SonicOS 7
セキュリティ サービス

管理ガイド

SONICWALL®

内容

1

サマリ

この機能を使用すると、ネットワークで動作する SonicWall ネットワーク セキュリティ装置は、プロキシ サーバ経由でインターネットにアクセスしてシグネチャをダウンロードすることができます。この機能では、SonicWall ネットワーク セキュリティ装置の登録を、プライバシーを危険にさらすことなくプロキシ サーバ経由で行うこともできます。

「**セキュリティ サービス > サマリ**」ページには、以下の設定があります。

- ライセンスの同期
- セキュリティ サービス設定
- プロキシ サーバを通してのシグネチャ ダウンロード
- セキュリティ サービスに関する情報

こうした最上位レベルの**セキュリティ サービス**設定では、最高レベルのセキュリティを目指した運用を選択したり、セキュリティ レベルを少し下げてネットワークのパフォーマンス レベルを向上させることを許可したりできます。

これらの設定は、グローバル ネットワーク、グループ、または単独の SonicWall ネットワーク セキュリティ装置を対象として選択できます。

ライセンスの同期

ライセンスを MySonicWall アカウントと同期するには、「**ライセンスの同期**」セクションの「**同期**」ボタンをクリックします。

セキュリティ サービス設定

セキュリティ サービス設定には、以下の設定が含まれます。

- **セキュリティ サービス設定**
  セキュリティ レベルには次の 2 つの選択肢があります。
  - **最高度セキュリティ（推奨）**－この設定では、脅威レベルに関係なく、すべてのトラフィックの検査が行われます。
  - **パフォーマンスの最適化** － 検査の対象を脅威レベルが高または中のトラフィックに制限します。スループットは向上しますが、その代わりにセキュリティが最高レベルではなくなります。

  SonicOS DPI クラスタリングを使用すると、最高のセキュリティ設定でのパフォーマンスが向上します。

- **ISDN 接続のためにアンチウイルストラフィックを抑える** – この設定を有効にすると、SonicWall アンチウイルスで更新を 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** – 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 SonicWall ネットワーク セキュリティ装置に指示するには、このオプションを選択します。
- **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 クライアント不要通知タイムアウト** – HTTP クライアント不要通知は、HTTP サーバから入り込んだ脅威が検知されたときにユーザに通知します。HTTP サーバから入り込んだ脅威が ゲートウェイ アンチウイルス または アンチスパイウェアに検出されたときに、SonicWall ネットワーク セキュリティ装置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)、最小値は 10 秒、最大値は 2147483647 秒です。これにより、装置がクライアント システムからの確認通知を待つ時間の長さが定義されます。

プロキシ サーバを通してのシグネチャ ダウンロード

プロキシ サーバのセットアップは、脅威シグネチャのダウンロードおよび装置の登録でのプライバシー管理のための手法として不可欠です。

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**」を選択します。
2. このフィールドが選択されている場合、次の 2 つのフィールドが使用可能になります。「**プロキシ サーバの名前または 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**」を選択します。

   ⓘ **補足:** パスワード フィールドが空のままの場合、この装置の現在のパスワードの値は変更されません。
5. 「**適用**」をクリックして変更を適用するか、「**キャンセル**」をクリックして変更を破棄します。

セキュリティ サービスに関する情報

このセクションで使用できる**シグネチャのインポート**機能は、(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または望ましくないネットワークを想定して設計された機能です。**シグネチャのインポート**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 MySonicWall アカウント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。

- デバイスがそれぞれ同じ MySonicWall 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 > サマリ**」に移動します。
2. 「**セキュリティ サービスに関する情報**」セクション（ページの一番下まで）スクロールします。
3. 機器の「**シグネチャ ファイル ID**」を記録します。
4. SonicWall ネットワーク セキュリティ装置の登録に使用した MySonicWall アカウントにログオンします。

   ⓘ **補足:** 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 アカウントに登録されているネットワーク セキュリティ装置上でのみ使用できます。
5. 「**リソース & サポート > ダウンロード センター**」に移動します。
6. 「**シグネチャのダウンロード**」をクリックします。
7. 「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。
8. 「**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。

   ⓘ **補足:** 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。
9. ネットワーク セキュリティ装置の管理インターフェースで「セキュリティ サービス > サマリ」ページに戻ります。
10. 「**シグネチャのインポート**」の横にある「**インポート**」ボタンをクリックします。
11. ファイル ダイアログが表示されたら、シグネチャ更新ファイルの場所に移動します。
12. 「**開く**」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。
13. 「**適用**」をクリックします。

2

コンテンツ フィルタの設 定

「**コンテンツ フィルタ**」ページにはフィルタ種別のリストや、SonicWall CFS オブジェクトおよびポリシーの検索ページへのリンクがあります。「**コンテンツ フィルタ種別**」をクリックして、表示するコンテンツ フィルタ オプションを選択します。

コンテンツ フィルタ種別	説明
SonicWall CFS	SonicWall CFS は標準のコンテンツ フィルタ サービスです。
Websense Enterprise	Websense Enterprise は SonicWall コンテンツ フィルタ サービスを拡張したものです。SonicWall と Websense Enterprise を組み合わせたソリューションを展開している組織は、HTTPS 接続に対するウェブ アクセス ポリシーを強制できます。

トピック:

SonicWall CFS

このセクションでは、管理者が SonicOS のクライアント側のコンテンツ フィルタ サービス（CFS）設定を構成できます。既定の SonicWall コンテンツ フィルタ サービス ポリシーは、CFS 購読なしで利用できます。有効な詳細 CFS 購読があれば、個別 CFS ポリシーを作成して、ネットワーク ゾーンに適用したり、組織内のユーザのグループに適用したりできます。

