SonicOS 7.0
ネットワーク ファイアウォール

管理ガイド

SONICWALL®

目次

1

詳細

このセクションでは、ファイアウォールの詳細設定の方法を説明します。設定するには、「**ネットワーク > ファイアウォール > 詳細**」ページに移動します。

トピック:

侵入検知と防止

侵入検知と防止を有効にするには:

1. 「**ネットワーク > ファイアウォール > 詳細**」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. 「**ファイアウォール > ファイアウォール > 詳細**」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。
4. 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 トラフィック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. 「**オブジェクト > 一致オブジェクト > アドレス**」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. 「**オブジェクト > 一致オブジェクト > サービス**」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. 「**ポリシー > ルールとポリシー > NAT ポリシー**」ページで、NAT ポリシーを作成します。

d. 「**ポリシー > ルールとポリシー > セキュリティ ポリシー**」ページで、アクセス ルールを作成します。

e. 「**ネットワーク > ファイアウォール > 詳細 > 動的ポート**」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。

5. 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。

   ⓘ | **補足:** 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。

6. 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。
7. 「**適用**」をクリックします。

ソース ルーティング パケット

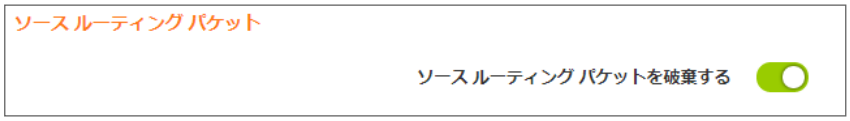
IP ソース ルーティングは、パケットの送信元が、送信先に到達するまでにパケットが使用するべきルータの一部またはすべてを指定できる、IP の標準オプションです。

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恐れがあるためです。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. 「**ネットワーク > ファイアウォール > 詳細**」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**」をクリックします。



アクセス ルール 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. 「**デバイス > ファイアウォール設定 > 詳細**」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。「**発信/着信 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. 「**デバイス > ファイアウォール設定 > 詳細**」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。

接続

ⓘ **重要:**「**接続**」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。

ⓘ **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。

特定の SPI および DPI の最大接続数については、お使いのファイアウォール プラットフォームに関する最新の SonicWall データシートを参照してください。

- NSa シリーズ – SonicWall NSa シリーズ用データシート
- TZ シリーズ – SonicWall TZ シリーズ用データシート
- SuperMassive シリーズ – SonicWall SuperMassive シリーズ用データシート

当社の製品シリーズの詳細については、SonicWall リソースのページを参照してください。最大接続数 (DPI SSL) など、ハイエンド、ミッドレンジ、エントリ レベル、および仮想ファイアウォールの詳細情報を「**By Product Series (製品シリーズ別)**」ドロップダウン メニューで検索します。

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。NSa 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。

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テーブルが「**接続**」グループの下に表示されます。

接続サービスを設定するには:

1. 「**デバイス > ファイアウォール設定 > 詳細**」に移動します。
2. 「**接続**」までスクロールします。

3. 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かわりに、最大 DPI 接続数を妥協します。

    ⓘ **補足:** 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。

IPv6 の詳細設定

IPv6 の詳細設定を行うには:

1. 「**デバイス > ファイアウォール設定 > 詳細**」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 時間超過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 時間超過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、漏えい、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せん。

    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)。

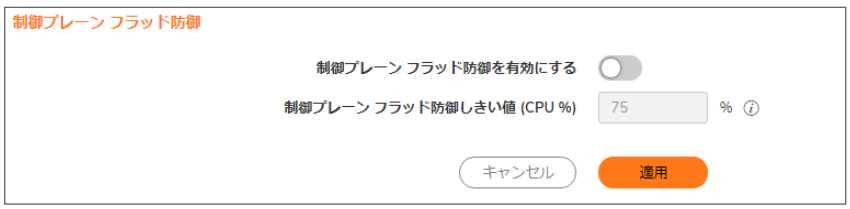
    - SonicWall 装置による IPv6 拡張ヘッダーの順序の確認を行う場合は、「**IPv6 拡張ヘッダーの順序の確認を強制する**」を選択します。このオプションは、既定では選択されていません。
13. SonicWall 装置にブロードキャスト ISATAP クエリに対する応答として NetBIOS 名の生成を行わせる場合は、「**ISATAP の NetBIOS 名クエリ応答を有効にする**」を選択します。このオプションは、既定では選択されていません。

