは説明のテキストを入力します。

9 「**OK**」を選択します。

基本帯域幅管理の有効化

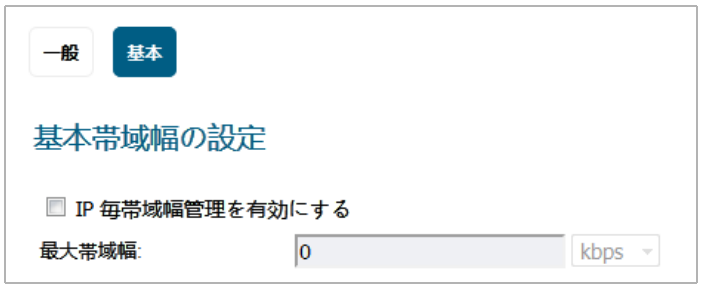
基本帯域幅管理では、SonicOS が帯域幅ルールおよびポリシーを、ファイアウォールを通過する個々の IP に対して強制できます。

基本帯域幅管理を帯域幅オブジェクトで有効にするには:

1 「**管理 |ポリシー > オブジェクト > 帯域幅オブジェクト**」に移動します。

2 変更する帯域幅オブジェクトの**編集**アイコンを選択します。「**帯域幅オブジェクトの設定**」ダイアログが表示されます。

3 「**基本**」を選択します。



4 「**IP 毎帯域幅管理を有効にする**」オプションを選択します。このオプションは、既定では選択されていません。最大の基本帯域幅の設定値が有効になっている場合、これらの設定は親のトラフィック等級の下にある個々の IP に適用されます。

5 「**最大帯域幅**」フィールドに、親のトラフィック等級の下にあるプロトコルに割り当てることができる最大の基本帯域幅を入力します。

   a 帯域幅の単位が「**kbps**」(既定) と「**Mbps**」のどちらであるかをドロップダウン メニューから選択します。

6 「**OK**」を選択します。

アクセス ルールでの帯域幅オブジェクトの有効化

詳細帯域幅管理を選択している場合、「**管理 |ポリシー > ルール > アクセス ルール**」で帯域幅オブジェクト (およびその設定) を有効にできます。

アクセス ルール内で帯域幅オブジェクトを有効にするには:

1 「**管理 |ポリシー > ルール > アクセス ルール**」に移動します。

2 以下のいずれかを実行します。

- 「**追加**」アイコンを選択して新しいアクセス ルールを作成します。「**ルールの追加**」ダイアログが表示されます。
- 適切なアクセス ルールの「**編集**」アイコンを選択します。「**ルールの編集**」ダイアログが表示されます。

3 「**帯域幅管理**」をクリックします。

4 送信方向の帯域幅オブジェクトを有効にするには、「**帯域幅管理**」の下にある「**送信帯域幅管理を有効にする (「許可」ルールのみ)**」を選択します。

5 「**帯域幅オブジェクト**」ドロップダウン メニューから、送信方向に必要な帯域幅オブジェクトを選択します。

6 受信方向の帯域幅オブジェクトを有効にするには、「**帯域幅管理**」の下にある「**受信帯域幅管理を有効にする (「許可」ルールのみ)**」を選択します。

7 「**帯域幅オブジェクト**」ドロップダウン メニューから、受信方向に必要な帯域幅オブジェクトを選択します。

8 帯域幅使用状況の追跡を有効にするには、「**帯域幅使用状況の追跡を有効にする**」オプションを選択します。

9 「**OK**」を選択します。

アクセス ルールでの帯域幅優先順位の有効化

グローバル帯域幅管理帯域幅管理を選択している場合、「**管理 |ポリシー > ルール > アクセス ルール**」で帯域幅優先順位を有効にできます。

アクセス ルール内で帯域幅優先順位を有効にするには:

1 「**管理 |ポリシー > ルール > アクセス ルール**」に移動します。

2 以下のいずれかを実行します。

- 「**追加**」アイコンを選択して新しいアクセス ルールを作成します。「**ルールの追加**」ダイアログが表示されます。
- 適切なアクセス ルールの「**編集**」アイコンを選択します。「**ルールの編集**」ダイアログが表示されます。

3 「**帯域幅管理**」をクリックします。

4 送信方向の帯域幅オブジェクトを有効にするには、「**帯域幅管理**」の下にある「**送信帯域幅管理を有効にする (「許可」ルールのみ)**」を選択します。 このオプションは、既定では選択されていません。

5 「**帯域幅優先順位**」ドロップダウン メニューで、送信方向の帯域幅優先順位を選択します。最高の優先順位は「**0 リアルタイム**」で、これが既定値です。最低の優先順位は「**7 最低**」です。

6 受信方向の帯域幅オブジェクトを有効にするには、「**帯域幅管理**」の下にある「**受信帯域幅管理を有効にする (「許可」ルールのみ)**」を選択します。 このオプションは、既定では選択されていません。

7 「**帯域幅優先順位**」ドロップダウン メニューで、受信方向の帯域幅優先順位を選択します。最高の優先順位は「**0 リアルタイム**」で、これが既定値です。最低の優先順位は「**7 最低**」です。

8 「**OK**」を選択します。

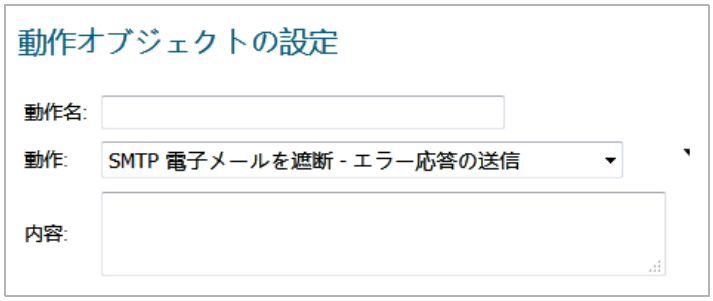
動作オブジェクトでの帯域幅オブジェクトの有効化

詳細帯域幅管理を選択している場合、「**ルール > アクセス ルール**」で帯域幅オブジェクト (およびその設定) を有効にできます。

動作オブジェクト内で帯域幅オブジェクトを有効にするには:

1 「**管理 |ポリシー > オブジェクト > 動作オブジェクト**」に移動します。

2 「**追加**」アイコンを選択して、新しい動作オブジェクトを作成します。「**動作オブジェクトの設定**」ダイアログが表示されます。



3 動作オブジェクトの名前を「**動作名**」フィールドに入力します。

4 「**動作**」から、「**帯域幅管理**」を選択します。これによって、アプリケーションレベルの帯域幅使用状況の制御と監視が可能になります。「**動作オブジェクトの設定**」ダイアログ上のオプションが変わります。

5 「**帯域幅統合方式**」ドロップダウン メニューで、適切な帯域幅統合方式を選択します。

- 「**ポリシー毎**」 (既定)
- 「**動作毎**」

6 送信方向で帯域幅管理を有効にするには、「**送信帯域幅管理を有効にする**」オプションを選択します。

a 「**帯域幅オブジェクト**」から、送信方向の帯域幅オブジェクトを選択します。

7 受信方向で帯域幅管理を有効にするには、「**受信帯域幅管理を有効にする**」オプションを選択します。

   a 「**帯域幅オブジェクト**」から、送信方向の帯域幅オブジェクトを選択します。

8 「**OK**」を選択します。

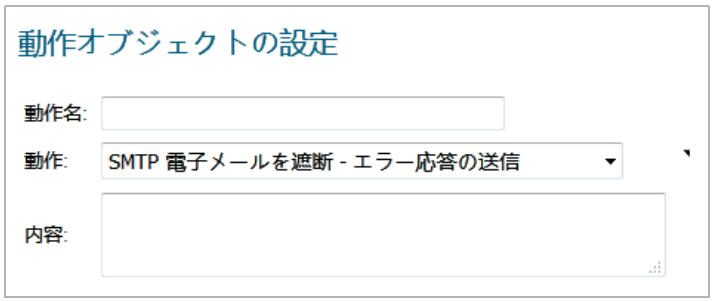
動作オブジェクトでの帯域幅優先順位と帯域幅オブジェクトの有効化

グローバル帯域幅管理帯域幅管理を選択している場合、「**管理 |ポリシー > ルール > アクセス ルール**」で帯域幅優先順位を指定し、帯域幅オブジェクト (およびその設定) を有効にすることができます。

動作オブジェクト内で帯域幅優先順位と帯域幅オブジェクトを有効にするには:

1 「**管理 |ポリシー > オブジェクト > 動作オブジェクト**」に移動します。

2 「**追加**」アイコンを選択して、新しい動作オブジェクトを作成します。「**動作オブジェクトの設定**」ダイアログが表示されます。



3 動作オブジェクトの名前を「**動作名**」フィールドに入力します。

4 「**動作**」から、「**帯域幅管理**」を選択します。これによって、アプリケーションレベルの帯域幅使用状況の制御と監視が可能になります。「**動作オブジェクトの設定**」ダイアログ上のオプションが変わります。

5 送信方向の帯域幅管理を有効にするには、優先順位用の「**送信帯域幅管理を有効にする**」オプションを選択します。

   a 「**帯域幅優先順位**」ドロップダウン メニューから、送信方向に必要な帯域幅オブジェクトを選択します。最高の優先順位は「**0 リアルタイム**」で、これが既定値です。最低の優先順位は「**7 最低**」です。

6 受信方向の帯域幅管理を有効にするには、優先順位用の「**受信帯域幅管理を有効にする**」オプションを選択します。

   a 「**帯域幅優先順位**」ドロップダウン メニューから、受信方向に必要な帯域幅オブジェクトを選択します。最高の優先順位は「**0 リアルタイム**」で、これが既定値です。最低の優先順位は「**7 最低**」です。

7 「**OK**」を選択します。

詳細帯域幅管理でのインターフェース帯域幅制限の設定

インターフェースに対して帯域幅制限を設定するには:

1 「**管理 | システム セットアップ > ネットワーク > インターフェース**」に移動します。

2 目的のインターフェースの「**編集**」アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

3 「**詳細設定**」を選択します。

4 「**帯域幅管理**」セクションが表示されるまで画面をスクロールします。

5 「**インターフェース送信帯域幅制限を有効にする**」オプションを選択します。このオプションは、既定では選択されていません。

このオプションの効果は次のとおりです。

- 選択されている場合、利用可能な最大送信帯域幅管理は定義されていますが、詳細帯域幅管理はポリシー ベースなので、その制限は対応するアクセス ルールまたはアプリケーション ルールが存在しなければ適用されません。
- 選択されていない場合は、帯域幅の制限はインターフェース レベルでは設定されませんが、送信トラフィックはその他のオプションを使用して調整できます。

a 「**最大インターフェース送信帯域幅 (kbps)**」フィールドに、このインターフェースの最大送信帯域幅を (キロビット毎秒単位で) 入力します。既定値は **384.000000** Kbps です。

6 「**インターフェース受信帯域幅制限を有効にする**」オプションを選択します。このオプションは、既定では選択されていません。このオプションの使用については、ステップ 5 を参照してください。

7 「**OK**」を選択します。

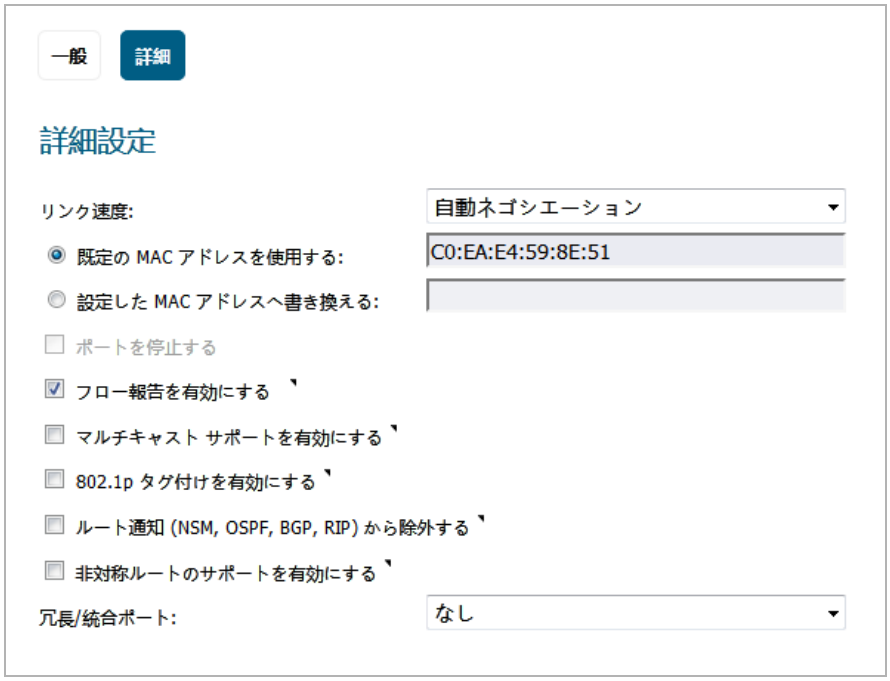
グローバル帯域幅管理でのインターフェース帯域幅制限の設定

インターフェースに対して帯域幅制限を設定するには:

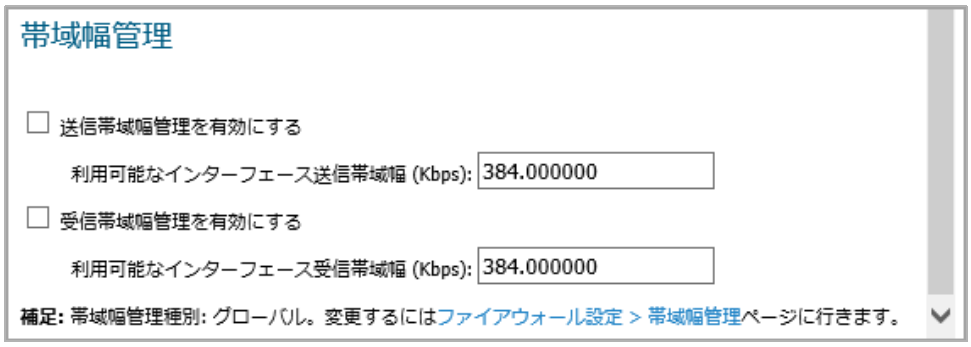
1 「**管理 | システム セットアップ > ネットワーク > インターフェース**」に移動します。

2 目的のインターフェースの「**編集**」アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

3 「**詳細設定**」を選択します。



4 「**帯域幅管理**」セクションが表示されるまで画面をスクロールします。



5 「**送信帯域幅管理を有効にする**」オプションを選択します。このオプションは、既定では選択されていません。

このオプションの効果は次のとおりです。

- 選択されている場合、利用可能な最大送信帯域幅管理は定義されていますが、詳細帯域幅管理はポリシー ベースなので、その制限は対応するアクセス ルールまたはアプリケーション ルールが存在しなければ適用されません。
- 選択されていない場合は、帯域幅の制限はインターフェース レベルでは設定されませんが、送信トラフィックはその他のオプションを使用して調整できます。

a 「**利用可能なインターフェース送信帯域幅 (kbps)**」フィールドに、このインターフェースの最大送信帯域幅を (キロビット毎秒単位で) 入力します。既定値は **384.000000** Kbps です。

6 「**受信帯域幅管理を有効にする**」オプションを選択します。このオプションは、既定では選択されていません。このオプションは、既定では選択されていません。このオプションの使用については、ステップ 5 を参照してください。

a 「**利用可能なインターフェース受信帯域幅 (kbps)**」フィールドに、このインターフェースの最大送信帯域幅を (キロビット毎秒単位で) 入力します。既定値は **384.000000** Kbps です。

7 「**OK**」を選択します。

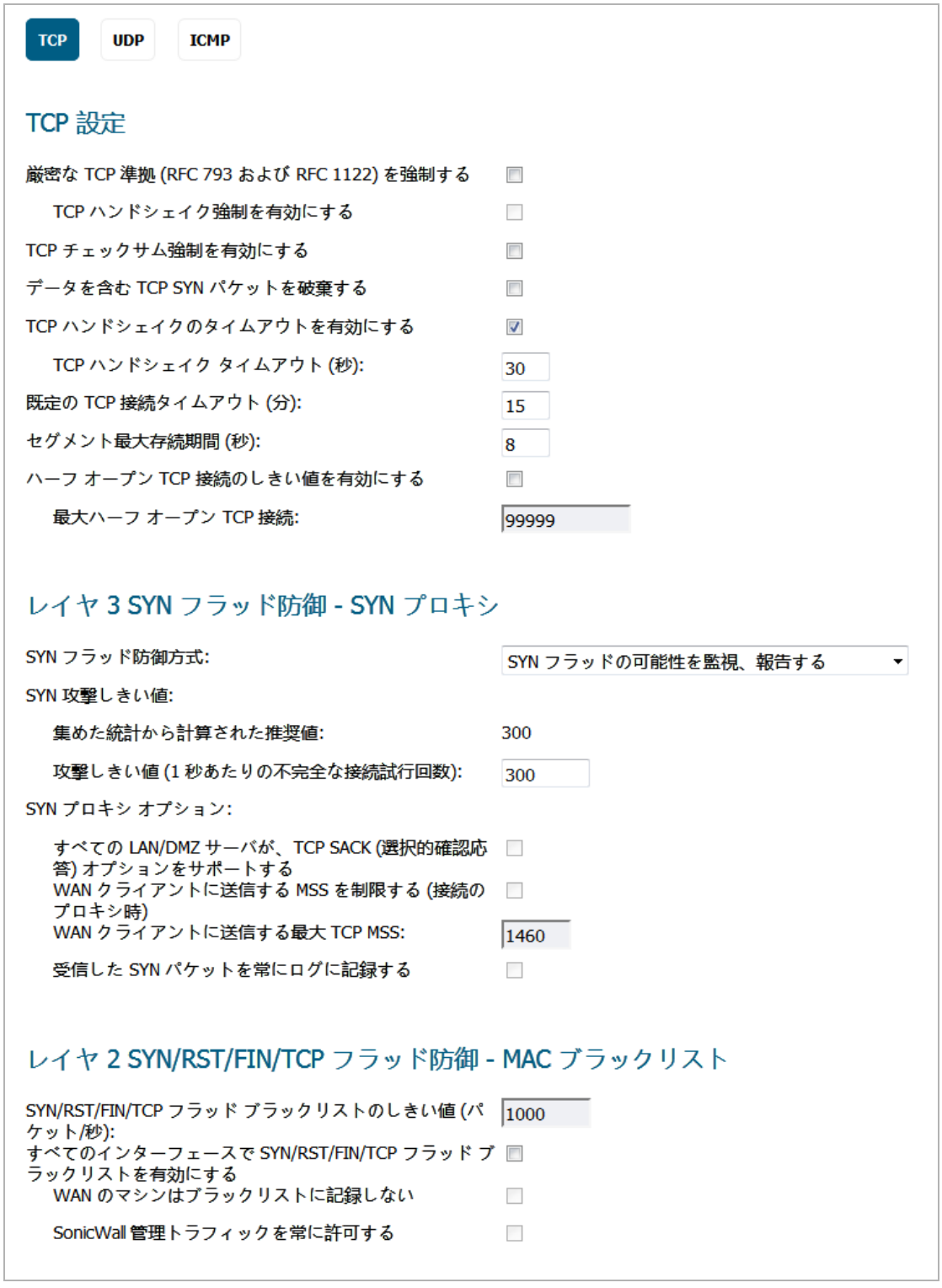
3

フラッド防御の設定

メモ：「制御プレーン フラッド防御」は、「**管理 | セキュリティ設定 > ファイアウォール設定 > 詳細設定** 」ページにあります。

- ファイアウォール設定 > フラッド防御 (51 ページ)

ファイアウォール設定 > フラッド防御



ⓘ **ヒント**：選択した設定はどれも「**適用**」を選択して有効にする必要があります。

「**ファイアウォール設定 > フラッド防御**」ページでは以下のことが行えます。

- 管理:
  - TCP (伝送制御プロトコル) トラフィックの設定 (レイヤ 2/レイヤ 3 フラッド防御、WAN DDOS 防御など)
  - UDP (ユーザ データグラム プロトコル) フラッド防御
  - ICMP (インターネット制御メッセージ プロトコル) または ICMPv6 フラッド防御
- セキュリティ装置を通過するトラフィックに関する統計の表示:
  - TCP トラフィック
  - UDP トラフィック
  - ICMP または ICMPv6 トラフィック

SonicOS は、定義された送信先への IPv6 UDP/ICMP トラフィック フローを監視することで、UDP/ICMP フラッド攻撃を防ぎます。1 つ以上の送信元が設定済みしきい値を超えた場合、指定の送信先への UDP/ICMP パケットは破棄されます。

トピック:

- 「TCP」ビュー (52 ページ)
- 「UDP」ビュー (64 ページ)
- 「ICMP」ビュー (67 ページ)

「TCP」ビュー

トピック:

- TCP 設定 (53 ページ)
- 「レイヤ 3 SYN フラッド防御 - SYN プロキシ」ビュー (54 ページ)
- レイヤ 3 SYNフラッド防御の設定 (56 ページ)
- レイヤ 2 SYN/RST/FIN/TCP フラッド防御 - MAC ブラックリストの設定 (58 ページ)
- WAN DDOS 防御 (TCP 以外のフラッド) (59 ページ)

TCP 設定

- **厳密な TCP 準拠 (RFC 793 および RFC 1122) を強制する** - いくつかの TCP タイムアウト ルールの厳密な要件に確実に従うようにします。この設定は TCP セキュリティを最大化しますが、これにより Windows Vista ユーザに対するウィンドウ スケーリング機能に問題が発生することがあります。このオプションは、既定では選択されていません。
  - **TCP ハンドシェイク強制を有効にする** - すべての TCP 接続に対して、TCP 3 ウェイハンドシェイクの成功を要求します。このオプションは、「**厳密な TCP 準拠 (RFC 793 および RFC 1122) を強制する**」が有効な場合にのみ利用可能です。
- **TCP チェックサム強制を有効にする** - 計算された TCP チェックサムが無効だった場合、パケットは破棄されます。このオプションは、既定では選択されていません。
- **TCP ハンドシェイクのタイムアウトを有効にする** - TCP 3 ウェイ ハンドシェイクによる接続が完了するまでのタイムアウト時間 (秒) を適用します。この時間内に TCP 3 ウェイ ハンドシェイクが完了しない場合、ハンドシェイクは破棄されます。このオプションは、既定では選択されています。
  - **TCP ハンドシェイクタイムアウト (秒)** : TCP ハンドシェイクによる接続が完了するまでの最長時間。既定値は **30** 秒です。
- **既定の TCP 接続タイムアウト (分)** - TCP トラフィックのアクセス ルールで割り当てられる既定の時間。TCP セッションのアクティブな時間がこの設定値を超えると、ファイアウォールにより TCP 接続がクリアされます。既定値は **15** 分です。最小値は 1 分、最大値は 999 分です。

  メモ：接続時タイムアウトを過度に大きく設定すると、古くなったリソースの再利用が遅くなり、極端な場合は接続キャッシュを使い果たす可能性もあります。

- **セグメント最大存続期間 (秒)** - TCP パケットが失効するまでの秒数を指定します。TCP 接続を正しく閉じるための適切な FIN/ACK 交換が問題なく実行されるように、アクティブにクローズされた TCP 接続が TIME_WAIT 状態にとどまる時間 (セグメント最大存続期間の 2 倍、つまり2MSL) を決定する際にも、この設定値が使用されます。既定値は **8** 秒です。最小値は 1 秒、最大値は 60 秒です。

- **ハーフ オープン TCP 接続のしきい値を有効にする** - ハーフ オープン TCP 接続数の最高しきい値に達した場合、新しい TCP 接続を拒否します。既定ではハーフ オープン TCP 接続が監視されていないので、このオプションは選択されていない状態が既定です。
    - **最大ハーフ オープン TCP 接続** - ハーフ オープン TCP 接続の最大数を指定し、「**ハーフ オープン TCP 接続しきい値を有効にする**」が選択されている場合にのみ使用可能です。既定の最大数は、最大接続キャッシュ数の半分の値です。

「レイヤ 3 SYN フラッド防御 - SYN プロキシ」ビュー

トピック:

- SYNフラッド防御モード (54 ページ)
- レイヤ 3 SYNフラッド防御の設定 (56 ページ)

SYNフラッド防御モード

SYN/RST/FIN フラッド防御は、ファイアウォールの背後にあるホストを DoS (サービス拒否) 攻撃や分散 DoS 攻撃から保護するために役立ちます。このような攻撃は、以下のいずれかの攻撃メカニズムを作成することでホストの使用可能リソースを使い果たすことを試みます。

- 無効な IP アドレスやなりすました IP アドレスを使用して、TCP SYN パケット、RST パケット、または FIN パケットを送信する。
- 半オープン TCP 接続を大量に作成する。

以降のセクションでは、いくつかの SYN フラッド防御方式について詳しく説明します。

- ステートレス Cookie を使用した SYN フラッド防御 (54 ページ)
- 階層別の SYN フラッド防御手法 (54 ページ)
- SYN ウォッチリストについて (55 ページ)
- TCP ハンドシェイクについて (55 ページ)

ステートレス Cookie を使用した SYN フラッド防御

SonicOS から導入された SYN フラッド防御の手法では、ステートレス SYN Cookie を使用します。 これにより、SYN フラッドの検出の信頼性が向上するとともに、ファイアウォールにおける全体的なリソース利用が改善されました。ステートレス SYN Cookie を使用することで、ファイアウォールは半オープン接続の状態を維持する必要がなくなります。そして、SEQr をランダムに設定する代わりに、暗号化計算で算出します。

階層別の SYN フラッド防御手法

SonicOS では、信頼される (内部) ネットワークと信頼されない (外部) ネットワークという 2 つの異なる環境から実行される SYNフラッドに対して、複数の保護手段を用意しています。一般的に、*信頼されない*WAN ネットワークからの攻撃は、ファイアウォールにより保護された 1 つ以上のサーバで発生します。*信頼される*LAN ネットワークからの攻撃は、1 つ以上の信頼されるネットワークの内部におけるウイルス感染が原因で発生し、1 つ以上のローカル ホストまたはリモート ホストに対して攻撃が実行されます。

どちらの攻撃シナリオに対してもファイアウォールで防御できるように、SonicOS 2 つの異なる階層に対応する 2 つの SYNフラッド防御メカニズムを備えています。どちらのメカニズムでも、SYNフ

ラッドの統計情報を収集して表示し、重要な SYNフラッド イベントについてはログ メッセージを生成します。

- **SYN プロキシ (レイヤ 3)** - このメカニズムでは、WAN クライアントの接続要求を保護対象サーバに転送する前に SYN プロキシ実装を使用して WAN クライアントを検証することで、信頼されるネットワーク内のサーバを WAN ベース SYNフラッド攻撃から保護します。SYN プロキシは WANインターフェースに対してのみ有効にできます。
- **SYN ブラックリスト (レイヤ2)** - このメカニズムでは、特定の機器による SYNフラッド攻撃の生成や、SYNフラッド攻撃の転送を阻止します。SYN ブラックリストは、任意のインターフェースに対して有効にできます。

SYN ウォッチリストについて

どちらの SYNフラッド防御メカニズムも、内部的な手法は 1 つのイーサネット アドレス リストに基づいています。 これは初回 SYN パケットをファイアウォールに送信する最もアクティブな機器のイーサネット アドレスのリストです。このリストは、*SYN ウォッチリスト*と呼ばれます。このリストにはイーサネット アドレスが含まれるため、SYN パケットを転送する機器のアドレスに基づいてすべての SYN トラフィックを追跡でき、送信元または送信先 IP アドレスを考慮する必要がありません。

ウォッチリストの各エントリには、*ヒット カウント*と呼ばれる値が含まれます。ある機器から初回 SYN パケットが受信されるたびに、その機器に対応するヒット カウントの値が 1 ずつ加算されます。TCP3 ウェイ ハンドシェイクが完了すると、ヒット カウントは 1 ずつ減算されます。特定の機器のヒット カウントは、その機器でヒット カウントがリセットされて以降に処理が保留されている半オープン接続の数に等しくなります。機器でヒット カウントがリセットされる頻度は、既定で 1 秒に 1 回です。

ログ メッセージの表示または状態の変更が必要であるかどうかを判断するときには、ログ、SYN プロキシ、SYN ブラックリストのすべてのしきい値がヒット カウント値と比較されます。SYNフラッド攻撃が発生すると、なりすまし接続が試行されるため、攻撃パケットを転送している機器からの保留中半オープン接続の数が急増します。攻撃しきい値を適切に設定していれば、通常のトラフィック フローではほとんど攻撃警告は発生せず、なおかつ攻撃によって深刻なネットワーク性能低下が生じる前に、攻撃を検出して防御することができます。

TCP ハンドシェイクについて

一般的な TCP ハンドシェイク (簡略) は、開始側が 32 ビット シーケンス (SEQi) 番号を持つ TCP SYN パケットを送信することで開始されます。その後、応答側が受信されたシーケンスを承認する SYN/ACK パケットを送信します。 SEQi+1 に等しい ACK と、ランダムな 32 ビット シーケンス番号 (SEQr) が送信されます。また、応答側は開始側からの ACK を待ち受ける状態を維持します。開始側からの ACK パケットには、次のシーケンス (SEQi+1) と、応答側から受信したシーケンスの承認 (SEQr+1 に等しい ACK を送信) が含まれます。この交換の例を以下に示します。

1 開始側 -> SYN (SEQi=0001234567、ACKi=0) -> 応答側

2 開始側 <- SYN/ACK (SEQr=3987654321、ACKr=0001234568) <- 応答側

3 開始側 -> ACK (SEQi=0001234568、ACKi=3987654322) -> 応答側

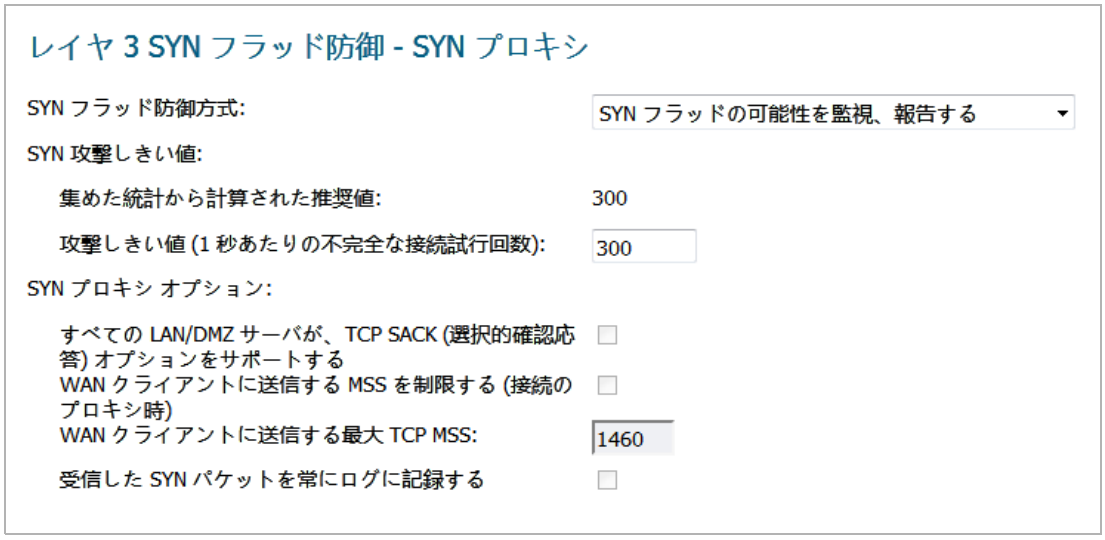
応答側ではすべての半オープン TCP 接続の状態を維持する必要があるため、SYN が受信される速度が応答側で処理またはクリアできる速度を超えると、メモリが枯渇する可能性があります。半オープン TCP 接続では 3 ウェイ ハンドシェイクが完了せず、接続が確立された状態に移行しません。ファイアウォールが開始側と応答側の間にある場合は、ファイアウォールが実質的な応答側となり、保護される実際の応答側 (プライベート ホスト) への TCP 接続のブローカ (*プロキシ*) として動作します。

レイヤ 3 SYNフラッド防御の設定

「SYNフラッド防御モード」では、半オープン TCP セッションと高頻度 SYN パケット送信に対する防御に使用する防御レベルを選択できます。この機能により、3 つの異なるレベルの SYN フラッド防御を設定できます。

SYN フラッド防御機能を設定するには、以下の手順に従います。

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > フラッド防御**」ページの「**レイヤ 3 SYN フラッド防御 - SYN プロキシ**」セクションに移動します。



2 「**SYN フラッド防御方式**」ドロップダウン メニューから、防御モードの種別を選択します。

- **SYN フラッドの可能性を監視、報告する** - 機器の全インターフェースでの SYN トラフィックの監視と、パケット数しきい値を超過した、SYN フラッドと疑われるアクティビティのログ記録を機器が行えるようにします。機器の SYN プロキシは有効にならないため、TCP3 ウェイ ハンドシェイクがそのまま転送されます。

  これは、最も低いレベルの SYNフラッド防御です。ネットワークがそれほど危険性の高い環境にない場合に、このオプションを選択します。

  ⓘ **重要**：この防御モードが選択されている場合、「**SYN プロキシ オプション**」は使用できません。

- **攻撃の疑いがある場合に、WAN クライアント接続をプロキシする** - 完了していない接続試行の回数 (毎秒) が指定されたしきい値を超過したときに、WAN インターフェースでの SYN プロキシ機能を有効にします。この方式では、攻撃中でも有効なトラフィックの処理を継続でき、パフォーマンスも低下しません。すべての WAN SYNフラッド攻撃が停止するまで、または SYN ブラックリスト機能を使用してすべての攻撃がブラックリストに登録されるまで、プロキシ モードは有効になります。

  これは、中間のレベルの SYNフラッド防御です。ネットワークが内部または外部からの SYNフラッド攻撃にさらされている場合に、このオプションを選択します。

- **常に WAN クライアント接続をプロキシする** - 常に SYN プロキシを使用するように機器を設定します。この方式では、すべてのなりすまし SYN パケットが機器を通過できなくなります。

  これは極端なセキュリティ手段です。SYN プロキシ機能によってすべての TCP SYN 接続試行への応答が機器に強制されるため、すべての TCP ポートでポート スキャンに応答す

るように機器に指示します。これにより、パフォーマンスが低下し、誤った警告が発生する場合があります。ネットワークが危険性の高い環境にある場合に限り、このオプションを選択してください。

3 「**SYN 攻撃しきい値**」設定オプションを選択すると、機器でパケットの破棄が開始される SYN フラッド アクティビティの下限が設定されます。装置では WAN TCP 接続の統計情報を収集し、毎秒の最大 WAN 接続数、平均最大 WAN 接続数、および不完全な WAN 接続数を追跡します。これらの統計に基づいて、SYNフラッドしきい値の値が提案されます。

- **集めた統計から計算された推奨値** - WAN TCP 接続統計をもとに提案される攻撃しきい値です。この値は変更できません。
- **攻撃しきい値 (1 秒あたりの不完全な接続試行回数)** - 機器でパケットの破棄が開始される、不完全な接続の試行回数 (毎秒) のしきい値を 5〜200,000 の任意の値に設定できます。既定の設定は、「**集めた統計から計算された推奨値**」です。

4 「**SYN プロキシ オプション**」を選択すると、SYN プロキシ モードになっている場合に WAN クライアントに送信されるオプションをより詳細に制御できます。

> **重要**：このセクション内の各オプションは、「**SYN フラッド防御**」方式で「**SYN フラッドの可能性を監視、報告する**」が選択されている場合、利用できません。

SYN プロキシを TCP 接続に適用する場合、初回 SYN パケットに対して生成した SYN/ACK 応答で応答し、それに対する応答 ACK を待ち受けてから、接続要求をサーバに転送します。SYNフラッド パケットで攻撃している機器は、SYN/ACK 応答に応答しません。ファイアウォールでは、このタイプの応答がない機器を攻撃元として識別し、その機器によるなりすまし接続試行を遮断します。SYN プロキシでは、SYN/ACK パケットに対して通常指定される TCP オプションにサーバがどのように応答するかを認識していなくても、ファイアウォールが SYN/ACK 応答を生成します。

- **すべての LAN/DMZ サーバが、TCP SACK (選択的確認応答) オプションをサポートする** - SACK (選択的応答確認) が有効になります。これにより、パケットを破棄できるようになり、どのパケットを受信したかが受信側機器によって知らされます。このオプションは既定では無効になっています。WAN からアクセスされるファイアウォールによって保護されるすべてのサーバが、SACK オプションをサポートするとわかっている場合にのみ、このチェックボックスをオンにしてください。
- **WAN クライアントに送信する MSS を制限する (接続のプロキシ時)** - 最大の MSS (Minimum Segment Size) 値を入力できるようになります。このように TCP セグメントのサイズのしきい値を設定することで、大きすぎてターゲット サーバに送信できないセグメントが発生することを防止します。例えば、サーバがIPsec ゲートウェイである場合、トラフィックをトンネリングするときに IPsec ヘッダーの領域を残すために、サーバで受信される MSS を制限する必要があることがあります。プロキシ シーケンスの際、ファイアウォールでは、サーバが SYN 生成済みパケットに応答するときにサーバに送信される MSS値を予測することはできません。セグメントのサイズを制御できるようにすることで、WAN クライアントに送信される生成済み MSS 値を制御することができます。このオプションは、既定では選択されていません。

  既定値の **1460** をオーバーライドする値を指定した場合、SYN/ACK Cookie でそのサイズ以下のセグメントがクライアントに送信されます。この値を小さく設定しすぎると、SYN プロキシを常時有効にしたときにパフォーマンスが低下する可能性があります。この値を高く設定しすぎると、サーバが小さな MSS 値を使って応答したときに、接続が壊れる可能性があります。

- **WAN クライアントに送信する最大 TCP MSS** -MSS の値です。既定値は **1460**、最小値は 32、最大値は 1460 です。

メモ：プロキシ WAN クライアント接続を使用する際には、これらのオプションを控えめに設定するようにしてください。これらの値は、SYN フラッドが発生したときにのみ接続に適用されるためです。これにより、攻撃中でも正規の接続が続行されます。

- **受信した SYN パケットを常にログに記録する** - 受信したすべての SYN パケットをログします。

レイヤ 2 SYN/RST/FIN フラッド防御 - MAC ブラックリスト

SYN/RST/FIN ブラックリスト機能は、SYN、RST、FIN ブラックリスト攻撃しきい値を超えた機器のリストを表示します。ファイアウォール機器では、パケット評価プロセスの初期段階で、ブラックリストに含まれている機器から送信されたパケットを破棄します。これにより、このようなパケットをファイアウォールでより多く処理できるようになり、ローカル ネットワークから発生した攻撃に対する防御と、WAN ネットワークに対するレイヤ 2防御が実現されます。

デバイスを SYN/RST/FIN ブラックリストとウォッチリストの両方に追加することはできません。ブラックリストを有効にすると、ブラックリストしきい値を超えた機器がウォッチリストから削除され、ブラックリストに追加されます。逆に、ファイアウォールがブラックリストから機器を削除すると、その機器はウォッチリストに戻されます。MAC アドレスがブラックリストに登録された機器は、その機器からのフラッドが停止してから約 3 秒後にブラックリストから削除されます。

レイヤ 2 SYN/RST/FIN/TCP フラッド防御 - MAC ブラックリストの設定

- **SYN/RST/FIN/TCP フラッド ブラックリストのしきい値 (パケット/秒)** - 毎秒許容される SYN、RST、FIN、および TCP パケットの最大数を指定します。最小値は 10、最大値は 800,000、既定値は **1,000** です。ブラックリストは比較的強力なローカル攻撃や WAN ネットワークからの激しい攻撃の防止を目的としているため、このしきい値には SYN プロキシしきい値よりも大きな値を設定する必要があります。

メモ：「**すべてのインターフェースで SYN/RST/FIN/TCP フラッド ブラックリストを有効にする**」が有効になっていない場合、このオプションは変更できません。

- **すべてのインターフェースで SYN/RST/FIN/TCP フラッド ブラックリストを有効にする** - ファイアウォールのすべてのインターフェースでブラックリスト機能が有効になります。このオプションは、既定では選択されていません。このオプションを選択すると、以下のオプションが使用できるようになります。
  - **WAN のマシンはブラックリストに記録しない** - WAN 上のシステムが決して SYN ブラックリストに追加されないようにします。これはファイアウォールの WAN ポートに向けた /WAN ポートからのトラフィックを遮断することがあるため、非選択のままにすることを推奨します。このオプションは、既定では選択されていません。

- **SonicWall 管理トラフィックを常に許可する** - ブラックリストに登録された機器からファイアウォールの WAN IP アドレス宛てに送信される IP トラフィックが除外されなくなります。これにより管理トラフィックとルーティング プロトコルが許可され、ブラックリストに登録された機器を経由した接続を維持することができます。このオプションは、既定では選択されていません。

WAN DDOS 防御 (TCP 以外のフラッド)

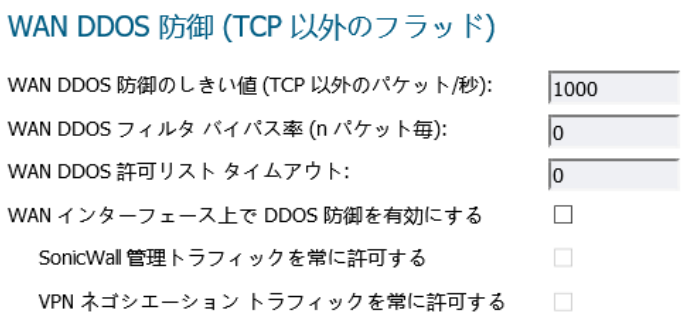
WAN DDOS 防御では、TCP 以外の DDOS 攻撃を防ぐことができます。したがって、TCP の SYN フラッドが懸念される場合、SYN フラッド防御と組み合わせて使用する必要があります。この機能の目的は、インターネットで TCP 以外のサービスを提供するよく知られたサーバ (中央の DNS サーバなど) の保護ではなく、LAN/DMZ 側で開始された TCP 以外のトラフィックの大部分が生じる LAN/DMZ ネットワークを保護することです。このネットワークでは WAN 側で開始されたトラフィックもわずかに生じる場合があります。

WAN DDOS 防御を有効にすると、WAN インターフェースで受信する非 TCP パケットのレートが追跡されます。非 TCP パケットのレートが指定のしきい値を超えると、WAN インターフェースで受信する非 TCP パケットはフィルタ処理されます。非 TCP パケットが転送されるのは、次の条件のうち少なくとも 1 つに該当する場合のみです。

- 送信元 IP アドレスが許可リストに含まれる
- そのパケットが SonicWall 管理トラフィックであり、「**SonicWall 管理トラフィックを常に許可する**」がオンである
- そのパケットが VPN ネゴシエーション トラフィック (IKE) であり、「**VPN ネゴシエーション トラフィックを常に許可する**」がオンである
- そのパケットが ESP パケットであり、ネットワーク セキュリティ装置で終了するトンネルの SPI と一致する
- そのパケットは、「**WAN DDOS フィルタ バイパス率 (n パケット毎)**」に指定された値と一致する *n* 個目のパケットである

これらの条件のいずれにも一致しないパケットは、パケット処理の早い段階で破棄されます。

「**WAN DDOS 防御 (TCP 以外のフラッド)**」は、「**管理 | セキュリティ設定 > ファイアウォール設定 > フラッド防御**」ページで設定します。



トピック:

- WAN DDOS 防御のしきい値 (TCP 以外のパケット/秒) (60 ページ)
- WAN DDOS フィルタ バイパス率 (*n パケット毎*) (60 ページ)
- WAN DDOS 許可リスト タイムアウト (60 ページ)
- WAN インターフェース上で DDOS 防御を有効にする (60 ページ)

WAN DDOS 防御のしきい値 (TCP 以外のパケット/秒)

「**WAN DDOS 防御のしきい値**」は、ホスト、範囲、またはサブネットへの送信が許可される 1 秒あたりの非 TCP パケット数の最大値を指定します。このしきい値を超えると WAN DDOS フラッド防御が始動されます。既定の非 TCP パケット数は 1000 です。最小値は 0、最大値は 10000000 です。

WAN DDOS フィルタ バイパス率 (*n* パケット毎)

フィルタ バイパス率を 0 以外にすると、通常なら WAN DDOS 防御で破棄される非 TCP パケットが破棄されず、LAN/DMZ ネットワークに渡されます。バイパス率では潜在的な攻撃を調整できますが、完全には遮断できません。送信元が許可リストに含まれていなくても一部のパケットの通過を許可することで、正当な WAN 側のホストからのパケットを LAN/DMZ 側に通過させるメカニズムを提供でき、応答が許可リストに入力されることによって、正当な WAN 側のホストからのそれ以降の非 TCP パケットが常に転送されるようになります。

フィルタ バイパス率の既定値は 0 なので、ヒューリスティックを試行するには、その前にこの値を変更する必要があります。フィルタ バイパス率を 0 以外にすると、許可リストの内容に関係なく、その値が表す割合でパケットが転送されます。例えば、この値を 2 に設定した場合、パケットが 1 つおきに LAN/DMZ ネットワークに転送されます (ポリシーなどを満たしている場合)。また、この値を 100 に設定した場合は、100 個目ごとに 1 つのパケットが転送されます。どの値が適切であるかは、潜在的な LAN 側のターゲット マシンの機能や、ユーザのネットワークの正当な非 TCP トラフィックのパターンの性質によって異なります。

WAN DDOS 許可リスト タイムアウト

ユーザが許可リスト タイムアウトを 0 以外に指定すると、設定した時間に許可リストのエントリが期限切れになります。許可リスト タイムアウトを 0 にすると、エントリは無期限になります。いずれの場合も、リスト内に未使用エントリがなくなると、特定のハッシュバケットで最も長い時間使用されていないエントリを新しいエントリに置き換えることができます。

WAN インターフェース上で DDOS 防御を有効にする

「**WAN インターフェース上で DDOS 防御を有効にする**」をオンにすると (既定では無効になっています)、次の 2 つのオプションが設定可能になります。

- SonicWall 管理トラフィックを常に許可する (60 ページ)
- VPN ネゴシエーション トラフィックを常に許可する (60 ページ)

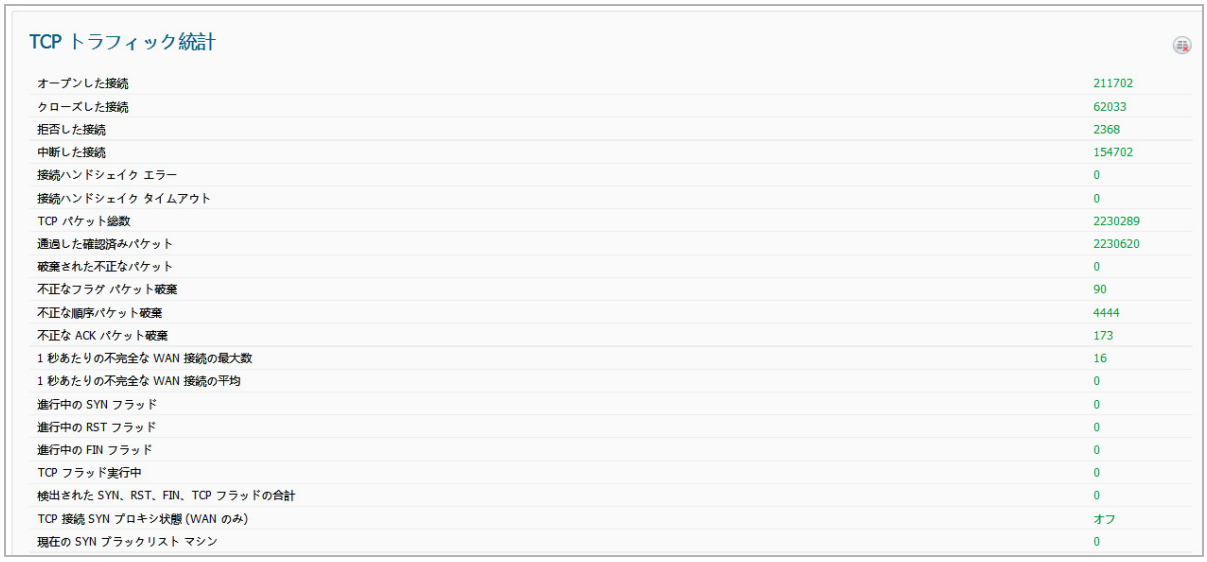
SonicWall 管理トラフィックを常に許可する

「**SonicWall 管理トラフィックを常に許可する**」を有効にすると (既定では無効になっています)、SonicWall 装置が TCP 以外の DDOS 攻撃を受けているときにも、装置の管理に必要なトラフィックは WAN ゲートウェイの通過を許可されます。

VPN ネゴシエーション トラフィックを常に許可する

「**VPN ネゴシエーション トラフィックを常に許可する**」を有効にすると (既定では無効になっています)、装置が TCP 以外の DDOS 攻撃を受けているときにも VPN のネゴシエーションが可能です。

TCP トラフィック統計



TCP トラフィック統計 テーブルに、「**TCP トラフィック統計**」テーブル内のエントリの説明を示します。テーブルに表示されている統計を消去して最初からやり直すには、テーブルの「**統計のクリア**」アイコンを選択します。

TCP トラフィック統計

統計	カウントアップ/表示の条件
オープンした接続	TCP 接続の開始側が SYN を送信したとき、または TCP 接続の応答側が SYN を受信したとき。
クローズした接続	開始側と応答側の両方が FIN を送信し ACK を受信して、TCP 接続が閉じられたとき。
拒否した接続	RST が検出され、応答側が SYN_RCVD 状態であるとき。
中断した接続	RST が検出され、応答側が SYN_RCVD 以外の状態であるとき。
接続ハンドシェイク エラー	ハンドシェイク エラーが発生したとき。
接続ハンドシェイク タイムアウト	ハンドシェイクがタイムアウトになったとき。
TCP パケット総数	TCP パケットが処理されるたび。
通過した確認済みパケット	次の場合にカウントアップされます。 • チェックサム妥当性検査で TCP パケットが合格したとき (TCP チェックサム妥当性検査が有効化されている場合)。 • 有効な SYN パケットが検出されたとき (SYN フラッド防御が有効化されている場合)。 • ACK フラグが設定されたパケットで SYN Cookie が妥当性検査に合格したとき (SYN フラッド防御が有効化されている場合)。

TCP トラフィック統計

統計	カウントアップ/表示の条件
破棄された不正なパケット	次の場合にカウントアップされます。 • TCP チェックサム妥当性検査で不合格になったとき (TCP チェックサム妥当性検査が有効化されている場合)。 • TCP SACK 許可オプションが検出されたが、計算されたオプションの長さが正しくないとき。 • TCP MSS (Maximum Segment Size) オプションが検出されたが、計算されたオプションの長さが正しくないとき。 • 計算された TCP SACK オプション データが最小サイズの 6 バイトを下回っているか、4 バイトのブロック サイズに適合しないとき。 • TCP オプションの長さが不正であると判断されたとき。 • 計算された TCP ヘッダーの長さが最小サイズの 20 バイトを下回ったとき。 • 計算された TCP ヘッダーの長さがパケットのデータ長よりも大きいとき。

不正なフラグ パケット破棄	次の場合にカウントアップされます。
	• 受信された SYN 以外のパケットを接続キャッシュ内で特定できないとき (SYN フラッド防御が無効化されている場合)。
	• セッションの確立中に、SYN、RST+ACK、SYN+ACK 以外のフラグが設定されたパケットが受信されたとき (SYN フラッド防御が有効化されている場合)。
	  • パケットに FIN、URG、PSH フラグが設定されている場合は、TCP XMAS スキャンがログに記録されます。
	  • パケットに FIN フラグが設定されている場合は、TCP FIN スキャンがログに記録されます。
	  • パケットにフラグが設定されていない場合は、TCP Null スキャンがログに記録されます。
	• SYN フラグとともに他の何らかのフラグが設定されているパケットによって新しい TCP 接続の開始が試行されたとき。
	• 確立済みの TCP セッション内で、SYN フラグの設定されたパケットが受信されたとき。
	• 確立済みの TCP セッション内で、ACK フラグの設定されていないパケットが受信されたとき。

不正な順序パケット破棄	次の場合にカウントアップされます。 • 確立済みの接続で受信されたパケットのシーケンス番号が、その接続の最も古い未承認シーケンス番号よりも小さい場合。 • 確立済みの接続で受信されたパケットのシーケンス番号が、その接続の最も古い未承認シーケンス番号にその接続で前回告知されたウィンドウ サイズを加えた数値よりも大きい場合。
不正な ACK パケット破棄	不正な ACK パケットが破棄されたとき。

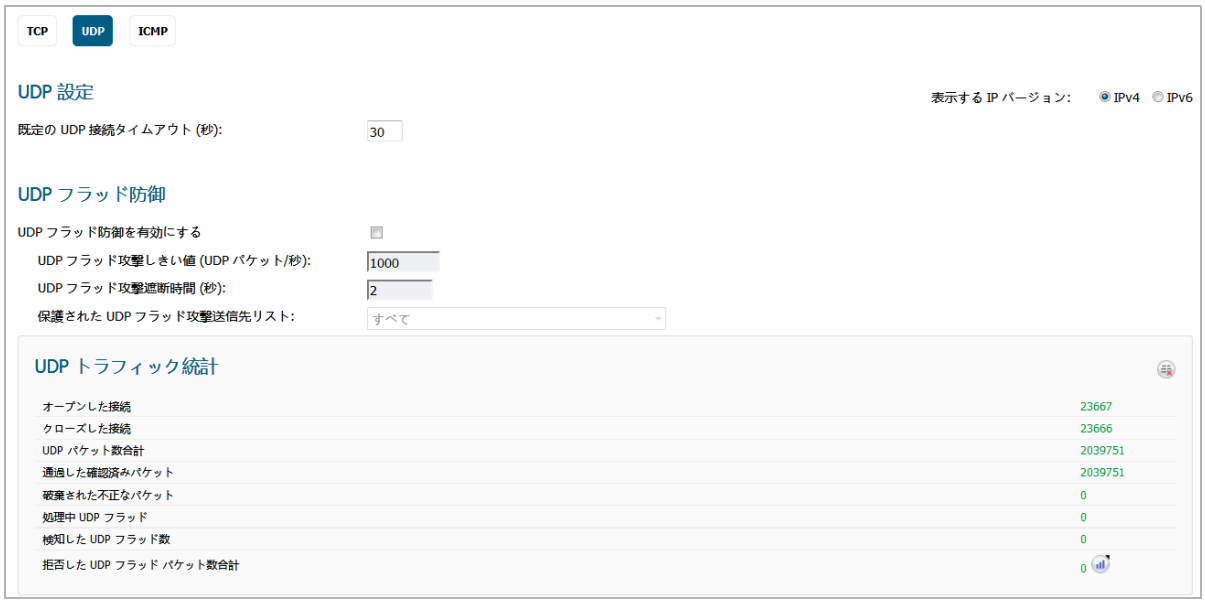
TCP トラフィック統計

統計	カウントアップ/表示の条件
1 秒あたりの不完全な WAN 接続の最大数	次の場合にカウントアップされます。 • 受信されたパケットに ACK フラグが設定されていて、かつ、RST および SYN フラグがどちらも設定されていない場合に、SYN Cookie が不正であると判断されたとき (SYN フラッド防御が有効化されている場合)。 • パケットの ACK 値 (シーケンス番号の乱数化オフセットにより調整された値) が接続の最も古い未承認シーケンス番号よりも小さいとき。 • パケットの ACK 値 (シーケンス番号の乱数化オフセットにより調整された値) が、接続で次に予測されるシーケンス番号よりも大きいとき。
1 秒あたりの不完全な WAN 接続の平均	1 秒あたりの不完全な WAN 接続数の平均値。
進行中の SYN フラッド	SYN フラッドが検知されたとき。
進行中の RST フラッド	RST フラッドが検知されたとき。
進行中の FIN フラッド	FIN フラッドが検知されたとき。
TCP フラッド実行中	TCP フラッドが検知されたとき。
検出された SYN、RST、FIN、TCP フラッドの合計	検出されたフラッド (SYN、RST、FIN、TCP) の総数。
TCP 接続 SYN プロキシ状態 (WAN のみ)	(WAN の場合のみ) TCP 接続 SYN プロキシが有効化どうかを示します。
現在の SYN ブラックリスト マシン	機器が SYN ブラックリストに登録されたとき。
現在の RST ブラック リスト マシン	機器が RST ブラックリストに登録されたとき。
現在の FIN ブラックリスト マシン	機器が FIN ブラックリストに登録されたとき。
現在の TCP ブラックリスト マシン	機器が TCP ブラックリストに登録されたとき。
SYN ブラックリスト イベント総数	SYN ブラックリストへの登録イベントが検知されたとき。
RST ブラックリスティング イベントの合計	RST ブラックリストへの登録イベントが検知されたとき。
FIN ブラックリスティング イベントの合計	FIN ブラックリストへの登録イベントが検知されたとき。
TCP ブラックリスト イベント合計	TCP ブラックリストへの登録イベントが検知されたとき。
拒否された SYN ブラックリスト パケットの合計	SYN ブラックリスト登録によって拒否された SYN パケットの総数。
拒否された RST ブラックリスト パケットの合計	SYN ブラックリスト登録によって拒否された RST パケットの総数。

TCP トラフィック統計

統計	カウントアップ/表示の条件
拒否された FIN ブラックリスト パケットの合計	SYN ブラックリスト登録によって拒否された FIN パケットの総数。
拒否された TCP ブラックリスト パケット合計	SYN ブラックリスト登録によって拒否された TCP パケットの総数。
受信した不正な SYN フラッド Cookie	SYN フラッド Cookie を受信したとき。
WAN DDoS フィルタ状況	DDOS フィルタが有効であるか無効であるかが表示されます。
WAN DDOS フィルタ - 拒否されたパケット	WAN DDOS フィルタによってパケットが拒否されたとき。
WAN DDOS フィルタ - 漏洩したパケット	WAN DDOS フィルタが、漏洩したパケットを拒否するとき。
WAN DDOS フィルタ - 許可リスト カウント	WAN DDOS フィルタが、許可リストのパケットを処理するとき。

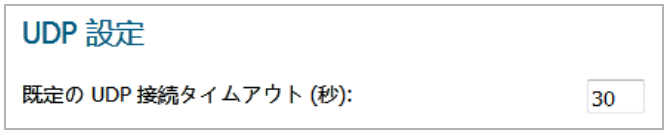
「UDP」ビュー



トピック:

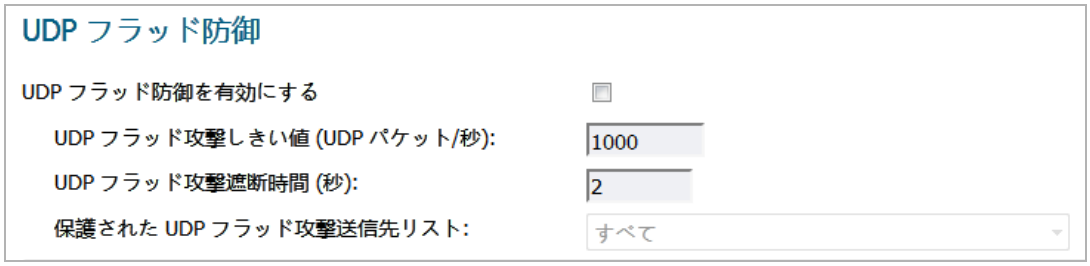
- UDP の設定 (65 ページ)
- UDP フラッド防御 (65 ページ)
- UDP トラフィック統計 (66 ページ)

UDP の設定



- **既定の UDP 接続タイムアウト (秒)** - UDP 接続がタイムアウトするまでの無動作時間を示す秒数。この値よりも、個別ルールで設定する UDP 接続タイムアウトが優先されます。

UDP フラッド防御



UDP フラッド攻撃は、サービス拒否 (DoS) 攻撃の一種です。リモート ホストのランダムなポートに対して大量の UDP パケットを送信することで開始されます。その結果、攻撃対象となったシステムのリソースが攻撃パケットの処理のために消費され、他のクライアントがシステムに到達できない状態に陥ります。

SonicWall UDP フラッド防御は、"監視と遮断" 手法で、このような攻撃からシステムを保護します。装置は、特定の送信先への UDP トラフィックを監視します。1 秒あたりの UDP パケット数が、指定の時間内で許容されるしきい値を超えた場合、装置はそれ以降に受信される UDP パケットを破棄してフラッド攻撃を撃退します。

UDP フラッド防御の状態に関係なく、装置で設定された DNS サーバとやり取りされる DNS のクエリや応答に使う UDP パケットは通過が許可されます。

UDP フラッド防御を設定するには、次の設定を使用します。

- **UDP フラッド防御を有効にする** - UDP フラッド防御を有効にします。このオプションは、既定では選択されていません。

  メモ：その他の「**UDP フラッド防御**」オプションをアクティブにするには、「**UDP フラッド防御を有効にする**」を有効にする必要があります。

- **UDP フラッド攻撃しきい値 (UDP パケット/秒)** - UDP フラッド防御を始動させるホスト、範囲、またはサブネットに送信される UDP パケットの 1 秒あたりの許容最大パケット数。このしきい値を超えると UDP フラッド防御が始動されます。最小値は 50、最大値は 1000000、既定値は **1000** です。

- **UDP フラッド攻撃遮断時間 (秒)** - 秒毎の UDP パケット数が攻撃しきい値を超え、その状態がここに指定した時間に達するまで継続した場合、UDP フラッド防御が有効化され、装置はそれ以降に受信される UDP パケットを破棄し始めます。最小値は 1 秒、最大値は 120 秒、既定値は **2** 秒です。

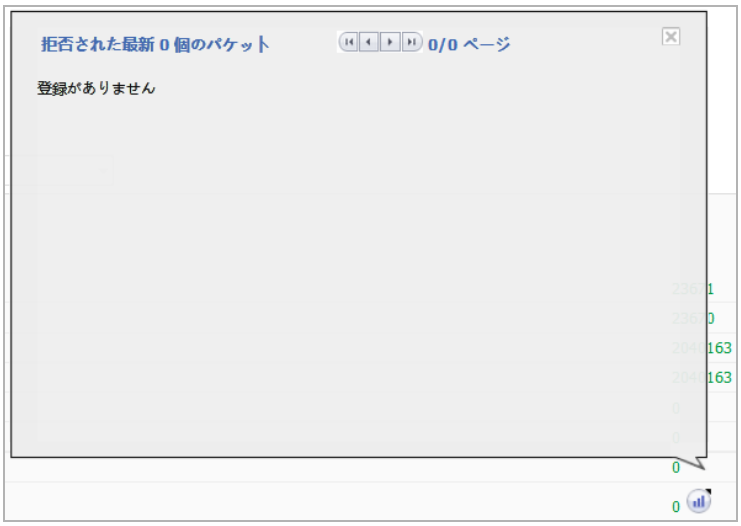
- **保護された UDP フラッド攻撃送信先リスト** - UDP フラッド防御で保護する送信先アドレス オブジェクトまたはアドレス グループ。既定値は「**すべて**」です。

  ヒント：ファイアウォールを通過する UDP パケットの合計に攻撃しきい値を適用するには、「**すべて**」を選択します。

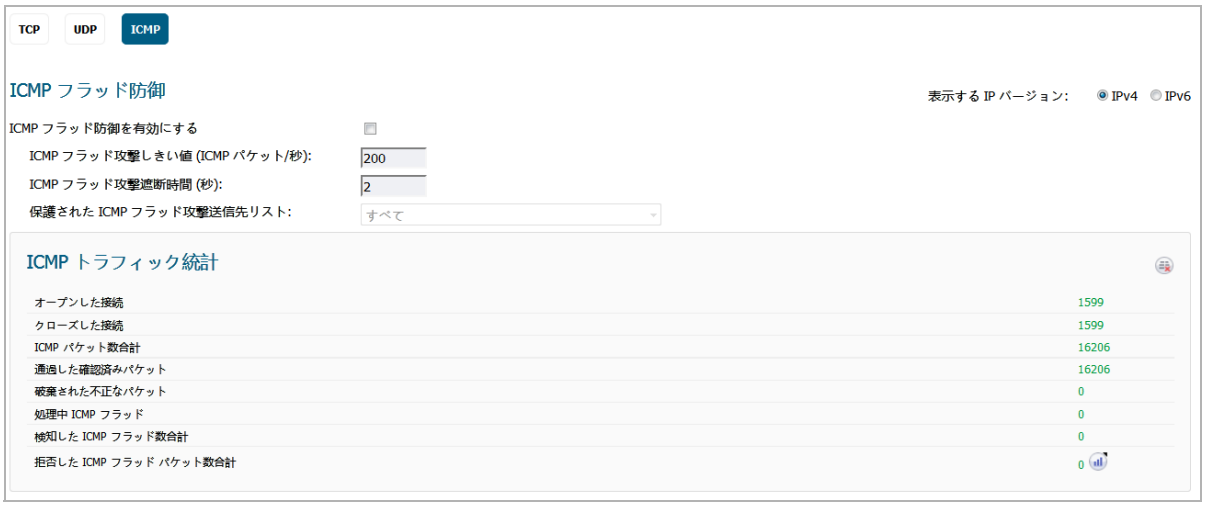
UDP トラフィック統計

「**UDP トラフィック統計**」テーブルには、UDP トラフィック統計 テーブルに示す統計が表示されます。テーブルに表示されている統計を消去して最初からやり直すには、テーブルの「**統計のクリア**」アイコンを選択します。

UDP トラフィック統計

統計	カウントアップ/表示の条件
オープンした接続	接続がオープン状態になったとき。
クローズした接続	接続がクローズされたとき。
UDP パケット数合計	UDP パケットが処理されるたび。
通過した確認済みパケット	チェックサム妥当性検査で UDP パケットが合格したとき (UDP チェックサム妥当性検査が有効化されている場合)。
破棄された不正なパケット	次の場合にカウントアップされます。 • UDP チェックサム妥当性検査で不合格になったとき (UDP チェックサム妥当性検査が有効化されている場合)。 • 計算された UDP ヘッダーの長さがパケットのデータ長よりも大きいとき。
処理中 UDP フラッド	現在、UDP フラッド攻撃しきい値を超えている個々の転送機器の数。
検知した UDP フラッド数	転送機器が UDP フラッド攻撃しきい値を超えたイベントの総数。
拒否した UDP フラッド パケット数合計	UDP フラッド攻撃の検出によって破棄されたパケットの総数。 **統計**アイコンを選択すると、ごく最近に拒否されたパケット数を示すポップアップ ダイアログが表示されます。 

「ICMP」ビュー



トピック:

- 表示する IP バージョン (67 ページ)
- ICMP/ICMPv6 フラッド防御 (67 ページ)
- ICMP/ICMPv6 トラフィック統計 (68 ページ)

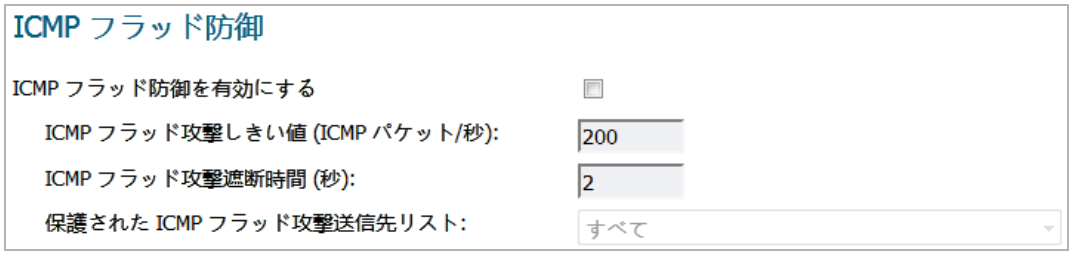
表示する IP バージョン

「**表示する IP バージョン**」で、IP バージョンを選択できます。**IPv4** または **IPv6**) を指定できます。選択した内容によって表示が異なります。

- **IPv4** を選択した場合、見出しとオプションには ICMP と表示されます。
- **IPv6** を選択した場合、見出しとオプションには ICMPv6 と表示されます。

ICMP/ICMPv6 フラッド防御

ICMP フラッド防御は、監視対象が ICMP/ICMPv6 フラッド攻撃であることを除き、UDP フラッド防御と同じ動作をします。唯一の違いは、ICMP フラッド防御では DNS クエリの通過が許可されないことです。



- **ICMP フラッド防御を有効にする** - ICMP フラッド防御を有効にします。

  メモ：その他の「ICMP フラッド防御」オプションをアクティブにするには、「**ICMP フラッド防御を有効にする**」を有効にする必要があります。

- **ICMP フラッド攻撃しきい値 (ICMP パケット/秒)** - ホスト、範囲、またはサブネットへの送信が許可される秒毎の ICMP パケット数の最大値。このしきい値を超えると ICMP フラッド防御が始動されます。最小値は 10、最大値は 100000 で、既定値は **200** です。
- **ICMP フラッド攻撃遮断時間 (秒)** - 秒毎の ICMP パケット数が攻撃しきい値を超え、その状態がここに指定した時間に達するまで継続した場合、ICMP フラッド防御が有効化され、装置はそれ以降に受信される ICMP パケットを破棄し始めます。最小値は 1 秒、最大値は 120 秒、既定値は **2** 秒です。
- **保護された ICMP フラッド攻撃送信先リスト** - ICMP フラッド防御で保護する送信先アドレス オブジェクトまたはアドレス グループ。既定値は「**すべて**」です。

  ヒント：ファイアウォールを通過する ICMP パケットの合計に攻撃しきい値を適用するには、「**すべて**」を選択します。

ICMP/ICMPv6 トラフィック統計

「**ICMP トラフィック統計**」テーブルには、ICMP/ICMPv6 トラフィック統計 テーブルに示す統計が表示されます。テーブルに表示されている統計を消去して最初からやり直すには、テーブルの「**統計のクリア**」アイコンを選択します。

ICMP/ICMPv6 トラフィック統計

統計	カウントアップ/表示の条件
オープンした接続	接続がオープン状態になったとき。
クローズした接続	接続がクローズされたとき。
UDP パケット数合計	ICMP/ICMPv6 パケットが処理されるたび。
通過した確認済みパケット	チェックサム妥当性検査で ICMP/ICMPv6 パケットが合格したとき (ICMP/ICMPv6 チェックサム妥当性検査が有効化されている場合)。
破棄された不正なパケット	次の場合にカウントアップされます。 • ICMP/ICMPv6 チェックサム妥当性検査で不合格になったとき (ICMP/ICMPv6 チェックサム妥当性検査が有効化されている場合)。 • 計算された ICMP/ICMPv6 ヘッダーの長さがパケットのデータ長よりも大きいとき。
処理中 ICMP/ICMPv6 フラッド	現在、ICMP/ICMPv6 フラッド攻撃しきい値を超えている個々の転送機器の数。

ICMP/ICMPv6 トラフィック統計

統計	カウントアップ/表示の条件
検知した ICMP/ICMPv6 フラッド数合計	転送機器が ICMP/ICMPv6 フラッド攻撃しきい値を超えたイベントの総数。
拒否した ICMP/ICMPv6 フラッド パケット数合計	ICMP/ICMPv6 フラッド攻撃の検出によって破棄されたパケットの総数。**統計** アイコンを選択すると、ごく最近に拒否されたパケット数を示すポップアップ ダイアログが表示されます。 

4

ファイアウォール マルチキャストの設定

- ファイアウォール設定 > マルチキャスト (70 ページ)
- マルチキャスト設定 (71 ページ)
- IGMP 状態テーブル (73 ページ)
- IGMP 状態テーブル (73 ページ)
- マルチキャストの有効化 (73 ページ)

ファイアウォール設定 > マルチキャスト

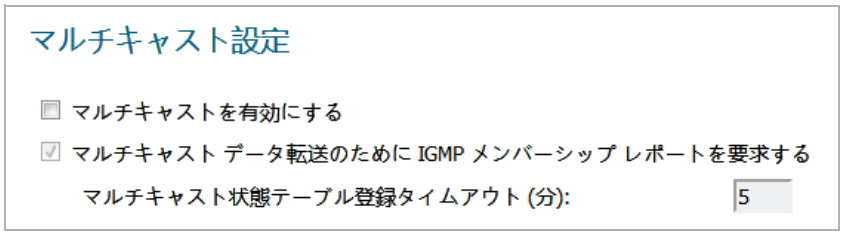
IP マルチキャストは、1 つのインターネット プロトコル (IP) パケットを同時に複数のホストに送信する手法です。マルチキャストは、インターネット トラフィックで急速に大きな位置を占めつつあるマルチメディア プレゼンテーションおよびビデオ会議に適しています。例えば、1 つのホストからオーディオ ストリームとビデオ ストリームが送信され、そのストリームを 10 個のホストで受信するとします。マルチキャストの場合、送信側ホストは特定のマルチキャスト アドレスを使って 1 つの IP パケットを送信します。受信側の 10 個のホストでは、そのアドレス宛てのパケットをリッスンして受信するように設定するだけで済みます。マルチキャストは、コネクションレス モードで動作するポイント ツー マルチポイント IP 通信メカニズムです。 ホストでは、ラジオのように“チューニング"することでマルチキャスト送信ストリームを受信します。

「**管理 | セキュリティ設定 > ファイアウォール設定 > マルチキャスト**」ページで、ファイアウォール上のマルチキャスト トラフィックを管理できます。

トピック:

- マルチキャスト設定 (71 ページ)
- マルチキャスト ポリシー (71 ページ)
- IGMP 状態テーブル (73 ページ)
- LAN 専用インターフェースでのマルチキャストの有効化 (74 ページ)
- VPN を使用したマルチキャストの有効化 (75 ページ)

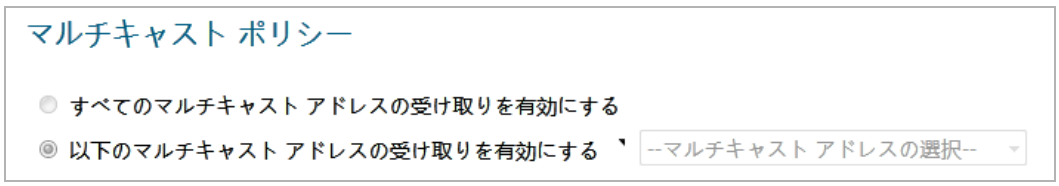
マルチキャスト設定



- **マルチキャストを有効にする** - マルチキャスト トラフィックをサポートするには、このオプションを選択にします。 このオプションは、既定では選択されていません。
- **マルチキャスト データ転送のために IGMP メンバーシップ レポートを要求する** - このオプションを選択すると、IGMP を使用してマルチキャスト グループ アドレスに追加されたインターフェースにのみマルチキャスト データを転送するように限定することで、パフォーマンスを向上します。このオプションは、マルチキャストが有効になっている場合にのみ使用できます。このオプションは、既定では選択されています。
- 「**マルチキャスト状態テーブル登録タイムアウト (分)**」- このフィールドの既定値は **5** です。このフィールドの値の範囲は 5～60 (分) です。以下のような場合、既定のタイムアウト値 5 を変更してください。
  - メンバーシップ問い合わせまたはメンバーシップ レポートがネットワーク上で失われている可能性がある。
  - ネットワーク上の IGMP トラフィックを減らしたいが、現在多数のマルチキャスト グループまたはマルチキャスト クライアントがある。これは、トラフィックをルーティングするルータがない状況の場合です。
  - IGMP ルータとタイミングを同期する必要がある。

マルチキャスト ポリシー

ヒント：これらのオプションを使用するには、マルチキャストを有効にする必要があります。



- 「**すべてのマルチキャスト アドレスの受け取りを有効にする**」- このラジオ ボタンは既定で無効になっています。このラジオ ボタンを選択すると、すべての (クラス D) マルチキャスト アドレスが受信されます。

  メモ：すべてのマルチキャスト アドレスを受信した場合、ネットワークのパフォーマンスが低下する可能性があります。

- 「**以下のマルチキャスト アドレスの受け取りを有効にする**」- このラジオ ボタンは既定で有効になっています。ドロップダウン メニューで、「**マルチキャスト オブジェクトの作成**」または「**マルチキャスト グループの作成**」を選択します。

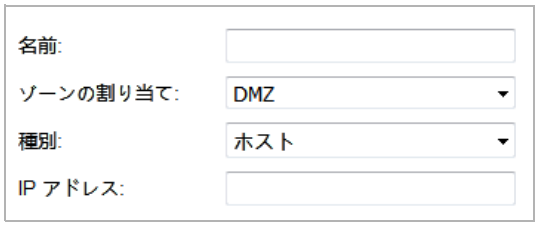
  メモ：MULTICAST ゾーンに関連付けられているアドレス オブジェクトおよびアドレス グループのみ選択できます。MULTICAST ゾーンに関連付けられるのは、224.0.0.1 ～ 239.255.255.255 の範囲のアドレスのみです。

  メモ：指定できるマルチキャスト アドレスは最大 200 個です。

マルチキャスト アドレス オブジェクトを作成するには:

1 「**マルチキャスト設定**」で、「**マルチキャストを有効にする**」を選択します。

2 「**マルチキャスト ポリシー**」の下にある「**以下のマルチキャスト アドレスの受け取りを有効にする**」ドロップダウン メニューで、「**マルチキャスト アドレス オブジェクトの作成**」を選択します。「**アドレス オブジェクトの追加**」ダイアログが表示されます。



3 「**名前**」フィールドでアドレス オブジェクトの名前を設定します。

4 「**ゾーンの割り当て**」ドロップダウン メニューから「**MULTICAST**」を選択します。

5 「**種別**」ドロップダウン メニューで、「**ホスト**」、「**範囲**」、「**ネットワーク**」、「**MAC**」、または「**FQDN**」を選択します。

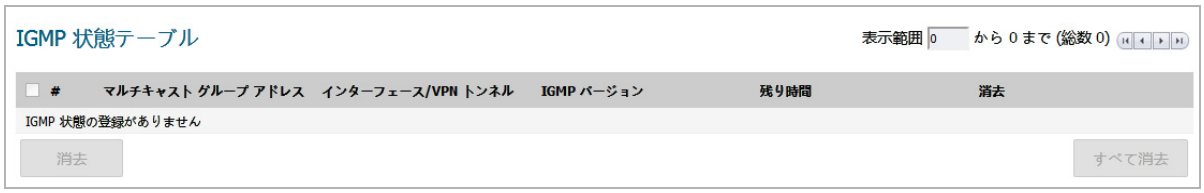
6 選択する**種別**に応じて、ダイアログのオプションは変化します。選択した内容によって次の手順が異なります。

種別	表示されるオプション
ホスト	**IP アドレス** - ホストまたはネットワークの IP アドレスを入力します。IP アドレスは、マルチキャストのアドレス範囲である224.0.0.0 ～ 239.255.255.255 の範囲内で指定する必要があります。
ネットワーク	• **ネットワーク** - ホストまたはネットワークの IP アドレスを入力します。IP アドレスは、マルチキャストのアドレス範囲である224.0.0.0 ～ 239.255.255.255 の範囲内で指定する必要があります。 • **ネットマスク/接頭辞長** - ネットワークのネットマスクを入力します。
範囲	「**開始アドレス**」と「**終了アドレス**」に、アドレス範囲の開始アドレスと終了アドレスを入力します。IP アドレスは、マルチキャストのアドレス範囲である224.0.0.1 ～ 239.255.255.255 の範囲内で指定する必要があります。

種別	表示されるオプション
MAC	• **MAC アドレス** - ホストまたはネットワークの MAC アドレスを入力します。 • **マルチホーム ホスト** - MAC アドレスがマルチホーム ホスト用である場合に選択します。 このオプションは、既定では選択されています。
FQDN	• **FQDN ホスト名** - ホストの完全修飾ドメイン名を入力します。 • **DNS 登録の TTL の手動設定 ... (120~86400 秒)** - DNS 登録の有効期間 (TTL またはホップ制限) を入力する場合に選択します。このオプションは、既定では選択されていません。選択すると、TTL フィールドがアクティブになります。範囲は 120 - 86400 秒です。

7 「**OK**」を選択します。

IGMP 状態テーブル



ここでは、**IGMP 状態テーブル**のフィールドについて説明します。

- 「**マルチキャスト グループ アドレス**」- インターフェースが属しているマルチキャスト グループ アドレスです。
- 「**インターフェース/VPN トンネル**」- VPN ポリシーのインターフェース (**LAN**など) です。
- 「**IGMP バージョン**」- IGMP バージョン (**V2** や **V3** など) を示します。
- **「残り時間」** - IGMP エントリが消去されるまでの残り時間です。
- **「消去」** - 特定のエントリを消去するためのアイコンが用意されています。
- 「**消去**」および「**すべて消去**」ボタン - 特定の登録を直ちに消去するには、その登録の左側にあるチェックボックスをオンにして、「**消去**」を選択します。すべての登録を直ちに消去するには、「**すべて消去**」ボタンを選択します。

マルチキャストの有効化

トピック:

- LAN 専用インターフェースでのマルチキャストの有効化 (74 ページ)
- VPN を使用したマルチキャストの有効化 (75 ページ)

LAN 専用インターフェースでのマルチキャストの有効化

トピック:

- LAN 専用インターフェースでのマルチキャストの有効化 (74 ページ)
- VPN トンネル経由でアドレス オブジェクトのマルチキャスト サポートを有効にする (74 ページ)

LAN 専用インターフェースでのマルチキャストの有効化

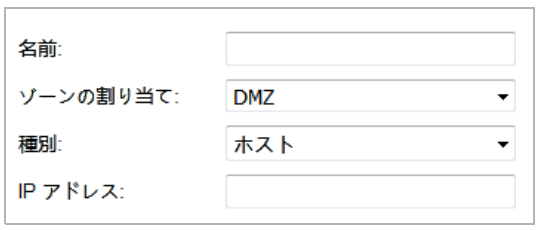
ファイアウォールの LAN 専用インターフェースのマルチキャスト サポートを有効化するには、以下の手順を実行します。

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > マルチキャスト**」ページに移動します。
2 「**マルチキャスト設定**」で、「**マルチキャストを有効にする**」を選択します。
3 「**マルチキャスト ポリシー**」で、「**すべてのマルチキャスト アドレスの受け取りを有効にする**」を選択します。
4 「**適用**」を選択します。
5 「**管理 | システム セットアップ > ネットワーク > インターフェース**」ページに移動します。
6 設定する LAN インターフェースの「**設定**」アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。
7 「**詳細設定**」を選択します。
8 「**マルチキャスト サポートを有効にする**」を選択します。
9 「**OK**」を選択します。

VPN トンネル経由でアドレス オブジェクトのマルチキャスト サポートを有効にする

VPN トンネルを使用してオブジェクトのマルチキャスト サポートを有効にするには、以下の手順を実行します。

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > マルチキャスト**」ページに移動します。
2 「**マルチキャスト設定**」で、「**マルチキャストを有効にする**」を選択します。
3 「**マルチキャスト ポリシー**」で、「**すべてのマルチキャスト アドレスの受け取りを有効にする**」を選択します。
4 ドロップダウン メニューから「**マルチキャスト アドレス オブジェクトの作成**」を選択します。「**アドレス オブジェクトの追加**」ダイアログが表示されます。



5 「**名前**」フィールドに、マルチキャスト アドレス オブジェクトの名前を入力します。

6 「**ゾーンの割り当て**」ドロップダウン メニューから、次のようにしてゾーンを選択します。「**DMZ**」、「**LAN**」、「**MULTICAST**」、「**SSLVPN**」、「**VPN**」、「**WAN**」、「**WLAN**」のいずれかのゾーンを選択します。

7 「**種別**」ドロップダウン メニューから種別を選択すると、選択内容に応じてその他のオプションが変わります。選択した内容によって表示が異なります。

- 「**ホスト**」を選択した場合は、「**IP アドレス**」フィールドに IP アドレスを入力します。
- 「**範囲**」を選択した場合は、「**開始アドレス**」フィールドと「**終了アドレス**」フィールドに開始アドレスと終了アドレスをそれぞれ入力します。
- 「**ネットワーク**」を選択した場合は「**ネットマスク**」フィールドにネットワーク IP アドレスを、「**ネットマスク/接頭辞長**」フィールドにネットマスクまたは接頭辞長を入力します。
- 「**MAC**」を選択した場合は、「**MAC アドレス**」フィールドに MAC アドレスを入力し、必要に応じて、「**マルチホーム ホスト**」チェックボックスをオンにします (既定でオンになっています)。
- 「**FQDN**」を選択した場合は、「**FQDN ホスト名**」フィールドに FQDN ホスト名を入力します。

8 「**OK**」を選択します。

9 「**管理 | 接続性 > VPN > 設定**」ページに移動します。

10 「**VPN ポリシー**」で、設定するグループ VPN ポリシーの**設定**アイコンを選択します。「**VPN ポリシー**」ダイアログが表示されます。

11 「**詳細設定**」を選択します。

12 「**詳細設定**」セクションで、「**マルチキャストを有効にする**」を選択します。

13 「**OK**」を選択します。

VPN を使用したマルチキャストの有効化

VPN を使用して WAN 全体でマルチキャストを有効にするには:

1 次のようにしてマルチキャストをグローバルに有効にします。

a 「**管理 | セキュリティ設定 > ファイアウォール設定 > マルチキャスト**」ページに移動します。

b 「**マルチキャストを有効にする**」を選択します。

c 「**適用**」ボタンを選択します。

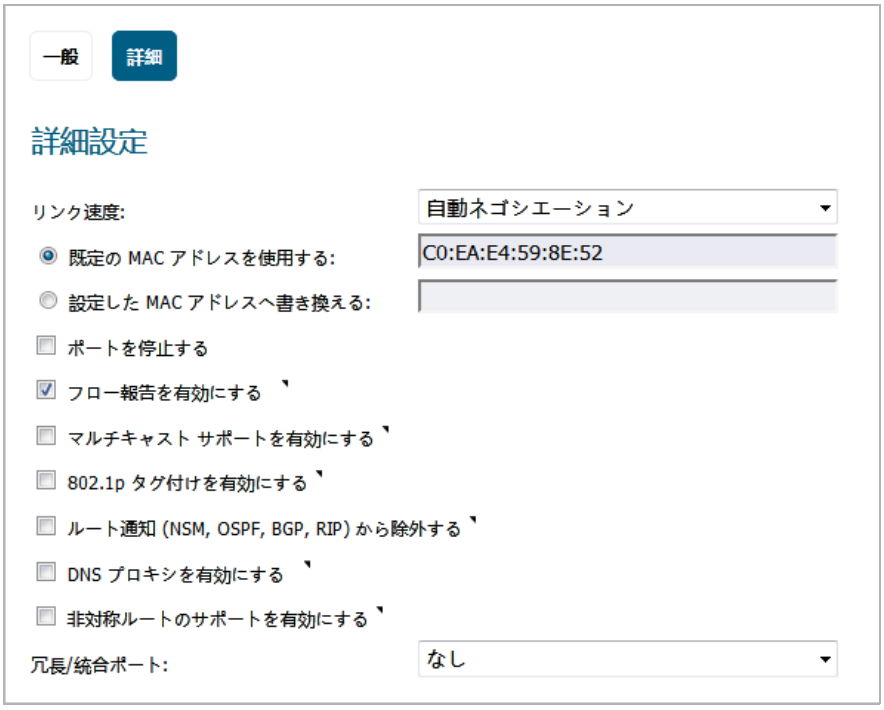
d 参加するすべてのセキュリティ装置のインターフェースごとに、ステップ a からステップ c を繰り返します。

2 マルチキャスト ネットワークに追加される各インターフェースで、マルチキャストのサポートを有効にします。

a 「**管理 | システム セットアップ > ネットワーク > インターフェース**」ページに移動します。

b 参加するインターフェースの**編集**アイコンを選択します。「**インターフェースの編集**」ダイアログが表示されます。

c 「**詳細設定**」を選択します。



d 「**マルチキャスト サポートを有効にする**」チェックボックスをオンにします。

e 「**OK**」を選択します。

f 参加するすべてのセキュリティ装置の参加インターフェースごとに、ステップ a からステップ e を繰り返します。

3 VPN ポリシーでセキュリティ装置間のマルチキャストを有効にします。

a 「**管理 | 接続性 > VPN > 基本設定**」ページに移動します。

b マルチキャスト処理が含まれているポリシーの**編集**アイコンを選択します。「**VPN ポリシー**」ダイアログが表示されます。

c 「**詳細設定**」を選択します。

メモ：既定では、WLAN の IGMP トラフィックに対する MULTICAST アクセス ルールは “禁止" に設定されています。追加するすべての装置について、WLAN ゾーンにマルチキャスト クライアントが存在する場合は、このアクセス ルールを “許可" に変更してマルチキャストを有効にする必要があります。

d 「**詳細設定**」セクションで、「**マルチキャストを有効にする**」を選択します。

e 「**OK**」を選択します。

4 サイト間でトンネルが動作していることを確認します。

5 マルチキャスト サーバ アプリケーションとクライアント アプリケーションを起動します。マルチキャスト サーバからマルチキャスト グループ (224.0.0.0 ～ 239.255.255.255) にマルチキャスト データが送信されると、ファイアウォールは IGMP 状態テーブルでそのグループを問い合わせ、データの転送先を決定します。同様に、装置が VPN ゾーンでデータを受信した場合も、IGMP 状態テーブルへの問い合わせによってデータの転送先を決定します。

IGMP 状態テーブル (更新直後) に、X3インターフェース上と 224.15.16.17 グループの vpnMcastServer トンネルにマルチキャスト クライアントがある旨の情報が示されます。

メモ：「すべてのマルチキャスト アドレスの受け取りを有効にする」を選択すると、「**IGMP 状態**」テーブルを表示したときに、想定外のエントリが表示される場合があります。この現象は、ホストで他のマルチキャスト アプリケーションが動作していることが原因で発生します。

5

サービス品質の管理

- ファイアウォール設定 > サービス品質の割付 (78 ページ)
- 分類 (78 ページ)
- 級割 (79 ページ)
- 制限 (80 ページ)
- 802.1p と DSCP QoS (81 ページ)
- 帯域幅管理 (93 ページ)
- 用語集 (93 ページ)