SonicWall CFS ポリシーの主な設定は、以下のページで行います。

- すべての CFS ポリシーは「**ポリシー | ルールとポリシー > コンテンツ フィルタ ルール**」ページからアクセスできます。
- すべての CFS オブジェクトは「**オブジェクト | 一致オブジェクト > コンテンツ フィルタ/URL**」ページからアクセスできます。

CFS ポリシーを設定した後、クライアント コンテンツ フィルタの設定を行えます。

SonicOS は、McAfee との提携によって購読ベースのクライアント コンテンツ フィルタ保護を提供しています。

トピック:

CFS 状況

「**CFS 状況**」セクションには、現在のライセンス状況、ライセンス失効期日、CFS サーバの利用可否が表示されます。

グローバル設定

「**コンテンツ フィルタ**」ページの「**グローバル設定**」セクションには、CFS ポリシーのグローバル設定の定義に関する情報が表示されます。このページ上のフィールドの多くには「i」(情報) アイコンがあります。このアイコンは、該当するフィールドに関する詳しい情報を提供します。「**グローバル設定**」セクションには、以下の設定オプションがあります。

最大 URL キャッシュ登録数	キャッシュできる URL エントリの最大数を選択できます。最小値は 25,600 で、最大値は 51,200 です。このフィールドの下の補足には、選択されているモデルのサポート対象範囲がわかる「ここ」という語のリンクがあります。
コンテンツ フィルタ サービス (CFS) を有効にする	この設定は既定で「**有効**」になっています。
サーバが利用不可の場合に遮断する	このオプションが選択されていると、CFS サーバが利用不可として検出された場合にすべてのウェブ アクセスが遮断されます。
サーバ タイムアウト	ネットワーク セキュリティ装置がこのタイムアウト値の時間内に CFS サーバからの応答を得られなかった場合、そのサーバは利用不可とマークされます。最小値は 2 秒、最大値は 10 秒、既定値は 5 秒です。「**サーバが利用不可の場合に遮断する**」が選択されていない場合、この設定は使用できません。
ローカル CFS サーバを有効にする	ローカル CFS サーバではこのチェックボックスをオンにします。この設定は既定で無効になっています。
プライマリ ローカル CFS サーバ	このフィールドは、プライマリ ローカル CFS サーバの IP アドレスを保持しています。「**ローカル CFS サーバを有効にする**」が選択されている場合に使用可能になります。
セカンダリ ローカル CFS サーバ	このフィールドは、セカンダリ ローカル CFS サーバの IP アドレスを保持しています。「**ローカル CFS サーバを有効にする**」が選択されている場合に使用可能になります。

CFS 除外

「**CFS 除外**」セクションにあるこのオプションは、管理者および複数のアドレス オブジェクトからのパケットがフィルタ処理なしで通過できるように設定できます。

管理者を除外する	このチェックボックスをオンにすると、管理者からのすべてのパケットが CFS モ

	ジュールを通過します。既定で有効になっています。
除外アドレス	必要に応じて、リストからアドレスを選択します。選択したすべてのアドレスのパケットが CFS モジュールを通過します。

CFS ユーザ定義種別

「**CFS ユーザ定義種別**」セクションでは、新しいユーザ定義 CFS 種別エントリを設定できます。管理者は、ユーザ定義ポリシーおよび種別を作成し、ドメイン名のエントリを柔軟性の高い既存の CFS 格付け種別構造に挿入することができます。種別の追加および削除をページで行うには、以下の手順に従います。

- 「**追加**」をクリックしてダイアログ ボックスを開きます。このダイアログ ボックスでは、種別をリストから選択してシステムの CFS 種別に追加できます。ドメイン名と種別を選択し、「**OK**」をクリックしてそれらを追加します。
- 「**コンテンツ フィルタ**」ページの「**更新**」をクリックして、変更を保存します。変更が済んだら、「**更新**」をクリックしてダイアログ ボックスを開き、変更の適用および保持のスケジュールを選択します。

Websense Enterprise

「**コンテンツ フィルタ種別**」フィールドの「**Websense Enterprise**」オプションにより、Websense Enterprise 設定を構成するためのページが表示されます。

トピック:

- Websense サーバ状況
- 一般設定
- ウェブ機能の遮断
- CFS 除外
- 遮断ページ

Websense サーバ状況

「**Websense サーバ状況**」セクションには、現在のライセンス状況、ライセンス失効期日、CFS サーバの利用可否が表示されます。

一般設定

「**一般設定**」セクションでは、Websense サーバに関する基本的な情報を設定できます。「i」アイコンをクリックすると、該当するフィールドでユーザが選択を行う際に役立つヒントが画面に表示されます。

「**Websense プローブを有効にする**」がオンになっている場合、プローブ動作を制御するためのオプションが使用可能になります。

ウェブ機能の遮断

「**ウェブ機能の遮断**」セクションでは、管理者による選択に従い、機能およびドメインの遮断システムを設定します。

CFS 除外

「**CFS 除外**」セクションにあるこのオプションは、管理者および複数のアドレス オブジェクトからのパケットがフィルタ処理なしで通過できるように設定できます。

管理者を除外する	このチェックボックスをオンにすると、管理者からのすべてのパケットが CFS モジュールを通過します。既定で有効になっています。
除外アドレス	必要に応じて、リストからアドレスを選択します。選択したすべてのアドレスのパケットが CFS モジュールを通過します。

遮断ページ

「**遮断ページ**」セクションでは、メッセージの遮断時に Websense Enterprise サーバによって表示されるメッセージをカスタマイズできます。

3

SonicWall ゲートウェイ アンチウイルス サービスの管理

SonicWall ゲートウェイ アンチウイルス（GAV）サービスは、SonicWall の IPS-Deep Packet Inspection v2.0 エンジンを使用して 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することにより、リアルタイムのウイルス対策を直接 SonicWall ネットワーク セキュリティ装置上で実現します。SonicWall GAV は、パケットの再構築が不要な SonicWall の手法をベースとし、複数のアプリケーション プロトコル、一般的な TCP ストリーム、圧縮トラフィックを検査します。パケットの再構築を SonicWall GAV 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 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。