    ⓘ **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. 「**デバイス > ファイアウォール設定 > 詳細**」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指定した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。

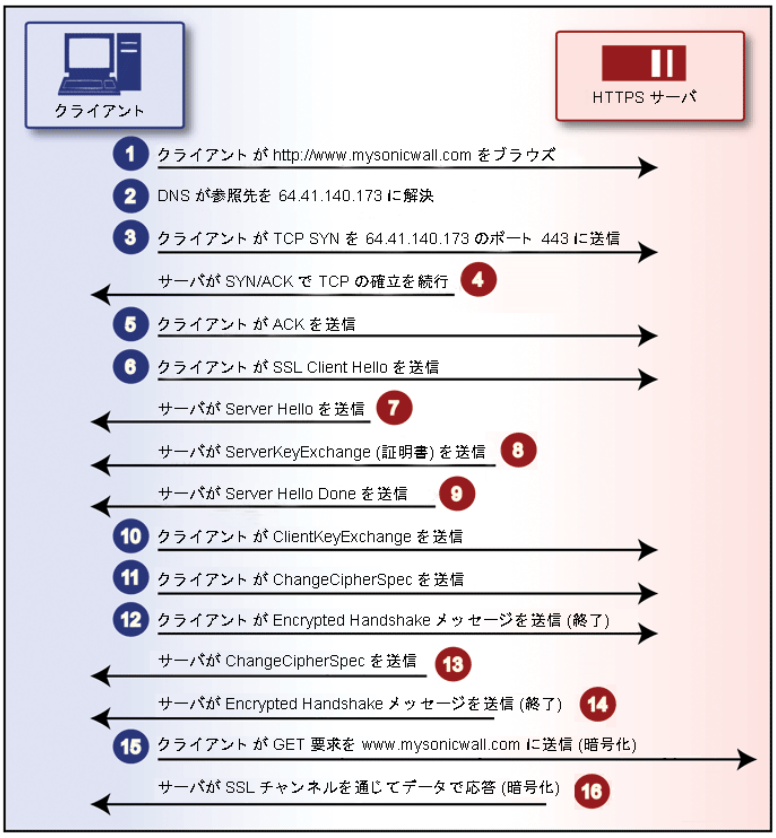
4. 「**適用**」をクリックします。

2

SSL 制御

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可視化するシステムで、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（上記の図を参照）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」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モ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。よく知られたこの種類の 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容易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ますが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、ゲートウェイに基づく識別と疑わしいSSLトラフィックの禁止が可能です。

トピック:

- SSL 制御の主な機能
- SSL 制御の重要な概念
- 注意事項と推奨事項

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みなされます。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。

機能	利点
	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。
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、応答で送信される Server Hello と証明書が検知し設定されたポリシーに従って評価します。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。

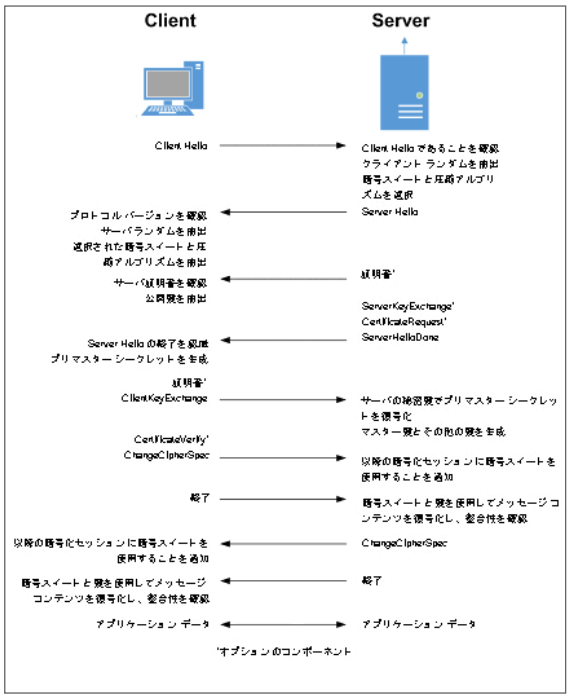
機能	利点
設定可能なアクションおよびイベント通知	SSL 制御機能によってポリシー違反が検出された場合に、イベントをログに記録して接続を遮断することができます。あるいは、イベントをログに記録するだけで接続を継続することもできます。