ファイアウォール設定 > サービス品質の割付

QoS (Quality of Service: サービス品質) とは、予測可能なネットワークの動作と性能を提供することを目的とした多様な方式を指します。この予測可能な性質は、VoIP (Voice over IP)、マルチメディア コンテンツ、発注システムやクレジット カード決済システムなどの重要な商用アプリケーションなどの特定の種類のアプリケーションにとって、極めて重要です。この種類の予測可能性は、帯域幅量の調整では実現されません。なぜなら、ネットワークにおいては帯域幅をどんなに増やしても任意の時点でその容量まで使い果たされる結果になるためです。QoS を正しく設定し実装することによってのみ、トラフィックを適切に管理し、望ましいレベルのネットワーク サービスを保証することが可能になります。

トピック:

- 分類
- 級割
- 制限
- 802.1p と DSCP QoS
- 帯域幅管理
- 用語集

分類

分類は、管理の必要なトラフィックを識別するための最初の手順として必要です。SonicOS では、トラフィックを分類するためのインターフェースとして、アクセス ルールを使用します。これにより、アドレス オブジェクト、サービス オブジェクト、スケジュール オブジェクトの要素の組み合わせを使用した、きめの細かい制御が提供されます。分類基準は、"**すべての HTTP トラフィック**" のよ

うに大まかに設定することも、"**毎週水曜日午前 2:12 のホスト A からサーバ B への SSH トラフィック**"のように詳細に設定することもできます。

SonicWall ネットワーク セキュリティ装置では、業界標準の外部の CoS 識別子、DSCP、802.1p を認識、割付、編集、生成することができます (802.1p と DSCP QoS (81 ページ) を参照してください)。

トラフィックは、識別または分類されると、管理可能になります。管理は、ネットワークが完全な自律システムである限り、完璧に効果的な SonicOS の帯域幅管理 (BWM) により内部的に実行されます。未知の構成の外部ネットワーク インフラ、または、帯域幅を争う他のホスト (例えば、インターネット) などのような、外部または中間の要素と一旦遭遇すると、保証と予測を提供する能力は低下します。言い換えれば、ネットワークのエンドポイントとその間にあるものがすべて管理内にある限りは、BWM は設定したとおりに動作します。一旦外部の要素が持ち込まれると、BWM の精度と有効性は低下し始めます。

しかし、すべてが失われるわけではありません。SonicOS でトラフィックを分類する場合、トラフィックに**タグを付ける**ことができます。この分類を CoS タグによって保持することができる特定の外部システムに通知することで、これらの外部システムも QoS の提供に関与することができます。

メモ：多くのサービス プロバイダは、802.1p や DSCP などの CoS タグをサポートしていません。また、標準的な設定のほとんどのネットワーク機器は、802.1p タグを認識できずに、タグ付けされたトラフィックを破棄します。

DSCP は互換性の問題を発生しませんが、多くのサービス プロバイダは、コード ポイントに関係なく、DSCP タグを単に取り除くか、無視します。

会社のネットワークまたはサービス プロバイダのネットワーク上で 802.1p または DSCP 級割を使用する場合は、これらの方式がサポートされていることを最初に確認する必要があります。内部ネットワーク機器が CoS 優先級割をサポートできること、およびこのサポートを提供するために正しく設定されていることを確認します。サービス プロバイダに確認します (CoS 方式を使用したQoS サポートを有償で提供しているところもあります)。

級割

トラフィックを分類した後、QoS 対応外部システム (例えば、プレミアム サービス プロバイダのインフラストラクチャかプライベート WAN 上で利用可能な、CoS 対応のスイッチやルータ) により処理されることになっている場合、トラフィックにタグを付けて、外部システムが分類を利用して適切な処理とホップ単位動作 (PHB) を提供できるようにする必要があります。

元々、これは RFC791 の 3 つの優先順位ビットと RFC1394 の ToS (サービス タイプ) フィールドとともに IP 層 (第 3 層) で試みられました。 これは、歴史を通じて、総勢 17 名が使用しました。後継の RFC2474 では、より実用的で広範囲にわたって使用することのできる、64 個までの分類とユーザ定義等級を提供する DSCP (Differentiated Services Code Point) が採用されています。DSCP は、RFC2598 (専用線の動作を提供するための緊急転送) と RFC2697 (等級内部での保証転送レベル。 金、銀、銅レベルとしても知られている) によりさらに拡張されました。

DSCP は、非互換の危険性がないので、パブリック ネットワークを通過するトラフィックのための安全な級割方式です。最悪の場合、パスに沿ったホップでは、DSCP タグが無視されるか除去される可能性がありますが、パケットの誤処理や破棄はほとんど発生しません。

CoS 級割のもう 1 つの一般的な方式は、IEEE802.1p です。802.1p は、MAC 層 (第 2 層) で動作し、実際には IEEE 802.1D 標準で定義されていますが、(同じ 16 ビット フィールドを共有して) IEEE 802.1Q VLAN 級割と密接に関連しています。DSCP とは異なり、802.1p は、802.1p 対応機器でのみ動作し、広く相互利用が可能であるわけではありません。さらに、802.1p は異なるパケット構造を持つので、広域ネットワークや、プライベート WAN をほとんど通過できません。それでもなお、802.1p は、ボイスやビデオ オーバー IP ベンダーの間で、幅広い支持を得ています。そこで、ネットワークの境界 (例えば、

WAN リンク) を横断する 802.1p をサポートするためのソリューションが、**802.1p を DSCP へ割り付ける**形で導入されました。

802.1p の DSCP への割付では、パケットが安全に WAN リンクを通過できるようにするために、ある LAN からの 802.1p タグが SonicOS によって DSCP の値に割り付けられます。パケットがWAN または VPN の反対側に到着すると、受信側 SonicOS 装置により、DSCP タグが LAN で使用するために 802.1p タグに戻されます。詳細については、802.1p と DSCP QoS (81 ページ) を参照してください。

制限

トラフィックは、利用可能な多くのポリシング、キューイング、シェイピングのどれかを使用して、制限 (管理) することができます。SonicOS は、帯域幅管理 (93 ページ) に詳しく説明されている、送信および受信帯域幅管理 (BWM) による内部的な制限機能を提供します。SonicOSの BWM は、十分な帯域幅を持つ完全な自律プライベート ネットワークにとって完璧に効果的なソリューションですが、より未知の外部ネットワーク要素や、帯域幅の競合に遭遇した場合に、効果的でなくなることがあります。競合の問題については、DSCP 級割: サンプル シナリオを参照してください。

トピック:

- QoS 対応ネットワークでのサイト間 VPN (80 ページ)
- パブリック ネットワークでのサイト間 VPN (80 ページ)

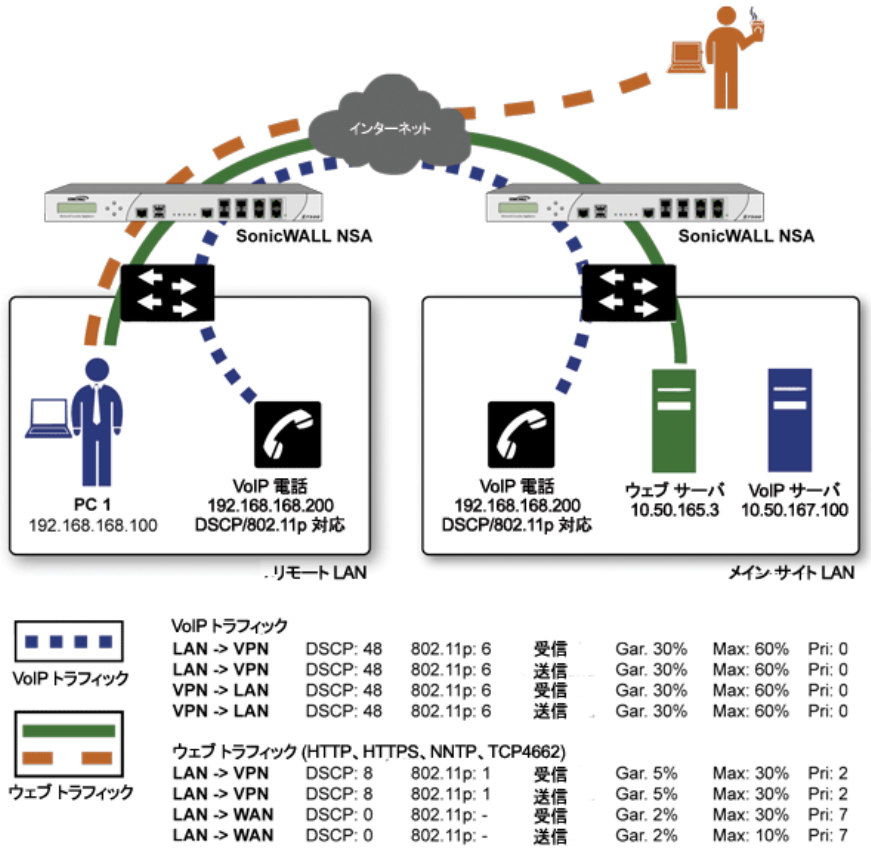
QoS 対応ネットワークでのサイト間 VPN

2 つのエンド ポイント間のネットワーク パスが QoS に対応している場合、SonicOS は、内部カプセル化パケットがトンネルの反対側で正常に解釈されるように DSCP タグを付けてることができます。 さらに、外部 ESP カプセル化パケットに DSCP タグを付けて、通過ネットワークの各ホップでその等級が解釈および適用されるようにできるようにすることもできます。SonicOS は、通過ネットワークを安全に通過できるように、内部ネットワークで作成された 802.1p タグを DSCP タグに割り当てることができます。パケットが反対側に到着すると、受信側 SonicWall 装置は、DSCP タグを内部ネットワークで解釈および適用できるように 802.1p タグに逆変換できます。

パブリック ネットワークでのサイト間 VPN

SonicOS 統合 BWM は、両方のエンド ポイントで受信トラフィックと送信トラフィックを分類および制御できるので、VPN 接続ネットワーク間のトラフィックを管理するのに非常に効果的です。エンド ポイント間のネットワークが QoS に対応していない場合、すべての VPN ESP は等しく認識および処理されます。通常、これらの中間ネットワークまたはそのパスに対する制御は行われないため、QoS を完全に保証することは困難ですが、より予測可能な動作を提供するのに役立ちます。

パブリック ネットワークでのサイト間 VPN



エンド ツー エンド QoS を提供するために、ビジネス クラスのサービス プロバイダは、彼らの IP ネットワーク上でトラフィックの制限サービスを提供するようになりました。通常、これらのサービスは、トラフィックの分類およびタグ付けに関して顧客の設備に依存します (一般に、DSCP などの標準の級割方式を使用します)。SonicOS は、分類後にトラフィックを DSCP 級割する機能に加え、外部ネットワークの横断と CoS の維持を可能にするための、802.1p タグを DSCP タグに割り付ける機能を備えています。VPN トラフィックの場合、SonicOS は、内部 (ペイロード) パケットだけでなく、外部 (カプセル化) パケットも同様に DSCP 級割できます。 これにより、QoS 対応サービス プロバイダは、暗号化された VPN トラフィックに対しても QoS を提供できます。

サービス プロバイダによって採用されている実際の制限方式は各種ありますが、一般的に、トラフィックに優先順位を付けるための重み付け公平キューイング (WFQ) のような等級をベースとしたキューイング方式や、テール ドロップやランダム初期検知などの輻輳を回避する方式が使用されています。

802.1p と DSCP QoS

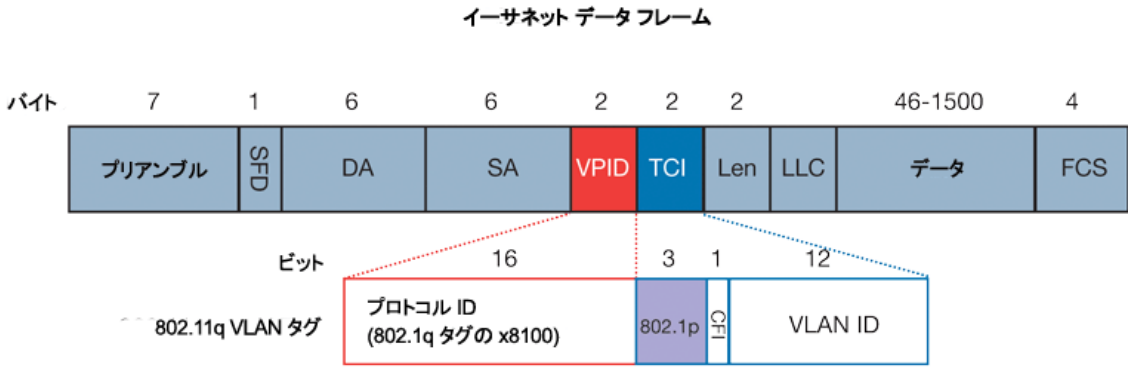
トピック:

- 802.1p の有効化 (82 ページ)
- DSCP 級割 (85 ページ)

802.1p の有効化

SonicOS では、QoS に対応する環境に参加している外部システムとの広い範囲での相互運用性を実現するために、第 2 層と第 3 層 CoS 方式をサポートしています。第 2 層の方式は、下図に示すように、フレームの優先順位を指定するために、イーサネット フレームのヘッダーに挿入された追加の 16 ビットのうちの 3 ビットを用いることのできる、IEEE 802.1p 標準です。

イーサネット データ フレーム



- **TPID**: TPID (Tag Protocol Identifier) は、バイト 12 から始まります (6 バイトの宛先アドレスと送信元アドレスの後)。2 バイトの長さで、タグ付けされたトラフィックは 0x8100 のイーサ種別を持ちます。
- **802.1p**: TCI (タグ制御情報 - バイト 14 から始まり、2 バイトの長さ) の最初の 3 ビットは、ユーザ優先順位を定義します (8 つ (2 の 3 乗) の優先順位レベルを与えます)。IEEE 802.1p では、これらの 3 ビットのユーザ優先順位の処理を定義しています。
- **CFI**: CFI (Canonical Format Indicator) は、単一ビットフラグで、イーサネット スイッチの場合は常に 0 に設定されます。CFI は、イーサネット ネットワークとトークン リング ネットワークの間の互換性のために使用されます。イーサネット ポートで受信されたフレームの CFI が 1 に設定されている場合、そのフレームは、タグ付けされていないポート用なので転送してはいけません。
- **VLAN ID**: VLAN ID (バイト 14 のビット 5 から始まる) は、VLAN の ID です。12 ビットあり、4,096 (2 の 12 乗) の VLAN ID を表現することができます。4,096 の ID のうち、ID 0 が優先順位フレームの識別に使用され、ID4,095 (FFF) が予約されているので、最大 4,094 の VLAN を設定できます。

802.1p のサポートは、802.1p タグを処理するインターフェース上で 802.1p 級割を有効にすることにより開始されます。802.1p は、SonicWall 装置の任意のイーサネット インターフェースで有効にすることができます。

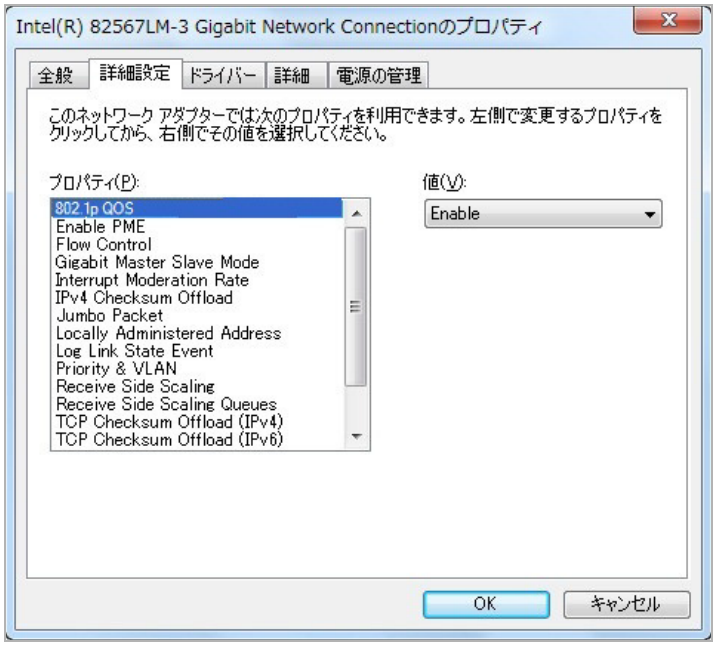
これらのタグの内部の 802.1p フィールドの動作は、アクセス ルールで制御することができます。既定の 802.1p アクセス ルール動作の「**なし**」は、特に指定しない限り、既存の 802.1p タグを 0 にリセットします (詳細は、QoS 級割の管理 (89 ページ) を参照)。

802.1p 級割を有効化すると、802.1p 対応ネットワーク機器により生成された着信 802.1p タグをターゲット インターフェースが認識できるようになり、また、アクセス ルールによる制御としてターゲット インターフェースが 802.1p タグを生成することが可能になります。SonicOS により挿入された 802.1p タグを持つフレームは、VLAN ID 0 を運びます。

802.1p タグは、アクセス ルールに従って挿入されるだけなので、インターフェース上で既定の設定で802.1p 級割を有効にしても、802.1p 非対応機器との通信は中断されません。

802.1p の場合、この優先順位付け方式を使用したいネットワーク機器による特定のサポートを必要とします。多くのボイスおよびビデオ オーバー IP 機器は、802.1p のサポートを提供していますが、機

能を有効化する必要があります。不確かな場合には、802.1p のサポートについて、装置の説明書を確認してください。同様に、多くのサーバとホストのネットワーク カード (NIC) は 802.1p をサポートする機能を持ちますが、通常この機能は既定で無効になっています。Win32 オペレーティング システムの場合、ネットワーク カードの「プロパティ」ページの「**詳細設定**」ビューで 802.1p の設定を確認および設定することができます。カードが 802.1p をサポートしている場合、「**802.1p QoS**」、「**802.1p Support**」、「**802.1p QoS Packet Tagging**」のような項目が表示されます。



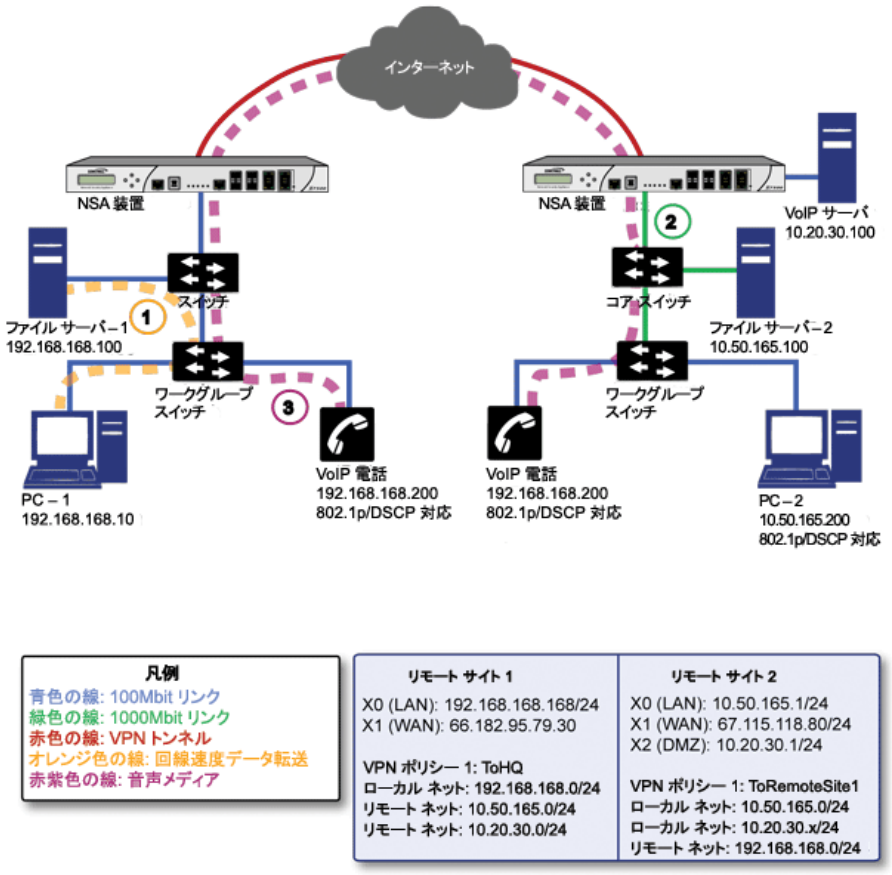
802.1p タグを処理するためには、ネットワーク インターフェースで機能が存在し有効にされている必要があります。これにより、ネットワーク インターフェースは、QoS 対応アプリケーションにより制御され、802.1p タグ付きのパケットを生成できます。既定では、一般的なネットワーク通信では、802.1p 非対応機器との互換性を維持するためにタグは挿入されません。

メモ：802.1p をサポートしていないネットワーク インターフェースは、802.1p のタグ付けされたトラフィックを処理できず、無視します。802.1p 級割を有効にするためのアクセス ルールを定義する場合は、ターゲット機器が 802.1p に対応することを確認してください。

また、(Ethereal 診断ツールを使用して) 802.1p 対応機器上でパケット監視を行う場合は、いくつかの 802.1p 対応機器でパケット監視内で 802.1p ヘッダーが表示されないことがある点にも注意してください。逆に言えば、802.1p 非対応機器上でパケット監視を行うと、ほとんど例外なくヘッダーが表示されますが、ホストはパケットを処理することができなくなります。

QoS 級割方式と DSCP 級割方式の間には潜在的な相互依存があるので、詳細については、89 ページの「QoS 級割の管理」を参照してください。 に進む前に、'DSCP 級割' について紹介し、相互依存が存在する理由について説明します。

DSCP 級割: サンプル シナリオ



DSCP 級割: サンプル シナリオ のシナリオでは、IPSec VPN により 'メイン サイト' に接続された**リモート サイト 1** を扱います。この企業は、プライベート VoIP シグナリング サーバをメイン サイトに配置して、内部で 802.1p/DSCP 対応 VoIP 電話システムを使用しています。メイン サイトでは、ギガビットとファースト イーサネットの混合した基盤を使用しています。 一方、リモート サイト 1 では、すべてファースト イーサネットを使用しています。内部トラフィックの優先順位付けのために、両方のサイトで 802.1p 対応スイッチが使用されています。

1 リモート サイト 1 の PC-1 は、23 テラバイトのパワーポイント プレゼンテーションをファイル サーバ 1 へ送信しており、ワークグループ スイッチと上流スイッチとの間の 100 Mbps のリンクは完全に飽和状態になっています。

2 メイン サイトで、802.1p/DSCP 対応 VoIP 電話 (`10.50.165.200`) のユーザが、VoIP 電話 (`192.168.168.200`) のユーザに電話をかけます。呼び出し元の VoIP 電話の 802.1p によりトラフィックに優先順位タグ 6 (音声) が付けられ、また、DSCP によりトラフィックに 48 のタグが付けられます。

   a コア スイッチとファイアウォールの間のリンクが VLAN の場合、スイッチによっては、ファイアウォールへ送信されるパケット内に、受信した 802.1p 優先順位タグを DSCP タグに加えて含めるものがあります (この動作はスイッチによって異なり、設定が可能な場合もあります)。

   b コア スイッチとファイアウォールの間のリンクが VLAN でない場合、スイッチが 802.1p 優先順位タグを含める方法はありません。802.1p 優先順位は削除され、(DSCP タグのみを含む) パケットがファイアウォールに転送されます。

VPN/WAN リンクを経由してパケットを送信する場合、ファイアウォールでパケット内に DSCP タグを含めることができますが、802.1p タグを含めることはできません。これは、VoIP トラフィックのすべての優先順位情報を失う結果となります。 なぜならば、パケットがリモートサイトに到着した際に、トラフィックの優先順位付けを行うための 802.1p MAC 層情報をスイッチが持たないからです。リモート サイト スイッチは、VoIP トラフィックを低優先順位のファイル転送と同じと見なします。リンクが飽和状態のため、VoIP フローは遅延し (パケットが破棄される場合もあります)、音質の低下を招く結果となります。

では、メイン サイト LAN からの重要な 802.1p 優先順位情報を VPN/WAN リンクを横断してリモート サイト LAN へと引き継ぐにはどうしたらよいのでしょうか。それには、QoS 割付を使用します。

QoS 割付は、第 2 層の 802.1p タグを第 3 層の DSCP タグに変換して、(割り付けられた形式で) 802.1p タグが 802.1p 非対応リンクを安全に横断できるようにする機能です。 パケットが配送のために次の 802.1p 対応セグメントに到着すると、QoS 割付機能により、DSCP が元の802.1p タグに変換され、第 2 層 QoS が利用できるようになります。

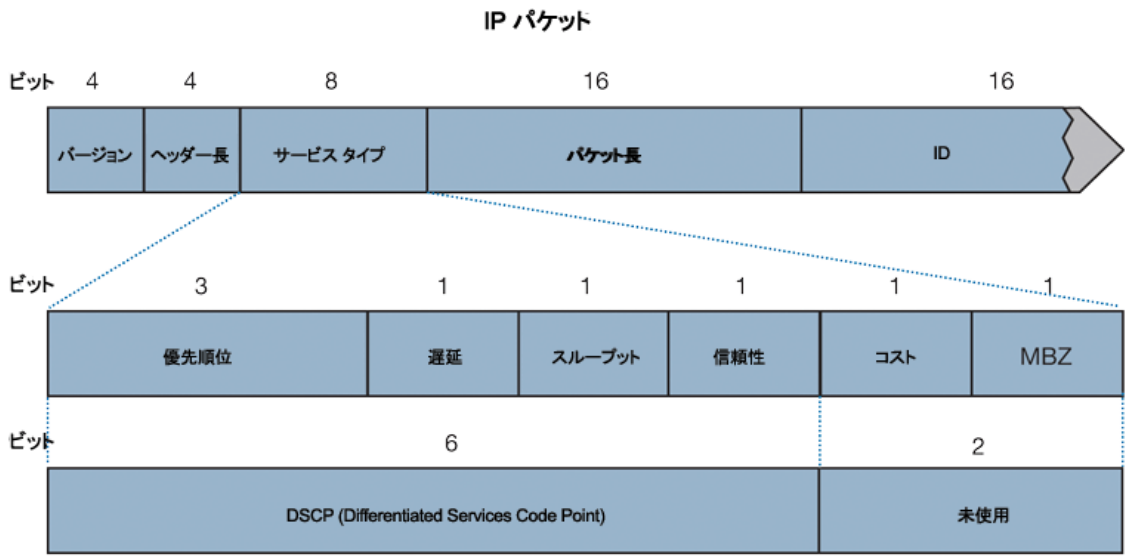
上記のシナリオでは、メイン サイトのファイアウォールで DSCP タグ (例えば、値 **48**) を VoIP パケットとカプセル化 ESP パケットに割り当てて、WAN にわたってレイヤ 3 QoS を適用します。この割り当ては、既存の DSCP タグを維持すること、または、802.1p タグから値を割り付けることにより発生します。VoIP パケットがリンクの反対側に到着すると、受信側 SonicWall によって逆の割付処理が行われます。 すなわち、DSCP タグが元の 802.1p タグに割り付けられます。

3 リモート サイトの受信側 SonicWall は、DSCP タグ範囲 48～55 を 802.1p タグ 6 に割り付けるように設定されています。ファイアウォールから発信されるパケットは、802.1p タグ 6 を運びます。スイッチは、それが音声トラフィックであると認識し、ファイル転送よりも優先して、リンクが飽和した場合でも QoS を保証します。

DSCP 級割

DSCP (Differentiated Services Code Point) 級割では、IP ヘッダー内の 8 ビットの ToS フィールドのうちの 6 ビットを使用して、最大 64 のトラフィックの等級 (またはコード ポイント) を提供します。DSCP は第 3 層の級割方式なので、802.1p の級割であったような互換性についての心配はありません。DSCP をサポートしていない機器では単にタグが無視されます。 最悪の場合でも、タグの値が 0 にリセットされるだけです。

DSCP 級割: IP パケット



DSCP 級割: IP パケットは、IP パケットと、ヘッダーの ToS 部分を拡大した図です。ToS ビットは、元々は優先順位とToS (遅延、スループット、信頼性、コスト) 設定のために使用されていましたが、その後、より多用途の DSCP 設定用に RFC2474 で再定義されました。

DSCP 級割: 一般的に使用されるコード ポイント テーブルに、一般的に使用されているコード ポイントと、従来の優先順位および ToS 設定に対する割り当てを示します。

DSCP 級割: 一般的に使用されるコード ポイント

DSCP	DSCP の説明	従来の IP 優先順位	従来の IP ToS (D、T、R)
0	最大努力型	0 (通常 - 000)	-
8	等級 1	1 (優先順位 - 001)	-
10	等級 1、金 (AF11)	1 (優先順位 - 001)	T
12	等級 2、銀 (AF12)	1 (優先順位 - 001)	D
14	等級 1、銅 (AF13)	1 (優先順位 - 001)	D、T
16	等級 2	2 (即時 - 010)	-
18	等級 2、金 (AF21)	2 (即時 - 010)	T
20	等級 2、銀 (AF22)	2 (即時 - 010)	D
22	等級 2、銅 (AF23)	2 (即時 - 010)	D、T
24	等級 3	3 (フラッシュ - 011)	-
26	等級 3、金 (AF31)	3 (フラッシュ - 011)	T
27	等級 3、銀 (AF32)	3 (フラッシュ - 011)	D
30	等級 3、銅 (AF33)	3 (フラッシュ - 011)	D、T
32	等級 4	4 (フラッシュ オーバライド - 100)	-
34	等級 4、金 (AF41)	4 (フラッシュ オーバライド - 100)	T
36	等級 4、銀 (AF42)	4 (フラッシュ オーバライド - 100)	D
38	等級 4、銅 (AF43)	4 (フラッシュ オーバライド - 100)	D、T
40	エキスプレス転送	5 (CRITIC/ECP[1] - 101)	-
46	緊急転送 (EF)	5 (CRITIC/ECP - 101)	D、T
48	制御用	6 (インターネット制御用 - 110)	-
56	制御用	7 (ネットワーク制御用 - 111)	-

1. ECP: Elliptic Curve Group (楕円曲線群)

DSCP 級割は、すべてのインターフェースの発着信トラフィックに対して、ゾーンのタイプを問わず、例外なく実行することができます。DSCP 級割は、「**QoS**」ビューのアクセス ルールで制御され、802.1p 級割と併用して使用できます。また、SonicOS 内部の帯域幅管理でも使用されます。

トピック:

- DSCP 級割と混在 VPN トラフィック (87 ページ)
- 802.1p CoS 4 - 負荷制御型の設定 (87 ページ)
- QoS 割付 (87 ページ)
- QoS 級割の管理 (89 ページ)

DSCP 級割と混在 VPN トラフィック

数ある安全対策と特性の中で、IPSec VPN では、ESP ヘッダーに追加される単調に増加するシーケンス番号に基づくアンチリプレイ機構を採用しました。シーケンス番号が重複するパケットは、シーケンス基準を満たさないという理由で破棄されます。このような基準の 1 つは、到着順序の異なるパケットの処理を管理します。SonicOS では、64 パケット分のリプレイ ウィンドウが提供されます。 すなわち、Security Association (SA) の ESP パケットが 64 パケットを超えて遅延した場合、パケットは破棄されます。

DSCP 級割を使用して VPN を横断するトラフィックに第 3 層 QoS を提供する場合は、この点を考慮する必要があります。さまざまなトラフィックが転送されている VPN トンネルがあるとします。高優先順位の DSCP タグが付けられたトラフィック (VoIP など)、低優先順位の DSCP タグが付けられたトラフィック、タグを付けられていないトラフィック、最大努力型 (FTP など) の DSCP タグが付けられたトラフィックが混在する場合、サービス プロバイダは、最大努力型の ESP パケットよりも、高優先順位の ESP パケットの処理と配送を最も優先します。その結果、トラフィックの条件によっては、最大努力型のパケットが 64 パケットを超えて遅延し、受信側の SonicWall のアンチリプレイ防御によりパケットが破棄される場合があります。

そのような現象が発生する場合 (例えば、低優先順位のトラフィックの過度の再送が発生する場合) は、高優先順位と低優先順位のトラフィック用に別個の VPN ポリシーを作成することをお勧めします。これを簡単に実現するには、高優先順位のホスト (例えば、VoIP ネットワーク) を、それら自身のサブネットに配置します。

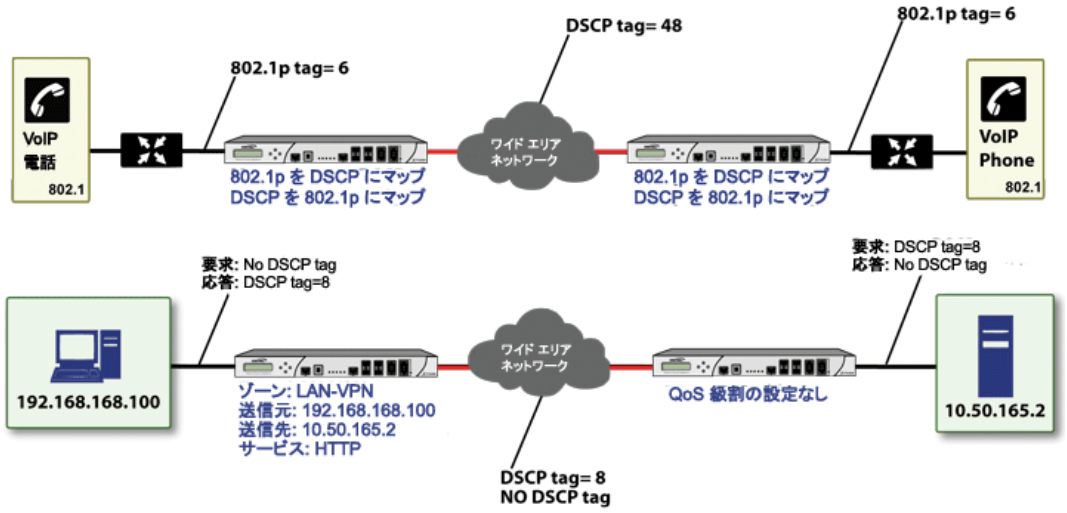
802.1p CoS 4 - 負荷制御型の設定

DSCP タグ 15 を既定の 802.1p 割付の 1 から 802.1p 割付の 2 に変更する場合、割付範囲は重複できないので、2 つの手順が必要です。範囲を重複して割付を行おうとすると、「DSCP 範囲は、既に存在するか、他の範囲と重複しています。」というエラーが発生します。最初に、802.1p CoS 1 に対する現在の終了範囲割付から 15 を削除し (802.1p CoS 1 の終了範囲割付を DSCP 14 に変更し)、次に 802.1p CoS 2 の開始範囲割付に DSCP 15 を割り当てます。

QoS 割付

QoS 割付の第 1 の目的は、WAN リンクを経由する送信の前に 802.1p タグと対応する DSCP タグを割り付け、リンクの反対側に到着したときに DSCP から 802.1p に割り付け戻すことにより、802.1p 非対応リンク (WAN リンクなど) を横断して 802.1p タグを維持できるようにすることにあります (QoS 割付を参照)。

QoS 割付



メモ：割付は、アクセス ルールの「QoS」ビューの動作として、「**参照**」を割り当てるまで行われません。割付テーブルは、アクセス ルールの参照の方針によって使用される対応を定義しているだけです。

802.1p サービス等級	変換先 DSCP	変換元 DSCP 範囲	設定
0 - 最大努力型	0 - 最大努力型/既定	0-7	
1 - バックグラウンド型	8 - 等級 1	8-15	
2 - 倹約型	16 - 等級 2	16-23	
3 - 最高努力型	24 - 等級 3	24-31	
4 - 負荷制御型	32 - 等級 4	32-39	
5 - 映像型 (遅延 100 ミリ秒以下)	40 - エキスプレス転送	40-47	
6 - 音声型 (遅延 10 ミリ秒以下)	48 - 制御用	48-55	
7 - ネットワーク制御型	56 - 制御用	56-63	

QOS 設定の初期化

例えば、既定のテーブルに従った場合、値が **2** の 802.1p タグは、送信用に **16** という DSCP 値が割り当てられ、値が **43** の DSCP タグは、受信用に **5** という 802.1p 値が割り当てられます。

これらの割付は再設定できます。802.1p タグ **4** の送信割付を既定の DSCP 値の **32** から **43** に変更したい場合、「**4 - 負荷制御型**」の**設定**アイコンを選択し、ドロップダウン ボックスから新しい「**変換先 DSCP**」の値を選択します。

802.1p CoS 1 の終了範囲の再割付

802.1p CoS 2 の開始範囲の再割付

「**QoS 設定の初期化**」ボタンを選択することにより、既定の割付に戻すことができます。

QoS 級割の管理

QoS 級割は、管理インターフェースの「**ポリシー | ルール > アクセス ルール**」ページにある「**ルールの追加/編集**」ダイアログの「**QoS**」ビューで設定します。

SonicOS のアクセス ルールで管理される 802.1p および DSCP 級割では、「**なし**」、「**維持**」、「**指定**」、「**参照**」の 4 つの方針が提供されます。DSCP の既定の方針は「**維持**」で、802.1p の既定の方針は「**なし**」です。

QoS 級割: 動作 テーブルに、両方の級割方式での各方針の動作について説明します。

QoS 級割: 動作

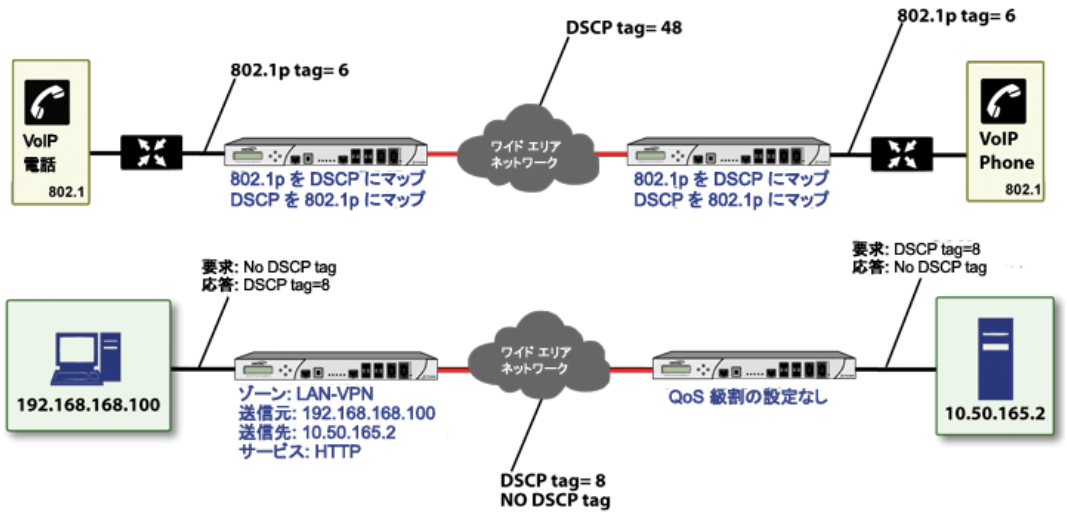
動作	802.1p (第 2 層 CoS)	DSCP (第 3 層)	注
なし	(アクセス ルールにより定義された) このトラフィック等級に一致するパケットがイーグレス インターフェースから送出されるとき、802.1p タグは追加されません。	DSCP タグは明示的に 0 に設定 (リセット) されます。	このトラフィック等級のターゲット インターフェースが VLAN 副インターフェースの場合、802.1q タグの802.1p 部分が明示的に 0 に設定されます。このトラフィック等級が VLAN 向けであり、優先順位付けに 802.1p が使用されている場合、「**維持**」、「**指定**」、「**参照**」方針を使用した特定のアクセス ルールをこのトラフィック等級に定義する必要があります。
維持	現存する 802.1p タグが維持されます。	現存する DSCP タグが維持されます。	

QoS 級割: 動作

動作	802.1p (第 2 層 CoS)	DSCP (第 3 層)	注
指定	表示されるドロップダウン メニューから明示的な 802.1p タグ値 (0〜7) を割り当てることができます。	表示されるドロップダウン メニューから明示的な DSCP タグ値 (0〜63) を割り当てることができます。	802.1p または DSCP 方針のどちらかを「**指定**」に設定し、もう一方を「**参照**」に設定した場合、明示的に指定された割り当てが最初に行われ、その後、もう一方がその割り当てに従って参照されます。
参照	「**ファイアウォール > QoS 割付**」ページで定義された割付設定が、DSCP タグから 802.1p タグへの割付に使用されます。	「**ファイアウォール** > QoS 割付」ページで定義された割付設定が、802.1 タグから DSCP タグへの割付に使用されます。追加の「**802.1p 級割を、DSCP 値に優先する**」チェックボックスが現れます。このチェックボックスを選択すると、割り付けられた 802.1p 値が、クライアントにより設定されたDSCP 値に優先して使用されます。これは、DSCP CoS 値を設定しているクライアントをオーバライドするのに有用です。	DSCP と 802.1p の両方で方針として「**参照**」を設定した場合、割付は一方向でのみ発生します。VLAN から 802.1p タグとともにパケットが到着した場合、DSCP が802.1p タグから割り付けられます。パケットが VLAN 宛ての場合、802.1p が DSCP タグから割り付けられます。

例として、両方向の DSCP タグの方針を提供する両方向 DSCP タグの方針を参照してください。

両方向 DSCP タグの方針



192.168.168.100 上のウェブ ブラウザから 10.50.165.2 上のウェブ サーバに対して HTTP アクセスを行うと、内部 (ペイロード) パケットと外部 (カプセル化 ESP) パケットに DSCP 値 8 のタグが付けられます。パケットがトンネルの反対側から出て、10.50.165.2 に配送されるとき、DSCP タグ値 8 が使用されます。10.50.165.2 からトンネル経由で応答パケットを (最初の SYN/ACKパケットから) 192.168.168.100 に送り返すとき、アクセス ルールにより、192.168.168.100 に配送される応答パケットに DSCP 値 8 のタグが付けられます。

この動作は、DSCP と 802.1p 級割の 4 つの QoS 方針設定のすべてに適用されます。

この動作の 1 つの実用的な応用例として、VPN ゾーン宛てのトラフィックに対する 802.1p 級割ルールの設定があります。VPN を横断して 802.1p タグを送信することはできませんが、VPN を横断して返された応答パケットに対して、トンネルからの出口で 802.1p タグを付けることができます。そのためには、物理的なイーグレス インターフェースで 802.1p のタグ付けを有効にし、ゾーンの「VPNアクセス ルール」で「なし」以外の 802.1p 級割方式を設定する必要があります。

関連するネットワーク機器の 802.1p との互換性を確認し、適用可能な SonicWall インターフェース上で 802.1p 級割を有効にした後は、802.1p タグを管理するためにアクセス ルールの設定を開始できます。

リモート サイト 1: アクセス ルール設定の例 テーブルに示すように、**リモート サイト 1** ネットワークに対して 2 つのアクセス ルールを設定することができます。

リモート サイト 1: アクセス ルール設定の例

設定	アクセス ルール1	アクセス ルール2
「一般」ビュー		
動作	許可	許可
送信元ゾーン	LAN	VPN
送信先ゾーン	VPN	LAN
サービス	VOIP	VOIP
送信元	LAN プライマリ サブネット	メイン サイトのサブネット
送信先	メイン サイトのサブネット	LAN プライマリ サブネット
許可ユーザ	すべて	すべて
スケジュール	常に有効	常に有効
ログを有効にする	有効	有効
断片化パケットを許可する	有効	有効
「Qos」ビュー		
DSCP 級割の方針	参照	参照
802.1p 級割を、DSCP 値に優先する	有効	有効
802.1p 級割の方針	参照	参照

最初のアクセス ルール (管理 LAN の「**VPN**」) は、以下の効果を持ちます。

- VPN 経由で **LAN プライマリ サブネット**から**メイン サイトのサブネット**に送信される、(サービス グループにより定義されている) **VoIP** トラフィックは、DSCP タグと 802.1p タグの両方について評価されます。
  - 「**参照**」に対する DSCP 級割方式と 802.1p 級割方式の組み合わせについては、QoS 級割の管理 (89 ページ) の表に説明しています。
  - 送信されたトラフィックに 802.1p タグ (例えば、CoS=6) のみが含まれている場合、VPN への内部 (ペイロード) パケットは、DSCP 値 48 でタグ付けられます。また、外部 (ESP) パケットも値 48 でタグ付けられます。
  - メイン サイトのファイアウォールによって戻りのトラフィックに DSCP タグ (CoS=48) が付けられていると仮定した場合、出口において CoS=6 の 802.1p タグが戻りのトラフィックに付けられます。
  - 送信されたトラフィックに DSCP タグ (例えば、CoS=48) のみが含まれている場合、DSCP 値が内部と外部の両方のパケットで維持されます。

- メイン サイトのファイアウォールによって戻りのトラフィックに DSCP タグ (CoS=48) が付けられていると仮定した場合、出口において CoS=6 の 802.1p タグが戻りのトラフィックに付けられます。
- 送信されたトラフィックに 802.1p タグ (CoS=6 など) と DSCP タグ (CoS=63 など) の両方が含まれている場合、802.1p タグが優先され、それに応じて割付が行われます。VPN への内部 (ペイロード) パケットは、DSCP 値 48 でタグ付けられます。また、外部 (ESP) パケットも値 48 でタグ付けられます。

メイン サイトのファイアウォールによって戻りのトラフィックに DSCP タグ (CoS=48) が付けられていると仮定した場合、出口において CoS=6 の 802.1p タグが戻りのトラフィックに付けられます。

2 番目のアクセス ルール (「VPN > LAN」) の効果を調べるには、メイン サイトで設定されたアクセス ルールを確認します (メイン サイト: アクセス ルール設定の例 テーブルを参照)。

メイン サイト: アクセス ルール設定の例

設定	アクセス ルール1	アクセス ルール2
「一般」ビュー		
動作	許可	許可
送信元ゾーン	LAN	VPN
送信先ゾーン	VPN	LAN
サービス	VOIP	VOIP
送信元	LAN サブネット	リモート サイト 1 サブネット
送信先	リモート サイト 1 サブネット	LAN サブネット
許可ユーザ	すべて	すべて
スケジュール	常に有効	常に有効
ログを有効にする	有効	有効
断片化パケットを許可する	有効	有効
「Qos」ビュー		
DSCP 級割の方針	参照	参照
802.1p 級割を、DSCP 値に優先する	有効	有効
802.1p 級割の方針	参照	参照

VPN 経由で**リモート サイト 1 サブネット**からメイン サイトの LAN ゾーンの **LAN サブネット**に送信される、(サービス グループにより定義されている) **VoIP** トラフィックには、着信 VoIP 通話用のアクセス ルールが適用されます。VPN ゾーンに到着したトラフィックには、802.1p タグはなく、DSCP タグだけが付けられています。

- DSCP タグ (例えば CoS=48) を含んでいるトンネルを出て行くトラフィックでは、DSCP 値が維持されます。LAN 上の目的地へパケットが配送される前に、メイン サイトのファイアウォールによって、「**QoS 割付**」設定 (例えば、CoS=6) に応じた 802.1p タグが付けられます。
- メイン サイトで電話を受けている VoIP 電話によって戻りのトラフィックに 802.1p タグ (例えば CoS=6) が付けられていると仮定した場合、戻りのトラフィックでは、VPN を経由して送り返される内部と外部の両方のパケットにおいて、変換割付に従って DSCP タグ (CoS=48) が付けられます。
- メイン サイトで電話を受けている VoIP 電話によって戻りのトラフィックに DSCP タグ (例えば CoS=48) が付けられていると仮定した場合、戻りのトラフィックでは、VPN を経由して送り返される内部と外部の両方のパケットにおいて、DSCP タグが維持されます。

- メイン サイトで電話を受けている VoIP 電話によって戻りのトラフィックに 802.1p タグ (例えば CoS = 6) と DSCP タグ (例えば CoS = 14) の両方が付けられていると仮定した場合、戻りのトラフィックでは、VPN を経由して送り返される内部と外部の両方のパケットにおいて、変換割付に従って DSCP タグ (CoS = 48) が付けられます。

帯域幅管理

帯域幅管理 (BWM) については、ファイアウォール設定 > 帯域幅管理 (24 ページ) を参照してください。

用語集

- **802.1p** - IEEE 802.1p は、802.1q ヘッダーの追加 16 ビット内の 3 つの優先順位ビット (合計 8 つの優先順位レベル) を使用してパケットのタグ付けを行う、レイヤ 2 (MAC 層) の CoS (Class of Service) メカニズムです。802.1p を使用したタグの生成、認識、処理を行うには互換性のある装置が必要です。 したがって、802.1p は、互換性のあるネットワーク上でのみ使用する必要があります。
- **帯域幅管理 (BWM)** - トラフィックのシェイピングやポリシングを行うために使用されるさまざまなアルゴリズムあるいは手法を指します。シェイピングは、送信トラフィックを管理することを表します。 ポリシングとは、受信トラフィックを管理することを表します (受付制御とも呼ばれます)。帯域幅管理には、さまざまなキューイングおよび破棄手法を含め、それぞれ独自の設計上の長所を持つ多くの異なる方式があります。SonicWall では、特定のタイプの受信トラフィックに対する破棄手法に加え、受信および送信 BWM 用にトークン ベース、等級ベースのキューイング方式を採用しています。
- **Class of Service (CoS)** - レイヤ 2 またはレイヤ 3 のタグのように、分類後にトラフィックに適用される、指示子または識別子です。CoS 情報は、ネットワーク上のトラフィックの等級を区別するため、およびサービス品質 (QoS) システム管理者によって定義された特殊な処理 (例えば、優先キューイング、短い待ち時間など) を提供するために、QoS システムによって使用されます。
- **分類** - ある種別 (等級) のトラフィックを識別 (区別) する行為です。QoS のコンテキスト内では、遅延、待ち時間、またはパケット紛失に対するトラフィックの感度に基づいてカスタマイズされた処理 (通常は優先するかどうか) を提供するために行われます。SonicOS では、アクセス ルールを使用して分類を行います。 分類は、送信元ゾーン、送信先ゾーン、送信元アドレス オブジェクト、送信先アドレス オブジェクト、サービス オブジェクト、スケジュール オブジェクトのうちのいくつか、またはすべてに基づいて行うことができます。
- **コード ポイント** - ホストあるいは中間のネットワーク機器によって IP パケットの DSCP 部分にマーク付け (タグ付け) される値です。現在、タグ付けされたトラフィックの等級 (昇順の優先順位) を定義するために、64 (0〜63) のコード ポイントを使用できます。
- **制限** - ネットワーク トラフィックにサービス品質を提供する多くの方法を記述するために使用される、広い意味を持つ用語です (破棄、キューイング、ポリシング、シェイピングを含みますが、これらに限定されるものではありません)。
- **DiffServ** (Differentiated Services) - 要件に基づいたトラフィックに合わせた処理を提供する目的で、IP ネットワーク上の異なるタイプや等級のトラフィックを区別するための基準です。DiffServでは、主に IP パケットの ToS ヘッダーの中でマークされたコード ポイント値に依存して、異なる等級のトラフィックを区別します。DiffServ のサービス レベルは、級割されたトラフィックが通過する各ルータ (または DiffServ が有効な他のネットワーク機器) 上でホップ ベースで実行さ

れます。現在、DiffServ のサービス レベルには、最低でも、**既定**、**保証転送**、**緊急転送**、および **DiffServ** があります。詳細については、DSCP 級割 (85 ページ) を参照してください。

- **破棄** - ネットワーク上で輻輳が発生するかもしれない時期の予測を試み、制限を超過したトラフィックを捨てることで輻輳を防ぐことを目的とする、QoS システムで採用されている輻輳回避メカニズムです。破棄は、キューがいっぱいになる状況を回避しようとするので、キューの管理アルゴリズムと見なすこともできます。高度な破棄メカニズムでは、取り扱いに慎重を要するトラフィックの破棄を回避するために CoS 級割が忠実に守られます。一般的な方式は、以下のとおりです。
  - **テール ドロップ** - いっぱいになったキューを無差別に処理する方法で、パケットの CoS 級割にかかわらず、キューの中の最後のパケットが破棄されます。
  - **ランダム初期検知 (RED)** - RED では、キューの状況を監視して、いついっぱいになるかを予測します。その後、グローバル同期の可能性を最小限にするために、ランダムにパケットを破棄します。RED の基本的な実装では、テール ドロップと同様に、CoS 級割は考慮されません。
  - **重み付けランダム初期検知 (WRED)** - 破棄決定プロセスにおいて DSCP 級割を考慮する、RED の実装です。
- **DSCP** (Differentiated Services Code Points) - RFC2747 に記載されている IP ヘッダーの ToS フィールドの再利用です。DSCP では、64 のコード ポイント値を使用して、DiffServ (Differentiated Services) を有効にします。その等級によってトラフィックを級割することによって、各パケットをネットワークに沿ったすべてのホップで適切に処理することができます。
- **グローバル同期** - キューがいっぱいになることに対処するために設計された輻輳回避方法である破棄の潜在的な副作用です。グローバル同期は、輻輳したリンクを通過する複数の TCP フローが同時に破棄されたとき (例えばテール ドロップ) に発生します。これらのフローのそれぞれに対して、ネイティブな TCP スロースタート メカニズムがほぼ同時に開始されると、リンクはこれらのフローによって再び溢れてしまいます。その結果、輻輳と不十分な利用が周期的に発生します。
- **保証帯域幅** - ある等級のトラフィックに常に与えられる、インターフェース上で利用可能な合計帯域幅に対して宣言された割合です。受信 BWM と送信 BWM の両方に適用されます。すべての BWM ルールにおける保証された帯域幅の合計は、利用可能な帯域幅の合計の 100%を超過することはできません。SonicOS では帯域幅管理機能が拡張され、速度制限機能が使用できます。第 2 層、3層、または 4 層ネットワーク トラフィックの最大速度を指定するトラフィック ポリシーを作成できます。これにより、プライマリ WAN リンクから、あまり多数のトラフィックを処理できないバックアップ接続へのフェイルオーバーが生じた場合でも、帯域幅管理が行えます。「保証された帯域幅」は 0%に設定することもできます。
- **受信 (イングレスまたは IBWM)** - 特定のインターフェースに入るトラフィックの速度のシェイピングを行う機能です。TCP トラフィックに対しては、送信の承認 (ACK) を遅らせ、送信元での速度を遅くさせることで、受信フローの速度を調整可能にして、実際のシェイピングを行うことができます。UDP トラフィックの場合、UDP にはネイティブなフィードバック制御がないので、破棄手法が使用されます。
- **IntServ** - RFC1633 で定義された統合サービス (Integrated Services) です。DiffServ のバックアップ CoS システムである IntServ は、各機器がトラフィックを送信する前にネットワーク要件を要求 (または予約) する点で、DiffServ と根本的に異なります。これには、ネットワーク上の各ホップが IntServ 対応である必要があり、また、各ホップですべてのフローの状態情報を保持する必要があります。SonicOS では、IntServ はサポートされません。IntServ の最も一般的な実装は RSVP です。
- **最大帯域幅** - ある等級のトラフィックに許可される最大帯域幅を定義する、インターフェース上で利用可能な合計帯域幅に対して宣言された割合です。受信 BWM と送信 BWM の両方に適用さ

れます。帯域幅の速度制限を指定する調整メカニズムとして使用されます。帯域幅管理機能が拡張され、速度制限機能が使用できます。第 2 層、3層、または 4 層ネットワーク トラフィックの最大速度を指定するトラフィック ポリシーを作成できます。これにより、プライマリ WANリンクが大量のトラフィックを処理できないバックアップ接続にフェイルオーバーする場合の帯域幅管理が可能になります。 「最大帯域幅」は 0%に設定することもできます。 その場合、すべてのトラフィックが遮断されます。

- **送信 (イーグレスまたは OBWM)** - インターフェースからトラフィックを送出する速度を制限することです。送信BWM では、8 つの優先順位キューを持つクレジット (またはトークン) ベースのキューイング システムを使用して、アクセス ルールによって分類される異なるタイプのトラフィックを処理します。
- **優先順位** - トラフィックの分類で使用される追加要素です。SonicOS では、8 つの優先順位リング (0=リアルタイム、7=最低) を使用して、BWM に使用されるキュー構造を構成しています。キューは、優先順位リングの順序で処理されます。
- **割付** - SonicOS による QoS の実装に関していえば、割付は、802.1p タグ付けをサポートしないネットワーク リンクを横断する 802.1p のタグを保持するために、レイヤ 2 CoS タグ (802.1p) とレイヤ 3 CoS タグ (DSCP) を相互に変換する機能です。割付の対応付けは、完全にユーザ定義可能で、また、割付の動作はアクセス ルールによって制御されます。
- **級割** (**タグ付け**または**色付け**とも呼ばれます) - 区別の目的でレイヤ 2 (802.1p) またはレイヤ 3 (DSCP) の情報をパケットに適用する行為です。その結果、パケットは、宛先へのパス上にあるネットワーク機器により、適切に分類 (認識) され、優先順位が付けられます。
- **MPLS** (マルチ プロトコル ラベル スイッチング) - この用語は QoS の分野でよく使用されますが、(SonicWall 装置を含む) ほとんどの顧客構内 IP ネットワーキング機器でネイティブにサポートされません。MPLS は、ネットワークに沿って概念的な接続志向のパス (LSP:ラベル スイッチ パス) を追加することにより IP ネットワーク機能を強化する、キャリア クラスのネットワーク サービスです。パケットが顧客構内ネットワークから外に出るときに、パケットはラベル エッジ ルータ (LER) によってタグ付けされます。これにより、ラベルを使用して LSP を判定できるようになります。 MPLS タグ自体は第 2 層と第 3 層の間に存在し、両方のネットワークの層の MPLS 特性を伝えます。MPLS は、第 2 層と第 3 層の VPN サービスの両方を提供する一方、既存の IPSec VPN 実装との相互運用が可能であるため、VPN で一般的になりつつあります。また、MPLS は、QoS 能力についても非常によく知られており、従来の DSCP 級割とも相互運用が可能です。
- **ホップ単位動作 (PHB)** - パケットが通過する各 DiffServ 対応ルータにおいて、パケットの DSCP 分類に基づいてパケットに適用される処理。破棄、再級割 (再分類)、最大努力型、保証転送、緊急転送などの動作があります。
- **ポリシング** - ネットワーク リンクを出入りするトラフィックの速度を制御する、トラフィックの制限機能。ポリシングの方法は、無差別にパケットを捨てる方式からアルゴリズムによるシェイピングまで、またさまざまなキューイング規則まで及びます。
- **キューイング** - リンクの利用可能な帯域幅を効果的に使用できるように、トラフィックを分類した後に、並べ替えのため、および個別に管理するために、キューが一般的に使われます。キューは、高優先順位のキューが常に多くのトラフィックを受信でき、低優先順位のキューよりも優先してサービスを受ける (キューからパケットが取り出される、または処理される) ように、さまざまな方式とアルゴリズムを使用して管理されます。以下に、いくつかの一般的なキュー規則を示します。
    - **FIFO** (First In First Out、先入れ先出し) - 最初に入ったパケットが最初に処理される、非常に単純な無差別型のキュー。
    - **等級ベース キューイング (CBQ)** - 高優先順位のトラフィックが優先的に処理される、パケットの CoS を考慮に入れたキューイング規則。

    - **重み付け公平キューイング (WFQ)** - パケットの IP 優先順位とフローの合計数に基づいた単純な式を使用してキューをサービスする規則。WFQ は、サービスを受ける高優先順位のフローが異常に大量にあると不安定になる傾向があり、望みとは逆の効果が生じることがしばしばあります。
    - **トークン ベース CBQ** - トークンを使用した CBQ の拡張。または、リンクの利用を円滑化または正常化して、過剰利用や不十分な利用を回避するのに役立つクレジット ベースのシステム。SonicOS の BWM で採用されています。
- **RSVP** (リソース予約プロトコル) - 一部のアプリケーションで採用されている IntServ シグナリング プロトコルであり、ネットワーク動作 (例えば、遅延や帯域幅) をネットワーク パスに沿って予約できるように、ネットワーク動作の事前要求が行われます。この予約パスを設定するには、パスに沿った各ホップが RSVP に対応しており、それぞれが要求されたリソースを予約することに同意する必要があります。この QoS システムは、現存しているフローの状態を各ホップが維持することを要求するため、いくぶんリソース集約的です。IntServの RSVP は DiffServ の DSCP とはかなり異なりますが、相互運用することができます。SonicOS では、RSVP はサポートされません。
- **シェイピング** - 通常、送信元に対する何らかのフィードバック メカニズムを用意することによってトラフィック フローの速度を変更するための、QoS システムによる試み。これの最も一般的な例は、TCP 速度の操作です。 つまり、TCP 送信元に送り返す承認 (ACK) をキューに入れることによって遅延させ、算出されるラウンドトリップ時間 (RTT) を増加させます。 これにより、TCP 固有の動作を利用して、送信元がデータを送信する速度を低下させます。
- **サービス種別 (ToS)** - CoS 情報を指定することのできる、IP ヘッダー内部のフィールド。歴史的にごくまれに、IP 優先順位ビットとともに、CoS を定義するために使用されていました。現在、ToS フィールドは、DiffServ のコード ポイント値により、かなり一般的に使用されています。

6

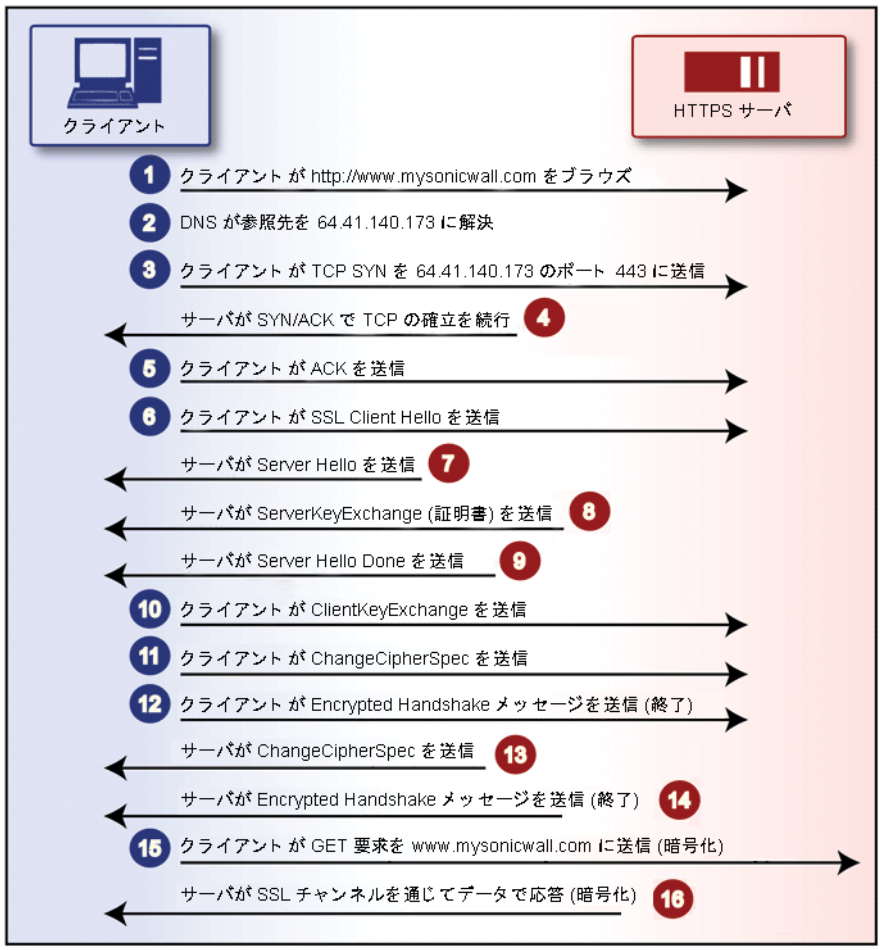
SSL 制御の設定

- SSL 制御について (97 ページ)
- ファイアウォール設定 > SSL 制御 (105 ページ)
- SSL 制御の設定 (105 ページ)
- ゾーンでの SSL 制御の有効化 (109 ページ)
- SSL 制御のイベント (110 ページ)

SSL 制御について

SonicOS には、SSL 制御機能があります。SSL 制御は、SSL セッションのハンドシェイクを認識するシステムで、SSL 接続の確立を制御するポリシーを構築できます。SSL (セキュア ソケット レイヤ) は、TCP ベースのネットワーク通信において中心的な規格であり、最も一般的な、よく知られているアプリケーションとして HTTPS (HTTP over SSL) があります。HTTP over SSL 通信にその通信手順を示します。SSL では、デジタル証明書に基づいてエンドポイントが識別され、暗号化されたダイジェスト ベースの機密性を有するネットワーク通信が行われます。

HTTP over SSL 通信



SSL を使用すると、HTTPS セッションの確立時にクライアントから要求された URL (Uniform Resource Locator、例えば https://www.mysonicwall.com など) を含むすべてのペイロードをはっきりわからないようにするという、セキュリティ上の効果が得られます。これは、HTTPS を使用すると、暗号化された SSL トンネルを使用して HTTP が転送されるからです。SSL セッションが確立される (HTTP over SSL 通信を参照) まで実際の対象リソース (www.mysonicwall.com) がクライアントによって要求されることはありませんが、SSL セッションが確立した後に、ファイアウォールやその他の中間機器がセッション データを検査することはできません。このため、URL ベースのコンテンツ フィルタ システムでは、IP アドレス以外の方法で要求を検査して、許可するかどうかを決定することはできません。

ホスト ヘッダー ベースの仮想ホスティング (定義については SSL 制御の重要な概念 (100 ページ) を参照) は効率的で人気があるため、IP アドレス ベースのフィルタは暗号化されていない HTTP に対して効果がありませんが、ホスト ヘッダー ベースの HTTPS サイトは滅多にないため、IP フィルタは効果的に機能します。しかし、この信頼は HTTPS サーバ オペレータが誠実であることに基づいたもので、SSL が人をだます目的では使用されないということを前提にしています。

ほとんどの場合、SSL は適切に使用されており、オンライン ショッピングまたはオンライン バンキングや、個人情報または貴重な情報のやり取りが行われるセッションなど、セキュリティが重視される通信で使用されています。しかし、SSL のコストが低下し続け、簡単に使用できるため、セキュリティ目的ではなく、あいまい化や隠蔽を目的とした信用性の乏しい SSL アプリケーションも増加しています。

よく使用されているカムフラージュの方法では、ブラウジングの詳細を隠したり、コンテンツ フィルタを回避する目的で、SSL で暗号化されたウェブ ベースのプロキシ サーバが使用されています。既知のこの種類の HTTPS プロキシ サービスを IP アドレスに基づいて遮断することは簡単ですが、単純なウェブ検索によって簡単に利用できる何千ものプライベート ホスト プロキシ サーバを遮断するこ

とは実際のところ不可能です。問題は、このようなサービスの数が増え続けていることではなく、これらのサービスの本質が予測できない点です。これらのサービスは、動的にアドレス指定された DSL およびケーブル モデム接続を使用するホーム ネットワーク上でホスティングされていることが多く、該当する IP が常に変わります。未知のこのような SSL を遮断するには、すべての SSL トラフィックを遮断する必要があり、実際には不可能です。

確立された SSL セッションを管理者が細かく調べて、ポリシー ベースで制御できるようにすることにより、SSL 制御機能にはこの問題に対処する方法が多数用意されています。現在の実装では SSL アプリケーション データの復号化は行いませんが、疑わしい SSL トラフィックをゲートウェイに基づいて識別して、許可しないことは可能です。

トピック:

- SSL 制御の主な機能 (99 ページ)
- SSL 制御の重要な概念 (100 ページ)
- 注意事項と推奨事項 (104 ページ)

SSL 制御の主な機能

SSL 制御: 機能と利点

機能	利点
コモンネーム ベースのホワイトリストおよびブラックリスト	明示的に許可または拒否する証明書サブジェクトのコモンネーム (「重要な概念」で説明します) のリストを定義することができます。エントリの文字列が含まれるものは一致と見なされます。例えば、ブラックリストのエントリが "prox"の場合、"www.megaproxy.com"、"www.proxify.com" および "proxify.net" は一致するものと判断されます。これにより、好ましくないと考えられるサブジェクトに対して発行された証明書を使用する SSL 交換のすべてを、簡単に遮断することができます。その一方で、組織に共通する文字列をホワイトリストで定義することにより、その組織内のすべての証明書を簡単に許可することができます。各リストには、最大 1,024 のエントリを定義できます。 クライアントがバックアップ ホスト名やバックアップ IP アドレスを使用して、これらのサイトへのアクセスを隠そうとした場合であっても、証明書に含まれるサブジェクトのコモンネームが検査されるため、サブジェクトは証明書で必ず検出され、ポリシーが適用されます。
自己署名証明書の制御	SSL でセキュリティ保護された適切なサイトでは、既知の認証局によって発行された証明書を使用することが一般的であり、これは SSL における信頼の基盤です。また同様に、(SonicWall ネットワーク セキュリティ装置のように) SSL によってセキュリティ保護されたネットワーク装置では、セキュリティ保護のための既定の方法として自己署名証明書を使用することが一般的です。したがって、閉鎖的な環境の自己署名証明書は疑わしくありませんが、公開されているサイトや商業利用サイトで使用されている自己署名証明書は疑わしいものです。自己署名証明書を使用する公開サイトでは、信頼性と識別のためではなく、暗号化のためだけにSSL が使用されていることがよくあります。完全に不正なサイトとは言い切れませんが、SSL で暗号化されたプロキシ サイトで一般的なように、隠蔽が目的である可能性が高いと言えます。 自己署名証明書を遮断するポリシーを設定できるため、このようなサイトと通信する危険性に対する防御が可能です。自己署名証明書を使用している既知の信頼できる SSL サイトとの通信が遮断されないようにするため、ホワイトリスト機能を使用して明示的に許可することができます。

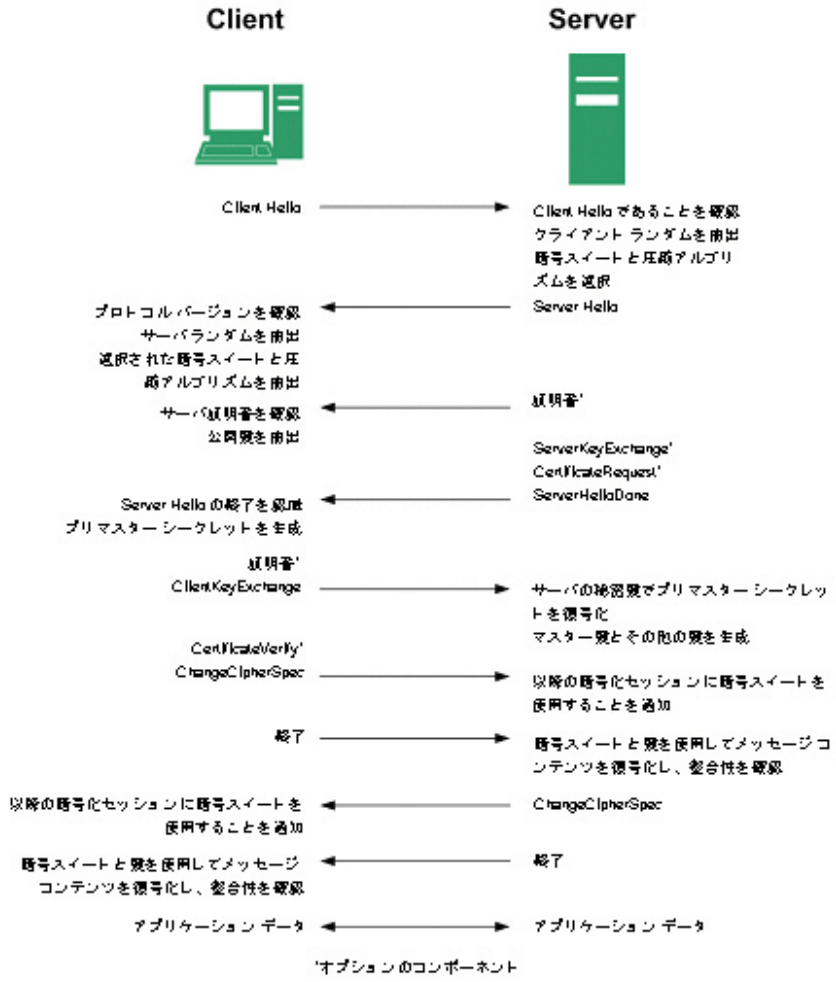
SSL 制御: 機能と利点

機能	利点
信頼できない認証局の制御	自己署名証明書が使用されている場合と同様、信頼できない CA によって発行された証明書が使用されている場合も、あいまい化のための信頼できない行為とは断定できませんが、信頼できるかどうか疑わしいことは確かです。 SSL 制御機能では、SSL 交換で使用される証明書の発行者とファイアウォールの証明書ストアに保存されている証明書を比較することができます。証明書ストアには、現在のウェブ ブラウザと同じように、約 100 個の既知の CA の証明書が保存されています。この証明書ストアに保存されていない CA によって発行された証明書が SSL 制御機能によって検出された場合、SSL 接続を禁止できます。 独自のプライベート認証局を組織で使用している場合は、このプライベート CA をファイアウォールの証明書ストアに簡単にインポートして、プライベート CA を信頼された CA として認識されるようにすることができます。証明書ストアには、最大 256 の証明書を保存できます。
SSL バージョン、暗号の強度、および証明書有効期間の制御	SSL 制御機能には、読み取られる可能性のある SSLv2 を禁止する機能、脆弱な暗号 (64 ビット未満の暗号) を禁止する機能、および証明書の日付の範囲が無効な SSL ネゴシエーションを禁止する機能など、ネゴシエーションの特性に基づいて SSL セッションを管理する追加機能あります。これにより、管理者は、暗号に関する未知の脆弱性やセキュリティ警告の無視または誤解によって生じる危険にさらされることのない、厳重にセキュリティ保護された環境を構築して、ネットワークのユーザに提供できます。
ゾーン ベースのアプリケーション	SSL 制御機能はゾーン レベルで適用されるため、ネットワーク上で SSL ポリシーを執行することができます。ファイアウォールは、SSL 制御機能が有効になっているゾーンのクライアントからファイアウォールを介して送信される Client Hello を検知すると、検査を開始します。ファイアウォールは、Server Hello と、設定されたポリシーに従った評価のために応答で送信される証明書を探します。例えば、LAN ゾーンで SSL 制御を有効にすると、LAN 上のクライアントから開始されて任意の送信先ゾーンに到達するすべての SSL トラフィックが検査されます。
設定可能なアクションおよびイベント通知	SSL 制御機能によってポリシー違反が検出された場合に、イベントをログに記録して接続を遮断することができます。 あるいは、イベントをログに記録するだけで接続を継続することもできます。

SSL 制御の重要な概念

- **SSL** - セキュア ソケット レイヤ (SSL) は、Netscape が 1995 年に導入したネットワーク セキュリティ メカニズムです。SSL は、2 つの通信アプリケーション (クライアントおよびサーバ) 間でのプライバシーの確保と、サーバ (および必要に応じてクライアント) の認証を目的としていました。SSL の最も有名なアプリケーションは HTTPS です。`http://` の代わりに `https://` で始まる URL によって指定される HTTPS は、インターネット上のウェブ トラフィックを暗号化する標準的な方式として認知されています。SSL HTTP 転送では一般的に TCP ポート 443 が使用されますが、通常の HTTP 転送では TCP ポート 80 が使用されます。SSL は HTTPS で最もよく知られていますが、SSL の使用用途は HTTP のセキュリティ保護に限られたものではありません。SSL は、SMTP、POP3、IMAP、および LDAP などのその他の TCP プロトコルのセキュリティ保護にも使用することができます。SSL セッションの確立は、SSL セッションの確立に示すように行われます。

SSL セッションの確立



- **SSLv2** - SSL の初期バージョンですが、現在も一般的に使用されています。SSLv2 では、いくつかの脆弱性、制限、および理論上の欠陥 (SSLv3 についての説明で比較します) が指摘されていて、セキュリティに厳格な人々の冷笑、軽蔑の対象であり、軽視されるのが当然と見なされています。
- **SSLv3** - SSLv3 は SSLv2 との下位互換性を保ちつつ、以下の点を改善する目的で作成されました。
  - Diffie-Helman を含む、代替鍵交換方式。
  - 鍵交換および一括暗号化の両方でのハードウェア トークンのサポート。
  - SHA、DSS、および Fortezza のサポート。
  - バンド外データ転送。
  - TLS - Transport Layer Security (SSLv3.1 とも呼ばれます) は SSLv3 に非常に似ていますが、SSL と TLS の相違点 テーブルに示した点において SSLv3 が改良されています。

SSL と TLS の相違点

SSL	TLS
暫定的な HMAC アルゴリズムを使用する	RFC 2104 に既定された HMAC を使用する
MAC をバージョン情報に適用しない	MAC をバージョン情報に適用する

SSL と TLS の相違点

SSL	TLS
パディング値を指定しない	パディングを指定された値に初期化する
不十分な警告	詳細な警告メッセージ

メモ：SonicOS 6.2.2.1 以降では、TLS 1.1 と 1.2 をサポートします。

- **MAC** - MAC (メッセージ認証コード) は、(MD5 または SHA1 のような) アルゴリズムをデータに適用して算出されます。MAC はメッセージ ダイジェストつまり一方向性ハッシュ コードであり、算出は非常に簡単ですが、実際に不可逆的なコードです。言い換えると、MAC だけを使用して、ダイジェストの元になっているメッセージを割り出すことは理論上不可能です。同様に、同一のMAC が算出される 2 つの異なるメッセージを見つけることも困難です。ある所定のデータに関して、受信側で算出された MAC が送信側で算出された MAC と一致する場合、受信側では、転送中にデータが変更されなかったと見なすことができます。
- **Client Hello** - TCP セッションの確立後、クライアントからサーバに送信される最初のメッセージ。このメッセージにより SSL セッションが開始されます。 メッセージは次の要素で構成されています。
  - **バージョン** - クライアントが通信での使用を希望する SSL のバージョン。通常は、クライアントでサポートされている SSL の最新バージョンです。
  - **乱数** - 32 ビットのタイムスタンプに 28 バイトの乱数構造を組み合わせたもの。
  - **セッションID** - セッション ID データが存在しない場合は空 (基本的に新しいセッションの要求の場合) です。 あるいは、前に発行されたセッション ID を表します。
  - **暗号スイート** - クライアントでサポートされる暗号化アルゴリズムのリストで、優先する順番に並んでいます。
  - **圧縮方式** - クライアントでサポートされる圧縮方式のリストです (通常はヌル)。
- **Server Hello** - Client Hello に対する SSL サーバの応答。SSL 制御機能によって検査が行われるのは SSL 交換のこの部分です。Server Hello には、セッションでネゴシエートされた SSL のバージョン、暗号、セッション ID、および証明書の情報が含まれています。X.509 サーバの実際の証明書自体は、SSL 交換の別の手順で使用されますが、通常は Server Hello と同じパケットで開始されます (終了も同じ場合があります)。
- **証明書** - X.509 の証明書は、電子的なセキュリティを確保するための、不変のデジタル スタンプです。証明書には、主に 4 つの特性があります。
  - 共通名または識別名 (CN または DN) によって証明書のサブジェクトが識別されます。
  - 通信相手との間のメッセージを暗号化および復号化するために使用する公開鍵が含まれます。
  - 証明書を発行した信頼できる組織 (認証局) のデジタル署名が含まれます。
  - 証明書が有効な日付の範囲が示されます。
- **サブジェクト** - 共通名 (CN) で識別される証明書の保証。クライアントが https://www.mysonicwall.com のような SSL サイトをブラウズした場合、サーバからサーバの証明書が送信され、クライアントで評価されます。クライアントでは、証明書の日付が有効であること、信頼できる CA によって発行された証明書であること、サブジェクトの CN が要求したホスト名に一致すること (つまり両方とも "www.mysonicwall.com" であること) が確認されます。サブジェクトのCN が一致しないとブラウザの警告が表示されますが、これは偽装行為の確かな証拠とは限りません。例えば、クライアントが https://mysonicwall.com をブラウズし、www.mysonicwall.com と同じ IP アドレスに解決された場合、サブジェクトの CN が www.mysonicwall.com と記載さ

れている証明書がサーバから示される場合があります。この場合、接続が完全に適切であるにもかかわらず、クライアントに警告が表示されます。

- **認証局 (CA)** - 認証局 (CA) は、証明書のサブジェクトの識別情報を確認することを主な目的として、証明書に署名することができる信頼できる団体です。よく知られている認証局には、VeriSign、Thawte、Equifax、Digital Signature Trust などがあります。一般的に、SSL フレームワークにおいて CA が信頼できると判断されるためには、ほとんどのウェブ ブラウザ、オペレーティング システムおよびランタイム環境で使用されているように、その証明書が信頼できるストアに格納されている必要があります。SonicOS の信頼できるストアには、「**管理 | システム セットアップ > 装置 > 証明書**」ページからアクセスできます。CA モデルは信頼の積み重ねに基づいています。 つまり、クライアントは (信頼できるストアに CA の証明書があることによって) CA を信頼し、CA は (証明書ごとにサブジェクトを発行することによって) サブジェクトを信頼するため、クライアントがサブジェクトを信頼する、ということになります。
- **信頼できない CA** - 信頼できない CA とは、クライアントの信頼できるストアに含まれていない CA のことです。SSL 制御機能における信頼できない CA とは、証明書が「**管理 | システム セットアップ > 装置 > 証明書**」にない CA のことです。
- **自己署名証明書** - 発行者の共通名とサブジェクトのコモンネームが同一の証明書で、証明書に自己署名されていることを意味します。
- **仮想ホスティング** - 1 つのサーバで複数のウェブ サイトをホスティングするために、ウェブ サーバで使用されている方式。一般的な仮想ホスティング実装は名前ベース (ホスト ヘッダー) の仮想ホスティングで、1 つの IP アドレスで複数のウェブ サイトをホスティングできます。ホスト ヘッダー仮想ホスティングでは、サーバがクライアントから送信された"Host:"ヘッダーを評価して、要求されたサイトを判断します。例えば、`www.website1.com` と `www.website2.com` が両方とも `64.41.140.173` に解決されるとします。この場合に、クライアントが"`GET /`"とともに"`Host: www.website1.com`"を送信すると、サーバからそのサイトに該当するコンテンツが返されます。

  一般的に、ホスト ヘッダー仮想ホスティングは HTTPS では使用されません。 これは、SSL 接続が確立されるまでホスト ヘッダーを読み取ることができない一方、サーバが証明書を送信するまでSSL 接続が確立できないからです。クライアントが要求しているサイトをサーバが判断できないため (SSL ハンドシェイクでは IP アドレスがわかるだけなので)、サーバは送信する適切な証明書を決定できません。いずれかの証明書を送信すれば SSL ハンドシェイクを開始できますが、証明書の名前 (サブジェクト) が一致しなければブラウザに警告が表示されます。
- **脆弱な暗号** - 相対的に脆弱な対称暗号。暗号が 64 ビット未満の場合、脆弱と分類されます。ほとんどの場合、エクスポート暗号は脆弱な暗号です。よく使われている脆弱な暗号 テーブルに、脆弱な暗号のリストを示します。

よく使われている脆弱な暗号

暗号	暗号化	プロトコル
EXP1024-DHE-DSS-DES-CBC-SHA	DES(56)	SSLv3、TLS (エクスポート)
EXP1024-DHE-CBC-SHA	DES(56)	SSLv3、TLS (エクスポート)
EXP1024-RC2-CBC-MD5	RC2(56)	SSLv3、TLS (エクスポート)
EDH-RSA-DES-CBC-SHA	DES(56)	SSLv3、TLS
EDH-DSS-DES-CBC-SHA	DES(56)	SSLv3、TLS
DES-CBC-SHA	DES(56)	SSLv2、SSLv3、TLS
EXP1024-DHE-DSS-RC4-SHA	RC4(56)	SSLv3、TLS (エクスポート)
EXP1024-RC4-SHA	RC4(56)	SSLv3、TLS (エクスポート)

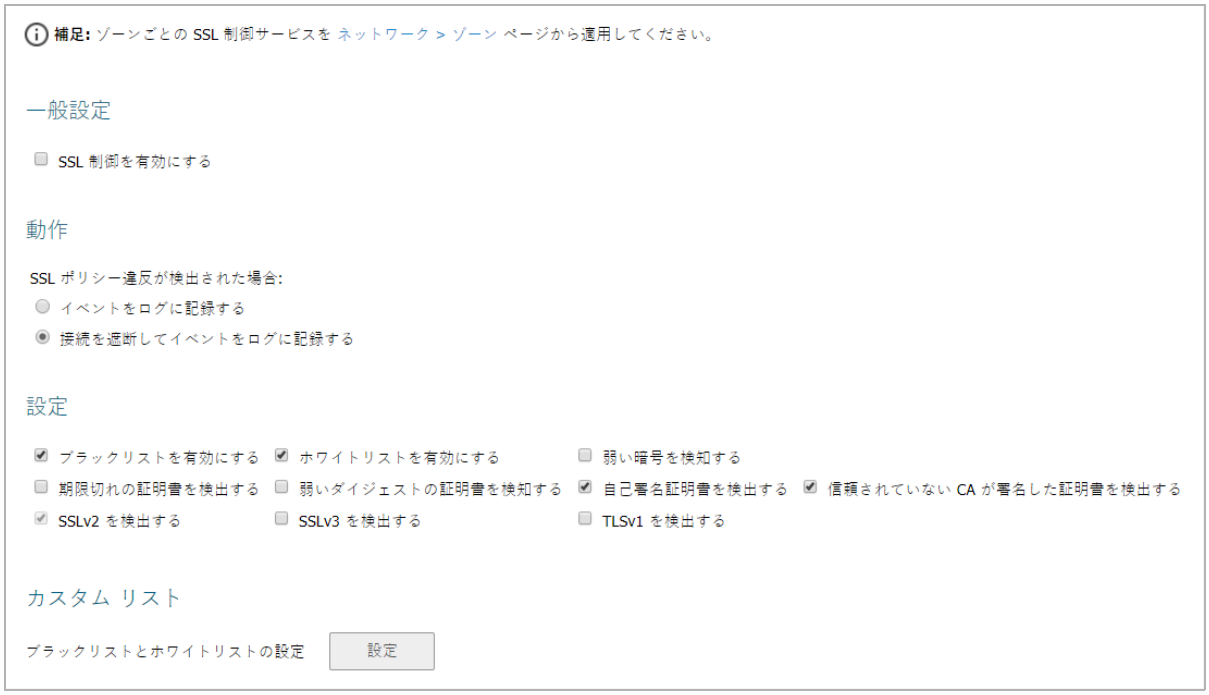
よく使われている脆弱な暗号

暗号	暗号化	プロトコル
EXP1024-RC4-MD5	RC4(56)	SSLv3、TLS (エクスポート)
EXP-EDH-RSA-DES-CBC-SHA	DES(40)	SSLv3、TLS (エクスポート)
EXP-EDH-DSS-DES-CBC-SHA	DES(40)	SSLv3、TLS (エクスポート)
EXP-DES-CBC-SHA	DES(40)	SSLv3、TLS (エクスポート)
EXP-RC2-CBC-MD5	RC2(40)	SSLv2、SSLv3、TLS (エクスポート)
EXP-RC4-MD5	RC4(40)	SSLv2、SSLv3、TLS (エクスポート)

注意事項と推奨事項

1. **自己署名および信頼できない CA の有効化** - これらの 2 つのオプションのいずれかを有効にする場合は、SSL でセキュリティ保護された組織内のネットワーク装置のコモンネームをホワイトリストに追加して、これらの機器への接続が遮断されないようにすることを強くお勧めします。例えば、SonicWall ネットワーク セキュリティ装置の既定のサブジェクト名は "192.168.168.168"、SonicWall SSL VPN 装置の既定のコモンネーム (共通名) は "192.168.200.1" です。
2. 組織独自のプライベート認証局 (CA) を導入している場合は、プライベート CA の証明書を「**システム > 証明書**」ストアにインポートすることを強くお勧めします (特に、信頼できない CA によって発行された証明書の遮断を有効にする場合)。この処理の詳細については、*SonicWall SonicOS 6.5 システム セットアップ*を参照してください。
3. 現段階では、SSL 制御機能による検査は TCP ポート 443 のトラフィックに対してのみ実行されます。標準以外のポートで行われる SSL のネゴシエーションは、現段階では検査されません。
4. **Server Hello の断片化** - SSL サーバによって Server Hello が断片化されることがまれにあります。この場合、現在の SSL 制御機能の実装では、Server Hello の復号化は行われません。SSL 制御ポリシーが SSL セッションに適用されず、SSL セッションが許可されることになります。
5. **セッションの終了処理** - SSL 制御機能では、ポリシー違反が検出されると SSL セッションを終了させますが、これは TCP 層でのセッションを終了させるに過ぎません。この時点では SSL セッションが不完全な状態であるため、クライアントのリダイレクトや、終了に関する何らかの情報通知をクライアントに行うことはできません。
6. **ホワイトリストの優先順位** - ホワイトリストは、他のすべての SSL 制御要素より優先されます。SSL サーバ証明書がホワイトリストのエントリに一致すると、SSL セッションの他の要素が設定されたポリシーの違反に該当する場合であっても、SSL セッションの続行が必ず許可されます。これは、意図的に行われています。
7. 事前インストール済み (既知の) CA 証明書は 93 通あります。これにより、リポジトリはほとんどのウェブ ブラウザで使用されているものに非常に近くなりました。証明書に関しては、これ以外に以下の点が変更されています。
   a. CA 証明書の最大数が 6 から 256 に増加しました。
   b. 個々の CA 証明書の最大サイズが 2,048 から 4,096 に増加しました。
   c. ホワイトリストおよびブラックリストのエントリの最大数が、それぞれ 1,024 になりました。