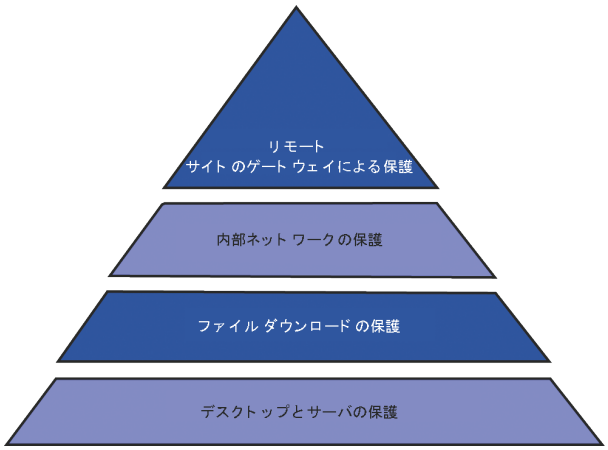
SonicWall GAV で防御できるのは、ネットワークの外部から侵入する脅威に限定されません。ネットワーク内部を起源とした脅威を抑止することもできます。SonicWall ゲートウェイ アンチウイルスは、SMTP、POP3、IMAP、HTTP、FTP、NetBIOS、インスタント メッセージングのほか、ピアツーピア アプリケーションやストリームベースの多くのプロトコルなど、多様なプロトコル上で動作し、広範囲にわたるネットワーク脅威に対する防御および制御機能を提供します。悪質なコードやウイルスを含んだファイルが圧縮されていると、従来のソリューションでは対応できない可能性があるため、SonicWall 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Capture ATP に記録されます。

トピック:

SonicWall GAV の多層型アプローチ

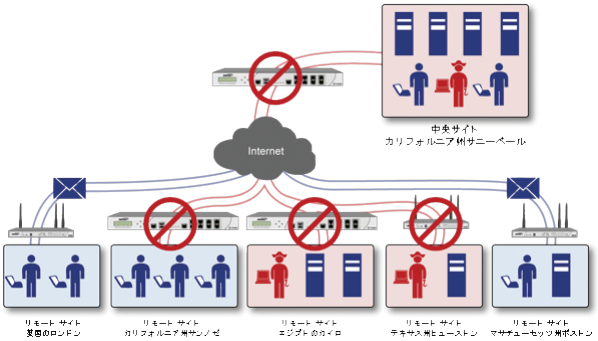
SonicWall ゲートウェイ アンチウイルスでは、多層型のネットワーク アンチウイルス防御が、デスクトップ、ネットワーク、リモート サイトなど、あらゆる場所に適用されます。「SonicWall GAV 多層型アプローチ」を参照してください。SonicWall GAV は、アンチウイルス ポリシーをゲートウェイで執行することにより、すべてのユーザに最新のアップデートを確実に適用し、ネットワークに入ってくるファイルを監視します。



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

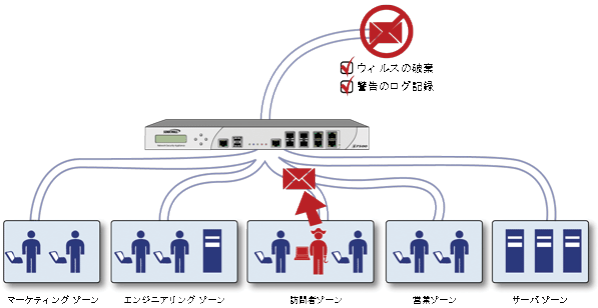
リモート サイトの保護



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 ネットワーク 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。

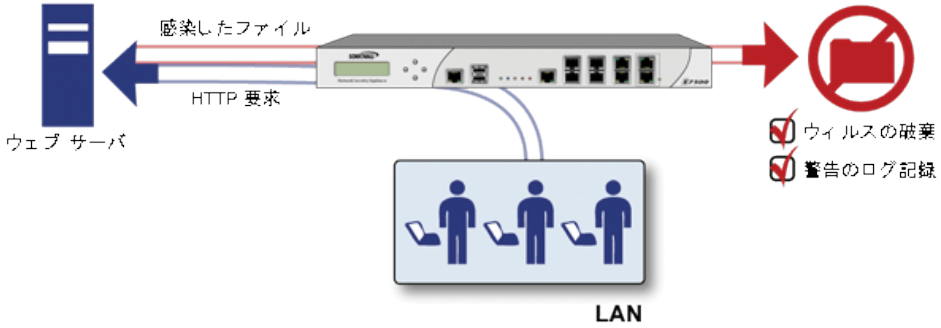
3. ウイルスはリモートのデスクトップに到達する前に検出されて遮断されます。
4. 検出されたウイルスはログに記録され、管理者に警告が送信されます。

内部ネットワークの保護



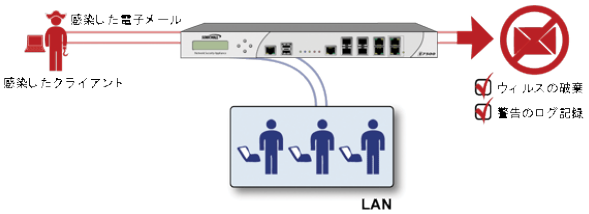
1. 内部のユーザによって持ち込まれたウィルスが社内に蔓延します。
2. すべてのファイルは、他のネットワーク ユーザが受け取る前にゲートウェイでスキャンされます。
3. ウイルスが検出されたファイルは破棄されます。
4. 検出されたウイルスはログに記録され、管理者に警告が送信されます。

