SonicOS 7

アンチスパム

管理者ガイド

SONICWALL®

目次

1

アンチスパム

補足: 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。

トピック:

アンチスパムについて

トピック:

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	• ウイルス	• スパム
• フィッシングの可能性大	• ウイルスの可能性大	• スパムの可能性大

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

ここでは、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構成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 ポリシーを構成するには、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
- アドレスおよびサービス オブジェクト

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

- 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 アドレスは評価順序通りに確認されます。

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	IP アドレスがこれより前のリストにない場合、ファイアウォールは評価の悪い IP アドレスでないかどうかを GRID ネットワークに確認します。
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。

評価	説明
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、「**ポリシー | ルールとポリシー > NAT ルール**」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 ルールとポリシーに関する管理者ガイド*』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許諾されていて有効になっている場合、「**ポリシー | アンチスパム > 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 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 プライベート IP アドレス** – (ファイアウォールの裏の) Exchange または SMTP サーバの内部 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、メッセージが表示されます。

「続行」を選択して、このウィザードの要求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

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。

「**ポリシー | ルールとポリシー > アクセス ルール**」ページには、アンチスパム用に生成されたルールが表示されます。

最上段の行は、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。これは、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、「**オブジェクト | 一致オブジェクト > サービス | サービス オブジェクト**」ページで作成されます。

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。

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。

ⓘ | **補足:** 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. 「**Submit (送信)**」をクリックします。
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. MySonicWall.com でナビゲーション バーから「**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。

2

状況

「**状況**」ページでは、アンチスパム サービス ダッシュボードのように、**サービス状況**（有効期限やバージョンなど）、各種**脅威の統計**、利用可能なサービス、「**電子メール ストリーム診断キャプチャ**」エリア（キャプチャを開始/終了し、そのデータを後で確認のためにダウンロードする機能）に簡単にアクセスできます。

「**状況**」ページには、「**ポリシー | アンチスパム > 状況**」からアクセスできます。

3

設定

「**ポリシー | アンチスパム > 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構成、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。

ⓘ **補足:** 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」を参照してください。

トピック:

- アンチスパムのアクティブ化
- ジャンク ストアのインストール
- 電子メール脅威種別の設定
- アクセス リストの設定
- 詳細オプションの設定

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. 「**ポリシー | アンチスパム > 設定**」に移動します。
2. 「**グローバル設定**」タブで、「**アンチスパム サービスを有効にする**」をクリックして、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。

   SonicWall アンチスパム サービスを有効にすると、次の処理が行われます:

   - RBL フィルタを無効にしてその設定をオーバーライドします。SonicWall GRID システムは、IP 評価チェック機能を提供します。
   - GAV を有効にする (個別にライセンスされていてまだ有効になっていない場合)
   - システム生成による NAT ポリシーおよびファイアウォール アクセス ルールを作成して有効化します。
   - 既存のメール サーバに対する個別ユーザ NAT およびルール ポリシーを無効化します。

   確認警告で「**続行**」をクリックすると、EULA のリンク先に記載された契約の利用条件に合意したものと見なされます。確認警告で「**続行**」をクリックすると、EULA のリンク先に記載された契約の利用条件に合意したものと見なされます。
3. 先へ進むには、「**続行**」をクリックします。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。
4. 「**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。
5. 必要に応じて、情報を変更します。
6. 「**次へ**」ボタンを選択します。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。
7. 「**確認**」をクリックします。

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およびインストール。「*ジャンク ストアのインストール*」を参照してください。
- 電子メール脅威種別の構成。「*電子メール脅威種別の構成*」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。

ⓘ **補足:** 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。

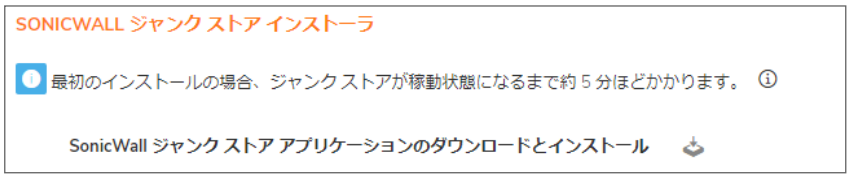
CASS 2.0 で使用可能な最新の機能を十分に活用するために、SonicWall ではジャンク ストアをスタンドアロン サーバにインストールすることを推奨しています。