ファイアウォール設定 > SSL 制御

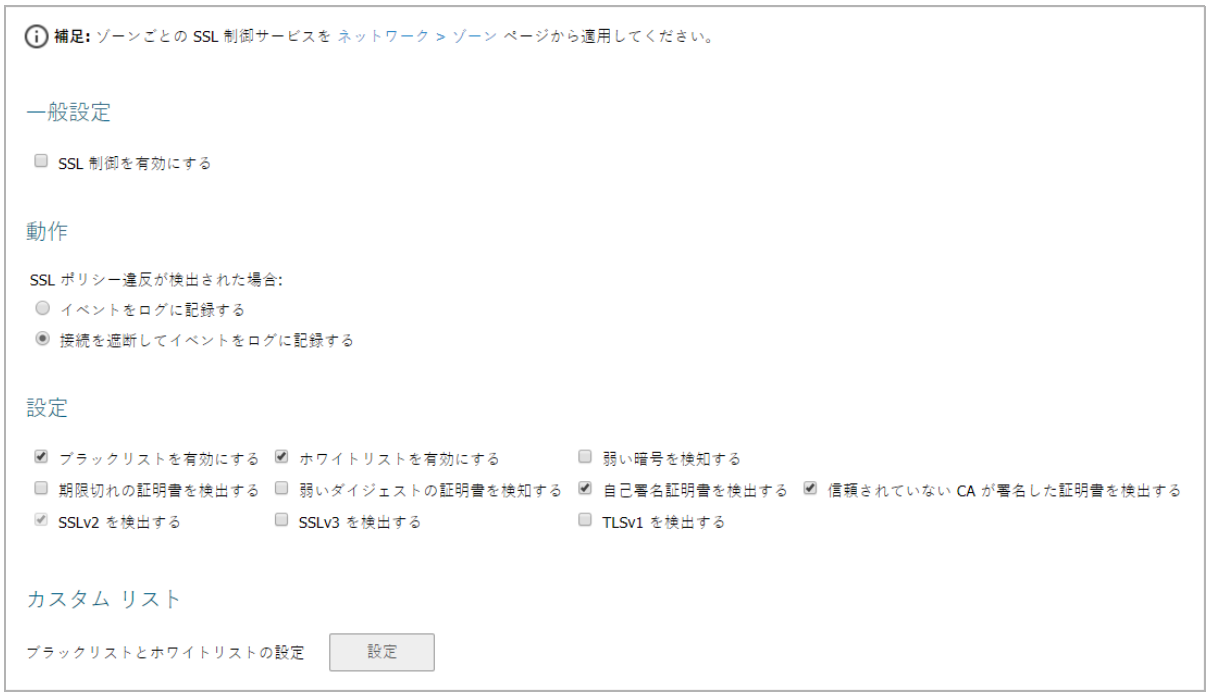


SSL 制御の設定

メモ：SSL 制御を設定する前に、ファイアウォールが IPv6 をサポートしていることを確認してください。「**システム > 診断**」ページの「**IPv6 ネットワーク設定の確認**」ツールを使用して確認できます。『*SonicWall SonicOS 6.5 調査*』を参照してください。

SSL 制御の設定は、「**管理**」ビューの「**セキュリティ設定 > ファイアウォール設定 > SSL 制御**」にあります。SSL 制御には、グローバル設定とゾーン単位の設定があります。既定では、SSL 制御はグローバル レベルでもゾーン レベルでも有効にされていません。それぞれのページには次のような制御項目

があります (このセクションで使われている用語の詳細については、SSL 制御の重要な概念 (100 ページ) を参照してください)。



トピック:

- 一般設定 (106 ページ)
- 動作 (106 ページ)
- 設定 (107 ページ)
- カスタム リスト (108 ページ)

一般設定

「**一般設定**」セクションでは、SSL 制御を有効または無効にできます。

- **SSL 制御を有効にする** - SSL 制御のグローバル設定。ゾーンに適用する SSL 制御を有効にするには、この設定をオンにする必要があります。このオプションは、既定では選択されていません。

動作

「**動作**」セクションでは、SSL ポリシー違反が検出されたときの動作として次のいずれかを選択します。

- **イベントをログに記録する** - 下の「**設定**」セクションで定義される SSL ポリシーに対する違反が検出された場合、イベントをログに記録しますが、SSL 接続の継続は許可されます。このオプションは、既定では選択されていません。
- **接続を遮断してイベントをログに記録する** - ポリシー違反が検出された場合、接続を遮断し、イベントをログに記録します。このオプションは、既定では選択されています。

設定

「**設定**」セクションでは、適用する SSL ポリシーを指定します。

- **ブラックリストを有効にする** - カスタム リストで設定されるブラックリスト内のエントリの検出を制御します。このオプションは、既定では選択されています。
- **ホワイトリストを有効にする** - 下部の「**リストの設定**」セクションで設定されるホワイトリスト内のエントリの検出を制御します。ホワイトリストのエントリは、他のすべての SSL 制御設定より優先されます。このオプションは、既定では選択されています。
- **弱い暗号を検知する** - 一般的にエクスポート暗号で使用される、64 ビット未満の対称暗号でネゴシエートされた SSL セッションの検出を制御します。このオプションは、既定では選択されていません。
- **期限切れの証明書を検出する** - 開始日が現在のシステム時間より前、または終了日が現在のシステム時間より後の証明書の検出を制御します。日付の検証は、ファイアウォールのシステム時間を使用して行われます。「**管理 | システム セットアップ > システム > 時間**」ページの「システム時間」を適切に設定してください。できれば、NTP と同期をとります。このオプションは、既定では選択されていません。
- **弱いダイジェストの証明書を検知する** - MD5 または SHA1 を使用して作成された証明書の検出を制御します。MD5 と SHA1 は安全と見なされていません。このオプションは、既定では選択されていません。
- **自己署名証明書を検出する** - 発行者とサブジェクトのコモンネーム (共通名) が同一の証明書の検出を制御します。このオプションは、既定では選択されています。

  SSL でセキュリティ保護された適切なサイトでは、既知の認証局によって発行された証明書を使用することが一般的であり、これは SSL における信頼の基盤です。また同様に、(SonicWall セキュリティ装置のように) SSL によってセキュリティ保護されたネットワーク装置では、セキュリティ保護のための既定の方法として自己署名証明書を使用することが一般的です。したがって、閉鎖的な環境の自己署名証明書は疑わしくありませんが、公開されているサイトや商業利用サイトで使用されている自己署名証明書は疑わしいものです。自己署名証明書を使用する公開サイトでは、信頼性と識別のためではなく、暗号化のためだけにSSL が使用されていることがよくあります。完全に不正なサイトとは言い切れませんが、SSL で暗号化されたプロキシ サイトで一般的なように、隠蔽が目的である可能性が高いと言えます。自己署名証明書を遮断するポリシーを設定できるため、このようなサイトと通信する危険性に対する防御が可能です。自己署名証明書を使用している既知の信頼できる SSL サイトとの通信が遮断されないようにするには、ホワイトリスト機能を使用して明示的に許可します。
- **信頼されていない CA が署名した証明書を検出する** - 発行者の証明書がファイアウォールの「**管理 | システム セットアップ > 装置 > 証明書**」の信頼できるストアにない証明書の検出を制御します。このオプションは、既定では選択されています。

  自己署名証明書が使用されている場合と同様、信頼できない CA によって発行された証明書が使用されている場合も、あいまい化のための信頼できない行為とは断定できませんが、信頼できるかどうか疑わしいことは確かです。SSL 制御機能では、SSL 交換で使用される証明書の発行者と、大半の既知の CA 証明書が含まれる SonicWall ファイアウォールに保存されている証明書を比較することができます。独自のプライベート認証局を組織で使用している場合は、このプライベート CA を SonicWall のホワイトリストに簡単にインポートして、プライベート CA を信頼された CA として認識されるようにすることができます。

- **SSLv2 を検出する** - SSLv2 交換の検出と遮断を制御します。SSLv2 は、ハンドシェイクの整合性チェックを実行しないため、暗号低下攻撃を受ける可能性が高いとわかっています。SSLv2 ではなく、SSLv3 または TLS を使用することを強くお勧めします。このオプションは、既定では選択されています。また、淡色表示となっており、変更できません。

- **SSLv3 を検出する** - SSLv3 交換の検出と遮断を制御します。このオプションは、既定では選択されていません。
- **TLSv1 を検出する** - TLSv1 交換の検出と遮断を制御します。このオプションは、既定では選択されていません。

カスタム リスト

「**カスタム リスト**」セクションでは、ユーザ定義のホワイトリストとブラックリストを設定できます。

- **ブラックリストとホワイトリストの設定** - SSL 証明書のコモンネーム (共通名) との比較に使用する文字列を定義できます。エントリでは大文字と小文字が区別され、パターン一致方式で使用されます。ブラックリストとホワイトリスト: パターン マッチング テーブルに例を示します。

ブラックリストとホワイトリスト: パターン マッチング

エントリ	一致する URL	一致しない URL
sonicwall.com	https://www.sonicwall.com、 https://csm.demo.sonicwall.com、 https://mysonicwall.com、 https://supersonicwall.computers.org、 https://67.115.118.87 [1]	https://www.sonicwall.de
prox	https://proxify.org、 https://www.proxify.org、 https://megaproxy.com、 https://1070652204 [2]	https://www.freeproxy.ru [3]

1. `67.115.118.67` は sslvpn.demo.sonicwall.com を解決すると得られる IP アドレスで、このサイトでは `sslvpn.demo.sonicwall.com` に対して発行された証明書が使用されています。したがって、証明書の共通名の比較が行われるため、“`sonicwall.com`” と一致する URL として検出されます。
2. これは、IP アドレス `63.208.219.44` の 10 進法表記です。 この証明書は `www.megaproxy.com` に対して発行されたものです。
3. `www.freeproxy.ru` サイトの証明書の共通名は `"-"` に対して発行された自己署名証明書であるため、“`prox`” には一致しません。ただし、自己署名証明書または信頼できない CA の証明書の制御を有効にすることで、この URL を簡単に遮断できます。

ホワイトリストとブラックリストを設定するには:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > SSL 制御**」ページに移動します。

2 「**設定**」を選択します。「**カスタム リスト**」ダイアログが表示されます。

3 ブラック リストまたはホワイト リストのテーブルに証明書を追加するには、対応する「**追加**」を選択します。「**ブラックリスト/ホワイトリスト ドメイン エントリの追加**」ダイアログが表示されます。

4 「**証明書コモンネーム**」フィールドに証明書の名前を入力します。

ヒント： リストの一致検出は、クライアントが要求した URL (リソース) ではなく、SSL 交換でやり取りされる証明書のサブジェクト コモンネームに基づいて行われます。

各リスト テーブルの下部にあるボタンを使用して、証明書を編集および削除できます。

5 「**OK**」を選択します。

SSL 制御設定を変更しても、その時点で確立している接続には反映されません。変更の確定後に行われる新しい SSL 交換のみが検査され、影響を受けます。

6 「**OK**」を選択します。

7 「**適用**」を選択します。

ゾーンでの SSL 制御の有効化

SSL 制御をグローバルに有効にして必要なオプションを設定した後、1 つまたは複数のゾーンで SSL 制御を有効にする必要があります。ファイアウォールは、SSL 制御機能が有効にされているゾーンのクライアントからファイアウォールを介して送信される Client Hello を検知すると、検査を開始します。続いて、Server Hello と、応答で送信される証明書が検知され、設定されたポリシーに従って評価されます。例えば、LAN ゾーンで SSL 制御を有効にすると、LAN 上のクライアントから開始され任意の送信先ゾーンに到達するすべての SSL トラフィックが検査されます。

メモ：あるゾーン (例えば、LAN ゾーン) の SSL 制御を有効にして、そのゾーンのクライアントがファイアウォールに接続された別のゾーン (例えば、DMZ ゾーン) の SSL サーバにアクセスする場合、そのサーバの証明書のサブジェクト コモンネームをホワイトリストに追加して、信頼できるアクセスが継続するようにすることをお勧めします。

ゾーンでSSL 制御を有効にするには、以下の手順に従います。

1 「**管理 | システム セットアップ > ネットワーク > ゾーン**」ページに移動します。

2 設定するゾーンの**設定**アイコンを選択します。「**ゾーンの編集**」ダイアログが表示されます。

3 「**SSL 制御を有効にする**」オプションを選択します。「ゾーンの編集」ダイアログの残りのオプションを設定する場合は、『*SonicWall SonicOS 6.5 システム セットアップ*』を参照してください。

4 「**OK**」を選択します。これで、このゾーンから開始されるすべての新しい SSL 接続に対して検査が実行されるようになります。

SSL 制御のイベント

ユーザが手動でログインした場合または CIA/シングル サイン オンによって識別された場合は、ログ イベントの補足セクション (非提示) にクライアントのユーザ名が含まれています。識別できなかったユーザについては、補足に「識別されていません」と表示されます。

SSL 制御: イベント メッセージ

#	イベント メッセージ	発生条件
1	SSL 制御: Certificate with invalid date【SSL 制御: 証明書の日付が不正】	証明書の開始日が SonicWall のシステム時刻より前か、終了日がシステム時刻より後です。
2	SSL Control: Certificate chain not complete【SSL 制御: 証明書チェーンが不完全】	信頼できる上位 CA を持つ中間 CA により証明書が発行されていますが、SSL サーバが中間証明書を提示しませんでした。このログ イベントは情報提供のためのもので、SSL 接続には影響しません。
3	SSL 制御: Self-signed certificate 【SSL 制御: 自己署名証明書】	証明書が自己署名証明書です (発行者の CN とサブジェクトが一致)。 **メモ**：自己署名証明書制御の強制については、注意事項と推奨事項 (104 ページ) を参照してください。
4	SSL 制御: Untrusted CA 【SSL 制御: 信頼できない CA】	ファイアウォールの「**システム > 証明書**」ストアにない CA によって証明書が発行されています。 **メモ**：自己署名証明書制御の強制については、注意事項と推奨事項 (104 ページ) を参照してください。
5	SSL 制御: Website found in blacklist 【SSL 制御: ブラックリストに登録されたウェブサイト】	サブジェクトの共通名がブラックリストに指定されたパターンと一致します。
6	SSL 制御: Weak cipher being used 【SSL 制御: 脆弱な暗号を使用】	ネゴシエーションされた対称暗号が 64 ビット未満でした。脆弱な暗号のリストについては、よく使われている脆弱な暗号 テーブルを参照してください。
7	#2、SSL Control: Certificate chain not complete【SSL 制御: 証明書チェーンが不完全】 を参照	#2、SSL Control: Certificate chain not complete【SSL 制御: 証明書チェーンが不完全】 を参照

SSL 制御: イベント メッセージ

#	イベント メッセージ	発生条件
8	SSL 制御: Failed to decode Server Hello 【SSL 制御: Server Hello のデコード失敗】	SSL サーバからの Server Hello を判読できませんでした。SonicWall 装置上の SSL サーバに接続する場合のように、証明書と Server Hello が別のパケットのときにも発生します。このログ イベントは情報提供のためのもので、SSL 接続には影響しません。
9	SSL 制御: Website found in whitelist 【SSL 制御: ホワイトリストに登録されたウェブサイト】	サブジェクト (通常はウェブサイト) の共通名がホワイトリストに指定されたパターンと一致します。SSLv2 や脆弱な暗号など、ネゴシエーションの中でその他のポリシーの違反があった場合でも、ホワイトリストのエントリは常に許可されます。
10	SSL 制御: HTTPS via SSL2 【SSL 制御: SSLv2 経由の HTTPS】	SSL セッションのネゴシエーションで SSL v2 が使用されました。 SSL v2 は特定のMan-in-the-Middle 攻撃を受けやすいとされています。SSLv2 ではなく、SSLv3 または TLSを使用することを強くお勧めします。

7

暗号制御の設定

- 暗号制御について (112 ページ)
- ファイアウォール設定 > 暗号制御 (112 ページ)

暗号制御について

SonicOS 6.5.4.1 以降では、TLS 暗号および SSH 暗号の一部またはすべてを許可または遮断できます。この機能は次のものに適用されます。

- DPI-SSL (ファイアウォールによって検査される TLS トラフィック)
- HTTPS MGMT (ファイアウォールにアクセスする TLS セッション)
- SSL 制御 (ファイアウォールを通過する TLS トラフィックを検査: 非 DPI-SSL)

TLS 暗号の変更はすべての TLS トラフィックに適用されます。

ファイアウォール設定 > 暗号制御 ページに表示される暗号のリストは、既知の TLS 暗号のリストです。暗号のリストは、サポートされている暗号のスーパーセットです。このリストには既知のすべての暗号が含まれていますが、DPI-SSL および HTTPS MGMT でサポートされている暗号の種類はそれよりもずっと少数です。例えば、DPI-SSL および HTTPS MGMT は、TLS 1.3 暗号をまだサポートしていません。また、**ファイアウォール設定 > 暗号制御** にリストされているいくつかの弱い暗号をサポートしていません。

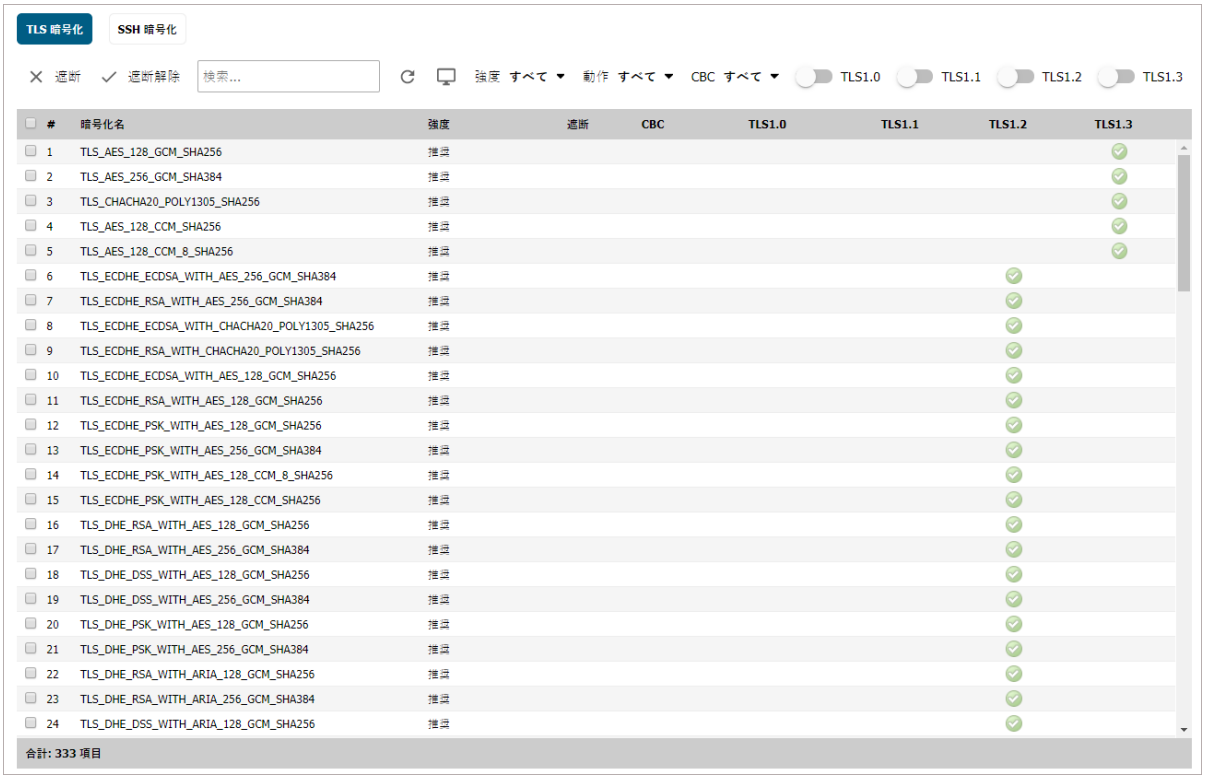
暗号は、セキュリティ強度に基づいて順序付けられており、最上位の暗号は下位の暗号よりも安全です。DPI-SSL および HTTPS MGMT 実装の両方は、**ファイアウォール設定 > 暗号制御** に基づいてサポートされる暗号の相対的な順序を使用します。つまり、DPI-SSL がサポートする暗号の場合、DPI-SSL は **ファイアウォール設定 > 暗号制御** にリストされている暗号に基づいてそれらを順序付けます。同じことが HTTPS MGMT 暗号にも当てはまります。

ファイアウォール設定 > 暗号制御

トピック:

- TLS 暗号 (113 ページ)
- SSH 暗号 (118 ページ)

TLS 暗号



暗号化名 暗号の名前

強度 暗号の強度:

- **推奨**
- **保護**
- **脆弱**
- **安全でない**

遮断 「**遮断**」アイコンは、使われないように遮断された暗号かどうかを示します

CBC 「**有効**」アイコンは、CBC (暗号ブロック連鎖) モードの暗号かどうかを示します

TLS1.0
TLS1.1
TLS1.2
TLS1.3

「**有効**」アイコンは、TLS (Transport Layer Security) プロトコル バージョンで使用されている暗号かどうかを示します

合計 テーブル内の暗号エントリの総数を示します

トピック:

- 暗号の遮断/遮断解除 (114 ページ)
- 暗号のフィルタリング (114 ページ)

暗号の遮断/遮断解除

暗号を遮断するには:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 暗号制御**」に移動します。

2 「**TLS 暗号**」を選択します。

3 次のどちらかを行います。

- 遮断する暗号を選択します。
- テーブル見出しにある該当するチェックボックスをオンにします。

4 「**X 遮断**」を選択します。「**遮断**」アイコンは、遮断された暗号ごとに「**遮断**」列に表示されます。

暗号の遮断を解除するには:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 暗号制御**」に移動します。

2 「**TLS 暗号**」を選択します。

3 次のどちらかを行います。

- 遮断解除する暗号を選択します。
- テーブル見出しにある該当するチェックボックスをオンにします。

4 「**遮断解除**」を選択します。遮断された暗号の「**遮断**」列に「**遮断**」アイコンが表示されなくなりました。

暗号のフィルタリング

暗号をフィルタリングして、許可または遮断する暗号を簡単に設定できます。

トピック:

- 表示オプションの選択 (114 ページ)
- 強度別に暗号を表示する (115 ページ)
- 遮断/遮断解除別で暗号を表示する (116 ページ)
- CBC モードのオン/オフ別に暗号を表示する (117 ページ)
- TLS プロトコル バージョン別に暗号を表示する (117 ページ)

表示オプションの選択

「**TLS 暗号**」テーブルは、どの TSL プロトコルでどの暗号がサポートされているかを示します。これらの暗号をサポートするその他のプロトコルを表示することもできます。

- DPI-SSL
- HTTPS 管理
- SSL 制御

「**表示**」アイコンは、機能的な使用例 (DPI-SSL、HTTPS MGMT、およびパススルー トラフィック) に基づいて暗号をフィルタリングするのに役立ちます。例えば、暗号 X が遮断されている場合、予想される動作は次のとおりです。

- **DPI-SSL** - 暗号 X はもはや TLS コンテキストの一部ではなく、オリジン サーバとのファイアウォール ハンドシェイクによって送信されるクライアント アドバタイズ暗号の一部ではありません。
- **HTTPS 管理** -暗号 X は、ファイアウォールで実行されている HTTPS 管理サーバ アプリケーションの一部ではありません。したがって、TLS クライアントが暗号 X のみをネゴシエートする場合、クライアントとファイアウォール間の TLS ハンドシェイクは失敗します。
- **SSL 制御** - これはファイアウォールを通過するトラフィック (DPI-SSL 復号化セッション以外) を指すため、ファイアウォールは、暗号 X を使用/ネゴシエートするオリジン クライアントとオリジン サーバ間の TLS 接続を遮断します。

他のプロトコルを表示するには:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 暗号制御**」に移動します。

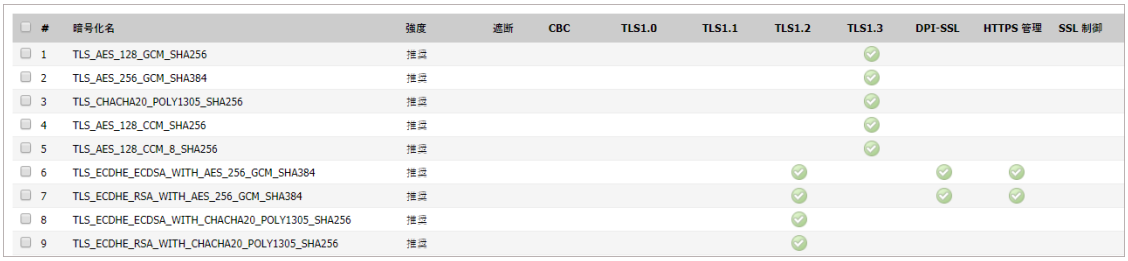
2 「**TLS 暗号**」を選択します。

3 「**表示オプション**」アイコンを選択します。「**表示する列の選択**」ポップアップが表示されます。

4 表示するプロトコルを選択します:

- **DPI-SSL** - このオプションは、既定では選択されていません。
- **HTTPS 管理** - このオプションは、既定では選択されていません。
- **SSL 制御** - このオプションは、既定では選択されていません。
- **数値フィールドにカンマを表示する** - このオプションは、既定では選択されています。

5 「**保存**」を選択します。列が「**TLS 暗号**」テーブルに追加されます。



#	暗号化名	強度	遮断	CBC	TLS1.0	TLS1.1	TLS1.2	TLS1.3	DPI-SSL	HTTPS 管理	SSL 制御
1	TLS_AES_128_GCM_SHA256	推奨						✓			
2	TLS_AES_256_GCM_SHA384	推奨						✓			
3	TLS_CHACHA20_POLY1305_SHA256	推奨						✓			
4	TLS_AES_128_CCM_SHA256	推奨						✓			
5	TLS_AES_128_CCM_8_SHA256	推奨						✓			
6	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	推奨					✓		✓	✓	
7	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	推奨					✓		✓	✓	
8	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	推奨					✓				
9	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	推奨					✓				

強度別に暗号を表示する

暗号は、その強度に従って評価されます。

- 推奨
- 保護
- 安全でない
- 脆弱

「**TLS 暗号**」テーブルは、すべての強度のすべての暗号を示します。「**TLS 暗号**」テーブルを制限して、特定の強度の暗号のみを表示できます。

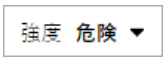
強度別に暗号を表示するには:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 暗号制御**」に移動します。

2 「**TLS 暗号**」を選択します。

3 強度を「**強度**」から選択します。既定は「**すべて**」です。

対応する強度を持つ暗号のみを示す「**TLS 暗号**」テーブルが再表示され、表示されている強度が「**強度**」ドロップダウン メニューに反映されます。



遮断/遮断解除別で暗号を表示する

「**TLS 暗号**」テーブルは、すべての遮断された暗号と遮断されていない暗号を示します。「**TLS 暗号**」テーブルを制限して、遮断または遮断解除された暗号のみを表示できます。

強度別に暗号を表示するには:

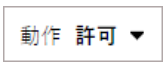
1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 暗号制御**」に移動します。

2 「**TLS 暗号**」を選択します。

3 「**動作**」から動作の許可/遮断を選択します。

- **すべて** (既定)
- **許可** (遮断解除)
- **遮断**

対応する動作を持つ暗号のみを示す「**TLS 暗号**」テーブルが再表示され、「**動作**」は表示された動作を反映します。



CBC モードのオン/オフ別に暗号を表示する

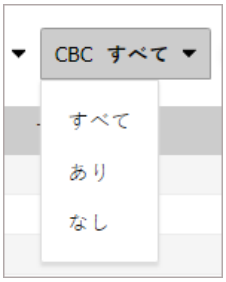
「**TLS 暗号**」テーブルは、CBC モードを使用しているかどうかに関係なく、すべての暗号のすべての暗号を示します。CBS モードがオンまたはオフの暗号のみを示すように表示を制限できます。

CBC モードがオンまたはオフの暗号を表示するには:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 暗号制御**」に移動します。

2 「**TLS 暗号**」を選択します。

3 「**CBC**」から、暗号の CBC モードがオンかオフかを選択します。



- **すべて** (既定)
- **あり** (CBC モード)
- **なし** (CBC モードでない)

選択に従って「**TLS 暗号**」テーブルが再表示され、CBC モードの暗号では「**CBC**」列の「**有効**」アイコンがオン、そうでない暗号では「**CBC**」列がオフになります。

TLS プロトコル バージョン別に暗号を表示する

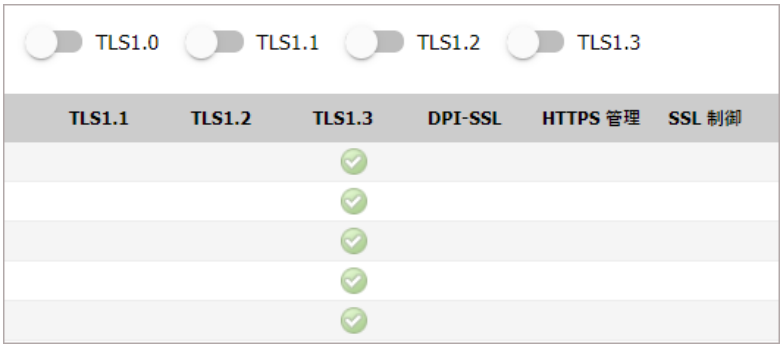
「**TLS 暗号**」テーブルは、すべての TLS プロトコル バージョンのすべての暗号を示します。サポートしている TLS プロトコルのバージョンごとに暗号の表示を制限できます。

TLS プロトコル別に暗号を表示するには:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 暗号制御**」に移動します。

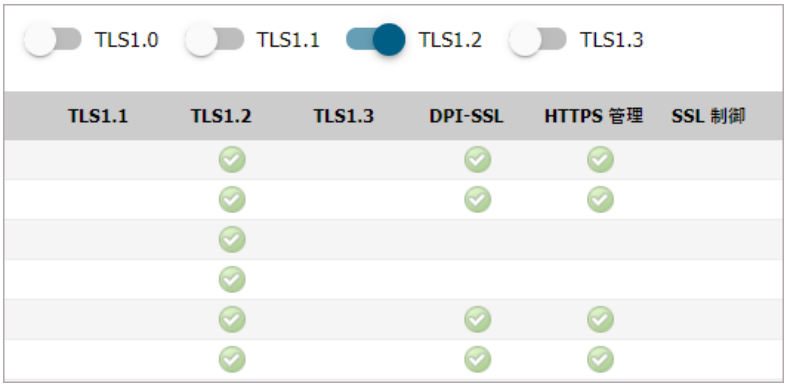
2 「**TLS 暗号**」を選択します。

3 表示する暗号の、**TLS** バージョンを選択します。



- **TLS1.0**
- **TLS1.1**
- **TLS1.2**
- **TLS1.3**

選択した TLS バージョンをサポートしている暗号のみを示すように表示が制限されます。



メモ：選択したバージョン以外もサポートしている暗号では、サポートされている他のバージョンについても「有効」アイコンが表示されます。

SSH 暗号

「管理 | セキュリティ設定 > ファイアウォール設定 > 暗号制御」の「SSH 暗号」ページでは、SonicOS でどの暗号化 SSH 暗号を使用するかを指定できます。

鍵交換アルゴリズム	通信する双方の間で暗号化鍵を交換するための暗号化アルゴリズムがリストされます
パブリック鍵アルゴリズム	パブリック鍵のペアを使用する非対称暗号化アルゴリズムがリストされます
暗号化アルゴリズム	FTP 転送など、ファイルの安全な転送に使用される暗号化アルゴリズムがリストされます
MAC アルゴリズム	MAC (メッセージ認証コード) 値に基づくメッセージ認証アルゴリズムがリストされます

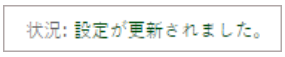
SSH 暗号を選択または選択解除するには:

1 「**管理 | セキュリティ設定 > ファイアウォール設定 > 暗号制御**」に移動します。

2 「**SSH 暗号**」を選択します。

重要：既定では、すべての SSH 暗号が選択されています。

3 使用または無視する SSH アルゴリズムを選択します。画面の下部に状況メッセージが表示されます。



ヒント：処理メッセージが短時間だけ表示されることもあります。

第 2 部

セキュリティ 設定 | セキュリティ サービス

- SonicWall セキュリティ サービスの管理
- コンテンツ フィルタ サービスの設定
- DPI-SSL 強制
- SonicWall クライアント アンチウイルスの有効化
- クライアント CF 強制の設定
- SonicWall ゲートウェイ アンチウイルス サービスの管理
- 侵入防御サービスの有効化
- キャプチャ ATP の設定
- アンチスパイウェア サービスの有効化
- SonicWall リアルタイム ブラックリストの設定
- 地域 IP フィルタの設定
- ボットネット フィルタの設定

8

SonicWall セキュリティ サービスの管理

- SonicWall セキュリティ サービスについて (121 ページ)
- セキュリティ サービスの設定 (122 ページ)

SonicWall セキュリティ サービスについて

SonicWall は、ネットワークに多層的なセキュリティを提供する購読ベースのさまざまなセキュリティ サービスを用意しています。SonicWall のセキュリティ サービスは、ネットワークとシームレスに統合して完全な保護を提供するように設計されています。

以下の購読制のセキュリティ サービスは、ファイアウォールの管理インターフェースの「**セキュリティ サービス**」に一覧表示されています。

- SonicWall コンテンツ フィルタ サービス
- SonicWall クライアント アンチウイルス
- SonicWall ゲートウェイ アンチウイルス
- SonicWall 侵入防御サービス
- SonicWall アンチスパイウェア
- SonicWall RBL フィルタ
- SonicWall 地域 IP フィルタ
- SonicWall ボットネット フィルタ

ヒント：ファイアウォールを 登録すると、無料トライアル版の SonicWall コンテンツ フィルタ サービス、SonicWall クライアント アンチウイルス、SonicWall ゲートウェイ アンチウイルス、SonicWall 侵入防御サービス、および SonicWall アンチスパイウェアをご試用いただけます。

SonicWall セキュリティ サービスは、SonicWall 管理インターフェースから直接、または https://www.mysonicwall.com から有効化および管理できます。

セキュリティ サービスの設定

以下のセクションでは、「**管理 | セキュリティ設定 > セキュリティ サービス > 基本設定**」ページの各パネルで実行するグローバル設定について説明します。

- ライセンスの表示と管理 (122 ページ)
- ライセンスの同期 (123 ページ)
- セキュリティ サービスの設定 (123 ページ)
- プロキシ サーバを通してのシグネチャ ダウンロード (124 ページ)
- セキュリティ サービスに関する情報 (124 ページ)
- シグネチャの手動更新 (124 ページ)

ライセンスの表示と管理

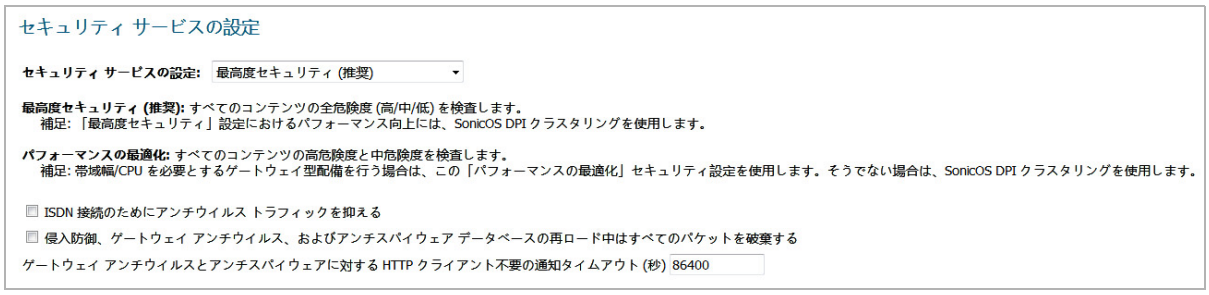
ページの上部に 2 つのリンクが表示されます。

- **ライセンスの概要を表示するには、「管理 > ライセンス」に移動します。** - 「**管理 | 更新 > ライセンス**」ページでリンクを選択して、ライセンスとその状況を表示します。
- **ライセンスを管理するには、www.mysonicwll.com にアクセスしてください。** 「MySonicWall」でリンクを選択して、ライセンスを試用、アップグレード、または購入/更新します。

ライセンスの同期

ライセンスを mysonicwall.com アカウントと同期するには、「**ライセンス情報を www.mysonicwall.com と同期する**」の後ろの「**同期**」ボタンを選択します。

セキュリティ サービスの設定

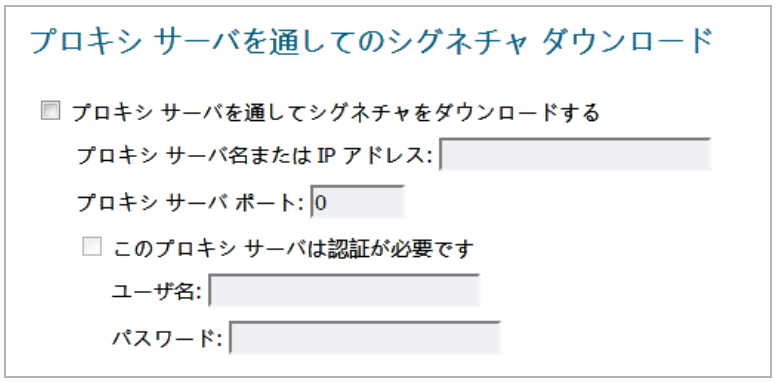


「**セキュリティ サービスの設定**」セクションには、SonicWall のセキュリティ サービスを調整する次のオプションがあります。

- **セキュリティ サービスの設定** - このドロップダウン メニューでは、SonicWall セキュリティ サービスを適用して、セキュリティとパフォーマンスのどちらを最大化するかを指定します。
  - **最高度セキュリティ (推奨)** - すべての脅威の可能性 (高/中/低) について、すべてのコンテンツを検査します。「最高度セキュリティ」設定におけるパフォーマンス向上には、SonicOS HA クラスタリングを使用します。
  - **パフォーマンスの最適化** - 高または中の脅威の可能性について、すべてのコンテンツを検査します。帯域幅または CPU を必要とするゲートウェイ型配備を行う場合は、この「パフォーマンスの最適化」セキュリティ設定を使用します。そうでない場合は、SonicOS HA クラスタリングを使用します。

  「**最高度セキュリティ (推奨)**」設定では、最大の防御が行われます。「**パフォーマンスの最適化**」設定では、既知の脅威の情報を使用して、脅威のランドスケープにおけるアクティブな脅威に対する高い防御が行われます。
- **ISDN 接続のためにアンチウイルス トラフィックを抑える** - この機能を選択すると、SonicWall アンチウイルスでアップデートを 1 日 1 回 (24 時間に 1 回) のみチェックし、“常時"インターネット接続していないユーザの送信トラフィックの頻度を減らすことができます。
- **侵入防御、ゲートウェイ アンチウイルス、およびアンチスパイウェア データベースの再ロード中はすべてのパケットを破棄する** - このオプションを選択すると、IPS、GAV、アンチスパイウェアのデータベースの更新中は、すべてのパケットを破棄することをファイアウォールに指定します。
- **ゲートウェイ アンチウイルスとアンチスパイウェアに対する HTTP クライアント不要の通知タイムアウト (秒)** - HTTP サーバから入り込んだ脅威が GAV またはアンチスパイウェアに検出されたときに、ファイアウォールがユーザに通知するまでのタイムアウト時間を設定します。既定のタイムアウトは 1 日 (86400 秒) です。

プロキシ サーバを通してのシグネチャ ダウンロード



このセクションで提供する機能は、シグネチャをダウンロードするためにプロキシ サーバ経由でインターネットにアクセスしなければならないネットワークで動作する SonicWall ネットワーク セキュリティ装置のためのものです。この機能では、プライバシーを危険にさらすことなく SonicWall ネットワーク セキュリティ装置の登録をプロキシ サーバ経由で行うこともできます。

プロキシ サーバ経由のシグネチャのダウンロードまたは装置の登録を有効にするには、以下の手順に従います。

1 「**プロキシ サーバを通してシグネチャをダウンロードする**」チェックボックスを選択します。

2 「**プロキシ サーバ名または IP アドレス**」フィールドに、プロキシ サーバのホスト名または IP アドレスを入力します。

3 「**プロキシ サーバ ポート**」フィールドに、プロキシ サーバへの接続に使用するポート番号を入力します。

4 プロキシ サーバで**ユーザ名**と**パスワード**が要求される場合は、「**このプロキシ サーバは認証が必要です**」チェックボックスを選択します。

5 その装置が MySonicWall.com に登録されていない場合は、さらに次の 2 つのフィールドが表示されます。

- **ユーザ名** - 装置の登録先となる mysonicwall.com アカウントのユーザ名を入力します。
- **パスワード** - mysonicwall.com アカウントのパスワードを入力します。

6 「**適用**」を選択します。

セキュリティ サービスに関する情報

このパネルは、現在使われていません。

シグネチャの手動更新

「シグネチャの手動更新」は、(セキュリティ上の理由から) 広帯域インターネットにおいて信頼できる接続が不可能な場合または望ましくない場合を想定して設計された機能です。「シグネチャの手動更新」機能を使用すると、最新のシグネチャを自由に更新できます。

1 シグネチャを http://www.mysonicwall.com から別のコンピュータ、USB ドライブ、その他のメディアにダウンロードします。

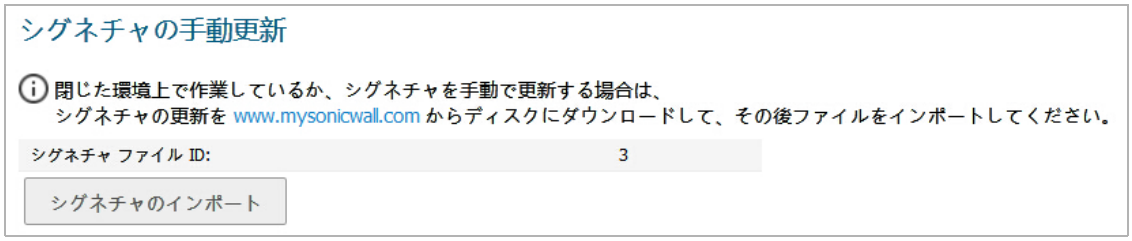
2 その後、ファイアウォールにシグネチャをアップロードします。

次の要件を満たすすべての SonicWall ネットワーク セキュリティ装置で、同じシグネチャ更新ファイルを使用できます。

- 機器がそれぞれ同じ mysonicwall.com アカウントに登録されている
- 機器がそれぞれ SonicWall ネットワークセキュリティ装置の同一クラスに属している

シグネチャ ファイルを手動で更新するには、次の手順に従います。

1 「**セキュリティ サービス > 状況**」ページで、ページの下部にある「**シグネチャの手動更新**」ヘッダーが表示されるまでスクロールします。機器の「**シグネチャ ファイル ID**」を記録します。



2 SonicWall ネットワーク セキュリティ装置の登録に使用した mysonicwall.com アカウントを使用して、http://www.mysonicwall.com にログオンします。

メモ：シグネチャ ファイルは、そのシグネチャ ファイルをダウンロードした mysonicwall.com アカウントに登録されているファイアウォール上でのみ使用できます。

3 「**ダウンロード**」ヘッダーの下部にある「**シグネチャのダウンロード**」を選択します。

4 「**シグネチャ ID:**」の隣にあるプルダウン ウィンドウで、ファイアウォール用の適切なSFID を選択します。

5 「**ここを選択してシグネチャ ファイルをダウンロードしてください。**」を選択して、シグネチャの更新ファイルをダウンロードします。

メモ：残りの手順は、インターネットから切断されている間でも実行することができます。

6 ファイアウォール管理インターフェースの「**セキュリティ サービス > 概要**」ページに戻ります。

7 「**シグネチャのインポート**」ボタンを選択します。

8 表示されたポップアップ ダイアログで、「**参照**」ボタンを選択し、シグネチャ更新ファイルのある場所に移動します。

9 「**インポート**」を選択します。ファイアウォール上で有効になっているセキュリティ サービス用のシグネチャをアップロードします。

9

コンテンツ フィルタ サービスの設定

重要：「**管理 | セキュリティ設定 > セキュリティ サービス > コンテンツ フィルタ**」には、SonicWall CFS 用と Websense Enterprise 用の 2 つのバリアントがあります。

- セキュリティ サービス > コンテンツ フィルタ: SonicWall CFS (127 ページ)
- セキュリティ サービス > コンテンツ フィルタ: Websense Enterprise (140 ページ)

セキュリティ サービス > コンテンツ フィルタ: SonicWall CFS

メモ: ワイヤ モードでは、コンテンツ フィルタ サービス (CFS) コンテンツがサポートされません。

コンテンツ フィルタ オブジェクトには、SonicWall コンテンツ フィルタ サービス (SonicWall CFS) のほか、サードパーティ製の製品 (Websense Enterprise) があり、いずれも「**管理 | セキュリティ設定 > セキュリティ サービス > コンテンツ フィルタ**」ページから有効化したり設定したりできます。

トピック:

- CFS について (128 ページ)
- CFS の有効化 (131 ページ)
- CFS ポリシーの設定 (133 ページ)
- CFS ユーザ定義種別の設定 (133 ページ)

CFS について

SonicWall™ コンテンツ フィルタ サービス (CFS) では、教育機関、企業、図書館、政府機関向けにコンテンツ フィルタが強化されています。こうした組織では、コンテンツ フィルタ オブジェクトの活用により、ウェブサイトを制御したり、学生や従業員が IT 部門から支給されたコンピュータを使用して組織のファイアウォールの背後からのアクセスを行ったりできるようになります。

メモ：CFS の詳細な説明やライセンスおよびインストールの手続きについては、『*SonicWall SonicOS 6.5 リリース ノート*』、『*SonicWall™ コンテンツ フィルタ サービス機能ガイド*』、および『*SonicWall™ コンテンツ フィルタ サービス アップグレード ガイド*』を参照してください。また、CFS ポリシー用のコンテンツ フィルタ オブジェクトの作成方法については、『*SonicWall SonicOS 6.5 ポリシー*』を参照してください。

CFS は、要求されたウェブサイトの内容を、評価済みの何百万という URI、IP アドレス、ウェブサイトが含まれている巨大なクラウド データベースと比較します。また、個別またはグループの ID や時刻に基づいてサイトへのアクセスを許可または拒否するポリシーを作成および適用するためのツールを提供します。

トピック:

- 脅威 API について (128 ページ)
- CFS ポリシーについて (129 ページ)
- コンテンツ フィルタ オブジェクトについて (129 ページ)
- CFS の動作 (130 ページ)
- CFS により個別のビデオを遮断する (130 ページ)
- CFS ログについて (131 ページ)

脅威 API について

重要：脅威 API は、設定前に有効にする必要があります。脅威 API とその有効化方法の詳細については、『*Threat API Reference Manual (脅威 API リファレンス マニュアル)*』を参照してください。

メモ：SonicOS 脅威 API を使用するには、ファイアウォールにコンテンツ フィルタ システム (CFS) ライセンスが必要です。

SonicOS 6.2.7 では、脅威 API 機能がサポートされるようになりました。SonicOS 脅威 API は、SonicWall ファイアウォール サービスへの API アクセスを提供します。現在のファイアウォール GUI/CLI ユーザインターフェースに比べて、脅威 API は簡潔で、標準 HTTP プロトコルを有効に利用します。クラウド配備へと向かう時代の流れの中、脅威 API は従来の SonicOS GUI/CLI よりも簡単に使用できます。

悪意のある脅威が URL や IP アドレスによってもたらされることがあります。これらの脅威のリストは大きく、頻繁に変更される可能性があります。SonicOS には URL と IP アドレスのユーザ定義リストを遮断する機能が既にありますが、ログインして手動でリストを更新する必要があるという点が不便です。API インターフェースを使用すると、これがはるかに容易になります。

脅威リストは、脅威 API の機能を使用して SonicOS に送信されます。脅威は次のどちらかの形式で追加できます。

- URL (`https://malicious123.example.com/malware`)
- IP アドレス (`10.10.1.25`)

サードパーティは脅威リストを生成し、脅威 API を使用してファイアウォールに渡すことができます。

脅威リスト内の IP アドレスについては、SonicOS はまず既定の脅威 API アドレス グループを作成し、次に脅威リスト内の IP アドレスごとにアドレス オブジェクト (AO) を作成します。その後、そのアドレス グループを参照して IP アドレスを遮断するファイアウォール アクセス ルールを設定します。

SonicOS は、CFS 脅威 URI リストに URL を追加します。関連付けられている CFS プロファイルで脅威 API 強制を有効にし、脅威リスト内の URL を遮断するようにコンテンツ フィルタ システム (CFS) ポリシーを設定します。脅威が CFS によって遮断されると、ユーザのブラウザに遮断メッセージが表示されます。

CFS ポリシーについて

CFS ポリシーを使うと、パケットを (設定済みの CFS 動作を適用することで) フィルタするか、ユーザにそのまま渡すかを決定することができます。CFS ポリシーは、パケットとの照合に使うフィルタ条件を定義します。

- 名前
- 送信元ゾーン
- 送信先ゾーン
- 送信元アドレス
- ユーザ/グループ
- スケジュール

パケットがすべての定義済みの条件に一致する場合、そのパケットは対応する CFS プロファイルに基づいてフィルタリングされ、CFS 動作が適用されます。

メモ：照合時に使用できるユーザ/グループの認証データがない場合、この条件に対する照合は行われません。特にシングル サインオンが使用される場合は、この方針によってパフォーマンスの問題が回避されます。

各 CFS ポリシーには優先順位レベルがあり、優先順位の高いポリシーが先に確認されます。

CFS では、すべての設定済みポリシーを管理するためにポリシー テーブルを内部で使用しています。ポリシー要素ごとに、設定データと実行時データによってテーブルが構築されています。設定データには、ポリシー名やプロパティなど、ユーザ インターフェースからポリシーを定義するパラメータが含まれています。実行時データには、パケット処理で使用されるパラメータが含まれています。

CFS では、条件に対して照合する際に、実行時のポリシー検索を高速化するためにポリシー検索テーブルも使用します。

- 送信元ゾーン
- 送信先ゾーン
- IPv4 AO
- IPv6 AO

コンテンツ フィルタ オブジェクトについて

CFS では、CFS ポリシー内のコンテンツ フィルタ オブジェクトを使って、フィルタ処理する URI とドメインを特定し、フィルタ時にどのタイプの動作を実行するかを指定します。コンテンツ フィルタ オブジェクトの詳細については、*SonicWall SonicOS 6.5 ポリシー*を参照してください。

CFS の格付け方式では、ドメインは、以下の 4 つのレベルのいずれかに格付けされます。ここでは、優先度の高いものから低いものへ並べています。

1 遮断
2 パスワード
3 確認
4 BWM (帯域幅管理)

URL がこれらのいずれの格付けにも分類されていない場合、操作は許可されます。

CFS の動作

1 パケットが到着し、CFS によって検査されます。
2 CFS は、パケットを設定済みの除外アドレスと照合し、一致する項目が見つかればパケットを許可します。
3 CFS は、ポリシーを確認して、パケット内の以下の条件に一致する最初のポリシーを探します。
   - 送信元ゾーン
   - 送信先ゾーン
   - アドレス オブジェクト
   - ユーザ/グループ
   - スケジュール
   - 有効状態
4 CFS は、一致したポリシーで定義されている CFS プロファイルを用いてフィルタリングを行い、そのパケットに対応する動作を返します。

   メモ：一致するポリシーが存在しない場合は、CFS による動作なしでパケットが通過します。

5 CFS は、一致したポリシーの CFS 動作オブジェクトで定義された動作を実行します。

CFS により個別のビデオを遮断する

SonicWall コンテンツ フィルタ サービス (CFS) で個別の YouTube ビデオを選択的にフィルタし、遮断できるようになりました。

メモ：SonicWall CFS では、*個別の* YouTube ビデオのみ遮断できます。ビデオの種別を遮断することはできません。SonicWall CFS サーバに、URI の「v=」パラメータで識別される特定のビデオの評価がある場合にのみ、この機能が有効になります。遮断する各ビデオの URI を個別に SonicWall CFS に追加する必要があります。

この機能は、ローカル CFS サーバの使用時にはサポートされません。SonicWall パブリック CFS サーバの使用時のみサポートされます。ローカル CFS サーバが持つブラックリスト/ホワイトリスト機能との競合を避けるためです。

この機能の使用に SonicOS の設定は不要です。

CFS ログについて

「管理 | ログと報告 > ログ設定 > 基本設定」では、**「セキュリティ サービス」**種別の下に**「コンテンツ フィルタ」**が追加されました。この新しい下位の種別は、次のログを表示します。

- CFS 警告
- アクセス済みのウェブサイト
- 遮断済みのウェブサイト

これらのログの設定については、『*SonicWall SonicOS 6.5 ログとレポート*』を参照してください。

CFS の有効化

重要：CFS を有効化し、CFS ポリシーを設定する前に、『*SonicWall SonicOS 6.5 ポリシー*』の説明に従ってコンテンツ フィルタ オブジェクトを設定してください。

CFS を有効にするには:

1. **「管理 | セキュリティ設定 > セキュリティ サービス > コンテンツ フィルタ」**ページに移動します。
2. **「コンテンツ フィルタ種別」**ドロップダウン メニューから、コンテンツ フィルタ サービスを選択します。
   - **SonicWall CFS** (既定)
   - **Websense Enterprise** (Websense Enterprise の設定方法については、セキュリティ サービス > コンテンツ フィルタ: Websense Enterprise (140 ページ) を参照)
3. **「グローバル設定」**セクションで、キャッシュできる最大 URL 登録数を**「最大 URL キャッシュ (登録数)」**フィールドに指定します。既定値は **51200** です。

   URL 格付けがキャッシュ内に URL 登録と共に保存されます。こうすることで、既知の URL の処理が速くなります。
4. すべてのパケットに対してコンテンツ フィルタを有効にするには、**「コンテンツ フィルタ サービス (CFS) を有効にする」**チェックボックスをオンにします。このオプションは、既定では選択されています。 すべてのパケットに対してコンテンツ フィルタを適用しない場合は、このオプションの選択を外します。
5. HTTPS サイトに対してコンテンツ フィルタを有効にするには、**「HTTPS コンテンツ フィルタを有効にする」**チェックボックスを選択します。このオプションは、既定では選択されていません。

   このオプションを有効にすると、CFS は URL 格付け検索を次の順序で実行します。

   a クライアント `hello` を検索してサーバ名を探します。CFS は、サーバ名を URL 格付けの取得に使用します。

   b サーバ名が使用できない場合は、SSL 証明書を検索してコモンネームを探します。CFS は、コモンネームを URL 格付けの取得に使用します。

   c サーバ名もコモンネームも使用できない場合は、CFS は、IP アドレスを URL 格付けの取得に使用します。
6. フィルタリング時の格付け要求の取得にタイムアウトを指定するには、**「サーバが利用不可の場合に遮断する」**チェックボックスを選択します。このオプションは、既定では選択されていません。

a このオプションを選択すると、「**サーバ タイムアウト**」フィールドが有効になります。CFS サービスが格付けの要求に応答しなければならない最大時間を秒単位で入力します。最小値は 2 秒、最大値は 10 秒、既定値は **5** 秒です。

7 管理者権限を持つアカウントからのすべての要求に対してコンテンツ フィルタをバイパスするには、「**CFS 除外**」セクションの「**管理者を除外する**」チェックボックスをオンにします。このオプションは、既定では選択されています。

8 アドレス オブジェクト種別からの要求に対してコンテンツ フィルタリングを省くには、「**除外アドレス**」ドロップダウン メニューを選択します。既定は「**なし**」です。また、「**アドレス オブジェクトの作成**」を選択して新しいアドレス オブジェクトを作成することもできます。アドレス オブジェクトの作成については、『*SonicWall SonicOS 6.5 ポリシー*』を参照してください。

9 「**適用**」を選択します。

ローカル CFS サーバの有効化

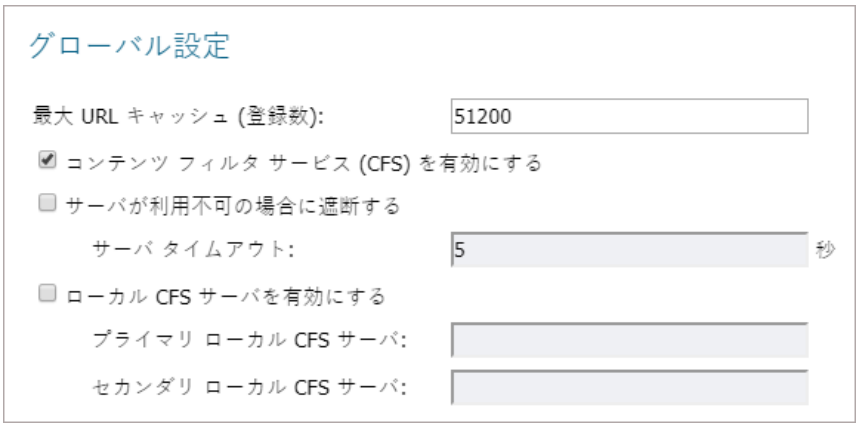
ローカル CFS レスポンダ (ローカル CFS) により、コンテンツ フィルタ サーバが、リモート パブリック レスポンダからではなく、ローカル レスポンダから直接 URL 格付けを受け取ることができるようになります。ローカル CFS の設定と使用については、『*ローカル CFS 管理者ガイド*』参照してください。

ローカル CFS レスポンダを有効にするには:

1 「**管理 | セキュリティ設定 > セキュリティ サービス > コンテンツ フィルタ**」ページに移動します。

2 「**コンテンツ フィルタ種別**」からコンテンツ フィルタ サービスとして**SonicWall CFS** (既定) を選択します。

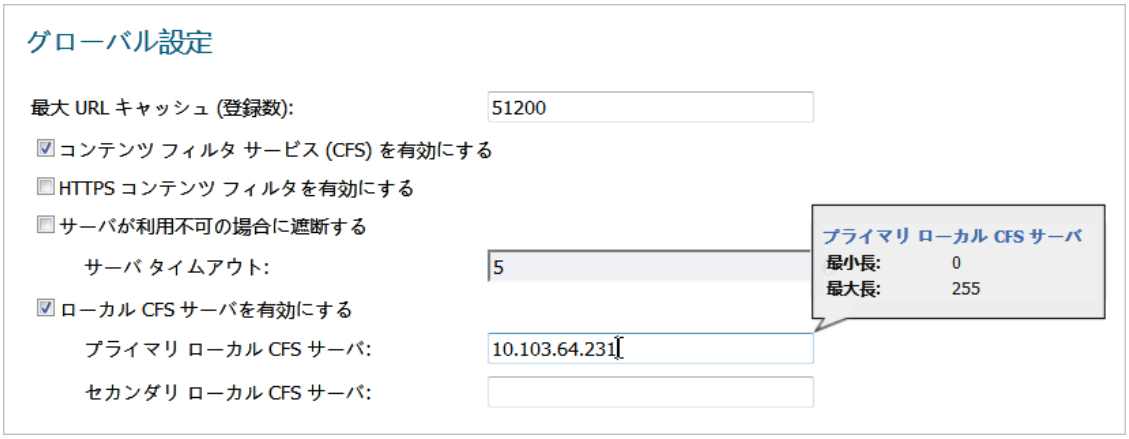
3 「**グローバル設定**」セクションまでスクロールします。



4 「**ローカル CFS サーバ を有効にする**」を選択します。

5 プライマリおよびセカンダリ ローカル CFS サーバの IP アドレスを「**プライマリ ローカル CFS サーバ**」と「**セカンダリ ローカル CFS サーバ**」フィールドに入力します。

6 「**プライマリ ローカル CFS サーバ**」の右にある**統計**アイコン上にマウス ポインタを置くと、入力したサーバの情報が表示されます。



7 「**適用**」を選択します。

CFS ポリシーの設定

CFS ポリシーを追加、編集、または削除するには、「**管理 | ポリシー > オブジェクト > コンテンツ フィルタ オブジェクト**」ページに移動します。詳細については、*SonicWall SonicOS6.5 ポリシー*を参照してください。

CFS ユーザ定義種別の設定

このセクションでは、CFS ユーザ定義種別テーブルについて説明し、この種別の設定、編集、および削除の手順を解説します。CFS ユーザ定義種別テーブルのインポートとエクスポートについても説明します。

トピック:

- CFS ユーザ定義種別テーブルについて (134 ページ)
- CFS ユーザ定義種別テーブルの検索 (134 ページ)
- CFS ユーザ定義種別の設定 (135 ページ)
- CFS ユーザ定義種別テーブルのエクスポート (137 ページ)
- CFS ユーザ定義種別テーブルのインポート (137 ページ)
- CFS ユーザ定義種別の編集 (139 ページ)
- CFS ユーザ定義種別の削除 (139 ページ)

CFS ユーザ定義種別テーブルについて

ドメイン ユーザ定義種別が適用されるドメインの IP アドレス。

種別 ユーザ定義種別に選択された種別。

設定 各ドメインについて**編集**アイコンと**削除**アイコンを表示します。

CFS ユーザ定義種別テーブルの検索

大きなテーブルから特定の IP アドレスを検索するには、次の操作を行います。

1 「ポリシーをアドレスで検索」フィールドに IP アドレスを入力します。IP アドレスは次のどちらかの形式で指定できます。

- `192.168.168.168`
- `fe80::c2ea:e4ff:fe59:a634`

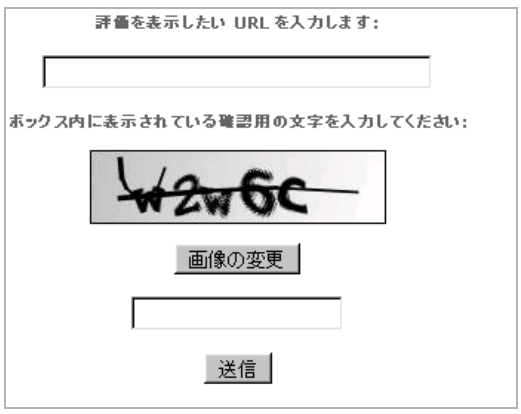
2 **検索** (虫眼鏡) アイコンを選択します。

検閲種別への登録要望

ウェブ サイトの格付けに誤りがあると考えられる場合や、新しい URI を登録したい場合は、次のいずれかの方法で SonicWall コンテンツ フィルタ サービスに登録要望を送信します。

- 「**セキュリティ サービス > コンテンツ フィルタ**」ページの上部にある「ウェブ サイト格付けに関する質問および新しい URL の追加に関しては、ここを選択してください。」のリンクをクリックします。
- http://cfssupport.sonicwall.com/Support/web/eng/newui/viewRating.jsp に移動します。

「**CFS URL 格付け要求**」フォームが表示されます。



CFS ユーザ定義種別の設定

特定の URL の格付けを変更できます。最大 5,000 件の登録がサポートされます。ユーザ定義種別は、バックエンド サーバによって提供されるこうした種別と同じようなプロセスです。CFS はある URL の格付けを確認する際に、まずユーザ格付けをチェックしてから、バックエンド サーバの格付けを確認します。CFS 種別は、バックエンド サーバから渡される設定文字列を使用して動的に管理および作成されます。

トピック: :

- ユーザ定義種別の有効化 (135 ページ)
- ユーザ定義種別の設定 (135 ページ)

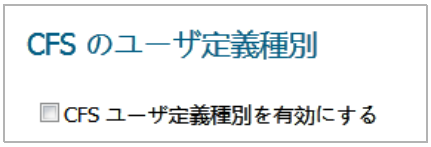
ユーザ定義種別の有効化

ユーザ定義種別を使用するには、このサービスを有効化する必要があります。

ユーザ定義種別を有効化するには:

1 「**管理 | セキュリティ設定 > セキュリティ サービス > コンテンツ フィルタ**」に移動します。

2 「**CFS ユーザ定義種別**」までスクロールします。



3 「**CFS ユーザ定義種別を有効にする**」チェックボックスをオンにします。このオプションは、既定では選択されていません。

4 「**適用**」を選択します。

ユーザ定義種別の設定

ユーザ定義種別を定義するには:

1 「**管理 | セキュリティ設定 > セキュリティ サービス > コンテンツ フィルタ**」に移動します。

2 「**CFS ユーザ定義種別**」までスクロールします。

3 「**追加**」を選択します。「**CFS のユーザ定義種別**」ダイアログが表示されます。

4 「**ドメイン**」フィールドに、ユーザ定義種別を適用するドメインの IP アドレスまたはドメイン名を入力します。

- IP アドレスは次のいずれかの形式で指定できます。
  - `192.168.168.168`
  - `fe80::c2ea:e4ff:fe59:a634`
- ドメイン名の `www.` プレフィックスは省きます。プレフィックスを含めて入力すると、確認を求めるメッセージが表示されます。このメッセージに「**OK**」を選択して応答すると、プレフィックスが「**ドメイン**」フィールド内のドメイン名から削除されます。

5 リストから最大 4 つの種別を選択します。

6 「**追加**」を選択します。

7 CFS ユーザ定義種別をさらに作成するには、種別ごとにステップ 4 からステップ 6 までの手順を繰り返します。

> **メモ**：作成したユーザ定義種別は、「**CFS のユーザ定義種別**」テーブルにそれぞれ 1 項目として登録されます。複数が 1 項目に連結されることはありません。

8 「**閉じる**」を選択します。「**CFS のユーザ定義種別**」テーブルが更新されます。

CFS ユーザ定義種別テーブルのエクスポート

「**CFS のユーザ定義種別**」テーブルは、.wri ファイルにエクスポートできます。このファイルは、編集したり、後でインポートするために保存しておくことができます。

CFS ユーザ定義種別テーブルをエクスポートするには:

1 「**管理 | セキュリティ設定 > セキュリティ サービス > コンテンツ フィルタ**」に移動します。

2 「**CFS のユーザ定義種別**」までスクロールします。

3 「**エクスポート**」を選択します。「**cfsCustomCategoryData.wri を開く**」ダイアログが表示されます。

4 ファイルを開く (既定のプログラムはメモ帳)、または保存することができます。次のようにします。

- ファイルを開きます。
- ファイルを保存した場合、ファイルは Downloads フォルダに cfsCustomCaegoryData.wri というファイル名でダウンロードされます。このファイルでは、各エントリの最後に改行文字が追加されます。

ⓘ **メモ**：ファイルには、「**CFS のユーザ定義種別**」テーブルの全登録項目が 1 行で記録されます。

5 「**OK**」を選択します。

CFS ユーザ定義種別テーブルのインポート

CFS ユーザ定義種別テーブルの登録項目が含まれるファイルをインポートすることができます。ファイル内の項目によって、テーブルの既存の項目が上書きされます。

ファイルには、次の形式で情報が登録されている必要があります。

DomainName/IPAddress: Rating1[, Rating2[, Rating3[, Rating4]]] Separator

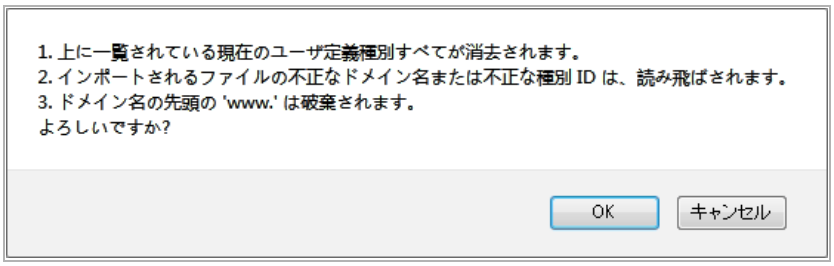
トークン	定義
DomainName	ドメイン名 (SonicWall など)。`www.` プレフィックスを含めて入力した場合、この部分は無視されます。
IPAddress	標準または IPv6 の IP アドレス。次の形式を使用できます。 • `192.168.168.168` • `fe80::c2ea:e4ff:fe59:a634`
格付け	「**CFS ユーザ定義種別の追加**」ダイアログに表示される 1 ～ 64 の種別格付け。種別ごとに最大 4 つの格付けを指定できます。
区切り文字	次の復帰または改行の文字を区切り文字に使用できます。 **区切り文字** / **スタイル** `\r\n` / Windows スタイルの改行文字 `\n` / UNIX スタイルの改行文字 `\r` / Mac OS スタイルの改行文字

ユーザ定義種別テーブルをインポートするには:

1 「**管理 | セキュリティ設定 > セキュリティ サービス > コンテンツ フィルタ.**」に移動します。

2 「**CFS のユーザ定義種別**」までスクロールします。

3 「**インポート**」を選択します。確認ダイアログが表示されます。



現在、CFS ユーザ定義種別テーブルにあるすべての項目が、ファイル内の項目で置き換えられます。残す必要がある項目は、ファイルに含まれている必要があります。

ⓘ **ヒント：** CFS ユーザ定義種別テーブルをエクスポートし、そのファイルの内容を変更してから、テーブルの項目をインポートします。

4 「**OK**」を選択します。

CFS ユーザ定義種別の編集

CFS ユーザ定義種別を編集するには:

1 編集する CFS ユーザ定義種別の「**編集**」アイコンをクリックします。「**CFS のユーザ定義種別**」ダイアログが表示されます。このダイアログは、「**CFS ユーザ定義種別の追加**」ダイアログと同じです。

2 変更を行うには、CFS ユーザ定義種別の設定 (135 ページ) の説明に従ってください。

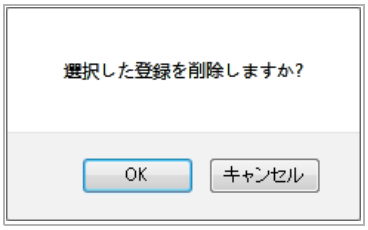
CFS ユーザ定義種別の削除

CFS ユーザ定義種別を削除するには:

1 次のいずれかを行います。

- 削除する CFS ユーザ定義種別の「**削除**」アイコンをクリックします。
- 削除する 1 つ以上の CFS ユーザ定義種別のチェックボックスをオンにします。「**削除**」ボタンが使用可能になります。ボタンをクリックします。

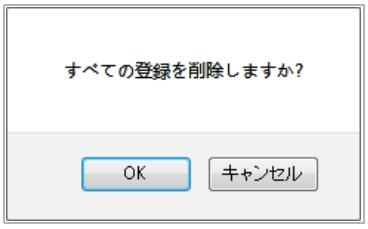
確認メッセージが表示されます。



2 「**OK**」を選択します。

すべての CFS ユーザ定義種別を削除するには:

1 「**すべて削除**」ボタンを選択します。



2 「**OK**」を選択します。すべての CFS ユーザ定義種別が削除されます。

セキュリティ サービス > コンテンツ フィルタ: Websense Enterprise

トピック:

- Websense Enterprise コンテンツ フィルタ種別の選択 (141 ページ)
- Websense サーバ状況の表示 (141 ページ)
- 一般設定の構成 (141 ページ)
- 遮断するウェブ機能の設定 (143 ページ)
- CFS 除外の設定 (143 ページ)
- 使用ポリシー遮断ページの作成 (144 ページ)

Websense Enterprise コンテンツ フィルタ種別の選択

コンテンツ フィルタ種別として Websense Filter を選択するには:

1 「**管理 | セキュリティ設定 > セキュリティ サービス > コンテンツ フィルタ**」に移動します。

2 「**コンテンツ フィルタ種別**」までスクロールします。

3 「**Websense Enterprise**」を選択します。オプションが次のように変化します。

4 Websense オプションを設定します。

5 「**適用**」を選択します。

ヒント： 「**適用**」を選択するまで、Websense サーバ状況は、コンテンツ フィルタ種別が Websense Enterprise ではないことを示します。

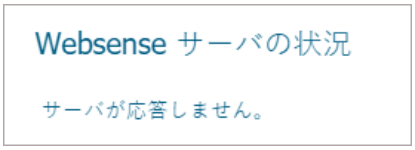
Websense サーバ状況の表示

Websense サーバ状況を表示するには:

1 「**管理 | セキュリティ設定 > セキュリティ サービス > コンテンツ フィルタ**」に移動します。

2 「**コンテンツ フィルタ種別**」に対して、**Websense Enterprise** が選択されていることを確認します。

3 「**コンテンツ フィルタ種別**」までスクロールします。



一般設定の構成

Websense Enterprise の一般設定を行うには:

1 「**管理 | セキュリティ設定 > セキュリティ サービス > コンテンツ フィルタ**」に移動します。

2 「**コンテンツ フィルタ種別**」に対して、**Websense Enterprise** が選択されていることを確認します。

3 「**一般設定**」までスクロールします。

4 「**Websense サーバ**」フィールドに、Websense サーバの IP アドレスを入力します。

5 「**ポート**」フィールドに、Websense サーバのポート番号を入力します。既定値は **15868** です。

6 「**ユーザ名**」フィールドに、Websense サーバのユーザ名を入力します。

7 「**最大 URL キャッシュ**」フィールドに、URL キャッシュの最大数を入力します。最小値は 5120、最大値は 51200、既定値は **5120** です。

8 HTTPS コンテンツ フィルタを有効にする場合は、「**HTTPS コンテンツ フィルタを有効にする**」を選択します。 このオプションは、既定では選択されています。

9 Websense プローブを監視するには、「**Websense 論理監視を有効にする**」を選択します。以下のオプションが利用可能になります。このオプションは、既定では選択されていません。

   a プローブの頻度を指定するには、「**サーバを確認する間隔**」フィールドにプローブ間隔を秒単位で入力します。最小値は 5 秒、最大値は 100 秒、既定値は **10** 秒です。

   b アクティブでない状態が一定期間経過した後に Websense を非アクティブ化するには、プローブの失敗回数を「**Websenseを停止するまでの未応答プローブ数**」フィールドに入力します。最小は 1 回、最大は 255 回で、既定は **3** 回です。

   c アクティブでない状態が一定期間経過した後に Websense を再びアクティブ化するには、プローブの成功回数を「**Websenseを再開するまでの成功プローブ数**」フィールドに入力します。最小値は 1、最大値は 255、既定値は **2** です。

10 サーバが利用できない場合にウェブ アクセスを遮断するには、「**サーバが利用不可の場合は遮断する**」を選択します。以下のオプションが利用可能になります。このオプションは、既定では選択されていません。

   a サーバ利用不可の状態がどれだけ続いたらアクセスを遮断するかを指定するには、「**サーバ タイムアウト**」フィールドにその時間を入力します。最小値は 1 秒、最大値は 10 秒、既定値は **5** 秒です。

11 「**適用**」を選択します。

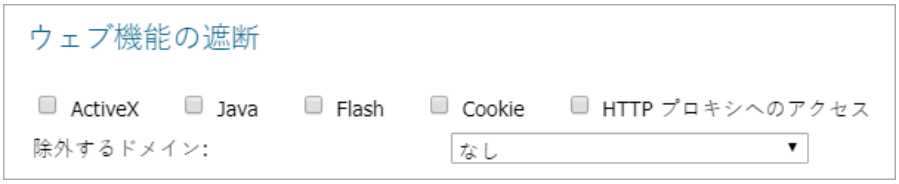
遮断するウェブ機能の設定

遮断するウェブ機能を指定するには:

1 「**管理 | セキュリティ設定 > セキュリティ サービス > コンテンツ フィルタ**」に移動します。

2 「**コンテンツ フィルタ種別**」に対して、**Websense Enterprise** が選択されていることを確認します。

3 「**ウェブ機能の遮断**」までスクロールします。



4 遮断する 1 つ以上の機能を選択します (既定ではどれも選択されていない):

- **ActiveX**
- **Java**
- **Flash**
- **Cookie**
- **HTTP プロキシへのアクセス**

5 「**除外するドメイン**」から、遮断対象から除外するドメインを指定します。既定は「**なし**」です。

6 「**適用**」を選択します。

CFS 除外の設定

CFS 除外を設定するには:

1 「**管理 | セキュリティ設定 > セキュリティ サービス > コンテンツ フィルタ**」に移動します。

2 「**コンテンツ フィルタ種別**」に対して、**Websense Enterprise** が選択されていることを確認します。

3 「**CFS 除外**」までスクロールします。

4 管理者を CFS から除外するには、「**管理者を除外する**」を選択します。 このオプションは、既定では選択されています。

5 「**除外アドレス**」から、除外するアドレスオブジェクト/グループを選択します。既定は「**なし**」です。

6 「**適用**」を選択します。

使用ポリシー遮断ページの作成

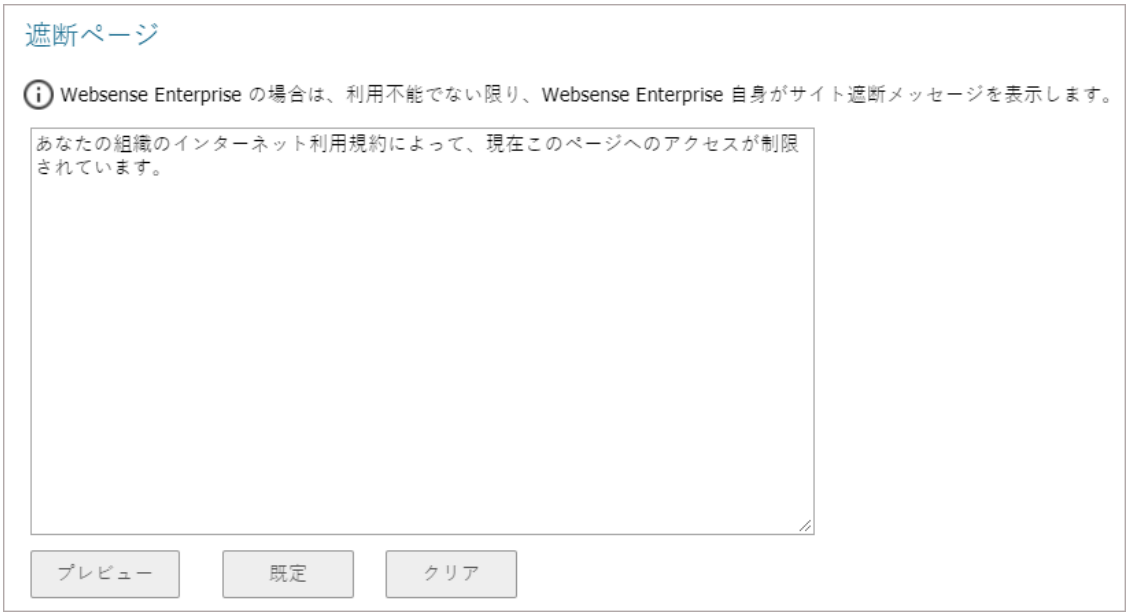
Websense Enterprise は、ウェブ ページが遮断されると既定のメッセージを表示します。会社の使用ポリシーを説明するユーザ定義メッセージを作成できます。

ユーザ定義遮断メッセージを作成するには:

1 「**管理 | セキュリティ設定 > セキュリティ サービス > コンテンツ フィルタ**」に移動します。

2 「**コンテンツ フィルタ種別**」に対して、**Websense Enterprise** が選択されていることを確認します。

3 「**遮断ページ**」までスクロールします。

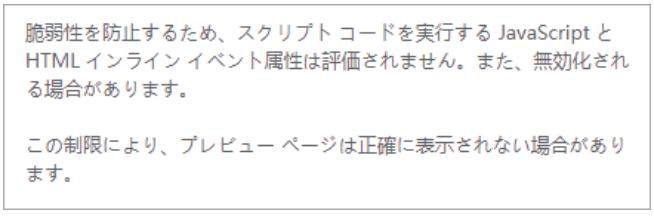


既定のメッセージが表示されます。

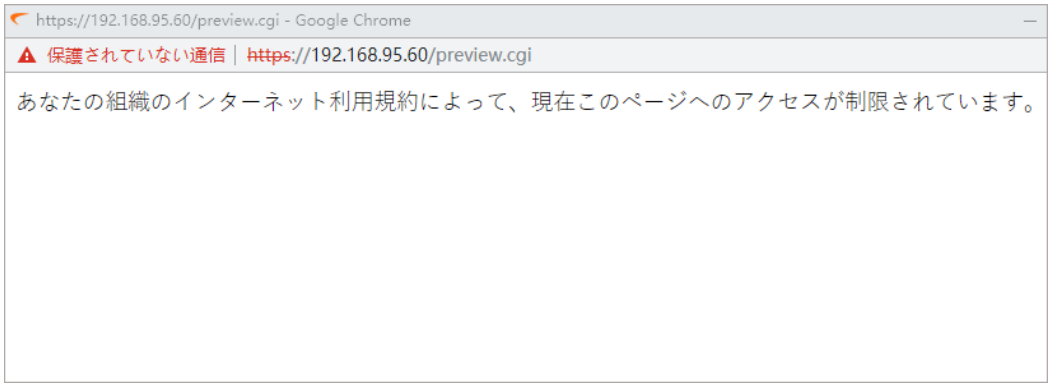
4 既定のメッセージをユーザ定義メッセージに置き換えます。

5 メッセージがユーザからどのように見えるか確認するには、「**プレビュー**」を選択します。

確認メッセージが表示されます。



a 「**OK**」を選択します。ポップアップ ダイアログが表示されます。



b ポップアップ ページを閉じます。

6 これを行うには、次の手順に従います。

- 「**遮断ページ**」フィールドの内容を消去します (「**クリア**」を選択する)。
- 既定のメッセージを復元します (「**既定**」を選択する)。

7 「**適用**」を選択します。

10

DPI-SSL 強制

ヒント： DPI-SSL の詳細については、DPI-SSL について (248 ページ) を参照してください。

- DPI-SSL 強制について (146 ページ)
- DPI-SSL 強制の管理 (147 ページ)

DPI-SSL 強制について

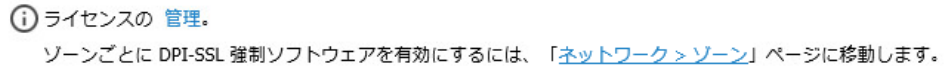
SonicWall ネットワーク セキュリティ装置で DPI-SSL サービスを有効にすると、ファイアウォールの背後にあるクライアントに関連する証明書がなければ、多くの場合、HTTPS ウェブ ページ経由での確認が必要になります。それ以外の場合、この手順を省略したければ、対応する DPI-SSL 証明書を手動でインストールする必要があります。対応する証明書をダウンロードし、インストールします。

この手順を簡略化し、クライアントが証明書を自動的にダウンロードしてインストールできるようにするために DPI-SSL 強制が必要となります。

トピック:

- リンク (147 ページ)
- DPI-SSL 強制状況 (147 ページ)
- DPI-SSL 強制 (147 ページ)

リンク



「**セキュリティ サービス > DPI-SSL 強制**」ページの上部に、以下のリンクが表示されます。

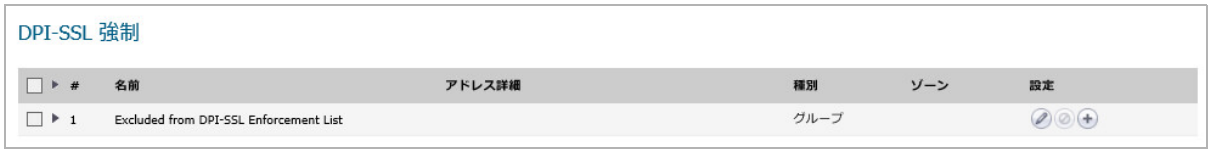
- ライセンスの表示と管理。
- ゾーンごとに DPI-SSL 強制サービスを設定できる「**管理 | システム セットアップ > ネットワーク > ゾーン**」ページを表示します。

DPI-SSL 強制状況

「**DPI-SSL 強制状況**」セクションには、DPI-SSL 強制状況機能のライセンス取得状況が示されます。

DPI-SSL 強制

「**DPI-SSL 強制**」セクションには、DPI-SSL 強制の対象に含まれるアドレスと除外されるアドレスのリストがあります。



DPI-SSL 強制の管理

「**管理 | セキュリティ設定 > セキュリティ サービス > DPI-SSL 強制**」ページで、次の項目を追加、編集、削除できます。

- DPI-SSL 強制リスト
- DPI-SSL 強制リストから除外

トピック:

- DPI-SSL 強制リストの編集 (148 ページ)
- DPI-SSL 強制リストへのポリシーの追加 (148 ページ)
- DPI-SSL 強制ポリシーの編集 (148 ページ)
- DPI-SSL 強制のためのゾーンの管理 (149 ページ)

DPI-SSL 強制リストの編集

DPI-SSL 強制リストを編集するには:

1 「**管理 | セキュリティ設定 > セキュリティ サービス > DPI-SSL 強制**」ページに移動します。

2 「**DPI-SSL 強制**」セクションまでスクロールします。

3 編集したいリストの横にある「**編集**」アイコンを選択します。「**アドレス オブジェクト グループの編集**」ダイアログが表示されます。

4 追加するアドレス オブジェクトを左の列から選択します。複数のアドレス オブジェクトを一度に選択できます。

5 **右矢印**ボタンを選択します。

グループからアドレス オブジェクトを削除するには、アドレス オブジェクトを選択し、**左矢印**ボタンを選択します。

6 「**OK**」を選択します。

DPI-SSL 強制リストへのポリシーの追加

DPI-SSL 強制リストに新しいポリシーを追加するには:

1 「**管理 | セキュリティ設定 > セキュリティ サービス > DPI-SSL 強制**」ページに移動します。

2 「**DPI-SSL 強制**」セクションまでスクロールします。

3 ポリシーを追加したいリストの横にある「**追加**」アイコンを選択します。「**アドレス オブジェクトの追加**」ダイアログが表示されます。

4 「**名前**」フィールドにサーバのニックネームを入力します。

5 「**ゾーンの割り当て**」から、サーバのゾーンを選択します。

6 「**種別**」から、ホストの種別を選択します。選択したホスト種別に応じて、以下の設定が変更されます。

7 選択した内容によって次の手順が異なります。

- **ホスト** (既定) - 「**IP アドレス**」フィールドに IP アドレスを入力します。
- **範囲** - 「**開始アドレス**」フィールドと「**終了アドレス**」フィールドに開始アドレスと終了アドレスを入力します。

8 「**OK**」を選択します。

DPI-SSL 強制ポリシーの編集

DPI-SSL 強制ポリシーを編集するには:

1 「**管理 | セキュリティ設定 > セキュリティ サービス > DPI-SSL 強制**」ページに移動します。

2 「**DPI-SSL 強制**」セクションまでスクロールします。

3 編集したいポリシーの横にある「**編集**」アイコンを選択します。「**アドレス オブジェクトの編集**」ダイアログが表示されます。

4 変更したい値を更新します。

5 「**OK**」を選択します。

DPI-SSL 強制のためのゾーンの管理

「**管理 | システム セットアップ > ネットワーク > ゾーン**」ページを使用して、特定のゾーンの DPI-SSL 強制を管理します。ゾーンに関する詳細は、*SonicWall SonicOS 6.5 システム セットアップ*を参照してください。

11

SonicWall クライアント アンチウイルスの有効化

- セキュリティ サービス > クライアント AV 強制
- クライアント アンチウイルス サービスの設定

セキュリティ サービス > クライアント AV 強制

アンチウイルス製品は、その性質上、すべての PC において定期的で積極的なメンテナンスが欠かせません。新しいウイルスが検出された場合は、組織内に配備されているすべてのアンチウイルス ソフトウェアを最新のウイルス定義ファイルで更新する必要があります。その更新を行わないと、アンチウイルス ソフトウェアの有効性が大幅に制限され、生産的な作業時間が遮断されます。知られているウイルスだけでも 50,000 種以上存在し、新しいウイルスが日々発見されていることを考えると、ウイルス対策を更新する作業そのものが大きな負担となる場合があります。残念ながら、中小企業の多くは、アンチウイルス ソフトウェアをメンテナンスできるだけの十分な IT スタッフを抱えていません。結果、ウイルス対策に隙が生まれ、データを喪失したり、社員の生産性低下につながることになります。

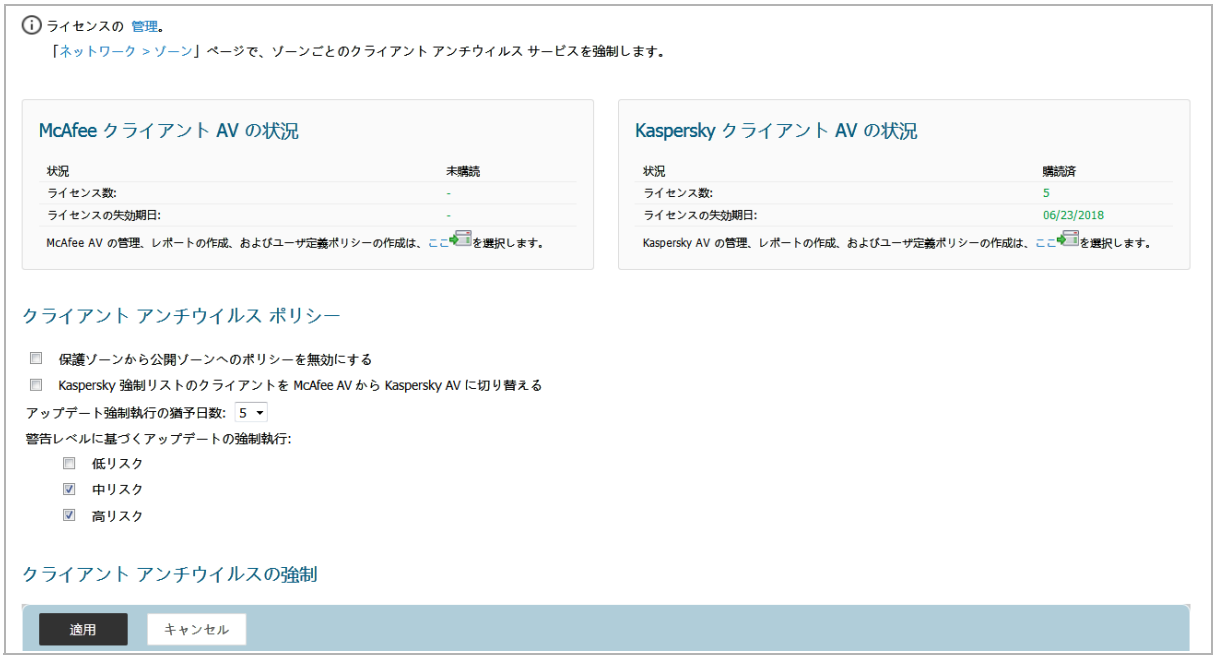
中小企業におけるウイルス対策の不備は、NIMDA や Code Red などのウイルスの蔓延を見れば明らかです。最新のウイルス定義ファイルのないユーザは、ウイルスを増殖させ他の多くのユーザおよびネットワークに悪影響を及ぼすことになります。SonicWall クライアント アンチウイルスは、このような事態を未然に防ぎ、ウイルス対策に新しいアプローチを提供するものです。SonicOS は、絶えずウイルス定義ファイルのバージョンを監視し、各ユーザのコンピュータに対し、新しいウイルス定義ファイルのダウンロードとインストールを自動的に開始します。さらに、すべてのユーザのインターネット アクセスは、それらが保護の対象となっている限り、ファイアウォールによって制限されるため、企業のウイルス対策ポリシーを確実に達成することができます。この新しいアプローチにより、ウイルス定義ファイルの最新バージョンがインストールされ、ネットワーク上の各PC で有効となり、不正アクセスしたユーザによってウイルス対策が無効になり、組織全体が感染することがないようにできます。