HTTP ファイルのダウンロード



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



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。

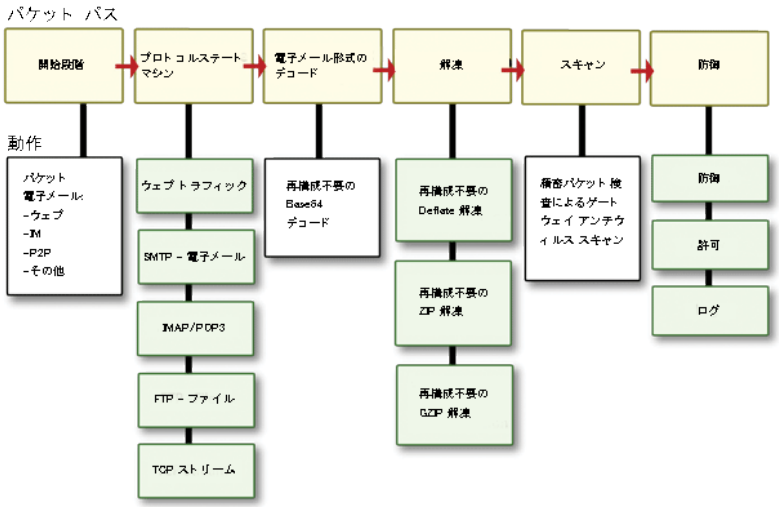
クラウド アンチウイルス データベース

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 ネットワーク セキュリティ装置の既存のゲートウェイ 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 アーキテクチャ

SonicWall ゲートウェイ アンチウイルス (GAV) は SonicWall の高性能な精密パケット検査バージョン 2.0 (DPIv2.0) エンジンをベースとしています。このエンジンは、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 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構築することなく、base64 のデコードを実行できます。パケットの再構築を SonicWall GAV 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構築が不要なウイルス 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。



パケットの再構築が不要な SonicWall の手法をベースとしながら、SonicWall GAV は、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。SonicWall GAV は 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 ネットワーク 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 アンチウイルス、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、侵入防御 ライセンスの有効化

これらのセキュリティ サービスを使用する前に、MySonicWall にネットワーク セキュリティ装置を登録する必要があります。『*クイック スタート ガイド*』の情報を参照して、MySonicWall アカウントを作成し、装置を登録してください。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 7 アップグレード ガイド*』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、および侵入防御の一部なので、受け取った有効化鍵は SonicWall ネットワーク 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 ゲートウェイ アンチウイルス、アンチスパイウェア、および侵入防御のライセンスが SonicWall ネットワーク セキュリティ装置で有効化されていない場合は、SonicWall リセラーまたは MySonicWall アカウント（米国およびカナダのお客様のみ）からライセンスを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 侵入防御の無料トライアル版を試用できます。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『*クイック スタート ガイド*』を参照してください。

SonicWall ゲートウェイ アンチウイルス防御のセットアップ

SonicWall ネットワーク 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にします。
2. SonicWall ゲートウェイ アンチウイルス防御をゾーンに適用します。

トピック:

- SonicWall ゲートウェイ アンチウイルス状況情報の表示
- SonicWall ゲートウェイ アンチウイルスの有効化
- ゾーンに対する SonicWall ゲートウェイ アンチウイルス防御の適用
- プロトコル フィルタの指定
- クラウド ゲートウェイ アンチウイルスの設定

SonicWall ゲートウェイ アンチウイルス状況情報の表示

「**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 ネットワーク 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 ゲートウェイ アンチウイルス シグネチャ データベース状況の確認
- SonicWall ゲートウェイ アンチウイルス シグネチャの更新

SonicWall ゲートウェイ アンチウイルス 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、以下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 ゲートウェイ アンチウイルス シグネチャ データベースの最終更新日時です（SonicWall ネットワーク セキュリティ装置の最終更新日時ではありません）。
- 「**最終確認**」には、SonicWall ネットワーク 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 ネットワーク 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 ゲートウェイ アンチウイルス サービスの有効期限が切れる日付が示されます。SonicWall ゲートウェイ アンチウイルスの購読期限が切れると、SonicWall IPS検査が停止し、SonicWall ゲートウェイ アンチウイルスの構成設定値が SonicWall ネットワーク セキュリティ装置から削除されます。これらの設定は、SonicWall ゲートウェイ アンチウイルス 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。
- 「**ゲートウェイ アンチウイルス**」セクションに次のように表示されます。**補足: ゾーンに対するゲートウェイ アンチウイルスを有効にするには、「ネットワーク > ゾーン」**ページで設定します。「**ネットワーク > ゾーン**」リンクをクリックすると、SonicWall ゲートウェイ アンチウイルスをゾーンに適用するための「**オブジェクト | 一致オブジェクト > ゾーン**」ページが表示されます。

SonicWall ゲートウェイ アンチウイルス シグネチャの更新

既定で、SonicWall ゲートウェイ アンチウイルスが稼働している SonicWall ネットワーク 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**」ボタンをクリックすると、SonicWall ゲートウェイ アンチウイルス データベースをいつでも手動で更新できます。

SonicWall ゲートウェイ アンチウイルスのシグネチャ更新は、セキュリティで保護されています。SonicWall ネットワーク 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。

SonicWall ゲートウェイ アンチウイルスの有効化

ご利用の SonicWall ネットワーク セキュリティ装置で SonicWall ゲートウェイ アンチウイルスを有効にするには、「**ゲートウェイ アンチウイルスのグローバル設定**」セクションで「**ゲートウェイ アンチウイルスを有効にする**」チェックボックスをオンにする必要があります。

SonicWall ゲートウェイ アンチウイルス防御が必要なすべてのゾーンを「**オブジェクト | 一致オブジェクト > ゾーン**」ページで指定してください。

ゾーンに対する SonicWall ゲートウェイ アンチウイルス防御の適用

SonicWall ゲートウェイ アンチウイルスをゾーンに適用するのは「**オブジェクト | 一致オブジェクト > 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「**オブジェクト | 一致オブジェクト > 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、「**オブジェクト | 一致オブジェクト > ゾーン**」ページで設定します。" のリンクをクリックしてください。これは「**SonicWall 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。