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. 「**ポリシー | アンチスパム > 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。

   ⓘ **補足:** 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. 「**ポリシー | アンチスパム > 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。
11. 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。
12. 「**ポリシー | 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。これらの構成後は、電子メールのフィルタ処理や並べ替えが構成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. 「**ポリシー | アンチスパム > 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、ウイルスの問題を含む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」を参照してください。ドロップダウンメニューから選択可能なオプション:

   - **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]

種別	動作
	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。

ⓘ **補足:** 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:

- ユーザ定義アクセス リストの設定
- アクセス リストへのホストの追加

ユーザ定義アクセス リストの設定

ユーザ定義アクセス リストを構成するには、以下の手順に従います

1. 「**ポリシー | アンチスパム > 設定**」ページで、「**ユーザ定義アクセス リスト**」タブをクリックします。

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、構成したいリストの**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**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**をクリックします。

5. 終了したら、「**OK**」をクリックします。

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. +アイコンをクリックします。「**ユーザ定義 SMTP サーバの追加**」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**」をクリックします。

詳細設定の構成

「**詳細設定**」タブでは、「**ポリシー | アンチスパム > 設定**」で説明した、電子メール オプションを設定できます。

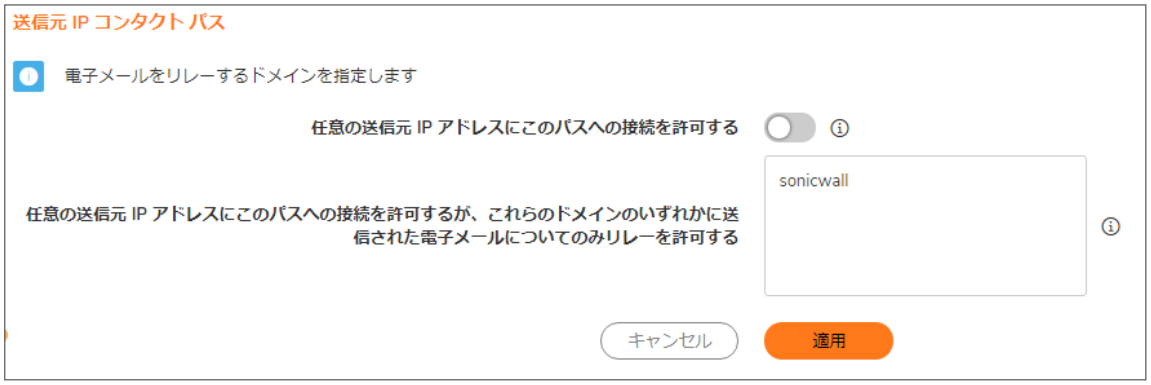
アンチスパム > 設定 | 詳細設定

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の許可/拒否**	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のタグを付け配信/削除	ジャンク ストアがスパム メッセージを受け入れることができない場合、それらを削除するか、あるいは件名行に次のような警告を添えて配信するかを選択できます: ［フィッシング］ アカウントを更新してください。 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 サーバ設定	**サーバ パブリック IP アドレス**	外部接続に使用できるサーバの 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。
	サーバ プライベート IP アドレス	内部トラフィック用のサーバの IP アドレスです。これは装置の裏にある内部メール サーバの 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

設定の種別	設定	説明
		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**」フィールドは淡色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 サブ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。

4

リレードメイン



「**ポリシー | アンチスパム > リレードメイン**」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。

トピック:

- オープン リレーについて
- 許可されたリレードメインのリスト作成

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構成された 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。