メモ：ファイアウォールの管理インターフェースを通じてアンチウイルスを執行するにはアンチウイルスを購読する必要があります。

SonicOS は、クライアント AV 強制のために McAfee と Kaspersky の両方のクライアント アンチウイルスをサポートしています。これらのサービスはそれぞれ個別にライセンスされるので、配備状況に応じて必要な数のライセンスを購入することができます。

クライアント アンチウイルス サービスの設定

ネットワーク アンチウイルス サービスの有効化については、ゲートウェイ アンチウイルス、アンチスパイウェア、および IPS サービスのライセンスの有効化を参照してください。



トピック:

- クライアント AV の状況 (151 ページ)
- クライアント アンチウイルス ポリシー (152 ページ)
- クライアント アンチウイルス強制 (153 ページ)

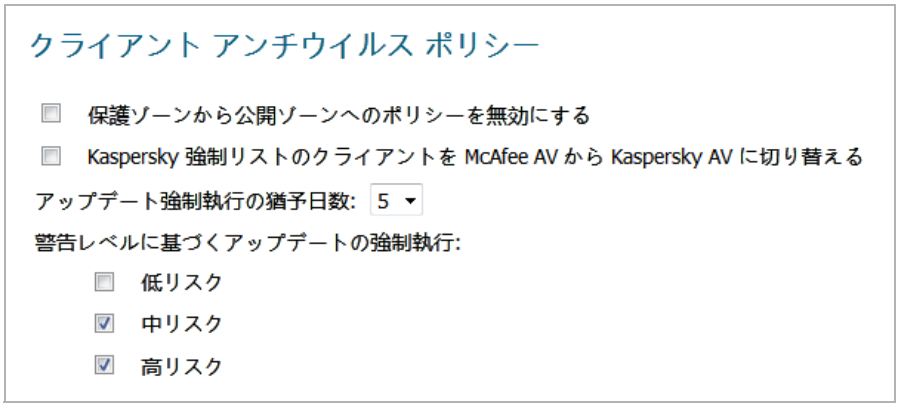
クライアント AV の状況

「**クライアント AV の状況**」セクション:

- ファイアウォールがライセンスされているかどうか、ライセンス数、およびライセンスが失効する期日を表示します。
- MySonicWall にログインするためのリンクがあります。ここでシステムやネットワークに関する詳細な情報を管理したり表示したりすることができます。このリンクを選択すると、MySonicWall ログイン用の「**ライセンス > ライセンス管理**」ページが表示されます。

- 「**管理 | システム セットアップ > ネットワーク > ゾーン**」ページへのリンクがあります。ここでゾーンごとにクライアント AV を設定できます。

クライアント アンチウイルス ポリシー



「**クライアント アンチウイルス ポリシー**」セクションでは、次の機能を使用できます。

- **保護ゾーンから公開ゾーンへのポリシーを無効にする** - このオプションが選択されていない場合は、保護ゾーンに配置されたコンピュータに対してアンチウイルス ポリシーが執行されます。このオプションを選択すると、保護ゾーン (例えば LAN) 上のコンピュータから公開ゾーン (例えば DMZ) 上のコンピュータへのアクセスが可能になります。 このアクセスは、LAN のコンピュータにアンチウイルス ソフトウェアがインストールされていない場合でも可能になります。
- **Kaspersky 強制リストのクライアントを McAfee AV から Kaspersky AV に切り替える** - 選択すると、Kaspersky 強制リストのクライアントのために McAfee AV ではなく Kaspersky AV が使用されます。
- **アップデート強制執行の猶予日数** - ここで、インターネットにアクセスする最大日数を定義しておくと、その日数が経過したときに、最新のウイルス更新ファイルが強制的にダウンロードされます。0 ～ 5 日を選択します。既定は **5** です。
- **警告レベルに基づくアップデートの強制執行** - SonicWall は、アンチウイルスを購読しているすべての SonicWall 装置に対して、ウイルス警告をブロードキャストします。利用可能な警告レベルは 3 つあり、そのうちの 2 つ以上を選択することができます。このオプションが選択されている状態で警告を受け取った場合、ユーザは VirusScan ASaP を最新版に更新してからでないと、インターネットにアクセスできません。このオプションは、「アップデート強制執行前の最大猶予日数」の選択よりも優先されます。また、すべてのウイルス警告がログ採取されるとともに、警告メッセージが管理者に送信されます。
    - **低リスク** - フィールドで報告されていないウイルスが、今後もフィールドで発見される可能性が低いと見なされた場合、危険度は “低" です。そのようなウイルスは、含まれているペイロードの破損が非常に深刻または予測不能な場合でも、その危険度“低"であることに変わりありません。このオプションは、既定では選択されていません。
    - **中リスク** - フィールドでウイルスが発見された場合、そのウイルスに使用されている感染メカニズムがあまり一般的でなければ、危険度は “中" です。ウイルスの感染率が低くとどっていて、そのペイロードが深刻でなければ、危険度を“低"に下げることもできます。同様に、ウイルスの感染率が上昇すれば、危険度を“高"に上げることができます。このオプションは、既定では選択されています。
    - **高リスク** - 危険度に "高" を割り当てるには、フィールドでウイルスが頻繁に報告されていて、しかもそのペイロードが少なくともやや深刻な破損の原因になりうるものでなければなりません。そのウイルスが非常に深刻または予測不能な破損を引き起こす場合は、

感染率が低くても、危険度に“高"を割り当てることが可能です。このオプションは、既定では選択されています。

クライアント アンチウイルス強制

「**クライアント アンチウイルスの強制**」テーブルには次の 2 つのエントリがあります。どちらのエントリも特定の**種別**の**グループ**が関連付けられています。

- ***サードパティ* クライアント AV 強制リスト** (ここで、***サードパーティ***は、どちらを使用しているかによって **McAfee** または **Kaspersky**)
- **クライアント AV 強制除外リスト**

各エントリに関連付けられている IP アドレスを表示するには、**展開** アイコンを選択します。各エントリの「**アドレス詳細**」、「**種別**」、および「**ゾーン**」が表示されます。強制リストをまだ設定していない場合、**展開**アイコンを選択すると、"**登録がありません**" と表示されます。

IP アドレスを非表示にするには、**折りたたみ**アイコンを選択します。

これらの 2 つのエントリは、編集または追加は可能ですが、削除することはできません。

トピック:

- クライアント AV 強制リストの作成
- クライアント AV 強制リストからアドレス オブジェクトを除外する
- どちらのリストにも含まれていないコンピュータを保護する

クライアント AV 強制リストの作成

メモ：事前定義されているアドレス オブジェクト (インターフェース IP、デフォルト ゲートウェイなど) は、個別に編集したり削除したりすることはできません。その**編集**および**削除**アイコンは淡色表示になっています。事前定義されているアドレス オブジェクトを「**クライアント AV 強制リスト**」から削除するには、リストそのものを編集します。ただし、自分で定義したアドレス オブジェクトは自由に編集または削除できます。

クライアント AV 強制リストには、クライアント AV に強制させるアドレス オブジェクトの IP アドレスを設定する必要があります。

アンチウイルスの強制を受け取る IP アドレスの範囲を定義するには、IP アドレスの範囲を含むアドレス オブジェクトを作成します。強制の対象とするコンピュータは、指定した IP アドレスの範囲に

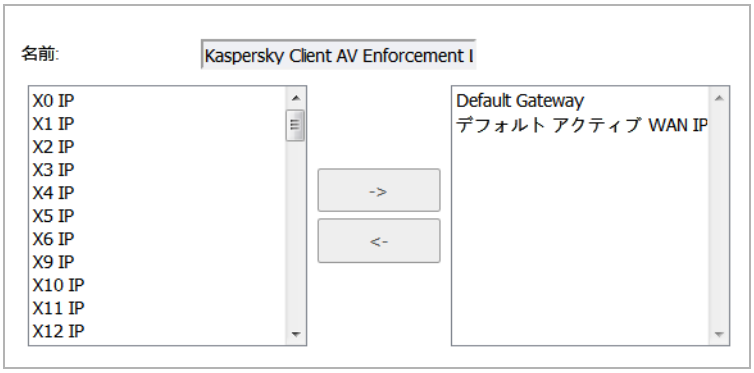
静的 IP アドレスを持たなければなりません。最大 64 個の IP アドレス範囲を強制の対象として入力できます。

クライアント AV 強制リストを既存のアドレス オブジェクトに基づいて作成するには、以下の手順に従います。

1 「**管理 | セキュリティ設定 > セキュリティ サービス > クライアント AV 強制**」ページに移動します。

2 「**クライアント アンチウイルスの強制**」セクションまでスクロールします。

3 「***サードパーティ クライアント AV 強制リスト***」の**編集**アイコンを選択します。「**アドレス オブジェクト グループの編集**」ダイアログが表示されます。



4 左側のリストから、クライアント AV 強制を行う IP アドレスを選択します。

5 **右矢印**ボタンを選択してエントリを右側のリストに移動します。

6 アドレス オブジェクトの追加が完了したら、「**OK**」を選択します。

アドレス オブジェクトをクライアント AV 強制リストに追加するには、以下の手順に従います。

1 「**管理 | セキュリティ設定 > セキュリティ サービス > クライアント AV 強制**」ページに移動します。

2 「**クライアント アンチウイルスの強制**」セクションまでスクロールします。

3 「***サードパーティ クライアント AV 強制リスト***」の**追加**アイコンを選択します。「**アドレス オブジェクトの追加**」ダイアログが表示されます。

4 「**名前**」フィールドに、わかりやすい名前を入力します。

5 「**ゾーンの割り当て**」ドロップダウン メニューからゾーンを選択します。

6 「**種別**」ドロップダウン メニューから、種別を選択します。

7 「**IP アドレス**」フィールドに、アドレス オブジェクトの IP アドレスを入力します。

8 「**OK**」を選択します。

クライアント AV 強制リストからアドレス オブジェクトを除外する

SonicWall クライアント アンチウイルスは、現在、Windows プラットフォームをサポートしています。インターネットにアクセスするには、他のオペレーティング システムを搭載したコンピュータをアンチウイルス ポリシーの適用対象から除外する必要があります。

注意：ウイルス攻撃からネットワークを完全に保護するためには、サーバおよびサポート対象外のマシンのみを保護対象から除外することと、そのマシンをアンチウイルス強制の対象から除外する前に各マシン上にサードパーティ製のアンチウイルス ソフトウェアをインストールすることをお勧めします。

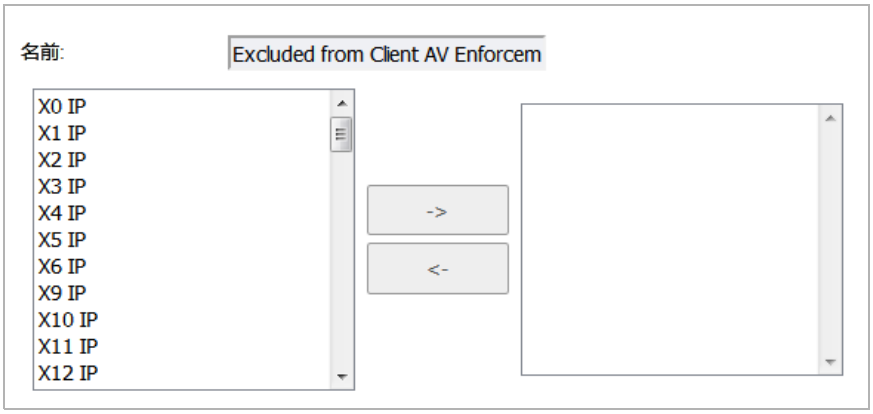
メモ：事前定義されているアドレス オブジェクト (インターフェース IP、デフォルト ゲートウェイなど) は、個別に編集したり削除したりすることはできません。その**編集**および**削除**アイコンは淡色表示になっています。事前定義されているアドレス オブジェクトを「**クライアント AV 強制除外リスト**」から削除するには、リストそのものを編集します。ただし、自分で定義したアドレス オブジェクトは自由に編集または削除できます。

除外アドレス オブジェクトを定義するには、以下の手順に従います。

1 「**管理 | セキュリティ設定 > セキュリティ サービス > クライアント AV 強制**」ページに移動します。

2 「**クライアント アンチウイルスの強制**」セクションまでスクロールします。

3 「**クライアント AV 強制除外リスト**」の**編集**アイコンを選択します。「**アドレス オブジェクト グループの編集**」が表示されます。



4 左側のリストから、除外対象のアドレス オブジェクトを選択します。

5 **右矢印**ボタンを選択してオブジェクトを右側のリストに移動します。

6 アドレス オブジェクトの除外が完了したら、「**OK**」を選択します。

アドレス オブジェクトを「クライアント AV 強制除外リスト」に追加するには、以下の手順に従います。

1 「**管理 | セキュリティ設定 > セキュリティ サービス > クライアント AV 強制**」ページに移動します。

2 「**クライアント アンチウイルスの強制**」セクションまでスクロールします。

3 「**クライアント AV 強制除外リスト**」の**追加**アイコンを選択します。「**アドレス オブジェクトの追加**」ダイアログが表示されます。

4 「**名前**」フィールドに、わかりやすい名前を入力します。

5 「**ゾーンの割り当て**」ドロップダウン メニューからゾーンを選択します。

6 「**種別**」ドロップダウン メニューから、種別を選択します。

7 「**IP アドレス**」フィールドに、アドレス オブジェクトの IP アドレスを入力します。

8 「**OK**」を選択します。

アドレス オブジェクトを「クライアント AV 強制除外リスト」に追加するには、以下の手順に従います。

1 「**クライアント アンチウイルスの強制**」セクションまでスクロールします。

2 「**クライアント AV 強制除外リスト**」の**追加**アイコンを選択します。「**アドレス オブジェクトの追加**」ダイアログが表示されます。

3 「**名前**」フィールドに、わかりやすい名前を入力します。

4 「**ゾーンの割り当て**」ドロップダウン メニューからゾーンを選択します。

5 「**種別**」ドロップダウン メニューから、種別を選択します。

6 「**IP アドレス**」フィールドに、アドレス オブジェクトの IP アドレスを入力します。

7 「**OK**」を選択します。

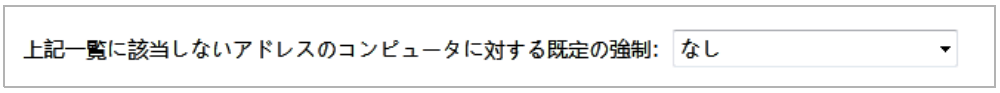
どちらのリストにも含まれていないコンピュータを保護する

どちらの強制リストにも含まれていないコンピュータに対して、適用する既定の強制の種別を指定できます。

強制リストに含まれていないコンピュータに既定の強制を指定するには、以下の手順に従います。

1 「**クライアント アンチウイルスの強制**」セクションまでスクロールします。

2 「**セキュリティ サービス > クライアント AV 強制**」ページの下部までスクロールします。



3 「**上記一覧に該当しないアドレスのコンピュータに対する既定の強制**」ドロップダウン メニューから既定の強制の種別を選択します。

- **なし** (既定)
- サードパーティ アンチウイルス プログラム (システムに応じて、McAfee か Kaspersky)

12

クライアント CF 強制の設定

- セキュリティ サービス > クライアント CF 強制
- クライアント CF 強制の有効化と設定
- ネットワーク ゾーンでクライアント CFS を有効化する

セキュリティ サービス > クライアント CF 強制

SonicWall クライアント CF 強制は、企業、学校、図書館、政府機関において、保護や生産性に関するポリシーを確実に適用します。SonicWall は、拡張性に優れた動的なデータベースを活用して、不適切で非生産的なウェブ コンテンツを遮断する、革新的なコンテンツ フィルタ アーキテクチャを構築しました。

クライアント CF 強制は、制御と柔軟性を理想的な組み合わせで提供し、最高水準の保護と生産性を確保します。クライアント CF 強制は、個々のユーザによる不適切なコンテンツへのアクセスを防止するとともに、組織の責任を軽減し、生産性を高めます。ウェブ サイトは、その中に含まれるコンテンツの種類に基づいて評価されます。コンテンツ フィルタ サービス (CFS) は、ウェブ サイトの評価と、そのユーザまたはグループに対するポリシー設定に基づいて、サイトへのアクセスを遮断または許可します。

企業は通常、装置上にフィルタ ポリシーを設定することによって、セキュリティ装置の境界内で閲覧が開始された場合のウェブ閲覧動作やコンテンツを制御することができます。ただし、その機器が境界の外に出ると、制御は失われます。クライアント CF 強制は、セキュリティ装置の境界外でも不適切で非生産的なウェブ コンテンツを遮断することにより、このギャップを埋めることを目的とします。

SonicWall セキュリティ装置をクライアント CF 強制と併用することで、すべてのエンドポイントに、ネットワークを最大限に保護するための最新ソフトウェア アップデートを自動的に、かつ一貫して確実に適用することができます。クライアントは、Windows と Mac PC の両方で動作するように設計されています。

クライアント CF 強制は、以下の 3 つの主要コンポーネントで構成されています。

- SonicOS が稼動するネットワーク セキュリティ装置。CFS のライセンスが簡単に適用および確認できます。また、強制の有効化/無効化や除外などの設定を行うことができます。
- クライアント CF 強制のインストールの自動開始。インターネット アクセスを試みる任意のクライアントに対し、クライアント ソフトウェアがインストールされていない場合は、インストールされるまでウェブ サイトのアクセスを遮断します。
- クライアント ポリシーとクライアント グループの管理。MySonicWall または装置上で稼動する SonicOS からアクセスされる、クラウド ベースの EPRS サーバを使用します。

トピック:

- クライアント CF 強制の有効化と設定
- ネットワーク ゾーンでクライアント CFS を有効化する

クライアント CF 強制の有効化と設定

このセクションでは、SonicOS におけるクライアント CF 強制の有効化と設定方法について説明します。

クライアント CF 強制のインストールを求める、ウェブ サイト遮断ページをユーザに表示する前に、クライアント CF 強制を SonicWall 装置上で有効化しておく必要があります。

メモ：MySonicWall でコンテンツ フィルタ クライアント (CFS) が有効になっていない場合は、それを有効にしてクライアント システムでクライアント コンテンツ フィルタ ポリシーを強制する必要があります。

セキュリティ サービスにおけるクライアント CF 強制の設定

クライアント CF 強制 用の設定を行うには、以下の手順に従います。

1 「**管理 | セキュリティ設定 > クライアント CF 強制**」ページに移動します。

2 「**クライアント CF 強制ポリシー**」セクションで、CFS 強制ポリシーを有効とする「**非活動化の猶予期間**」の日数をドロップダウン リストから選択します。

「**クライアント CF 強制リスト**」セクションには、クライアント CF 強制リストと、クライアント CF 強制除外リストを含むテーブルがあります。

いずれかのリストを設定するには、そのリストの**設定**アイコンを選択します。「アドレス オブジェクト グループの編集」ダイアログが表示されます。表示されたリストから、グループに含める値または含めない値を選択します。

3 **クライアント CF 強制リスト**と、**クライアント CF 強制除外リスト**に対し、リストにエントリを作成済みである場合は、リスト タイトルの横にある矢印をクリックすることによって、エントリを表示できます。いずれかのリストにエントリを追加するには、その行の設定アイコンを選択します。

4 「**上記一覧に該当しないアドレスのコンピュータに対する既定の強制**」というラベルの付いたフィールドで、ドロップダウン リストから「**クライアント CF 強制**」を選択します。このフィールドは、「**クライアント CF 強制リスト**」セクションの下にあります。これを選択すると、装置を介してインターネットに接続する他のすべてのコンピュータにおいて、強制クライアントのインストールを促すメッセージが表示されます。設定済みのコンピュータのみにサービスを適用する場合は、ドロップダウン リストから「**なし**」を選択できます。

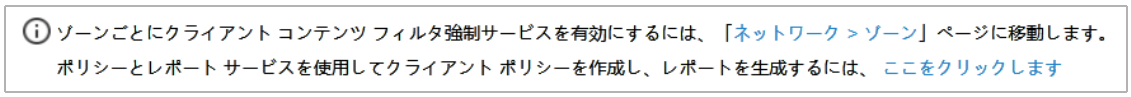
5 「**適用**」を選択します。

ネットワーク ゾーンでクライアント CFS を有効化する

クライアント コンテンツ フィルタは、ゾーンごとに強制されます。

ゾーンごとに CFS を強制するには:

1 「**セキュリティ サービス > クライアント CF 強制**」ページの上部で、「**補足**」にある「**ネットワーク > ゾーン**」リンクを選択します。



「**ネットワーク > ゾーン**」ページが表示されます。

2 クライアント コンテンツ フィルタ サービスを適用するゾーンの「**設定**」ボタンを選択します。「**ゾーンの追加**」ダイアログが表示されます。

3 「**クライアント CF サービスを有効にする**」チェックボックスをオンにします。

4 「**OK**」を選択します。

13

SonicWall ゲートウェイ アンチウイルス サービスの管理

- ゲートウェイ アンチウイルス サービスSonicWall について (162 ページ)
- SonicWall ゲートウェイ アンチウイルス保護のセットアップ (167 ページ)
- SonicWall GAV シグネチャの表示 (178 ページ)

ゲートウェイ アンチウイルス サービス SonicWall について

SonicWall ゲートウェイ アンチウイルス (GAV) サービスは、SonicWall セキュリティ装置上で直接動作しながらリアルタイムのウイルス対策を実現します。SonicWall の IPS-Deep Packet Inspection v2.0 エンジンを使用することにより、SonicWall ゲートウェイを通過するすべてのトラフィックを検査します。パケットの再組み立てが不要な SonicWall の手法をベースとしながら、一般的な TCP ストリームや圧縮トラフィックのほか、さまざまなアプリケーション プロトコルを検査できます。パケットの再組み立てを SonicWall GAV そのものが実行する必要はないため、スキャン エンジンによるファイル サイズの制限はありません。Base64 デコード、ZIP、LHZ、GZIP (LZ77) の解凍も、単一パス、パケット単位の原則で実行されます。

SonicWall ゲートウェイ アンチウイルス は、脅威からの保護を実現するために、ダウンロードしたファイルや電子メールで送られてきたファイルを、ウイルスの脅威を示すシグネチャから成る動的に更新される包括的なデータベースと照らしてチェックします。データベースには有害なウイルスのシグネチャが多岐にわたって格納され、動的に更新されるため、あらゆるウイルスをデスクトップに到達する前に検出、抑止できます。新しいシグネチャは、SonicWall の SonicAlert Team、サードパーティ ウイルス解析者、オープンソース開発者、および他のソースの組み合わせにより作成され、データベースに追加されます。

SonicWall GAV で防御できるのは、ネットワークの外部から侵入する脅威に限定されません。ネットワーク内部を起源とした脅威を抑止することもできます。SonicWall ゲートウェイ アンチウイルスは、SMTP、POP3、IMAP、HTTP、FTP、NetBIOS、インスタント メッセージングのほか、ピアツーピア アプリケーションやストリームベースの多くのプロトコルなど、多様なプロトコル上で動作し、広範囲にわたるネットワーク脅威に対する防御および制御機能を提供します。悪質なコードやウイルスを含んだファイルが圧縮されていると、従来のソリューションでは対応できない可能性があるため、SonicWall GAV には、パケット単位でファイルを自動的に解凍しスキャンする高度な解凍技術が統合されました。

SonicWall GAV は、サポート対象の電子メール プロトコルを解析して、ヘッダーのフィールド (`to`、`cc`、`bcc`) を調査します。これらのフィールドの情報が表示され、送信者と受信者の両方のキャプチャ ATP に記録されます。

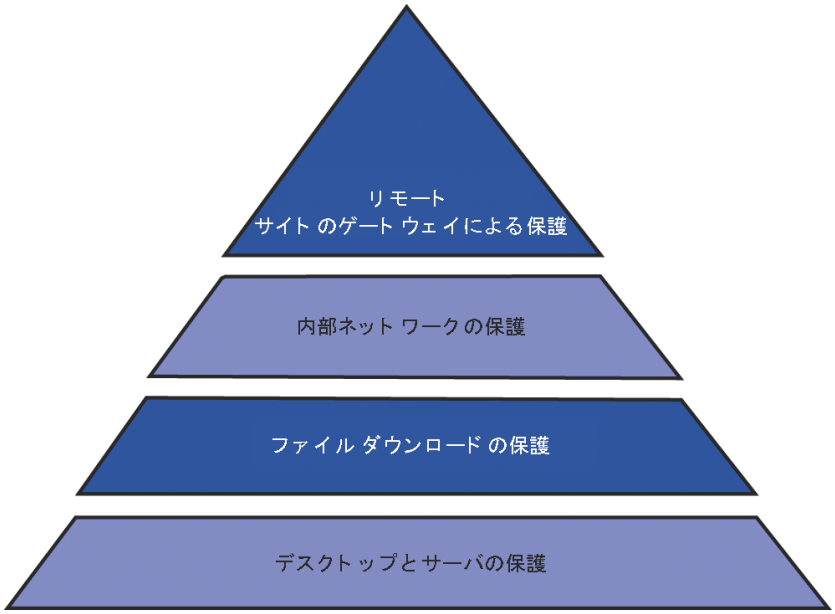
トピック:

- SonicWall GAV の多層型アプローチ
- SonicWall GAV の手法
- ゲートウェイ アンチウイルス、アンチスパイウェア、および IPS サービスのライセンスの有効化
- SonicWall ゲートウェイ アンチウイルス保護のセットアップ
- SonicWall GAV シグネチャの表示

SonicWall GAV の多層型アプローチ

SonicWall GAV では、多層型のネットワーク アンチウイルス保護が、デスクトップ、ネットワーク、リモート サイトなど、あらゆる場所に適用されます。SonicWall GAV の多層型アプローチを参照してください。アンチウイルス ポリシーをゲートウェイで執行することにより、すべてのユーザに最新のアップデートを確実に適用し、ネットワークに入ってくるファイルを監視します。

SonicWall GAV の多層型アプローチ

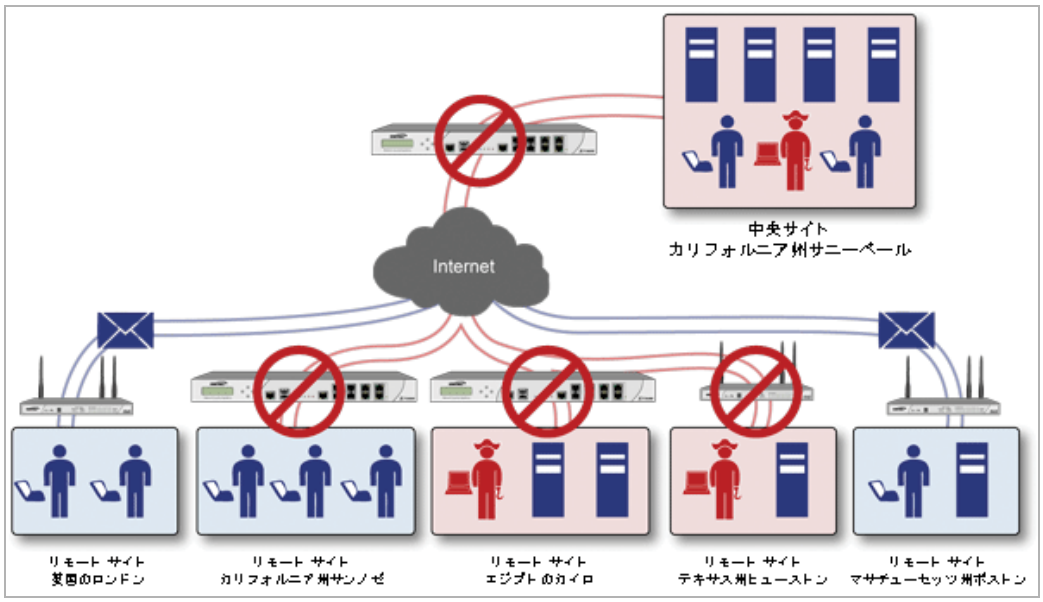


トピック:

- リモート サイトの保護
- 内部ネットワークの保護
- HTTP ファイルのダウンロード
- サーバの保護
- クラウド アンチウイルス データベース

リモート サイトの保護

リモート サイトの保護



1 本社とリモート サイト間で通常の電子メールやファイルが送信されます。

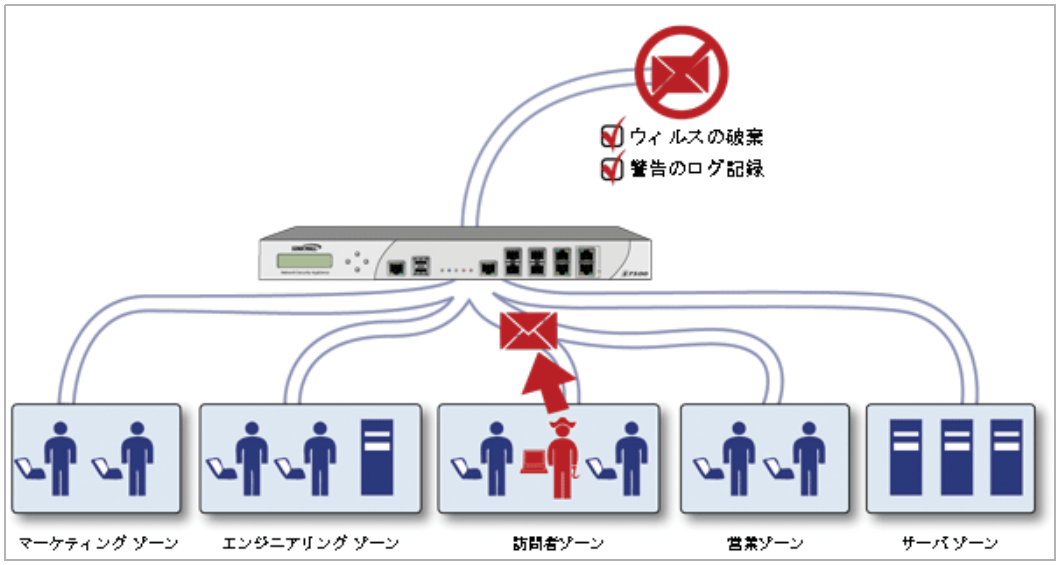
2 SonicWall GAV は、SonicWall セキュリティ装置上のファイルや電子メール メッセージをスキャンして分析します。

3 ウイルスはリモートのデスクトップに到達する前に検出されて遮断されます。

4 検出されたウイルスはログに記録され、管理者に警告が送信されます。

内部ネットワークの保護

内部ネットワークの保護



1 内部のユーザによって持ち込まれたウイルスが社内に蔓延します。

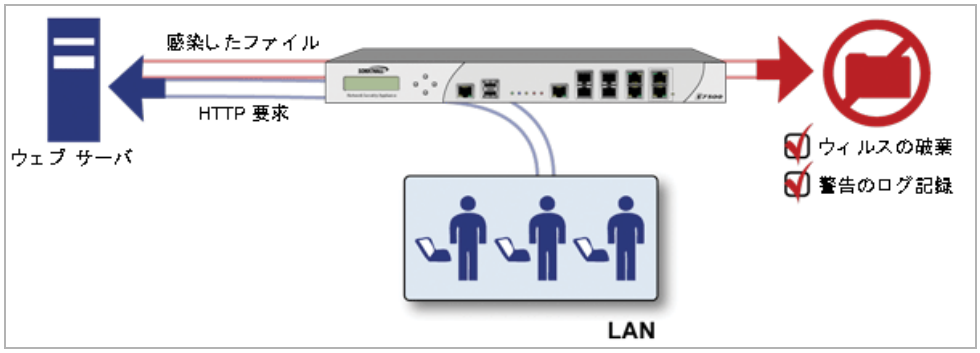
2 すべてのファイルは、他のネットワーク ユーザが受け取る前にゲートウェイでスキャンされます。

3 ウイルスが検出されたファイルは破棄されます。

4 検出されたウイルスはログに記録され、管理者に警告が送信されます。

HTTP ファイルのダウンロード

HTTP ファイルのダウンロード



1 クライアントがウェブからファイルをダウンロードしようとします。

2 ファイルがインターネットからダウンロードされます。

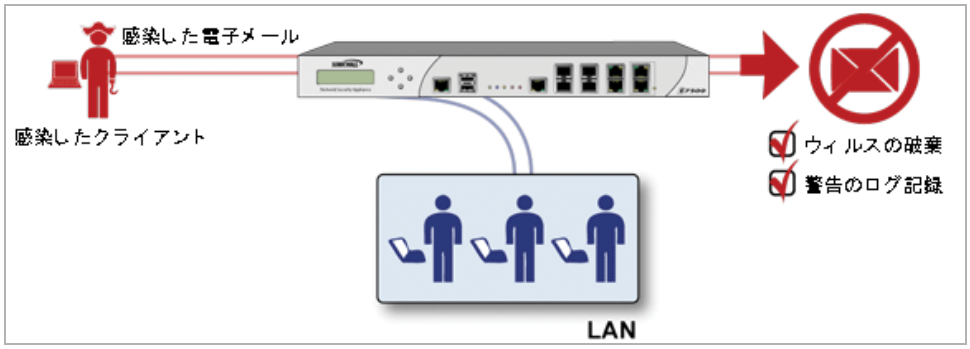
3 ファイルに悪質なコードやウイルスが潜んでいないかが、SonicWall GAV エンジンにより解析されます。

4 ウイルスが検出されたファイルは破棄されます。

5 検出されたウイルスはログに記録され、管理者に警告が送信されます。

サーバの保護

サーバの保護



1 外部のユーザから電子メールが送られてきます。

2 SonicWall GAV エンジンが、電子メールに悪質なコードやウイルスが潜んでいないかを、電子メール サーバに到達する前に解析します。

3 ウイルスが検出された場合は、その脅威を封じる措置が講じられます。

4 電子メールは送信者に送り返され、ウイルスがログに記録され、管理者に警告が送信されます。

クラウド アンチウイルス データベース

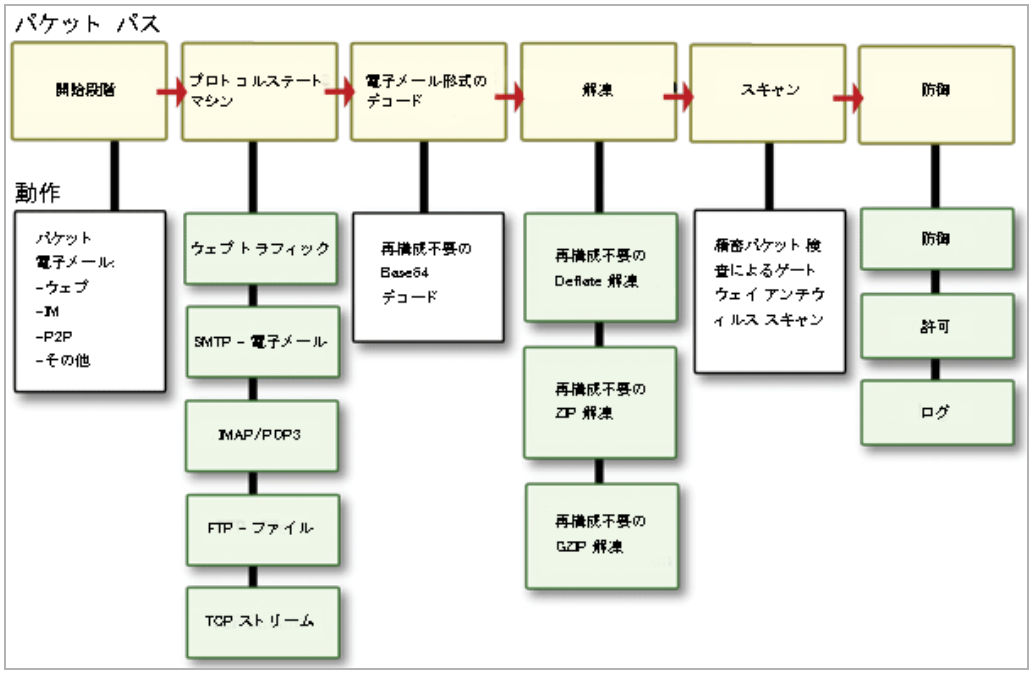
クラウド ゲートウェイ アンチウイルス機能は、危険なマルウェア検体が増え続ける現状に対抗するために、SonicWall ファイアウォールの現在のゲートウェイ アンチウイルス スキャン メカニズムを引き継ぎながら拡張する、高度なマルウェア スキャン ソリューションを提供します。

クラウド ゲートウェイ アンチウイルスは、再組み立て不要精密パケット検査 (RFDPI) エンジンの機能を拡張するために、データセンター ベースのマルウェア分析サーバに問い合わせを行います。このアプローチは、現在どんな大きな処理オーバヘッドの増加も装置自身に加えずにサポートされるすべてのプロトコルで、無制限なサイズの無制限な数のファイルをスキャン可能な、遅延の少ないのリアルタイム ソリューションを提供することによって、RFDPI ベースのマルウェア検出の基礎を保ちます。この追加レイヤのセキュリティにより、SonicWall の次世代ファイアウォールは現在の保護を拡張して数百万ものマルウェア要素をカバーすることができます。

SonicWall GAV の手法

SonicWall GAV は、SonicWall の高性能 DPIv2.0 エンジン (Deep Packet Inspection version 2.0) をベースとし、すべてのスキャンを SonicWall セキュリティ装置上で直接実行します。SonicWall GAV には、ファイルを自動的に解凍し、パケット単位でスキャンすることによって、ウイルスやマルウェアを検出する高度な解凍技術が採用されています。SonicWall GAV の手法を参照してください。SonicWall GAV エンジンは、base64 形式でエンコードされたメール ストリーム全体を再組み立てすることなく、base64 のデコードを実行できます。パケットの再組み立てを SonicWall GAV そのものが実行する必要はないため、スキャン エンジンによるファイル サイズの制限はありません。Base64 デコード、ZIP、LHZ、GZIP (LZ77) の解凍も、単一パス、パケット単位の原則で実行されます。SonicWall GAV エンジンが備える再組み立てが不要なウイルス スキャン機能は、ストリーム内のバイトを一切バッファリングすることなくストリームをスキャンすることのできる精密パケット検査エンジンから継承されたものです。

SonicWall GAV の手法



パケットの再組み立てが不要な SonicWall の手法をベースとしながら、一般的な TCP ストリームや圧縮トラフィックのほか、さまざまなアプリケーション プロトコルを検査できます。SonicWall GAV のプロトコル検査の中枢を担っているのは、個々のサポート プロトコルに特化された高性能なステート マシンです。SMTP、POP3、IMAP、HTTP、FTP、NetBIOS、インスタント メッセージング、ピア ツー ピア アプリケーションから、ストリーム ベースのプロトコルまで、今日のネットワーク環境で広く用いられているほとんどのプロトコルに対応しています。これにより、ネットワークを脅かす目的に用いられる可能性のあるバックドアを閉鎖できると同時に、従業員の生産性向上およびインターネット帯域幅の確保も可能になります。

ヒント： SonicWall セキュリティ装置がインターネットに接続されていて、mySonicWall.com での登録が完了している場合、SonicWall ゲートウェイ アンチウイルス、SonicWall アンチスパイウェア、および SonicWall 侵入防御サービス用の 30 日間の無料トライアルを有効化することができます。これらのトライアルは管理インターフェースの「**セキュリティ サービス > ゲートウェイ アンチウイルス**」ページ、「**セキュリティ サービス > アンチスパイウェア**」ページ、および「**セキュリティ サービス > 侵入防御**」ページから個別に有効化してください。

ゲートウェイ アンチウイルス、アンチスパイウェア、および IPS サービスのライセンスの有効化

これらのセキュリティ サービスを利用するには、MySonicWall で装置を登録する必要があります。MySonicWall アカウントの作成と装置の登録については、『*導入ガイド*』を参照してください。閉じた環境でのサービスのアップグレードについては、 *『SonicWall SonicOS 6.5 更新』* を参照してください。

SonicWall アンチスパイウェアは SonicWall ゲートウェイ アンチウイルス、アンチスパイウェア、および侵入防御サービスに含まれているので、受け取った有効化鍵は SonicWall セキュリティ装置上で 3 つのサービスのいずれにも使用できます。

SonicWall セキュリティ装置上で SonicWall ゲートウェイ アンチウイルス、アンチスパイウェア、および侵入防御サービスのライセンスが有効化されていない場合は、そのライセンスを SonicWall の再販業者から、または mySonicWall.com アカウント (アメリカ合衆国およびカナダのお客様に限定) を通して購入する必要があります。

無料トライアル バージョンのアクティブ化

SonicWall ゲートウェイ アンチウイルス、SonicWall アンチスパイウェア、および SonicWall 侵入防御サービスには、ユーザが試用できる無料トライアル バージョンが用意されています。無料トライアル版のセキュリティ サービス (一部またはすべて) を有効化する方法については、お使いの装置の『*導入ガイド*』を参照してください。

SonicWall ゲートウェイ アンチウイルス保護のセットアップ

SonicWall セキュリティ装置で SonicWall ゲートウェイ アンチウイルスのライセンスを有効化しても、ネットワークが自動的に保護されるわけではありません。

SonicWall ゲートウェイ アンチウイルスを設定するには、以下の手順に従います。

1 SonicWall ゲートウェイ アンチウイルスを有効化します。

2 SonicWall ゲートウェイ アンチウイルスの保護をゾーンに適用します。

メモ：SonicWall ゲートウェイ アンチウイルスの詳細なセットアップ手順については、『*SonicWall ゲートウェイ アンチウイルス管理者ガイド*』を参照してください。

トピック:

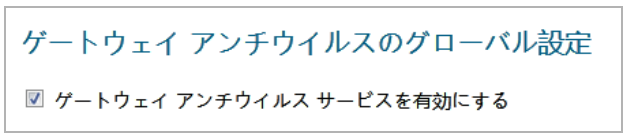
- 「セキュリティ サービス > ゲートウェイ アンチウイルス」ページ
- SonicWall GAV の有効化
- ゾーンに対する SonicWall GAV 保護の適用
- SonicWall GAV の状況情報の表示
- プロトコル フィルタの指定
- ゲートウェイ AV 設定値の設定
- クラウド ゲートウェイ アンチウイルスの設定

「セキュリティ サービス > ゲートウェイ アンチウイルス」ページ

「**セキュリティ サービス > ゲートウェイ アンチウイルス**」ページには、お使いの SonicWall セキュリティ装置で動く SonicWall GAV を設定するための項目があります。また、アンチウイルス状況とアンチウイルス シグネチャもここで表示されます。

SonicWall GAV の有効化

お使いの SonicWall セキュリティ装置で動く SonicWall GAV を有効にするには、「**ゲートウェイ アンチウイルスのグローバル設定**」セクションの「**ゲートウェイ アンチウイルス サービスを有効にする**」チェックボックスをオンにする必要があります。



SonicWall GAV 保護の必要なすべてのゾーンを「**システム セットアップ | ネットワーク > ゾーン**」ページで指定してください。

ゾーンに対する SonicWall GAV 保護の適用

SonicWall GAV をゾーンに適用するのは「**ネットワーク > ゾーン**」ページでゾーンを追加または編集するときです。「**セキュリティ サービス > ゲートウェイ アンチウイルス**」ページから「**ネットワーク > ゾーン**」ページをすばやく表示できます。"**補足:**ゾーンに対するゲートウェイ アンチウイルスの有効化は、「ネットワーク > ゾーン」ページで設定します。" のリンクを選択してください。これは「**ゲートウェイ アンチウイルス状況**」セクションにあります。

メモ：SonicWall GAV 保護をゾーンに適用する手順は、ゾーンに対する SonicWall GAV 保護の適用参照してください。

SonicWall GAV の状況情報の表示

「**ゲートウェイ アンチウイルス状況**」セクションには、アンチウイルス シグネチャ データベースの状態 (例えば、データベースのタイムスタンプ、SonicWall シグネチャ サーバで最新版データベースの有無が確認された最終日時など) が表示されます。SonicWall セキュリティ装置は、起動時および 1 時間ごとに自動的にデータベースの同期化を試みます。

トピック:

- SonicWall GAV シグネチャ データベース状況の確認
- SonicWall GAV シグネチャの更新

SonicWall GAV シグネチャ データベース状況の確認

「**ゲートウェイ アンチウイルス状況**」セクションには、次の情報が表示されます。

- 「**シグネチャ データベース**」には、シグネチャ データベースをダウンロードする必要があるかどうか、あるいはダウンロードが完了したかどうかが示されます。
- 「**シグネチャ データベースのタイムスタンプ**」に表示されるのは、SonicWall GAV シグネチャ データベースの最終更新日時です (SonicWall セキュリティ装置の最終更新日時ではない)。
- 「**最終確認**」には、SonicWall セキュリティ装置がシグネチャ データベースの更新の有無をチェックした最終日時が示されます。SonicWall セキュリティ装置は、起動時および 1 時間ごとに自動的にデータベースの同期化を試みます。
- 「**ゲートウェイ アンチウイルスの失効期日**」には、SonicWall GAV サービスの有効期限が切れる日付が示されます。SonicWall GAV の購読期限が切れると、SonicWall IPS 検査が停止し、SonicWall GAV の構成設定値が SonicWall セキュリティ装置から削除されます。これらの設定は、SonicWall GAV ライセンスを以前に設定された状態に更新し終えると、自動的に復旧されます。

「**ゲートウェイ アンチウイルス状況**」セクションに、"**補足**: ゾーンに対するゲートウェイ アンチウイルスの有効化は、「ネットワーク > ゾーン」ページで設定します。" と表示されます。ネットワーク > ゾーンリンクを選択すると、SonicWall GAV をゾーンに適用するための「**ネットワーク > ゾーン**」ページが表示されます。

メモ：SonicWall GAV 保護をゾーンに適用する手順は、ゾーンに対する SonicWall GAV 保護の適用参照してください。

SonicWall GAV シグネチャの更新

既定で、SonicWall GAV が稼動している SonicWall セキュリティ装置は 1 時間に 1 回 SonicWall シグネチャ サーバをチェックします。新しいシグネチャの更新の有無を管理者が継続的にチェックする必要はまったくありません。また、「**ゲートウェイ アンチウイルス状況**」セクションにある「**更新**」ボタンを選択して、SonicWall GAV データベースを随時に手動で更新することもできます。

SonicWall GAV シグネチャの更新内容は、セキュリティで保護されています。SonicWall セキュリティ装置は最初に、SonicWall 分散執行型手法のライセンス登録時に作成された事前共有鍵を使用して、自己認証する必要があります。シグネチャの要求は HTTPS 経由で転送され、その際にサーバ証明書が完全検証されます。

プロトコル フィルタの指定

SonicWall GAV は、違反があるペイロードを転送するプロトコルの種別をアプリケーションレベルで感知することによって、アプリケーションのコンテキストにおいて特定のアクションを実行し、違反があるペイロードを円滑に拒絶できます。

トピック:

- 受信検査の有効化
- 発信検査の有効化
- ファイル転送の制限
- ゲートウェイ AV 設定のリセット

受信検査の有効化

既定では、着信の **HTTP**、**FTP**、**IMAP**、**SMTP**、および **POP3** トラフィックがすべて、SonicWall GAV で検査されます。必要に応じて汎用的な **TCP ストリーム**を有効化すれば、他のすべての TCP ベース トラフィック (例えば、標準ポートを使用していない SMTP や POP3、IM プロトコル、P2P プロトコルなど) を検査することもできます。

SonicWall GAV のコンテキストにおいて「**受信検査を有効にする**」プロトコル トラフィック処理とは、次のトラフィックを対象とした処理を指します (着信トラフィックの検査: SMTP *対 他のすべてのトラフィック*テーブル を参照)。

- 保護ゾーン、無線ゾーン、または暗号化ゾーンから開始され、任意のゾーン宛てに送出される非SMTP トラフィック
- パブリック ゾーンから非保護ゾーン宛てに送出される非 SMTP トラフィック
- 非保護ゾーンから開始され、保護ゾーン、無線ゾーン、暗号化ゾーン、またはパブリック ゾーン宛てに送出される SMTP トラフィック
- 保護ゾーン、無線ゾーン、または暗号化ゾーンから開始され、保護ゾーン、無線ゾーン、または暗号化ゾーン宛てに送出される SMTP トラフィック

着信トラフィックの検査: SMTP *対* 他のすべてのトラフィック

SMTP トラフィック

宛先 送信元	信頼済み	暗号化	無線	公開	非保護
信頼済み	√	√	√		
暗号化	√	√	√		
無線	√	√	√		
公開	√	√	√	√	√
非保護	√	√	√	√	√

他のすべてのトラフィック

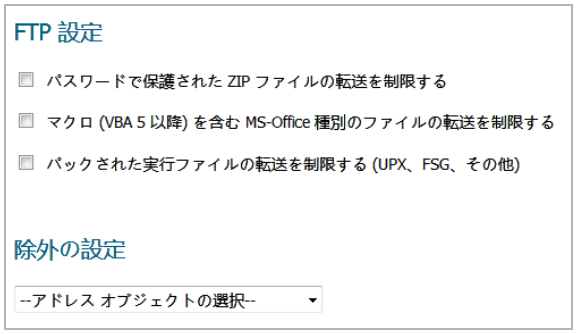
宛先 送信元	信頼済み	暗号化	無線	公開	非保護
信頼済み	√	√	√	√	√
暗号化	√	√	√	√	√
無線	√	√	√	√	√
公開					√
非保護					

発信検査の有効化

「**発信検査を有効にする**」機能は、HTTP、FTP、SMTP、TCP トラフィックに対して利用できます。

ファイル転送の制限

プロトコル (TCP ストリーム以外) ごとに、「**ゲートウェイ アンチウイルスのグローバル設定**」セクションの各プロトコルの下にある「**設定**」ボタンを選択して、特定の属性を持つファイルの転送を制限することができます。



トピック:

- FTP 設定
- 除外の設定

FTP 設定

転送の制限に関係する **FTP 設定**には次のものがあります。

- **パスワードで保護された ZIP ファイルの転送を制限する** - パスワード保護された ZIP ファイルに対して、有効化されたプロトコル経由での転送を無効にします。このオプションは、検査を有効化したプロトコル (HTTP、FTP、SMTP など) でのみ機能します。
- **マクロ (VBA 5 以降) を含む MS-Office 種別のファイルの転送を制限する** - Microsoft Office 97 以降の VBA マクロが収録されたファイルの転送を無効にします。
- **パックされた実行ファイルの転送を制限する (UPX、FSG、その他)** - パックされた実行ファイルの転送を無効にします。

  パッカーは、実行可能ファイルを圧縮するユーティリティです (圧縮に加えて暗号化することもある)。それが正当な目的で使われるなら問題ありませんが、アンチウイルス アプリケーションでの実行可能ファイルの検出を邪魔すべく不明瞭化を意図して使われることもあります。パッカーはメモリ内でファイルを展開するヘッダーを追加し、次にそのファイルを実行します。

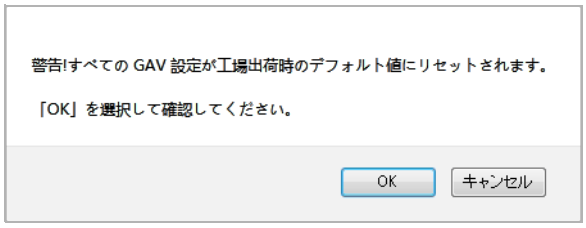
  SonicWall ゲートウェイ アンチウイルスは現在、最も一般的なパック形式である、UPX、FSG、PKLite32、Petite、ASPack を認識します。その他の形式は、SonicWall GAV シグネチャのアップデートとともに動的に追加されます。

除外の設定

- ドロップダウン メニュー - 選択したアドレス オブジェクトを転送の制限に関係する FTP 設定から除外します。

ゲートウェイ AV 設定のリセット

1 すべてのゲートウェイ アンチウイルス (AV) 設定を出荷時の既定値にリセットするには、「**ゲートウェイ AV 設定のリセット**」ボタンを選択します。確認メッセージが表示されます。



2 「**OK**」を選択します。

ゲートウェイ AV 設定値の設定

「**ゲートウェイ アンチウイルスのグローバル設定**」セクションの下部にある「**ゲートウェイ AV の設定**」ボタンを選択すると、「**ゲートウェイ アンチウイルス設定**」ダイアログが表示されます。このダイアログでは、クライアント不要の警告通知を設定したり、SonicWall GAV 除外リストを作成したりできます。

トピック:

- ゲートウェイ AV 設定値の設定
- HTTPクライアント不要の通知の設定
- SonicWall GAV 除外リストの設定

ゲートウェイ AV 設定値の設定

ゲートウェイAV のオプションを設定するには、以下の手順を実行します。

1 電子メールまたは添付ファイルでウイルスが検出されたとき SonicWall GAV からクライアントへ電子メール メッセージ (SMTP) を送信しないよう抑制するには、「**SMTP 応答を無効にする**」チェックボックスをオンにします。このオプションは、既定では選択されていません。

2 EICAR Standard Anti-Virus Test ファイルは、SonicWall ゲートウェイ AV サービスの適切な動作をチェックして確認する特別なウイルス シミュレータ ファイルです。EICAR の検出を抑制するには、「**EICAR テスト ウイルスの検出を無効にする**」チェックボックスをオンにします。このオプションは、既定では選択されています。

3 バイト サービング (byte serving) による送信 (HTTP メッセージまたはファイルの一部分だけを送信すること) を許可するには、「**ゲートウェイ アンチウイルス HTTP Byte-Range 要求を有効にする**」チェックボックスをオンにします。このオプションは、既定では選択されています。

SonicWall ゲートウェイ アンチウイルス (GAV) セキュリティ サービスは、悪意が疑われるコンテンツを部分的に取得して再組み立てすることを阻止するために、既定で HTTP Byte-Range 要求の使用を抑制しています。これは接続を打ち切って悪意のあるペイロードをユーザがもう受信できないようにすることで達成されます。このオプションを選択すると、この既定の動作が無効になります。

4 FTP 'REST' 要求の使用を許可してメッセージやファイルの部分的な取得と再組み立てを行えるようにするには、「**ゲートウェイ アンチウイルス FTP 'REST' 要求を有効にする**」チェックボックスをオンにします。このオプションは、既定では選択されています。

SonicWall GAV は、悪意が疑われるコンテンツを部分的に取得して再組み立てすることを阻止するために、既定で FTP 'REST' (restart) 要求の使用を抑制しています。これは接続を打ち切って悪意のあるペイロードをユーザがもう受信できないようにすることで達成されます。このオプションを選択すると、この既定の動作が無効になります。

5 圧縮率の高いファイル (またはファイルの一部分) のスキャンを抑制するには、「**高圧縮率のファイルの一部をスキャンしない**」チェックボックスをオンにします。このオプションは、既定では選択されています。

6 zip/gzip による圧縮が多段階で行われているファイルを遮断するには、「**複数レベルで zip/gzip 圧縮されているファイルを遮断する**」チェックボックスをオンにします。このオプションは、既定では選択されています。

7 ゲートウェイ AV を検出専用モード (ウイルス トラフィックの検出とログへの記録だけを行い、トラフィックを止めないモード) にするには、「**検出専用モードを有効にする**」チェックボックスをオンにします。このオプションは、既定では選択されていません。

HTTPクライアント不要の通知の設定

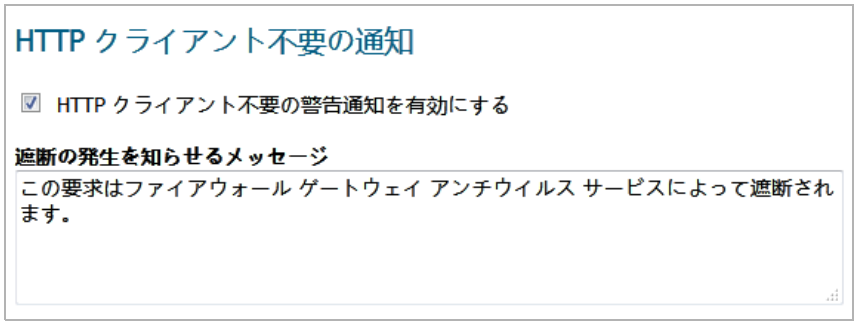
「HTTP クライアント不要の通知」は、HTTP サーバから入り込んだ脅威が GAV に検出されたときに、ユーザに通知する機能です。

この機能が無効化されている場合、HTTP サーバから送られてきた脅威を GAV が検出すると、その脅威は GAV によって遮断され、ユーザに空白の HTTP ページが表示されます。たいていの場合、ユーザはページの再ロードを試みます。 脅威はユーザには意識されないためです。「HTTPクライアント不要の通知」機能によって、HTTP サーバからの脅威が GAV に検出されたことが、ユーザに通知されます。

ヒント： HTTP クライアント不要の通知機能は、SonicWall アンチスパイウェアでも利用できます。

この機能を設定するには、以下の手順を実行します。

1 「**HTTP クライアント不要の警告通知を有効にする**」チェックボックスをオンにします。このオプションは、既定では選択されています。



2 必要に応じて、「**遮断の発生を知らせるメッセージ**」フィールドにメッセージを入力します。既定のメッセージは "この要求はファイアウォール ゲートウェイ アンチウイルス サービスによって遮断されます" です。

ヒント： 「**セキュリティ サービス > 基本設定**」ページの「**セキュリティ サービスの設定**」という見出しの下で、HTTP クライアント不要通知のタイムアウトを設定できます。

SonicWall GAV 除外リストの設定

除外リストにリストされた IP アドレスに対しては、トラフィックのウイルス スキャンがバイパスされます。「**ゲートウェイ AV 除外リスト**」セクションでは、SonicWall GAV スキャンの対象から除外するアドレス オブジェクトを選択するか、IP アドレスの範囲を定義できます。

注意：SonicWall GAV の保護対象から除外する項目は、慎重に指定してください。

IP アドレスを除外範囲に追加するには:

1 「**管理 | セキュリティ設定 > セキュリティ サービス > ゲートウェイ アンチウイルス**」に移動します。

2 「**ゲートウェイ アンチウイルスのグローバル設定**」セクションまでスクロールします。

3 「**ゲートウェイ AV の設定**」ボタンを選択します。

4 「**ゲートウェイ AV 除外リスト**」セクションの「**ゲートウェイ アンチウイルス除外リストを有効にする**」チェックボックスをオンにして除外リストを有効化します。

5 以下のいずれかを選択します。

- 「**アドレス オブジェクトを使用する**」ラジオ ボタン
  a) ドロップダウン メニューからアドレス オブジェクトを選択します。
  b) 「ステップ 6」に移動します。
- 「**アドレス範囲を使用する**」ラジオ ボタン
  a) 「**追加**」ボタンを選択します。「**ゲートウェイ アンチウイルス範囲の追加**」ダイアログが表示されます。

  b) 「**開始 IP アドレス**」フィールドおよび「**終了 IP アドレス**」フィールドに IP アドレスの範囲を入力します。
  c) 「**OK**」を選択します。ここで入力した IP アドレスの範囲は、「**ゲートウェイ アンチウイルス除外リスト**」テーブルに表示されます。

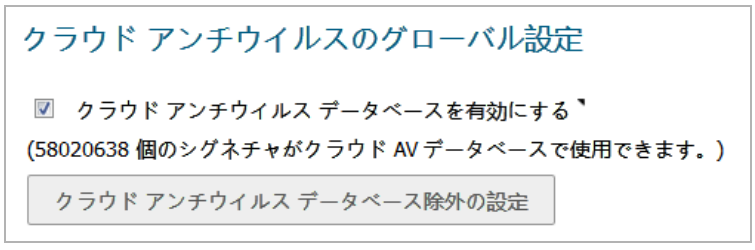
ⓘ **メモ：**エントリを変更するには、「**設定**」列の「**編集**」アイコンを選択します。また、エントリを削除するには、「**削除**」アイコンを選択します。除外リストのすべてのエントリを削除するには、「**すべて削除**」ボタンを選択します。

6 「**OK**」を選択します。

クラウド ゲートウェイ アンチウイルスの設定

クラウド ゲートウェイ アンチウイルス機能を有効にするには、以下の手順を実行します。

1 「**セキュリティ サービス > ゲートウェイ アンチウイルス > クラウド アンチウイルスのグローバル設定**」セクションに移動します。

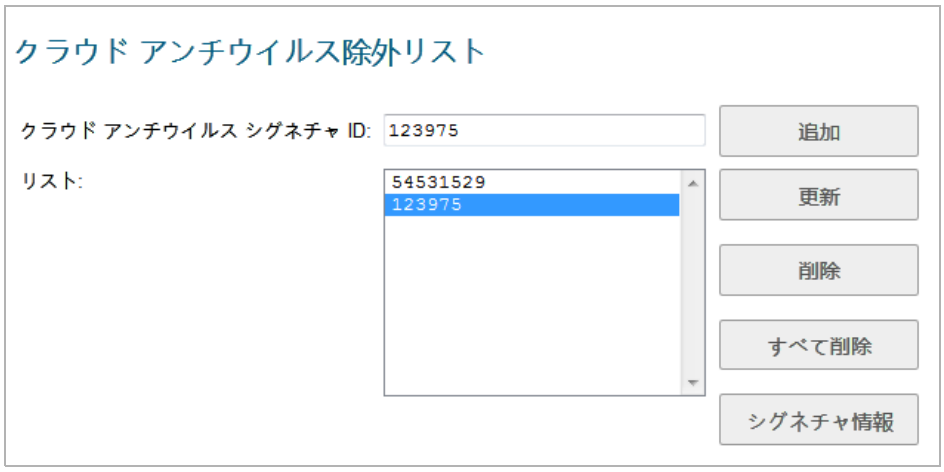


2 「**クラウド アンチウイルス データベースを有効にする**」チェックボックスをオンにします。(このオプションは既定でオンになっています。)

特定のクラウド シグネチャを執行対象から除外することもできます。これで、偽陽性による誤検出の問題を軽減したり、特定のウイルス ファイルを必要に応じてダウンロードしたりできます。

除外リストを設定するには、次の手順に従います。

1 「**クラウド アンチウイルス データベース除外の設定**」を選択します。「**クラウド アンチウイルス除外の追加**」ダイアログが表示されます。



2 「**クラウド アンチウイルス シグネチャ ID**」フィールドにシグネチャ ID を入力します。ID は数値でなければなりません。

3 「**追加**」を選択します。

4 追加するシグネチャ ID ごとに、ステップ 2 とステップ 3 を繰り返します。

5 必要に応じて、シグネチャ ID を更新します。

   a 「**リスト**」フィールドでシグネチャ ID を選択します。

   b 更新後のシグネチャを「**クラウド アンチウイルス シグネチャ ID**」フィールドに入力します。

   c 「**更新**」を選択します。

6 必要に応じて、以下の削除を行います。

   - 特定のシグネチャ ID を削除する場合は、「**リスト**」フィールドで削除する ID を選択し、「**削除**」を選択します。
   - すべてのシグネチャ、「**すべて削除**」を選択します。

7 シグネチャの最新情報を表示するには、リスト内のシグネチャ ID を選択して、「**シグネチャ情報**」ボタンを選択します。シグネチャの情報が SonicALERT ウェブサイトに表示されます。

8 クラウド アンチウイルス除外リストの設定を完了したら、「**OK**」を選択します。

SonicWall GAV シグネチャの表示

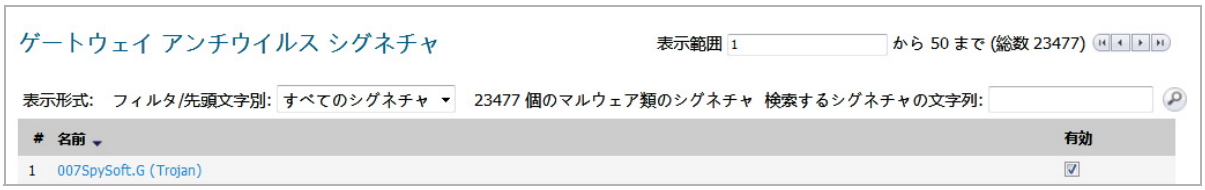
「**ゲートウェイ アンチウイルス シグネチャ**」セクションでは、SonicWall GAV シグネチャ データベースの内容を表示できます。「**ゲートウェイ アンチウイルス シグネチャ**」テーブルに表示されるエントリはいずれも、SonicWall セキュリティ装置にダウンロードされた SonicWall GAV シグネチャ データベースから取得されたものです。マルウェア類のシグネチャの個数がテーブルの上部に表示されます。

メモ：時間の経過につれてデータベース内のシグネチャ エントリも変わり、新たな脅威に対する対処が可能となります。

トピック:

- シグネチャの表示
- ゲートウェイ アンチウイルス シグネチャ テーブルの操作
- ゲートウェイ アンチウイルス シグネチャ データベースでの検索

シグネチャの表示



シグネチャは、さまざまな形式で表示できます。

ヒント：シグネチャのフィルタリングを行うと、見つかったシグネチャの個数がデータベース内のシグネチャの総数とともに表示されます。

- **表示形式** - 「**フィルタ/先頭文字別**」ドロップダウン メニューから、以下のいずれかを選択します。
  - **すべてのシグネチャ** - テーブル内のすべてのシグネチャを表示します。 1 ページあたりの表示個数は、最高 50 個です。
  - **0 - 9** - メニューから選択した番号で始まるシグネチャ名を表示します。
  - **A - Z** - メニューから選択した英字で始まるシグネチャ名を表示します。
- **検索文字列** - 特定の文字列を含むシグネチャを表示します。
  a 「**検索するシグネチャの文字列**」フィールドに文字列を入力します。
  b 「**虫眼鏡**」アイコンを選択します。

ゲートウェイ アンチウイルス シグネチャ テーブルの操作

「**ゲートウェイ アンチウイルス シグネチャ**」テーブルには、SonicWall GAV シグネチャが 1 ページあたり 50 個まで表示されます。「**表示範囲**」フィールドには、最初のシグネチャのテーブル数が表示されます。テーブルの操作方法については、『*SonicWall SonicOS 6.5 SonicOS について*』を参照してください。

ゲートウェイ アンチウイルス シグネチャ データベースでの検索

シグネチャ データベースの検索を行うには、「**検索するシグネチャの文字列**」フィールドに検索文字列を入力し、「**検索**」アイコンを選択します。

指定した文字列に一致するシグネチャだけが「**ゲートウェイ アンチウイルス シグネチャ**」テーブルに表示されます。

14

侵入防御サービスの有効化

- 侵入防御サービスについて (181 ページ)
- 侵入防御サービスの設定 (183 ページ)

侵入防御サービスについて

侵入防御サービス (IPS) は、ウェブ、電子メール、ファイル転送、Windows サービス、DNS などの主要ネットワーク サービスに対する拡張保護を実現する構成可能な高性能精密パケット検査エンジンを備えています。SonicWall IPS は、アプリケーションの脆弱性ばかりでなくトロイの木馬、ピアツーピア、スパイウェア、バックドア侵入企図から保護することを目的に設計されています。また、SonicWall の精密パケット検査エンジンで使用されている広範なシグネチャ言語により、アプリケーションおよびプロトコルで新たに見つかった脆弱性に対する事前対処的な防御を実現します。SonicWall IPS は、SonicWall の業界で有力な分散執行型手法 (DEA) を介して新しいハッカー攻撃のシグネチャの管理および更新に伴う高価で時間のかかる負担を軽減します。SonicWall IPS の詳細なシグネチャ情報によって攻撃をグローバル、攻撃グループ別、またはシグネチャごとに検出して防止することで、柔軟性を祭壇源に高めるとともに、偽陽性による誤検出を抑制できます。

トピック:

- SonicWall 精密パケット検査 (181 ページ)
- SonicWall 精密パケット検査の概要 (182 ページ)
- 用語集 (183 ページ)
- IPS 状況 (184 ページ)
- IPS グローバル設定 (184 ページ)

SonicWall 精密パケット検査

精密パケット検査では、パケットのデータ部分を確認します。精密パケット検査技術には、侵入検出と侵入防御があります。 侵入検出は、トラフィック内の異常を検出して管理者に警告します。侵入防御は、トラフィック内の異常を検出してそれに対応し、トラフィックの通過を阻止します。侵入防御はトラフィックの異常を検出して反応することによりトラフィックの通過を阻止します。

精密パケット検査は、通過するトラフィックをルールに基づいてファイアウォールで分類できるようにする技術です。これらのルールには、パケットの第 3 層および第 4 層の内容に関する情報ばかりでなく、アプリケーション データ (例、FTP セッション、HTTP ウェブ ブラウザ セッション、またはミドルウェア データベース接続) など、パケットのペイロードの内容を記述している情報も含まれています。管理者はこの技術により、ファイアウォールを通過する侵入を、検出してログに記録するだけでなく、阻止することができます (例えば、パケットの破棄、TCP 接続のリセットなど)。SonicWall の精密パケット検査技術は、TCP 断片化が発生していない場合と同様に TCP断片化バイト ストリーム検査を適切に処理します。

SonicWall 精密パケット検査の概要

精密パケット検査技術を使用すると、ファイアウォールでプロトコル内を精査し、アプリケーション層で情報を検証して、アプリケーションの脆弱性を対象とした攻撃を阻止できます。これは、SonicWall 侵入防御サービスの背後にある技術です。SonicWall の精密パケット検査技術は、SonicWall 分散執行型手法から配布される動的シグネチャ更新を可能にします。

以下の手順では、SonicWall 精密パケット検査手法の仕組みを説明しています。SonicWall 精密パケット検査手法を参照してください。

1 パターン定義言語インタープリタは、既知および不明なプロトコル、アプリケーション、企図の検出と防止のために記述できるシグネチャを使用します。

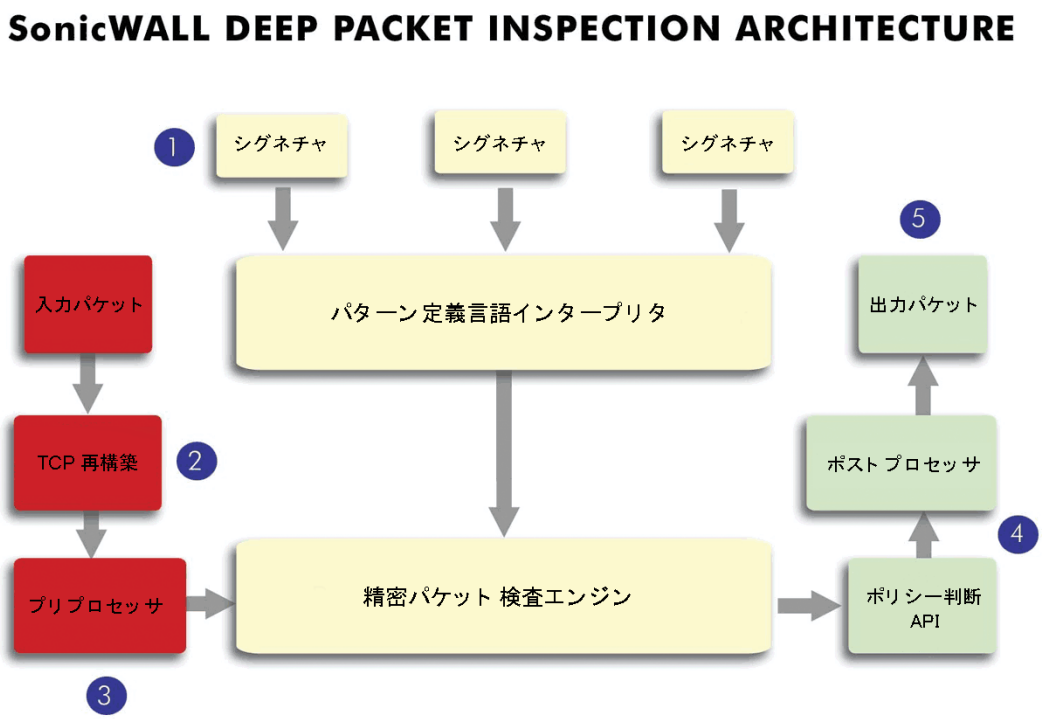
2 順不同で到着する TCP パケットは、精密パケット検査フレームワークにより再構築されます。

3 精密パケット検査エンジンの前処理には、パケットのペイロードの正規化を伴います。例えば、HTTP 要求は URL エンコードされる場合があり、このため、要求はペイロードで適切なパターン一致を実行するために URL デコードされます。

4 精密パケット検査エンジンのポストプロセッサは、変更なしにパケットを渡すか、パケットを削除するか、TCP 接続をリセットするアクションを実行します。

5 SonicWall の精密パケット検査フレームワークは、パケットが順不同でない限り、再構築を実行することなく TCP の断片全体で完全なシグネチャー致をサポートします。これにより、プロセッサとメモリの効率的な使用が可能になり、パフォーマンスが向上します。

SonicWall 精密パケット検査手法



用語集

- **ステートフル パケット検査** - パケットのヘッダーを調べ、ポート、プロトコル、および IP アドレスに基づいてアクセスを制御します。
- **精密パケット検査** - パケットのデータ部分が調査されます。ファイアウォールでプロトコル内を精査し、アプリケーション層で情報を検証して、アプリケーションの脆弱性を対象とした攻撃を阻止できます。
- **侵入検知** - 情報技術の隙を狙った悪質なアクティビティを特定してフラグを設定するプロセスです。
- **偽陽性** - 誤って検出された攻撃トラフィックのパターンを指します。
- **侵入防御** - トラフィックの異常や悪質なアクティビティを検出し、それに対処することです。
- **シグネチャ** - 侵入、ワーム、アプリケーション悪用、ピア ツー ピア、インスタント メッセージングなどのトラフィックを検出して阻止することを目的に作成されたコードです。

侵入防御サービスの設定

侵入防御サービス (IPS) は、「**管理 | セキュリティ設定 > セキュリティ サービス > 侵入防御**」ページ (いくつかのパネルがある) で設定されます。

- IPS 状況
- IPS グローバル設定
- IPS ポリシー

トピック:

- IPS 状況 (184 ページ)
- IPS グローバル設定 (184 ページ)
- ゾーンに対する IPS 保護の設定 (188 ページ)
- IPS ポリシー (188 ページ)

IPS 状況

「**IPS 状況**」パネルには、シグネチャ データベースおよび SonicWall IPS ライセンスに関する状況情報が表示されます。

「**IPS 状況**」パネルには、次の情報が表示されます。

- 「**シグネチャ データベース**」には、シグネチャ データベースがダウンロード中か、ダウンロード済みか、またはダウンロードする必要があるかが示されます。シグネチャ データベースは、およそ 1 時間ごとに自動的に更新されます。また、「**IPS 状況**」セクションにある「**更新**」ボタンを選択して、IPS データベースを随時に手動で更新することもできます。
- 「**シグネチャ データベースのタイムスタンプ**」に表示される日時は、SonicWall セキュリティ装置ではなく IPS シグネチャ データベースが最後に更新された日時です。
- 「**最終確認**」には、SonicWall セキュリティ装置がシグネチャ データベースの更新の有無をチェックした最終日時が示されます。SonicWall セキュリティ装置は、起動時および 1 時間ごとに自動的にデータベースの同期化を試みます。
- 「**IPS サービスの失効期日**」には、IPS サービスの有効期限が切れる日付が示されます。IPS の購読期限が切れると、SonicWall IPS 検査が停止し、IPS の構成設定値が SonicWall セキュリティ装置から削除されます。これらの設定は、IPS のライセンスを更新すると、自動的に復元されます。
- **メモ:** ゾーンごとに侵入防御サービスを有効にするには、「ネットワーク > ゾーン」ページに移動します。

  ここに示す「ネットワーク > ゾーン」を選択すると、「**管理 | システム セットアップ > ネットワーク > ゾーン**」ページが表示され、ゾーンの IPS を設定できます。ゾーンに対する IPS 保護の設定を参照してください。

IPS グローバル設定

「**IPS グローバル設定**」パネルには、ファイアウォール上で SonicWall IPS を有効にするための主要な設定があります。

SonicWall IPS を有効にするには、ファイアウォール上で IPS をグローバルに有効にして攻撃のクラスを選択します。必要に応じて、**IPS 除外リスト**を設定することもできます。

トピック:

- IPS を有効にする (185 ページ)
- IPS 除外リストの設定 (186 ページ)
- IPS 設定と IPS ポリシーのリセット (187 ページ)
- ゾーンに対する IPS 保護の設定 (188 ページ)

IPS を有効にする

ファイアウォール上で IPS を有効にするには、以下の手順を実行します。

1 「**セキュリティ設定 | セキュリティ サービス > 侵入防御**」ページに移動します。

2 下にスクロールして「**IPS グローバル設定**」セクションを表示します。

3 「**IPS を有効にする**」を選択します。

4 以下の**シグネチャ グループ**のそれぞれについて、設定する動作 (**すべて防御**、**すべて検知**、または両方) を選択します。

- **高危険度のシグネチャ**
- **中危険度のシグネチャ**
- **低危険度のシグネチャ**

メモ：ファイアウォールで侵入防御を有効にするには、これらの**シグネチャ グループ**のうち 1 つ以上のグループに「**すべて防御**」を指定する必要があります。「**すべて防御**」が選択されていない場合、ファイアウォールで侵入防御は動作しません。

メモ：シグネチャ グループのすべてのグループに「**すべて防御**」と「**すべて検知**」の両方を選択すると、最も危険で破壊的な攻撃からネットワークを保護できます。

各種の攻撃が頻繁にすばやく繰り返されることがあるので、すべての攻撃を記録するとログがすぐに一杯になってしまいます。ログに記録される攻撃の重複数を減らすには、「**ログ冗長フィルタ (秒)**」フィールドに、同じ攻撃が「**調査 | ログ > イベント ログ**」ページで単一のエントリとして記録される秒数を入力します。この間隔の範囲は 0 ～ 86400 秒です。攻撃のさまざまな優先順位の既定値は次のとおりです。

- **高危険度のシグネチャ**: **0** 秒
- **中危険度のシグネチャ**: **0** 秒
- **低危険度のシグネチャ**: **60** 秒

5 「**適用**」を選択します。

IPS 除外リストの設定

(オプション) IPS 除外リストを設定するには、次の手順を実行します。

1 「**管理 | セキュリティ設定 > セキュリティ サービス > 侵入防御**」ページに移動します。

2 下にスクロールして「**IPS グローバル設定**」セクションを表示します。

3 「**IPS を有効にする**」を選択します。

4 「**IPS の設定**」ボタンを選択します。

「**IPS 除外リスト**」ダイアログが表示されます。

5 「**IPS 除外リストを有効にする**」を選択します。

6 「**アドレス オブジェクトを使用する**」オプションまたは「**アドレス範囲を使用する**」オプションを選択します。

7 「**アドレス オブジェクトを使用する**」オプションを選択した場合は、除外するアドレス オブジェクトをメニューから選択します。

8 「**アドレス範囲を使用する**」オプションを選択した場合は、「**追加**」ボタンを選択します。

「**IPS 範囲の追加**」ダイアログが表示されます。

9 「**開始 IP アドレス**」ボックスおよび「**終了 IP アドレス**」ボックスに、除外する IP アドレスの範囲を入力します。

10 「**OK**」を選択します。

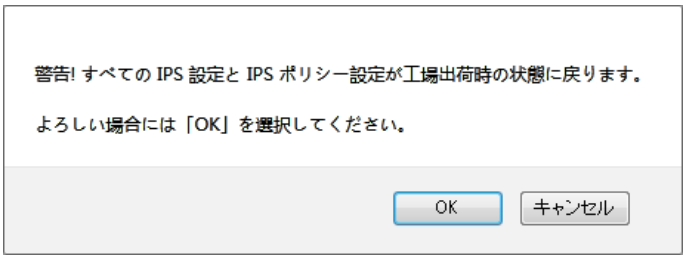
IPS 設定と IPS ポリシーのリセット

IPS 設定と IPS ポリシーをリセットするには、以下の手順を実行します。

1 「**管理 | セキュリティ設定 > セキュリティ サービス > 侵入防御**」ページに移動します。

2 下にスクロールして「**IPS グローバル設定**」セクションを表示します。

3 「**IPS の設定とポリシーをリセット**」を選択します。以下のメッセージが表示されます。



4 「**OK**」を選択します。

画面の下部に、以下のメッセージが表示されます。状況 : 設定が更新されました。

ゾーンに対する IPS 保護の設定

「**管理 | システム セットアップ > ネットワーク > ゾーン**」ページで、SonicWall IPS をゾーンに適用すると、各ネットワーク ゾーンと WAN の間だけでなく、内部ゾーン間でも SonicWall IPS を執行することができます。例えば、LAN ゾーン上の SonicWall IPS を有効にすると、すべての送受信 LAN トラフィックに対してSonicWall IPS を執行することができます。

「**セキュリティ サービス > 侵入防御** 」ページの「**IPS 状況**」セクションで、**ネットワーク > ゾーン** リンクを選択して「**管理 | システム セットアップ > ネットワーク > ゾーン** 」ページにアクセスします。「**ネットワーク > ゾーン**」ページにリストされているゾーンに SonicWall IPS を適用します。

ゾーン上の SonicWall を有効にするには、次の手順を実行します。

1 「**管理 | システム セットアップ > ネットワーク > ゾーン**」ページに移動するか、「**管理 | セキュリティ設定 > セキュリティ サービス > 侵入防御** 」ページの「**IPS 状況**」セクションから、**ネットワーク > ゾーン** リンクを選択します。「**ネットワーク > ゾーン**」ページが表示されます。

2 「**ゾーンの設定**」テーブルの「**設定**」列で、SonicWall IPS を適用する対象のゾーンの**編集**アイコンを選択します。「**ゾーンの編集**」ダイアログが表示されます。

3 「**IPS を有効にする**」を選択します。チェックマークが表示されます。SonicWall IPS を無効にするには、このオプションをクリアします。

4 「**OK**」を選択します。

「**ネットワーク > ゾーン**」ページで作成した新規のゾーンに対しても、SonicWall IPS 保護を有効にすることができます。「**追加**」アイコンを選択すると、「**ゾーンの追加**」ダイアログ (設定内容は「**ゾーンの編集**」ダイアログと同じ) が表示されます。

IPS ポリシー

「**IPS ポリシー**」パネルを使用すると、SonicWall IPS のシグネチャを表示し、シグネチャの処理をシグネチャの種別またはシグネチャごとに設定することができます。種別とは攻撃の種類に基づいてシグネチャをグループ分けしたものです。

シグネチャは以下の方法で表示できます。

- 種別の設定の表示および設定 (189 ページ)
- シグネチャの設定の表示および設定 (190 ページ)
- 特定の種別のシグネチャの表示および設定 (190 ページ)
- 優先順位メニュー (191 ページ)
- シグネチャ IDの検索 (191 ページ)

種別の設定の表示および設定

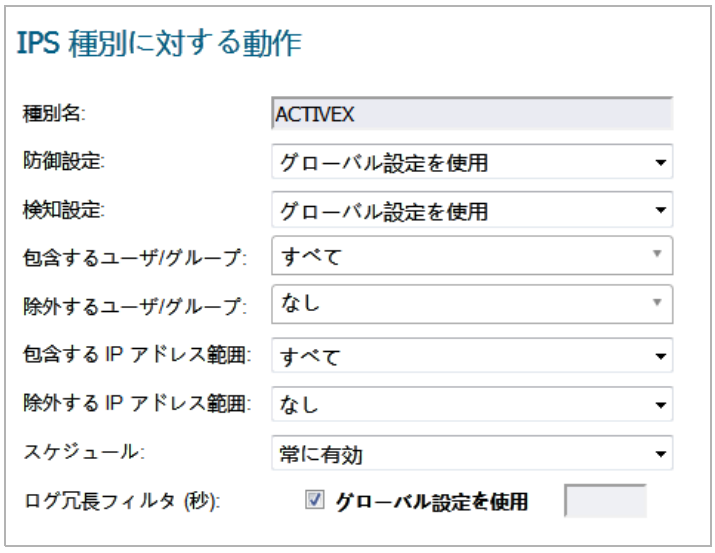
「**表示形式**」行の「**シグネチャ種別**」メニューを使用すると、「**種別**」列に表示する種別またはシグネチャを選択できます。「**すべての種別**」または「**すべてのシグネチャ**」を選択したり、「**ACTIVEX**」や「**DNS**」などの個々の種別を選択したりすることができます。個々の種別を選択すると、その種別のシグネチャが表示されます。

「**種別**」列の列見出しの横にある上または下向きの矢印をクリックすると、昇順または降順で種別およびシグネチャを並べ替えることができます。

特定の種別に対する IPS 種別の設定を表示または変更するには、以下の手順を実行します。

1 「**シグネチャ種別**」メニューで「**すべての種別**」を選択します。

2 該当する種別の「**設定**」列で**編集**アイコンを選択します。「**IPS 種別に対する動作**」ダイアログが表示されます。



3 「**防御設定**」および「**検知設定**」メニューから、「**グローバル設定を使用**」、「**有効**」、または「**無効**」を選択します。「**グローバル設定を使用**」を選択すると「**IPS グローバル設定**」セクションで設定した値が使用されますが、このメニューで「**有効**」または「**無効**」を選択して「**IPS グローバル設定**」をオーバーライドすることもできます。

4 残りのメニューで目的の値を選択します。

5 「**ログ冗長フィルタ (秒)**」オプションでは、「**IPS グローバル設定**」セクションで設定した値を使用する場合、「**グローバル設定を使用**」を選択します。

6 「**OK**」を選択します。

シグネチャの設定の表示および設定

特定のシグネチャに対する IPS シグネチャの設定を表示または変更するには、以下の手順を実行します。

1 「**シグネチャ種別**」メニューで「**すべてのシグネチャ**」を選択します。

2 該当するシグネチャの「**設定**」列で**編集**アイコンを選択します。「**シグネチャに対する動作**」ダイアログが表示されます。

最初の 5 つのボックスはグレーアウトされています。それらのボックスには、そのシグネチャについて設定できないデータが表示されます。

3 「**防御設定**」および「**検知設定**」メニューから、「**有効**」または「**無効**」を選択します。「**種別設定を使用**」オプションは無効になっています。

4 残りのメニューで目的の値を選択します。

5 「**ログ冗長フィルタ (秒)**」オプションでは、「**IPS グローバル設定**」セクションで設定した値を使用する場合、「**種別設定を使用**」を選択します。

6 「**OK**」を選択します。

特定の種別のシグネチャの表示および設定

特定の種別のシグネチャを表示および設定するには、以下の手順を実行します。

1 「**シグネチャ種別**」メニューで、個々の種別の中から 1 つを選択します。その種別のシグネチャが表示されます。

2 該当するシグネチャの「**設定**」列で**編集**アイコンを選択します。「**シグネチャに対する動作**」ダイアログが表示されます。

最初の 5 つのボックスはグレーアウトされています。それらのボックスには、そのシグネチャについて設定できないデータが表示されます。

3 「**防御設定**」および「**検知設定**」メニューから、「**有効**」または「**無効**」を選択します。「**種別設定を使用**」オプションは無効になっています。

4 残りのメニューで目的の値を選択します。

5 「**ログ冗長フィルタ (秒)**」オプションでは、「**IPS グローバル設定**」セクションで設定した値を使用する場合、「**種別設定を使用**」を選択します。

6 「**OK**」を選択します。

優先順位メニュー

「**優先順位**」メニューでは、表示したいシグネチャの優先順位を指定できます。

表示したいシグネチャの優先順位を指定するには、次の手順を実行します。

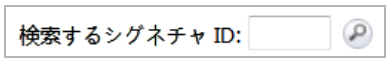
- 「**優先順位**」メニューから、次の優先順位のいずれかを選択します。
  - **すべて**
  - **高い**
  - **中間**
  - **低い**

シグネチャ IDの検索

「**検索するシグネチャ ID**」ボックスを使用すると、特定のシグネチャに対する IPS シグネチャの設定を表示または変更できます。

特定のシグネチャに対する IPS シグネチャの設定を表示または変更するには、以下の手順を実行します。

1 「**検索するシグネチャ ID**」ボックスに、シグネチャ ID を入力します。



2 このフィールドの横の「**検索**」アイコンを選択します。「**シグネチャに対する動作**」ダイアログが表示されます。

最初の 5 つのフィールドはグレーアウトされています。それらのフィールドには、そのシグネチャについて設定できないデータが表示されます。

3 「**防御設定**」および「**検知設定**」メニューから、「**有効**」または「**無効**」を選択します。「**種別設定を使用**」オプションは無効になっています。

4 残りのメニューで目的の値を選択します。

5 「**ログ冗長フィルタ (秒)**」オプションでは、「**IPS グローバル設定**」セクションで設定した値を使用する場合、「**種別設定を使用**」を選択します。

6 「**OK**」を選択します。

15

キャプチャ ATP の設定

- セキュリティ サービス > キャプチャ ATP
- キャプチャ ATP について
- キャプチャ ATP の有効化
- 「セキュリティ サービス > キャプチャ ATP」ページについて
- キャプチャ ATP の設定
- GAV またはクラウド アンチウイルスの無効化

セキュリティ サービス > キャプチャ ATP

重要：Capture Advanced Threat Protection (キャプチャ ATP) はゲートウェイ アンチウイルス (GAV) と同様に、ファイアウォールに対するアドオン セキュリティ サービスであり、ファイアウォールで有害ファイルを識別するために使用します。

キャプチャ ATP は、SonicOS 6.5 以降を実行するすべての SuperMassive シリーズ、NS*a* シリーズ、NSA シリーズ、TZ600/TZ600P、および TZ500/TZ500W ファイアウォールでサポートされています。ただし、キャプチャ機能はアクティブ/アクティブ DPI モードではサポートされません。

キャプチャ ATP を有効にするには、最初にライセンスを取得し、さらにゲートウェイ アンチウイルス (GAV) サービスとクラウド アンチウイルス データベース サービスを有効にする必要があります。キャプチャ ATP のライセンスを取得すると、MySonicWall アカウントでキャプチャ ATP の状況を確認でき、警告と通知を設定して受け取ることができるようになります。

キャプチャ ATP とそのライセンス方法、および MySonicWall アカウントを使って警告と通知を設定および受け取る方法については、『*SonicOS 6.5 キャプチャ ATP 機能ガイド*』を参照してください。

キャプチャ ATP について

Capture Advanced Threat Protection (キャプチャ ATP) を追加すると、ファイアウォールは、あるファイルが悪質なものかを識別するため、そのファイルをクラウドに転送できます。クラウドでは SonicWall キャプチャ ATP サービスがファイルを分析して、ウイルスなどの有害な要素が含まれるかどうかを確認します。続いてキャプチャ ATP は、結果をファイアウォールに送信します。分析と報告は、ファイルがファイアウォールによって処理されている間にリアルタイムで実行されます。