プロトコル フィルタの指定

SonicWall ゲートウェイ アンチウイルスは、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
- 送信検査の有効化
- ファイル転送の制限
- ゲートウェイ アンチウイルス設定のリセット

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 ゲートウェイ アンチウイルスによって検査されます。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 ゲートウェイ アンチウイルス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。

- 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

SMTP トラフィック

	送信先	保護	暗号化	無線	パブリック	非保護
送信元						
保護		✔	✔	✔		
暗号化		✔	✔	✔		
無線		✔	✔	✔		
パブリック		✔	✔	✔	✔	✔
非保護		✔	✔	✔	✔	✔

その他すべてのトラフィック

	送信先	保護	暗号化	無線	パブリック	非保護
送信元						
保護		✔	✔	✔	✔	✔
暗号化		✔	✔	✔	✔	✔
無線		✔	✔	✔	✔	✔
パブリック						✔
非保護						

送信検査の有効化

「**送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」ボタンをクリックして、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 ゲートウェイ アンチウイルス シグネチャのアップデートと共に動的に追加されます。

除外設定

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 アンチウイルス設定のリセット

すべてのゲートウェイ アンチウイルス設定を出荷時の既定値にするには、以下の手順に従います。

1. 「**ゲートウェイ AV 設定のリセット**」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**」をクリックします。

ゲートウェイ アンチウイルスの設定

「**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 アンチウイルス設定の構成**」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 ゲートウェイ アンチウイルス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 アンチウイルスの設定
- 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 アンチウイルスの設 定

ゲートウェイ アンチウイルス オプションを設定するには、以下の手順に従います。

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 ゲートウェイ アンチウイルス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**」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. EICAR Standard Anti-Virus Test ファイルは、SonicWallゲートウェイ アンチウイルス 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**」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. 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**」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。

   SonicWall ゲートウェイ アンチウイルス 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」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. ゲートウェイ アンチウイルス 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 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。
6. 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**」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す。
7. 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**」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. ゲートウェイ アンチウイルス サービスを検出専用モード (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**」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。

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ゲートウェイ アンチウイルス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、その脅威はゲートウェイ アンチウイルスによって遮断され、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ゲートウェイ アンチウイルス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**」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。
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 > サマリ**」ページの「**セキュリティ サービス設定**」の見出しの下で、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 アドレスに関しては、トラフィックに対するウイルス スキャンが回避されます。「**ゲートウェイ AV 除外リスト**」セクションでは、SonicWall ゲートウェイ アンチウイルス 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 ゲートウェイ アンチウイルス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、以下の手順に従います。

1. 「**ポリシー | 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 アンチウイルス設定の構成**」ボタンをクリックします。
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**」を選択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
        1. 「**アドレス オブジェクトを使用する**」リストからアドレス オブジェクトを選択します。
        2. 「**OK**」をクリックします。
    - 「**アドレス範囲を使用する**」ラジオ ボタン
        1. 「**追加**」アイコンをクリックします。「**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。
        2. 「**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。
        3. 「**OK**」をクリックします。ここで入力した IP アドレスの範囲は、「**ゲートウェイ AV 除外リスト**」テーブルに表示されます。
            1. エントリを変更するには、「**構成**」列にある「**編集**」アイコンをクリックします。
            2. エントリを削除するには、「**削除**」アイコンをクリックします。
            3. 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**」ボタンをクリックします。
        4. 「**OK**」をクリックします。

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、以下の手順に従います。

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**」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**」を選択します。(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、以下の手順に従います。

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。
   追加するシグネチャ ID ごとに前の 2 つのステップを繰り返します。
4. 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**」をクリックします。
5. 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。
6. 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。
7. 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**」をクリックします。

SonicWall ゲート ウェイ アンチウイルス 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 ゲートウェイ アンチウイルス 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 ゲートウェイ アンチウイルス ネットワーク セキュリティ装置にダウンロードされた SonicWall 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。

ⓘ **補足:** 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 テーブルへの移動
- 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** — 「開始文字」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。
  1. 「**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。
  2. 「**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 テーブルへの移動

SonicWall ゲートウェイ アンチウイルス シグネチャは「**ゲートウェイ アンチウイルス シグネチャ**」テーブルに 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、「*補足情報 SonicOS*」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。

4

アンチスパイウェア サービス

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（GAV）、アンチスパイウェア、および 侵入防御 サービス（IPS）統合脅威管理ソリューションに含まれます。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 サービスを組み合わせると、ネットワーク全体に対する包括的なリアルタイム ゲートウェイ セキュリティ ソリューションを実現できます。

SonicWall アンチスパイウェア のライセンスを有効化した後は、管理インターフェースで SonicWall アンチスパイウェアを有効にして設定する必要があります。この作業を完了しないと、アンチスパイウェア ポリシーをネットワーク トラフィックに適用できません。

SonicWall アンチスパイウェア サービスを設定する手順については、『*SonicWall アンチスパイウェア サービス管理ガイド*』を参照してください。この管理ガイドを入手できる SonicWall ウェブサイトの URL は次のとおりです。
https://www.sonicwall.com/ja-jp/support/technical-documentation.