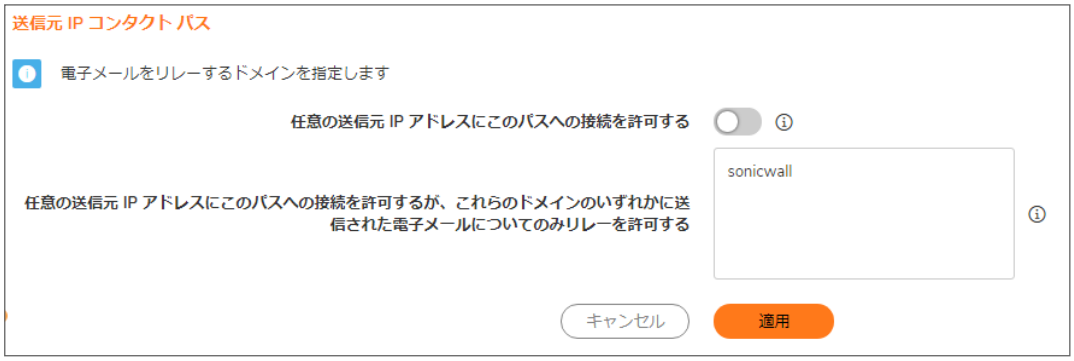
CASS がオープン リレーとして構成されている場合、受信者ドメイン宛てのものではないメールも中継されます。オープン リレーとして構成されていない CASS は、リストされている受信者ドメインのいずれかを持つ電子メールは中継しますが、リストされていないドメイン宛ての電子メールは中継しません。そのようなメールは拒否されます。許可されたリレードメインをリストすることで、メールがユーザ宛てのものでない場合も、不要な電子メールの中継を回避できます。

許可されたリレー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。

許可されたリレードメインをリスト化するには、以下の手順に従います

1. 「**ポリシー | アンチスパム > リレードメイン**」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. リレードメインを制限するかどうかを選択します。
   - **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 に進みます。

△ **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. 「**適用**」を選択します。

5

ジャンク ボックス メッセージ

「**ポリシー | アンチスパム > ジャンクボックス メッセージ**」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。

ⓘ | **補足:** 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 メッセージ」テーブルに表 示される情 報

「ジャンク ボックス メッセージ」テーブルには、隔離メッセージに関する情報とフィルタ適用の可否が表示されます。

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。脅威カテゴリの詳細については、「電子メールの脅威種別の設定」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のオプション」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。
送信元	送信者の電子メール アドレスです。
件名	電子メールの件名行です。
日付/時刻	電子メールが送信された日付と時刻です。

「**ジャンク ボックス メッセージ**」テーブルの上部にあるボタンを使用すると、「ポリシー アンチスパム ジャンク ボックス メッセージ」ページで以下のジャンク ストア管理タスクを実行できます（「「ジャンク ボックス メッセージ」テーブルのボタン」を参照）。

「ジャンク ボックス メッセージ」テーブルのボタン

ボタン	機能
フィルタ	列の条件を使用して、ジャンク ボックス結果を絞り込みやすくするソートおよびフィルタ機能を開きます。
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

ボタン	機能
	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。
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。
再表示	すべてのデータを更新します。
設定	「ジャンク ボックス設定」にある「一般」および「動作設定」を開きます。
列	見出しをクリックして列データを追加または削除します。

ジャンク ボックス メッセージの管 理

ジャンク ストア メッセージのフィルタ適用、削除、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. 「**ポリシー |アンチスパム > ジャンク ボックス メッセージ**」ページで、「ジャンク ボックス メッセージ」テーブル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**」をクリックします。

     ⓘ **補足:** 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。
- 「**受信者電子メール 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**」をクリックします。

4. 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。

6

ジャンク ボックス設定

「**ポリシー | 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. 「**一般設定**」セクションでスライダーを使用して、「**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. 「**送信者を受信者の許可リストに自動的に追加する**」頻度を選択します。「**問い合わせる**」オプションが既定で選択されています。
    - 無効
    - 問い合わせる
    - 常に有効

3. 必要に応じて「**動作設定**」を有効または無効にします。
4. 「**保存**」をクリックします。

7

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。「**ポリシー | 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構成するには、「**ポリシー | アンチスパム > 詳細**」ページに移動します。

「**ポリシー | アンチスパム > ジャンク ボックス サマリ**」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構成します。
- **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。

トピック:

- ジャンク ボックス サマリの管理

ジャンク ボックス サマリの管 理

ジャンク ボックス 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、「**無効**」を選択します。
2. 「**タイム ゾーン**」から、ユーザが電子メール通知を受信するタイム ゾーンを選択します。「**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。
3. 「**サマリの頻度**」ドロップダウン メニューで「**1 週間ごと**」または「**隔週**」を選択した場合は、「**サマリを送信する時刻**」および「**サマリを送信する曜日**」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。
   - **どの時間でも**
   - **特定の時間**
4. **サマリを送信する曜日** – ドロップダウン メニューから曜日を選択します。
   - **どの日でも**
   - **特定の日** (日を選択してください)。
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** (既定)
   - **ジャンクの可能性が高いメッセージ** (確実なジャンクは表示しない)
6. サマリ電子メールの「**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. 「**プレーン サマリの送信**」で、サマリに画像を含めるかどうかを指定します。
8. 「**サマリ電子メールにジャンク統計を表示する**」で、ジャンク統計を含めることができます。
9. 「**その他の設定**」セクションで「**ジャンク ボックス サマリを代理人に送信する**」を有効にすると、サマリ電子メールが指定された代理人へ送信されます。
10. 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)
11. 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。
12. 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。
13. 「**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**: フィールドに電子メール アドレスを入力します。

14. 「**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。
15. 「**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。
16. 「**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。この設定が構成されている場合、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**」をクリック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。
17. 「**保存**」をクリックします。

8

ユーザ表示セットアップ

「**ポリシー | 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構成できます。

トピック:

- ユーザ画面セットアップの構成

ユーザ画面セットアップの構成

ⓘ | **補足:** 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. 「**一般設定**」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**」を有効にします。このオプションは既定で有効です。
2. 「**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**」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。

3. 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。
4. 「**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。
5. 必要な変更をすべて加えたら、「**保存**」をクリックします。

9

アドレス帳

「**ポリシー | 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**」リストを構成できます。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。

「**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。

トピック:

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

「**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。アドレス帳を**許可**リストにインポートしたり、企業アドレス帳を 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

ⓘ | **補足:** 管理者によって企業遮断リストに追加された送信者は、すべてのユーザに対して自動的に遮断され、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。アドレス帳を遮断リストにインポートしたり、企業アドレス帳を 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することができます。

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. 「**ポリシー | アンチスパム > アドレス帳**」で適切なビューに移動します。
2. 「**追加**」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

「**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**」が使用可能になります。
3. 「**削除**」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. 「**ポリシー | アンチスパム > アドレス帳**」に移動します。
2. 適切なビューを選択します。
3. 「**インポート**」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。
4. 「**参照**」をクリックします。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。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、コンマ区切りのアドレス帳エントリです。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ます。

   例を以下に示します。

   ```
   <TAB>E<TAB>A<TAB>email1@company.com,email2@company.com<CR>

   <TAB>L<TAB>B<TAB>list1@company.com,list2@company.com<CR>
   ```

6. 「**開く**」を選択します。
7. 「**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**」をクリックします。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**」をクリックします。

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**」ボタンをクリック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**」をクリックします。

10

ユーザ管 理

「**ポリシー | 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かまいません。
プライマリ電子メール	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「**ポリシー	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。

トピック:

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. 「**ポリシー | 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. 「**ユーザおよびグループの更新**」をクリックします。

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. 「**ポリシー | 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 ユーザ向けの認証を有効にする**」を選択します。注意を促すメッセージが表示されます。
3. 「**OK**」をクリックします。

ユーザの表示

「**ユーザ テーブル**」には、ログイン可能なすべてのユーザが表示されます。ユーザーにフィルタを適用し、現在表示したいユーザのみを表示するには、以下の操作を実行します。

- ユーザ種別の選択: 表示するユーザの種別の選択
- ソース（サーバ）の選択: 「表示するサーバのユーザの選択」を参照してください
- 特定ユーザの指定: 「ユーザの検索」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. 「**ポリシー | 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**」を選択します。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**」を選択します。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**」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. 「**ポリシー | 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**
      - **プライマリ電子メール**
   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**」をクリックします。「**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**」をクリックします。