キャプチャ ATP クラウドに送信されるすべてのファイルは、暗号化された接続を経由します。ファイルの分析は数分で完了し、有害であると判定された場合を除き、削除されます。有害ファイルは、暗号化された HTTPS 接続経由で SonicWall Threats Research チームに送信され、詳細に分析されたのち、脅威に関する情報の充実に活用されます。それ以外の場所にファイルを分析用に転送することはありません。有害ファイルは、脅威に関する情報に活用した後、受信から 30 日以内に削除されます。

キャプチャ ATP は、ファイル分析報告 (脅威報告) を作成して、脅威となる動作に関する詳細な情報を提供します。

ファイアウォールは顧客が保有する施設内にありますが、キャプチャ ATP のサーバとデータベースは SonicWall の施設内にあります。ファイアウォールは、キャプチャ ATP クラウドとの間にセキュアな接続を作成してから、データの転送を開始します。

キャプチャ ATP は、ゲートウェイ アンチウイルス (GAV) およびクラウド アンチウイルス サービスと連携して動作します。キャプチャ ATP は、GAV によって解析された電子メール ヘッダー情報 (to、cc、bcc) もログ/表示します。

キャプチャ ATP の詳細については、『*SonicOS 6.2.6 キャプチャ ATP 機能ガイド*』を参照してください。

トピック:

- ファイルの前処理 (194 ページ)
- 分析が完了するまでのファイルの遮断 (194 ページ)
- 暗号化接続を使ったファイル送信
- キャプチャ ATP によるわかりやすいファイル名表示 (195 ページ)
- キャプチャ ATP ライセンスの有効化

ファイルの前処理

キャプチャ ATP に分析のため送信されるすべてのファイルは、最初に GAV で前処理され、有害または無害と判定されます。GAV の設定を使って、GAV とキャプチャ ATP によるスキャンから除外するアドレス オブジェクトを選択または定義することもできます。

前処理で有害または無害と判定されたファイルは、キャプチャ ATP で分析されません。前処理段階でファイルが有害か無害か判定されなかった場合、ファイルは分析のためキャプチャ ATP に送信されます。

分析が完了するまでのファイルの遮断

HTTP/HTTPS ダウンロードについては、**「判定が返ってくるまでファイルのダウンロードを遮断する」**というオプションがあります。これは、キャプチャ ATP がファイルを完全に分析し、有害または無害と判定するまで、一切のパケットを通過させないというものです。ファイルは、最後のパケットが分析されるまで保留となります。ファイルにマルウェアが含まれる場合、最後のパケットが破棄され、ファイルは遮断されます。脅威報告には、脅威や感染に対処するために必要な情報が記載されています。

暗号化接続を使ったファイル送信

すべてのファイルは、暗号化接続を使用してキャプチャ ATP クラウドに送信されます。SonicWall はこれらのファイルを保存しません。すべてのファイル タイプは、有害、無害の区別なく、一定の期間が過ぎればキャプチャ ATP サーバから削除されます。

SonicWall プライバシー ポリシーは、https://www.mysonicwall.com/privacypolicy.aspx で参照できます。

キャプチャ ATP によるわかりやすいファイル名表示

次の非 HTTP プロトコルに対し、SonicWall Capture Advanced Threat Protection が、スキャン済みファイルをわかりやすいファイル名でログに記録します。

- SMTP
- POP3
- FTP
- IMAP
- NetBIOS:

この機能を使用すると、キャプチャ ATP によってスキャンされているファイルとその状況 (「**監視 | イベント サマリ > キャプチャ ATP | 状況**」テーブルやログ メッセージにおいて、これらのプロトコル種別のファイル名について表示される) を簡単に識別できます。わかりやすいファイル名には、最大 256 文字を使用できます。

次の要素は解析できません:

- TCP プロトコル ストリームのファイル名情報。
- 単一のネットワーク パケットに含まれていないファイル名。

SonicOS の設定は不要です。

キャプチャ ATP ライセンスの有効化

重要：キャプチャ ATP の実行にはゲートウェイ アンチウイルス サービスが必要です。このサービスもライセンスが有効になっている必要があります。

キャプチャ ATP サービス ライセンスを有効化すると、SonicOS の左側にあるナビゲーション パネル (左側のナビゲーション パネル) の DPI-SSL の下に**キャプチャ ATP** が表示されます。キャプチャ ATP のライセンスが取得されていない場合は、左側のナビゲーション パネルに表示されません。

メモ：キャプチャ ATP サービス ライセンスをアクティブ化してから間もなく**キャプチャ ATP** が表示されない場合は、「**管理 | 更新 > ライセンス**」ページの「**同期**」ボタンを選択してください。

ライセンスを有効化するには、すべてのサービス ライセンスを表示できる「**更新 > ライセンス**」ページに移動し、キャプチャ ATP のライセンスを初期化します。ライセンスの詳細については、『*SonicWall SonicOS 6.5 更新*』を参照してください。

キャプチャ ATP の有効化

重要： キャプチャ ATP を有効化する前に、ゲートウェイ アンチウイルスとクラウド アンチウイルスを有効にしてください。

キャプチャ ATP のライセンスは取得済みでもまだサービスを有効化していない場合は、次のメッセージが表示されます。

> キャプチャ ATP は現在動作していません。トラブルシュートは以下の「基本セットアップ確認リスト」をご覧ください。

無効モードでは「**基本セットアップ確認リスト**」セクションは表示されますが、他のセクションはグレー表示になります。

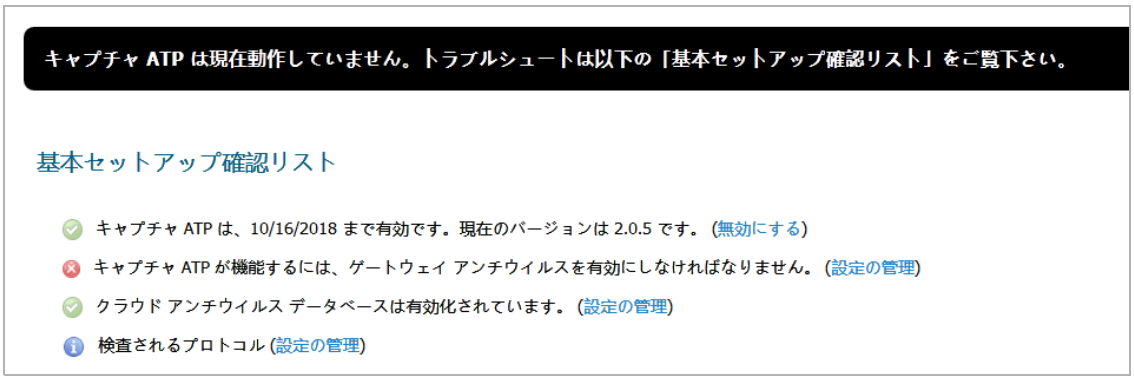
キャプチャ ATP を有効化するには:

1 「**管理 | セキュリティ設定 > セキュリティ サービス > ゲートウェイ アンチウイルス**」に移動します。

2 SonicWall ゲートウェイ アンチウイルス サービスの管理 (162 ページ) の説明に従って、ゲートウェイ アンチウイルス (GAV) とクラウド アンチウイルスを有効化します。

3 また、GAV またはクラウド アンチウイルスを設定することもできます。この設定は、キャプチャ ATP にも適用されます。

4 「**管理 | セキュリティ設定 > セキュリティ サービス > キャプチャ ATP**」に移動します。キャプチャ ATPが有効になっていないと、次の警告メッセージが表示されます。



5 「**基本セットアップ確認リスト**」セクションの「**キャプチャ ATP 購読は *<日付>* まで有効です。ただしサービスは現在有効化されていません。(有効にする)**」で「**(有効にする)**」をクリックします。警告メッセージが消え、ステータス インジケータが緑色のチェックマークに変わります。

「セキュリティ サービス > キャプチャ ATP」ページについて

トピック:

- 基本セットアップ確認リスト
- 帯域幅管理

- 除外
- ユーザ定義の遮断動作

基本セットアップ確認リスト

基本セットアップ確認リスト:

- キャプチャ ATP および関連コンポーネント、GAV、およびクラウド アンチウイルスのステータスを表示します。
- エラーが発生していれば、その状態が表示されます。
- キャプチャ ATP サービスを有効または無効に設定できます。
- GAV、クラウド アンチウイルス、およびプロトコル検査を設定できる「**管理 | セキュリティ設定 > セキュリティ サービス > ゲートウェイ アンチウイルス**」ページへのリンクがあります。
- プロトコル検査の設定と、受信方向と送信方向のどちらが有効化されているかが表形式で表示されます。

メモ：このセクションで表示されるメッセージについては、キャプチャ ATP の状況 テーブル から プロトコル検査設定 テーブル までを参照してください。緑色のチェックマークは**有効**を意味し、赤い X マークは**無効**を意味します。

キャプチャ ATP の状況

アイコン	メッセージ	リンク	動作
有効	キャプチャ ATP サービスは、*更新日*まで有効です。	無効にする	このリンクをクリックすると、キャプチャ ATP がオフに切り替わり、サービスが無効モードになります。この変更を適用するために「**適用**」をクリックする必要はありません。
無効	キャプチャ ATP の購読は*更新日*まで有効ですが、サービスは現在有効ではありません。	有効にする	このリンクをクリックすると、キャプチャ ATP がオンに切り替わり、サービスが有効モードになります。この変更を適用するために「**適用**」をクリックする必要はありません。
無効	キャプチャ ATP の購読は、*更新日* に期限切れで終了しました。	更新する	このリンクをクリックすると、MySonicWall に移動してサービスを更新できます。

ゲートウェイ アンチウイルス状況

アイコン	メッセージ	リンク	動作
有効	ゲートウェイ アンチウイルスは有効化されています。	設定の管理	このリンクを選択すると、「**セキュリティ サービス > ゲートウェイ アンチウイルス**」ページが表示されます。
無効	キャプチャ ATP が機能するには、ゲートウェイ アンチウイルスを有効にしなければなりません。	設定の管理	このリンクを選択すると、「**セキュリティ サービス > ゲートウェイ アンチウイルス**」ページが表示されます。

クラウド アンチウイルス データベース状況

アイコン	メッセージ	リンク	動作
有効	クラウド アンチウイルス データベースは有効化されています。	設定の管理	このリンクを選択すると、「**セキュリティ サービス > ゲートウェイ アンチウイルス**」ページが表示されます。
無効	キャプチャ ATP が機能するには、クラウド アンチウイルス データベースを有効にしなければなりません。	設定の管理	このリンクを選択すると、「**セキュリティ サービス > ゲートウェイ アンチウイルス**」ページが表示されます。

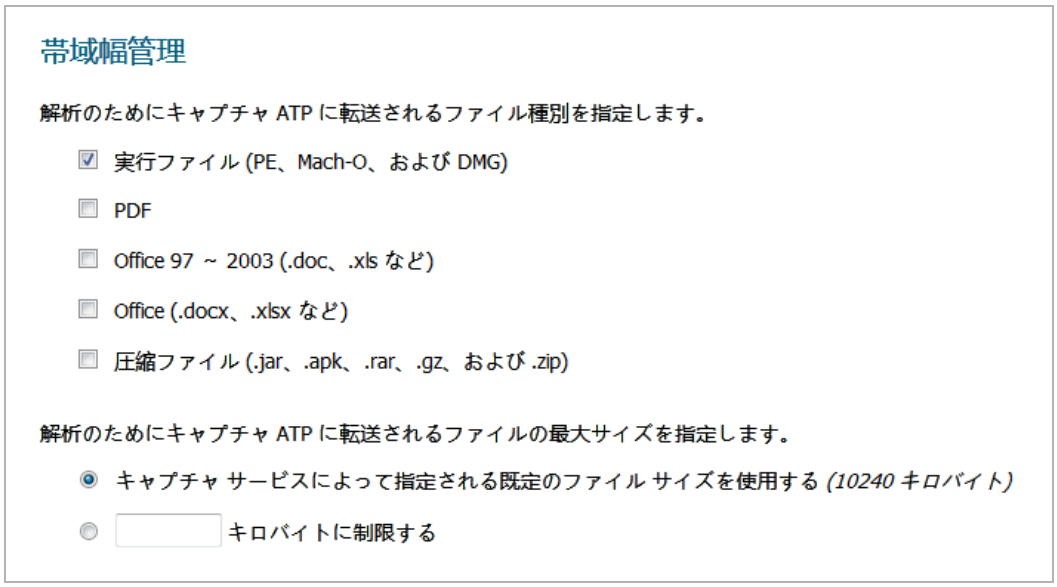
「**検査されるプロトコル**」の表には、「セキュリティ サービス > ゲートウェイ アンチウイルス」ページに移動できる「設定の管理」リンクも提供されています。ここでは、HTTP、FTP、IMAP、SMTP、POP、CIFS、TCP ストリームなどのネットワーク トラフィック プロトコルを指定して、検査を有効または無効に設定できます。各プロトコルは、受信トラフィックまたは送信トラフィックを区別して管理できます。

「**検査されるプロトコル**」の表には、次のように各プロトコルの現在の検査設定が方向別に示されます (プロトコル検査設定を参照)。

プロトコル検査設定

アイコン	メッセージ
有効	プロトコルは検査されます。
無効	プロトコルは検査されません。
該当なし	検査がこのプロトコルのこの方向には適用が不可能であることを意味します。

帯域幅管理



「**帯域幅管理**」セクションでは、キャプチャ ATP に送信できるファイルのタイプを選択し、送信できるファイルの最大サイズを指定することができます。また、検査から除外するアドレス オブジェクトも指定できます。

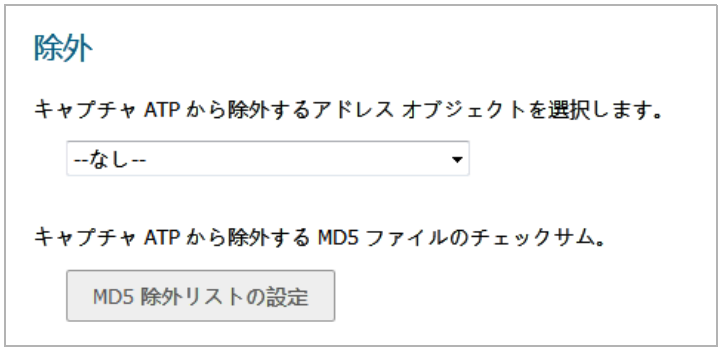
既定では、「**実行ファイル (PE、Mach-O、および DMG)**」ファイル タイプのみが有効です。

最大ファイル サイズの既定のオプションは、「**キャプチャ サービスによって指定される既定のファイル サイズを使用する (10240 キロバイト)**」です。このオプションを選択すると、ファイル サイズは 10 MB に制限されます。

「**キロバイトに制限する**」を選択すると、個別の値を入力できます。この値は、ゼロではなく、なおかつ既定の制限値より大きくない数値でなければなりません。

「**キャプチャ ATP から除外するアドレス オブジェクトを選択します。**」を使用する場合は、ドロップダウン リストからアドレス オブジェクトを選択したり、新しいアドレス オブジェクトを作成することもできます。選択したアドレス オブジェクトのメンバーは、キャプチャ ATP サービスによる検査から除外されます。

除外



「**除外**」セクションでは、キャプチャ ATP からアドレス オブジェクトや MD5 ハッシュ関数を除外することができます。

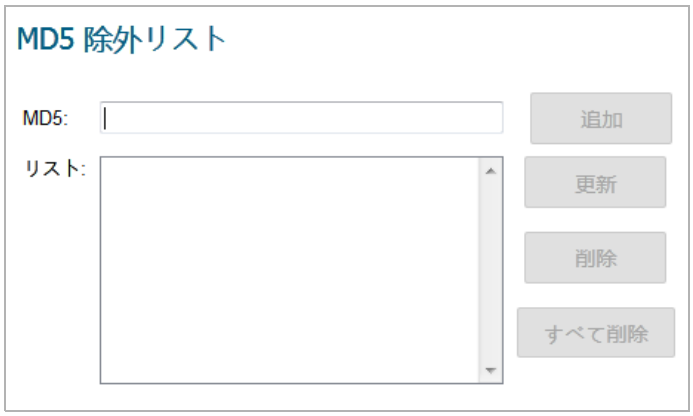
アドレス オブジェクトを除外するには:

1 アドレス オブジェクトをドロップダウン メニューから選択するか、新しく作成します。

2 「**適用**」を選択します。

MD5 ファイルを除外するには:

1 「**MD5 除外リストの設定**」ボタンを選択します。「**MD5 除外リスト**」ダイアログが表示されます。



2 除外する 16 進数 32 桁のハッシュ関数を追加します。

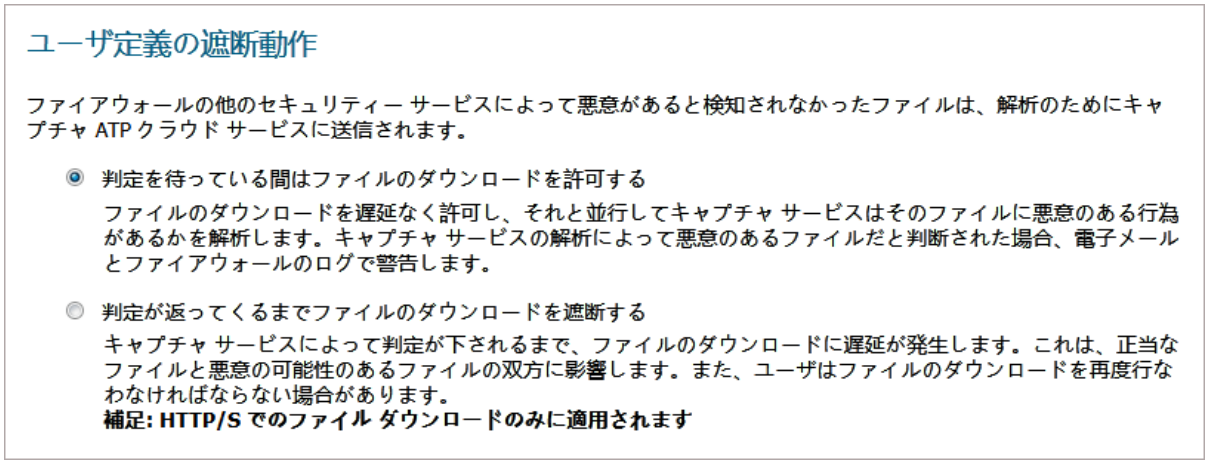
3 「**追加**」を選択します。

4 複数のファイルを追加するには、ハッシュ関数ごとにステップ 2 とステップ 3 を繰り返します。

5 「**OK**」を選択します。

6 「**適用**」を選択します。

ユーザ定義の遮断動作

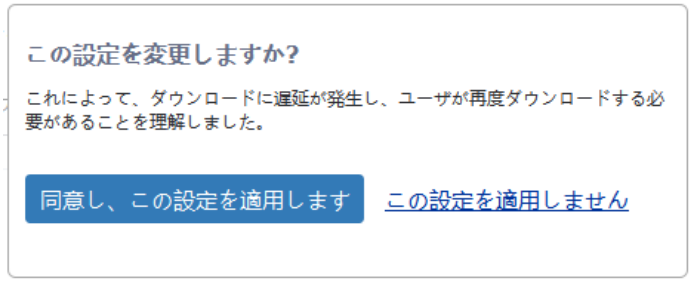


「**ユーザ定義の遮断動作**」セクションでは、「**判定が返ってくるまでファイルのダウンロードを遮断する**」機能を選択できます。

既定のオプションは、「**判定を待っている間はファイルのダウンロードを許可する**」です。この設定を使うと、キャプチャ サービスがファイルの有害要素を分析している間も、ファイルのダウンロードは遅延なく許可されます。キャプチャ サービスの分析でファイルが有害と判定されたかどうか

は、電子メールのアラートで通知するように設定したり、ファイアウォールのログをチェックして確認することができます。

「判定が返ってくるまでファイルのダウンロードを遮断する」機能は、厳格な制御が望ましい状況でのみ使用してください。この機能をオンにすると、警告のダイアログが表示されます。



「判定が返ってくるまでファイルのダウンロードを遮断する」機能が有効になると、他のオプションが使用可能になります。次の方法を選択できます。

- **「キャプチャ サービスから判定が返ってくるまでファイルのダウンロードが遮断されないよう除外するアドレス オブジェクトを選択する」**から、アドレス オブジェクトを選択します。既定は**「なし」**です。
- **「キャプチャ サービスから判定が返ってくるまでファイルのダウンロードが遮断されないよう除外するファイル種別を指定する」**から 1 つ以上のファイル種別を選択します。
  - **実行ファイル (PE、Mach-O、および DMG)**
  - **PDF**
  - **Office 97-2003 (.doc、.xls など)**
  - **Office (.docx、.xlsx など)**
  - **圧縮ファイル (.jar、.apk、.rar、.gz、および .zip)**

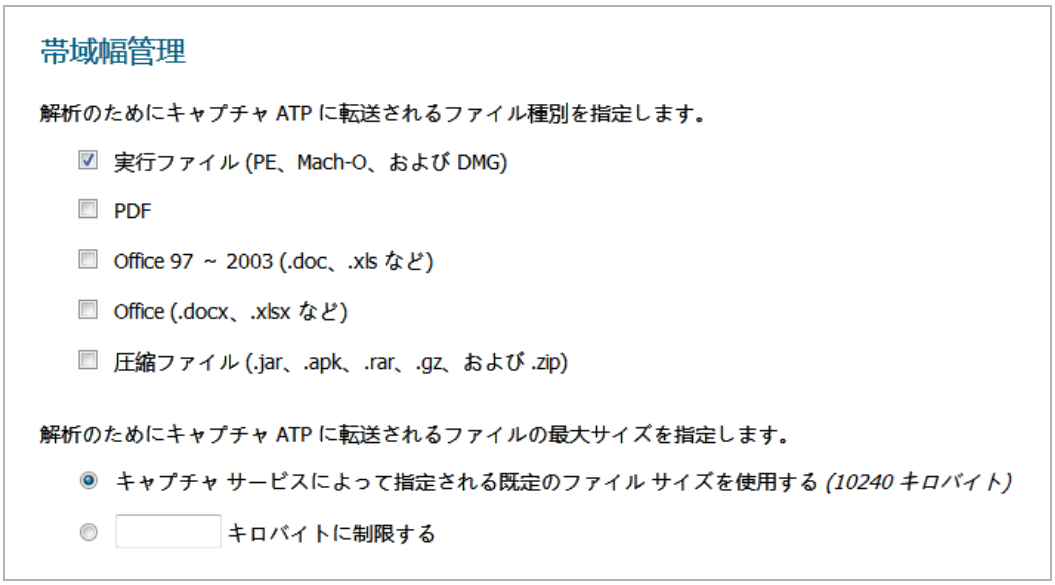
キャプチャ ATP の設定

キャプチャ ATP を設定するには:

1 **「キャプチャ ATP > 設定」**に移動します。

2 キャプチャ ATP、GAV、クラウド アンチウイルス データベース、関連するプロトコルが有効化されていることを確認します。

3 「**帯域幅管理**」セクションで、キャプチャ ATP の分析対象とするファイル タイプを選択します。既定では、「**実行ファイル (PE、Mach-O、および DMG)**」のみが有効です。



4 規定では、「**キャプチャ サービスによって指定される既定のファイル サイズを使用する**」 ***(10240 キロバイト)*** が選択されています。このサイズを変更するには、「**キロバイトに制限する**」フィールドに 1 から 10240 までの値を入力します。

5 必要に応じて、「**キャプチャ ATP から除外するアドレス オブジェクトを選択します。**」ドロップダウン メニューからアドレス オブジェクトを選択してキャプチャ ATP からアドレス オブジェクトを除外することもできます。

6 必要に応じて、「**MD5 除外リストの設定**」ボタンを選択して「**MD5 除外リスト**」ダイアログを表示し、MD5 チェックサムに基づいてファイルを除外することもできます。

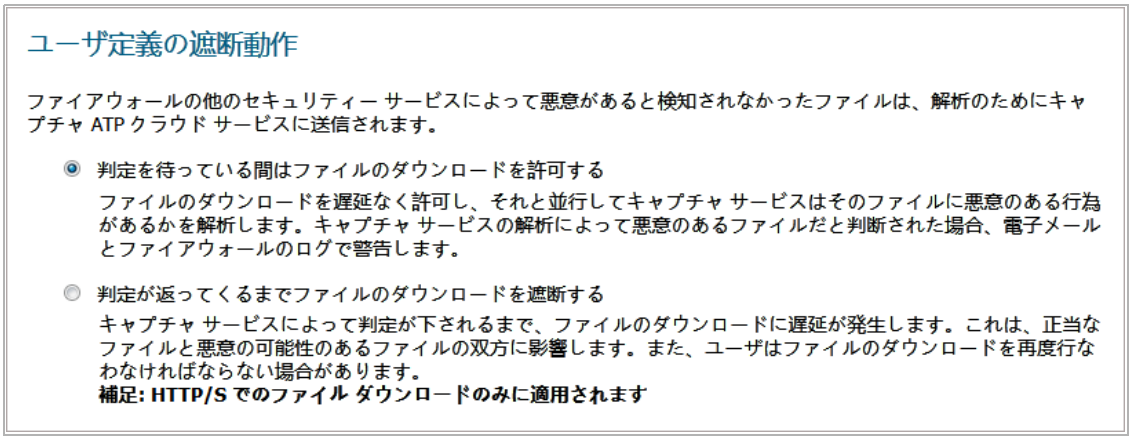
   a 「**MD5**」フィールドに 16 進数 32 桁のハッシュを追加します。

   b 「**追加**」を選択します。

   c 除外するファイルごとにステップ a とステップ b を繰り返します。

   d 「**OK**」を選択します。

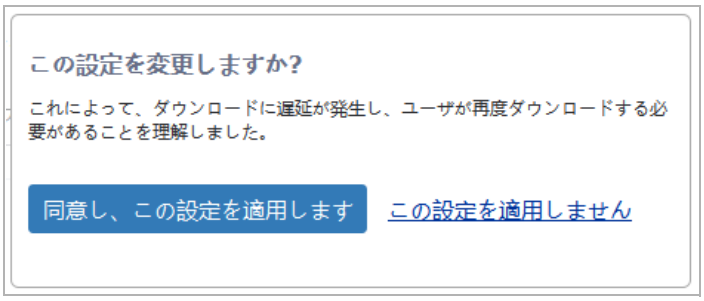
7 HTTP/HTTPS ファイルを分析する場合は、「**ユーザ定義の遮断動作**」セクションで、分析が完了するまですべてのファイルを遮断するかどうかを指定できます。



既定では、「**判定を待っている間はファイルのダウンロードを許可する**」が選択されます。

重要：「**判定が返ってくるまでファイルのダウンロードを遮断する**」機能は、厳格な制御が望ましい状況でのみ使用してください。

この機能をオンにすると、警告のダイアログが表示されます。



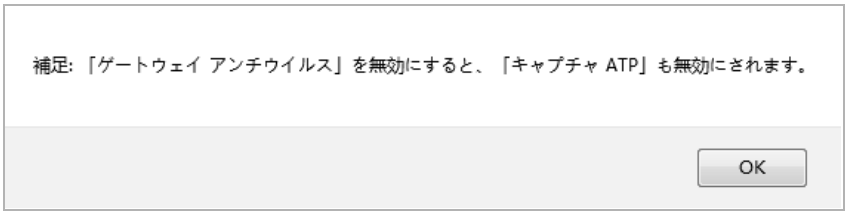
次のオプションがあります。

- 「**同意し、この設定を適用します**」ボタンをクリックすると、「**判定が返ってくるまでファイルのダウンロードを遮断する**」オプションが有効になります。変更を反映するには、「**適用**」ボタンを選択する必要もあります。
- 「この設定を**適用しません**」リンクを選択すると、ダイアログが閉じられ、「**判定を待っている間はファイルのダウンロードを許可する**」はオンの状態にとどります。

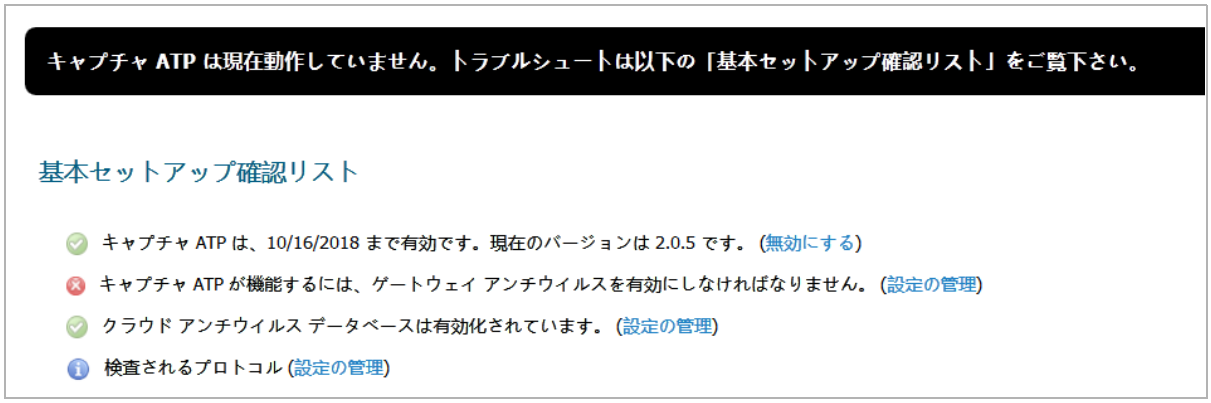
8 「**適用**」を選択します。

GAV またはクラウド アンチウイルスの無効化

「**セキュリティ設定 | セキュリティ サービス > ゲートウェイ アンチウイルス**」ページでゲートウェイ アンチウイルスまたはクラウド アンチウイルス サービスのチェックボックスをオフにすると、各サービスを無効にすることができます。キャプチャ ATP が有効なときにどちらかのサービスを無効にすると、キャプチャ ATP も無効になることを警告するメッセージがポップアップで表示されます。



キャプチャ ATP は、ゲートウェイ アンチウイルスまたはクラウド アンチウイルスが無効になると、機能を停止します。例えば、ゲートウェイ アンチウイルスが有効ではないと、「**キャプチャ ATP > 設定**」ページに「**キャプチャ ATP が機能するには、ゲートウェイ アンチウイルスを有効にしなければなりません。**」というメッセージと「設定の管理」リンクが表示されます。このリンクを選択すると、「**セキュリティ サービス > ゲートウェイ アンチウイルス**」ページに移動し、GAV を有効化できます。



16

アンチスパイウェア サービスの有効化

- アンチスパイウェアについて (205 ページ)
- セキュリティ サービス > アンチスパイウェア (206 ページ)
- アンチスパイウェア ポリシーの設定 (211 ページ)

アンチスパイウェアについて

SonicWall ゲートウェイ アンチウイルス、アンチスパイウェア、および侵入防御サービス ソリューションは、ウイルス、ワーム、トロイの木馬、スパイウェア、およびソフトウェア脆弱性に対する総合的なリアルタイム防御を提供するソリューションであり、SonicWall アンチスパイウェアはその一部を成しています。

SonicWall アンチスパイウェア サービスは、スパイウェアのインストールおよび配信をゲートウェイで遮断するとともに、以前にインストールされていたスパイウェアが収集した情報を外部に伝達してしまうのを拒絶することによって、侵害的なスパイウェアからネットワークを防御します。SonicWall アンチスパイウェアは、他のアンチスパイウェア プログラム (例えば、既存のスパイウェア アプリケーションをホストから除去するプログラムなど) と連携して動作します。スパイウェアに対する防御手段を補足するために、ホストベースのアンチスパイウェア ソフトウェアの使用あるいはインストールを推奨します。

SonicWall アンチスパイウェアは、ActiveX ベースのコンポーネントのインストール場所 (すなわち、スパイウェア配信先として最も一般的な場所) での着信接続を分析します。また、ゲートウェイをまたいで着信したセットアップ実行ファイルおよびキャビネット ファイルを検査して、スパイウェア セットアップ ファイルを LAN に流出させている接続をリセットします。スパイウェア (アドウェアやキーロガーなど) にバンドルされたフリーウェアなども、検査対象となるファイル パッケージです。

アンチスパイウェア サービスのインストールよりも先に、LAN ワークステーションにスパイウェアがインストールされていた場合、アンチスパイウェア サービスは発信トラフィックを調べて、スパイウェアに感染しているクライアントで発生したストリームがないかどうか確認し、該当する接続があればリセットします。例えば、スパイウェアがユーザのブラウジング習慣をプロファイリングして、そのプロファイル情報をホームに送信しようとすると、ファイアウォールはトラフィックをつきとめて接続をリセットします。

SonicWall アンチスパイウェア サービスでは、次のような防御が提供されます。

- 悪意あるスパイウェア プログラムを配布する手段として最も頻繁に使用される、ActiveX コンポーネントの自動インストールによるスパイウェアの侵入を防ぎます。
- ネットワーク経由で転送されるスパイウェアの脅威をスキャンしてログに記録し、新しいスパイウェアが検出または阻止された場合、管理者に警告を通知する。
- 既存のスパイウェア プログラムとインターネット上のハッカーやサーバとのバックグラウンド通信を阻止して、機密情報の転送を防ぐ。

- スパイウェア プログラムのインストールを管理者が選択的に許可または拒否できるようにして、ネットワーク アプリケーションをきめ細かく制御できるようにする。
- SMTP、IMAP またはウェブベースの電子メールを介して転送されてきた電子メールをスキャンして感染メールを阻止することによって、電子メールで送信されたスパイウェアの脅威を防ぐ。

セキュリティ サービス > アンチスパイウェア

「**管理 | セキュリティ設定 > セキュリティ サービス > アンチスパイウェア**」ページには、SonicWall セキュリティ装置上のサービスを管理するための構成設定値が表示されます。

「**セキュリティ サービス > アンチスパイウェア**」ページは 3 つのセクションに分かれています。

- **アンチスパイウェア状況** - シグネチャ データベースの状態に関する状況情報、SonicWall アンチスパイウェアのライセンス、およびその他の情報が表示されます。
- **アンチスパイウェア グローバル設定** - SonicWall セキュリティ装置上で SonicWall アンチスパイウェアを有効にするための鍵設定が表示され、攻撃の 3 つのクラスに応じた SonicWall アンチスパイウェアの全体的な保護、およびその他の設定オプションを指定します。
- **アンチスパイウェア ポリシー** - SonicWall アンチスパイウェアのシグネチャを表示し、シグネチャの処理をシグネチャの種別またはシグネチャごとに構成することができます。種別とは製品または製造元に基づいてシグネチャをグループ分けしたものです。

メモ：SonicWall アンチスパイウェアのライセンスを有効化したら、アンチスパイウェアのポリシーがネットワーク トラフィックに適用される前に、SonicWall 管理インターフェース上でアンチスパイウェアを有効にし、構成する必要があります。

トピック:

- アンチスパイウェア状況 (207 ページ)
- アンチスパイウェア グローバル設定 (207 ページ)

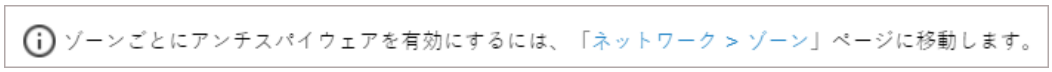
- ゾーンに対するアンチスパイウェア保護の適用 (208 ページ)
- アンチスパイウェア ポリシー (209 ページ)

アンチスパイウェア状況

「**アンチスパイウェア状況**」セクションには、シグネチャ データベースの状態 (例えば、データベースのタイムスタンプ、SonicWall シグネチャ サーバに最新シグネチャがあるかどうかがチェックされた最終日時など) が表示されます。SonicWall セキュリティ装置は、起動時および 1 時間ごとに自動的にデータベースの同期化を試みます。

- **シグネチャ データベース** - シグネチャ データベースが SonicWall セキュリティ装置にダウンロードされていることを示します。
- **シグネチャ データベースのタイムスタンプ** - シグネチャ データベースの最終更新日時を表示します。「**シグネチャ データベースのタイムスタンプ**」に表示される日時は、SonicWall セキュリティ装置ではなく SonicWall アンチスパイウェア シグネチャ データベースが最後に更新された日時です。
- 「**最終確認**」には、SonicWall セキュリティ装置がシグネチャの更新の有無をチェックした最終日時が示されます。
- **アンチスパイウェアの失効期日** - SonicWall アンチスパイウェアのライセンスの失効期日を表示します。SonicWall アンチスパイウェアの購読期限が切れると、SonicWall アンチスパイウェア検査が停止し、SonicWall アンチスパイウェアの構成設定値が SonicWall セキュリティ装置から削除されます。これらの設定は、SonicWall アンチスパイウェア ライセンスを更新すると、自動的に以前の設定状態に復元されます。

次のメモには、個々のゾーンでアンチスパイウェアを設定できる「**管理 | セキュリティ設定 > ネットワーク > ゾーン**」ページへのリンクが含まれています。



アンチスパイウェア グローバル設定

「**アンチスパイウェア グローバル設定**」パネルでは、次の攻撃レベルに基づいて、攻撃をグローバルに防御および検知できます。

- **高危険度のスパイウェア** - これらのスパイウェア アプリケーションは、キーロガーやポルノ ダイヤラーなどネットワークに対して最も危険なものであるか、または、セキュリティ脆弱性を含む可能性があります。削除は極めて困難か、不可能である可能性があります。
- **中危険度のスパイウェア** - これらのスパイウェア アプリケーションは、ネットワーク トラフィックの増加やパフォーマンスの低下など、ネットワークの中断を引き起こす可能性があります。削除は極めて困難である可能性があります。
- **低危険度のスパイウェア** - これらのスパイウェア アプリケーションは、侵害性の低いアクティビティで特徴付けられ、緊急の脅威ではありません。ユーザをプロファイリングする可能性がありますが、通常は簡単に削除できます。

ヒント：SonicWall では、「**高危険度のスパイウェア**」と「**中危険度のスパイウェア**」に対して「**すべて防御**」を有効にし、最も有害なスパイウェアからネットワークを保護することを推奨します。

アンチスパイウェア保護では、グローバルなスパイウェア脅威を管理するための 2 つの方法を提供します (「**すべて検知**」と「**すべて防御**」)。「シグネチャ グループ」パネルで「**すべて防御**」アクションを指定して、SonicWall セキュリティ装置においてアンチスパイウェアがグローバル レベルで発生するようにする必要があります。

「**シグネチャ グループ**」パネルで、シグネチャ グループに対して「**すべて防御**」を有効にすると、SonicWall セキュリティ装置は、接続を自動的に破棄およびリセットして、トラフィックが送信先に到達するのを防ぎます。

「**シグネチャ グループ**」パネルで、シグネチャ グループに対して「**すべて検知**」を有効にすると、SonicWall セキュリティ装置は、そのグループの任意のシグネチャに一致するすべてのトラフィックをログに記録し、警告を発しますが、トラフィックに対しては何の処置も講じません。トラフィックは、目的とする送信先に到達します。SonicWall ログは、「**ログ > 表示**」ページに表示されます。SonicWall セキュリティ装置による警告の処理方法は、「**ログ > 自動化**」ページで設定します。

△ **注意：「すべて検知」のみを選択する場合は、注意が必要です。「すべて検知」のみを選択すると、そのグループの任意のシグネチャに一致するトラフィックについてログが記録され、警告が送信されますが、トラフィックに対しては何の処置も講じられません。トラフィックは、目的とする送信先に到達します。**

「**シグネチャ グループ**」パネルで、シグネチャ グループに対して「**すべて検知**」と「**すべて防御**」の両方を有効にすると、SonicOS は、そのグループの任意のシグネチャに一致するトラフィックについてログを記録し、警告を送信するとともに、接続を自動的に破棄およびリセットして、トラフィックが送信先に到達するのを防ぎます。

送信スパイウェア通信の検査の有効化

スパイウェア通信の送信トラフィックをスキャンするための、「**送信スパイウェア通信の検査を有効にする**」オプションが提供されています。

ゾーンに対するアンチスパイウェア保護の適用

ファイアウォールで SonicOS が稼動している場合は、「**ネットワーク > ゾーン**」ページで SonicWall アンチスパイウェアをゾーンに適用すると、アンチスパイウェアを各ネットワーク ゾーンと WAN の間だけでなく内部ゾーン間にも適用できます。例えば、LAN ゾーン上でアンチスパイウェアを有効にすると、すべての送受信 LAN トラフィックに対してアンチスパイウェアを適用することができます。

「**セキュリティ サービス > アンチスパイウェア**」ページの上部にある、**ネットワーク > ゾーン** リンクをクリックして、「**管理 | システム セットアップ > ネットワーク > ゾーン**」ページにアクセスします。「**ネットワーク > ゾーン**」ページにリストされているゾーンの 1 つにアンチスパイウェアを適用します。

ゾーンに対してアンチスパイウェアを有効にするには、以下の手順に従います。

1 ファイアウォール管理インターフェースで、「**管理 | システム セットアップ > ネットワーク > ゾーン**」ページに移動します。（または、「**管理 | セキュリティ設定 > セキュリティ サービス > アンチスパイウェア** 」ページから、**ネットワーク > ゾーン** リンクを選択します。「**管理 | システム セットアップ > ネットワーク > ゾーン**」ページが表示されます。

2 「**ゾーンの設定**」パネルの「**設定**」列で、SonicWall アンチスパイウェアを適用するゾーンの**編集**アイコンを選択します。「**ゾーンの編集**」ダイアログが表示されます。

3 「**アンチスパイウェアを有効にする**」オプションを選択します。チェックマークが表示されます。SonicWall アンチスパイウェアを無効にするには、このオプションをクリアします。

4 「**OK**」を選択します。

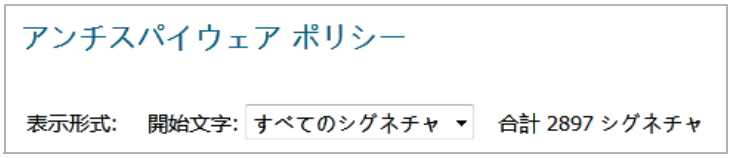
「**管理 | セキュリティ設定 > セキュリティ サービス > アンチスパイウェア**」ページで作成した新規のゾーンに対しても、SonicWall アンチスパイウェア保護を有効にすることができます。「**追加**」アイコンを選択すると、「**ゾーンの追加**」ダイアログ (設定内容は「**ゾーンの編集**」ダイアログと同じ) が表示されます。

アンチスパイウェア ポリシー

「**アンチスパイウェア ポリシー**」セクションでは、SonicWall アンチスパイウェアによるシグネチャの処理方法を、シグネチャの種別またはシグネチャごとに表示および管理することができます。種別とは製品または製造元によってシグネチャをグループ分けしたもので、「**表示形式**」メニューに一覧表示されます。

「**アンチスパイウェア ポリシー**」パネルに一覧表示されるエントリは、SonicWall アンチスパイウェア シグネチャ データベースからファイアウォールにダウンロードされたものです。種別とシグネチャは、アンチスパイウェア サービスによって動的に更新されます。時間の経過に伴い、新しい脅威に対応して種別とシグネチャは動的に変化します。

さまざまなビューで「**表示形式**」メニューを使用して、シグネチャを表示することができます。このメニューでは、「**アンチスパイウェア ポリシー**」パネルに表示する種別またはシグネチャを指定できます。「**すべてのシグネチャ**」を選択するか、または、スパイウェア名の先頭の文字または数字を選択することができます。



メニューから「**すべてのシグネチャ**」を選択すると、すべてのシグネチャが種別ごとに表示されます。「**アンチスパイウェア ポリシー**」パネルには、すべての種別とそのシグネチャが表示されます。種別の見出しによって、シグネチャ エントリが分類されます。これらの見出しでは、「**防御**」と「**検知**」の列に「**グローバル**」と表示され、「**アンチスパイウェア グローバル設定**」セクションで定義したグローバル設定であることが示されます。

トピック:

- 「アンチスパイウェア ポリシー」パネル (210 ページ)
- スパイウェア情報の表示 (210 ページ)
- シグネチャ データベースでの検索 (210 ページ)
- 種別またはシグネチャ エントリの並べ替え (210 ページ)

「アンチスパイウェア ポリシー」パネル

「**アンチスパイウェア ポリシー**」パネルには、各シグネチャ エントリに関する以下の情報が表示されます。

- **製品** - スパイウェア名または製造元を表示します。
- **名前** - スパイウェアの名前をリンクとして表示します。名前リンクを選択すると、スパイウェアに関する SonicAlert 情報が表示されます。
- **ID** - シグネチャの SonicWall データベース ID 番号。
- **防御** - チェック マークがある場合は、防御が有効です。グローバルまたは種別の防御設定から変更を加えると、緑色のチェック マークが「**検知**」列に表示されます。
- **検知** - チェック マークがある場合は、検知が有効です。グローバルまたは種別の検知設定から変更を加えると、緑色のチェック マークが「**検知**」列に表示されます。
- **危険度** -「**シグネチャ グループ**」パネルの定義に基づき、「**低**」、「**中**」、または「**高**」の危険度で攻撃シグネチャを定義します。
- **コメント** - ポリシーに関する簡単な説明を表示します。
- **設定** - 種別見出しの「**設定**」列の編集アイコンを選択すると、「**アンチスパイウェア種別の編集**」ウィンドウが表示されます。個々のシグネチャに対する「**設定**」列の編集アイコンを選択すると、「**アンチスパイウェア シグネチャの編集**」ウィンドウが表示されます。これらのウィンドウでは、特定の種別またはシグネチャに対して、グローバル設定とは異なる処理を定義できます。

スパイウェア情報の表示

「**アンチスパイウェア ポリシー**」パネルで「**名前**」列のスパイウェア名リンクを選択すると、スパイウェアに関する詳細情報を示す「**SonicALERT**」ページが表示されます。

シグネチャ データベースでの検索

シグネチャ データベースの検索を実行するには、「**検索するシグネチャの文字列**」フィールドに検索文字列を入力し、アイコンを選択します。

種別またはシグネチャ エントリの並べ替え

「**アンチスパイウェア ポリシー**」パネルの見出し (「**名前**」、「**ID**」、「**防御**」、「**検知**」、または「**危険度**」) を選択すると、その見出しに基づいてパネル エントリが並べ替えられます。列見出し名の上向き矢印は、エントリが降順に並んでいることを示します。列見出し名の下向き矢印は、エントリが昇順に並んでいることを示します。

アンチスパイウェア ポリシーの設定

トピック:

- 種別ポリシーの設定 (211 ページ)
- シグネチャ ポリシーの設定 (212 ページ)

種別ポリシーの設定

種別ごとの設定によって、防御と検知のグローバル設定をオーバーライドすることができます。「**高危険度のスパイウェア**」、「**中危険度のスパイウェア**」、「**低危険度のスパイウェア**」を含む、「**すべて防御**」と「**すべて検知**」のグローバル設定は、「**アンチスパイウェア グローバル設定**」セクションで設定します。種別には、「**シグネチャ グループ**」パネルで定義された危険度を任意の組み合わせで含めることができます。

使用可能なシグネチャ種別は、「**アンチスパイウェア ポリシー**」セクションの「**表示形式**」メニューに一覧表示されます。種別ごとに防御および検知動作を設定すると、グローバルな危険度設定 (「低」、「中」、または「高」) にかかわらず、その種別のすべてのシグネチャにそれが適用されます。

トピック:

- グローバルな防御および検知設定の種別ごとのオーバーライド (211 ページ)
- SonicWall アンチスパイウェア設定を既定に戻す (212 ページ)

グローバルな防御および検知設定の種別ごとのオーバーライド

1. 「**種別**」メニューで、「**すべての種別**」または個々の種別を選択します。
2. 「**すべての種別**」を選択した場合は、変更する種別の「**設定**」列にある**編集**アイコンを選択すると、「**アンチスパイウェア種別の編集**」ダイアログが表示されます。
3. 個々の種別を選択した場合は、「**種別**」メニューの右側にある**編集**アイコンを選択します。「**アンチスパイウェア種別の編集**」ダイアログが表示されます。
4. 「**防御**」に対するグローバル設定を変更する場合は、「**防御**」メニューで「**有効**」または「**無効**」を選択します。
5. 「**検知**」に対するグローバル設定を変更する場合は、「**検知**」メニューで「**有効**」または「**無効**」を選択します。
6. 検知と防御の両方のグローバル設定を変更する場合は、「**検知**」と「**防御**」のメニューで「**有効**」または「**無効**」を選択します。
7. 以下の設定では、この SonicWall アンチスパイウェア種別で包含または除外する、特定のユーザ/グループ、IP アドレス範囲、スケジュール オブジェクトを選択できます。
    - **包含するユーザ/グループ** - この SonicWall アンチスパイウェア種別で包含するユーザ/グループを選択します。既定は「**すべて**」です。
    - **除外するユーザ/グループ** - この SonicWall アンチスパイウェア種別で除外するユーザ/グループを選択します。既定は「**なし**」です。

- **包含する IP アドレス範囲** - この SonicWall アンチスパイウェア種別で包含する IP アドレス範囲を選択します。既定は「**すべて**」です。
- **除外する IP アドレス範囲** - この SonicWall アンチスパイウェア種別で除外する IP アドレス範囲を選択します。既定は「**なし**」です。
- **スケジュール** - この SonicWall アンチスパイウェア種別を有効にするスケジュール時間を選択します。既定は「**常に有効**」です。

8 「ログ冗長フィルタ」設定を既定のグローバル設定から変更する場合は、「**ログ冗長フィルタ (秒)**」の「**種別設定を使用**」チェックボックスをオフにして、時間を秒数で入力します。

9 「**OK**」を選択して変更を保存します。

ヒント：「**種別**」メニューで「**すべてのシグネチャ**」を選択すると、すべての種別とそのシグネチャが「**アンチスパイウェア ポリシー**」パネルに表示され、種別と、種別に含まれるシグネチャの両方が設定できます。

SonicWall アンチスパイウェア設定を既定に戻す

作成したすべてのユーザ定義の種別とシグネチャ設定を削除し、「**すべて防御**」と「**すべて検知**」のグローバル設定と「**ログ冗長フィルタ (秒)**」設定をリセットするには、「**アンチスパイウェア グローバル設定**」セクションの「**アンチスパイウェア設定とポリシーのリセット**」ボタンを選択します。

シグネチャ ポリシーの設定

「**種別**」メニューから「**すべてのシグネチャ**」を選択すると、すべてのシグネチャが種別ごとに表示されます。「**すべてのシグネチャ**」では、アンチスパイウェア データベース内のすべてのシグネチャが表示されます。

その種別に対して、「**すべて防御**」と「**すべて検知**」のグローバル設定が有効である場合は、その種別とそれに含まれるすべてのシグネチャの「**防御**」と「**検知**」の列に、「**グローバル**」と表示されます。

特定のシグネチャ種別を選択すると、その種別のシグネチャが表示されます。

メモ：SonicWall アンチスパイウェアに独自の個別シグネチャをインポートしたり、シグネチャエントリを削除したりすることはできません。

注意：グローバルな「高危険度のスパイウェア」と「中危険度のスパイウェア」のシグネチャ動作をオーバーライドする際には注意が必要です。脆弱性を招く可能性があるためです。変更を加えた後に、既定のグローバルなシグネチャ設定に戻すには、「アンチスパイウェア設定とポリシーのリセット」ボタンを選択して既定の設定を復元します。

トピック:

- グローバルな防御および検知設定の種別ごとのオーバーライド (211 ページ)
- SonicWall アンチスパイウェア設定を既定に戻す (213 ページ)

シグネチャに対する種別ごとの検知および防御設定のオーバーライド

シグネチャに対する種別ごとの検知および防御属性をオーバーライドするには、以下の手順に従います。

1 「**アンチスパイウェア ポリシー**」パネルで、変更するシグネチャを表示します。そのエントリの「**設定**」列にある**編集**アイコンを選択すると、「**アンチスパイウェアの編集**」ダイアログが表示されます。

2 「**防御**」に対する種別設定を変更する場合は、「**防御**」メニューで「**有効**」または「**無効**」を選択します。

3 「**検知**」に対する種別設定を変更する場合は、「**検知**」メニューで「**有効**」または「**無効**」を選択します。

4 検知と防御の両方の種別設定を変更する場合は、「**検知**」と「**防御**」のメニューで「**有効**」または「**無効**」を選択します。

5 以下の設定では、この SonicWall アンチスパイウェア シグネチャで包含または除外する、特定のユーザ/グループ、IP アドレス範囲、スケジュール オブジェクトを選択できます。

- **包含するユーザ/グループ** - この SonicWall アンチスパイウェア シグネチャで包含するユーザ/グループを選択します。既定は「**すべて**」です。
- **除外するユーザ/グループ** - この SonicWall アンチスパイウェア シグネチャで除外するユーザ/グループを選択します。既定は「**なし**」です。
- **包含する IP アドレス範囲** - この SonicWall アンチスパイウェア シグネチャで包含する IP アドレス範囲を選択します。既定は「**すべて**」です。
- **除外する IP アドレス範囲** - この SonicWall アンチスパイウェア シグネチャで除外する IP アドレス範囲を選択します。既定は「**なし**」です。
- **スケジュール** - この SonicWall アンチスパイウェア シグネチャを有効にするスケジュール時間を選択します。既定は「**常に有効**」です。

6 「ログ冗長フィルタ」設定を種別設定から変更する場合は、「**ログ冗長フィルタ (秒)**」の「**種別設定を使用**」チェックボックスをオフにして、時間を秒数で入力します。

7 「**OK**」を選択して変更を保存します。

SonicWall アンチスパイウェア設定を既定に戻す

作成したすべてのユーザ定義の種別とシグネチャ設定を削除し、「**すべて防御**」と「**すべて検知**」のグローバル設定と「**ログ冗長フィルタ (秒)**」設定をリセットするには、「**アンチスパイウェア グローバル設定**」セクションの「**アンチスパイウェア設定とポリシーのリセット**」ボタンを選択します。

17

SonicWall リアルタイム ブラックリストの設定

- セキュリティ サービス > RBL フィルタ (214 ページ)
- リアルタイム ブラックリスト フィルタについて (215 ページ)
- RBL フィルタの設定 (215 ページ)

セキュリティ サービス > RBL フィルタ

リアルタイム ブラックリスト フィルタについて

SMTP リアルタイム ブラックリスト (RBL) は、スパム送信者が使用する SMTP の IP アドレスを公開するためのメカニズムです。こうした情報は数多くの組織によって収集されており、無料の http://www.spamhaus.org や有償の https://10.1.1.10 にアクセスします。

メモ：SMTP RBL はどちらかと言えば強引なスパム フィルタ手法です。スパム アクティビティの報告結果を基に編集されているため、正当なアドレスでも不正なものとして検出されてしまう場合があります。SonicOS に実装されている SMTP RBL フィルタでは、さまざまな微調整のメカニズムを備えることによってフィルタの精度を高めています。

RBL リスト プロバイダは、各自のリストを DNS を使用して公開しています。ブラックリストに登録された IP アドレスは、リスト プロバイダの DNS ドメインのデータベースに格納されており、SMTP サーバの IP アドレスを逆順に表記した値をドメイン名の前に付加することによって参照できます。127.0.0.2 ～ 127.0.0.11 の応答コードは、どのような理由でブラックリストに登録されているのかを示しています。

Blocked Response Codes
127.0.0.2 - Open Relay
127.0.0.3 - Dialup Spam Source
127.0.0.4 - Spam Source
127.0.0.5 - Smart Host
127.0.0.6 - Spamware Site
127.0.0.7 - Bad List Server
127.0.0.8 - Insecure Script
127.0.0.9 - Open Proxy Server

例えば、IP アドレスが 1.2.3.4 である SMTP サーバが、RBL リスト プロバイダ sbl-xbl.spamhaus.org のブラックリストに登録されているとき、DNS クエリとして4.3.2.1.sbl-xbl.spamhaus.org を送信すると、そのサーバがスパムの送信元であることを示す127.0.0.4 という応答が返されるので、その接続は破棄すべきであると判断できます。

メモ：最近のスパムは、そのほとんどがハイジャックされたコンピュータやゾンビ化したコンピュータから (つまり、小さな SMTP サーバを本人に気付かれないようにコンピュータに忍ばせ、それを踏み台として) 送信されていることがわかっています。正当な SMTP サーバとは異なり、これらのゾンビ化したコンピュータがメールの配信に失敗した場合に再試行することはまれです。そのため、一旦 RBL フィルタによって遮断されたスパムについては、それ以降、配信が再試行されることはありません。

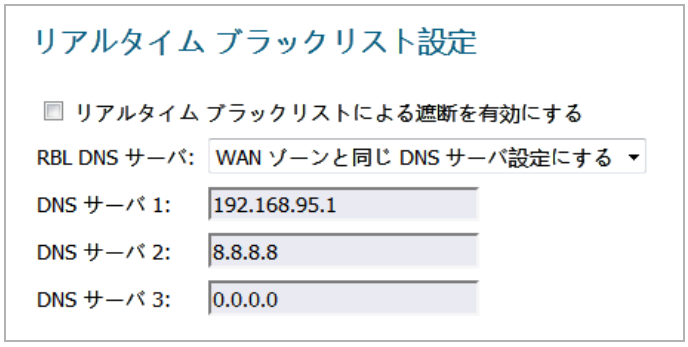
RBL フィルタの設定

トピック:

- RBL 遮断の有効化 (216 ページ)
- RBL サービスの追加 (216 ページ)
- ユーザ定義 SMTP サーバ リストの設定 (217 ページ)
- SMTP IP アドレスのテスト (219 ページ)

RBL 遮断の有効化

「**RBL フィルタ**」ページの「**リアルタイム ブラックリスト設定**」セクションで「**リアルタイム ブラックリストによる遮断を有効にする**」を有効化すると、WAN 側のホストからの着信接続または WAN 側のホストへの発信接続が、有効な各 RBL サービスと照合されます (「**RBL DNS サーバ**」で設定した DNS サーバに DNS 要求が送信される)。



DNS サーバを指定するには「RBL DNS サーバ」メニューを使用します。「**WAN ゾーンと同じ DNSサーバ設定にする**」または「**マニュアルで DNS サーバを指定する**」を選択できます。「**マニュアルで DNS サーバを指定する**」を選択した場合は、「**DNS サーバ**」フィールドに DNS サーバのアドレスを入力してください。

設定が終了したら、「**適用**」を選択します。

DNS の応答は収集されて、キャッシュに格納されます。DNS クエリの応答からブラックリストに登録されていることが判明した場合、そのサーバはフィルタの対象となります。キャッシュに格納される応答の存続時間は TTL 値に基づいており、ブラックリストに登録されていないことが判明した場合は TTL=2 時間でキャッシュされます。キャッシュがいっぱいになった場合、キャッシュ エントリが FIFO (先入れ先出し) 方式で順次破棄されます。

IP アドレスをチェックする際は、このキャッシュに基づいて接続を破棄すべきかどうかが判断されます。初期状態では IP アドレスがキャッシュに存在しないため、最初に DNS 要求を実行する必要があります。有害であることが確認されるまで IP アドレスは無害と仮定されるため、チェックの結果、接続が許可されることになります。DNS 要求を実行すると、独立したタスクとして結果がキャッシュされます。それ以降、同じ IP アドレスからのパケットをチェックするときに、その IP アドレスがブラックリストに登録されていた場合は接続が破棄されるようになります。

RBL サービスの追加

その他の RBL サービスを「**リアルタイム ブラックリスト サービス**」セクションに追加することができます。

RBL サービスを追加するには、「**追加**」ボタンを選択します。「**RBL ドメインの追加**」ダイアログで、問い合わせ先となる RBL ドメインを指定して有効化し、必要な応答コードを指定します。ほとんどの RBL サービスは、提供している応答をウェブ サイトで公開していますが、通常は「**すべての応答を遮断**」を選択して構いません。

「**RBL サービス**」テーブルには RBL サービスごとの統計が記録され、それらはサービス エントリの右に表示される統計アイコンにマウスを重ねることによって参照できます。

ユーザ定義 SMTP サーバ リストの設定

「**ユーザ定義 SMTP サーバリスト**」セクションでは、SMTP サーバのホワイトリスト (明示的許可) とブラックリスト (明示的拒否) をアドレス オブジェクトを使って作成できます。このリストに含まれるエントリについては RBL の問い合わせの手順が省略されます。

メモ：「RBL User White List」または「RBL User Black List」内のエントリを表示するには、リストのチェックボックスの右側にある矢印を選択します。

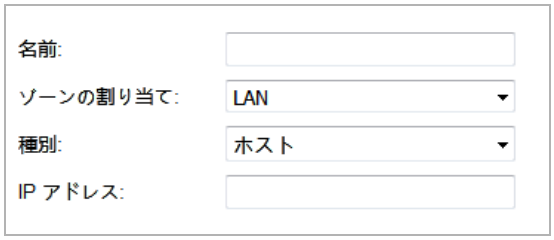
トピック:

- ホワイト リストの設定 (218 ページ)
- ブラック リストの設定 (218 ページ)

ホワイト リストの設定

例えば、パートナー サイトの SMTP サーバからの SMTP 接続を常に受け入れるようにする場合は、次の手順に従います。

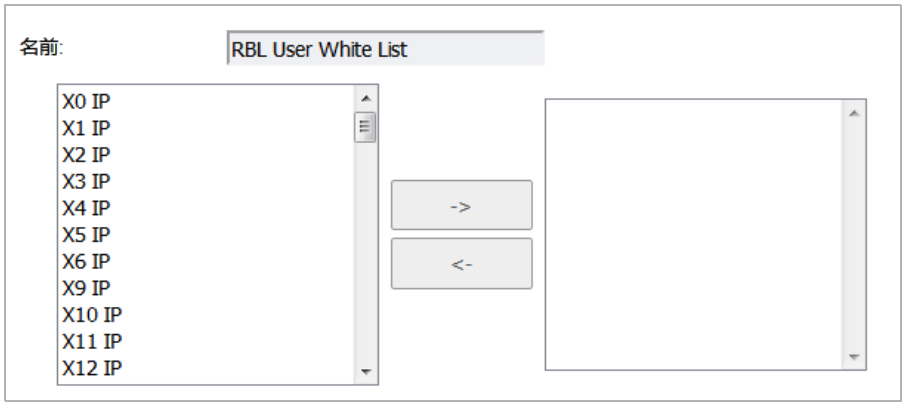
1 サーバのアドレス オブジェクトを作成します。具体的には、「**サーバの追加:**」の「**追加**」ボタン。「**アドレス オブジェクトの追加**」ダイアログが表示されます。



2 アドレス オブジェクトを設定します。

3 「**OK**」を選択します。「**ユーザ定義 SMTP サーバ リスト**」テーブルの「**RBL User White List**」にアドレス オブジェクトが追加されます。

4 「**RBL User White List**」行の「**設定**」列の**編集**アイコンを選択します。「**アドレス オブジェクト グループの編集**」ウィンドウが表示されます。



5 「アドレス オブジェクト」を選択して追加し、右矢印を選択します。

6 「**OK**」を選択します。

これでテーブルが更新され、そのサーバとの SMTP 通信が常に許可されるようになります。

ブラック リストの設定

1 「**RBL User Black List**」行の「**設定**」列の**編集**アイコンを選択します。「**アドレス オブジェクトの編集**」ダイアログが表示されます。

2 「アドレス オブジェクト」を選択して追加し、右矢印を選択します。

3 「**OK**」を選択します。

SMTP IP アドレスのテスト

「**調査 | ツール > システム診断**」ページにも、特定の SMTP の IP アドレス (または RBL サービスや DNS サーバ) をテストできる「**リアルタイム ブラックリスト調査**」という機能が用意されています。このページの詳細については、『*SonicWall SonicOS 6.5 調査*』を参照してください。

テストで使用する既知のスパム送信元のリストについては、以下を参照してください。
http://www.spamhaus.org/sbl/latest/.

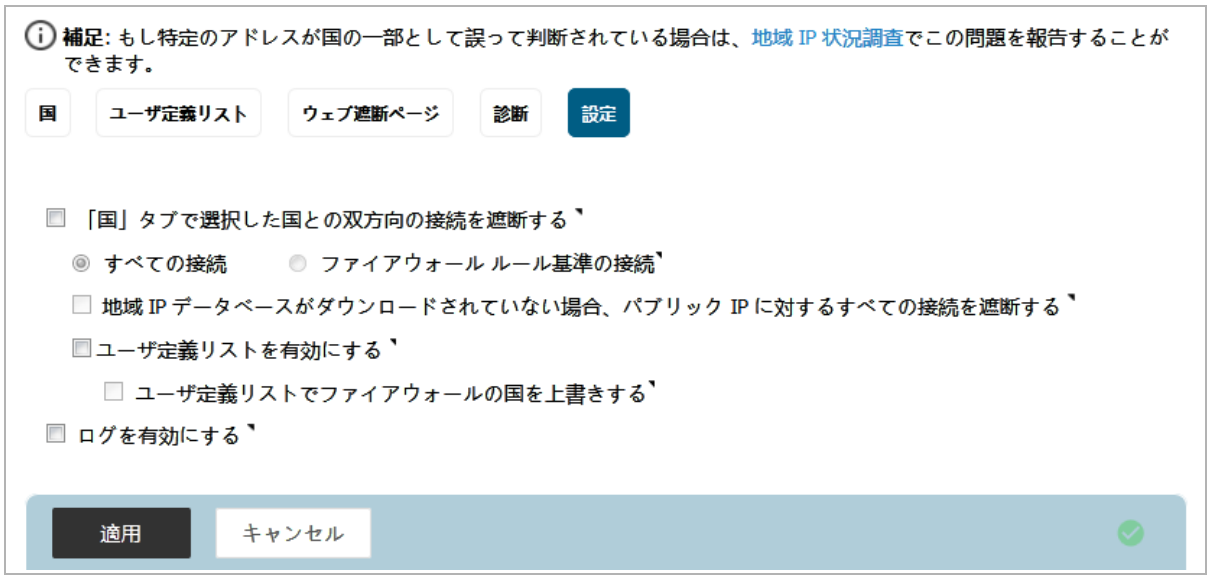
18

地域 IP フィルタの設定

メモ：地域 IP フィルタ機能は、TZ300 シリーズ以上の装置で使用できます。

- セキュリティ サービス > 地域 IP フィルタ
- 地域 IP フィルタの設定
- ユーザ定義国リストの作成
- ウェブ遮断ページの設定のカスタマイズ
- 地域 IP フィルタ診断の使用

セキュリティ サービス > 地域 IP フィルタ



地域 IP フィルタ機能を使用すると、地理的位置に基づいて双方向の接続を遮断することができます。SonicWall ファイアウォールは IP アドレスを使って接続の場所を決定します。また、地域 IP フィルタ機能では、IP アドレスの識別に影響するユーザ定義国リストを作成できます。

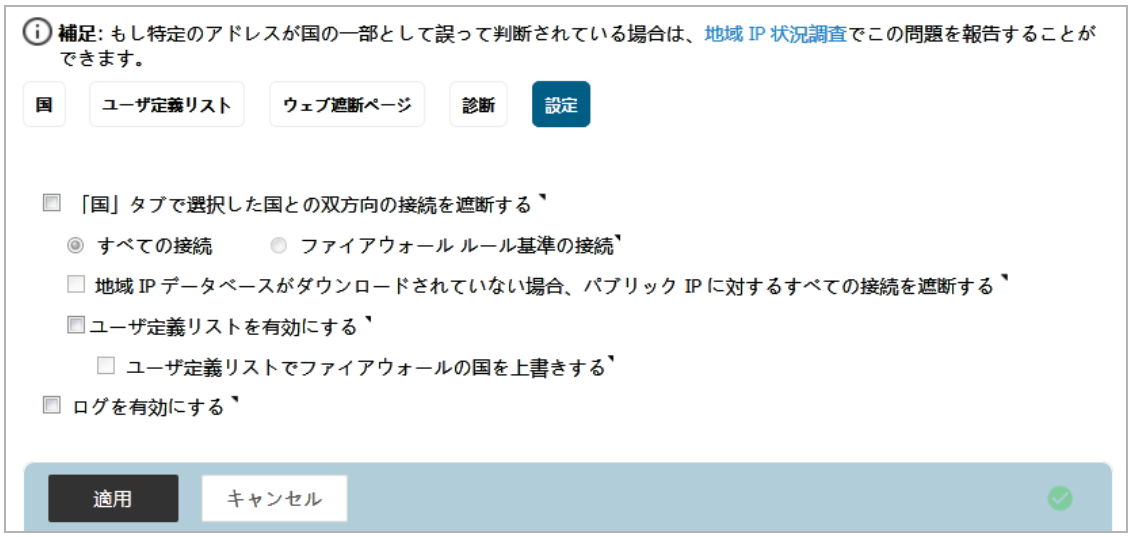
地域 IP フィルタ機能を使用すると、ウェブ サイト遮断時に表示されるユーザ定義メッセージを作成することもできます。

また、地域 IP フィルタ診断ツールを使用すると、解決された場所の表示、地域 IP キャッシュの統計やユーザ定義の国の統計の監視、地域 IP サーバの調査を行うことができます。

地域 IP フィルタの設定

地域 IP フィルタを設定するには、以下の手順に従います。

1 「**管理 | セキュリティ設定 > セキュリティ サービス > 地域 IP フィルタ**」ページに移動します。



2 指定した国との双方向の接続をすべて遮断するために「**「国」タブで選択した国との双方向の接続を遮断する**」チェックボックスをオンにします。このオプションは、既定では選択されています。

このオプションが有効な場合、指定した国に対する双方向の接続がすべて遮断されます。除外リストを指定すれば、選択した IP をこの動作の対象から除外できます (以下のステップ 10 を参照)。

このオプションを選択すると、次の 2 つのオプションが使用できるようになります。

3 地域 IP フィルタの 2 つのモードから、1 つ選択します。

- **すべての接続**: ボットネットサーバとの双方向の接続すべてを遮断します。このオプションは、既定では選択されています。
- **ファイアウォール ルール基準の接続**: ファイアウォールに設定されたアクセス ルールに一致する接続だけを遮断します。

4 地域 IP データベースがダウンロードされていないとき、パブリック IP に対するすべての接続を遮断するには、「**地域 IP データベースがダウンロードされていない場合、パブリック IP に対するすべての接続を遮断する**」オプションを選択します。このオプションは、既定では選択されていません。

5 ユーザ定義リストを有効にするには、「**ユーザ定義リストを有効にする**」チェックボックスをオンにします。このオプションは、既定では選択されていません。

「**ユーザ定義リストを有効にする**」チェックボックスの状況によって次のような違いがあります。

- オフの場合は、ファイアウォールの国データベースのみが検索されます。ステップ 6 へ進みます。
- オンの場合は、「**ユーザ定義リストでファイアウォールの国を上書きする**」チェックボックスが使用可能になります。

「**ユーザ定義リストを有効にする**」チェックボックスをオンにしてユーザ定義リストを有効にすると、IP アドレスに関する国の識別に影響を及ぼす場合があります。「**ユーザ定義リストでファイアウォールの国を上書きする**」の状況によって次のような違いがあります。

- オフの場合、国の識別は次の順序で行われます。
  1) ファイアウォールの国データベースが検索されます。識別が解決されなかった場合は、次の処理が行われます。
  2) ユーザ定義国リストが検索されます。
- オンの場合、国の識別は次の順序で行われます。
  1) ユーザ定義国データベースが検索されます。識別が解決されなかった場合は、次の処理が行われます。
  2) ファイアウォールの国リストが検索されます。

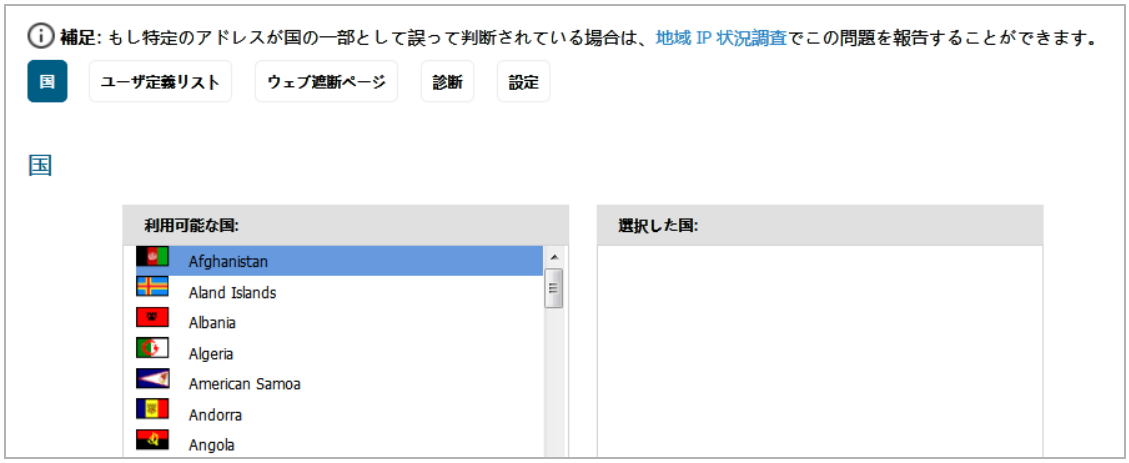
どちらの場合も、解決結果に従った対処が行われます。

6 地域 IP フィルタ関連のイベントをログするために、「**ログを有効にする**」 を選択します。このオプションは、既定では選択されていません。

7 「**国**」の下の「**選択した国**」テーブルで、遮断する国を選択します。既定では、どの国も遮断されません。

8 「**利用可能な国**」テーブルで国を選択し、「**選択した国**」テーブルにドラッグします。

メモ：遮断された国は、「**利用可能な国**」テーブルで選択時に強調表示されます。



9 リストされていない国をともかく遮断する場合は、「**すべての不明な国を遮断する**」オプションを選択します。不明なパブリック IP に対する接続がすべて遮断されます。このオプションは、既定では選択されていません。

10 認可された IP アドレスに対するすべての接続を必要に応じて除外リストとして設定することもできます。次のいずれかの方法で設定します。

- アドレス オブジェクトまたはアドレス グループを「**地域 IP 除外オブジェクト**」ドロップダウン メニューから選択します。既定は「**Default Geo-IP and Botnet Exclusion Group**」です。
- 「**地域 IP 除外オブジェクト**」ドロップダウン メニューから「**アドレス オブジェクトの作成...**」または「**アドレス グループの作成...**」を選択して、新規のアドレス オブジェクトまたはアドレス グループを作成します。

  地域 IP 除外オブジェクトとは、地域 IP フィルタの遮断から除外する、IP アドレスのグループまたは範囲を指定するネットワーク アドレス オブジェクト グループです。このアド

レス オブジェクトまたはグループ内のすべての IP アドレスは、それが遮断対象の国のものであっても許可されます。

例えば、国 A からのすべての IP アドレスを遮断するように設定されており、国 A からの IP アドレスが検出された場合に、このアドレスが「**地域 IP 除外オブジェクト**」リストに含まれていれば、この IP アドレスとの間の双方向のトラフィックの通過が許可されます。

この機能が正しく動作するためには、国データベースがファイアウォールにダウンロードされている必要があります。このダウンロードが失敗している場合は、「**ユーザ定義リスト**」ページの右上にある「**状況**」アイコンが黄色になります。緑色の状況は、データベースが正しくダウンロードされていることを示します。「**状況**」アイコンを選択すると、追加の情報が表示されます。

国データベースをダウンロードするには、ファイアウォールがアドレス `utmgbdata.global.sonicwall.com` を解決できなければなりません。

ユーザが遮断対象の国のウェブ ページへのアクセスを試みると、そのユーザのウェブブラウザ上に遮断ページが表示されます。

メモ：遮断対象の国への接続が一時的で、ファイアウォールがその IP アドレスのキャッシュを持っていない場合は、接続が即時に遮断されないことがあります。結果として、遮断対象の国への接続が時折 AppFlow 監視に現れることがあります。しかしながら、それと同じ IP アドレスへの追加の接続は即時に遮断されます。

11 「**適用**」を選択して変更を有効にします。

ユーザ定義国リストの作成

アドレス オブジェクト	アドレス オブジェクトに与えられた名前。
国	フラグ アイコン (既知の場合) および国の名前。
コメント	アドレス オブジェクトが作成されたときに生成されたコメント。
設定	**編集**アイコンと**削除**アイコンがあります。
合計	**ユーザ定義リスト**内のエントリ数が表示されます。

IP アドレスは誤った国に関連付けられることがあります。こうした分類の誤りがあると、IP アドレスの不適切/不必要なフィルタリングが行われる可能性があります。ユーザ定義国リストがあれば、ファイアウォールで特定の IP アドレスに関連付けられている国よりも優先することで、こうした問題を解決できます。

トピック:

- ユーザ定義リストの作成 (224 ページ)
- ユーザ定義リスト エントリの編集 (226 ページ)
- ユーザ定義リストのエントリの削除 (227 ページ)

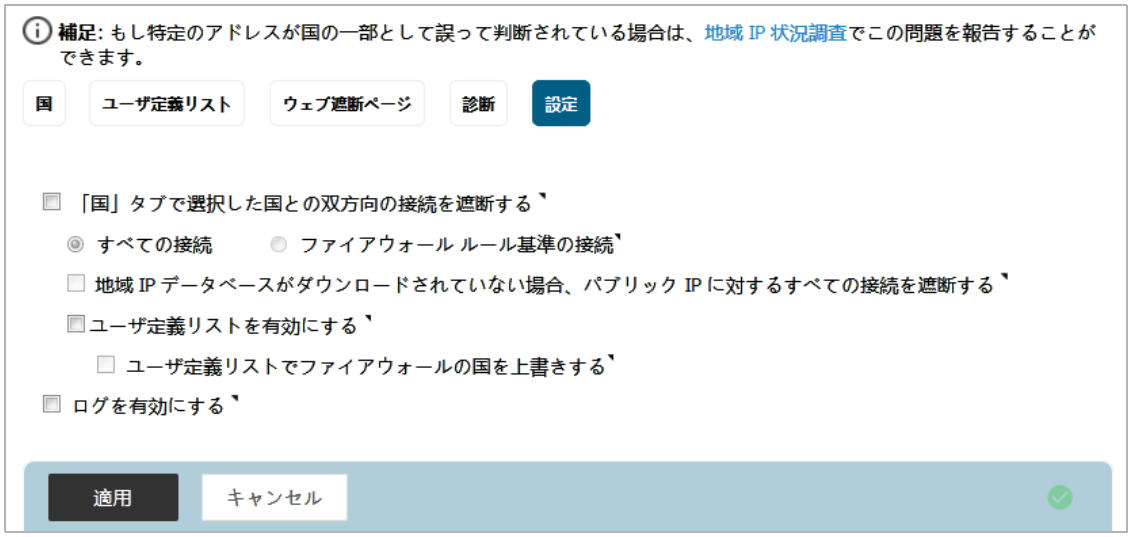
ユーザ定義リストの作成

重要：ファイアウォールでユーザ定義国リストを使用するには、地域 IP フィルタの設定 (221 ページ) の説明に従って、このリストを有効にする必要があります。

ユーザ定義国リストを作成するには、以下の手順に従います。

1 「**管理 | セキュリティ設定 > セキュリティ サービス > 地域 IP フィルタ.**」に移動します。

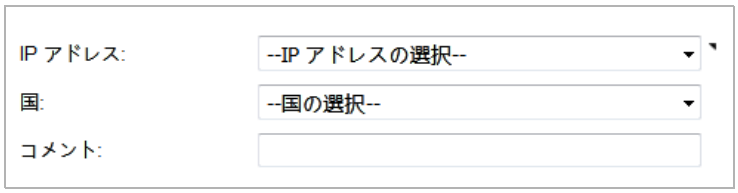
2 「**設定**」を選択します。



3 「**ユーザ定義リストを有効にする**」を選択します。

4 「**ユーザ定義リスト**」を選択します。

5 **追加**アイコンを選択します。「**ユーザ定義リストの追加**」ダイアログが表示されます。



6 「**IP アドレス**」ドロップダウン メニューから、IP アドレス オブジェクトを選択するか、新しいアドレス オブジェクトを作成します。

重要：アドレス オブジェクトは、ユーザ定義国リストにある他のどのアドレス オブジェクトとの重複も許されません。ただし、異なるアドレス オブジェクトに同じ国 ID を持たせることはできます。

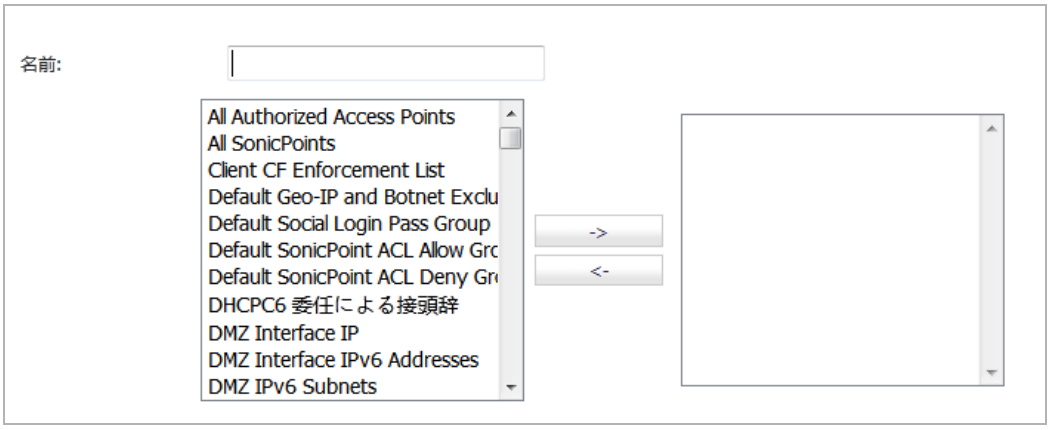
- **アドレス オブジェクトの作成...** - 「**アドレス オブジェクトの追加**」ダイアログが表示されます。

『*SonicWall SonicOS 6.5 ポリシー*』の説明に従って、新しいアドレス オブジェクトを作成します。ただし、次の制限があります。

- 許可されている種別は次のとおりです。
  - **ホスト**
  - **範囲**
  - **ネットワーク**
  - 上記の種別の任意の組み合わせで構成されるグループ

  その他すべての種別は、許可されていない種別であり、ユーザ定義国リストに追加できません。

- **アドレス グループの作成...** - 「**アドレス オブジェクト グループの追加**」ダイアログが表示されます。



*SonicWall SonicOS 6.5 ポリシー*の説明に従って、新しいアドレス オブジェクトを作成します。

- 既に定義されているアドレス オブジェクトまたはアドレス グループ

7 「**国**」ドロップダウン メニューから国を選択します。

8 必要に応じて、「**コメント**」フィールドにコメントを入力します。

9 「**OK**」を選択します。

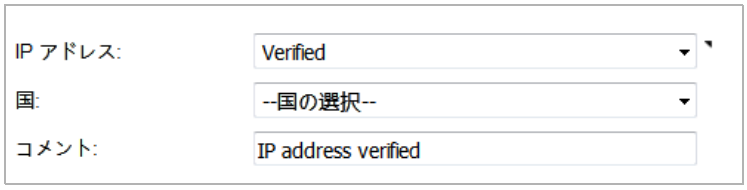
ユーザ定義リスト エントリの編集

ユーザ定義リスト エントリを編集するには、以下の手順に従います。

1 「**管理 | セキュリティ設定 > セキュリティ サービス > 地域 IP フィルタ.**」に移動します。

2 「**ユーザ定義リスト**」を選択します。

3 編集するエントリの「**設定**」列にある「**編集**」アイコンを選択します。「**ユーザ定義リストの追加**」ダイアログが、IP アドレスとそのエントリについてのコメントと共に表示されます。



4 「**国**」ドロップダウン メニューから国を選択し、その他任意の変更を行います。

5 「**OK**」を選択します。「**ユーザ定義リスト**」テーブルが更新されます。

ユーザ定義リストのエントリの削除

ユーザ定義リストのエントリを削除するには、以下の手順に従います。

1 次のいずれかを行います。

- エントリの「**設定**」列にある**削除**アイコンを選択します。
- エントリのチェックボックスをオンにし、「**削除**」ボタンを選択します。

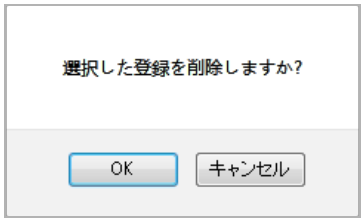
確認メッセージが表示されます。

2 「**OK**」を選択します。

複数のエントリを削除するには、以下の手順に従います。

1 削除するエントリのチェックボックスをオンにします。「**削除**」ボタンが使用可能になります。

2 「**削除**」ボタンを選択します。確認メッセージが表示されます。

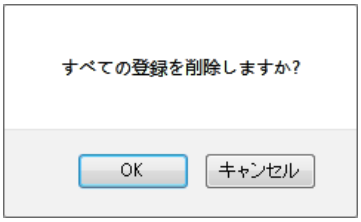


3 「**OK**」を選択します。

すべてのエントリを削除するには、以下の手順に従います。

1 テーブル見出しにある該当するチェックボックスをオンにします。

2 「**削除**」ボタンを選択します。確認メッセージが表示されます。



3 「**OK**」を選択します。

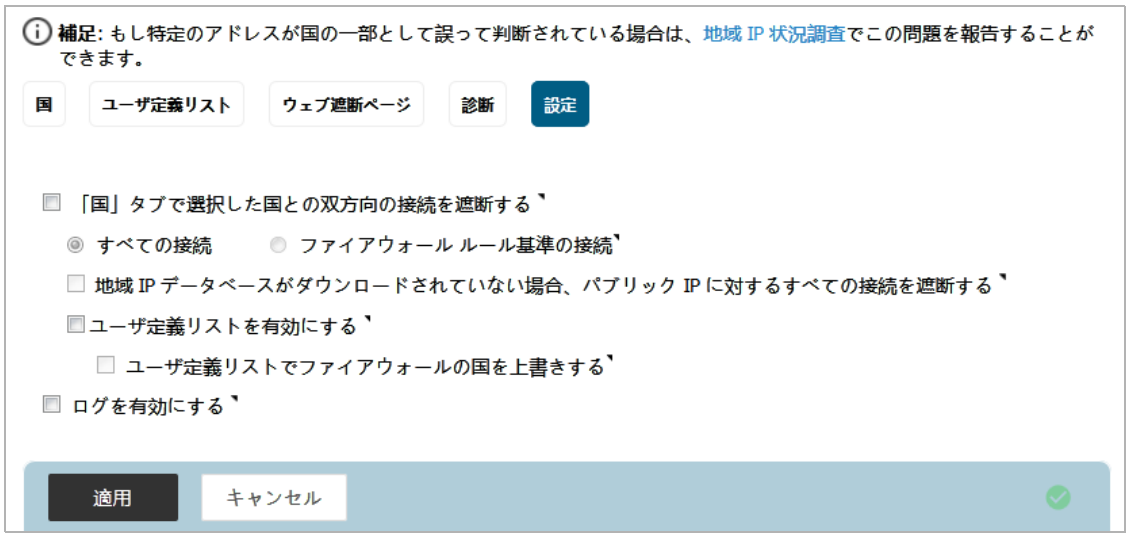
ウェブ遮断ページの設定のカスタマイズ

地域 IP フィルタには、遮断されたページにユーザがアクセスしようとしたときに表示される既定のメッセージがあります。IP アドレスとそれが検出された国、IP アドレスの遮断理由などの詳細な情報を、このメッセージで表示できます。ユーザ定義メッセージを作成してユーザ定義ロゴを含めることもできます。

ユーザ定義ウェブ遮断メッセージを作成するには、以下の手順に従います。

1 「**管理 | セキュリティ設定 > セキュリティ サービス > 地域 IP フィルタ**」に移動します。

2 「**設定**」を選択します。



3 「**ウェブ遮断ページ**」を選択します。

4 「**地域 IP フィルタ遮断の詳細を含める**」オプションを選択します。このオプションを有効にすると、遮断理由、IP アドレス、国などの、遮断の詳細が表示されます。無効にすると、情報は表示されません。既定では、このオプションは選択されています。このオプションは、既定では選択されています。

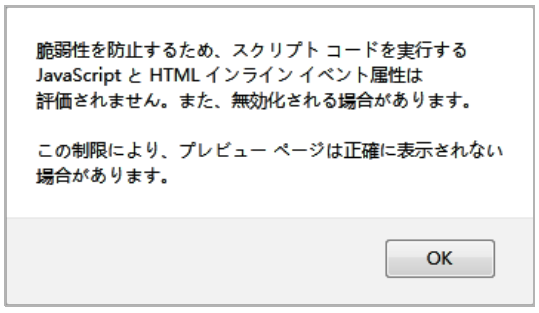
5 以下のいずれかを実行します。

- 「**警告文**」フィールドに表示されている既定のメッセージ、「このサイトはネットワーク管理者によって遮断されています。」を使用する場合は、「**既定の遮断ページ**」ボタンを選択し、ステップ 7 に進みます。
- 地域 IP フィルタ遮断ページに表示するカスタム メッセージを「**警告文**」フィールドで指定します。指定できるメッセージは最大 100 文字です。

6 必要に応じて、「**Base64 でエンコードされたロゴ アイコン**」フィールドで、Base 64 エンコード GIF アイコンを既定の SonicWall ロゴの代わりに表示するように指定できます。

メモ：有効なアイコン画像を使用し、サイズをできるだけ小さくしてください。推奨サイズは 400 x 65 です。

7 カスタマイズしたメッセージとロゴ (または既定のメッセージとロゴ) のプレビューを表示するには、「**プレビュー**」ボタンを選択します。警告メッセージが表示されます。



8 「**OK**」を選択します。「**ウェブ サイトが遮断されました**」というメッセージが表示されます。

9 「**ウェブ サイトが遮断されました**」というメッセージを閉じます。

10 「**適用**」を選択します。

地域 IP フィルタ診断の使用

「**セキュリティ サービス > 地域 IP フィルタ**」ページの「**診断**」ビューには、いくつかのツールが用意されています。

- 解決された位置の表示 (231 ページ)
- 地域 IP キャッシュ統計 (231 ページ)
- ユーザ定義の国の統計 (232 ページ)
- 地域ロケーション サーバ調査を確認する (232 ページ)
- アドレスの指定に誤りがある場合 (233 ページ)