ご利用の SonicWall ネットワーク セキュリティ装置でアンチスパイウェアを有効にして設定するには、「**ポリシー | セキュリティ サービス > アンチスパイウェア**」に移動します。アンチスパイウェア管理インターフェースの画面は、以下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
- アンチスパイウェア グローバル設定
- シグネチャ グループ
- プロトコル
- アンチスパイウェア シグネチャ

アンチスパイウェア状 況

画面のこのセクションには、シグネチャ データベース、SonicWall アンチスパイウェアのライセンス、その他詳細の状況に関する情報が表示されます。最新の利用可能なデータベースの日時が示されます。あるゾーンでアンチスパイウェア サービスを有効にする場合は、「**ゾーン**」画面へのリンクになっている「**ゾーン**」という語をクリックします。

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を有効にする** – ご利用の SonicWall ネットワーク セキュリティ装置で アンチスパイウェア を有効にするための主な設定を使用可能にするには、このオプションを選択します。
- **WAN、LAN/WorkPort、DMZ/HomePort/WLAN/OPT** – アンチスパイウェアを有効にした後は、インターフェースに関するこれら 3 つのチェックボックスが使用可能になります。スパイウェアを有効化したいものをオンにします。最初に、ご利用の SonicWall ネットワーク セキュリティ装置で SonicWall アンチスパイウェアをグローバルで有効な状態にしておく必要があります。

シグネチャ グループ

- 3つの異なる危険レベルごとに異なる保護を選択できます。
  - **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**
- **すべて防御** – このレベルの攻撃すべてについて検知、ログ記録、防御を行うには、このオプションを選択します。

  △ **注意: 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」の各シグネチャ グループで「すべて防御」を有効にして、特に大きな損害や混乱につながるスパイウェア アプリケーションに対してアンチスパイウェア防御を実施することを推奨しています。スパイウェアに関するログ記録と警告のために、「すべて検知」を有効にすることもできます。**
- **すべて検知** – 検知とログ記録のみを行うには、このオプションを選択します。
- **ログ冗長フィルタ (秒)** – 同じ攻撃に対するエントリによってログ記録の負荷が過剰になるのを防ぐには、このフィールドに値を入力します。例えば、30 秒という値を入力した場合、その期間に 100 回の SubSeven 攻撃があったとしても、その 30 秒間にログに記録されるのは 1 回の攻撃だけとなります。
- **設定の構成** – 攻撃レベルの図の上に表示されるボタンの 1 つです。「**アンチスパイウェア設定**」ダイアログボックスを表示します。
  - **アンチスパイウェア 設定**
    - **SMTP 応答を無効にする** – 電子メールまたは添付ファイルの中のウイルスが検出されたときに、SonicWall アンチスパイウェアからクライアントに宛てた電子メール メッセージ (SMTP) の送信を抑止するには、このチェックボックスをオンにします。
  - **HTTP クライアント不要の通知**
    - **HTTP クライアント不要の警告通知を有効にする** – このチェックボックスをオンにすると、その下のボックスに、要求が遮断されたときに表示されるメッセージを入力できます。
  - **アンチスパイウェア除外リスト**
    - **アンチスパイウェア除外リストを有効にする** – 除外リストによってスパイウェアを制限できるようにするには、このチェックボックスをオンにします。セキュリティ装置は、指定されたアドレス オブジェクトまたは IP 範囲についてアンチスパイウェアの強制適用を回避します。このチェックボックスをオンにすると、除外オブジェクトのアドレスを指定するために、以降のフィールドが使用可能になります。
    - 除外リストに追加するアドレス オブジェクトまたはアドレス範囲を選択します。

- **シグネチャ データベースの更新** – クリックすると、シグネチャタブにあるリストが再表示されます。ダイアログ ボックスが表示され、変更するスケジュールに関する詳細情報の入力が求められます。
- **設定のリセット** – クリックすると、設定が工場出荷時の状態にリセットされます。ダイアログ ボックスが表示され、変更するスケジュールに関する詳細情報の入力が求められます。

プロトコル

アンチスパイウェア ソフトウェアによって**受信検査を有効にする**プロトコルを選択できます。

- 選択する各プロトコルのチェックボックスをオンにします。
- **発信スパイウェア通信検査を有効にする** – このオプションをクリックすると、検査で発信トラフィックが使用可能になります。

アンチスパイウェア シグネチャ

SonicWall アンチスパイウェアを使用すると、アンチスパイウェア ポリシーを種別およびシグネチャ レベルで設定して、SonicWall アンチスパイウェア防御をご利用のネットワーク環境の要件に基づいて柔軟かつきめ細やかにカスタマイズできます。こうしたユーザ定義 SonicWall アンチスパイウェア ポリシーは、アドレス オブジェクト、アドレス グループ、ユーザ グループのほか、強制スケジュールの作成にも適用できます。

「**シグネチャ**」行にある「**構成**」をクリックすると、以下のフィールドを「**アンチスパイウェア シグネチャ設定**」ダイアログ ボックスで設定できます。

フィールド	説明
製品名	設定のために選択した行に表示される名前
防御	アンチスパイウェアによる防御をデバイスに対して有効または無効にできます。
検知	アンチスパイウェアによる検知をデバイスに対して有効または無効にできます。
包含するユーザ/グループ	アンチスパイウェア設定を次のグループ種別のメンバーに適用します。All、Administrators、Everyone、ゲスト サービス、Trusted Users、Content Filtering Bypass、Limited Administrators
除外するユーザ/グループ	アンチスパイウェア設定を次のグループ種別のメンバーには適用しません。All、Administrators、Everyone、ゲスト サービス、Trusted Users、Content Filtering Bypass、Limited Administrators
包含する IP アドレス範囲	指定された種別の指定 IP アドレス範囲に含まれるすべてのユーザにアンチスパイウェア設定を適用できます
除外する IP アドレス範囲	指定された種別の指定 IP アドレス範囲に含まれるすべてのユーザを除外できます
スケジュール	スケジュールを設定できます
ログ冗長フィルタ	フィルタを設定するには、このチェックボックスをオンにします
製品設定を使用する (秒)	フィルタのチェックボックスがオンになっている場合、この設定は使用できません

5

侵入防御 サービス

侵入防御 サービス (IPS) は、新しい攻撃や、ネットワークを潜在的なリスクにさらす不適切な使用からネットワークを保護するために頻繁に更新される購読ベースのサービスです。

トピック:

侵入防御 サービス について

SonicWall 侵入防御 サービス (SonicWall 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 (DPI) 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アーキテクチャ (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、柔軟性を最大限に高めるとともに、偽陽性による誤検出を抑制できます。

精密パケット検査 (DPI) 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 SonicWall セキュリティ装置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、SonicWall ネットワークセキュリティ装置を通過する侵入を、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 (パケットの破棄、TCP 接続のリセットなど)。SonicWall の DPI 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。

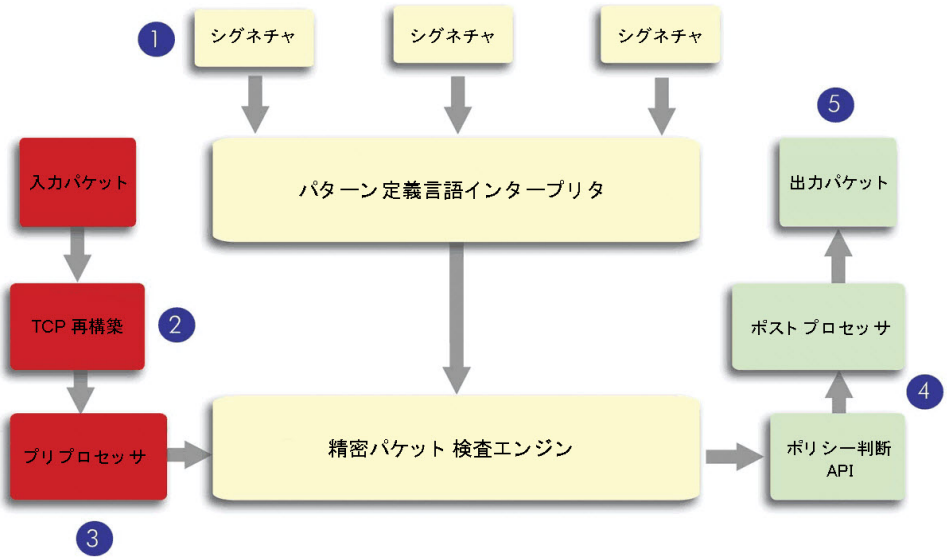
精密パケット検査 (DPI) 技術を使用すると、SonicWall ネットワーク ファイアウォール装置でプロトコル内を精査し、アプリケーション層で情報を検証して、アプリケーションの脆弱性を対象とした攻撃を阻止できます。これは、

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 分散執行型アーキテクチャから配布される動的シグネチャ更新を可能にします。

SonicWall 精密パケット検査アーキテクチャは、以下のように機能します。

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、その場合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、パケットを破棄するか、場合によっては 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、再構築を一切実行することなく 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 DEEP PACKET INSPECTION ARCHITECTURE



TCP パケットが正しい順序で到着しなかった場合、SonicWall IPS エンジンは検査前にそれらの再構築を行います。ただし、SonicWall の IPS フレームワークは、完全な再構築の実施を必要とすることなく 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。SonicWall 独自の再構築が不要な一致ソリューションにより、CPU およびメモリリソースの要件が大幅に低下します。

侵入防御 サービスの有効化

1 台以上の SonicWall ネットワーク セキュリティ装置で 侵入防御の設定を行うには、以下の手順に従います。

1. グローバル アイコン、グループ、または SonicWall ネットワーク セキュリティ装置を選択します。
2. 「**セキュリティ サービス > 侵入防御**」に移動し、「侵入防御」画面の 3 つのセクションで必要な変更を行います。

IPS 状況

画面の最上部には、システムの侵入防御 サービスの状況が表示されます。**使用可能な最新のシグネチャ データベース**の日時と、IPS が有効になっているゾーンがわかります。あるゾーンで侵入防御 サービスを有効にする場合は、このセクションにある「**ゾーン**」という語をクリックすると、そのゾーンへのリンクを取得できます。

IPS グローバル設定

- **IPS を有効にする** – この設定をクリックすると、侵入防御が有効になります。サービスが有効になった後、次の 3 つのチェックボックスが使用可能になります。

  監視するインターフェース ポート (WAN、LAN、または DMZ/WLAN/OPT) のチェックボックスをオンにします。これら 3 つのチェックボックスは「**IPS を有効にする**」がオンの場合に使用可能になります。
- 次のセクションでは、監視する攻撃のレベルと方法を設定できます。「**高危険度の攻撃**」、「**中危険度の攻撃**」、「**低危険度の攻撃**」で異なるレベルの防御を設定できます。
  - **すべて防御** – このレベルの攻撃すべてについて検知、ログ記録、防御を行うには、このオプションを選択します。
  - **すべて検知** – 検知とログ記録のみを行うには、このオプションを選択します。
  - **ログ冗長フィルタ (秒)** – 同じ攻撃に対するエントリによってログ記録の負荷が過剰になるのを防ぐには、このフィールドに値を入力します。例えば、30 秒という値を入力した場合、その期間に 100 回の SubSeven 攻撃があったとしても、その 30 秒間にログに記録されるのは 1 回の攻撃だけとなります。
  - **Configure IPS Settings (IPS 設定の構成)** – 攻撃レベルの図の下に表示される 4 つのボタンの 1 つです。以下のダイアログ ボックスが表示されます。
    - **IPS 除外リスト**
    - **IPS 除外リストを有効にする** – 指定された IP アドレス オブジェクトまたは指定された範囲のアドレス オブジェクトに対する侵入防御 強制をスキップするように SonicWall セキュリティ装置を設定するには、このフィールドを選択します。以下のフィールドは、このフィールドが選択されている場合のみ使用可能です。
      - **アドレス オブジェクトを使用する** – 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。
      - **アドレス範囲を使用する** – 除外するアドレス範囲の制限を入力します。アドレス範囲が選択されている場合は、選択対象すべてを追加または削除できます。