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。

- 手動については、「ユーザ テーブルへのユーザの手動追加」を参照してください。
- インポートについては、「ユーザ テーブルへのユーザのインポート」を参照してください。

ⓘ **補足:** ログイン可能なユーザのリストに、すべての従業員を追加することを推奨します。企業のメーリング リストのアドレスとエイリアス（`info@example.com` など）を追加して、それらのエイリアスに送信された迷惑メールを確実にフィルタリングできるようにする必要もあります。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、以下の手順に従います:

1. 「**ユーザ テーブル**」の上にある「**追加**」ボタンをクリックします。「**ユーザの追加**」ダイアログが表示されます。
2. 「**プライマリ 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**」をクリックします。「**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. 「**参照**」をクリックします。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、エントリ同士を改行コード <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>
   ```

   例を以下に示します。

   ```
   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「**ポリシー | 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. 「**ポリシー | アンチスパム > ユーザ管理**」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**」ボタンをクリックします。別のウィンドウに そのユーザの「**Email Security 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。
4. 「**ポリシー | 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** アイコンをクリックします。

11

LDAP 構成

「**ポリシー | アンチスパム > LDAP 構成**」ページでは、LDAP サーバに固有のさまざまな構成を行うことができます。

このセクションには、ファイアウォール上で構成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。

- **名前** – サーバのニックネームが表示されます。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: 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。
- **アカウント情報** – アクティブ ユーザ名が表示されます。
- **動作** – **編集**アイコンと**削除**アイコンがあります。

トピック:

- LDAP サーバの追加
- LDAP クエリの設定
- LDAP マッピングの追加
- LDAP サーバ設定の編集
- LDAP サーバの削除

LDAP サーバの追加

新しい LDAP サーバを構成して、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。「**ポリシー | アンチスパム > LDAP 構成**」ページで情報を正しく入力しないと、自分のジャンク ボックスへのログインが許可されているユーザの完全なリストが返されません。このリストに含まれていないユーザについては、その電子メールはフィルタリングされるのに、ユーザが個人用のジャンク ボックスにログインできません。
LDAP 設定に情報を適切に入力するには、「**LDAP 設定**」タブ、「**LDAP クエリ パネル**」タブ、「**LDAP マッピングの追加**」タブ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. 「**ポリシー | アンチスパム > LDAP 構成**」に移動します。
2. 「**+LDAP の追加**」をクリックします。「**LDAP サーバの追加**」ダイアログが表示されます。

3. 必要に応じて、「**LDAP 設定**」タブで、「**拡張 LDAP マッピング フィールドを表示**」オプションを有効にします。このオプションを有効にすると、セカンダリ サーバ用のフィールドが表示されます。
4. 「**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**」オプション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。
5. 「**LDAP 設定**」タブで、「新しい LDAP サーバの設定を構成します。

   ⓘ **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 ldapservern (n は連番) です。
   - **プライマリ サーバ名または IP** – LDAP サーバのサーバ名または IP アドレスです。
   - **ポート** – 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 サーバまたは IP** – セカンダリ LDAP サーバのサーバ名または IP アドレスです。

     ⓘ **補足:** 「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。
   - **セカンダリ サーバ ポート** – 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
  - Exchange
  - Open LDAP
  - Lotus-Domino
  - iPlanet
  - **その他**
- **管理ドメイン** – カンマで区切った英数字列: ハイフンとドットは使用できますが、スペースは使用できません。最大 200 文字。複数のドメインはカンマで区切ります。例: company.com, payroll.company.com, net-engr.com
- **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 照会を許可する** – 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。この委任は「照会」と呼ばれ、管理者またはユーザがログインすると実行されます。照会されたログイン要求にはとても時間がかかり、20 秒以上かかることもあります。このオプションは、既定では選択されていません。

ⓘ **補足:** 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てください。データや設定が失われることはありません。

6. ユーザの LDAP ログイン方式を構成します。
   - **匿名を許可する** (既定) – 多くの LDAP サーバは、要求されれば誰にでもユーザのリストを提供するように構成されています。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 9 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。
7. 「**ログイン**」を選択した場合、「**ユーザ名**」と「**パスワード**」を指定してください。