解決された位置の表示

「**解決された位置の表示**」ボタンを選択すると、解決された IP アドレスに関するポップアップ テーブルに次の情報が表示されます。

- **インデックス**
- **IP アドレス**
- **国**

地域 IP キャッシュ統計

「**地域 IP キャッシュ統計**」テーブルには次の情報が含まれます。

- **ロケーション サーバ IP**
- **解決された登録数**
- **解決されなかった登録数**
- **現在の登録数**
- **最大登録数**
- **ロケーション マップ数**

ユーザ定義の国の統計

「**ユーザ定義の国の統計**」テーブルには、リスト内のエントリ数やエントリの検索回数に関する情報が含まれています。

- **登録数**
- **コール回数**
- **検索失敗回数**
- **解決回数**

地域ロケーション サーバ調査を確認する

地域 IP フィルタには、以下の確認のために IP アドレスを調査する機能もあります。

- ドメイン名または IP アドレス
- 発信国と、それがボットネット サーバとして分類されているかどうか

メモ：同様のボットネット ロケーション サーバ調査ツールを「**管理 | セキュリティ設定 > システム サービス > ボットネット フィルタ**」ページから利用することもできます。

この地域ロケーションとボットネット サーバ調査ツールは、「**調査 | ツール > システム診断**」ページからもアクセスできます。

地域サーバを調査するには、以下の手順に従います。

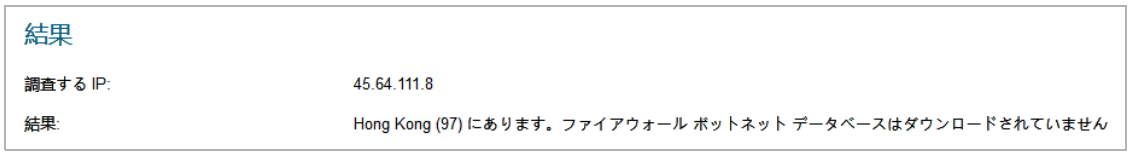
1 「**管理 | セキュリティ設定 > セキュリティ サービス > 地域 IP フィルタ**」に移動します。

2 「**診断**」を選択します。

3 「**地域ロケーション サーバ調査を確認する**」セクションまでスクロールします。

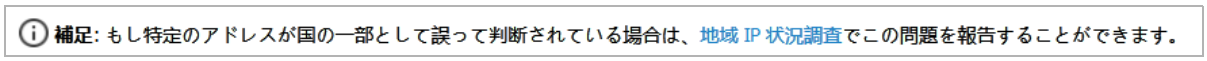
4 「**調査する IP**」フィールドに IP アドレスを入力します。

5 「**実行**」を選択します。「**結果**」見出しの下に IP アドレスに関する調査結果が表示されます。



アドレスの指定に誤りがある場合

特定のアドレスが国の一部として誤って指定されていると判断された場合は、その問題を報告することもできます。「**管理 | セキュリティ設定 > セキュリティ サービス > 地域 IP フィルタ**」ページの「**補足**」にある「**地域 IP 状況調査**」リンクを選択してください。



このリンクにより「**Submit IP for Geolocation Review**」 (地理位置情報の再調査のための IP 提出) ページが表示されます。

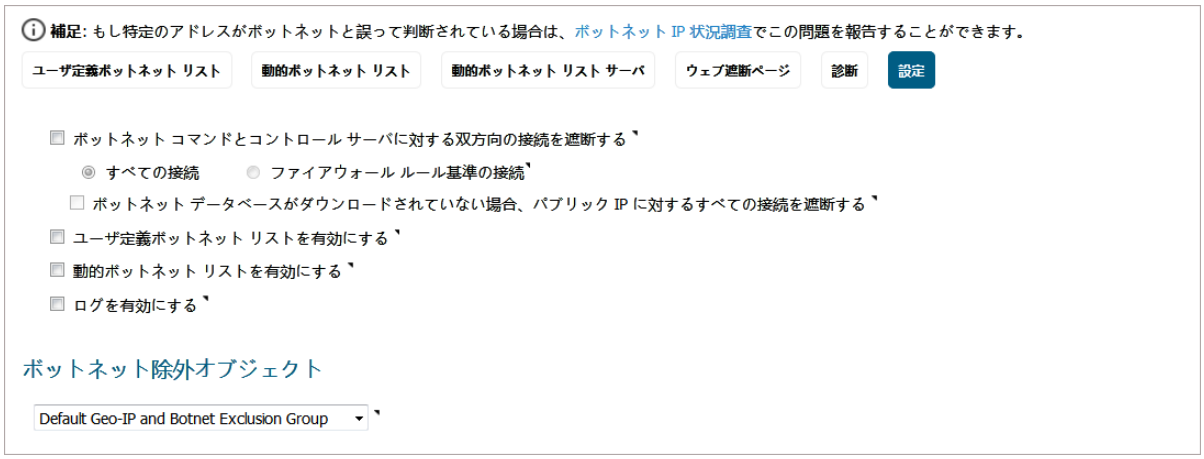
19

ボットネット フィルタの設定

メモ：ボットネット フィルタ機能は、TZ 300 シリーズ以降の装置で使用できます。

- セキュリティ サービス > ボットネット フィルタ (234 ページ)
- ボットネット フィルタの設定 (235 ページ)
- ユーザ定義ボットネット リストの作成 (236 ページ)
- 動的 HTTP 認証の設定 (240 ページ)
- ウェブ遮断ページの設定のカスタマイズ (242 ページ)
- ボットネット フィルタ診断の使用 (243 ページ)
- ボットネット機能およびデータベースの状況表示 (246 ページ)

セキュリティ サービス > ボットネット フィルタ



ボットネット フィルタ機能を使うと、ボットネット コマンドとコントロール サーバに対する双方向の接続を遮断したり、ユーザ定義ボットネット リストを作成したりできます。

ボットネット フィルタ機能を使用すると、ウェブ サイト遮断時に表示されるユーザ定義メッセージを作成できます。また、動的ボットネットの HTTP 認証を許可することができます。

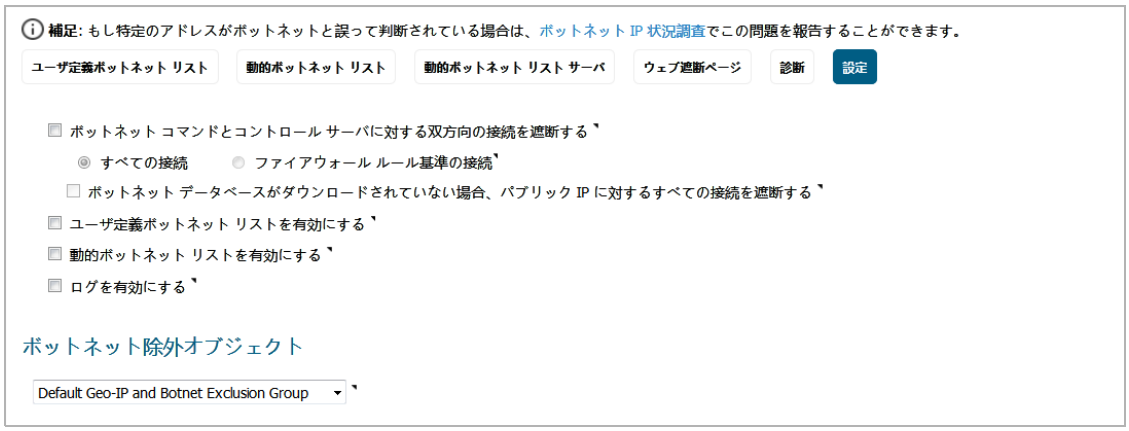
また、ボットネット フィルタ診断ツールを使用すると、ボットネットの表示、ボットネット キャッシュの統計やユーザ定義ボットネットの統計の監視、ボットネット サーバの調査を行うことができます。

ボットネット フィルタの設定

ボットネット フィルタを設定するには、以下の手順に従います。

1 「**管理 | セキュリティ設定 > セキュリティ サービス > ボットネット フィルタ**」ページに移動します。

2 「**設定**」を選択します。



3 ボットネット コマンドとコントロール サーバとして指定されているすべてのサーバを遮断するために「**ボットネット コマンドとコントロール サーバに対する双方向の接続を遮断する**」オプションを選択にします。ボットネット コマンドとコントロール サーバに対する双方向の接続がすべて遮断されます。このオプションは、既定では選択されていません。

このオプションが選択されている場合、ラジオ ボタンと「**ボットネット データベースがダウンロードされていない場合、パブリック IP に対するすべての接続を遮断する**」オプションが使用可能になります。

選択した IP アドレスをこの遮断動作の対象から除外するには、以下に示す手順で除外リストを使用するか、ユーザ定義ボットネット リストの作成 (236 ページ) の説明に従って、ユーザ定義ボットネット リストを作成します。

4 「**ボットネット コマンドとコントロール サーバに対する双方向の接続を遮断する**」が選択されている場合、以下のオプションが使用できるようになります。

a ボットネット フィルタの 2 つのモードから、1 つ選択します。

- **すべての接続**: ボットネット サーバとの双方向の接続すべてを遮断します。これは既定のボットネット遮断モードです。
- **ファイアウォール ルール基準の接続**: 装置上で設定されたアクセス ルールに一致する接続だけを遮断します。

b ボットネット データベースがダウンロードされていないとき、パブリック IP に対するすべての接続を遮断する場合は「**ボットネット データベースがダウンロードされていない場合、パブリック IP に対するすべての接続を遮断する**」を選択します。このオプションは、既定では選択されていません。

5 ユーザ定義ボットネット リストを有効にするには、「**ユーザ定義ボットネット リストを有効にする**」チェックボックスをオンにします。このオプションは、既定では選択されていません。

「**ユーザ定義ボットネット リストを有効にする**」チェックボックスがオンになっていない場合は、ファイアウォールのボットネット データベースが検索されます。「ステップ 6」に移動します。

「**ユーザ定義ボットネット リストを有効にする**」チェックボックスをオンにしてユーザ定義リストを有効にすると、IP アドレスに対する国の識別に影響を及ぼす場合があります。

a ボットネット識別時には、ユーザ定義ボットネット リストが最初に検索されます。

b IP アドレスが解決されない場合は、ファイアウォールのボットネット データベースが検索されます。

ユーザ定義ボットネット リストからの IP アドレスが解決されない場合、そのアドレスはボットネット IP アドレスまたは非ボットネット IP アドレスのどちらかとして識別され、その結果に従って対処が行われます。

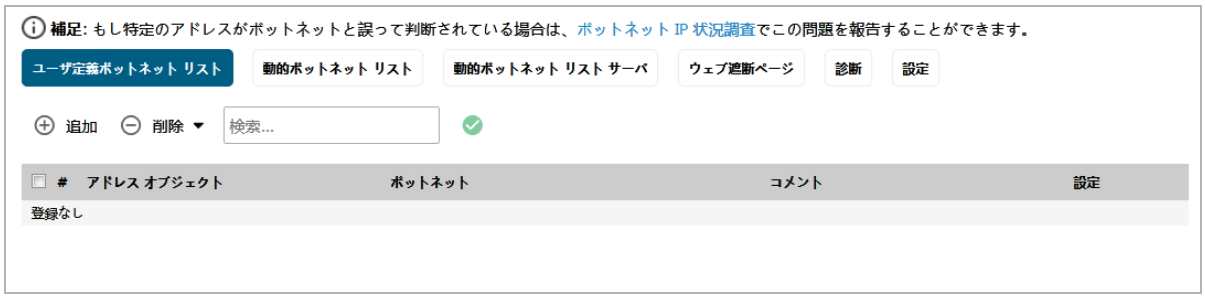
6 ボットネット フィルタ関連のイベントをログするために、「**ログを有効にする**」を選択します。

7 必要に応じて、指定したアドレス オブジェクト/アドレス グループに属するすべての IP アドレスを含む除外リストを設定できます。このリストに属するすべての IP アドレスが遮断の対象から除外されます。除外リストを有効にするには、「**ボットネット除外オブジェクト**」ドロップダウン メニューからアドレス オブジェクトまたはアドレス グループを選択します。

既定の除外オブジェクトは「Default Geo-IP and Botnet Exclusion Group」です。『*SonicWall SonicOS 6.5 ポリシー*』の説明に従って、独自のアドレス オブジェクトやアドレス グループオブジェクトを作成することができます。

8 「**適用**」を選択します。

ユーザ定義ボットネット リストの作成



アドレス オブジェクト	アドレス オブジェクトまたはアドレス グループ エントリの名前。
ボットネット	エントリが作成時にボットネットとして定義されていたかどうかを示すアイコン。黒丸はボットネットを、白丸は非ボットネットを示します。
コメント	エントリについて追加したコメント。
設定	エントリの**編集**アイコンと**削除**アイコンがあります。
合計	**ユーザ定義ボットネット リスト**内のエントリ数が表示されます。

IP アドレスはボットネットとして誤ってマークされることがあります。こうした分類の誤りがあると、IP アドレスの不適切/不必要なフィルタリングが行われる可能性があります。ユーザ定義ボットネット リストがあれば、特定の IP アドレスに対するボットネット タグよりも優先することで、こうした問題を解決できます。

トピック:

- ユーザ定義ボットネット リストの作成 (237 ページ)
- ユーザ定義ボットネット リストのエントリの編集 (239 ページ)
- ユーザ定義ボットネット リストのエントリの削除 (239 ページ)

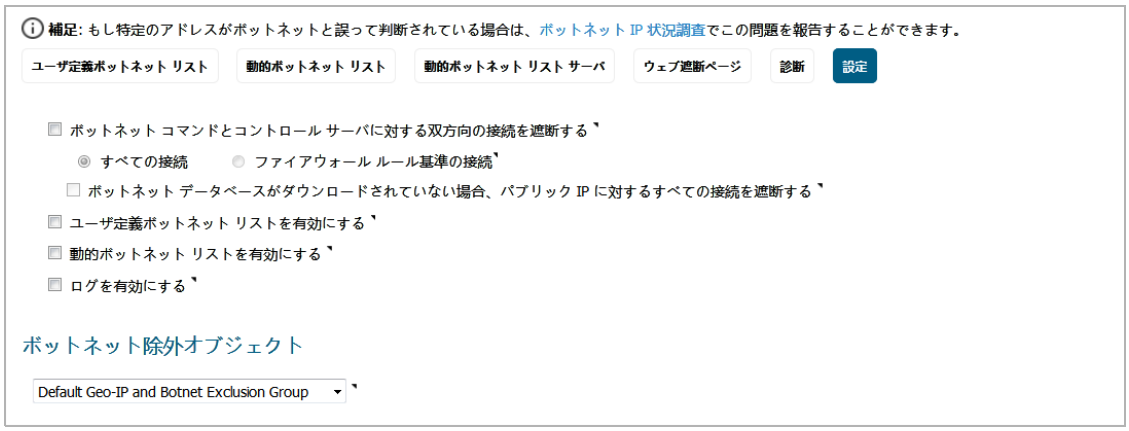
ユーザ定義ボットネット リストの作成

重要：ファイアウォールでユーザ定義ボットネット リストを使用するには、ボットネット フィルタの設定 (235 ページ) の説明に従って、このリストを有効にする必要があります。

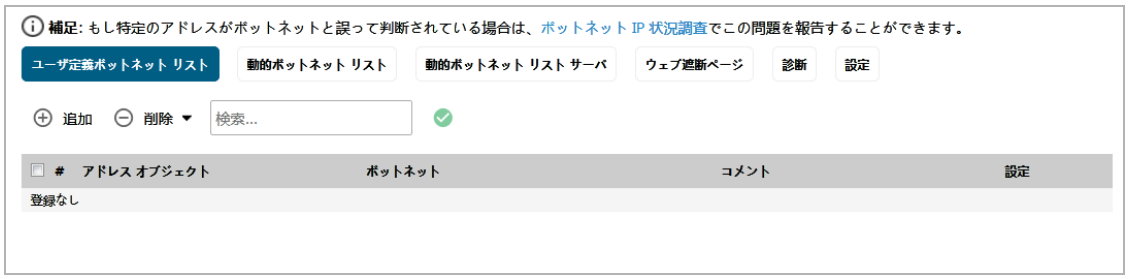
ユーザ定義ボットネット リストを作成するには、以下の手順に従います。

1 「**管理 | セキュリティ設定 > セキュリティ サービス > ボットネット フィルタ**」ページに移動します。

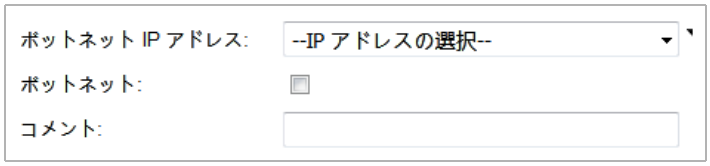
2 「**設定**」を選択します。



3 「**ユーザ定義ボットネット リスト**」を選択します。



4 **追加**アイコンを選択します。「**ユーザ定義ボットネット リストの追加**」ダイアログが表示されます。



5 「**ボットネット IP アドレス**」ドロップダウン メニューから、IP アドレス オブジェクトを選択するか、新しいアドレス オブジェクトを作成します。

重要：アドレス オブジェクトは、ユーザ定義国リストにある他のどのアドレス オブジェクトとの重複も許されません。ただし、異なるアドレス オブジェクトに同じ国 ID を持たせることはできます。

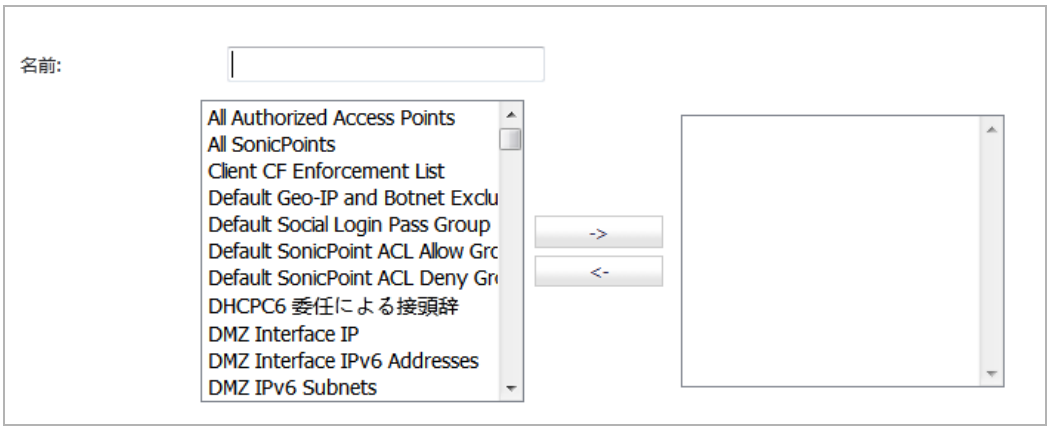
- **アドレス オブジェクトの作成...** - 「**アドレス オブジェクトの追加**」ダイアログが表示されます。

『*SonicWall SonicOS 6.5 ポリシー*』の説明に従って、新しいアドレス オブジェクトを作成します。ただし、次の制限があります。

- 許可されている種別は次のとおりです。
  - **ホスト**
  - **範囲**
  - **ネットワーク**
  - 上記の 3 つの種別の任意の組み合わせで構成されるグループ

  その他すべての種別は、許可されていない種別であり、ユーザ定義ボットネット リストに追加できません。

- **アドレス グループの作成...** - 「**アドレス オブジェクト グループの追加**」ダイアログが表示されます。



『*SonicWall SonicOS 6.5 ポリシー*』の説明に従って、新しいアドレス オブジェクトを作成します。

- 既に定義されているアドレス オブジェクトまたはアドレス グループ

6 このアドレス オブジェクトが既知のボットネットである場合は、「**ボットネット**」チェックボックスをオンにします。

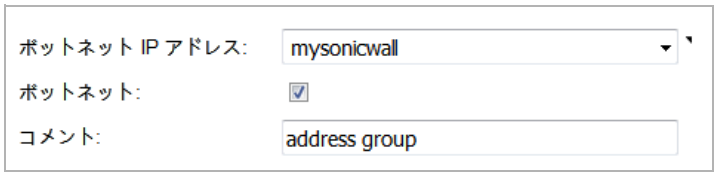
7 必要に応じて、「**コメント**」フィールドにコメントを入力します。

8 「**OK**」を選択します。

ユーザ定義ボットネット リストのエントリの編集

ユーザ定義ボットネット リストのエントリを編集するには、以下の手順に従います。

1 「**ユーザ定義ボットネット リスト**」テーブルで、編集するエントリの「**設定**」列にある「**編集**」アイコンを選択します。「**ユーザ定義ボットネット リストの追加**」ダイアログにそのエントリが表示されます。



2 変更を加えます。

3 「**OK**」を選択します。「**ユーザ定義ボットネット リスト**」テーブルが更新されます。

ユーザ定義ボットネット リストのエントリの削除

ユーザ定義ボットネット リストのエントリを削除するには、以下の手順に従います。

1 次のいずれかを行います。

- エントリの「**設定**」列にある**削除**アイコンを選択します。
- エントリのチェックボックスをオンにし、「**削除**」ボタンを選択します。

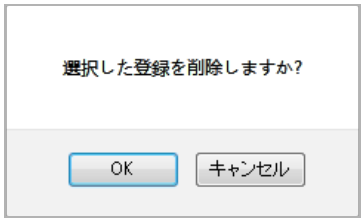
確認メッセージが表示されます。

2 「**OK**」を選択します。

複数のエントリを削除するには、以下の手順に従います。

1 削除するエントリのチェックボックスをオンにします。「**削除**」ボタンが使用可能になります。

2 「**削除**」を選択します。確認メッセージが表示されます。

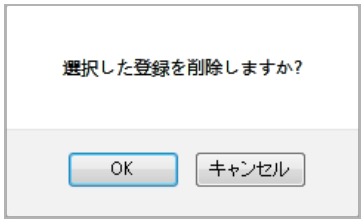


3 「**OK**」を選択します。

すべてのエントリを削除するには、以下の手順に従います。

1 テーブル見出しにある該当するチェックボックスをオンにします。

2 「**削除**」を選択します。確認メッセージが表示されます。



3 「**OK**」を選択します。

動的 HTTP 認証の設定

SonicOS 6.5.2 では、動的ボットネットの設定で HTP URL に対するユーザ名とパスワードが受け入れられ、その情報が HTTP ヘッダーで送信されるため、ファイアウォールは必要な情報を取得します。

動的 HTTP 認証を設定するには:

1 「**管理 | セキュリティ設定 > セキュリティ サービス > ボットネット フィルタ**」に移動します。

2 「**動的ボットネット リスト サーバ**」を選択します。

3 「**ボットネット リストの定期ダウンロードを有効にする**」を選択します。 このオプションは、既定では選択されていません。

4 「**ダウンロード間隔**」からダウンロードの頻度を選択します。

- **5 分** (既定)
- **15 分**
- **1 時間**
- **24 時間**

ファイアウォールは、指定された間隔でボットネット ファイルをサーバからダウンロードします。

5 ファイルを取得するためにファイアウォールがバックエンド サーバとの通信で使用するプロトコルを「**プロトコル**」から選択します。

- **FTP** (既定)
- **HTTPS**

6 「**サーバ IP アドレス**」フィールドに、ボットネット リスト ファイルをダウンロードするサーバの IP アドレスを入力します。

7 「**ログイン ID**」フィールドに、ファイアウォールがサーバへの接続に使用するログイン ID を入力します。

8 「**パスワード**」フィールドに、ファイアウォールがサーバへの接続に使用するパスワードを入力します。

9 「**ディレクトリ パス**」フィールドに、ファイアウォールがボットネット ファイルを取得するファイアウォールのディレクトリ パスを入力します。このサーバ ディレクトリ パスは、既定のルート ディレクトリからの相対パスです。

10 「**ファイル名**」フィールドに、ダウンロードするサーバ上のファイルの名前を入力します。

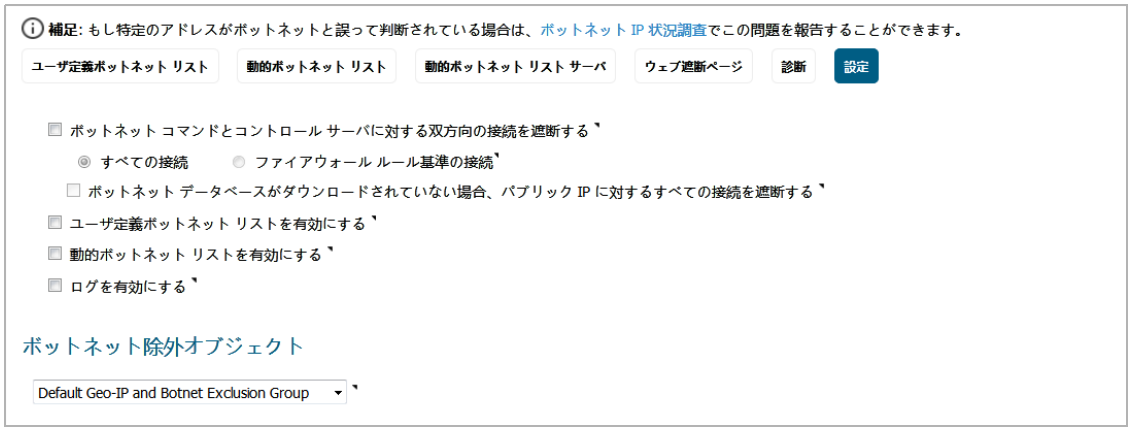
11 「**適用**」を選択します。

ウェブ遮断ページの設定のカスタマイズ

ボットネット フィルタには、ページが遮断されたときに表示される既定のメッセージがあります。このメッセージはカスタマイズしたり、独自のロゴを含めたりすることができます。

ユーザ定義メッセージを作成してユーザ定義ロゴを含めるには、以下の手順に従います。

1 「**管理 | セキュリティ設定 > セキュリティ サービス > ボットネット フィルタ**」に移動します。



2 「**ボットネット フィルタ遮断の詳細を含める**」オプションを選択します。このオプションは、既定では選択されています。

このオプションを有効にすると、遮断理由、IP アドレス、国などの、遮断の詳細が表示されます。このオプションを無効にすると、すべての情報が表示されなくなります。

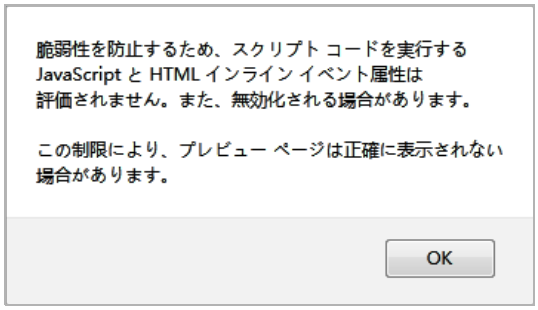
3 以下のいずれかを実行します。

- 「**警告文**」フィールドに表示されている既定のメッセージ、「このサイトはネットワーク管理者によって遮断されています。」を使用する場合は、「**既定の遮断ページ**」ボタンを選択し、ステップ 4 に進みます。
- 地域 IP フィルタ遮断ページに表示するカスタム メッセージを「**警告文**」フィールドで指定します。指定できるメッセージは最大 100 文字です。

4 必要に応じて、「**Base64 でエンコードされたロゴ アイコン**」フィールドで、Base 64 エンコード GIF アイコンを表示するように指定することもできます。

メモ：有効なアイコン画像を使用し、サイズをできるだけ小さくしてください。推奨サイズは 400 x 65 です。

5 カスタマイズしたメッセージとロゴ (または既定のメッセージとロゴ) のプレビューを表示するには、「**プレビュー**」ボタンを選択します。警告メッセージが表示されます。



6 「**OK**」を選択します。「**ウェブ サイトが遮断されました**」というメッセージが表示されます。

7 「**ウェブ サイトが遮断されました**」というメッセージを閉じます。

8 「**適用**」を選択します。

ボットネット フィルタ診断の使用

「**管理 | セキュリティ設定 > セキュリティ サービス > ボットネット フィルタ**」ページの「**診断**」ビューには、いくつかのツールが用意されています。

- 解決されたボットネット位置の表示 (244 ページ)
- ボットネット キャッシュ統計 (244 ページ)
- ボットネットの統計 (245 ページ)
- ボットネットサーバ調査を確認する (245 ページ)
- アドレスの指定に誤りがある場合 (246 ページ)

解決されたボットネット位置の表示

「**診断**」セクションの「**ボット ネット を表示**」を選択すると、以下の情報から成る、解決された IP アドレスに関するテーブルが表示されます。

- **インデックス**
- **IP アドレス** - ボットネットの IP アドレス

ボットネット キャッシュ統計

「**ボットネット キャッシュ統計**」テーブルには次の情報が含まれます。

- **ロケーション サーバ IP**
- **解決された登録数**
- **解決されなかった登録数**
- **現在の登録数**

- **最大登録数**
- **検知されたボットネット**

ボットネットの統計

「**診断**」ビューには、ユーザ定義ボットネットと動的ボットネットの両方の統計が表示されます。「**ユーザ定義ボットネットの統計**」および「**動的ボットネットの統計**」テーブルには、リスト内のエントリ数やエントリの検索回数に関する情報が含まれています。

- **登録数**
- **コール回数**
- **検索失敗回数**
- **解決回数**

ボットネットサーバ調査を確認する

ボットネット フィルタには、以下の確認のために IP アドレスを調査する機能もあります。

- ドメイン名または IP アドレス
- 発信国と、サーバがボットネット サーバとして分類されているかどうか

メモ：ボットネット サーバ調査ツールは、「**システム > 診断**」ページからも利用できます。

ボットネット サーバを調査するには、以下の手順に従います。

1 「**管理 | セキュリティ設定 > セキュリティ サービス > ボットネット フィルタ**」に移動します。

2 「**診断**」を選択します。

3 「**ボットネット サーバ調査の確認**」セクションまでスクロールします。

4 「**調査する IP**」フィールドに IP アドレスを入力します。

5 「**実行**」を選択します。「**結果**」 見出しの下に IP アドレスに関する調査結果が表示されます。

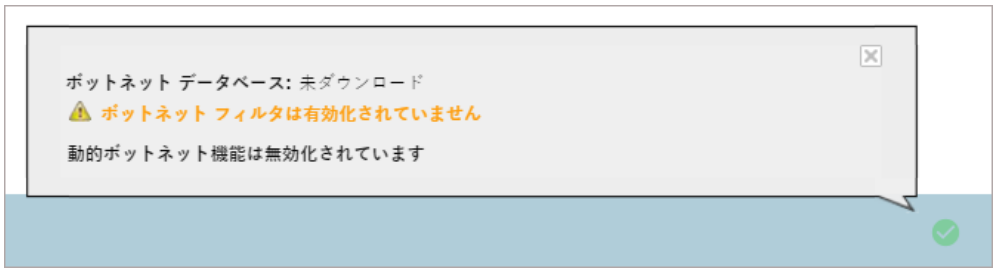
アドレスの指定に誤りがある場合

補足: もし特定のアドレスがボットネットと誤って判断されている場合は、ボットネット IP 状況調査でこの問題を報告することができます。

あるアドレスが間違ってボットネットとしてマークされていると考えられる場合、またはボットネットとしてマークされるべきと考えられる場合は、問題を SonicWall ボットネット IP 状況調査で報告してください。具体的には、「**管理 | セキュリティ設定 > セキュリティ サービス > ボットネット フィルタ**」ページの「**補足**」にあるリンクを選択するか、次の URL に移動します: SonicWall ボットネット IP 状況調査。

ボットネット機能およびデータベースの状況表示

ボットネット機能およびデータベースの状況を表示するには、「状況」アイコンを選択します。状況を示すポップアップが表示されます。



ポップアップを閉じるには、「**X**」をクリックします。

第 3 部

セキュリティ 設定 | 復号化サービス

- DPI-SSL について
- DPI-SSL/TLS クライアントの設定
- DPI-SSL/TLS サーバの設定
- DPI-SSH の設定

20

DPI-SSL について

メモ：DPI-SSL は、暗号化された HTTPS トラフィックやその他の SSL ベースの IPv4 と IPv6 のトラフィックの検査を実現する個別にライセンスされる機能です。

- DPI-SSL について (248 ページ)
- 配備方針 (251 ページ)
- DPI SSL のカスタマイズ (252 ページ)
- 装置モデル別の接続 (252 ページ)

DPI-SSL について

トピック:

- サポートされる機能 (248 ページ)
- セキュリティ サービス (251 ページ)

サポートされる機能

セキュア ソケット レイヤの精密パケット検査 (DPI-SSL) は、SonicWall の精密パケット検査技術を拡張して、暗号化された HTTPS トラフィックおよびその他の SSL ベースのトラフィックを検査できるようにするものです。SSL トラフィックを透過的に復号化して脅威をスキャンし、脅威や脆弱性が見つからなかった場合には再度暗号化して送信先に送信します。

暗号化された HTTPS およびその他の SSL ベースのトラフィックを DPI-SSL で分析することによって、セキュリティ、アプリケーションの制御、データ漏洩の抑止を強化できます。DPI-SSL サポートは、次のとおりです。

- Transport Layer Security (TLS) ハンドシェイク プロトコル 1.2 およびそれより前のバージョン - SonicOS 6.2.5.1 以降では、TLS 1.2 通信プロトコルが DPI-SSL 配備でのファイアウォールとサーバとの間の SSL 検査/復号化時にサポートされるようになりました (これまで、TLS 1.2 のサポートはクライアントとファイアウォール間に限られていました)。また、SonicOS は他の領域でも TLS 1.2 をサポートしています。
- SHA-256 - 再署名されたすべてのサーバ証明書は、SHA-256 ハッシュ アルゴリズムによって署名が行われます。
- Perfect Forward Secrecy (PFS) - 通知された暗号スイートでは、Perfect Forward Secrecy ベースの暗号やその他のより強力な暗号が弱い暗号よりも優先されます。その結果、クライアントやサーバは、より強力な暗号をサポートしていない場合を除き、弱い暗号をネゴシエートしないことが見込まれます。

DPI-SSL は SSL トンネル上でのアプリケーション レベルの帯域幅管理もサポートします。アプリケーション ルールの HTTP 帯域幅管理ポリシーは、アプリケーション ルールに対してDPI-SSL を有効にしているときに HTTPS でアクセスするコンテンツにも適用されます。

クライアントとサーバの両方の DPI-SSL をアクセス ルールによって制御できます。

トピック:

- ローカル CRL のサポート (249 ページ)
- TLS 証明書状況要求拡張機能 (249 ページ)
- SSH X11 転送の遮断 (249 ページ)
- ECDSA 関連暗号のサポート (250 ページ)
- 独立して動作する DPI-SSL および CFS HTTPS コンテンツ フィルタ (250 ページ)
- 復号化されたパケットに保持される元のポート番号 (251 ページ)

ローカル CRL のサポート

証明書失効リスト (CRL) は、予定された有効期限になる前に発行元の証明書認証機関 (CA) が取り消した、もはや信頼されないデジタル証明書のリストです。このリストについて CA に連絡する際の問題は、ブラウザが CA のサーバに到達したかどうか、または攻撃者が失効チェックをバイパスするために接続をインターセプトしたかどうかを確認できないことです。

ローカル CRL は、通常の CRL (つまり、オンライン CRL) を基準に決まります。通常の CRL の場合、クライアントは CRL 配布ポイントから CLR をダウンロードする必要があります。クライアントが CRL をダウンロードできない場合、既定では、クライアントは証明書を信頼します。通常の CRL とは異なり、ローカル CRL は、DPI-SSL のインポート メモリに失効した証明書のリストをローカルに保持して、証明書が失効しているかどうかを確認します。

この機能の詳細については、テクニカル サポートにお問い合わせください。

TLS 証明書状況要求拡張機能

DPI-SSL は、新しい TLS 証明書状況要求拡張機能 (正式には OCSP stapling) をサポートします。この拡張機能をサポートすることにより、既に確立されているチャネルを通じて証明書状況情報が DPI-SSL クライアントに配信されるため、オーバーヘッドが削減され、パフォーマンスが向上します。

この機能の詳細については、『*SonicWall SonicOS 6.5 システム セットアップ*』を参照するか、テクニカル サポートにお問い合わせください。

SSH X11 転送の遮断

メモ：X11 転送には、有効な SonicWall DPI-SSH ライセンスが必要です。

X は、Unix ワークステーション用の一般的なウィンドウ システムです。X を使用すると、ユーザは、ユーザのローカル ディスプレイでウィンドウを開くリモート X アプリケーションを実行できます (逆の場合は、リモート ディスプレイでローカル アプリケーションを実行します)。ファイアウォールおよび管理者がリモート接続を遮断した後にリモート サーバが外部にある場合、ユーザはまだ SSH トンネリングを使用すればローカル マシンで X ディスプレイを取得できます。したがって、ユーザはファイアウォール上のアプリケーションベースのセキュリティ ポリシーを迂回し、セキュリティ リ

スクを引き起こすことができます。アプリケーションと X サーバの間の X プロトコル セッションはネットワークを介して送信されている間は暗号化されないため、X11 プロトコル接続を SSH 接続経由でルーティングして、セキュリティと強力な認証を提供できます。この機能は X11 転送と呼ばれます。SSH クライアントは、SSH サーバに接続するときに X 転送を要求します (クライアントで X 転送が有効になっていると仮定)。サーバがこの接続で X 転送を許可している場合、ログインは正常に進行しますが、サーバは舞台裏で特別な手順を実行します。ターミナル セッションの処理に加えて、サーバはリモート マシンで実行されるプロキシ X サーバとして自身を設定し、プロキシ X ディスプレイを指すようにリモート シェルで DISPLAY 環境変数を設定します。X クライアント プログラムは、実行されるとプロキシに接続します。プロキシは実際の X サーバと同様に動作し、SSH クライアントにプロキシ X クライアントとして動作するよう指示し、ローカル マシンの X サーバに接続します。SSH クライアントとサーバは協力して、2 つの X セッション間の SSH パイプを介して X プロトコル情報をやり取りします。X クライアント プログラムは、ディスプレイに直接接続されているかのように画面に表示されます。DPI-SSH X11 転送は、次のクライアントをサポートしています。

- Cygwin 用の SSH クライアント
- Putty •secureCRT
- Ubutu の SSH
- CentOS の SSH

DPI-SSH X11 転送は、次の SSH サーバをサポートしています。

- Fedora
- Ubuntu

SSH X11 転送では、ルート モードとワイヤ モードの両方がサポートされます。対象が

- ワイヤ モードでは、DSSH X11 転送は保護 (直列トラフィックのアクティブ DPI) モードでのみサポートされます。
- ルート モードでは、制限はありません。

SSH X11 転送でサポートされる接続の最大数は、DPI-SSH と同じです。1000.DPI-SSH。

ECDSA 関連暗号のサポート

DPI-SSL クライアントは ECDSA（楕円曲線デジタル署名アルゴリズム）暗号をサポートしています:

- TLS_ECDHE_ECDSA_WIATH_AES_128_GCM_SHA256
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256

独立して動作する DPI-SSL および CFS HTTPS コンテンツ フィルタ

DPI-SSL および CFS HTTPS コンテンツ フィルタは、同時に有効にでき、次のように機能します。

- DPI-SSL クライアント検査が無効になっている場合、コンテンツ フィルタ サービスは HTTPS 接続をフィルタリングします。
- DPI-SSL クライアント検査が有効になっているが、コンテンツ フィルタ オプションが選択されていない場合、コンテンツ フィルタ サービスは HTTPS 接続をフィルタリングします。
- DPI-SSL クライアント検査が有効で、コンテンツ フィルタ オプションが選択されている場合、CFS は HTTPS 接続をフィルタリングしません。

復号化されたパケットに保持される元のポート番号

暗号化接続の DPI-SSL/DPI-SSH 接続の場合、復号化されたパケットは送信先ポートが 80 と表示されます (HTTPS の場合)。復号化されたパケットがパケット キャプチャ/Wireshark で確認されると、元のポート番号を保持するようになりました。ポート番号の変更はパケット キャプチャにのみ適用され、実際のパケットまたは接続キャッシュには適用されません。

セキュリティ サービス

DPI-SSL を使用できるセキュリティ サービスおよび機能は、次のとおりです。

ゲートウェイ アンチウイルス	コンテンツ フィルタ
ゲートウェイ アンチスパイウェア	アプリケーション ファイアウォール
侵入防御	

配備方針

DPI-SSL の主な配備シナリオには次の 2 つがあります。

- **クライアント DPI-SSL**: 装置の LAN 上のクライアントが WAN 上のコンテンツにアクセスするときに、HTTPS トラフィックを検査するために使用します。DPI-SSL に対する除外は、コモンネームまたは種別を基準にして行うことができます。
- **サーバ DPI-SSL**: リモート クライアントが WAN 経由で接続して装置の LAN 上のコンテンツにアクセスするときに、HTTPS トラフィックを検査するために使用します。

プロキシ配備

DPI-SSL はプロキシ配備をサポートしています。プロキシ配備では、すべてのクライアント ブラウザがプロキシ サーバにリダイレクトされますが、装置はクライアント ブラウザとプロキシ サーバの間に存在します。このシナリオでは、ドメインが仮想ホスティング サーバに含まれる場合や、同じサーバ IP を複数のドメインで使用できる一部のクラウド配備内でのドメイン除外など、すべての DPI-SSL 機能がサポートされます。

また、通常のデータ センター サーバ ファームでは、サーバ上の SSL 処理の負荷を軽減するために、前面に負荷分散装置やリバース SSL プロキシを配置しています。サーバの前面に位置して復号化を行っている負荷分散装置の場合、通常、装置には負荷分散装置の IP しかわかりません。負荷分散装置は、内容を復号化し、この接続の割り当て先となる特定のサーバを決定します。今回、DPI-SSL には IP ベースの除外キャッシュを無効にするためのグローバル ポリシー オプションが用意されました。IP ベースの除外キャッシュがオフになっていても、除外は機能し続けます。

DPI SSL のカスタマイズ

重要：NetExtender SSL VPN ゲートウェイを DPI SSL IP アドレス除外リストに追加してください。NetExtender トラフィックは PPP によってカプセル化されており、このようなトラフィックを SSL VPN によって復号化しても意味のある結果は得られません。

一般には、装置を通過するありとあらゆるトラフィックを保護することが DPI-SSL のポリシーです。この点がセキュリティのニーズに合うことも合わないこともあるので、DPI-SSL では処理の対象をカスタマイズすることができます。

DPI-SSL には、DPI の処理から除外される組み込み (既定) ドメインのリスト (データベース) が付随します。このリストへの追加はいつでも行うことができ、追加したエントリはどれでも削除できます。また、DPI 処理の対象としての組み込みエントリの除外と包含を切り替えることもできます。DPI-SSL では、コモンネームまたは種別 (バンキング、医療など) によってドメインを除外したり含めたりすることもできます。

ただし、コモンネームと種別のどちらによるものかに関係なく、除外されたサイトは、装置を回避してクライアント マシンにダウンロードされるエクスプロイト キットや、無防備なクライアントに偽りのサイト/証明書を提示する中間者の乗っ取りによって今後悪用されうるセキュリティ上のリスクになる可能性があります。こうしたリスクを回避するために、DPI-SSL では除外されるサイトを除外前に認証することができます。

ネットワーク内での HTTPS 接続の割合が増え、新しい https サイトが現れてくるので、最新バージョンの SonicOS であっても、組み込み/既定除外の完全なリストを用意することはまず不可能です。新しいクライアント アプリケーションに特有の実装やサーバ実装が原因で DPI-SSL によるインターセプトが発生した場合、一部の HTTPS 接続はエラーになるので、シームレスなユーザ エクスペリエンスを実現するためには、装置上でのこうしたサイトの除外が必要になる場合があります。SonicOS は、このような失敗した接続のログを保持しています。こうした接続エラーは、トラブルシューティングを行ったり、信頼できるエントリを除外リストに追加するために利用したりできます。

サイトの除外/包含に加えて、DPI-SSL では、グローバルな認証ポリシーとグローバルなポリシーに対するきめ細かな除外ポリシーの両方を用意しています。例えば、接続の認証を行うためのグローバルポリシーでは、信頼できる新しい CA 証明書や、安全性の高いプライベート (または企業にとってローカルな配備の) クラウド ソリューションの自己署名サーバ証明書など、基本的に安全な接続が遮断される可能性があります。管理者は、きめ細かいオプションを使用して、グローバル認証ポリシーから個々のドメインを除外できます。

同じサーバ (証明書) でサポートされるドメインのリストに含まれているドメインに対して除外を設定できます。つまり、サーバ証明書によっては複数のドメイン名が含まれているものがありますが、1 つのサーバ証明書が対象としているすべてのドメインを除外することなく、これらのドメインのうち 1 つだけを除外したい場合があります。例えば、`youtube.com` を除外して、他のすべてのドメイン (`google.com` など) を除外せずに済ませることができます。`*.google.com` は、`youtube.com` がサブジェクト代替名拡張の下での代替ドメインとしてリストされているサーバ証明書のコモンネームであるにもかかわらずです。

装置モデル別の接続

クライアント DPI-SSL によってサポートされる、プラットフォームごとの最大同時接続数 テーブルに、各プラットフォームと、装置がクライアント DPI-SSL 検査を実行できる同時接続の最大数を示します。

クライアント DPI-SSL によってサポートされる、プラットフォームごとの最大同時接続数

ハードウェア モデル	DPI-SSL の同時接続の最大数	ハードウェア モデル	DPI-SSL の同時接続の最大数	ハードウェア モデル	DPI-SSL の同時接続の最大数
NS*a* 9650	500,000	SM 9600	12,000	TZ600/TZ600P	10,000
NS*a* 9450	325,000	SM 9400	10,000	TZ500/TZ500 W	5,000
NS*a* 9250	150,000	SM 9200	8,000	TZ400/TZ400 W	4,000
NS*a* 6650	150,000			TZ300/TZ300P/TZ300 W	3,000
NS*a* 5650	80,000	NSA 6600	6,000	SOHO W	1,000
NS*a* 4650	60,000	NSA 5600	4,000		
NS*a* 3650	40,000	NSA 4600	3,000		
NS*a* 2650	30,000	NSA 3600	2,000		
		NSA 2600	1,000		

メモ：NS*a* シリーズ、SuperMassive 9200、9400、9600、および NSA 3600 シリーズ (およびそれ以降) のファイアウォールにおいて、DPI 設定が 250,000 以上で、かつ動的接続サイジングが設定されているとき、ファイアウォールは DPI-SSL 接続数を動的に増やすことができます。詳細については、動的接続サイジング (16 ページ) を参照してください。

21

DPI-SSL/TLS クライアントの設定

- 復号化サービス > DPI-SSL/TLS クライアント (254 ページ)
- DPI-SSL 状況の表示 (255 ページ)
- DPI-SSL/TLS クライアントの設定 (255 ページ)

復号化サービス > DPI-SSL/TLS クライアント

ヒント： DPI-SSL の詳細については、DPI-SSL について (248 ページ) を参照してください。

DPI-SSL 状況の表示

「**DPI-SSL 状況**」セクションには、現在の DPI-SSL 接続数、ピーク接続数、最大接続数が表示されます。

DPI-SSL/TLS クライアントの設定

一般に、DPI-SSL/TLS クライアントの配備シナリオは、LAN 上のクライアントが WAN 上のコンテンツを参照するときに HTTPS トラフィックを検査するために使用します。このシナリオでは、ファイアウォールは検査対象のコンテンツに対する証明書と秘密鍵を所持していないのが普通です。装置は、DPI-SSL 検査を実行した後で、リモート サーバから送信された証明書を書き直し、新規に生成したこの証明書に署名します。これには、クライアント DPI-SSL の設定で指定した証明書が使用されます。既定では、これはファイアウォールの認証局 (CA) の証明書ですが、別の証明書を指定することもできます。証明書の信頼のエラーを防ぐために、ユーザに対しては、ブラウザの信頼済み証明書の一覧にこの証明書を追加するよう指示する必要があります。

トピック:

- 一般設定の構成 (255 ページ)
- 再署名認証局の選択 (259 ページ)
- 除外と包含の設定 (260 ページ)
- コモンネームによる除外/包含 (261 ページ)
- クライアント DPI-SSL の例 (269 ページ)

一般設定の構成

トピック:

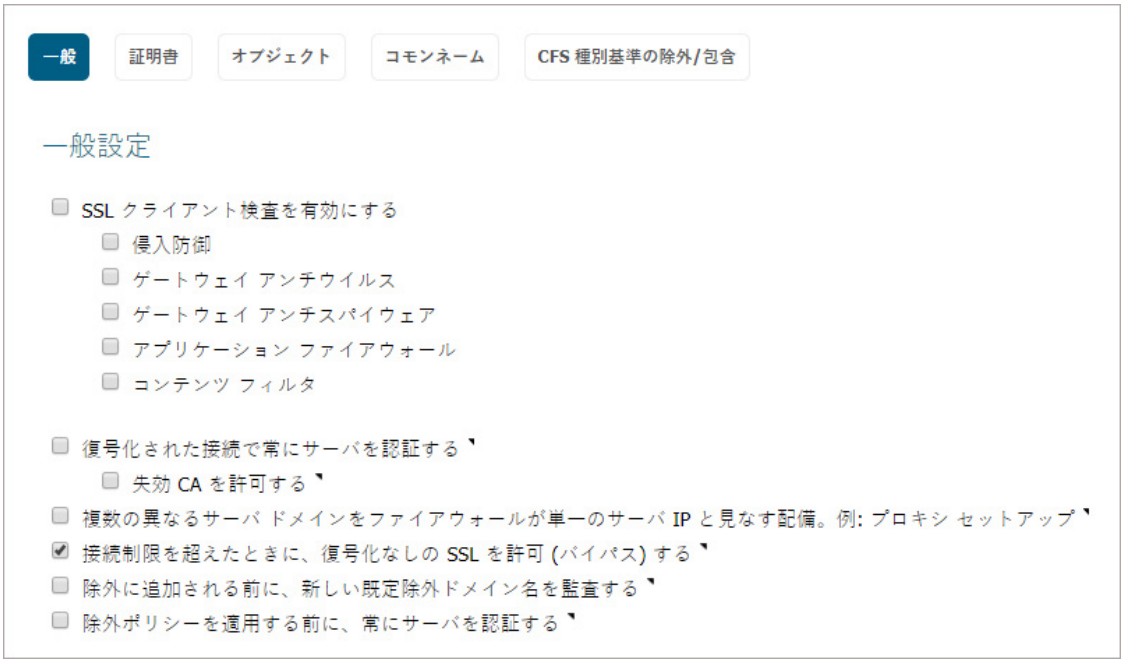
- SSL クライアント検査を有効にする (255 ページ)
- ゾーンの DPI-SSL クライアントを有効にする (258 ページ)
- ゾーンの DPI-SSL サーバを有効にする (258 ページ)

SSL クライアント検査を有効にする

SSL クライアント検査を有効にするには:

1 「**管理 | セキュリティ設定 > 復号化サービス > DPI-SSL/TLS クライアント**」に移動します。

2 「**一般**」を選択します。



3 「**SSL クライアント検査を有効にする**」を選択します。このオプションは、既定では選択されていません。

4 検査を実行するサービスを 1 つ以上選択します。既定では何も選択されていません。

- **侵入防御**
- **ゲートウェイ アンチウイルス**
- **ゲートウェイ アンチスパイウェア**
- **アプリケーション ファイアウォール**
- **コンテンツ フィルタ**

5 復号化 / インターセプトされた接続についてサーバの認証を行うには、「**復号化された接続で常にサーバを認証する**」を選択します。有効にすると、DPI-SSL によって以下のような接続が遮断されます。

- 信頼できない証明書を使用するサイトへの接続。
- Client Hello のドメイン名が、この接続のサーバ証明書に照らして検証できない場合。

このオプションは、既定では選択されていません。このオプションを選択すると、「**失効 CA を許可する**」が使用可能になります。

ⓘ **重要**：このオプションは、高いレベルのセキュリティが必要な場合にのみ有効にします。遮断された接続は、接続エラー リストに表示されます (接続エラーの表示 (266 ページ)を参照してください)。

ⓘ **ヒント**： このオプションを有効にする場合は、「**CFS カテゴリベースの除外をスキップする**」オプション (コモンネームの除外/包含 (263 ページ) を参照) を使用して、このグローバル認証オプションから特定のドメインを除外します。これは、信頼できるサイトのあらゆるサーバ関連エラーをオーバーライドするのに役立ちます。

6 期限切れまたは中間の CA を許可するには、「**失効 CA を許可する**」を選択します。このオプションは、既定では選択されていません。 これを選択しないと、Client Hello のドメイン名が、この接続のサーバ証明書に照らして正当であると確認できない場合、接続は遮断されます。

7 除外のためにサーバ IP アドレスベースの動的キャッシュの使用を無効にするには、「**複数の異なるサーバ ドメインをファイアウォールが単一のサーバ IP と見なす配備。例: プロキシ セットアップ**。 このオプションは、既定では選択されていません。

このオプションは、装置がクライアント ブラウザとプロキシ サーバの間に存在する場合を含め、すべてのクライアント ブラウザがプロキシ サーバにリダイレクトされるプロキシ配備で役に立ちます。ドメインが、前面に負荷分散装置を配置したサーバ ファームの一部として、または、同じサーバ IP を複数のドメインで使用できるクラウド配備内で、仮想ホスティング サーバに含まれる場合のドメイン除外など、すべての DPI-SSL 機能がサポートされています。

そのような配備では、装置から見えるすべてのサーバ IP がプロキシ サーバの IP になっています。そのため、プロキシ配備では、IP ベースの除外キャッシュを無効にしておく必要があります。このオプションを有効にしても、SonicOS が除外を実行する機能に影響はありません。

8 既定では、DPI-SSL の接続制限を超える新しい接続はバイパスされます。接続制限を超えた場合に、新しい接続が破棄されずに復号化をバイパスできるようにするには、「**接続制限を超えたときに、復号化なしの SSL を許可 (バイパス) する**」チェックボックスをオンにします。このオプションは、既定では選択されています。

DPI-SSL の接続制限を超える新しい接続が確実に破棄されるようにするには、このチェックボックスをオフ (無効) にします。

9 新しい組み込みの除外ドメイン名を監査したうえで除外のために追加するには、「**除外に追加される前に、新しい既定除外ドメイン名を監査する**」チェックボックスをオンにします。このチェックボックスは、既定ではオンになっていません。

このオプションを有効にすると、組み込みの除外リストが変更されるたびに (例えば、新しいファームウェア イメージのアップグレードやその他のシステム関連の動作があるとき)、その変更を知らせる通知用ポップアップ ダイアログが「**復号化サービス > DPI-SSL/TLS クライアント**」ページに表示されます。新しい変更の内容を検査/監査し、組み込みの除外リストに対する新しい変更のうち任意のもの、一部、またはすべてを許可または拒否することができます。この時点で、実行時除外リストは更新され、新しい変更が反映されます。

このオプションを無効にすると、SonicOS は、組み込み除外リストに対する新しい変更すべての許可および追加を自動的に行います。

10 コモンネームまたは種別の除外ポリシーの適用前にサーバの認証を必ず行うには、「**除外ポリシーを適用する前に、常にサーバを認証する**」チェックボックスをオンにします。このオプションは、既定では選択されていません。有効にすると、DPI-SSL によって以下のような除外された接続が遮断されます。

- 信頼できない証明書を使用するサイトへの接続。
- Client Hello のドメイン名が、この接続のサーバ証明書に照らして検証できない場合。

これは、除外ポリシーの適用前にサーバ接続を認証する場合に便利な機能です。このオプションを有効にすると、装置は、接続に対する除外を無分別に適用したり、その結果として除外サイトや除外対象種別に属するサイトについてのセキュリティ ホールを生み出したりすることがなくなります。これは、バンキングサイトが種別として除外されている場合に特に重要です。

サーバ証明書と Client Hello でのドメイン名の両方を検証したうえで除外ポリシーを適用することで、SonicOS は信頼できないサイトを拒否したり、ある主のゼロデイ攻撃の発生を潜在的に阻止したりできます。SonicOS の実装では、「信頼だけでなく検証も」というアプローチを採用しており、除外ポリシーの基準に適合するドメイン名をまず検証するようにし、それによって無防備なクライアントによるフィッシングや URL リダイレクト関連の攻撃を防止しています。

重要：サブジェクト代替名拡張における代替ドメインを除外する場合は、このオプションを有効にすることをお勧めします。

ⓘ **ヒント：** このオプションを有効にする場合は、「**CFS カテゴリベースの除外をスキップする**」オプション (コモンネームの除外/包含 (263 ページ) を参照) を使用して、このグローバル認証オプションから特定のドメインを除外します。これは、信頼できるサイトのあらゆるサーバ関連エラーをオーバーライドするのに役立ちます。

11 「**適用**」を選択します。

ゾーンの DPI-SSL クライアントを有効にする

ゾーンの DPI-SSL クライアントを有効にするには:

12 「**管理 | システム セットアップ > ネットワーク > ゾーン**」に移動します。

ⓘ **ヒント：** ゾーンの設定については、『*SonicWall SonicOS 6.5 システム セットアップ*』を参照してください。

13 設定するゾーンの「**編集**」アイコンを選択します。「**ゾーンの編集**」ダイアログが表示されます。

14 「**SSL クライアント検査を有効にする**」を選択します。 このオプションは、既定では選択されていません。

15 ゾーンの設定を終了します。

16 「**OK**」を選択します。

17 DPI-SSL クライアント検査を有効にする各ゾーンに対して、ステップ 13 からステップ 16 を繰り返します

ゾーンの DPI-SSL サーバを有効にする

ゾーンの DPI-SSL サーバを有効にするには:

1 「**管理 | セキュリティ設定 > 復号化サービス > DPI-SSL/TLS クライアント**」に移動します。

ⓘ **ヒント：** DPI-SSL サーバの設定については、DPI-SSL/TLS サーバの設定 (272 ページ) を参照してください。

2 「**SSL サーバ検査を有効にする**」を選択します。このオプションは、既定では選択されていません。

3 1 つ以上の検査種別を選択します。

4 「**適用**」を選択します。

5 「**管理 | システム セットアップ > ネットワーク > ゾーン**」に移動します。

ⓘ **ヒント：** ゾーンの設定については、*SonicWall SonicOS 6.5 システム セットアップ* を参照してください。

6 設定するゾーンの「**編集**」アイコンを選択します。「**ゾーンの編集**」ダイアログが表示されます。

7 「**SSL サーバ検査を有効にする**」を選択します。このオプションは、既定では選択されていません。

8 ゾーンの設定を終了します。

9 「**OK**」を選択します。

10 DPI-SSL サーバ検査を有効にする各ゾーンに対して、ステップ 6 からステップ 8 を繰り返します

再署名認証局の選択

再署名証明書は、その認証局の証明書がファイアウォールによって信頼されている場合のみ、元の証明書の署名認証局を置き換えます。認証局が信頼されていない場合、証明書は自己署名になります。証明書エラーを避けるために、DPI-SSL によって保護されているデバイスによって信頼されている証明書を選択してください。

メモ：DPI SSL 認証局 (CA) による証明書の要求/作成については、ナレッジ ベースの記事「*DPI-SSL 証明書再署名を目的とした DPI-SSL 認証局 (CA) による証明書の要求/作成方法*」 (SW14090) を参照してください。

再署名証明書を選択するには、以下の手順に従います。

1 「**管理 | セキュリティ設定 > 復号化サービス > DPI-SSL/TLS クライアント**」ページに移動します。

2 「**証明書**」を選択します。

3 「**証明書**」ドロップダウン メニューから使用する証明書を選択します。既定では、DPI-SSL は、「既定の **SonicWall の DPI-SSL CA 証明書**」を使用して、検査したトラフィックを再署名します。

メモ：求める証明書が表示されない場合は、「**管理 | システム セットアップ > 装置 > 証明書**」ページでそれをインポートできます。『*SonicWall SonicOS 6.5 システム セットアップ*』を参照してください。

PKCS-12 形式の証明書については、『*SonicWall SonicOS 6.5 システム セットアップ*』を参照してください。

4 選択した証明書をファイアウォールにダウンロードするには、**(ダウンロード)** リンクを選択します。「***ファイル名を開く***」ダイアログが表示されます。

ヒント： 利用可能な証明書を表示するには、**(証明書の管理)** リンクを選択して、「**管理 | システム セットアップ > 装置 > 証明書**」ページを表示します。

a 「**ファイルを保存する**」ラジオ ボタンが選択されていることを確認してください。

b 「**OK**」を選択します。

ファイルがダウンロードされます。

5 「**適用**」を選択します。

ブラウザへの信頼の追加

再署名認証局による証明書の再署名を正しく行うためには、ブラウザがこの認証局を信頼する必要があります。この信頼は、ブラウザの信頼できる CA のリストに再署名証明書をインポートすることによって確立できます。お使いのブラウザの指示に従って、再署名証明書をインポートしてください。

除外と包含の設定

既定では、DPI-SSL を有効にすると、それが装置上のすべてのトラフィックに適用されます。DPI-SSL 検査を適用するトラフィックを、以下のようにカスタマイズできます。

- 「**除外/包含**」リストで、除外/包含するオブジェクトとグループを指定します。
- 「**コモンネーム**」除外では、指定したホスト名が除外されます。
- 「**CFS 種別基準の除外/包含**」では、指定した種別が CFS 種別に基づいて除外または包含されます。

このカスタマイズにより、同じサーバ (証明書) でサポートされるドメインのリストに含まれているドメインに対する代替名の個別の除外/包含が可能になります。大量のトラフィックを処理する配備において、DPI-SSL が CPU に及ぼす影響を軽減し、DPI-SSL 検査の同時接続が最大数に達するのを防ぐために、信頼できる送信元を除外することが有効となる場合があります。

メモ：Google ドライブ、Apple iTunes、または証明書がピン留めされたその他任意のアプリケーションの使用時にファイアウォールで DPI-SSL が有効になっている場合、こうしたアプリケーションはサーバに接続できない可能性があります。アプリケーションが接続できるようにするには、関連するドメインを DPI-SSL から除外します。例えば、Google ドライブが機能するようにするには、以下のドメインを除外します。

- `.google.com`
- `.googleapis.com`
- `.gstatic.com`

Google のすべてのアプリケーションは 1 つの証明書を使用しているので、これらのドメインを除外すれば各種 Google アプリケーションが DPI-SSL をバイパスできるようになります。

あるいは、クライアント マシンを DPI-SSL から除外します。

トピック:

- オブジェクト/グループの除外/包含 (261 ページ)
- コモンネームによる除外/包含 (261 ページ)
- CFS 種別基準の除外/包含の指定 (268 ページ)
- コンテンツ フィルタ (269 ページ)
- アプリケーション ルール (271 ページ)

オブジェクト/グループの除外/包含

DPI-SSL クライアント検査をカスタマイズするには:

1 「**管理 | セキュリティ設定 > 復号化サービス > DPI-SSL/TLS クライアント**」ページに移動します。

2 「**オブジェクト**」を選択します。

3 「**アドレス オブジェクト/グループ**」の「**除外**」と「**包含**」のドロップダウン メニューで、DPI-SSL 検査に対して除外/包含するアドレス オブジェクト/グループを選択します。既定では、「**除外**」は「**なし**」、「**包含**」は「**すべて**」に設定されています。

> **ヒント：** 「**包含**」ドロップダウン メニューは、指定する除外リストの微調整に使用できます。例えば、「**除外**」ドロップダウン メニューで「**Remote-office-California**」というアドレス オブジェクトを選択し、「**包含**」ドロップダウン メニューで「**Remote-office-Oakland**」というアドレス オブジェクトを選択します。

4 「**サービス オブジェクト/グループ**」の「**除外**」と「**包含**」のドロップダウン メニューで、DPI-SSL 検査に対して除外/包含するアドレス オブジェクト/グループを選択します。既定では、「**除外**」は「**なし**」、「**包含**」は「**すべて**」に設定されています。

5 「**ユーザ オブジェクト/グループ**」の「**除外**」と「**包含**」のドロップダウン メニューで、DPI-SSL 検査に対して除外/包含するアドレス オブジェクト/グループを選択します。既定では、「**除外**」は「**なし**」、「**包含**」は「**すべて**」に設定されています。

6 「**適用**」を選択します。

コモンネームによる除外/包含

除外リストに信頼されたドメイン名を追加できます。信頼されたドメインを組み込みの除外データベースに追加すると、DPI-SSL が CPU に及ぼす影響が軽減され、装置で DPI-SSL 検査対象の同時接続が最大数に達するのを防ぐことができます。

トピック:

- DPI SSL 既定除外の状況の表示 (262 ページ)
- コモンネームの除外/包含 (263 ページ)
- 個別コモンネームの削除 (265 ページ)
- 接続エラーの表示 (266 ページ)
- 既定除外を手動で更新する (267 ページ)

DPI SSL 既定除外の状況の表示

ファイアウォールは、MySonicWall の DPI SSL 既定除外データベースの更新を定期的にチェックし、「**DPI SSL 既定除外状況**」セクションにデータベースの最新の状況を表示します。既定除外を手動で更新する (267 ページ) で説明されているように、ファイアウォール上のデータベースを手動で更新できます。

既定除外の状況を表示するには:

1 「**管理 | セキュリティ設定 > 復号化サービス > DPI-SSL/TLS クライアント**」に移動します。

2 「**DPI SSL 既定除外状況**」までスクロールします。

既定除外タイムスタンプ	既定除外データベースが更新された日時。
最終確認	ファイアウォールが既定除外データベースをチェックした日時。

コモンネームの除外/包含

コモンネーム (共通名) によってエンティティを除外/包含するには:

1 「**管理 | セキュリティ設定 > 復号化サービス > DPI-SSL/TLS クライアント**」ページに移動します。

2 「**コモンネーム**」を選択します。

3 「**コモンネーム:**」までスクロールします**除外/包含**。

4 以下のオプションを選択することで、コモンネームの表示を制御できます。

- **表示形式**に関するオプション:
  - **すべて** - すべてのコモンネームを表示します。
  - **既定** - カスタマイズされていないコモンネームのみを表示します。
  - **個別** - 管理者が追加したコモンネームのみを表示します。
- **動作**に関するオプション:
  - **すべて** - 除外されたものと CFS 種別による除外のオーバーライドの両方を表示します。
  - **除外** - 除外されたコモンネームのみを表示します。
  - **CFS 種別基準の除外をスキップする** - 選択した CFS 種別基準の除外オプションをオーバーライドする個別のコモンネームのみを表示します。

> **メモ：**「**CFS 種別基準の除外をスキップする**」オプションを使用すると、グローバルな包含オプション「**復号化された接続で常にサーバを認証する**」および「**除外ポリシーを適用する前に、常にサーバを認証する**」から特定のドメインを除外できます。

5 既定では、すべての組み込みコモンネームが承認されています。組み込みコモンネームの承認は、以下の操作によって拒否できます。

a コモンネームの「**設定**」列にある**拒否** アイコンを選択します。確認メッセージが表示されます。

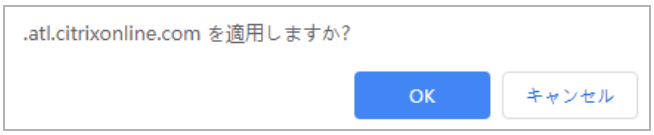
b 「**OK**」を選択します。

拒否アイコンが**承認** アイコンになり、「**ビルトイン**」列の「**承認**」が「**拒否**」になります。

ヒント： 組み込みのコモンネームは変更も削除もできませんが、拒否したり許可したりすることはできます。

拒否された組み込みコモンネームを許可するには、以下の手順に従います。

a **許可**アイコンを選択します。確認メッセージが表示されます。



b 「**OK**」を選択します。

6 個別のコモンネームを追加するには、「**コモンネーム除外/包含**」テーブルの下にある「**追加**」ボタンを選択します。「**コモンネームの追加**」ダイアログが表示されます。

a フィールドに 1 つ以上のコモンネームを追加します。複数のエントリがある場合は、カンマまたは改行文字で区切ります。

b 「**動作**」の種別を指定します。

- **除外** (既定)
- **CFS 種別基準の除外をスキップする**
- サーバを認証することによって接続が遮断される場合にこのドメインのサーバの認証を見合わせるには、「**サーバの認証をスキップする**」を選択します。このオプションは、サーバが信頼されたドメインである場合にのみ有効にします。

c DPI-SSL は、ある接続がインターセプト (包含) されるか除外されるかを、ポリシーまたは設定に基づいて動的に決定します。DPI-SSL によって接続のドメイン名が抽出されると、同じサーバ/ドメインに対する以降の接続で除外情報が使用できるようになります。

動的な除外キャッシュ (サーバ IP 基準とコモンネーム基準の両方) の使用を無効にするには、「**除外ポリシーを適用する前に、常にサーバを認証する**」チェックボックスをオンにします。このオプションは、既定では選択されていません。

d 「**適用**」を選択します。

「**コモンネーム除外/包含**」テーブルが更新され、「**ビルトイン**」列が「**個別**」になります。「**除外ポリシーを適用する前に、常にサーバを認証する**」オプションが選択されている場合は、「**ビルトイン**」列の「**個別**」の隣に**情報**アイコンが表示されます。

#	コモンネーム	動作	ビルトイン	設定
1	.agni.lindenlab.com	除外	承認	⊖
2	.atl.citrixonline.com	除外	承認	⊖

情報アイコンをマウスでポイントすると、どの個別属性が選択されていたかがわかります。「**接続エラー リスト**」を使用して追加されたコモンネームの場合、情報アイコンによって以下のエラーの種別が示されます。:

- **CFS 種別による除外をスキップ**
- **サーバ認証をスキップ**
- **サーバの認証に失敗**
- **クライアント ハンドシェイクに失敗**
- **サーバ ハンドシェイクに失敗**

エントリを削除するには、「**設定**」列の**削除**アイコンを選択します。

7 フィルタを指定してコモンネームを検索できます。

a 「**フィルタ**」フィールドに、次の構文で名前を指定して入力します。名前:コモンネーム。

b 「**フィルタ**」ボタンを選択します。

8 「**適用**」を選択します。

個別コモンネームの削除

個別コモンネームを削除するには:

1 以下のいずれかを実行します。

- 「**設定**」列で、個別コモンネームの**削除**アイコンを選択します。

- 「**除外**」で名前を選択したうえで、「**削除**」ボタンを選択します。
- 「**すべて削除**」を選択すると、すべてのコモンネームが削除されます。確認メッセージが表示されます。「**OK**」を選択します。

2 「**適用**」を選択します。

接続エラーの表示

SonicOS は、最近の DPI-SSL クライアント関連の接続エラーのリストを保持しています。これは以下の点で有効性の高い機能です。

- DPI-SSL によってエラーになった接続をリスト表示
- エラーになった接続を監査可能
- 不具合のあるドメインを自動的に除外する仕組みを提供

ダイアログには、実行時の接続エラーが表示されます。接続エラーは、以下の理由のいずれかによって発生する可能性があります。

- クライアントとのハンドシェイクの失敗
- サーバとのハンドシェイクの失敗
- Client Hello 内のドメイン名の検証の失敗
- サーバの認証の失敗 (サーバ証明書の発行者が信頼できない)

このエラー リストは実行時にのみ利用可能です。エラーごとにログに記録される数値は、1 つのエラー種別でバッファ全体の領域を超過することがないように、制限されています。

接続エラー リストを使用するには、以下の手順に従います。

1 「**接続失敗の表示**」ボタンを選択します。「**接続エラーリスト**」ダイアログが表示されます。

このリストの各エントリには、次の項目が表示されます。

- **クライアント アドレス**

- **サーバ アドレス**
- **コモンネーム** - 接続に失敗したドメインのコモンネームです。このエントリは、自動除外リストに追加する前に、インラインで編集できます。
- **エラー メッセージ** - この接続の除外について適切な判断ができるように、接続に関連付けられたコンテキスト情報を提供します。

2 除外リストにエントリを追加するには、以下の手順に従います。

a 項目を選択します。

b エントリを編集します。

c 「**除外**」ボタンを選択します。

3 エントリを削除するには、以下の手順に従います。

a エントリを選択します。

b 「**消去**」ボタンを選択します。

4 すべてのエントリを削除するには、「**すべて消去**」ボタンを選択します。

5 終了したら、「**閉じる**」ボタンを選択します。

既定除外を手動で更新する

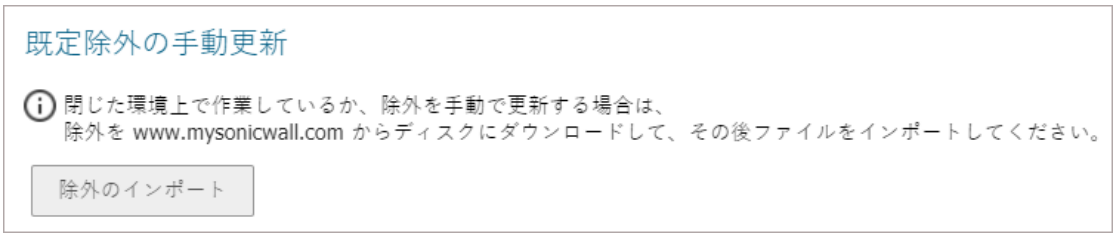
環境が閉じている場合、または既定除外を手動で更新する場合は、www.mysonicwall.com から既定除外データベースをダウンロードしてインポートできます。

既定除外を手動で更新するには:

1 www.mysonicwall.com から既定除外データベースをインポートします。

2 「**管理 | セキュリティ設定 > 復号化サービス > DPI-SSL/TLS クライアント**」ページに移動します。

3 「**既定除外の手動更新**」セクションまでスクロールします。



4 「**除外のインポート**」を選択します。「**既定除外のインポート**」ダイアログが表示されます。

5 「**ファイルを選択**」を選択します。「**ファイルのアップロード**」ダイアログが表示されます。

6 ダウンロードした既定除外データベース ファイルを開きます。

「**DPI SSL 既定除外状況**」セクションで、「**コモンネーム除外/包含**」テーブルと、ファイアウォールで使用されている既定のデータベースの状況が更新されます。

CFS 種別基準の除外/包含の指定

コンテンツ フィルタ種別によってエンティティを除外/包含できます。

CFS 種別基準の除外/包含を指定するには、以下の手順に従います。

1 「**管理 | セキュリティ設定 > 復号化サービス > DPI-SSL/TLS クライアント**」ページに移動します。

2 「**CFS 種別基準の除外/包含**」を選択します。

リストの状況は、ビューの一番上にあるアイコンで示されます。緑のアイコンはコンテンツ フィルタがライセンスされていることを示し、赤いアイコンはライセンスされていないことを示します。このアイコンにマウス カーソルを合わせると、ポップアップで状況が表示されます。

3 選択した種別を含めるか除外するかを選択するには、次のどちらかを選択します。

- **除外** (既定)
- **包含**

既定では、すべての種別の選択が解除されています。

4 包含/除外する種別を選択します。すべての種別を選択する場合は、「**すべての種別を検閲する**」チェックボックスを選択します。

5 必要に応じて、ステップ 3 およびステップ 4 を繰り返して、他方のリストを作成します。

6 また、ドメインのコンテンツ フィルタ種別情報が DPI-SSL で利用可能でない場合に接続を除外するために、「**コンテンツ フィルタ種別を使用できない場合に接続を除外する**」チェックボックスをオンにすることもできます。このオプションは、既定では選択されていません。

ほとんどの場合、HTTPS ドメインの種別情報は、ファイアウォール キャッシュにおいてローカルで利用可能です。種別情報がローカルで利用可能でない場合、DPI-SSL は、クライアントまたはサーバ通信を遮断することなく、種別情報をクラウドから取得します。まれに、DPI-SSL が判断を行うための種別情報が利用可能でない場合があります。既定では、そのようなサイトが DPI-SSL で検査されます。

7 「**適用**」を選択します。

クライアント DPI-SSL の例

トピック:

- コンテンツ フィルタ (269 ページ)
- アプリケーション ルール (271 ページ)

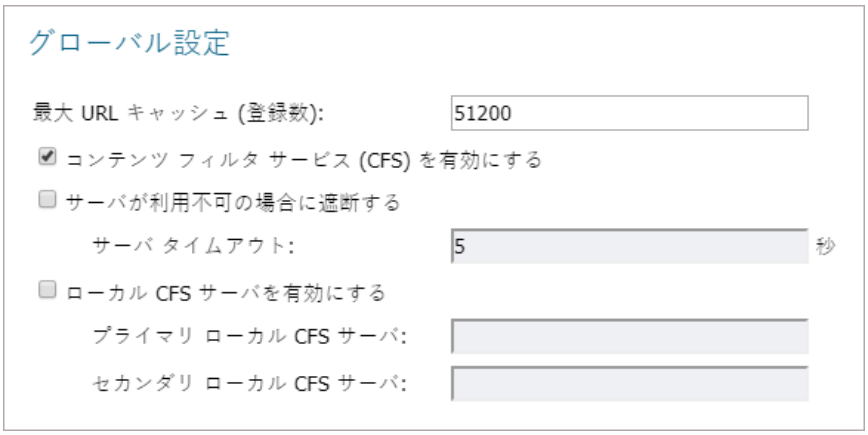
コンテンツ フィルタ

HTTPS および SSL ベースのトラフィック上で SonicWall のコンテンツ フィルタの実行に DPI-SSL を使用するには:

1 「**管理 | セキュリティ設定 > セキュリティ サービス > コンテンツ フィルタ**」に移動します。

2 「**コンテンツ フィルタ種別**」としてドロップダウン メニューで「**SonicWall CFS**」が選択されていることを確認します。

3 「**グローバル設定**」セクションまでスクロールします。

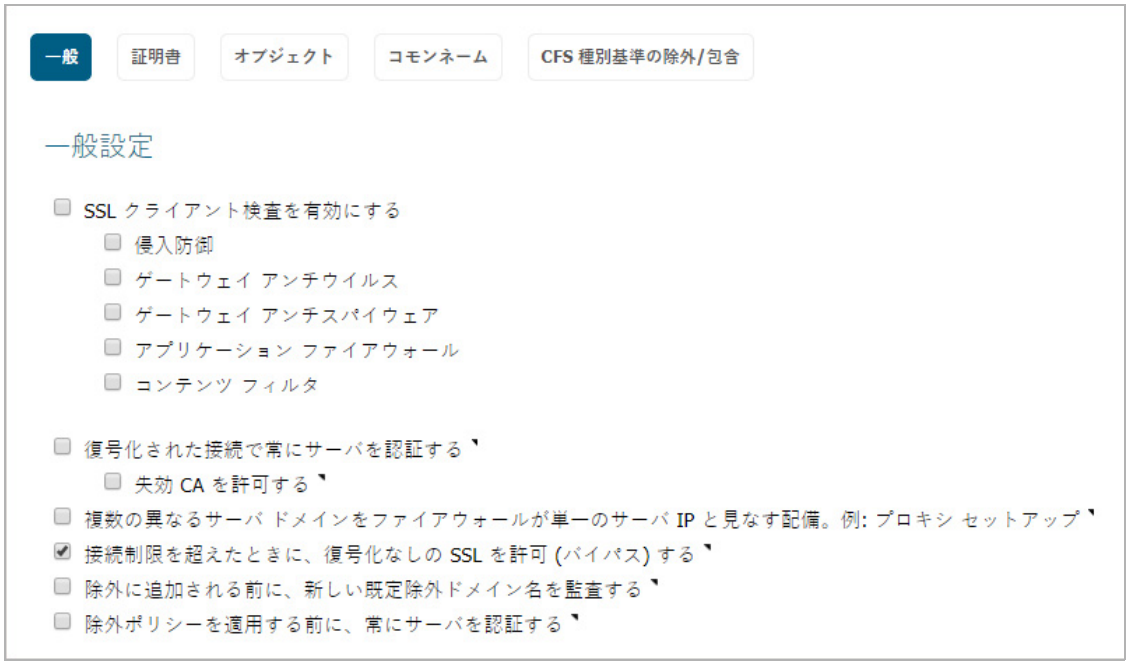


4 「**コンテンツ フィルタ サービス (CFS) を有効にする**」を選択します。

5 「**適用**」を選択します。

6 「**管理 | セキュリティ設定 > 復号化サービス > DPI-SSL/TLS クライアント**」ページに移動します。

7 「**一般**」を選択します。



8 「**SSL クライアント検査を有効にする**」チェックボックスをオンにします。

9 「**コンテンツ フィルタ**」チェックボックスをオンにします。

10 「**適用**」を選択します。

11 HTTPS プロトコルを使用して、遮断されるサイトに移動し、適切に遮断されることを確認します。

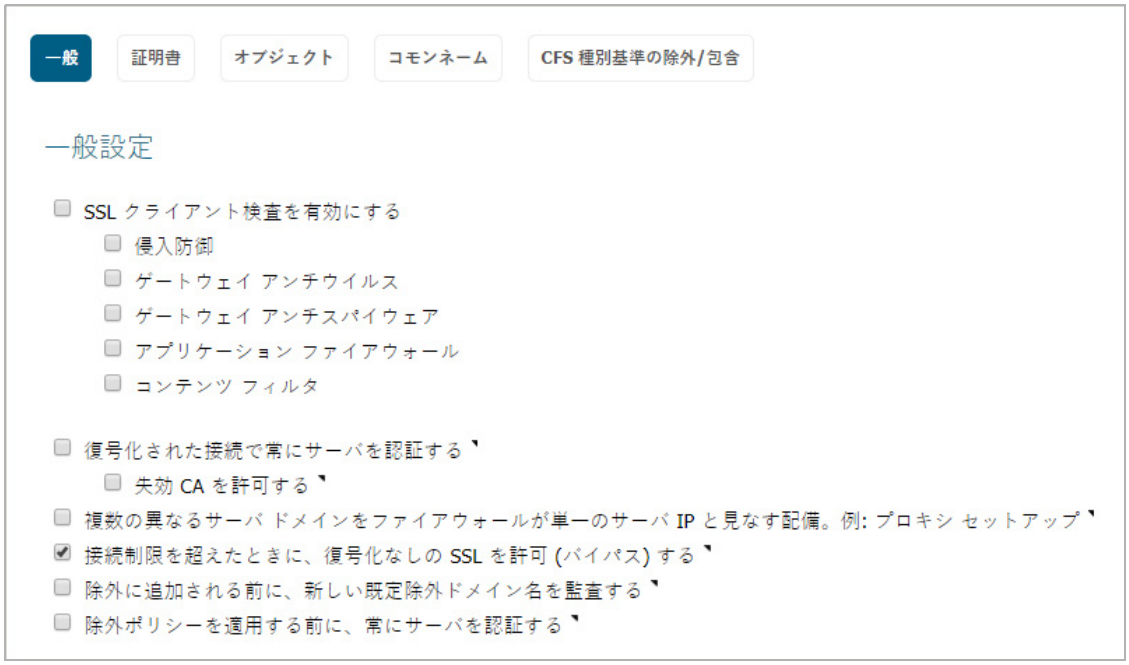
メモ：DPI-SSL 上のコンテンツ フィルタで HTTPS アクセスを初めて遮断したときには、空白のページが表示されます。ページを更新すると、ファイアウォールの遮断ページが表示されます。

アプリケーション ルール

アプリケーション ファイアウォール ルールでフィルタリングするには、「**管理 | セキュリティ設定 > 復号化サービス > DPI-SSL/TLS クライアント** 」ページと「**管理 |ポリシー > ルール > アプリケーション制御** 」ページの両方でルールを有効にする必要があります。

1 「**管理 | セキュリティ設定 > 復号化サービス > DPI-SSL/TLS クライアント**」ページに移動します。

2 「**一般**」を選択します。



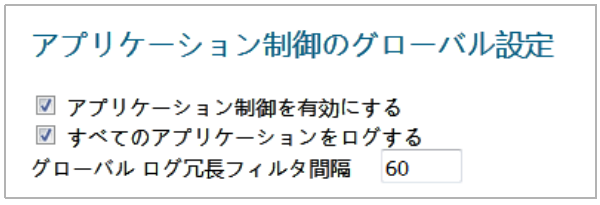
3 「**SSL クライアント検査を有効にする**」チェックボックスをオンにします。

4 「**アプリケーション ファイアウォール**」チェックボックスをオンにします。

5 「**適用**」を選択します。

6 「**管理 |ポリシー > ルール > アプリケーション 制御**」ページに移動します。

7 「**アプリケーション ルールのグローバル設定**」セクションまでスクロールします。



8 「**アプリケーション制御を有効にする**」を選択します。このオプションは、既定では選択されていません。

9 ポリシーの動作として「**ページの遮断**」を設定し、Microsoft Internet Explorer ブラウザを遮断するように、HTTP クライアント ポリシーを設定します。アプリケーション ルールの設定方法については、『*SonicWall SonicOS 6.5 ポリシー*』を参照してください。

10 「**適用**」を選択します。

11 Internet Explorer から HTTPS プロトコルで任意のウェブサイトにアクセスし、遮断されることを確認します。

22

DPI-SSL/TLS サーバの設定

- 復号化サービス > DPI-SSL/TLS サーバ (272 ページ)
- DPI-SSL/TLS サーバの設定 (273 ページ)

復号化サービス > DPI-SSL/TLS サーバ

メモ：DPI SSL については、DPI-SSL について (248 ページ) を参照してください。

通常、サーバ DPI-SSL の配備シナリオは、リモート クライアントが WAN 経由で接続してファイアウォールの LAN 上のコンテンツにアクセスするときに、HTTPS トラフィックを検査するために使用します。サーバ DPI-SSL では、アドレス オブジェクトと証明書のペアリングを設定できます。アドレス オブジェクトへの SSL 接続を検出した装置は、ペアリングされた証明書を提示し、接続するクライアントと SSL のネゴシエーションを行います。

その後、ペアリングでサーバがクリアテキストと定められている場合は、サーバの元の (NAT 再割付後の) ポートに対して標準の TCP 接続が行われます。ペアリングがクリアテキストと定められていない場合、サーバへの SSL 接続がネゴシエーションされます。これにより、接続のエンドツーエンドの暗号化に対応できます。

メモ：この配備方針では、ファイアウォールの所有者が元のコンテンツ サーバの証明書と秘密鍵を所持しています。サーバの元の証明書を装置にインポートし、サーバ DPI-SSL の UI で、サーバ IP アドレスとサーバ証明書の適切な割付を作成する必要があります。

DPI-SSL/TLS サーバの設定

トピック:

- DPI-SSL/TLS サーバの一般設定 (273 ページ)
- 除外と包含の設定 (273 ページ)
- サーバと証明書のペアリングの設定 (274 ページ)

DPI-SSL/TLS サーバの一般設定

サーバDPI-SSL 検査を有効にするには:

1 「**管理 | セキュリティ設定 > 復号化サービス > DPI-SSL/TLS サーバ**」ページに移動します。

2 「**一般設定**」セクションまでスクロールします。

3 「**SSL サーバ検査を有効にする**」を選択します。

4 検査を実行するサービスを 1 つ以上選択します。

- **侵入防御**
- **ゲートウェイ アンチウイルス**
- **ゲートウェイ アンチスパイウェア**
- **アプリケーション ファイアウォール**

5 「**適用**」を選択します。

6 「**SSL サーバ**」セクションにスクロールして、DPI-SSL 検査を適用するサーバを設定します。サーバと証明書のペアリングの設定 (274 ページ) を参照してください。

除外と包含の設定

既定では、DPI-SSL を有効にすると、装置のすべてのトラフィックに適用されます。包含/除外リストを設定すると、DPI-SSL 検査を適用するトラフィックをカスタマイズできます。**包含/除外**リストでは、オブジェクトまたはグループを指定できます。大量のトラフィックを処理する配備において、DPI-SSL が CPU に及ぼす影響を軽減し、DPI-SSL 検査の同時接続が最大数に達するのを防ぐために、信頼できる送信元を除外することが有効となる場合があります。

DPI-SSL サーバ検査をカスタマイズするには:

1 「**管理 | セキュリティ設定 > 復号化サービス > DPI-SSL/TLS サーバ**」ページに移動します。

2 「**包含/除外**」セクションまでスクロールします。

3 「**アドレス オブジェクト/グループ**」の「**除外**」から、DPI-SSL 検査から除外するアドレス オブジェクト/グループを選択します。既定では、「**除外**」は「**なし**」に設定されています。

4 「**アドレス オブジェクト/グループ**」の「**包含**」から、DPI-SSL 検査に含めるアドレス オブジェクト/グループを選択します。既定では、「**包含**」は「**すべて**」に設定されています。

> **ヒント：** 「**包含**」は、指定した除外リストを微調整するために使用できます。例えば、「**除外**」から **Remote-office-California** アドレス オブジェクトを選択し、「**包含**」から **Remote-office-Oakland** アドレス オブジェクトを選択します。

5 「**ユーザ オブジェクト/グループ**」の「**除外**」から、DPI-SSL 検査から除外するアドレス オブジェクト/グループを選択します。既定では、「**除外**」は「**なし**」に設定されています。

6 「**ユーザ オブジェクト/グループ**」の「**包含**」から、DPI-SSL 検査に含めるアドレス オブジェクト/グループを選択します。既定では、「**包含**」は「**すべて**」に設定されています。

7 「**適用**」を選択します。

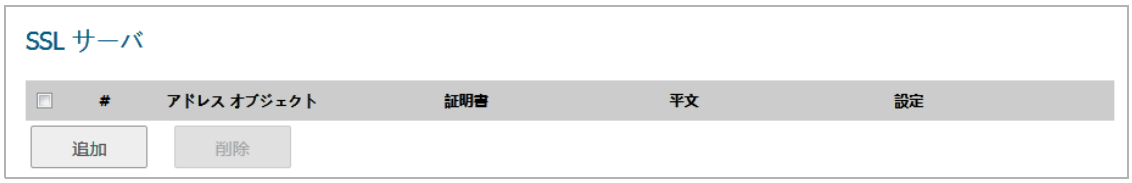
サーバと証明書のペアリングの設定

サーバ DPI-SSL の検査では、トラフィックに対して DPI-SSL 検査を実行する各サーバへのトラフィックの署名にどの証明書を使用するかを指定する必要があります。

サーバと証明書のペアリングを設定するには:

1 「**管理 | セキュリティ設定 > 復号化サービス > DPI-SSL/TLS サーバ**」ページに移動します。

2 「**SSL サーバ**」セクションまでスクロールします。



3 「**追加**」を選択します。「**SSL サーバの設定**」ダイアログが表示されます。

4 「**アドレス オブジェクト/グループ**」で、DPI-SSL 検査を適用するサーバに対応するアドレス オブジェクト/グループを選択します。

5 「**SSL 証明書**」で、サーバへのトラフィックの署名に使用する証明書を選択します。詳細情報の参照先は次のとおりです。

- 装置への新しい証明書のインポートについては、再署名認証局の選択 (259 ページ) を参照してください。
- Linux 証明書の作成については、『*SonicWall SonicOS 6.5 システム セットアップ*』を参照してください。