SSL 制御の重要な概念

SSL 制御について理解するための重要な概念には、次のものがあります。

- **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、以下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みなされています。
- **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、以下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
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

ⓘ | **補足:** SonicOS 7.0 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み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、「**デバイス > 設定 > 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「**デバイス > 設定 > 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。以下の表に、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

暗号	暗号化	プロトコル
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)
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「**デバイス > 設定 > 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)。
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。

SSL 制御の設定

ⓘ **補足:** 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。「**ネットワーク > ファイアウォール > 詳細**」ページの「**IPv6 詳細構成**」オプションを使用して確認できます。

SSL 制御の設定は、「**ネットワーク > ファイアウォール > 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用する用語の詳細については、「SSL 制御の重要な概念」を参照してください)。

一般設定

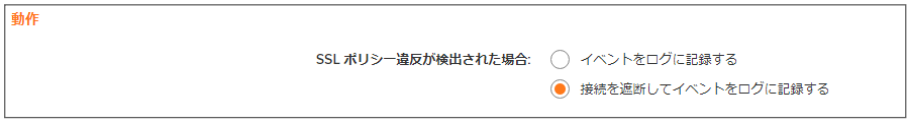
「**一般設定**」セクションでは、SSL 制御を有効または無効にできます。

- **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** — 「ユーザ定義リスト」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。
- **脆弱な暗号を検知する** — 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。「**デバイス > 設定 > 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。
- **脆弱な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。

  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。
- **自己署名証明書を検出する** — 発行者の証明書がファイアウォールの「**デバイス > 設定 > 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。
- **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「**デバイス > 設定 > 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 証明書を 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。

ユーザ定義リスト

「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 マッチング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」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	https://www.sonicwall.de
prox	https://proxify.org、https://www.proxify.org、	https://www.freeproxy.ru

エントリ	一致する URL	一致しない URL
	https://megaproxy.com、https://1070652204	

- 67.115.118.87 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。
- 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。
- *www.freeproxy.ru* サイトの証明書の共通名は ″ー″ 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。

ブラックリストを設定するには、以下の手順に従います。

1. 「**ネットワーク > ファイアウォール > SSL 制御 > ユーザ定義リスト > ブラックリスト**」に移動します。
2. 「+」アイコンを選択します。「**ブラックリストの追加**」ダイアログが表示されます。

3. 「**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。

4. 「**追加**」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。

ホワイトリストを設定するには、以下の手順に従います。

1. 「**ネットワーク > ファイアウォール > SSL 制御 > ユーザ定義リスト > ホワイトリスト**」に移動します。
2. 「+」アイコンを選択します。「**ホワイトリストの追加**」ダイアログが表示されます。

3. 「**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。

4. 「**追加**」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。

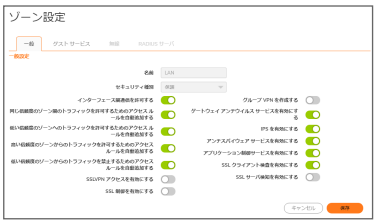
ゾーンでの SSL 制御の有効化

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。ファイアウォールは、応答で送信される Server Hello と証明書が検知し設定されたポリシーに従って評価します。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。

ⓘ **補足:** 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. 「**オブジェクト > 一致オブジェクト > ゾーン**」ページに移動します。
2. 該当するゾーンの「**編集**」アイコンを選択します。「**ゾーン設定 > 一般**」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。
4. 「**保存**」をクリックします。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 Control: Certificate with invalid date【SSL 制御: 証明書の日付が無効】	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 Control: 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）。 自己署名証明書制御の強制については、次を参

#	イベント メッセージ	発生条件
		照してください「ゾーンでの SSL 制御の有効化」。
4	SSL Control: Untrusted CA【SSL 制御: 信頼できない CA】	ファイアウォールの「**デバイス > 設定 > 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。 自己署名証明書制御の強制については、次を参照してください「ゾーンでの SSL 制御の有効化」。
5	SSL Control: 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 Control: 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、次を参照してください「ゾーンでの SSL 制御の有効化」。
7	SSL Control: 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。
8	SSL Control: 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。
9	SSL Control: 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。