   ユーザ名は、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. 構成した設定をテストするには、「**LDAP ログインのテスト**」をクリックします。「**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 クエリの設定

ⓘ **ヒント:** 「**LDAP 設定**」タブで「**構成の保存時に LDAP クエリ フィールドを自動入力する**」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 (http://www.ldapbrowser.com/download/index.php から入手可能) を実行します。
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**」タブの「**LDAP ユーザのクエリ**」セクションに移動します。
2. オプションの「**LDAP グループのクエリ**」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
```

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。

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。

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「**電子メール 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。例を以下に示します。

   - `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。

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 ユーザのクエリ**」セクションにある青いアイコン「**ユーザ クエリのテスト**」をクリックします。
7. 「**保存**」をクリックして変更を保存します。
8. 「LDAP グループのクエリ」セクションに移動します。

   ⓘ | **ヒント:** 「**設定**」セクションの「**LDAP クエリ フィールドを自動入力**」フィールド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**」をクリック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. 「**ユーザ ログイン名の属性**」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 メンバーの属性**」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 メンバーシップの属性**」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 ユーザのクエリ**」セクションにある青いアイコン「**ユーザ クエリのテスト**」をクリックします。
15. 「**保存**」をクリックして変更を保存します。

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**」タブで NetBIOS ドメイン名を指定する必要があります。

ⓘ | **補足:** 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**」をクリックします。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. 「**ポリシー | アンチスパム > LDAP 構成**」の「**LDAP マッピングの追加**」パネルに移動します。

3. 「**別のサーバを使用した認証を有効にする**」オプションを有効にして、その後のオプションを起動します。
4. 使用している **LDAP サーバ種別**をドロップダウン メニューから選択します。
5. 「**プライマリ サーバ名または IP アドレスとポート**」および「**セカンダリ サーバ名または IP アドレスとポート**」を両方入力して、プライマリ サーバとセカンダリ サーバ間のマッピングを作成します。
6. 残りのフィールドを入力し、「**保存**」をクリックして割付を完了します。

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 サーバを構成するには、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
   - LDAP クエリ パネル – 「LDAP クエリの設定」を参照
   - LDAP マッピングの追加 – 「LDAP マッピングの追加」を参照

LDAP サーバの削除

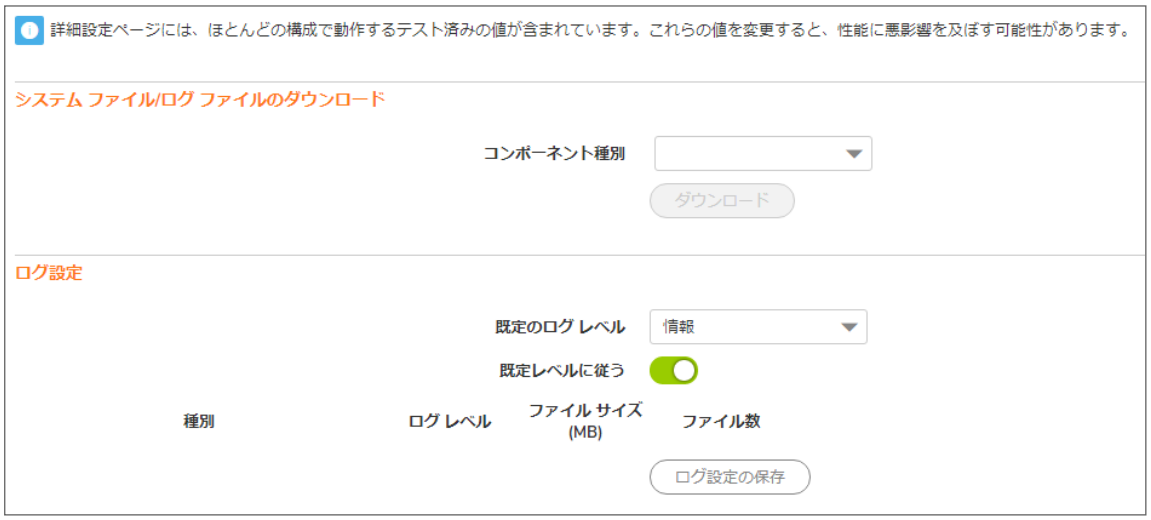
LDAP サーバを削除するには、以下の手順に従います

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」をクリックします。「**ポリシー | アンチスパム > LDAP 構成**」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。

12

詳細

「**ポリシー | アンチスパム > 詳細**」ページでは、ログおよびシステム構成ファイルをサーバからダウンロードしたり、ログ レベルを構成したりできます。



トピック:

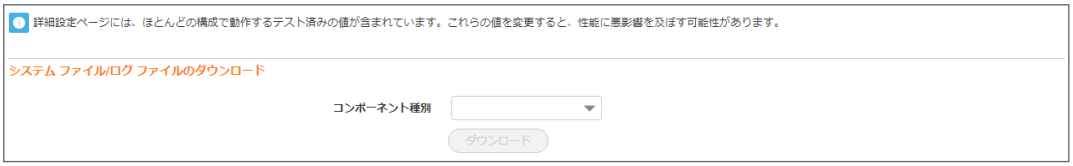
- システム ファイル/ログ ファイルのダウンロード
- ログ設定の選択

システム ファイル/ログ ファイルのダウンロード

ⓘ **補足:** 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. 「**ポリシー | アンチスパム > 詳細**」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. 「**コンポーネント種別**」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。選択すると、ファイル名がオレンジに変わります。「**ダウンロード**」ボタンがアクティブになります。