ヒント： (証明書の管理) リンクをクリックすると、「**管理 | システム セットアップ > 装置 > 証明書**」ページが表示されます。

6 SSL オフロードを有効にするには、「**平文**」を選択します。サーバと証明書のペアリングを追加するとき、「**平文**」オプションを使用すると暗号化されていないデータをサーバに送信できます。このオプションは、既定では選択されていません。

重要：この設定が適切に動作するためには、このサーバに対する NAT ポリシーを「**管理 | ポリシー > ルール > NAT ポリシー**」ページで作成し、オフロード サーバに対するトラフィックを SSL ポートから非SSL ポートに割り付ける必要があります。トラフィックは、443 以外のポートに送信する必要があります。例えば、SSL オフロードで HTTPS トラフィックを使用している場合、適切な動作のためには、トラフィックをポート 443 からポート 80 に再割付する受信 NAT ポリシーを作成する必要があります。

7 「**追加**」を選択します。

23

DPI-SSH の設定

- DPI-SSH について
- DPI-SSH ライセンスの有効化
- DPI-SSH の設定

DPI-SSH について

重要：アンチスパイウェアの TCP ストリームはサポートされないので、DPI-SSH についてはゲートウェイ アンチスパイウェア サービスは機能しません。このオプションをオンにしても何も実行されません。

精密パケット検査 (DPI) は、通過するトラフィックをパケットの第 3 層および第 4 層の内容のシグネチャに基づいてパケット フィルタ ファイアウォールで分類できるようにする技術です。DPI は、パケットのペイロードの内容 (第 7 層アプリケーション データ) を記述する情報も提供します。DPI は、SonicWall ファイアウォールを通過するパケットのデータおよびヘッダーを調べる SonicOS の既存の機能であり、プロトコル違反、ウイルス、スパム、侵入、または定義済みの条件がないか検索して、パケットを通過させるかどうか、また、他の処理や追跡のために別の送信先へルーティングするかどうかを判断します。

SSH (セキュア シェル) は、ネットワークに接続された 2 台のコンピュータ間で、保護されたデータ通信、リモート コマンドライン ログイン、リモート コマンド実行、その他の保護されたネットワーク サービスを利用するための暗号化ネットワーク プロトコルです。SSH は、保護されていないネットワーク上の保護されたチャネルを介して、SSH サーバ プログラムを実行するサーバと SSH クライアント プログラムを実行するクライアントを接続します。このプロトコルには、SSH-1 および SSH-2 という 2 つのバージョンがあります。SonicWall では SSH-2 のみをサポートしています。SSH-1 のセッションはインターセプトされず、検査されません。

重要：異なるバージョン番号の SSH クライアントを同時に使用することはできません。

SSH などの暗号化されたメッセージを効果的に検査するには、先にペイロードを復号化します。DPI-SSH は、中間者 (MITM) やパケット プロキシとしての役割を果たします。事前設定のエンドツーエンド通信は切断され、事前共有鍵は使用できません。

DPI-SSH は 1 つの SSH トンネルを 2 つのトンネルに分割し、両方のトンネルからのパケットを復号化して検査を実行します。パケットが DPI の検査で合格した場合、DPI-SSH は再暗号化したパケットをトンネルに送信します。パケットが検査で不合格だった場合は、ポリシーに基づいて別の送信先にルーティングされるか、統計情報収集用に送信され、DPI-SSH は接続をリセットします。

トピック:

- サポートされるクライアント/サーバと接続数 (277 ページ)
- サポートされる鍵交換アルゴリズム (277 ページ)
- 注意 (277 ページ)

サポートされるクライアント/サーバと接続数

SSH はシェルではなく、保護されたチャネルであり、このチャネル (トンネル) を介して、シェル、ファイル転送、X11 転送など、さまざまなサービスを提供します。

DPI-SSH では、ルート モードとワイヤ モードの両方がサポートされます。ワイヤ モードでは、DPI-SSH は保護 (直列トラフィックのアクティブ DPI) モードでのみサポートされます。ルート モードでは、制限はありません。

SSH がサポートする各種のクライアントとサーバの実装をサポートされるクライアント/サーバ テーブルに示します。

サポートされるクライアント/サーバ

サポートされる DPI-SSH クライアント	サポートされる DPI-SSH サーバ
Cygwin 用の SSH クライアント	Fedora の SSH サーバ
Putty	Ubuntu の SSH サーバ
secureCRT	
Ubuntu の SSH	
CentOS の SSH	
Cygwin の SFTP クライアント	
Cygwin の SCP	
Winscp	

DPI-SSH がサポートする最大接続数は 250 です。

サポートされる鍵交換アルゴリズム

DPI-SSH では、以下の鍵交換アルゴリズムがサポートされます。

- Diffie-Hellman-group1-sha1
- Diffie-Hellman-group14-sha1
- ecdh-sha2-nistp256

DPI-SSH は、クライアント側で DSA 鍵、サーバ側で RSA 鍵をサポートします。

注意

ローカル マシンに SSH サーバ鍵が既に保存されている場合は、それを削除する必要があります。例えば、サーバに対して SSH を既に使用していて、サーバ DSS 鍵が保存されている場合、DSS 鍵をローカル ファイルから削除しないと SSH セッションが失敗します。

`ssh-keygen` ユーティリティを使用してもパスワードをバイパスできません。

Putty では GSSAPI が使用されます。このオプションは SSH2 専用で、より強力な暗号化認証を利用できます。最初の通信時に、ローカルのトークンまたは鍵がローカル クライアントとサーバに保存されます。ただし、メッセージと処理は DPI-SSH の開始前に交換されるので、DPI-SSH は GSSAPI トークンを含めて、開始前に交換された内容については関知しません。GSSAPI オプションが有効になっていると DPI-SSH は失敗します。

クライアント側では、DPI-SSH が有効になっている場合、SSH 2.x または 1.x クライアントを使用できます。ただし、異なるバージョン番号のクライアントを同時に使用することはできません。

ゲートウェイ アンチスパイウェア検査とアプリケーション ファイアウォール検査は、「**管理 | セキュリティ設定 > 復号化サービス > DPI-SSH**」ページでこれらのオプションを選択してもサポートされません。

DPI-SSH ライセンスの有効化

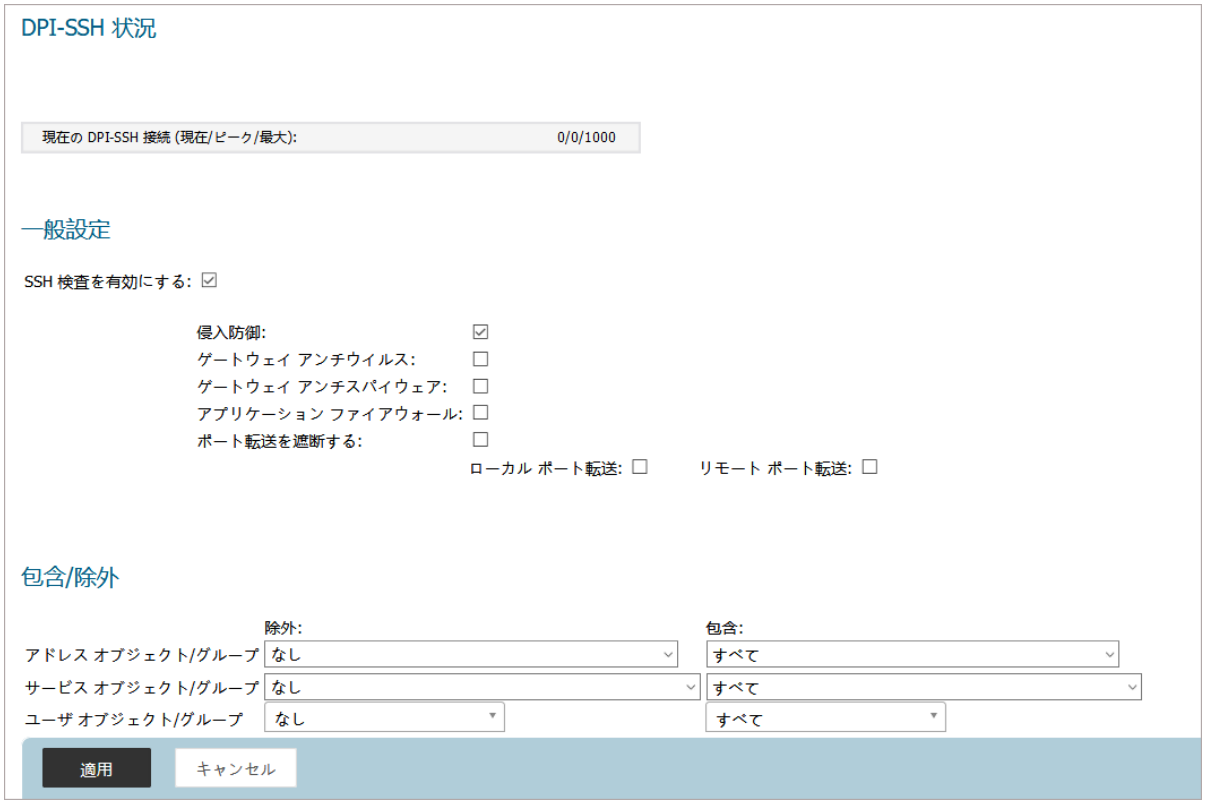
DPI-SSH は既定でフルライセンスされていますが、ライセンスを有効化する必要があります。最初に「**管理 | セキュリティ設定 > 復号化サービス > DPI-SSH**」を選択すると、メッセージが表示されます。「アップグレードが必要です」というメッセージが表示されます。

アップグレードが必要ない場合は、DPI-SSH の設定 (278 ページ) に進んでください。ライセンスのアクティブ化の詳細については、装置の『*クイック スタート ガイド*』を参照してください。

DPI-SSH の設定

重要：アンチスパイウェアの TCP ストリームはサポートされないので、DPI-SSH についてはゲートウェイ アンチスパイウェア サービスは機能しません。これに該当するチェックボックスをオンにしても何も実行されません。

「**管理 | セキュリティ設定 > 復号化サービス > DPI-SSH**」ページで DPI-SSH を設定します。



トピック:

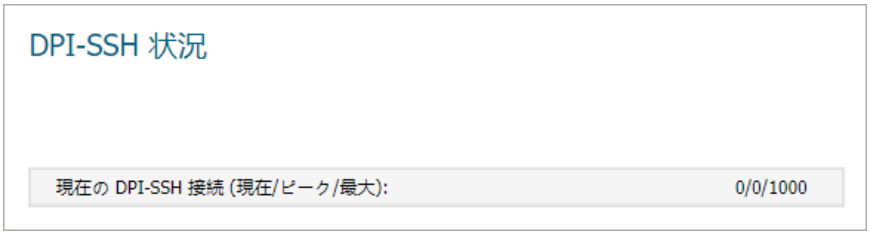
- 接続状況の表示 (279 ページ)
- クライアント DPI-SSH 検査の設定 (280 ページ)
- クライアント DPI-SSH 検査のカスタマイズ (282 ページ)

接続状況の表示

DPI-SSH 接続の状況を表示するには:

1 「**管理 | セキュリティ設定 > 復号化サービス > DPI-SSH**」に移動します。

2 「**DPI-SSH 状況**」までスクロールします。



状況には以下の値が示されます。

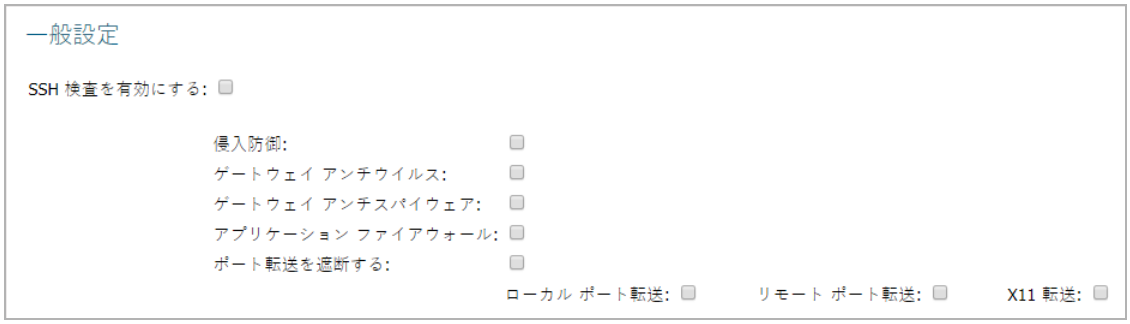
- 現在の DPI-SSH 接続数
- ピーク時の DPI-SSH 接続数
- DPI-SSH 接続の最大数

クライアント DPI-SSH 検査の設定

クライアント DPI-SSH 検査は、「**復号化サービス > DPI-SSH**」の「**一般設定**」セクションで設定します。

クライアント DPI-SSH 検査を有効にするには:

1 「**一般設定**」セクションで、「**SSH 検査を有効にする**」オプションを選択します。 このオプションは、既定では選択されていません。



2 以下のサービス検査の中から 1 つ以上の種別を選択します。既定では何も選択されていません。

- **侵入防御**
- **ゲートウェイ アンチウイルス**
- **ゲートウェイ アンチスパイウェア**

  重要：アンチスパイウェアの TCP ストリームはサポートされないので、DPI-SSH についてはゲートウェイ アンチスパイウェア サービスは機能しません。このオプションをオンにしても何も実行されません。

- **アプリケーション ファイアウォール**
- **ポート転送を遮断する**: これらのオプションの詳細については、ポート転送の DPI-SSH 遮断 (280 ページ) を参照してください。
  - **ローカル ポート転送**
  - **リモート ポート転送**
  - **X11 転送**

3 「**適用**」を選択します。

ポート転送の DPI-SSH 遮断

SSH ではポート転送を使用して、SSH 経由で他のアプリケーションに接続するトンネルを作成することができます。ポート転送では、ローカルまたはリモート コンピュータ (インターネット上のコンピュータなど) が、プライベート LAN 内の特定のコンピュータまたはサービスに接続できます。ポート転送により、パケットは、そのアドレスまたはポート番号が新しい送信先アドレスに変換され、ルーティング ルールに従ってその送信先に転送されます。これらのパケットは新しい送信先とポート番号を持つため、ファイアウォールのセキュリティ ポリシーを回避する可能性があります。

SonicWall ネットワーク セキュリティ装置のアプリケーションベースのセキュリティ ポリシーが回避されるのを防ぐために、SonicOS では、ローカルとリモートの両方のポート転送に対し、SSH ポート転送機能の遮断がサポートされています。

- *ローカルのポート転送*によって、ローカル ネットワークのコンピュータは別のサーバに接続できます。それは外部サーバである場合もあります。
- *動的ポート転送*では、1 つのローカルポートを、リモートのすべての宛先にデータをトンネルで送信するよう設定できますが、これは、*ローカル ポート転送*の特殊なケースと見なされるでしょう。
- *リモート ポート転送*では、リモート ホストを内部サーバに接続できます。

SSH ポート転送は、次のサーバをサポートしています。

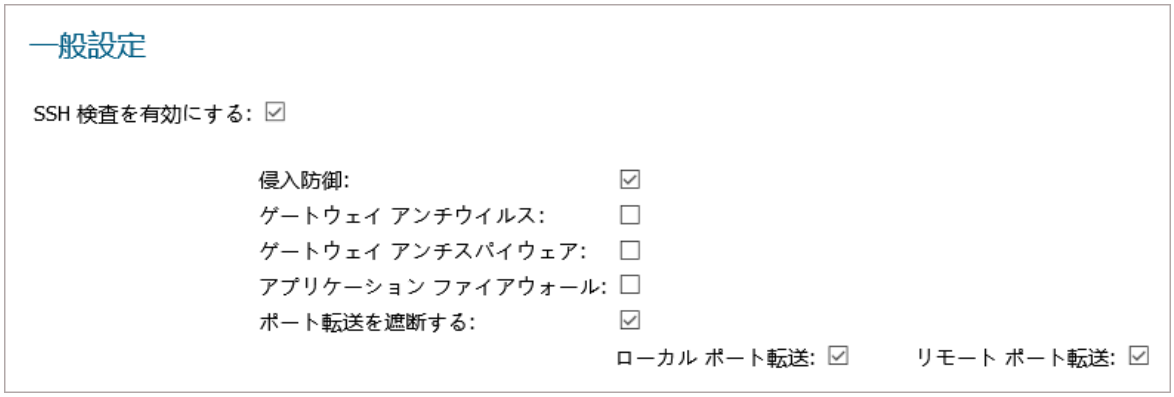
- Fedora の SSH サーバ
- Ubuntu の SSH サーバ

SSH ポート転送は以下の両方をサポートしています。

- ルート モード
- ワイヤ モード - 保護モードのみでサポートされます

SSH ポート転送と DPI-SSH ポート転送はともに、最大 1000 接続をサポートします。

SSH ポート転送の機能を遮断するには、DPI-SSH を有効にする必要があります。遮断機能が有効になっている場合にローカルまたはリモート ポート転送が実行されると、SonicOS が、これらの要求を遮断し、接続をリセットします。



SSH ポート転送の遮断を有効にするには:

1 「**管理 | セキュリティ設定 > 復号化サービス > DPI-SSH**」ページに移動します。

2 「**一般設定**」セクションで、「**ポート転送を遮断する**」チェックボックスをオンにします。

3 遮断するポート転送の種類に応じて、「**ローカル ポート転送**」と「**リモート ポート転送**」のどちらかまたは両方のチェックボックスをオンにします。

4 「**適用**」を選択します。

DPI-SSH ポート転送は、次のクライアントをサポートしています。

- Cygwin 用の SSH クライアント
- Putty
- SecureCRT
- Ubuntu の SSH
- CentOS の SSH

クライアント DPI-SSH 検査のカスタマイズ

既定では、DPI-SSH を有効にすると、それがファイアウォール上のすべてのトラフィックに適用されます。「**包含/除外**」セクションで、DPI-SSH 検査を適用するトラフィックをカスタマイズできます。

DPI-SSH クライアント検査をカスタマイズするには:

1 「**復号化サービス > DPI-SSH**」ページの「**包含/除外**」セクションに移動します。

2 「**アドレス オブジェクト/グループ**」の「**除外**」と「**包含**」のドロップダウン メニューで、DPI-SSH 検査に対して除外/包含するアドレス オブジェクト/グループを選択します。既定では、「**除外**」は「**なし**」、「**包含**」は「**すべて**」に設定されています。

3 「**サービス オブジェクト/グループ**」の「**除外**」と「**包含**」のドロップダウン メニューで、DPI-SSH 検査に対して除外/包含するアドレス オブジェクト/グループを選択します。既定では、「**除外**」は「**なし**」、「**包含**」は「**すべて**」に設定されています。

4 「**ユーザ オブジェクト/グループ**」の「**除外**」と「**包含**」のドロップダウン メニューで、DPI-SSH 検査に対して除外/包含するアドレス オブジェクト/グループを選択します。既定では、「**除外**」は「**なし**」、「**包含**」は「**すべて**」に設定されています。

5 「**適用**」を選択します。

第 4 部

セキュリティ 設定 | アンチスパム

重要:アンチスパムは、SuperMassive シリーズまたは NS*a* 9250 以降のファイアウォールではサポートされていません。

- アンチスパムについて
- アンチスパムの有効化とアクティブ化
- アンチスパム ログの設定
- RBL フィルタの設定
- 中継ドメインの指定
- ジャンク ボックス設定の構成
- ジャンク サマリの管理
- ジャンク ボックスの表示の設定
- ユーザに表示される設定の構成
- 企業の許可および遮断リストの設定
- ユーザの管理
- LDAP サーバの設定
- Anti-Spam Desktop ボタンのダウンロード

24

アンチスパムについて

重要：アンチスパムは、SuperMassive シリーズまたは NS*a* 9250 以降のファイアウォールではサポートされていません。

メモ：アンチスパムは、既存のファイアウォールにアンチスパム、アンチフィッシング、およびアンチウイルスの各機能を追加する手軽で効率的かつ効果的な方法を提供する個別にライセンスされた機能です。

- アンチスパムについて (284 ページ)
- アンチスパム サービスの仕組み (285 ページ)
- アンチスパム ライセンスの購入 (290 ページ)

アンチスパムについて

トピック:

- アンチスパムとは (284 ページ)
- メリット (285 ページ)

アンチスパムとは

アンチスパム機能は、既存のファイアウォールにアンチスパム、アンチフィッシング、およびアンチウイルスの各機能を追加する手軽で効率的かつ効果的な方法を提供します。

アンチスパムの一般的な設定では、管理者が SonicOS インターフェースでアンチスパムを選択してそのライセンス処理を行うことによって、アンチスパム機能の追加できます。その後、ファイアウォールでは、SonicWall Email Security 製品と同じ高度なスパム フィルタ技術を使用して、ユーザに配信されるジャンク電子メールの量を削減できます。

アンチスパム機能によって受信メッセージを分析する方法として、主に次の 2 つがあります。

- 高度な IP 評価管理
- クラウドベースの高度なコンテンツ管理

IP アドレス評価では、GRID ネットワークを使用して既知のスパム送信者の IP アドレスを識別し、こうした送信者からメールはすべて接続の許可さえ行わずに拒否します。GRID ネットワーク送信者 IP 評価管理では、着信接続要求の IP アドレスを一連のリストおよび統計情報と照合して、その接続によって有用な電子メールが配信される可能性があるかどうかを確認します。こうしたリストは、SonicWall GRID ネットワークの協調インテリジェンスを使用して収集されます。既知のスパム送信者

はファイアウォールに接続できないため、そうした送信者によるジャンク電子メールのペイロードによってターゲット システムのシステム リソースが消費されることは決してありません。

既知のスパム送信者から届いたものではない電子メールは、"GRID プリント" に基づいて分析されます。GRID プリントは、SonicWall の研究所で生成され、何百万というビジネス エンドポイント、何億というメッセージ、および GRID ネットワークのユーザからの何十億という評価の投票に基づいています。弊社の GRID ネットワークは、複数の SonicWall ソリューションからのデータを使用して、世界中の脅威のランドスケープに対する防御となる協調インテリジェンス ネットワークを作成しています。GRID プリントは、電子メール メッセージに含まれるデータを外部にさらすことなくメッセージを一意に識別します。

アンチスパム サービスでは、ある電子メールが適合する脅威はスパム、スパム可能性大、フィッシング、フィッシング可能性大、ウイルス、ウイルス可能性大のいずれか *1 つのみ*であると判断します。電子メール メッセージ内の脅威を評価する際には、次の優先順位が使用されます。

- フィッシング
- フィッシングの可能性大
- ウイルス
- ウイルスの可能性大
- スパム
- スパム可能性大

例えば、メッセージがウイルスとスパムの両方に該当する場合、スパムよりウイルスの優先順位が高いため、メッセージはウイルスとして分類されます。

アンチスパム サービスによって上記の脅威の*いずれでもない*と判断されたメールは、良性の電子メールと見なされ、送信先サーバに配信されます。

メリット

アンチスパム保護をファイアウォールに追加すると、ジャンク メッセージがユーザの受信箱に届いてユーザの目に触れる前に検閲されて拒否されるので、システム全体としての効率性が向上します。

- ネットワーク内のジャンク電子メールによって消費される帯域幅およびリソース量の削減
- メール サーバに送信される受信メッセージ数の削減
- 組織に対する脅威の軽減 (ユーザがウイルス スパムを選択して不意にコンピュータに感染させる可能性がないため)
- フィッシング攻撃からのユーザ保護の強化

アンチスパム サービスの仕組み

このセクションでは、SonicWall GRID ネットワークを含むアンチスパム機能について、またこの機能全体として SonicOS とどのように相互作用するのかを説明します。SonicOS との重要な接続でポイントとなるのが、アドレス オブジェクトとサービス オブジェクトの 2 つです。アドレスおよびサービス オブジェクトは、アンチスパム機能を SonicOS で円滑に機能するように設定するために使用します。例えば、受信電子メールをアーカイブすると共にフィルタを介して送信するように NAT ポリシーを設定するには、アンチスパム サービス オブジェクトを使用します。

包括的なアンチスパム サービスは、メッセージのヘッダーと内容を分析し、協調 GRID プリントを使用してスパム電子メールを遮断します。

トピック:

- GRID ネットワーク (286 ページ)
- アドレスおよびサービス オブジェクト (287 ページ)

GRID ネットワーク

送信者 IP 評価機能を備えた GRID 接続管理は、SonicWall Email Security と SonicOS のアンチスパム サービスで使用されます。GRID ネットワーク送信者 IP 評価は、特定の IP アドレスが SonicWall GRID ネットワークのメンバーに関して持つ評価です。この機能を有効にすると、評価の悪い IP アドレスからの電子メールは受け付けられません。SonicOS が既知の悪性 IP アドレスからの接続を許可しない場合は、そうした IP アドレスからのメールが電子メール サーバに届くことは決してありません。

GRID ネットワーク送信者 IP 評価では、着信接続要求の IP アドレスを一連のリストおよび統計情報と照合して、その接続によって有用な電子メールが配信される可能性があるかどうかを確認します。こうしたリストは、SonicWall GRID ネットワークの協調インテリジェンスを使用して収集されます。既知のスパム送信者はファイアウォールに接続できないため、そうした送信者によるジャンク電子メールのペイロードによってターゲット システムのシステム リソースが消費されることは決してありません。

トピック:

- メリット
- 送信者 IP 評価による GRID 接続管理と接続管理の優先順位

メリット

- 80 パーセントものジャンク電子メールがネットワーク内に受け入れられる前に接続レベルで遮断されます。スパム保護のレベルを維持するのに必要なリソースが減少します。
- サーバでのジャンク電子メールの受信に帯域幅が浪費されることがなく、その分析と削除だけで済みます。
- グローバル ネットワークが、スパム送信者を監視し、正規のユーザによる自らの IP 評価の保存 (必要な場合) に役立ちます。

送信者 IP 評価による GRID 接続管理と接続管理の優先順位

ファーストタッチ ファイアウォールに要求が送信されると、アンチスパム サービスによって要求者が '評価' されます。この評価は、既知の良性送信者のホワイト リストと既知のスパム送信者の遮断リストから、サービス拒否しきい値に基づいて収集されます。

IP 評価が有効な場合、送信元 IP アドレスが 評価順序の順で確認されます。

評価順序

評価	説明
許可リスト	このリスト上にある IP アドレスは、接続管理によってメッセージを通過させることができます。メッセージは、通常どおりにファイアウォールによって分析されます。
遮断リスト	この IP アドレスは、ファイアウォールへの接続が禁止されます。
評価リスト	これより前のリストにない IP アドレスは、ファイアウォールによってチェックされ、評価の悪い IP アドレスでないかどうかが確認されます。

評価順序

評価	説明
延期リスト	この IP アドレスからの接続は延期されます。設定されているインターバル時間が経過するまでは接続が許可されません。
DoS	これより前のリストにない IP アドレスは、ファイアウォールによってチェックされ、サービス拒否しきい値を超えていないかどうかが確認されます。しきい値を超えている場合、装置は既存の DoS 設定を使用して処置を講じます。

IP アドレスがこれらのテストにすべてパスした場合に限り、ファイアウォールはそのサーバによる接続とメールの転送を許可します。IP アドレスがこれらのテストにパスしなかった場合は、SMTP サーバが存在しないことを示す、SonicOS から要求側サーバへのメッセージが生成されます。接続要求は受け入れられません。

アドレスおよびサービス オブジェクト

SonicOS のアンチスパム機能は、顧客の電子メール サーバを管理するためのアドレスおよびサービス オブジェクトをサポートしています。これらのオブジェクトは、アンチスパム サービスの NATおよびアクセス ルール ポリシーで使用されます。自動作成されたルールは、編集不可能であり、アンチスパム サービスが無効になっても削除されることはありません。

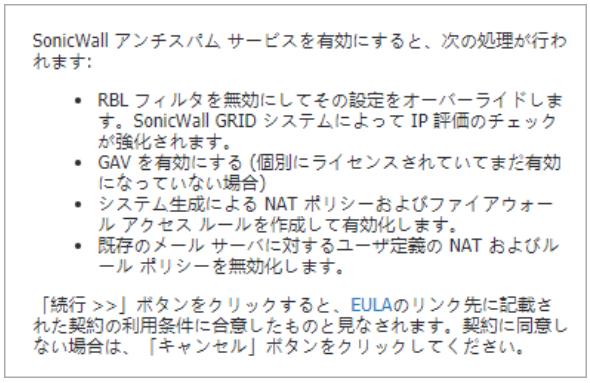
アンチスパム サービスを有効にすると、電子メール トラフィックを制御およびリダイレクトするためのNAT ポリシーとアクセス ルールが作成されます。ポリシーとルールは、「**管理 |ポリシー > ルール > NAT ポリシー**」ページに表示されますが、編集することはできません。自動作成されたこれらのポリシーは、アンチスパム サービスが有効な場合にのみ使用できます。これらのルールとポリシーの詳細については、*SonicWall SonicOS 6.5 ポリシー*を参照してください。

アンチスパム サービスがライセンスされていて有効になっている場合、「**管理 | セキュリティ設定 > アンチスパム > 基本設定**」ページにアンチスパムを有効にする 1 つのオプションが表示されます。配備済みのシナリオに対する既存の個別アクセス ルールおよび NAT ポリシーが存在しない場合、このオプションを選択すると、**送信先メール サーバ ポリシー ウィザード**が起動されます。生成されたポリシーのセットアップ時には、電子メールがファイアウォールの後にどこにルーティングされるのかをアンチスパム サービスが知っている必要があります。具体的には、送信先メール サーバの IP アドレスとそのゾーンの割り当てが必要です。**送信先メール サーバ ポリシー ウィザード**は、こうしたデータが見つからない場合に起動されます。

このウィザードでは次の情報が必要です。

- **送信先メール サーバのパブリック IP アドレス** - SMTP によって外部 MTA (メッセージ転送エージェント) が接続する IP アドレス。
- **送信先メール サーバのプライベート IP アドレス** - Exchange または SMTP サーバの (ファイアウォールの後の) 内部 IP アドレス。
- **ゾーンの割り当て** - Exchange サーバが割り当てられるゾーン。
- **受信電子メール ポート** - 電子メールの送信先となる TCP サービス ポート番号。受信 SMTP ポートとも呼ばれます。

この情報が必要な場合、次のメッセージが表示されます。



「続行」を選択して、このウィザードのリクエストを一通り確認します。

このウィザードによって作成されたポリシーおよびアドレス オブジェクトは、編集可能であり、アンチスパム サービスが無効になってもシステム内に残ります。

トピック:

- アンチスパム サービスの有効時に作成されたオブジェクト
- ウィザードによって作成されたオブジェクト
- ポリシーとオブジェクトの変更

アンチスパム サービスの有効時に作成されたオブジェクト

このセクションでは、ファイアウォール アクセス ルールや NAT ポリシーおよびサービスオブジェクトとして自動生成されたルールおよびオブジェクトの種類の例を示します。これらのオブジェクトは、編集不可能であり、アンチスパム サービスが無効になっても削除されることはありません。

「**管理 |ポリシー > ルール > アクセス ルール**」ページには、アンチスパムに使用される生成されたルールが表示されます。

#	ゾーン	> ゾーン	優先順位	送信元	送信先	サービス	動作	ユーザ	フロー報告	パケット監視	コメント	有効	設定
	WAN												
46	WAN	> LAN	1	すべて	パブリック メール サーバ アドレス グループ	SMTP (アンチスパム インバウンド ポート)	許可	すべて					
47	WAN	> LAN	2	すべて	デフォルト アクティブ WAN IP	SonicWALL Anti-Spam Service	許可	すべて					
48	WAN	> LAN	3	すべて	User Mail Server Public IP	SMTP (アンチスパム インバウンド ポート)	許可	すべて					
49	WAN	> LAN	4	すべて	すべて	すべて	許可	すべて					
50	WAN	> WAN	1	すべて	すべての X1 管理 IP	SNMP	許可	すべて					

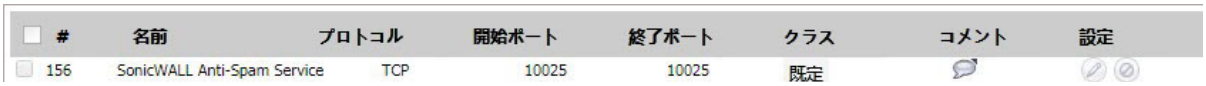
赤で囲まれた行は、アンチスパムを有効にしたときに生成されるアクセス ルールです。緑で囲まれた行は、既存のメール サーバ ポリシーが存在しない場合にアンチスパム機能によって作成される既定のルールです。

また、以下のアクセス ルールを作成することもできます。

- 任意の送信元からすべての WAN IP アドレスへの着信電子メール (SMTP) 用の WAN-WANルール

- アンチスパム サービス ポート (既定では 25 番) を使用して処理された、Email Security Service からすべての WAN IP アドレスへの電子メール用の WAN-LAN ルール

アンチスパム サービス オブジェクトは、「**ポリシー | オブジェクト > サービス オブジェクト**」ページで作成されます。



#	名前	プロトコル	開始ポート	終了ポート	クラス	コメント	設定
156	SonicWALL Anti-Spam Service	TCP	10025	10025	既定		

このサービス オブジェクトは、生成された NAT ポリシーによって参照されます。

22	すべて	デフォルト アクティブ WAN IP	パブリック メール サーバ アドレス グループ	SonicWALL Email Security Service	SMTP (アンチスパム インバウンド ポート)	SMTP (電子メール送信)	すべて	すべて	22			
23	すべて	オリジナル	パブリック メール サーバ アドレス グループ	SonicWALL Email Junk Store	SMTP (アンチスパム インバウンド ポート)	SonicWALL Anti-Spam Service	すべて	すべて	23			
24	すべて	オリジナル	デフォルト アクティブ WAN IP	Destination Mail Server Private IP	SonicWALL Anti-Spam Service	SMTP (電子メール送信)	すべて	すべて	24			
25	すべて	オリジナル	パブリック メール サーバ アドレス グループ	Destination Mail Server Private IP	SMTP (アンチスパム インバウンド ポート)	SMTP (電子メール送信)	すべて	すべて	25			
26	すべて	オリジナル	User Mail Server Public IP	User Mail Server Private IP	SMTP (アンチスパム インバウンド ポート)	SMTP (電子メール送信)	すべて	すべて	26			
27	インターフェース IP	U0 IP	すべて	オリジナル	すべて	オリジナル	すべて	U0	27			
28	すべて	オリジナル	test1	WLAN Subnets	FTP データ	Gopher	すべて	すべて	28			
29	インターフェース IP	X3 IP	すべて	オリジナル	すべて	オリジナル	すべて	X3	29			
30	インターフェース IP	X5 IP	すべて	オリジナル	すべて	オリジナル	すべて	X5	30			
31	すべて	オリジナル	デフォルト アクティブ WAN IP	SonicWALL Email Junk Store	SonicWALL Anti-Spam Service	オリジナル	すべて	すべて	31			
32	すべて	X5 IP	すべて	オリジナル	すべて	オリジナル	X4	X5	32			
33	すべて	X5 IP	すべて	オリジナル	すべて	オリジナル	X2	X5	33			
34	すべて	X5 IP	すべて	オリジナル	すべて	オリジナル	X0	X5	34			

赤で囲まれた行は、アンチスパムを有効にしたときに生成されるポリシーです。緑で囲まれた行は、既存のメール サーバ ポリシーが存在しない場合にアンチスパム機能によって作成される既定のポリシーです。

ウィザードによって作成されたオブジェクト

管理者によるウィザードとの対話によって作成されたオブジェクトは、編集可能であり、アンチスパム サービスが無効になってもシステム内に残ります。

ポリシーの自動生成には、以下の考慮事項を適用します。

- **パブリック メール サーバ アドレス グループ**と呼ばれる、システムのアドレス グループ オブジェクトが、生成されたポリシーに対する変換前の送信先の既定値として作成されます。このグループには、アドレス オブジェクトである**送信先メール サーバのパブリック IP** が含まれます。このオブジェクトは、ウィザードの実行時に与えられた IP アドレス値を取ります。
- 既に SonicWall 機器に SMTP 用の既存のポリシーがある場合には、以下の手順が実行されます。
  - 既存のポリシーの変換前の送信先がホスト タイプのアドレス オブジェクトの場合、生成されたポリシーは**パブリック メール サーバ アドレス グループ** オブジェクトを変換前の送信先として使用します。
  - 既存のポリシーの変換前の送信先が非ホスト タイプのアドレス オブジェクトの場合、生成されたポリシーはこの非ホスト タイプのアドレス オブジェクトを変換前の送信先として使用します。
  - SMTP 用のパブリック IP アドレスが 2 つ以上存在する場合、**パブリックメール サーバ アドレス グループ**にアドレス オブジェクトを手動で追加できます。

ポリシーとオブジェクトの変更

diag.html ページで「**GRID 名前キャッシュをリセットする**」ボタンを使用して、GRID 名前キャッシュ内のすべてのエントリを消去できます。

「**ポリシーとオブジェクトを削除する**」ボタンを使用して、アンチスパム アドレス、およびサービスをオフにしたときに削除されないサービス オブジェクトとポリシーを削除できます。このボタンを選択すると、自動生成されたすべてのオブジェクトとポリシーが削除されます。この操作は、アンチスパム サービスがオフの場合のみ許可されます。

もう 1 つの **diag.html** ページには、アンチスパムに関連した以下のオプションがあります。

- **アンチスパムに関係する接続に対し SYN フラッド防御を無効にする** - SMTP (25) ポートとアンチスパム サービス (10025) ポートに対して、SYN フラッド保護は既定で有効になっています。このオプションによって、保護を無効にします。
- **GRID IP レピュテーション確認だけを使用する** - このオプションを選択すると、プローブ処理の結果がオーバーライドされ、アンチスパム サービスが使用できない場合 (admin down) をシミュレートします。電子メールを送信する際、SYN フラッド チェックと GRID IP チェックのどちらも引き続き実行されますが、その他の電子メール スキャンは実行されません。

アンチスパム ライセンスの購入

アンチスパム機能を使用するために必要な配備の前提条件は、次のとおりです。

- ライセンス済みの SonicWall ネットワーク セキュリティ装置
- 装置用のアンチスパム ライセンス
- 次のいずれかの Microsoft Windows Server:
  - Windows Server 2012 R2 64 ビット
  - Windows Server 2012 (64 ビット)

- Windows SBS 2008 R2 Server (64 ビット)
- SBS 2008 (64 ビット)

ファイアウォール用のアンチスパム ライセンスは、mySonicWall.com から直接購入できるほか、再販業者からも購入できます。

メモ：使用前に、SonicWall ネットワーク セキュリティ装置を mySonicWall.com に登録する必要があります。

アンチスパム ライセンスを購入するには、以下の手順に従います。

1 SonicWall 装置の管理に使用しているコンピュータでウェブ ブラウザを開きます。

2 **場所**または**アドレス** フィールドに "**http://www.mySonicWall.com**" と入力します。

3 mySonicWall.com アカウントの**ユーザ名**と**パスワード**を適切なフィールドに入力します。

4 「**提出**」ボタンを選択します。

5 左側のナビゲーション バーで、「**私の製品**」を開きます。

6 アンチスパム機能を追加する装置を選択します。

7 アンチスパム ライセンスの登録を行います。

8 装置のウェブ管理インターフェースにログインします。

9 ナビゲーション bar.mySonicWall.com から「**管理 | 更新 > ライセンス**」ページに移動します。

10 「**セキュリティ サービスのオンライン管理**」セクションで、該当するリンクを選択して、ライセンスを有効化または更新します。あるいは、「**手動でアップグレード**」セクションで、キーまたはキーセットを入力します。

11 mySonicWall.com のログイン情報を入力します。

25

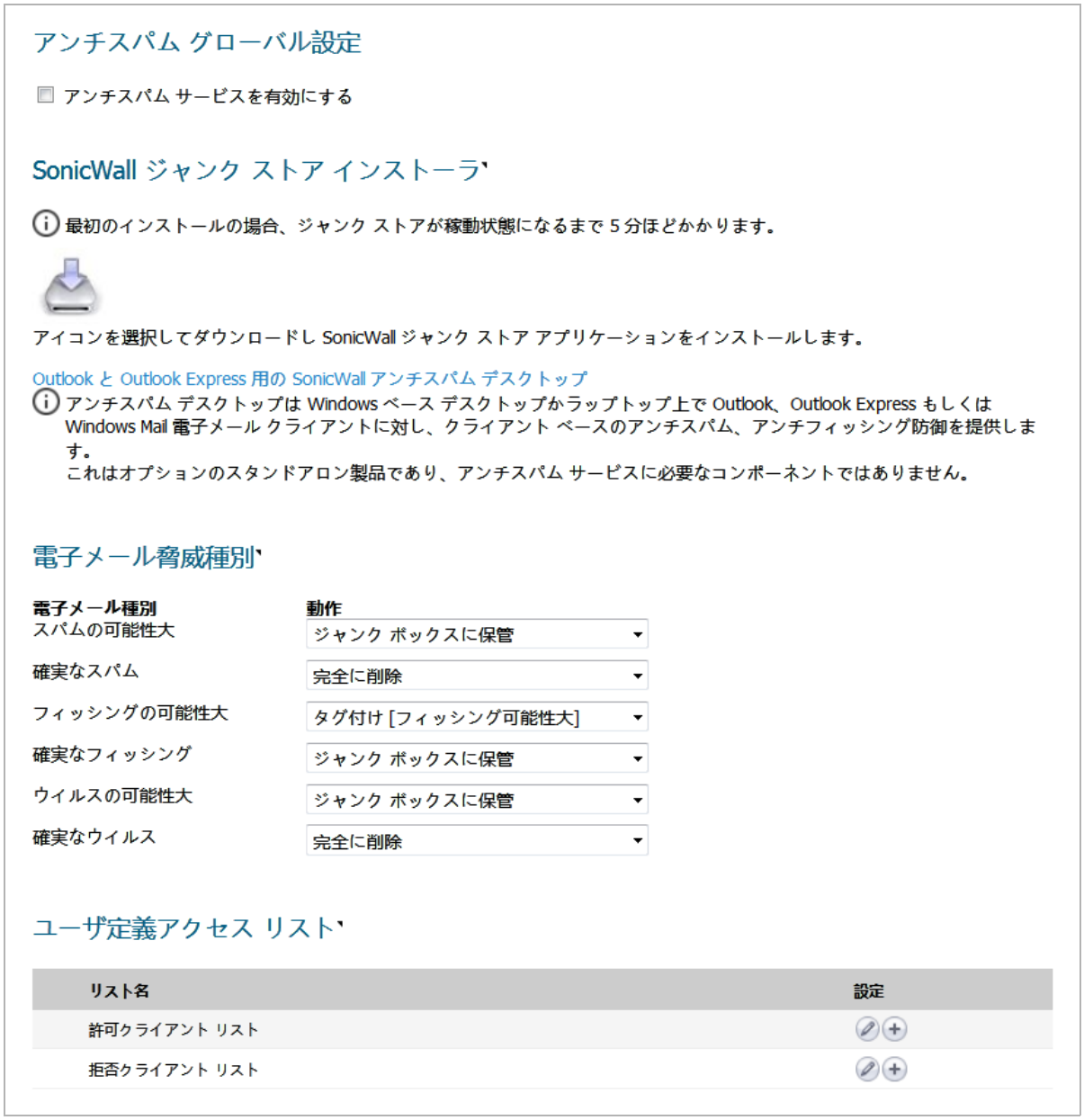
アンチスパムの有効化とアクティブ化

メモ：アンチスパムは、SuperMassive シリーズまたは NS*a* 9250 以降のファイアウォールではサポートされていません。

ヒント： アンチスパム機能とそのライセンス方法の詳細については、アンチスパムについて (284 ページ) を参照してください。

- アンチスパム > 基本設定 (293 ページ)
- アンチスパムのアクティブ化 (293 ページ)
- ジャンク ストアのインストール (295 ページ)
- 電子メール脅威種別の設定 (296 ページ)
- アクセス リストの設定 (298 ページ)
- 詳細オプションの設定 (300 ページ)

アンチスパム > 基本設定



「**管理 | セキュリティ設定 > アンチスパム > 基本設定**」ページでは、アンチスパム機能のアクティブ化、電子メール脅威種別の設定、アクセス リストの変更、詳細オプションの設定を行うことができます。

ヒント： アンチスパム機能とそのライセンス方法の詳細については、アンチスパムについて (284 ページ) を参照してください。

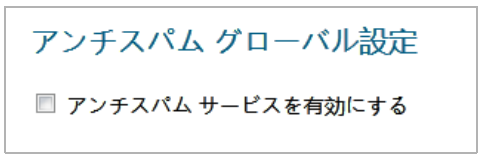
アンチスパムのアクティブ化

アンチスパムの登録が済んだら、アクティブにして、スパム、フィッシング、およびウイルス メッセージに対するファイアウォール レベルの保護を開始します。

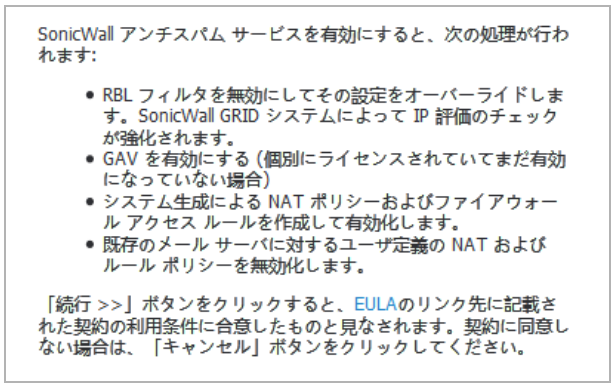
アンチスパムをアクティブにするには、以下の手順に従います。

1 「**管理 | セキュリティ設定 > アンチスパム > 基本設定**」に移動します。

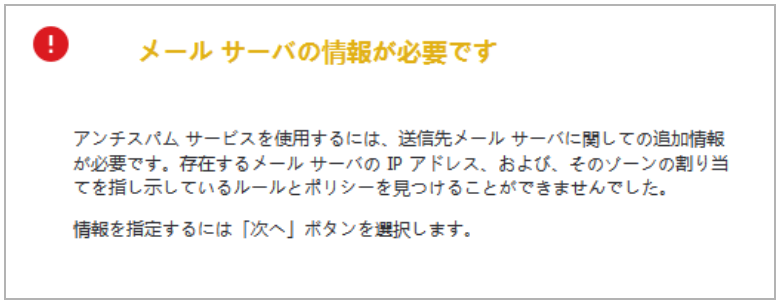
2 「**アンチスパム グローバル設定**」セクションまでスクロールします。



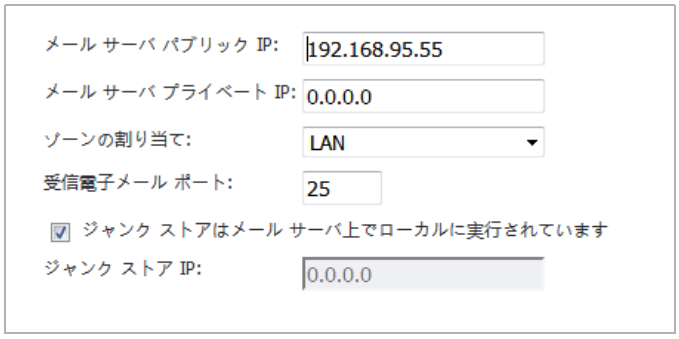
3 「**アンチスパム サービスを有効にする**」を選択して、アンチスパム機能を有効にします。アンチスパム サービスを有効にした場合の効果を説明するとともに、処理の続行に対する同意を求めるメッセージが表示されます。



4 続行するには、「**続行>>**」ボタンを選択します。使用されるメール サーバについての別のメッセージが表示されます。



5 「**次へ >>**」ボタンを選択します。サーバに関する情報を要求するダイアログが表示されます。ダイアログの各設定には、システムから取得した情報が入力されています。



6 必要に応じて、情報を変更します。

7 「**次へ >>**」を選択します。インストール中に作成されるものを説明するメッセージが表示されます。

8 「**確認**」を選択します。

アンチスパム アプリケーションがインストールされると、以下のことが可能になります。

- ジャンク ボックスのダウンロードとインストール。ジャンク ストアのインストール (295 ページ) を参照してください。
- 電子メール脅威種別の設定。電子メール脅威種別の設定 (296 ページ) を参照してください。

ジャンク ストアのインストール

アンチスパムでは、Microsoft Exchange Server 上にジャンク ストアを作成できます。ジャンク ストアは、エンドユーザが分析できるようにメッセージを検疫し、統計情報を提供します。Exchange システムにログインし、ブラウザを開いて管理インターフェースにログインし、ジャンク ストアをインストールします。

メモ：SonicWall は Sendmail や Lotus Domino など、Exchange 以外の SMTP サーバもサポートしますが、これらのサーバのいずれかにジャンク ストアをインストールする必要はありません。SonicWall Email Security 製品と同様に、CASS 2.0 の機能を使用するとジャンク ストアをスタンドアロン サーバにインストールできます。

CASS 2.0 で使用可能な最新の機能を十分に活用するために、SonicWall ではジャンク ストアをスタンドアロン サーバにインストールすることを推奨しています。

ジャンク ストアをインストールするには、以下の手順に従います。

1 Exchange システムにログインします。

2 ウェブ ブラウザを開きます。

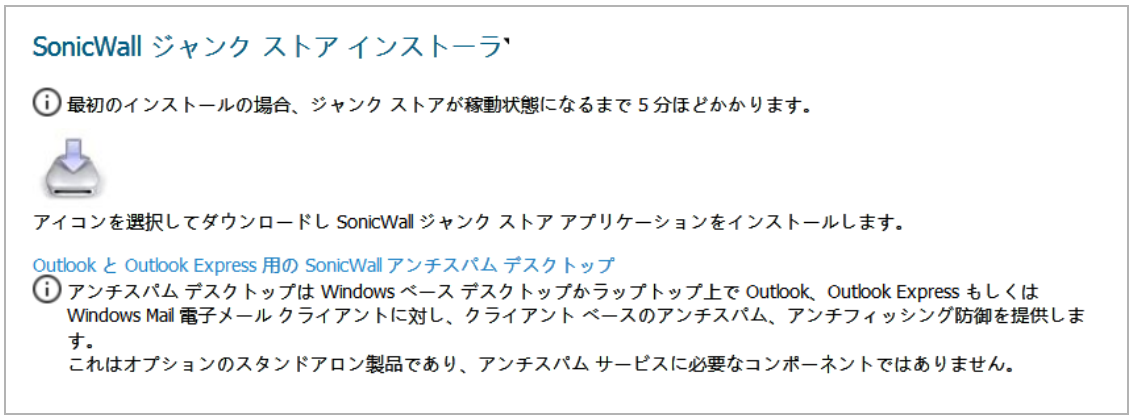
重要：SonicWall ジャンク ストア アプリケーションをダウンロードしてインストールするには、ジャンク ストア アプリケーションをインストールするシステム上に以下のものが必要です。

- Internet Explorer 6 以上
- Microsoft Exchange Server
- Email Downloader ActiveX コンポーネント (IE 用)

3 SonicOS インターフェースにログインします。

4 「**管理 | セキュリティ設定 > アンチスパム > 基本設定**」ページに移動します。

5 「**SonicWall ジャンク ストア インストーラ**」セクションに移動します。



6 **ジャンク ストア インストーラ** アイコンを選択して、Windows サーバにジャンク ストアをインストールします。

メモ：ジャンク ストア アプリケーションを初めてインストールする場合は、ジャンク ストアが動作するまでに 5 ～ 15 分ほどかかります。

7 ウェブ サイトが SonicWall Email Security アドオンを読み込もうとしている、という警告がブラウザに表示されます。

a 情報バーを選択します。

b ポップアップ メニューの「**ActiveX コントロールのインストール**」を選択します。セキュリティ警告の画面が表示されます。

8 「**インストール**」を選択して、ActiveX コントロールをインストールします。

9 「**管理 | セキュリティ設定 > アンチスパム > 基本設定** 」ページで、再び「**ジャンク ストア インストーラ**」アイコンを選択します。プログレス バーがページに表示されます。

10 ダウンロードが完了するとインストーラが起動します。

メモ：ジャンク ストアへのデータの移行が完了するには、長い時間がかかることがあります。

11 「**監視 | 現在の状況 > アンチスパム状況**」ページに移動し、SonicWall ジャンク ストアが「**利用可能**」になっていることを確認します。

電子メール脅威種別の設定

アンチスパムをアクティブにした後、プリファレンスを設定します。これらの設定後は、電子メールのフィルタ処理や並べ替えが設定に従って行われます。

ユーザのメッセージに関する既定の設定を行うには、以下の手順に従います。

1 「**管理 | セキュリティ設定 > アンチスパム > 基本設定** 」ページで、「**電子メール脅威種別**」セクションまでスクロールします。

2 スパム、フィッシング、ウイルスの問題が含まれている (またはその可能性がある) メッセージに対する既定の設定を選択します。ドロップダウン メニューで使用可能なオプションについては、電子メール脅威種別の設定: オプション テーブルを参照してください。

- **スパムの可能性大** (既定: **ジャンク ボックスに保管**)
- **確実なスパム** (既定: **完全に削除**)
- **フィッシングの可能性大** (既定: **タグ付け [フィッシング可能性大]**)
- **確実なフィッシング** (既定: **ジャンク ボックスに保管**)
- **ウイルスの可能性大** (既定: **ジャンク ボックスに保管**)
- **確実なウイルス** (既定: **完全に削除**)

電子メール脅威種別の設定: オプション

種別	動作
フィルタリング オフ	この脅威種別では、アンチスパムがどの電子メールに対してもスキャンや検閲を行わないので、すべての電子メール メッセージが受信者に配信されます。
タグ付け [タグ]	電子メールの件名行に次のようなタグが付けられます。 • **[スパム可能性大]** • **[スパム]** • **[フィッシング可能性大]** • **[フィッシング]** • **[ウイルス可能性大]** • **[ウイルス]** このオプションを選択するとユーザによる電子メールのコントロールが可能になり、ユーザは不要なメッセージをジャンク化することができます。
ジャンク ボックスに保管	電子メール メッセージがジャンク ボックスに保存されます。適切な権限を持つユーザおよび管理者はメッセージを非ジャンク化することができます。
完全に削除	電子メール メッセージが完全に削除されます。 **注意：このオプションを選択した場合、組織は必要なメッセージを失うリスクを負うことになります。**

ヒント： 2 つ以上のドメインを使用する場合は、「マルティプル ドメイン」オプションを選択します。詳細については、SonicWall または SonicWall 再販業者にお問い合わせください。

3 「**適用**」を選択します。

アクセス リストの設定

「**ユーザ定義アクセス リスト**」セクションでは、電子メール配信のための接続が許可または拒否されるクライアントを指定することで、静的な許可リストや拒否リストを管理できます。

メモ：これらのリストでのエントリ設定は、GRID IP 評価チェックの結果よりも優先されます。

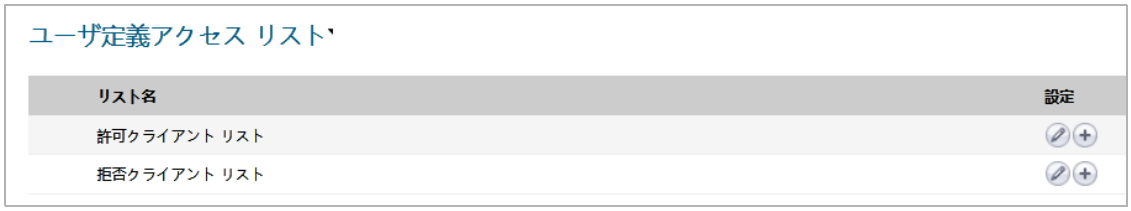
トピック:

- アクセス リストの設定 (298 ページ)
- アクセス リストへのホストの追加 (299 ページ)

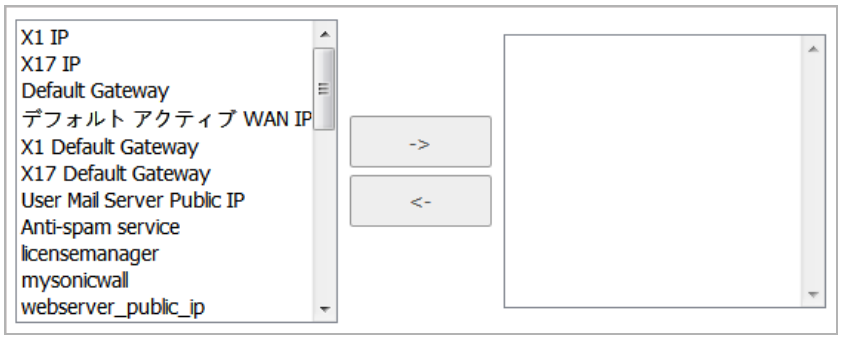
アクセス リストの設定

リストを設定するには、以下の手順に従います。

1 「**管理 | セキュリティ設定 > アンチスパム > 基本設定**」ページで、「**ユーザ定義アクセス リスト**」セクションまでスクロールします。



2 **許可クライアント リスト**と**拒否クライアント リスト**のうち、設定したいリストの**編集**アイコンを選択します。「**許可/拒否クライアント リスト**」ダイアログが表示されます。



3 「**グループに含まれる**」列に追加する項目を「**グループに含まれない**」列から選択します。

4 **右矢印**ボタンを選択します。

「**グループに含まれる**」列から項目を削除するには:

a 「**グループに含まれる**」列から項目を選択します。

b **左矢印**ボタンを選択します。

5 終了したら、「**OK**」ボタンを選択します。

アクセス リストへのホストの追加

リストにホストを追加するには、以下の手順に従います。

1 「**ユーザ定義アクセス リスト**」セクションまでスクロールします。

2 **ホストの追加**アイコンを選択します。「**許可/拒否リストにホストを追加する**」ダイアログが表示されます。

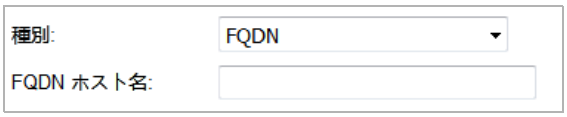
3 ホストの名前を「**名前**」フィールドに入力します。

4 「**種別**」ドロップダウン メニューで、ホストの種類を選択します。選択したホスト種別に応じて、以下の設定が変更されます。

5 選択した内容によって次の手順が異なります。

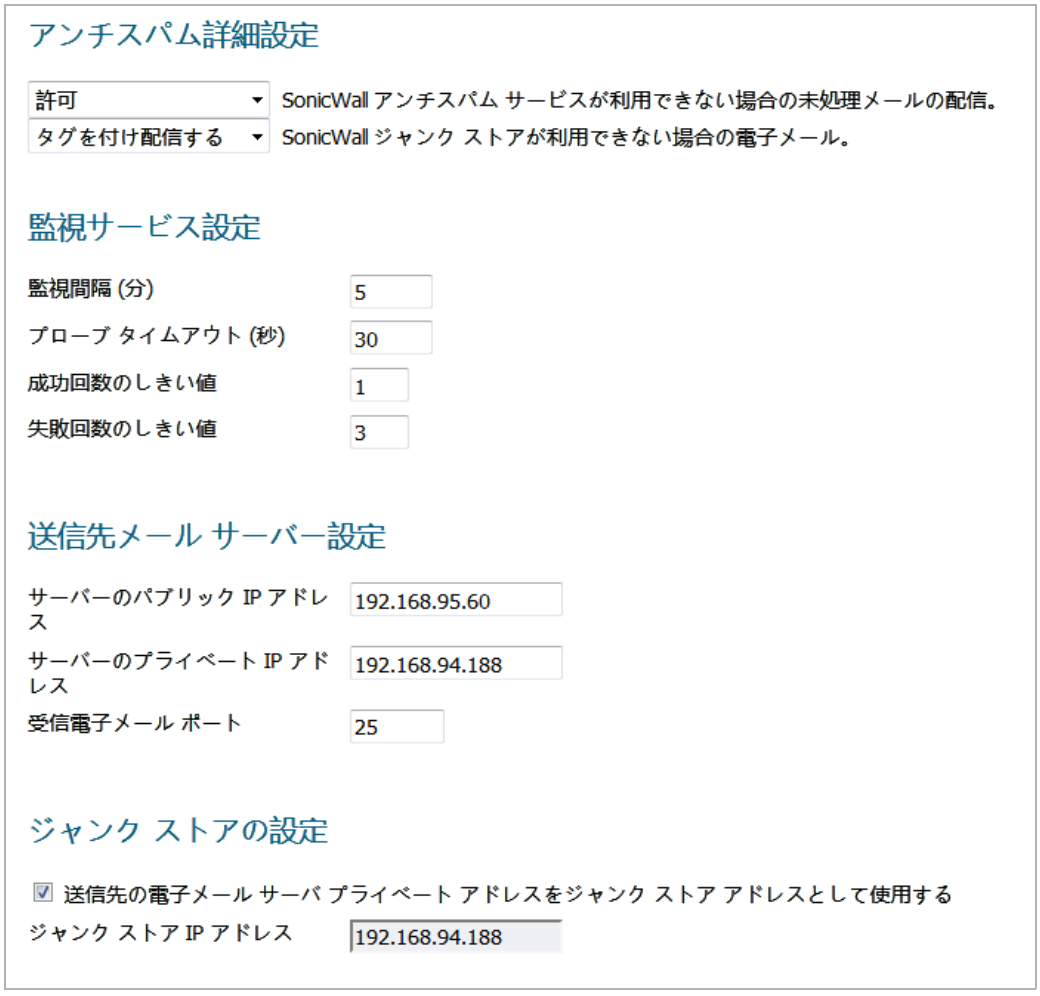
- **ホスト** (既定) -「**IP アドレス**」フィールドに IP アドレスを入力します。
- **範囲** -「**開始アドレス**」フィールドと「**終了アドレス**」フィールドに開始アドレスと終了アドレスを入力します。

- **FQDN** -「**FQDN ホスト名**」フィールドに FQDN ホスト名を入力します。



6 「**OK**」を選択します。

詳細オプションの設定


アンチスパム詳細設定
許可
SonicWall アンチスパム サービスが利用できない場合の未処理メールの配信。
タグを付け配信する
SonicWall ジャンク ストアが利用できない場合の電子メール。
監視サービス設定
監視間隔 (分)
5
プローブ タイムアウト (秒)
30
成功回数のしきい値
1
失敗回数のしきい値
3
送信先メール サーバー設定
サーバーのパブリック IP アドレス
192.168.95.60
サーバーのプライベート IP アドレス
192.168.94.188
受信電子メール ポート
25
ジャンク ストアの設定
送信先の電子メール サーバ プライベート アドレスをジャンク ストア アドレスとして使用する
ジャンク ストア IP アドレス
192.168.94.188

「**詳細オプション**」セクションでは、アンチスパム > 基本設定: 詳細オプション テーブルに記されている電子メール オプションを設定できます。:.

アンチスパム > 基本設定: 詳細オプション

設定の種別	設定	説明
アンチスパム詳細設定	**SonicWall アンチスパム サービスが利用できない場合の未処理メールの配信。**	アンチスパム サービスが有効でないか、その他の何らかの理由で使用できない場合、未処理の電子メールをすべて配信するか、すべて拒否するかを選択できます。良性の電子メールだけでなく、スパム メッセージもユーザに配信されます。 ドロップダウン メニューから次のいずれかを選択します。 • **許可** (既定) • **拒否**
	SonicWall ジャンク ストアが利用できない場合の電子メール。	ジャンク ストアがスパム メッセージを受け入れられない場合、それらを削除するか、あるいは件名行に "[Phishing] Please renew your account" のような警告を添えて配信するかを選択できます。 ドロップダウン メニューから次のいずれかを選択します。 • **タグを付け配信する** (既定) • **削除**
監視サービス設定	**監視間隔 (分)**	WAN および LAN ネットワークで Email Security コンポーネントのプローブ処理を行うためのタイマーの周期を分単位で設定します。最小値は 1 分、最大値は 60 分、既定値は **5** 分です。
	プローブ タイムアウト (秒)	エラーとしてフラグを立てる前にターゲットからの応答をプローブが待つ時間を秒単位で設定します。最小値は 30 秒、最大値は 300 秒、既定値は **30** 秒です。
	成功回数のしきい値	エンティティが動作していると宣言するために必要な連続成功応答回数を設定します。応答回数の最小値は 1、最大値は 10、既定値は **1** です。
	失敗回数のしきい値	エンティティが到達不能であると宣言するために必要な連続失敗応答回数を設定します。応答回数の最小値は 1、最大値は 10、既定値は **3** です。
送信先メール サーバー設定	**サーバーのパブリック IP アドレス**	外部接続に使用できるサーバーの IP アドレスです。MTA はこの WAN IP アドレスを SMTP 接続で使用します。この数値は、アンチスパムおよびジャンク ストアをアクティブ化してインストールする際に管理者が指定したアドレスによって設定されています。このアドレスは変更できます。

アンチスパム > 基本設定: 詳細オプション

設定の種別	設定	説明
	サーバーのプライベート IP アドレス	内部トラフィック用のサーバーの IP アドレスです。これは装置の背後にある内部メールサーバーの IP アドレスです。この数値は、アンチスパムおよびジャンク ストアをアクティブ化してインストールする際に管理者が指定したアドレスによって自動的に設定されています。このアドレスは変更できます。
	受信電子メール ポート	装置が受信電子メールを受け取るために開いている TCP サービス ポートです。最小値は 0、最大値は 65535、既定の設定は「***関数によって生成***」です。
ジャンク ストアの設定	**送信先の電子メール サーバ プライベート アドレスをジャンク ストア アドレスとして使用する**	ジャンク ストアが送信先の電子メール サーバにある場合は、このチェックボックスを選択します。アドレスは、アンチスパムおよびジャンク ストアをアクティブ化してインストールする際に管理者が指定したアドレスによって自動的に設定されます。このアドレスは変更できます。このチェックボックスは既定でオンになっています。そのため、「ジャンク ストア IP アドレス」フィールドはグレー表示になっています。 ***アドレスを変更するには、以下の手順に従います。*** 1 チェックボックスをオフにします。「ジャンク ストア IP アドレス」フィールドが使用可能になります。 2 サーバが存在する場所のジャンク ストア IP アドレスを入力します。
その他	**電子メール システム検知を有効にする**	ネットワーク内にある使用可能な電子メール システム リソースの検出を有効にします。このチェックボックスは既定でオンになっています。

26

アンチスパム ログの設定

メモ：アンチスパムは、SuperMassive シリーズまたは NS*a* 9250 以降のファイアウォールではサポートされていません。

- アンチスパム > 詳細
- システム ファイル/ログ ファイルのダウンロード
- ログ情報の量およびレベルの選択

アンチスパム > 詳細

「**アンチスパム > 詳細設定**」ページでは、ログおよびシステム設定ファイルをサーバからダウンロードしたり、ログ レベルを設定したりできます。

トピック:

- システム ファイル/ログ ファイルのダウンロード
- ログ情報の量およびレベルの選択

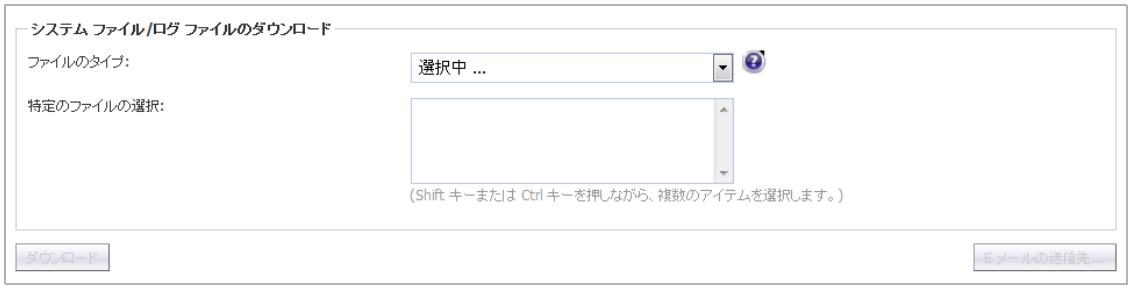
システム ファイル/ログ ファイルのダウンロード

メモ：一部のログ ファイル名 (commonlogs ディレクトリにあるものなど) には、2 桁の数字が含まれています。例えば、12.log といったファイル名になります。この "12" は、ごく最近の月の 12 日のログであることを示しています。また、ログ ファイル名の最後が数字で終わっているものもあります。例えば、MlfThumbUpdate_2.log といったファイル名です。この "2" は、このファイルよりも新しいログが存在すること示しています。最新のログは MlfThumbUpdate.log です。その次に新しいログは MlfThumbUpdate_0.log であり、続いて MlfThumbUpdate_1.log という順序になっています。

ほとんどのログ データは、そのログを生成したサーバのローカル時間ではなく、グリニッジ標準時 (GMT) に従っています。これはログ ファイルの名前にも当てはまります。

SonicWall Email Security サーバからログ ファイルまたはシステム設定ファイルをダウンロードするには、以下の手順に従います。

1 「**アンチスパム > 詳細設定**」の「**システム ファイル/ログ ファイルのダウンロード**」セクションに移動します。



2 「**ファイルのタイプ**」ドロップダウン メニューからダウンロードするファイルの種別を選択します。「**特定のファイルの選択**」リストにそのファイル種別が設定されます。

3 「**特定のファイルの選択**」種別から、特定の項目を 1 つ以上選択します。複数のファイルを選択するには、Shift キーまたは Ctrl キーを押しながらファイルを選択します。「**ダウンロード**」ダウンロード および「**E メールの送信先**」E メールの送信先... ボタンがアクティブになります。

メモ：選択したファイルが結合されて 1 つの zip ファイルになります。

4 次のどちらかを選択します。

- 「**ダウンロード**」ボタン - ファイルをローカル ハード ドライブにダウンロードする場合。

- 「**E メールの送信先**」ボタン - ファイルを電子メールで送信する場合。「**送信先**」ダイアログが表示されます。

a) 送信者の電子メール アドレスを「**この E メール アドレスからファイルを送信**」フィールドに入力します。既定値は「**postmaster**」です。

b) 受信者の電子メール アドレスを「**受信者 E メールアドレス**」フィールドに入力します。

c) 「**送信**」ボタンを選択します。

メモ：電子メール システムの制限によっては、非常に大きなファイルやディレクトリを電子メールで送信すると問題が発生する可能性があります。

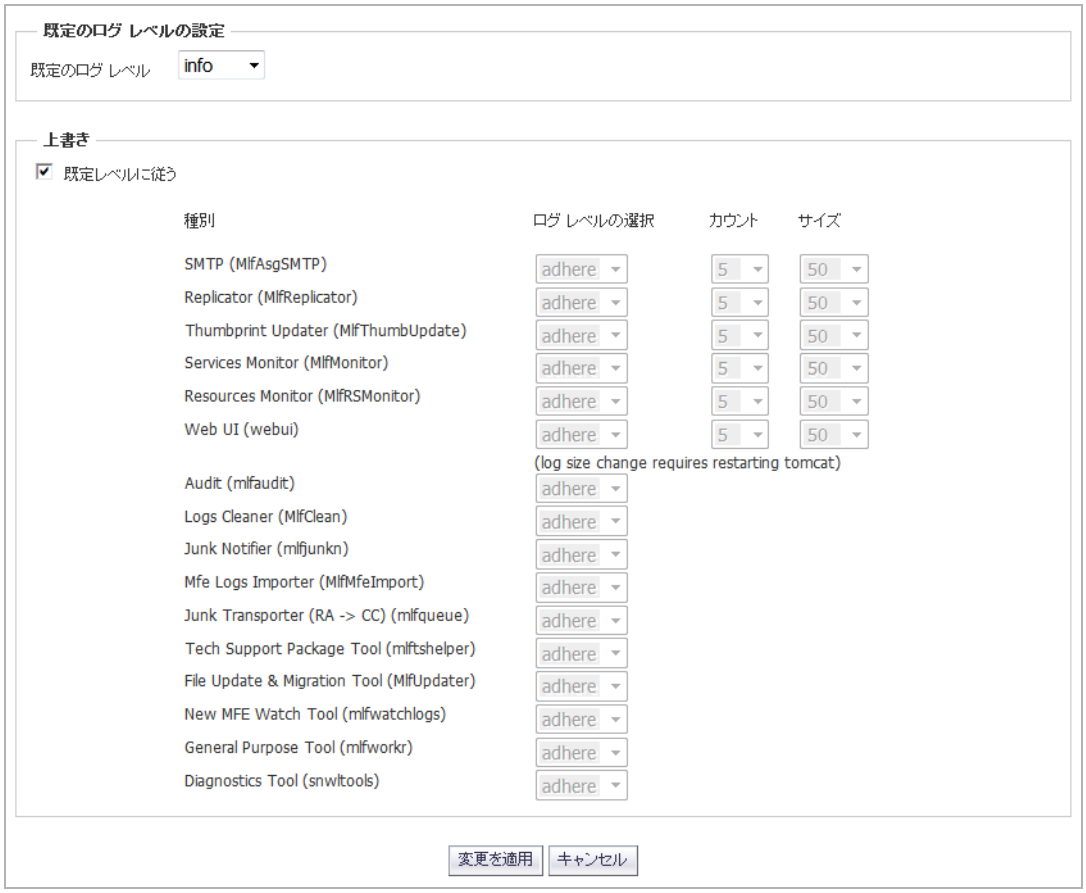
ログ情報の量およびレベルの選択

ログに格納されるシステム レポート情報のレベルや量は、「**他の設定**」セクションで選択できます。

ログ情報のレベルおよび量を設定するには、以下の手順に従います。

1 「**アンチスパム > 詳細設定**」の「**他の設定**」セクションに移動します。

2 「**管理** 管理 」ボタンを選択します。「**ログ レベルの設定**」ダイアログが表示されます。



3 「**既定のログ レベル**」ドロップダウン メニューから既定のログ レベルを選択します。レベルは最も低いものから最も高いものまで順に表示されます。

> **メモ**：既定のログ レベルを高くするほど、記録されるイベントの数が増えます。例えば、**情報**レベルでは、**トレース** レベルと**デバッグ** レベルのイベントも記録されます。

- **トレース** - 最も低いレベル
- **デバッグ**
- **info** - 既定値
- **警告**
- **エラー**
- **致命的** - 最も高いレベル

すべてのログは、特にオーバーライドされない限り、ここで設定されている既定のレベルに従います。

4 「**上書き**」セクションでログに対する変更を行う場合は、「**既定レベルに従う**」チェックボックスをオフにします。すべてのサービス種別ですべてのドロップダウン メニューがアクティブになります。

5 特定のサービスや下位サービスのログ レベルを変更するには、変更するサービス/下位サービスの「**ログ レベルの選択**」ドロップダウン メニューから、適切なログ レベルを選択します。レベルには、ステップ 3 にあるのと同じものに加えて「**adhere**」オプションがあります。

> **メモ**：すべてのサービスおよび下位サービス種別の既定のログ レベルは「**adhere**」になっています。つまり、「**既定のログ レベル**」ドロップダウン メニューで設定されているログ レベルが使用されます。

6 必要に応じて、保持するログ ファイルの数を選択します。既定では、ジャンク ボックスが以下の各サービスについて保持するログ ファイルの数は 3 になっています。

- SMTP
- サムプリント アップデータ
- リソース モニタ
- レプリケーター
- サービス モニタ
- ウェブ UI

4 番目のログ ファイルが生成されると、最も古いログ ファイルが破棄され、2 番目に古かったものが最も古いログ ファイルに、3 番目に古かったものが 2 番目に古いログ ファイルになります。

a あるサービスについて保持するログの数は、そのサービスの「**カウント**」ドロップダウン メニューから数値を選択して増やすことができます。

- **3**
- **5**
- **6**
- **7**
- **8**
- **9**
- **10**

ログの数を減らすと、ディスク領域の節約になりますが、古いデータを参照できなくなる場合があります。ログの数を増やすと、データの保持量は増えますが、より多くのディスク領域を消費します。

7 必要に応じて、サービス ログ (ステップ 6 を参照) のサイズを「**サイズ**」ドロップダウン メニューから選択します。各ログの既定のサイズは **10MB** です。

ログのサイズは、10MB (既定値) から 100MB まで、10MB 単位で増やすことができます。ログ サイズを小さくするとディスク領域の節約になり、大きくすると格納できるデータ量が増えます。

> **重要**：ログのサイズを変更するには、Tomcat サーバを再起動する必要があります。

8 「**変更を適用**」を選択して変更を保存します。

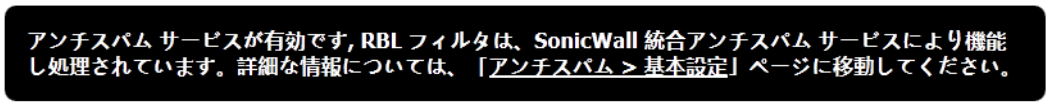
ログ レベルを既定値に戻すには、以下の手順に従います。

1 「**デフォルトにリセットする**」 キャンセル ボタンを選択します。

27

RBL フィルタの設定

メモ：アンチスパム サービスは、標準の SonicOS RBL フィルタの高度な上位集合です。そのため、アンチスパムを有効にすると、RBL フィルタは自動的に無効になり、その情報と「**管理 | セキュリティ設定 > アンチスパム > 基本設定**」ページへのリンクを伴うメッセージが表示されます。



アンチスパムが有効でない場合は、「**管理 | セキュリティ設定 > アンチスパム > リアルタイム ブラックリスト設定**」ページで設定を行うことができます。ただし、すべてのアンチスパムおよびジャンク ボックス ページは使用できません。

メモ：アンチスパムは、SuperMassive シリーズまたは NS*a* 9250 以降のファイアウォールではサポートされていません。

- アンチスパム > リアルタイム ブラックリスト フィルタ (309 ページ)
- RBL リストについて (309 ページ)
- RBL フィルタの有効化 (310 ページ)
- RBL サービスの管理 (311 ページ)
- ユーザ定義 SMTP サーバ リスト (315 ページ)
- リアルタイム ブラック リストのテスト (317 ページ)

アンチスパム > リアルタイム ブラックリスト フィルタ

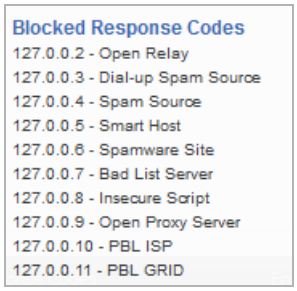
RBL リストについて

SMTP リアルタイム ブラックリスト (RBL) は、スパム送信者が活動の起点または中継点として利用している SMTP サーバの IP アドレスを公開するためのメカニズムです。こうした情報は数多くの組織によって収集されており、無料のhttp://www.spamhaus.org や有償のhttps://10.1.1.10 にアクセスします。

メモ：SMTP RBL はどちらかと言えば強引なスパム フィルタ手法です。スパム アクティビティの報告結果を基に編集されているため、正当なアドレスでも不正なものとして検出されてしまう場合があります。SonicOS に実装されている SMTP RBL フィルタでは、さまざまな微調整のメカニズムを備えることによってフィルタの精度を高めています。

RBL リスト プロバイダは、各自のリストを DNS を使用して公開しています。ブラックリストに登録された IP アドレスは、リスト プロバイダの DNS ドメインのデータベースに格納されており、SMTP サーバの IP アドレスを逆順に表記した値をドメイン名の前に付加することによって参照できます。

127.0.0.2 ～ 127.0.0.11 の応答コードは、どのような理由でブラックリストに登録されているのかを示しています。



例えば、IP アドレスが 1.2.3.4 である SMTP サーバが、RBL リスト プロバイダ sbl-xbl.spamhaus.org のブラックリストに登録されているとき、DNS クエリとして 4.3.2.1.sbl-xbl.spamhaus.org を送信すると、そのサーバがスパムの送信元であることを示す 127.0.0.4 という応答が返されるので、その接続は破棄すべきであると判断できます。

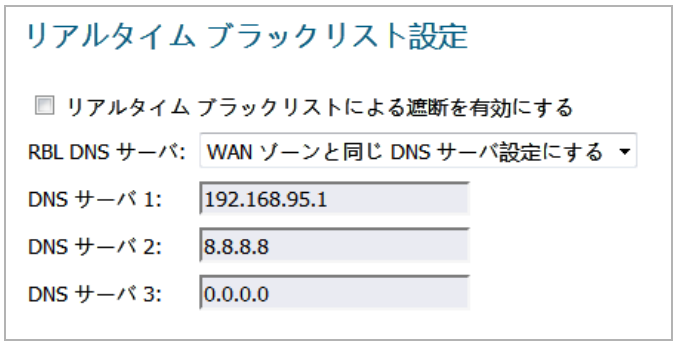
メモ：最近のスパムは、そのほとんどがハイジャックされたコンピュータやゾンビ化したコンピュータから (つまり、小さな SMTP サーバを本人に気付かれないようにコンピュータに忍ばせ、それを踏み台として) 送信されていることがわかっています。正当な SMTP サーバとは異なり、これらのゾンビ化したコンピュータがメールの配信に失敗した場合に再試行することはまれです。そのため、RBL フィルタによって遮断されたスパムについては、それ以降、配信が再試行されることはありません。

ブラックリスト クエリに対する SonicOS の応答

DNS の応答は収集されて、キャッシュに格納されます。DNS クエリの応答からブラックリストに登録されていることが判明した場合、そのサーバはフィルタの対象となります。キャッシュに格納される応答の存続時間は TTL 値に基づいており、ブラックリストに登録されていないことが判明した場合は TTL=2 時間でキャッシュされます。キャッシュがいっぱいになった場合、キャッシュ エントリが FIFO (先入れ先出し) 方式で順次破棄されます。

IP アドレスをチェックする際は、このキャッシュに基づいて接続を破棄すべきかどうかが判断されます。初期状態では IP アドレスがキャッシュに存在しないため、DNS 要求を実行する必要があります。有害であることが確認されるまで IP アドレスは無害と仮定されるため、チェックの結果、接続が許可されることになります。DNS 要求を実行すると、独立したタスクとして結果がキャッシュされます。それ以降、同じ IP アドレスからのパケットをチェックするときに、その IP アドレスがブラックリストに登録されていた場合は接続が破棄されます。

RBL フィルタの有効化



リアルタイム ブラック リストによる遮断が有効になっている場合、WAN 側のホストからの着信接続または WAN 側ホストへの発信接続が、有効にされている各 RBL サービスを使って (「RBL DNS サーバ」で設定された DNS サーバに DNS 要求を送信することによって) チェックされます。

リアルタイム ブラック リスト フィルタを有効にするには、以下の手順に従います。

1 「**セキュリティ設定 | アンチスパム > リアルタイム ブラックリスト フィルタ**」ページに移動します。

2 「**リアルタイム ブラックリストによる遮断を有効にする**」チェックボックスをオンにします。

3 RBL DNS サーバのドロップダウン メニューから DNS サーバを選択します。

- **WAN ゾーンと同じ DNS サーバ設定にする** (既定) - DNS サーバの IP アドレスは「**DNS サーバ 1/2/3**」フィールドにグレーで表示されます。
- **マニュアルで DNS サーバを指定する** -「**DNS サーバ 1/2/3**」フィールドが使用可能になります。

a) 「**DNS サーバ 1/2/3**」フィールドに、DNS サーバの IP アドレスを 1 つ以上入力します。

4 「**適用**」を選択します。

RBL サービスの管理

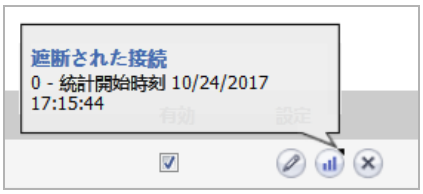
その他の RBL サービスを「**リアルタイム ブラックリスト サービス**」セクションに追加することができます。

「**リアルタイム ブラックリスト サービス**」セクションには、使用可能な RBL サービスに関する情報やそうしたサービスのための動作が表示されています。

- **RBL サービス** - RBL サービスの名前です。SonicWall によって 2 つのサービスが提供されていますが、別のものを追加することができます。
  - sbl-xbl.spamhaus.org - リアルタイムのアンチスパム保護機能をインターネット ネットワークに提供している Spamhaus プロジェクトです。
  - dnsbl.sorbs.net - DNS ベースのブラックリスト (DNSBL) データベースへのアクセスを提供している SORBS (Spam and Open Relay Blocking System) です。
- **応答コード** - **コメント** アイコンをマウスでポイントすると、応答コードのリストが表示されます。応答コードについては、RBL リストについてを参照してください。
- **有効** - RBL サービスを有効にするには、このチェックボックスをオンにします。提供されている 2 つのサービスのチェックボックスは、既定でオンになっています。

RBL サービスを無効にするには、該当するチェックボックスをオフにします。この操作によってエントリがテーブルから削除されることはないので、後でサービスを有効にすることができます。

- **設定** - 以下に示すさまざまな動作のアイコンが表示されます。
  - **編集**アイコン -「**RBL ドメインの編集**」ダイアログを表示します。RBL サービスの編集を参照してください。
  - **統計**アイコン - 遮断された接続に関する情報を表示します。



こうした統計を消去するには、「統計のクリア」ボタンを選択します。

  - **削除**アイコン - RBL サービスのエントリを削除します。RBL サービスの削除を参照してください。

トピック:

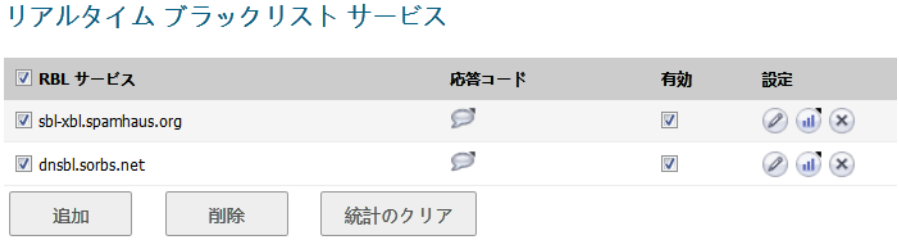
- 統計のクリア (312 ページ)
- RBL サービスの追加 (313 ページ)
- RBL サービスの編集 (314 ページ)
- RBL サービスの削除 (315 ページ)

統計のクリア

ブラック リスト サービスのために保持されている統計情報を消去することができます。

統計を消去するには、以下の手順に従います。

1 該当するチェックボックスをオンにすることでサービスを選択します。すべてのサービスの統計を消去するには、「**RBL サービス**」の隣にある見出し内のチェックボックスをオンにします。「**統計のクリア**」ボタンがアクティブになります。



2 「**統計のクリア**」ボタンを選択します。

RBL サービスの追加

RBL サービスを追加するには、以下の手順に従います。

1 「**セキュリティ設定 | アンチスパム > リアルタイム ブラックリスト フィルタ**」ページで、「**リアルタイム ブラックリスト サービス**」セクションが表示されるまでスクロールします。

2 「**追加**」ボタンを選択します。「**RBL ドメイン設定**」ダイアログが表示されます。

3 「**RBL ドメイン**」フィールドで、問い合わせが行われる RBL サービスのドメイン名を指定します。

4 「**RBL ドメインを有効にする**」チェックボックスをオンにして、サービスの使用を有効にします。

5 該当するチェックボックスをオンにすることで、想定される応答コードを指定します。ほとんどの RBL サービスは、提供している応答をウェブ サイトで公開していますが、通常は「**すべての応答を遮断**」を選択して構いません。

> **ヒント：** 「**すべての応答を遮断**」チェックボックスをオンにすると、遮断されるすべての応答のチェックボックスがオンになります。「**すべての応答を遮断**」チェックボックスをオフにすると、遮断されるすべての応答のチェックボックスがオフになります。

6 「**OK**」を選択します。RBL サービスが「**リアルタイム ブラック リスト サービス**」テーブルに追加されます。

RBL サービスの編集

RBL サービスを編集するには、以下の手順に従います。

1 「**セキュリティ設定 | アンチスパム > リアルタイム ブラックリスト フィルタ**」ページで、「**リアルタイム ブラックリスト サービス**」セクションが表示されるまでスクロールします。

2 変更する RBL サービスの**編集**アイコンを選択します。「**RBL ドメインの追加**」ダイアログが表示されます。

3 必要に応じて、「**RBL ドメイン**」フィールドで、問い合わせが行われる RBL サービスのドメイン名を編集します。

> ⓘ **ヒント：** 「**リアルタイム ブラック リスト サービス**」テーブルの該当する「**有効**」チェックボックスをオン (オフ) にすることで、RBL サービスを有効 (無効) にすることができます。

4 必要に応じて、「**RBL ドメインを有効にする**」チェックボックスをオン (オフ) にして、サービスの使用を有効 (無効) にします。

5 また、該当するチェックボックスをオン (オフ) にすることで、想定される応答コードを選択 (選択解除) することもできます。

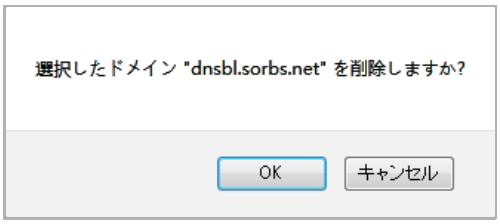
> ⓘ **ヒント：** 「**すべての応答を遮断**」チェックボックスをオンにすると、遮断されるすべての応答のチェックボックスがオンになります。「**すべての応答を遮断**」チェックボックスをオフにすると、遮断されるすべての応答のチェックボックスがオフになります。

6 「**OK**」を選択します。

RBL サービスの削除

RBL サービスを削除するには、以下の手順に従います。

1 「**リアルタイム ブラック リスト サービス**」テーブルで、サービスの**削除**アイコンを選択します。次の警告メッセージが表示されます。

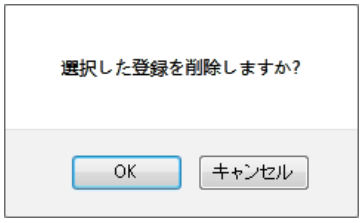


2 「**OK**」を選択します。「**リアルタイム ブラック リスト サービス**」テーブルからエントリが削除されます。

1 つまたは複数の RBL サービスを削除するには、以下の手順に従います。

1 「**リアルタイム ブラック リスト サービス**」テーブルで、1 つ以上のサービスのチェックボックスをオンにします。「**削除**」ボタンが使用可能になります。

2 「**削除**」ボタンを選択します。次の警告メッセージが表示されます。



3 「**OK**」を選択します。「**リアルタイム ブラック リスト サービス**」テーブルからエントリが削除されます。

ユーザ定義 SMTP サーバ リスト

メモ：**RBL User White List** および **RBL User Black List** は変更できますが、削除することはできません。

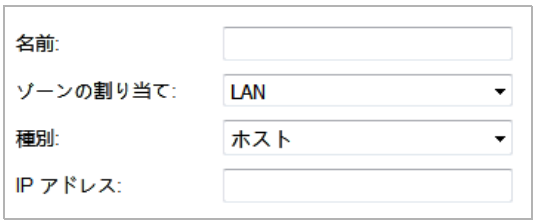
「**ユーザ定義 SMTP サーバリスト**」セクションでは、SMTP サーバのホワイトリスト (明示的許可: **RBL User White List**) およびブラックリスト (明示的拒否: **RBL User Black List**) をアドレス オブジェクトを使って作成できます。これらのリストに含まれるエントリについては RBL の問い合わせの手順が省略されます。

パートナー サイトの SMTP サーバからの SMTP 接続を常に受け入れるようにする場合は、次の手順に従います。

1 「**セキュリティ設定 | アンチスパム > リアルタイム ブラックリスト フィルタ**」ページで、「**ユーザ定義 SMTP サーバ リスト**」セクションが表示されるまでスクロールします。

2 次のようにして、追加するサーバのアドレス オブジェクトを作成します。

a 「**追加**」ボタンを選択します。「**アドレス オブジェクトの追加**」ダイアログが表示されます。



b 「**名前**」フィールドにサーバのニックネームを入力します。

c 「**ゾーンの割り当て**」ドロップダウン メニューからサーバのゾーンを選択します。

d 「**種別**」ドロップダウン メニューから、ホストの種別を選択します。選択したホスト種別に応じて、以下の設定が変更されます。

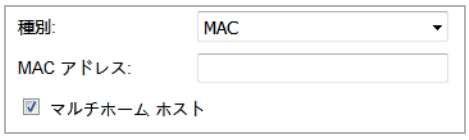
e 選択した内容によって次の手順が異なります。

- **ホスト** (既定) -「**IP アドレス**」フィールドに IP アドレスを入力します。
- **範囲** -「**開始アドレス**」フィールドと「**終了アドレス**」フィールドに開始アドレスと終了アドレスを入力します。

- **ネットワーク**

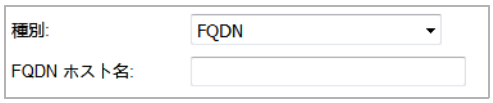
  - 「**ネットワーク**」フィールドにネットワークを入力します。
  - 「**ネットマスク/接頭辞長**」フィールドにネットマスクを入力します。

- **MAC**



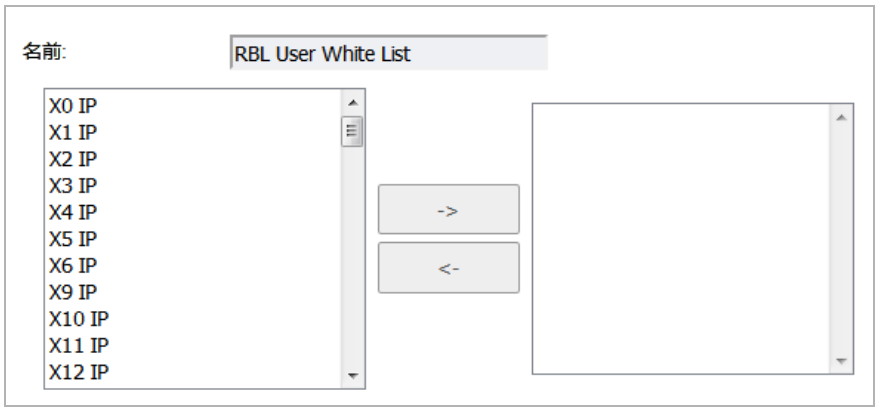
- 「MAC アドレス」フィールドに MAC アドレスを入力します。
- ホストがマルチホーム ホストの場合、「**マルチホーム ホスト**」チェックボックスをオンにします。それ以外の場合は、このチェックボックスをオフにします。このチェックボックスは既定でオンになっています。

- **FQDN** -「**FQDN ホスト名**」フィールドに FQDN ホスト名を入力します。



f 「**OK**」を選択します。

3 「**RBL User White List**」の「**設定**」列にある**編集**アイコンを選択します。「**アドレス オブジェクト グループの編集**」ダイアログが表示されます。



4 追加するアドレス オブジェクトを左の列から選択します。複数のアドレス オブジェクトを一度に選択できます。

5 **右矢印**ボタンを選択します。

グループからアドレス オブジェクトを削除するには、アドレス オブジェクトを選択し、**左矢印**ボタンを選択します。

6 「**OK**」を選択します。これでテーブルが更新され、そのサーバとの SMTP 通信が常に許可されるようになります。

リアルタイム ブラック リストのテスト

「**調査 | ツール | システム診断**」ページにも、「**診断ツール**」セクションに特定の SMTP の IP アドレス (または RBL サービスや DNS サーバ) をテストできる「**リアルタイム ブラックリスト調査**」という機能が用意されています。この機能については、『*SonicWall SonicOS 6.5 調査*』を参照してください。

テストで使用する既知のスパム送信元のリストについては、以下を参照してください。
http://www.spamhaus.org/sbl/latest/.