3

暗号化制御

SonicOS では、TLS 暗号化および SSH 暗号化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。

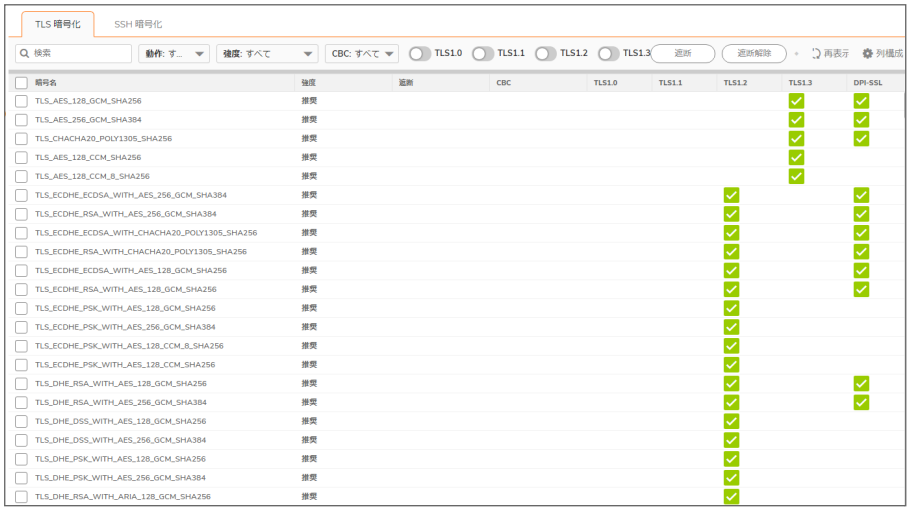
- DPI-SSL（ファイアウォールによって検査される TLS トラフィック）
- https 管理（ファイアウォールにアクセスする TLS セッション）
- SSL 制御（ファイアウォールを通過する TLS トラフィックを検査: 非 DPI-SSL）

TLS 暗号化の変更はすべての TLS トラフィックに適用されます。

「**ネットワーク > ファイアウォール > 暗号化制御**」ページに表示される暗号のリストは、既知の TLS 暗号化のリストです。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 管理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 管理は、TLS 1.3 暗号化をまだサポートしていません。また、「**ネットワーク > ファイアウォール > 暗号化制御**」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 管理の実装は、どちらも「**ネットワーク > ファイアウォール > 暗号化制御**」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「**ネットワーク > ファイアウォール > 暗号化制御**」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 管理暗号にも当てはまります。

TLS 暗号化



暗号名	暗号の名前
強度	暗号の強度: • **推奨** • **安全** • **脆弱** • **危険**
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

トピック:

- 暗号の遮断/遮断解除
- 暗号のフィルタリング

暗号の遮断/遮断解除

暗号を遮断するには、以下の手順に従います。

1. 「**ネットワーク > ファイアウォール > 暗号化制御**」に移動します。
2. 「**TLS 暗号化**」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. 「**遮断**」を選択します。選択された暗号を遮断するための確認ダイアログが表示されます。
5. 「**OK**」をクリックします。「**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、以下の手順に従います。

1. 「**ネットワーク > ファイアウォール > 暗号化制御**」に移動します。
2. 「**TLS 暗号化**」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。選択された暗号を遮断解除するための確認ダイアログが表示されます。
5. 「**OK**」をクリックします。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
- 強度別に暗号を表示する
- 動作別で暗号を表示する
- CBC モードの有無で暗号を表示する
- TLS プロトコル バージョン別に暗号を表示する

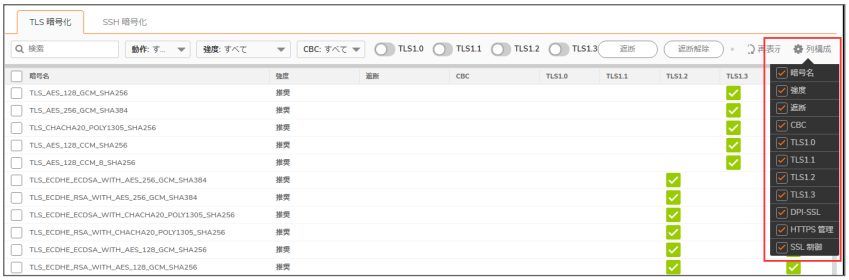
表示オプションの選択

「**TLS 暗号化**」テーブルは、どの TLS 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

TLS 暗号化をプロトコルに基づいてフィルタするには、以下の手順に従います。

1. 「**ネットワーク > ファイアウォール > 暗号化制御**」に移動します。
2. 「**TLS 暗号化**」を選択します。
3. 「**列構成**」オプションを選択します。「表示/非表示にする列を選択します」ドロップダウンが表示されます。