   ⓘ | **補足:** 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. 「**ダウンロード**」をクリックして、ファイルをローカル ハード ドライブにダウンロードします。

ログ設定の選択

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、「**ログ設定**」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構成するには、以下の手順に従います

1. 「**ポリシー | アンチスパム > 詳細**」の「**ログ設定**」セクションに移動します。

2. 「**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。

   ⓘ | **補足:** 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** – 既定
   - **情報**
   - **警告**
   - **エラー**
   - **致命的** – 最も高いレベル

   「**既定レベルを順守する**」オプションを有効にすると、すべてのログは既定レベルを順守します。
3. 「**ログ設定**」セクションでログに変更を加えるには、「**既定レベルを順守する**」を無効にします。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。

4. 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**」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。レベルは、ステップ 3 のレベルと同じであるほか、「**順守**」オプションのレベルとも同じです。
5. 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「**順守**」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、「**ファイル数**」で保持するログ 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 3 つのログ ファイルを保持します。

   - 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「**ファイル数**」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「**ファイル サイズ (MB)**」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. 「**ログ設定の保存**」をクリックして、加えた変更を保存します。

13

ダウンロード

「**ポリシー | アンチスパム > 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し、素早くアクセスできます。

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。
  - **Windows (64 ビット) 用 Anti-Spam Desktop for Outlook (64 ビット) トライアル版**
- 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 (64 ビット)**

14

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、次の URL を開きます:
https://www.sonicwall.com/ja-jp/support

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。
- 次のサイトでコミュニティ フォーラムのディスカッションに参加したり、その内容を閲覧したりする:
  https://community.sonicwall.com/technology-and-support
- ビデオ チュートリアルを視聴する。
- https://mysonicwall.com 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 サービスを要請する。

SonicWall サポートに連絡するには、次の URL を開きます: https://www.sonicwall.com/ja-jp/support/contact-support

このドキュメントについて

補足: メモ アイコンは、補足情報があることを示しています。

重要: 重要アイコンは、補足情報があることを示しています。

ヒント: ヒント アイコンは、参考になる情報があることを示しています。

注意: 注意アイコンは、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恐れがあることを示しています。

警告: 警告アイコンは、物的損害、人身傷害、または死亡事故につながるおそれがあることを示します。

SonicOS アンチスパム 管理者ガイド
更新日 – 2021 年 3 月
ソフトウェア バージョン – 7
232-005638-00 Rev B

エンド ユーザ製品利用規約

SonicWall エンド ユーザ製品利用規約を参照する場合は、次に移動してください: https://www.sonicwall.com/ja-jp/legal

オープン ソース コード

SonicWall Inc. 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、書面によるリクエストを以下の宛先までご送付ください。

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035