28

中継ドメインの指定

メモ：アンチスパムは、SuperMassive シリーズまたは NSa 9250 以降のファイアウォールではサポートされていません。

- アンチスパム > 中継ドメイン (318 ページ)
- オープン リレーについて (319 ページ)
- 許可された中継ドメインのリスト作成 (319 ページ)

アンチスパム > 中継ドメイン

「**管理 | セキュリティ設定 > アンチスパム > 中継ドメイン**」ページでは、CASS による電子メールの中継が許可されているドメインのリストを作成できます。電子メールを中継できるドメインを制限することで、オープン リレーの問題を回避できます。

オープン リレーについて

オープン リレーとは、ローカル ユーザからのものでもローカル ユーザ宛てのものでもない電子メール メッセージの中継 (送信/受信) を第三者に許可するように設定された SMTP サーバです。そのため、このようなサーバは通常、スパム送信者の標的となります。

CASS がオープン リレーとして設定されている場合、受信者ドメイン宛てのものではないメールも中継されます。オープン リレーとして設定されていない CASS は、リストされている受信者ドメインのいずれかを持つ電子メールは中継しますが、リストされていないドメイン宛ての電子メールは中継しません。そのようなメールは拒否されます。許可された中継ドメインをリストすることで、メールがユーザ宛てのものでない場合も、不要な電子メールの中継を回避できます。

許可された中継ドメインのリスト作成

中継に使用されるすべてのドメインをリスト化できます。

許可された中継ドメインをリスト化するには、以下の手順に従います。

1 「**管理 | セキュリティ設定 > アンチスパム > 中継ドメイン**」に移動します。

2 「**設定**」セクションまでスクロールします

3 中継ドメインを制限するかどうか選択します。

- **どのソース IP アドレスでもこのパスに接続できます。** - すべてのドメインにメッセージの中継を許可します。「ステップ 5」に移動します。

△ **注意：このオプションを選択すると、CASS がオープン リレーになる可能性があります。メールは、受信者のドメイン宛てのものでなくても中継されます。そのため、スパムの送信に利用されるおそれがあります。**

- **どの IP アドレスでもこのパスに接続できますが、中継は、この中のいずれかのドメインに送信された E メールに対してのみ許可されています。** - リストにあるドメインのみがメッセージを中継できます。

4 メッセージの中継が許可されるドメインをフィールドに入力します。ドメインが複数ある場合は、改行コード (<CR>) で区切ります。

5 「**変更を適用**」を選択します。

29

ジャンク ボックス設定の構成

メモ：アンチスパムは、SuperMassive シリーズまたは NS*a* 9250 以降のファイアウォールではサポートされていません。

- アンチスパム > ジャンク ボックス設定

アンチスパム > ジャンク ボックス設定

「**アンチスパム > ジャンクボックス設定**」ページでは、以下の設定を行うことができます。

- メッセージを破棄するまでジャンク ボックスに保管しておく期間。
- 1 ページあたりに表示されるジャンク ボックス メッセージの数。
- ユーザがメッセージを非ジャンク化したときの動作。

メッセージ管理を実行するには、以下の手順に従います。

1 「**メッセージ管理**」セクションの「**削除するまでジャンク ボックスに保管する日数**」ドロップダウン メニューから、ジャンク メールを削除するまでに保持する日数を選択します。最小値は 1 日、最大値は 180 日、既定値は **15 日**です。

2 「**調査 | ログ | アンチスパム ジャンクボックス**」ページの「**受信**」ビューにある「**見つかったメッセージ**」セクションに表示するメッセージの行数を「**画面に表示するジャンク ボックス メッセージの数**」ドロップダウン メニューから選択します。最小値は 10 行、最大値は 400 行、既定値は **400 行**です。

3 非ジャンク化された送信者を受信者の許可リストに追加するかどうかを「**ユーザがメッセージを非ジャンク化したとき**」で選択します。既定ではどちらのオプションも選択されていません。

- **送信者を自動的に受信者の許可リストに追加する**
- **送信者を受信者の許可リストに追加しない**

4 「**変更を適用**」を選択します。

既定の設定に戻すには、以下の手順に従います。

1 「**デフォルトにリセットする**」ボタンを選択します。

30

ジャンク サマリの管理

メモ：アンチスパムは、SuperMassive シリーズまたは NS*a* 9250 以降のファイアウォールではサポートされていません。

- アンチスパム > ジャンクボックス サマリ (322 ページ)
- ジャンク サマリの管理 (323 ページ)
- 既定値に戻す (326 ページ)

アンチスパム > ジャンクボックス サマリ

ジャンク ストアは、ユーザのジャンク サマリに置かれているすべてのメッセージをリストした電子メール メッセージをユーザに送信します。「**アンチスパム > ジャンク ボックス サマリ**」ページでは、ユーザのためのジャンク サマリを設定できます。

ログに記録されるメッセージの種別を設定するために、「**アンチスパム > 詳細設定**」ページへのリンクが用意されています。

「**アンチスパム > ジャンクボックス サマリ設定**」ページでは、以下のオプションを設定できます。

- **頻度の設定** - ジャンク ボックス サマリが管理者に送信される頻度および時間を設定します。
- **メッセージ設定** - サマリに何を含めるか、またサマリにグラフィックを含めるかどうかを設定します。
- **その他の設定** - メッセージのシングルクリック表示や認証などのオプションを設定します。
- **他の設定** - サマリの送信者、電子メールの件名、ユーザの URL などを設定します。

ジャンク サマリの管理

ジャンク サマリを管理するには、以下の手順に従います。

1 「**ジャンクボックス サマリ設定**」ページの「**頻度の設定**」セクションにある「**サマリの頻度**」ドロップダウン メニューから、サマリが管理者に送信される頻度を選択します。

最低の頻度は **14 日ごと**、最高の頻度は **1 時間ごと**、既定値は **1 日ごと**です。サマリが管理者に送信されないようにするには、「**なし**」を選択します。

2 ユーザが電子メール通知を受け取る時刻をカスタマイズする場合は、「**サマリを送信する時刻**」オプションから時刻を選択します。

メモ：個々のユーザはこの設定をオーバーライドできます。

- **1 日のうちいつでも** (既定)
- **次の時刻から 1 時間以内** - ドロップダウン メニューから時刻を選択します。既定値は**午前 0 時**です。

3 「**サマリの頻度**」ドロップダウン メニューで「**7 日ごと**」または「**14 日ごと**」を選択した場合は、「**サマリを送信する日**」オプションが使用可能になります。ユーザが電子メール通知を受け取る日付をカスタマイズするには、次のどちらかを選択します。

メモ：個々のユーザはこの設定をオーバーライドできます。

- **1 週間のうちいつでも** (既定)
- **サマリを送信する日** - ドロップダウン メニューから曜日を選択します。既定値は**月曜日**です。

4 必要に応じて、「**タイム ゾーン**」ドロップダウン メニューからグリニッジ標準時 (GMT) を選択して、頻度の決定に使用されるようにします。

5 「**メッセージ設定**」セクションの「**サマリの対象**」オプションからメッセージ サマリに含める対象を選択します。

- **すべてのジャンク メッセージ** (既定)
- **ジャンクの可能性が高いメッセージのみ (確実なジャンクは表示しない)**

6 必要に応じて、「**サマリ E メールの言語**」ドロップダウン メニューから電子メールの言語を選択します。

7 「**平文サマリ (グラフィックなし) を送信**」の場合は、「**平文サマリ**」チェックボックスを使用して、サマリにグラフィックを含めるかどうかを選択します。既定では、サマリにグラフィックが含まれています。

a どちらかのバージョンのサンプルを表示するには、該当するリンクを選択します。

- **平文の例を表示**

ジャンク ボックス サマリ :biz@example.com

組織は、過去 24 時間以内に 8040 個のジャンク E メールと 1122 個の良性 E メールを受信しました。

遮断されたジャンク E メール数 :24
前回のジャンク ボックス サマリ以降に、以下の E メールがあなたの個人用ジャンク ボックスに保管されました。これらの E メールは 90 日後に削除されます。これらのメッセージを受信するには、「非ジャンク化」をクリックしてください。メッセージは受信トレイに配信されるようになります。

ジャンク ボックス サマリ

[非ジャンク化] [表示]	johnn@180solutions.com	Re:180 Advertising
[非ジャンク化] [表示]	dmcswzzain@hotmail.com	-*- YES, Earn a Doctors income wi...
[非ジャンク化] [表示]	support@ebay.com	Win Free Stuff
[非ジャンク化] [表示]	spammer@corp.net	Take Some Viagra, its Cheap
[非ジャンク化] [表示]	jlef@mb12.com	Enlarge another body part
[非ジャンク化] [表示]	sally@getitup.com	Nigerian Prince wants your PIN number
[非ジャンク化] [表示]	edd@aled.net	Mortgage rates that are just OK
[非ジャンク化] [表示]	aber@ls.i.ua	95% off of our Yahts
[非ジャンク化] [表示]	save@real-profesions.com	Become a surgeon in only two weeks
[非ジャンク化] [表示]	openit@dareyou.com	Open this attachment:crack.exe
[非ジャンク化] [表示]	cuz@find-family.com	Your long lost half cousin
[非ジャンク化] [表示]	tic-tac@halatosis.com	Does your breath stink?Mine did
[非ジャンク化] [表示]	smash-mouth@onthesun.com	Hey now, your an all-star, go play
[非ジャンク化] [表示]	wow@cards-for-all.com	Playing cards of Canada's Most Wanted
[非ジャンク化] [表示]	mr.tingles@petstylist.com	Pajamas for your Poodle
[非ジャンク化] [表示]	info@paypal.com	Paypal lost your info.Please submit again
[非ジャンク化] [表示]	strawberry@jam12.net	Platinum Membership to the Jam Club
[非ジャンク化] [表示]	sir@mixalot.com	I like big butts and I can not lie
[非ジャンク化] [表示]	hard-drive@yourpc.com	A Message From Your Computer:I need updates
[非ジャンク化] [表示]	warning@alertsPC.com	*!Alert.Read this.Click on buttons or BOOM
[非ジャンク化] [表示]	31331@haxor.i.ua	l33t H@x0r eZ xP10ts
[非ジャンク化] [表示]	ez@speller.com	Learn to read words like a Pro
[非ジャンク化] [表示]	biggy@fat-guru.com	Secret strategies of staying unemployed and fat
[非ジャンク化] [表示]	opportunity@yesyoucan.com	Crop dusting jobs for Arab Americans

個人用のジャンク E メール遮断設定を管理するには、標準のユーザ名とパスワードを使用して次のサイトにログインしてください。
http://twinpeaks.corp.example.com

Junk blocking by SonicWall, Inc.

- **グラフィックの例を表示**

SONICWALL | Junk Box Summary
for sotot@sonicwall.com

組織が過去 24 時間に受け取ったメッセージ
8375 個のジャンク E メール
2094 個の良性 E メール

遮断されたジャンク E メール数 :8

前回のジャンク ボックス サマリ以降に、以下の E メールがあなたの個人用ジャンク ボックスに保管されました。これらの E メールは 90 日後に削除されます。これらのメッセージを受信するには、「非ジャンク化」をクリックしてください。メッセージは受信トレイに配信されるようになります。

E メールの送信先:biz@example.com　　ジャンク ボックスにアクセス

	送信者	件名	脅威
非ジャンク化 | 表示	support@ebay.com	Official notice to biz@mailfrontier.com from Ebay Inc.	フィッシング
非ジャンク化 | 表示	dmcswzzain@hotmail.com	-*- YES, Earn a Doctors income wi...	スパム
非ジャンク化 | 表示	spammer@corp.net	Win Free Stuff	スパム
非ジャンク化 | 表示	jlef@mb12.com	Take Some Viagra, its Cheap	スパム
非ジャンク化 | 表示	sally@getitup.com	Enlarge another body part	スパム
非ジャンク化 | 表示	edd@aled.net	Nigerian Prince wants your PIN number	スパム
非ジャンク化 | 表示	aber@ls.ua	Morgage rates that are really just ok	スパム
非ジャンク化 | 表示	savenow@yahts.com	95% off of our Yahts	スパム

アンチスパム設定
許可/遮断リストの管理
アンチスパム適用度の設定

スパム管理設定
スパム E メールに対する措置の変更
ジャンク ボックス サマリの送信頻度/時期の変更
他の人への管理権限の委譲
ジャンク E メール レポートの参照
アンチスパム アプリケーションのダウンロード

個人用のジャンク E メール遮断設定を管理するには、
標準のユーザ名とパスワードを使用して次のサイトにログインしてください。
http://mtrose.corp.example.com

Junk blocking by SonicWall, Inc.

b ウィンドウを閉じます。

8 「**その他の設定**」セクションで、電子メール ジャンクボックス サマリ通知の表示方法を「**メッセージの [シングル クリック] 表示を有効にする**」オプションから選択します。

- **オフ**
- **メッセージのみを表示 (ユーザはユーザ名やパスワードを入力することなくメッセージをプレビューすることができます)**(既定)
- **完全アクセス (ジャンク ボックス サマリ内の任意のリンクを選択すると、この特定のユーザ設定への完全アクセス権限が与えられます)**

9 電子メール メッセージを非ジャンク化するための認証をユーザに許可するには、「**非ジャンクの認証を有効化**」チェックボックスをオンにします。このオプションは、既定では選択されていません。

10 ジャンク ボックス サマリ通知を LDAP のユーザのみに制限するには、「**LDAP に登録されているユーザにのみジャンク ボックス サマリ メールを送信**」チェックボックスをオンにします。

11 非 LDAP ユーザの認証を有効にするには、「**非 LDAP ユーザの認証を有効にするにはここを選択してください**」のリンクを選択します。「**アンチスパム > ユーザ**」ページが表示されます。ユーザの管理の詳細については、ジャンク サマリの管理を参照してください。

12 「**他の設定**」セクションでは、「**サマリ送信元電子メール アドレス**」からオプションを選択することで、サマリの送信方法を選択します。:

- **受信者自身の電子メール アドレスからサマリを送信** (既定)
- **この電子メール アドレスからサマリを送信**

a) フィールドに電子メール アドレスを入力します。

13 「**サマリ送信元氏名**」フィールドに、サマリ電子メールの場合にユーザの電子メールに表示される氏名を選択します。既定の名前は「**ジャンク サマリ管理者**」です。

14 「**電子メール件名**」フィールドに、ジャンク ボックス サマリ メールの件名を入力します。既定の設定は「**遮断されたジャンク電子メールのサマリ**」です。

15 「**ユーザ画面の URL**」フィールドは、サーバ設定に基づいて自動的に入力されます。ジャンク ボックス サマリ メールのすべてのリンクの基礎になります。この設定が行われている場合、ユーザの受信済み電子メール脅威がリストされている、各ユーザのジャンク ボックス サマリ メールが送信されます。

ジャンク ボックス サマリ メールには、以下の操作を行うための URL が含まれます。

- 検疫された電子メールの表示。
- 検疫された電子メールの非ジャンク化。ユーザは、ジャンク ボックス サマリ メール内のリンクを選択することによって、そのメール内の項目を非ジャンク化できます。
- ジャンク ボックスへのログイン。

重要：この URL を変更した場合は、接続が確実に行われるように、「**接続のテスト**」 接続のテスト ボタンを選択してリンクをテストします。テストが失敗する場合は、URL が正しいかどうかを確認します。

16 「**変更を適用**」ボタンを選択します。

既定値に戻す

いつでもすべてのカスタム設定を既定の設定に戻すことができます。

既定の設定に戻すには、以下の手順に従います。

1 「**戻す**」ボタンを選択します。

31

ジャンク ボックスの表示の設定

メモ：アンチスパムは、SuperMassive シリーズまたは NS*a* 9250 以降のファイアウォールではサポートされていません。

- アンチスパム > ジャンク ボックス
- ジャンク ボックス タブについて
- メッセージの検索
- ジャンク ストア内のメッセージの管理

アンチスパム > ジャンク ボックス

「調査 | ログ > アンチスパム > ジャンクボックス」ページでは、Exchange サーバまたは SMTP サーバのジャンク ストア内に現在あるすべての電子メール メッセージを表示、検索、および管理できます。

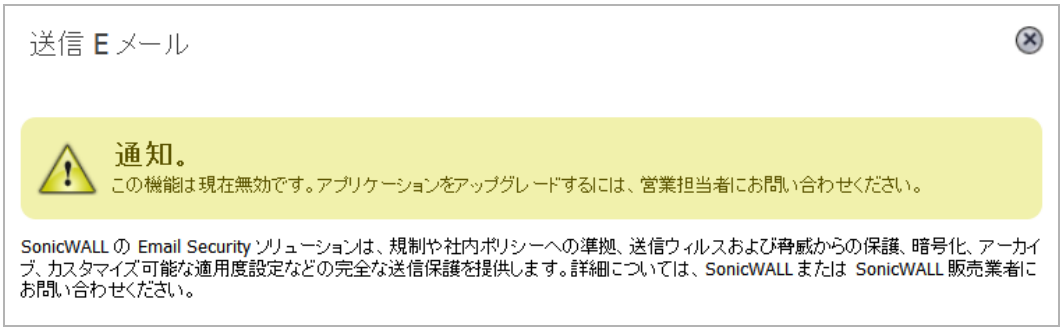
メモ：このページは、ジャンク ストアがインストールされている場合にのみ使用できます。

ジャンク ボックス タブについて

「**調査 | ログ | アンチスパム ジャンクボックス**」ページには、次の 2 つのタブがあります。

- **受信** - 受信メッセージのみが表示されます。
- **送信** - 送信メッセージのみが表示されます。

メモ：「**送信**」ビューを表示できない場合は、ジャンク ストアのライセンスをアップグレードする必要があります。**疑問符**アイコンを選択すると、次のメッセージが表示されます。



2 つのタブの機能と表示は同じです。各ビューには次の 2 つのセクションがあります。

- **簡易/詳細検索モード**
- **見つかったメッセージ**

どちらのセクションも、**展開/折りたたみ**アイコンを選択することで展開したり折りたたんだりできます。

「**簡易検索モード**」セクションには、他のページへのリンクが 2 つあります。

- ジャンク メールを破棄するまでの保持期間を変更するには、セクションの一番上にある「**ジャンク ボックス内のアイテムを nn 日後に削除します**」の末尾にあるリンクを選択します。
- 「**アンチスパム > ジャンクボックス設定**」ページを表示するには、セクションの一番下にある「**設定**」ボタンを選択します。

「見つかったメッセージ」テーブルに表示される情報

「**見つかったメッセージ**」テーブルには、隔離メッセージに関する以下の情報が表示されます。

隔離メッセージに関する情報

列	格納または示唆する内容
チェックボックス アイコン	テーブル内の各項目のチェックボックス。見出しにある**チェックボックス** アイコンを選択すると、テーブル内のすべての項目が選択されます。
送信先	受信者の電子メール アドレスです。
脅威	電子メールがもたらす脅威の種別。脅威の種別についての詳細な情報については、電子メール脅威種別の設定の電子メール脅威種別の設定: オプション テーブルを参照してください。
クリップ アイコン	電子メールに添付ファイルがあります。
件名	電子メールの件名行です。

隔離メッセージに関する情報

列	格納または示唆する内容
送信元	送信者の電子メール アドレスです。
受信	電子メールが送信された日付です。

「**見つかったメッセージ**」テーブルの上部と下部にあるボタンを使用すると、以下のジャンク ストア管理タスク (メッセージ テーブルのボタン テーブル を参照) を「**調査 | ログ | アンチスパム ジャンクボックス**」ページで実行できます。

メッセージ テーブルのボタン

ボタン	機能
削除	選択されているメッセージをジャンク ストアから完全に削除します。すべてのメッセージを削除するには、テーブルの見出しにあるチェックボックスをオンにします。
非ジャンク化	選択されているメッセージをジャンク ストアから削除し、アドレス指定されているユーザに配信します。配信日時は、それぞれのメッセージがユーザのメールボックスに配信されたときに Exchange サーバによって設定されます。
コピーの宛先	選択されているメッセージをジャンク ストアに保管したまま、そのコピーをユーザに送信します。

メッセージの検索

ジャンク ストア内に見つかったメッセージに対し、次の 2 つの種別の検索を実行できます。

- 簡易検索 (簡易検索の実行を参照)
- 詳細検索 (詳細検索の実行を参照)

簡易検索の実行

ジャンク ストアを検索するには:

1 「**調査 | ログ | アンチスパム ジャンクボックス**」ページで、「**受信**」ビューまたは「**送信**」ビューを選択します。

2 検索するテキストを「**検索対象**」フィールドに入力します。

文の語句は引用符 (") で囲みます。ブール演算子 (AND、OR、NOT) を使用できます。

3 「**対象タブ**」ドロップダウン メニューから検索の範囲とする電子メール フィールドを選択します。

- **件名** (既定)
- **送信元**
- **宛先**
- **一意のメッセージ ID**

4 「**対象**」ドロップダウン メニューで、検索する日付を選択します。

- 「**--- すべて表示 ---**」 (既定)
- **今日**
- 特定の日付。日付の数はジャンク メッセージの保持期間の長さによって変わります。

5 「**検索**」ボタンを選択して、検索を実行します。

結果はページの「**見つかったメッセージ**」セクションに表示され、最上部にはメッセージが表示されます。検索に成功した場合、メッセージには「**成功**」という単語が含まれており、メッセージ全体が緑色で強調表示されます。検索に成功しなかった場合、メッセージには「**警告**」という単語が含まれており、メッセージ全体が黄色で強調表示されます。

6 「**Messages Found**」テーブルを元の状態に戻すには、以下の手順に従います。

a 「**検索対象**」フィールドからデータを削除します。

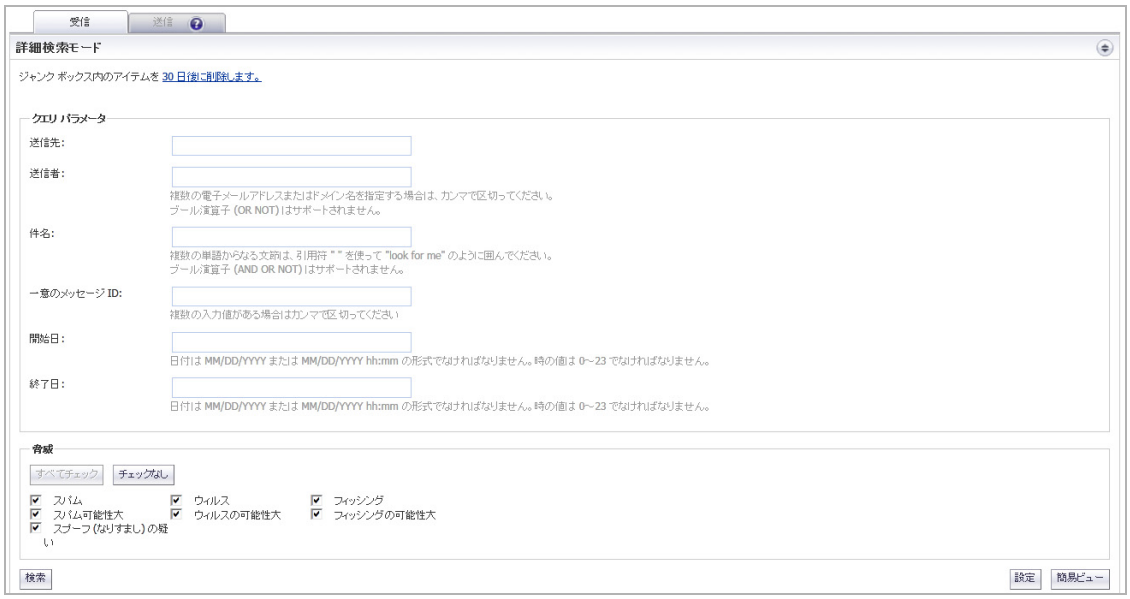
b 「**検索**」を選択します。

詳細検索の実行

1 「**調査 | ログ > アンチスパム ジャンクボックス**」ページで、「**受信**」ビューまたは「**送信**」ビューを選択します。

メモ：設定を変更するには、「**ジャンク ボックス内のアイテムを *nn* 日後に削除します**」にあるリンクを選択して、「**アンチスパム > ジャンクボックス設定**」ページを表示します。

2 「**詳細ビュー**」ボタンを選択します。「**簡易検索モード**」が展開されて「**詳細検索モード**」セクションになります。



3 「**クエリ パラメータ**」セクションでは、1 つ以上の「**クエリ パラメータ**」フィールドに検索条件を入力します。

パラメータ	クエリ基準
送信先	受信者の電子メール アドレスです。
送信者	送信者の電子メール アドレスです。 複数の電子メール アドレスやドメイン名はカンマで区切ります。ブール演算子 OR および NOT がサポートされています。
件名	電子メールの件名です。 文の語句は引用符 (") で囲みます。ブール演算子 AND、OR、および NOT がサポートされています。
一意のメッセージ ID	一意のメッセージ ID です。 複数の入力値がある場合はカンマで区切ります。
開始日	検索する最初の日付です。 日付は次のいずれかの形式で入力します。 • MM/DD/YYYY • MM/DD/YYYY hh:mm (時間の部分には 0 ～ 23 [24 時間表示] の値を指定します)。
終了日	検索する最後の日付です。 日付は次のいずれかの形式で入力します。 • MM/DD/YYYY • MM/DD/YYYY hh:mm (時間の部分には 0 ～ 23 [24 時間表示] の値を指定します)。

4 「**脅威**」セクションでは、検索対象となる脅威の種別を指定します。既定では、すべての種別が選択されています。

検索に含めたくない種別があれば、該当するチェックボックスをオフにして、その種別の選択を解除します。すべての種別の選択を解除するには、「**チェックなし**」 チェックなし ボタンを選択します。すべての種別の選択が解除され、「**すべてチェック**」 すべてチェック ボタンがアクティブになり、「**チェックなし**」ボタンが淡色表示になります。

「**アンチスパム > 設定**」ページの「**ジャンク ボックスに保管**」に設定されている電子メール脅威の種別の 1 つに属するメッセージだけが、ジャンク ストアに含められます。ただし、その種別のメッセージがジャンク ストアに保管されているかどうかに関係なく、このページにはすべての種別が表示されます。

ⓘ **メモ**：これらの設定を変更するには、「**設定**」ボタンを選択します。「**アンチスパム > ジャンクボックス設定**」ページが表示されます。

5 「**検索**」ボタンを選択して、検索を実行します。

結果はページの「**見つかったメッセージ**」セクションに表示され、最上部にはメッセージが表示されます。検索に成功した場合、メッセージには「**成功**」という単語が含まれており、メッセージ全体が緑色で強調表示されます。検索に成功しなかった場合、メッセージには「**警告**」という単語が含まれており、メッセージ全体が黄色で強調表示されます。

6 「**簡易ビュー**」に戻るには、「**簡易ビュー**」ボタンを選択します。

7 「**見つかったメッセージ**」テーブルを元の状態に戻すには、以下の手順に従います。

a 「**検索対象**」フィールドからデータを削除します。

b 「**検索**」を選択します。

ジャンク ストア内のメッセージの管理

ⓘ **ヒント**：ジャンク ストアの検索を行わない場合は、「**簡易/詳細検索モード**」セクションの**折りたたみ**アイコンを選択します。

ジャンク ストア メッセージの削除、非ジャンク化、またはコピーの送信を行うことができます。

ジャンク ストアを管理するには、以下の手順に従います。

1 「**調査 | ログ | アンチスパム ジャンクボックス**」ページで、「**見つかったメッセージ**」テーブルが表示されるまで画面をスクロールします。

2 管理するメッセージのチェックボックスをオンにします。

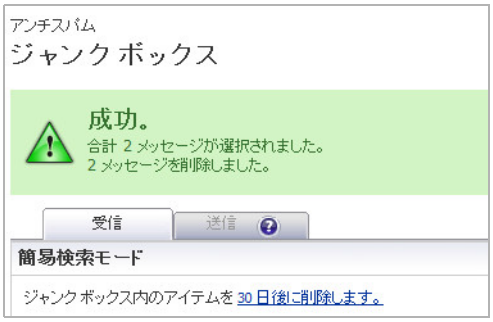
ⓘ **ヒント**：すべてのメッセージを選択するには、テーブル見出しのチェックボックスをオンにします。すべてのチェックボックスが選択されます。

3 以下のようにして管理タスクを実行します。

- 選択されているメッセージをジャンク ストアから完全に削除するには、「**削除**」ボタンを選択します。

  メモ：メッセージは 30 日後に自動的に削除されます。

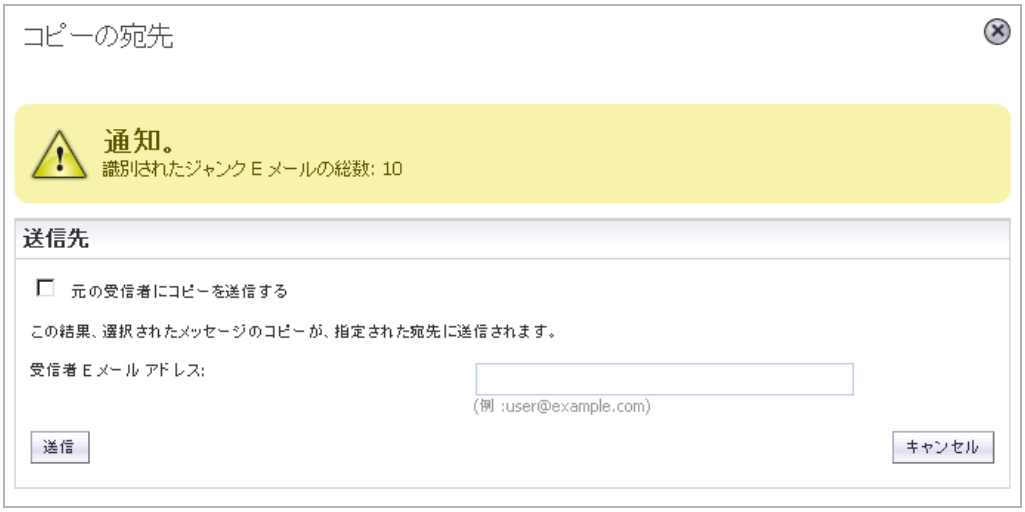
  選択されているメッセージの削除は直ちに行われます。削除前の確認用ダイアログ ボックスは表示されません。削除に成功した場合、ページの上部に緑色で通知が表示されます。削除に失敗した場合は、赤色で通知が表示されます。



- 選択されているメッセージをジャンク ストアから削除して受信者に配信するには、「**非ジャンク化**」ボタンを選択します。

  選択されているメッセージは非ジャンク化され、直ちに送信されます。この動作を実行する前の確認用ダイアログ ボックスはありません。この動作の実行に成功した場合、ページの上部に緑色で通知が表示されます。削除に失敗した場合は、赤色で通知が表示されます。

- 選択されているメッセージのコピーをユーザに送信するには、「**コピーの宛先**」ボタンを選択します。「**コピーの宛先**」ダイアログが表示されます。



  a) 以下のいずれかを実行します。
  - 「**元の受信者にコピーを送信する**」を選択します。
  - 「**受信者 E メール アドレス**」フィールドに電子メール アドレスを入力します。

  b) 「**送信**」 送信 ボタンを選択します。

選択されているメッセージは直ちに送信されます。この動作を実行する前の確認用ダイアログ ボックスはありません。この動作の実行に成功した場合、ページの上部に緑色で通知が表示されます。削除に失敗した場合は、赤色で通知が表示されます。

32

ユーザに表示される設定の構成

メモ：アンチスパムは、SuperMassive シリーズまたは NSa 9250 以降のファイアウォールではサポートされていません。

- アンチスパム > ユーザ画面セットアップ
- ユーザ画面セットアップの構成
- 既定の設定に戻す

アンチスパム > ユーザ画面セットアップ

「アンチスパム > ユーザ表示設定」ページでは、ユーザに対して表示する設定を選択および設定できます。

ユーザ画面セットアップの構成

メモ：選択されているオプションがユーザのナビゲーション ツールバーに表示されます。

ユーザに表示される設定を構成するには、以下の手順に従います。

1 「**ユーザ画面セットアップ**」セクションでは、ユーザが自分のアドレス帳（人、企業、リスト）をナビゲーション ツールバーに表示できるようにするために、「**アドレス帳**」チェックボックスをオンにします。このオプションは、既定では選択されています。

2 ヘルプデスクがユーザの電子メールに関する問題を表示できるようにするには、「**ヘルプデスク ユーザへの監査ビューを許可**」チェックボックスをオンにします。このオプションは、既定では選択されていません。

3 「**ユーザ ダウンロード設定**」セクションでは、Outlook ユーザによるジャンク ボタンのダウンロードを許可するために、「**ユーザに SonicWall Junk Button for Outlook のダウンロードを許可**」チェックボックスをオンにします。このオプションは、既定では選択されています。

4 Outlook および Outlook Express のユーザに Anti-Spam Desktop のダウンロードを許可するために、「**ユーザに SonicWall Anti-Spam Desktop for Outlook と Outlook Express のダウンロードを許可**」チェックボックスをオンにします。このオプションは、既定では選択されています。

5 Outlook ユーザに Secure Mail プラグインのダウンロードを許可するために、「**SonicWall Secure Mail の Outlook プラグインのダウンロードをユーザに許可する**」チェックボックスをオンにします。このオプションは、既定では選択されています。

6 「**検疫されたジャンク メールのプレビュー設定**」セクションで、ユーザに検疫されたジャンク メールのプレビューを許可するために、「**ユーザは自分が所有する検疫済みジャンク メールをプレビュー可能**」チェックボックスをオンにします。このオプションは、既定では選択されています。

7 管理者がすべての検疫されたジャンク メールをプレビューできるようにするには、「**管理者**」チェックボックスをオンにします。このオプションは、既定では選択されています。

メモ：管理者には、既定で、組織全体のすべての検疫済みジャンク メールをプレビューできるアクセス権があります。このオプションを変更するには、「**管理者**」チェックボックスをオフにします。

8 必要な変更をすべて行った後、「**変更を適用**」ボタンを選択します。

既定の設定に戻す

いつでもすべての設定を工場出荷時の設定に戻すことができます。

それまでに行われた変更をすべてクリアして既定の設定に戻すには、次の操作を行います。

1 「**戻す**」ボタンを選択します。

33

企業の許可および遮断リストの設定

メモ：アンチスパムは、SuperMassive シリーズまたは NS*a* 9250 以降のファイアウォールではサポートされていません。

- アンチスパム > アドレス帳 (336 ページ)
- タブについて (337 ページ)
- 許可または遮断リストへの項目の追加 (338 ページ)
- 許可または遮断リストからの項目の削除 (339 ページ)
- アドレス帳エントリのインポート (339 ページ)
- アドレス帳エントリのエクスポート (340 ページ)
- 許可および遮断リストの検索 (340 ページ)

アンチスパム > アドレス帳

「**アンチスパム > アドレス 帳**」ページでは、組織の許可リストと遮断リストを設定できます。これらのリストは、組織のリストとファイアウォールによって提供されるリストにある許可する送信者と遮断する送信者をそれぞれ統合したものです。

メモ：「**遮断**」ビューでアドレスのフィルタに使用できるのは人、IP、企業だけですが、「**許可**」ビューでは人、企業、IP、リストによるアドレスのフィルタが可能です。

リストが長すぎる場合は、検索機能を使用して必要なテーブル エントリのみを表示できます。

タブについて

「**許可**」および「**遮断**」という 2 つのタブは、ほぼ同じです。ただし、「**人**」、「**企業**」、「**IP**」という検索種別はどちらのページにもありますが、「**リスト**」は「**許可**」ページにしかありません。

トピック:

- 許可リスト
- 遮断リスト

許可リスト

「**許可**」ビューでは、人、企業、IP アドレス、またはリストに対し、組織へのメールの送信を許可できます。アドレス ブックを許可リストにインポートしたり、企業アドレス ブックを Excel スプレッドシートやテキスト ファイルにエクスポートしたりできます。

遮断リスト

メモ：管理者によって企業遮断リストに追加された送信者は、すべてのユーザで自動的に遮断され、管理者だけがリストから削除できます。

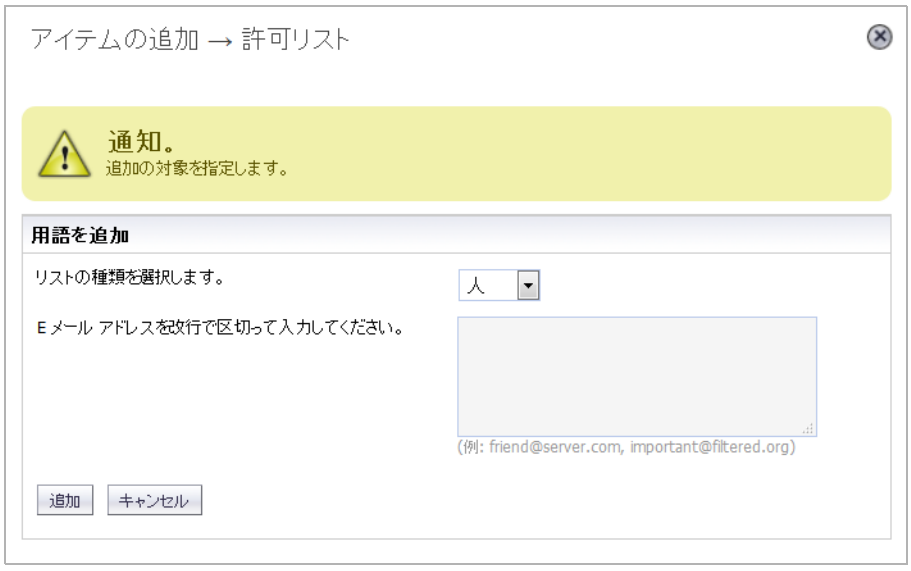
「**遮断**」ビューでは、人、企業、IP アドレスに対し、組織へのメールの送信を制限できます。アドレス ブックを遮断リストにインポートしたり、企業アドレス ブックを Excel スプレッドシートやテキスト ファイルにエクスポートしたりできます。

許可または遮断リストへの項目の追加

企業許可/遮断リストに項目を追加するには、以下の手順に従います。

1 「**アンチスパム > アドレス 帳**」の適切なビューに移動します。

2 「**追加**」ボタンを選択します。「**アイテムの追加 → 許可リスト**」ダイアログが表示されます。



3 「**リストの種類を選択します。**」ドロップダウン メニューからリスト ユーザの種別を選択します。

- **人**
- **企業**
- **リスト** (「**許可**」ビューでのみ使用可能)
- **IP**

4 フィールドにアドレス/ドメインを入力します。フィールド名は、選択したリスト種別によって次のように異なります。

- **人 - 改行コードで区切って IP アドレスを入力します**

- **企業 - 改行コードで区切ってドメインを入力します**
- **リスト - 改行コードで区切ってメーリング リストを入力します**
- **IP - 改行コードで区切って IP アドレスを入力します**

5 「**追加**」を選択して終了します。アドレス/ドメインは、「**許可/遮断**」ビューの「**リスト**」に追加されます。

許可または遮断リストからの項目の削除

企業許可/遮断リストから送信者を削除するには、以下の手順に従います。

1 適切なビューを選択します。

2 削除する電子メール アドレスの隣にあるチェックボックスをオンにします。「**削除**」ボタンが使用可能になります。

3 「**削除**」ボタンを選択します。削除の成功を確認するためのメッセージが表示されます。

ヒント： すべてのエントリを削除するには、テーブル見出しのチェックボックスをオンにします。

アドレス帳エントリのインポート

1 つ以上のアドレス帳からエントリをインポートできます。

アドレス帳のエントリをインポートするには、以下の手順に従います。

1 適切なビューを選択します。

2 「**インポート**」ボタンを選択します。「**アドレス帳のインポート**」ダイアログが表示されます。

3 「**Browse...**」ボタンを選択します。Windows の「**ファイル アップロード**」ダイアログが表示されます。

4 アップロードするファイルを選択します。次の形式になっている必要があります。

<TAB>D/L/E/I<TAB>A/B<TAB>*アドレス リスト*<CR>

ここで、

D/L/E/I は、ドメイン/リスト/電子メール/IP アドレス、

A/B は、許可/遮断、

アドレス リストは、カンマで区切られたアドレス帳エントリであり、

電子メール アドレス、ドメイン、IP アドレス、リストは改行コードで区切られたものです。

以下に例を示します。

```
<TAB>E<TAB>A<TAB>email1@company.com,email2@company.com<CR>
<TAB>L<TAB>B<TAB>list1@company.com,list2@company.com<CR>
```

5 「**開く**」を選択します。

6 「**インポート**」を選択します。

アドレス帳エントリのエクスポート

エントリを Excel スプレッドシートまたはテキスト ファイルにエクスポートできます。

アドレス帳のエントリをエクスポートするには、以下の手順に従います。

1 適切なビューで、「**エクスポート**」ボタンを選択します。Windows の「***ファイル名を開く***」ダイアログが表示されます。

2 以下のどちらかを選択してください。

- **Microsoft Excel で開く (既定)**
- **ファイルを保存する**

3 「**OK**」を選択します。

許可および遮断リストの検索

検索フィールドは、「**許可**」および「**遮断**」テーブル内の許可エントリや遮断エントリをすばやく見つけ出すために使用できます。このフィールドには、「**許可**」ビューまたは「**遮断**」ビューからアクセスできます。

許可または遮断リストを検索するには、以下の手順に従います。

1 適切なビューを選択します。

2 「**検索**」セクションに移動します。

3 「**検索**」フィールドにアドレスまたはドメインを入力します。複数のエントリを入力する場合はカンマで区切ります。

4 また、検索バーの下のチェックボックスを選択することで、検索対象のアドレスの**種別** (**人**、**企業**、**IP**、または**リスト** [許可リストのみ]) でフィルタ処理できます。

5 「**実行**」ボタンを選択して、検索を開始します。結果は「**リスト**」テーブルに表示されます。

検索フィールドを消去するには、以下の手順に従います。

1 「**リセット**」ボタンを選択します。

34

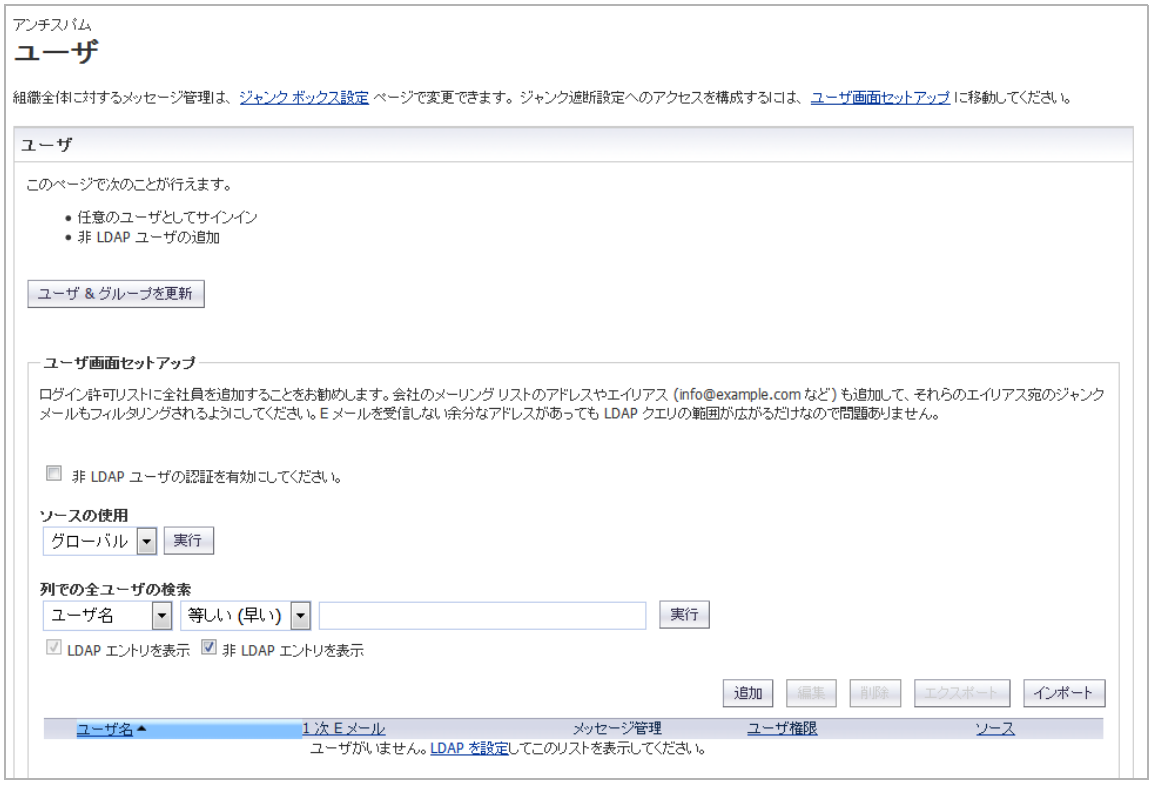
ユーザの管理

メモ：アンチスパムは、SuperMassive シリーズまたは NS*a* 9250 以降のファイアウォールではサポートされていません。

- アンチスパム > ユーザ管理 (341 ページ)
- ユーザ テーブルの更新 (342 ページ)
- LDAP 以外のユーザ認証の有効化 (342 ページ)
- ユーザの表示 (343 ページ)
- ユーザの追加 (345 ページ)
- ユーザとしてのサインイン (347 ページ)

アンチスパム > ユーザ管理

「**アンチスパム > ユーザ管理**」ページでは、グローバル サーバと LDAP サーバの両方のすべてのユーザを追加、削除、および管理できます。LDAP 設定の詳細については、ユーザの管理を参照してください。



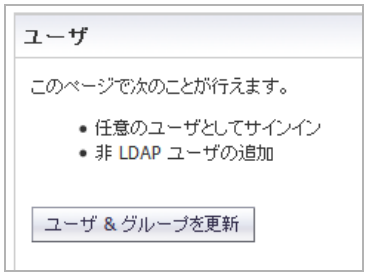
「**ユーザ**」テーブルには、以下の情報が表示されます。

列	説明
ユーザ名	ユーザのユーザ名です。プライマリ電子メール アドレスの一部でなくても構いません。
1 次 E メール	ユーザの電子メール アドレスです。
メッセージ管理	ユーザが「**アンチスパム > ジャンク ボックス サマリ**」ページの設定に従っているか、それともその設定を変更しているかを表示します。 • **既定** - すべての管理者の設定が使用されます • **個別** - ユーザが 1 つ以上の設定を変更しています
ユーザ権限	CASS ではユーザの権限を変更できないので、必ず「**ユーザ**」になります。
ソース	ユーザのサーバ名を表示します。

ユーザ テーブルの更新

ユーザ テーブル内のユーザのリストを更新するには、以下の手順に従います。

1 「**アンチスパム > ユーザ管理**」の「**ユーザ**」セクションに移動します。



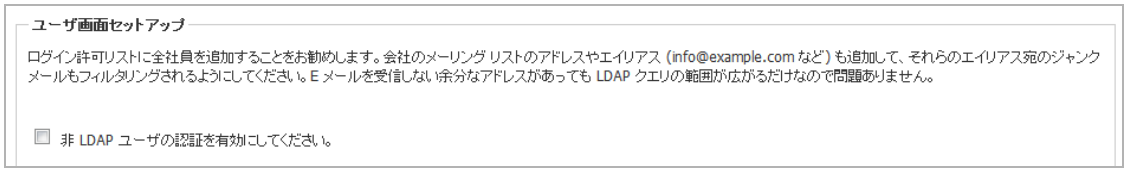
2 「**ユーザ＆グループを更新**」  ボタンを選択します。

LDAP 以外のユーザ認証の有効化

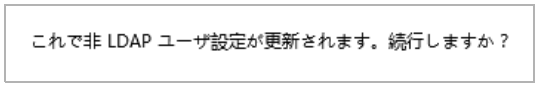
非 LDAP ユーザ向けの認証を有効にする必要があります。

非 LDAP ユーザ向けの認証を有効にするには、以下の手順に従います。

1 「**アンチスパム > ユーザ管理**」の「**ユーザ表示設定**」セクションが表示されるまで画面をスクロールします。



2 「**非 LDAP ユーザの認証を有効にしてください。**」チェックボックスをオンにします。注意を促すメッセージが表示されます。



3 「**OK**」を選択します。

ユーザの表示

「**ユーザ テーブル**」には、ログインできるすべてのユーザが表示されます。以下の操作により、ユーザをフィルタ処理してその時点で確認したいユーザだけを表示できます。

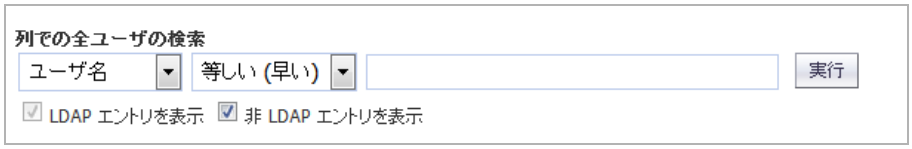
- ユーザ種別の選択。表示するユーザの種別の選択 (343 ページ)
- ソース (サーバ) の選択。表示するサーバのユーザの選択 (343 ページ) を参照してください。
- 特定ユーザの指定。ユーザの検索 (344 ページ)を参照してください。

表示するユーザの種別の選択

すべてのユーザを表示したり、LDAP ユーザまたは非 LDAP ユーザのみを表示したりできます。

表示するユーザの種別を選択するには、以下の手順に従います。

1 「**アンチスパム > ユーザ管理**」の「**列での全ユーザの検索**」セクションが表示されるまで画面をスクロールします。



2 次のいずれかのユーザ種別を選択します。

- LDAP のみの場合 - 「**LDAP エントリを表示**」チェックボックスをオンにします。システムに LDAP ユーザしかいない場合は、これが既定の設定です。
- 非 LDAP のみの場合 - 「**非 LDAP エントリを表示**」チェックボックスをオンにします。システムに非 LDAP ユーザしかいない場合は、これが既定の設定です。
- LDAP と非 LDAP の両方の場合 - どちらのチェックボックスもオンにします。システムにどちらの種別のユーザもいる場合は、これが既定の設定です。

表示するサーバのユーザの選択

「**ユーザ**」テーブルに制限をかけて、特定のサーバのユーザのみを表示できます。

ソース (サーバ) を選択するには、以下の手順に従います。

1 「**ユーザ表示設定**」のフィルタ セクションに移動します。

2 「**ソースの使用**」ドロップダウン メニューから、表示するサーバ (ソース) を選択します。

- **グローバル** (既定) - グローバル サーバは常に使用可能です
- LDAP サーバ名 - 1 つ以上の LDAP サーバが追加されている場合、すべてのサーバ名がリストに表示されます。

3 **実行**ボタンをクリックします。

ユーザの検索

ユーザが 1 人だけが表示されるように制限をかけることができます。

ユーザを検索するには、以下の手順に従います。

1 「**アンチスパム > ユーザ管理**」の「**ユーザ表示設定**」セクションのフィルタ セクションに移動します。

2 「**列での全ユーザの検索**」のドロップダウン メニューおよびフィールドで、選択基準を入力します。

a 最初のドロップダウン メニューで次の項目を選択します。

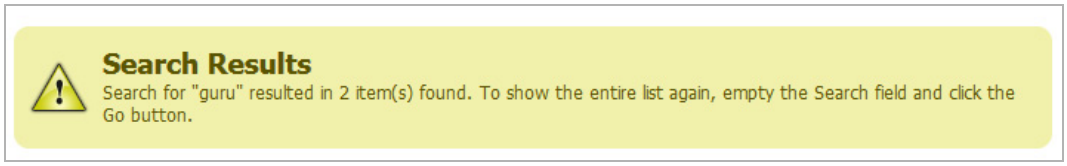
- **ユーザ名**
- **1 次 E メール**

b 2 番目のドロップダウン メニューにある以下の条件によって検索のフィルタ処理を行います。

- **等しい (早い)** (既定)
- **始まる (普通)**
- **含む (遅い)**

c フィールドにユーザの情報を入力します。

3 「**実行**」を選択します。「**ユーザ**」テーブルには、指定された基準を満たす電子メールのみが表示されます。また、ページの一番上にはメッセージが表示されます。



ユーザ テーブルの表示を復元するには、以下の手順に従います。

1 「**列での全ユーザの検索**」フィールドから検索基準を削除します。

2 「**実行**」を選択します。

ユーザの追加

次のような方法で、ログイン可能なユーザのリストにユーザを追加できます。

- 手動。ユーザ テーブルへのユーザの手動追加 (345 ページ) を参照してください。
- インポート。ユーザ テーブルへのユーザのインポート (346 ページ) を参照してください。

メモ：ログイン可能なユーザのリストにはすべての従業員を追加することをお勧めします。企業のメーリング リストのアドレスおよびエイリアス (`info@example.com` など) も、そうしたエイリアスに送信されたジャンク メールをフィルタ処理できるように追加する必要があります。LDAP クエリを幅広いものにしすぎた結果、電子メールを受信していない余分なアドレスがここに表示されたとしても問題はありません。

ユーザ テーブルへのユーザの手動追加

グローバル サーバまたはLDAP サーバにユーザを追加するには:

1 「**ユーザ テーブル**」の上にある「**追加**」ボタンを選択します。「**ユーザの追加**」ダイアログが表示されます。

2 「**1 次アドレス**」フィールドにユーザのプライマリ アドレスを入力します。

3 ユーザが LDAP ユーザの場合は、そのユーザのパスワードを「**パスワード**」および「**パスワードの確認**」フィールドに入力します。

4 「**ソースの使用**」ドロップダウン メニューから、ユーザが属するサーバを選択します。

5 必要に応じて、「**エイリアス (オプション)**」フィールドにユーザのエイリアスを入力します。エイリアスが複数の場合は、各エントリを改行コード (<CR>) で区切ります。

6 「**追加**」を選択してユーザを追加します。

ユーザ テーブルへのユーザのインポート

ファイルからユーザのリストをインポートするには、以下の手順に従います。

1 「**ユーザ テーブル**」の上にある「**インポート**」ボタンを選択します。「**ユーザのインポート**」ダイアログが表示されます。

2 「**インポート モード**」を選択して、インポートされたファイルをどのように取り扱うかを選択します。

- **追記** - 承認済みユーザのリストが含まれているファイルの末尾にユーザを追加します。
- **上書き** - 既存のユーザをインポートされたユーザで置き換えます。

3 ソースとして使用するサーバを指定します。

- **グローバル**
- LDAP サーバ名

4 「**Browse...**」ボタンを選択します。Windows の「**ファイル アップロード**」ダイアログが表示されます。

5 アップロードするファイルを選択します。ファイルの形式は、プライマリ アドレスとエイリアスの間をタブ <TAB> で区切り、エントリどうしを改行コード <CR> で区切った次のようなものになっている必要があります。

```
primary_email1@company.com<TAB>primary_email1@company.com<CR>
```

以下に例を示します。

```
primary_email1@company.com<TAB>primary_email@company.com<CR>
primary_email1@company.com<TAB>alias1@company.com<CR>
```

```
primary_email1@company.com<TAB>alias2@company.com<CR>
```

ユーザが LDAP 内に既に存在する場合、エントリは次のようになります。

```
primary_email2@company.com<TAB>alias1@company.com<CR>
primary_email2@company.com<TAB>alias2@company.com<CR>
```

6 「**開く**」を選択します。

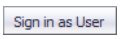
7 「**インポート**」を選択します。

ユーザとしてのサインイン

ユーザのアカウントにサインインすると、ユーザの Email Security の「**調査 | ログ > アンチスパム ジャンクボックス**」を確認できます。

ユーザとしてサインインするには、以下の手順に従います。

1 「**アンチスパム > ユーザ**」の「**ユーザ**」テーブルに移動します。

2 サインインするユーザのチェックボックスをオンにします。「**ユーザとしてサインイン**」 

ボタンがアクティブになります。

3 「**ユーザとしてサインイン**」ボタンを選択します。別のウィンドウに Email Security によるそのユーザの「**アンチスパム > ジャンク ボックス**」ページが表示されます。

4 の「**アンチスパム > ユーザ管理**」ページに戻るには、Email Security ページの**ログアウト** アイコンを選択します。

35

LDAP サーバの設定

メモ：アンチスパムは、SuperMassive シリーズまたは NS*a* 9250 以降のファイアウォールではサポートされていません。

- アンチスパム > LDAP 構成 (348 ページ)
- 利用可能な LDAP サーバ (349 ページ)
- LDAP サーバの追加 (349 ページ)
- LDAP クエリの設定 (353 ページ)
- LDAP マッピングの追加 (356 ページ)
- グローバル LDAP 設定の構成 (357 ページ)
- LDAP サーバ設定の編集 (358 ページ)
- LDAP サーバの削除 (359 ページ)

アンチスパム > LDAP 構成

「**アンチスパム > LDAP 設定**」ページでは、LDAP サーバに固有のさまざまな設定を行うことができます。

メモ：**展開/折りたたみ**アイコンを選択すると、すべてのパネルを表示または非表示にすることができます。

利用可能な LDAP サーバ

このセクションには、ファイアウォール上で設定されているすべての LDAP サーバに関する情報が表示されます。

- 「**ニックネーム**」- サーバのニックネームを表示します。リンクを選択すると、「**サーバ設定**」、「**LDAP クエリ パネル**」、「**LDAP マッピングの追加**」の各セクションが表示されます。
- **サーバ名: ポート** - サーバの IP アドレスとポートが表示されます。
- **タイプ** - サーバの種別 (Active Directory、OpenLDAP など) が表示されます。
- **ログイン方法**
- **アカウント情報** - 表示
- **設定** - **編集**アイコンと**削除**アイコンがあります。

LDAP サーバの追加

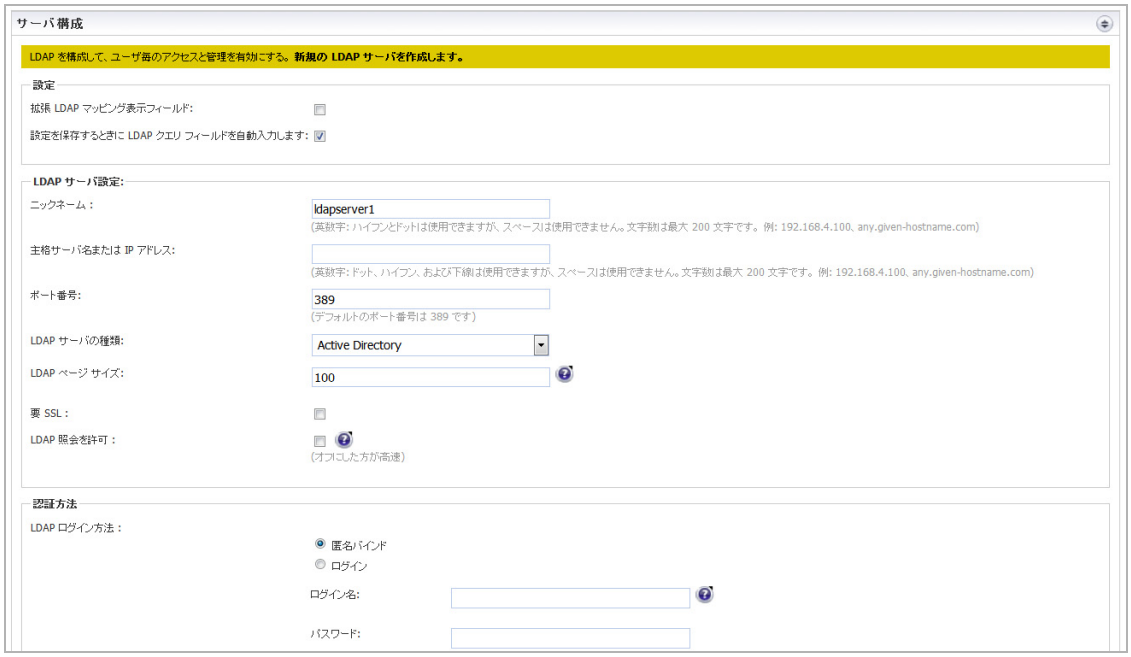
新しい LDAP サーバを設定して、ユーザ単位のアクセスおよび管理を有効にします。

重要：アンチスパムは、既存の Active Directory サーバまたは LDAP サーバを使用して、個人用ジャンク ボックスにログインするエンド ユーザの認証を行います。自らのジャンク ボックスへのログインを許可されているユーザの完全なリストを返すためには、「**アンチスパム > LDAP 構成**」ページに情報が正しく入力されている必要があります。このリストに表示されないユーザは、自らの電子メールがフィルタ処理されていますが、個人用のジャンク ボックスにログインすることができません。

LDAP 設定に情報を適切に入力するには、「**サーバ設定**」パネル、「**LDAP クエリ**」パネル、「**LDAP マッピングの追加**」パネルの設定を完了する必要があります。

LDAP サーバを追加するには、以下の手順に従います。

1 「**利用可能な LDAP サーバ**」セクションで、「**サーバの追加** サーバの追加」ボタンを選択します。「**サーバ構成**」セクションが展開されます。



2 必要に応じて、「**設定**」セクションの「**拡張 LDAP マッピング 表示フィールド**」チェックボックスを有効にします。このオプションを有効にすると、「**LDAP サーバ設定**」セクションにセカンダリ サーバ用のフィールドが赤で表示されます。

3 「**LDAP クエリ パネル**」内のフィールドが自動的に入力されるようにするには、「**設定を保存するときに LDAP クエリ フィールドを自動入力します**」チェックボックスがオンになっていることを確認します。このオプションは、既定では選択されています。

4 「**LDAP サーバ設定**」セクションで、新しい LDAP サーバの設定を行います。

> **ヒント**：プライマリおよびセカンダリ名と IP アドレスには、ハイフン (-) とピリオド (.) を含む英数字を 200 文字まで使用できますが、空白は使用できません。例:
>
> 192.168.4.100
> host-name123.com

- **ニックネーム** - LDAP サーバのわかりやすい名前を入力します。既定の名前は `ldapserver`*n* (*n* は連番) です。
- **主格サーバ名または IP アドレス** - LDAP サーバのサーバ名または IP アドレスです。

- **ポート番号** - LDAP サーバのポート番号です。既定のポート番号は **389** です。
- **セカンダリ サーバ名または IP アドレス** - セカンダリ LDAP サーバのサーバ名または IP アドレスです。

  メモ：「セカンダリ サーバ名または IP アドレス」および**「ポート番号」**オプション (赤色) は、**「拡張 LDAP マッピング フィールドを表示する」**を「設定」セクションで選択した場合にのみ表示されます。

- **ポート番号** - セカンダリ LDAP サーバのポート番号です。既定のポート番号は **389** です。
- **LDAP サーバの種類** - ドロップダウン メニューから次のいずれかを選択します。
  - **Active Directory**
  - **Lotus Domino**
  - **Exchange 5.5**
  - **Sun ONE iPlanet**
  - **その他**
- **LDAP ページ サイズ** - LDAP サーバ上で問い合わせが行われる最大ページ サイズを入力します。既定値は **100** です。

注意：問い合わせが行われる最大ページ サイズを指定する設定は、Active Directory を含む多数の LDAP サーバにあります。LDAP ページ サイズの設定が最大ページ サイズを超えている場合、LDAP サーバでもパフォーマンス上の問題が発生する可能性があります。この項目の調整が必要になる状況は滅多にありませんが、その場合は SonicWall テクニカル サポートまでお問い合わせください。

- **要 SSL** - LDAP サーバが SSL を要求するようにするには、このチェックボックスをオンにします。このオプションは、既定では選択されていません。
- **LDAP 照会を許可** - LDAP サーバが複数あってそれぞれで情報が異なる可能性がある場合は、このオプションを選択します。LDAP 照会が有効になっている場合、ある LDAP サーバが情報取得のためのログイン要求の一部を、より多くの情報を持っている別の LDAP サーバに委任できます。こうした委任は照会と呼ばれ、管理者またはユーザのログイン時に発生します。照会されたログイン要求は、処理が非常に遅くなり、20 秒以上かかる可能性があります。このオプションは、既定では選択されていません。

  メモ：以下の場合は、このオプションを無効にすることで、管理者およびユーザのログイン処理速度を上げることができます。
  - LDAP サーバが 1 台のみ。
  - 2 台以上の LDAP サーバがすべて同じ情報を共有している。

  ヒント：念のために、照会を無効にした後、ログインから遮断されるユーザがいないかどうかテストし、データや設定が失われていないことを確認してください。

5 **「認証方法」**セクションで、ユーザの LDAP ログイン方式を設定します。

- **匿名バインド** (既定) - 多くの LDAP サーバは、要求されればだれにでもユーザのリストを提供するように設定されています。これを*匿名バインド*と呼びます。

  ヒント：まずこのオプションを選択してから、テストを行います。ステップ 8 を参照してください。

- **ログイン** -「**匿名バインド**」オプションでうまくいかない場合は、このオプションを選択します。その後、ユーザ名とパスワードを入力して、LDAP からユーザのリストを取得します。

6 選択した内容によって次の手順が異なります。

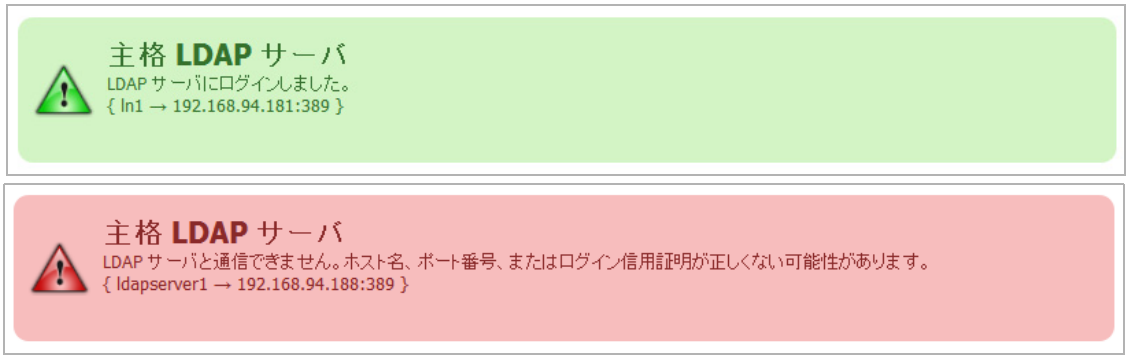
- 「**匿名バインド**」を選択した場合は、ステップ 8 に進みます。
- 「**ログイン**」を選択した場合は、ステップ 7 に進みます。

7 **ログイン名**と**パスワード**を指定します。

ログイン名は、ユーザによる LDAP リソースへのアクセスを許可するために使用される資格情報です。LDAP サーバの種別ごとにログイン名の形式があります。利用するサーバに適した形式を使用してください。

ヒント：形式の違いの例を確認するには、「**ログイン名**」フィールドの隣にある**疑問符**アイコンを選択します。

8 行った設定をテストするには、「**LDAP ログインのテスト**」 Test LDAP Login ボタンを選択します。「**テスト結果**」メッセージが表示されます。



9 「**変更を保存**」を選択して LDAP サーバの追加を完了します。「**LDAP クエリ パネル**」および「**LDAP マッピングの追加**」パネルが表示されます。

LDAP クエリの設定

ヒント：「**設定**」セクションで「**設定を保存するときに LDAP クエリ フィールドを自動入力します**」オプションを選択した場合は、「**LDAP クエリ パネル**」に既定値が自動的に設定されます。

ユーザがジャンクボックスに正常にログインできるようにするには、以下の手順に従います。

ヒント：LDAP ツリー全体を調べて LDAP 構造とそのさまざまな属性やオブジェクト クラスを包括的に把握するには、無料のプログラム Softerra LDAP Browser 2.5 (以下から入手可能) を実行します。

http://www.ldapbrowser.com/download/index.php

Windows PC でこのプログラムをダウンロードします。プログラムの実行中は、ご利用のネットワークにとって最適なクエリを決定するために、ネットワーク上のユーザを参照し、その属性を調べます。

1 「**LDAP クエリ パネル**」の「**LDAP ユーザに対するクエリ情報**」セクションに移動します。

ヒント：「**設定**」セクションの「**設定を保存するときに LDAP クエリ フィールドを自動入力します**」をオンにしていない場合は、「**ユーザ フィールドを自動入力**」ボタンを選択することで自動入力を行うことができます。

2 オプションのグループ機能を使用するには、「**検索を開始するディレクトリ ノード**」フィールド内に、ディレクトリ内のすべてのグループの情報が格納されているノードを示す完全な LDAP ディレクトリ パス (LDAP 内のディレクトリ) を指定します。このパスにより、LDAP グループの検索範囲が適度に絞り込まれます。

LDAP に含まれている情報は、通常のファイル システムの場合と非常によく似たディレクトリ ツリーの形で整理されます。各ディレクトリは、name=value というペアとして指定されます。ここで、

- name は通常、次のいずれかです。

DC (ドメイン コンポーネント)	OU (組織単位)
DN (識別名)	O (組織)

- **値**は通常、完全に指定されたホスト名の 1 セグメント (例: sales.companyxyz.com 内の単語 companyxyz) です。

LDAP 内の特定のノードを指定するには、カンマ区切りのリストを使用します。複数のノードを指定して検索するには、完全パスの間にアンパサンド (&) を使用します。

例えば、companyxyz 内にある特定のマシンのホスト名が computer27.sales.companyxyz.com の場合、LDAP パスは次のようになります。

```
DC=computer27,DC=sales,DC=companyxyz,DC=com
```

ヒント：さまざまなディレクトリ種別での例を確認するには、「**検索を開始するディレクトリ ノード**」フィールドの隣にある**疑問符**アイコンを選択します。

3 「**フィルタ**」フィールドには、標準の LDAP フィルタ構文で LDAP フィルタを入力します。

アンチスパムには、ユーザやメーリング リストの検索および識別方法を指示する必要があります。「**フィルタ**」フィールドにオブジェクト クラスやメール属性を具体的に記述することで、LDAP クエリの処理時に非プライマリ電子メール アカウント (プリンタ、コンピュータなど) が除外されます。プライマリ ユーザ アカウントのみに注目するとクエリの処理速度が向上します。

「**フィルタ**」フィールドには、次のサンプル構文が記されています。

```
(&(|(objectClass=group)(objectClass=person)(objectClass=publicFolder))
(mail=*))
```

すべての LDAP フィルタは括弧内にグループ化されており、フィルタ自体にも文字列全体を囲む括弧のペアがあります。左から 2 番目の文字がアンパサンド (&) になっています。この LDAP フィルタ構文はプレフィックス表記です。これは、このフィルタが、それぞれ括弧でグループ化された 3 つの下位フィルタの論理的 AND のみを返すことを意味します。その他の演算子としては、OR を表すパイプ (|) や NOT を表す感嘆符 (!) があります。

ヒント：さまざまなディレクトリ種別での例を確認するには、「**フィルタ**」フィールドの隣にある**疑問符**アイコンを選択します。

4 「**ユーザ　ログイン名の属性**」フィールドに、ユーザがログイン名に使用するテキスト属性を指定します。このフィールドで一般的に受け入れられる属性は、既定値である **sAMAccountName** です。この属性は、Microsoft Windows やその他すべての環境で機能するはずです。

重要：このフィールドは、連動して機能する「**フィルタ**」フィールドと一致している必要があります。sAMAccountName を変更する場合は、「**フィルタ**」フィールドと「**ユーザ ログイン名の属性**」フィールドも一緒に変更する必要があります。

ヒント：さまざまなディレクトリ種別での例を確認するには、「**ユーザ ログイン名の属性**」フィールドの隣にある**疑問符**アイコンを選択します。

5 単一のユーザをそのユーザのジャンク ボックスに関連付けるための電子メール アドレス、従業員 ID、電話番号、またはその他のエイリアス属性を「**E メール エイリアスの属性**」フィールドで指定します。

多くの企業では、1 人のエンド ユーザが複数の電子メール アカウントを持っており、それらはすべて本来の 1 つの電子メール アカウントにマッピングされています。例えば、JohnS@example.com と John.Smith@example.com はどちらも John Smith の受信ボックスで有効な電子メール アドレスになっていることがあります。アンチスパムでは、こうした状況に対応するために、あるエンド ユーザのさまざまな電子メール アドレスの電子メールすべてをグループ化する 1 つのジャンク電子メール ボックスをそのユーザが持つことができるようにしています。

このフィールドで一般的に受け入れられる属性は **proxyAddresses** です。他の属性はすべてカンマで区切る必要があります。以下に例を示します。

- `proxyAddresses,legacyExchangeDN`
- `proxyAddresses,EmployeeID,PhoneNumber`

ヒント：Microsoft Windows 環境では、多くの場合、1 つの属性 **proxyAddresses** だけで十分です。
さまざまなディレクトリ種別での例を確認するには、「**E メール エイリアスの属性**」フィールドの隣にある**疑問符**アイコンを選択します。

6 必要に応じて、設定した内容が適切に機能するかどうかをテストによって確認します。そのためには、「**LDAP ユーザに対するクエリ情報**」セクションにある「**ユーザ クエリのテスト** ユーザ クエリのテスト 」ボタンを選択します。

7 「**LDAP ユーザに対するクエリ情報**」セクションにある「**変更を保存**」を選択して、変更内容を保存します。

8 「**LDAP グループに対するクエリ情報**」セクションに移動します。

ヒント：「**設定**」セクションの「**設定を保存するときに LDAP クエリ フィールドを自動入力します**」をオンにしなかった場合は、「**グループ フィールドを自動入力** グループ フィールドを自動入力 」ボタンを選択することで自動入力を行うことができます。

9 オプションのグループ機能を使用するには、「**検索を開始するディレクトリ ノード**」フィールド内に、ディレクトリ内のすべてのグループの情報が格納されているノードを示す完全な LDAP ディレクトリ パス (LDAP 内のディレクトリ) を指定します。この設定により、LDAP グループの検索範囲が適度に絞り込まれます。この設定の詳細については、ステップ 2 を参照してください。

10 ユーザやメーリング リストの検索および識別方法をアンチスパムに指示するには、「**フィルタ**」フィールドに標準の LDAP フィルタ構文で LDAP フィルタを入力します。このフィールドには、サンプル構文が記されています。この設定の詳細については、ステップ 3 を参照してください。

11 「**グループ名の属性**」フィールドで、グループ名に対応するグループの属性を指定します。

12 グループを指定する一般的な方法として、メーリング リストがあります。LDAP のメーリング リスト エントリには、そのリストのメンバーを指定する特別なフィールドが 1 つあります。「**グループ メンバの属性**」フィールドにはその情報を入力します。

13 一部の LDAP 設定では、LDAP 内の各ユーザのエントリの内部に、そのユーザが所属するグループまたはメーリング リストの一覧を示す属性があります。「**ユーザ メンバシップの属性**」フィールドでその属性を指定します。

14 必要に応じて、設定した内容が適切に機能するかどうかをテストによって確認します。そのためには、「**LDAP グループに対するクエリ情報**」セクションにある「**ユーザ クエリのテスト** ユーザ クエリのテスト 」ボタンを選択します。

15 「**LDAP グループに対するクエリ情報**」セクションにある「**変更を保存**」を選択して、変更内容を保存します。

LDAP マッピングの追加

Microsoft Windows 環境を使用している場合は、「**LDAP マッピングの追加**」パネルで NetBIOS ドメイン名を指定する必要があります。

メモ：NetBIOS ドメイン名は、Windows 2000 以前のドメイン名と呼ばれることもあります。

LDAP マッピングを追加するには、以下の手順に従います。

1 ドメイン名を決定します。

   a ドメイン コントローラにログインします。

   b 「**スタート** > **すべてのプログラム** > **管理ツール** > **Active Directory ドメインと信頼関係**」を選択します。

   c 「**Active Directory ドメインと信頼関係**」ダイアログでドメインを選択します。

   d 「**操作**」を選択します。

   e 「**プロパティ**」を選択します。ドメインの「**プロパティ**」ダイアログの「**一般**」ビューに、ドメイン名が表示されます。

   f ドメイン名を記録します。

2 「**アンチスパム** > **LDAP 設定**」の「**LDAP マッピングの追加**」パネルに移動します。

3 NetBIOS ドメイン名を「**ドメイン**」フィールドに追加します。最大 200 文字の英数字を追加できます。複数のドメインはカンマで区切ります。ハイフン (-) とピリオド (.) を使用できます。

4 「**変更を保存**」を選択します。

5 Lotus Domino など、特定の LDAP サーバでは、いくつかの有効な電子メール アドレスが LDAPに表示されません。「**変換ルール**」セクションでは、SonicWall Email Security 装置が特定の電子メール アドレスを解釈する方法を変更して、電子メール アドレスを LDAP サーバにマップできるようにします。

   次のようにします。

   - 上記のサーバが 1 台でも存在する場合は、ステップ 6 に進みます。
   - 上記のサーバが 1 台もない場合、LDAP の設定は終了です。

6 これらのアドレスをマップするには、「**ルールの表示** ルールの表示 」ボタンを選択します。「**LDAP の使用**」ダイアログが表示されます。

7 使用している LDAP サーバをドロップダウン メニューから選択します。

8 「**実行**」を選択します。

9 必要に応じて、マッピングを追加します。

a 「**IF/THEN**」ドロップダウン メニューおよびフィールドから以下のように選択を行います。

- **ドメインが** - あるドメインから別のドメインへのマッピングをフィールドにさらに追加し、マップされるドメインを指定します
  - **次に置き換え** - ドメインを指定したものに置き換えます

    例: 「**IF ドメインが**」 engr.corp.com 「**THEN 次に置き換え**」 corp.com とすると、anybody@engr.corp.com 宛ての電子メールが anybody@corp.com に送信されます
  - **以下を追加** - 2 番目のドメインを有効なドメインのリストに追加します

    例: 「**IF ドメインが**」 corp.com 「**THEN 以下を追加**」 engr.corp.com とすると、corp.com が有効な LDAP ドメインのリストに見つかった場合、engr.corp.com がリストに追加されます
- **左側の文字が** - 文字置換マッピングを追加します。このフィールドには、置き換えの対象となる文字を指定します。
  - **次に置き換え** - 指定さえた文字が電子メール アドレス内の記号 (@) の左側にあれば、そのすべてを新しい文字で置き換えます

    例: 「**IF 左側の文字が**」 _ 「**THEN 次に置き換え**」 - とすると、Jane_Doe@corp.com 宛ての電子メールがJane-Doe@corp.com に送信されます
  - **以下を追加** - 2 番目の電子メール アドレスを、有効な電子メール アドレスのリストに追加します

    例: 「**IF 左側の文字が**」 _ 「**THEN 以下を追加**」 - とすると、Jane_Doe@corp.com と Jane-Doe@corp.com のどちら宛ての電子メールも有効な電子メール アドレスになります

b 「**マッピングの追加**」 マッピングの追加 ボタンを選択して、変換ルールの追加を完了します。

メモ：マッピングを削除するには、そのマッピングの「**削除**」ボタンを選択します。

グローバル LDAP 設定の構成

グローバル LDAP 設定は、すべての LDAP サーバ設定に普遍的に適用されます。

グローバル設定を構成するには、以下の手順に従います。

1 「**アンチスパム > LDAP 設定**」の「**グローバル設定**」パネルに移動します。

2 「**ドメインのエイリアス**」セクションで、1 台以上のサーバについて 1 つ以上のエイリアスを、サーバ 1 台あたり最大 200 文字の英数字で入力します。複数のエイリアスがある場合はカンマで区切ります。ハイフン (-)、アンダースコア (_) は使用できますが、スペースは使用できません。

エンド ユーザはここに設定されているエイリアスを使用して認証を行う必要があります。Active Directory サーバの場合、この疑似ドメインは NetBIOS ドメイン名と対になる LDAP ニックネームです。「**設定**」セクションで該当するオプションが選択されている場合、ログオン画面のドロップダウン メニューでは任意のエイリアスが認証のために使用可能になります。

3 エンド ユーザがログオン時にドメインおよびエイリアスのリストを確認できるようにするには、「**設定**」セクションで「**認証のためにエンド ユーザにドメインの一覧を表示する**」を選択します。このオプションは、既定で選択されています。

4 「**Usermap 頻度**」フィールドで、ユーザのリストを何分おきに更新するかを指定します。

この設定は、エイリアスのリストとグループ メンバーのリストに適用されます。ほとんどの場合、この設定の値を大きくするのは LDAP サーバの負荷を少なくする場合に限られます。その他の設定内容にもよりますが、ユーザ リストの取得は 24 時間 (1440 分) に一度行うのが妥当であり、その結果、LDAP サーバの負荷も低下します。

ⓘ **メモ**：ユーザマップの更新頻度は、ユーザがログオンできるかどうかには影響しません。ユーザのログオンには LDAP ディレクトリの内容がリアルタイムに反映されます。

5 「**変更を保存**」を選択します。

LDAP サーバ設定の編集

LDAP サーバ設定を編集するには、サーバを追加する場合と同じ設定が必要になります。

LDAP サーバを設定するには、以下の手順に従います。

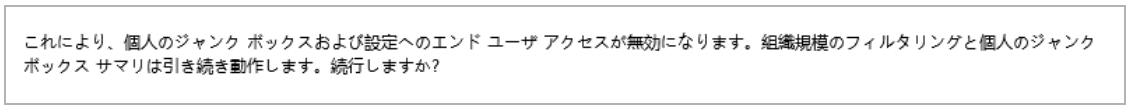
1 利用可能な LDAP サーバのリストから、**編集**アイコンを選択します。以下のセクションが編集のために展開されます。

- **サーバ設定** - LDAP サーバの追加を参照してください。
- **LDAP クエリ パネル** - LDAP クエリの設定を参照してください。
- **LDAP マッピングの追加** - LDAP マッピングの追加を参照してください。

LDAP サーバの削除

LDAP サーバを削除するには、以下の手順に従います。

1 削除するサーバの**削除**アイコンを選択します。次の警告メッセージが表示されます。



2 「**OK**」を選択します。「**アンチスパム > LDAP 設定**」ページの一番上に成功を示すメッセージが表示されます。

36

Anti-Spam Desktop ボタンのダウンロード

メモ：アンチスパムは、SuperMassive シリーズまたは NS*a* 9250 以降のファイアウォールではサポートされていません。

- アンチスパム > ダウンロード

アンチスパム > ダウンロード

「**アンチスパム > アンチスパム ツール ダウンロード**」ページでは、SonicWall の最新のスパム遮断ボタンのいずれかをデスクトップにダウンロードしてインストールできます。

リンクを選択することで、以下のボタンをデスクトップにダウンロードできます。

- 必要なものと不要なものを Email Security に対して容易かつ迅速に教えるための「ジャンク化」および「非ジャンク化」ボタン。次のいずれかを選択します。
  - **Anti-Spam Desktop for Outlook (32 ビット) および Outlook Express (トライアル バージョン) on Windows (32 ビット)**
  - **Anti-Spam Desktop for Outlook (32 ビット) および Outlook Express (トライアル バージョン) on Windows (64 ビット)**
  - **Anti-Spam Desktop for Outlook (64 ビット) および Outlook Express (トライアル バージョン) on Windows (64 ビット)**
- 必要なものを Email Security に対して容易かつ迅速に教えるための「ジャンク化」ボタン。次のいずれかを選択します。
  - **Junk Button for Outlook (32 ビット)**
  - **Junk Button for Outlook (64 ビット)**

第 5 部

セキュリティ設定 | 付録

- SonicWall サポート

A

SonicWall サポート

有効なメンテナンス契約が付属する SonicWall 製品をご購入になったお客様や、トライアル バージョンをお持ちのお客様は、テクニカル サポートを利用できます。

サポート ポータルには、問題を自主的にすばやく解決するために使用できるセルフヘルプ ツールがあり、24 時間 365 日ご利用いただけます。サポート ポータルにアクセスするには、https://www.sonicwall.com/ja-jp/support に移動します。

サポート ポータルでは、次のことができます。

- ナレッジ ベースの記事や技術文書を閲覧する。
- ビデオ チュートリアルを視聴する。
- MySonicWall にアクセスする。
- SonicWall のプロフェッショナル サービスに関して情報を得る。
- SonicWall サポート サービスおよび保証に関する情報を確認する。
- トレーニングや認定プログラムに登録する。
- テクニカル サポートやカスタマー サービスを要求する。

SonicWall サポートへの連絡方法は、https://www.sonicwall.com/ja-jp/support/contact-support をご覧ください。

このドキュメントについて

凡例

警告： **物的損害、けが、または死亡に至る可能性があることを示しています。**

注意： **手順に従わないとハードウェアの破損やデータの消失が生じるおそれがあることを示しています。**

重要、メモ、ヒント、モバイル、またはビデオ: 補足情報があることを示しています。

SonicWall SonicOS 6.5 セキュリティ設定
更新日 - 2019 年 9 月
ソフトウェア バージョン - 6.5.4
232-002573-04 Rev A

エンド ユーザ製品契約

SonicWall エンド ユーザ製品利用規約を参照する場合は、https://www.sonicwall.com/ja-jp/legal/license-agreements に移動してください。

オープン ソース コード

SonicWall では、該当する場合は、GPL、LGPL、AGPL のような制限付きライセンスによるオープン ソース コードについて、コンピュータで読み取り可能なコピーをライセンス要件に従って提供できます。コンピュータで読み取り可能なコピーを入手するには、"SonicWall Inc." を受取人とする 25.00 米ドルの支払保証小切手または郵便為替と共に、書面による要求を以下の宛先までお送りください。

General Public License Source Code Request
SonicWall Inc. Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035