4. 表示するプロトコルを選択します:
    a. **すべて選択** – このオプションは、既定では選択されています。
    b. **DPI-SSL** – このオプションは、既定では選択されています。
    c. **HTTPS 管理** – このオプションは、既定では選択されています。
    d. **SSL 制御** – このオプションは、既定では選択されています。

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
- 安全
- 危険
- 脆弱

「TLS 暗号化」テーブルは、すべての強度のすべての暗号を示します。「TLS 暗号化」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. 「**ネットワーク > ファイアウォール > 暗号化制御**」に移動します。
2. 「**TLS 暗号化**」を選択します。
3. 「強度」ドロップダウンから必要なオプションを選択します。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 暗号化」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。

動作別で暗号を表示する

「TLS 暗号化」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 暗号化」テーブルを制限して、許可または遮断された暗号のみを表示できます。

許可/遮断された暗号を表示するには、以下の手順に従います。

1. 「**ネットワーク > ファイアウォール > 暗号化制御**」に移動します。
2. 「**TLS 暗号化**」を選択します。
3. 「**動作**」ドロップダウンから動作の許可/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 暗号化」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 モードの有無で暗号を表示する

「TLS 暗号化」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 モードが有効または無効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. 「**ネットワーク > ファイアウォール > 暗号化制御**」に移動します。
2. 「**TLS 暗号化**」を選択します。
3. 「CBC」から、暗号の CBC モードが有効か無効かを選択します。

- すべて（既定）
- 有（CBC モード）
- 無（CBC モードでない）

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

TLS プロトコル バージョン別に暗号を表示する

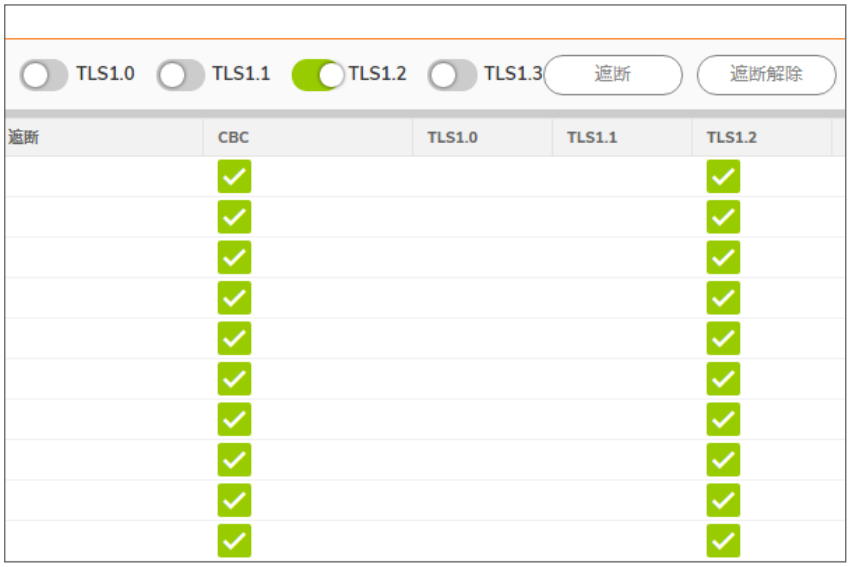
「TLS 暗号化」テーブルは、すべての TLS プロトコル バージョンのすべての暗号を示します。サポートしている TLS プロトコルのバージョンごとに暗号の表示を制限できます。

TLS プロトコル別に暗号を表示するには:

1. 「**ネットワーク > ファイアウォール > 暗号化制御**」に移動します。
2. 「**TLS 暗号化**」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。



ⓘ **補足:** 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 暗号化

「**ネットワーク > ファイアウォール > 暗号化制御**」の「SSH 暗号化」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
公開鍵アルゴリズム	公開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 暗号化を選択または選択解除するには:

1. 「**ネットワーク > ファイアウォール > 暗号化制御**」に移動します。
2. 「**SSH 暗号化**」を選択します。
3. 使用または無視する SSH アルゴリズムを選択します。

ⓘ | **重要:** 既定では、すべての SSH 暗号化が選択されています。

4

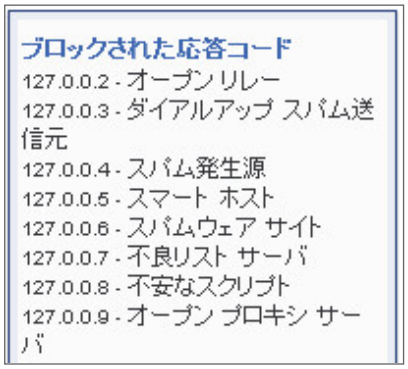
リアルタイム ブラックリスト (RBL) フィルタ

RBL フィルタは、送信側 IP アドレスに基づいて SMTP メールを遮断するように設計されています。送信側 IP アドレスは、疑わしいスパム送信者、悪意のある/オープン メール リレーなどからなるデータベースで検索されます。RBL フィルタは、疑わしい電子メール サーバからの SMTP メールを防ぎます。

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://ers.trendmicro.com/?lang=ja_jp などが知られています。

ⓘ **補足:** 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。

ⓘ **補足:** 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、いったん 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
- RBL サービスの追加
- ユーザ定義 SMTP サーバ リストの設定
- SMTP IP アドレスのテスト

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**」タブで「**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「**手動で DNS サーバを指定する**」を選択できます。「**手動で 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。

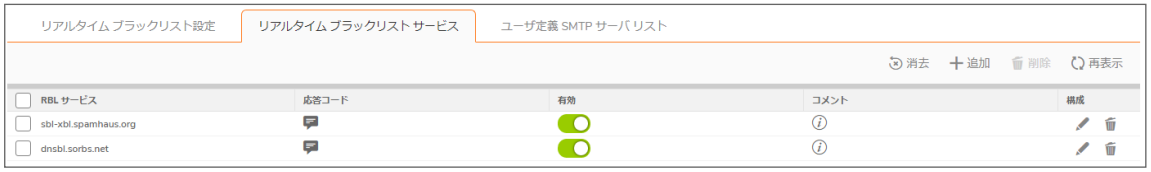
設定が終了したら、「**適用**」を選択します。

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**」タブ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**」アイコンを選択します。「**ブラックリスト サービスの追加**」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 サービスごとの接続詳細が記録され、それらはサービス エントリの右に表示される情報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**」タブでは、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。

ⓘ **補足:** 「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
- ブラック リストの設定

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. 「**追加**」アイコンを使用して、サーバのアドレス オブジェクトを作成します。「**ユーザ定義 SMTP サーバの追加**」ダイアログが表示されます。

2. アドレス オブジェクトを設定します。
3. 「**OK**」をクリックします。「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。

   ⓘ **補足:** ホワイト リスト アドレス オブジェクトを削除するには、「RBL User White List」行の三角形のアイコンを選択し、「**削除**」アイコンを選択します。

ブラック リストの設定

1. 「**追加**」アイコンを使用して、サーバのアドレス オブジェクトを作成します。「**ユーザ定義 SMTP サーバの追加**」ダイアログが表示されます。

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 Black List」にアドレス オブジェクトが追加されます。

   ⓘ **補足:** ブラック リスト アドレス オブジェクトを削除するには、「RBL User Black List」行の三角形のアイコンを選択し、「**削除**」アイコンを選択します。

SMTP IP アドレスのテスト

「**デバイス > 診断 > リアルタイム ブラックリスト**」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。

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、http://www.spamhaus.org/sbl/latest/ を参照してください。

5

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 サービスを要求する。

SonicWall サポートに連絡するには、次の URL にアクセスします。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 ネットワーク ファイアウォール 管理ガイド
更新日 – 2021 年 3 月
ソフトウェア バージョン – 7.0
232-005445-10 Rev C

エンドユーザ製品契約

SonicWall エンドユーザ製品契約を参照する場合は、以下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、書面による要求を以下の宛先までお送りください。

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