- **Update IPS Signature Database (IPS シグネチャ データベースの更新)** – すべてのシグネチャのダウンロードをファームウェアに強制する場合に選択します。
- **Reset IPS Settings & Policies (IPS 設定とポリシーのリセット)** – クリックすると、IPS 設定が既定値にリセットされます。
- **Import CSV File (CSV ファイルのインポート)** – このボタンにより CSV ファイルがインポートされます。
- このページの設定が完了したら、「**OK**」または「**キャンセル**」をクリックします。

保存 – スケジュールに関する詳細情報と、行った個々の変更の保持を要求するダイアログ ボックスが表示されます。

キャンセル – 画面上のすべての設定を消去します。

侵入防御 サービス ポリシー

このセクションでは、管理者が個々の攻撃に対する設定を行えます。

1. 表示する攻撃の種別を特定します。種別で並べ替えるには、「**種別**」リストで種別を選択します。優先順位で並べ替えるには、「**優先順位**」リストで優先順位レベルを選択します。
2. 設定する攻撃の種別を特定した後、その行にある「**Config/Edit (構成/編集)**」をクリックします。選択した攻撃の「**IPS シグネチャ設定**」に関する具体的な情報が得られるダイアログ ボックスが表示されます このダイアログ ボックスの上部には、選択した「**シグネチャ**」行からの情報が設定されています。
3. 編集が必要な各種別のダイアログ ボックスで以下のフィールドを設定します。
    - **防御** – この種別の攻撃に対する攻撃の防御を有効にするか、無効にするか、攻撃種別に対する既定のグローバル設定を使用するかをリストから選択します。
    - **検知** – この種別の攻撃に対する攻撃の検知を有効にするか、無効にするか、攻撃種別に対する既定のグローバル設定を使用するかをリストから選択します。
    - **包含するユーザ/グループ** – この攻撃種別でどのユーザまたはグループを含めるかをリストから選択します。
    - **除外するユーザ/グループ** – この攻撃種別でどのユーザまたはグループを除外するかをリストから選択します。
    - **包含する IP アドレス範囲** – この攻撃種別で含める IP アドレス範囲をリストから選択します。
    - **除外する IP アドレス範囲** – この攻撃種別で除外する IP アドレス範囲をリスト ボックスから選択します。
    - **スケジュール** – この攻撃種別に対して攻撃の防御を強制する時間範囲をリストから選択します。
    - **ログ冗長フィルタ (秒)** – フィルタを設定する時間 (秒単位) を入力するか、「**種別設定を使用する**」を選択します。
4. **保存** – このオプションを選択すると「侵入防御」ページに戻ります。変更が適用されます。
5. **キャンセル** – このオプションを選択すると変更が破棄されます。

6

地域 IP フィルタの設定

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 ネットワーク セキュリティ装置は 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。

トピック:

地域 IP フィルタの設定

「**設定**」ページには、地域 IP フィルタで構成できる設定のグループが表示されます。こうした設定のいくつかの横には、その設定に関する画面上のヒントを表示する（情報）アイコンがあります。

- **「国」タブで選択した国との双方向の接続を遮断する** – このオプションは既定で選択されています。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ると、選択した IP の遮断を除外できます。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。
  - **すべての接続** – 地域フィルタの 2 つのモードのうち 1 つを選択します。ファイアウォールとの双方向の接続すべてをフィルタします。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** – こちらを選択すると、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が遮断のためにフィルタされます。
- **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** – このオプションは、既定では選択されていません。地域 IP データベースがダウンロードされていない場合、こちらを選択するとパブリック IP アドレスからの接続試行はすべて破棄されます。
- **ユーザ定義リストを有効にする** – このオプションは、既定では選択されていません。ユーザ定義リストは、IP アドレスに対する国の割り当ての誤りを訂正するために使用されます。このチェックボックスをオンにすると、「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」が使用可能になります。

- **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** – この選択肢は「ユーザ定義リストを有効にする」がオンになっている場合に限り使用できます。選択すると、ユーザ定義リストにより、差異がある場合にファイアウォール リストを上書きできます。ユーザ定義リストを有効にしていても、この上書きを選択しない限りファイアウォール リストが優先されます。
- **ログを有効にする** – 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、フィルタ イベントのログが有効になります。

「**国**」ページには、地域 IP フィルタによって特定の国を遮断するように構成できる設定のグループが表示されます。

- **遮断する国**テーブル – 遮断する国のチェックボックスをオンにします。既定では、どの国も遮断されません。テーブル上部のチェックボックスをオンにして、すべての国を選択し、その後、遮断の対象から除外する国を個別にクリックして選択解除することができます。
- **すべての不明な国を遮断する** – リストされていない国をすべて遮断する場合は、この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。
- **地域 IP 除外オブジェクト** – 承認された IP アドレスに対するすべての接続の除外リストを設定できます。

  リストからアドレス グループを選択します。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、ページの右上にある「**状況**」インジケータが黄色になります。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。

  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 `geodnsd.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。

  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。

次のどちらかをクリックします。

- 変更を確認する場合は「**適用**」。
- 変更をキャンセルする場合は「**リセット**」。

ユーザ定義国リストの作成

このセクションでは、遮断または許可する IP アドレスのユーザ定義リストを作成できます。これは、例えば、遮断される国に IP アドレスが誤って関連付けられていて、そのアドレスを許可したい場合に役立ちます。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。

ネットワーク セキュリティ装置で**ユーザ定義リスト**を優先的に使用するには、そのリストを有効にして「**Override Firewall List (ファイアウォール リストを上書きする)**」を選択する必要があります。

ユーザ定義リスト アドレス オブジェクトを追加するには、以下の手順に従います。

1. 「**追加**」をクリックして「**アドレス位置の追加**」ダイアログ ボックスを開きます。
2. 「**IP アドレス**」リストで、IP アドレスを選択します。
3. 「**国**」リストで、国を選択します。
4. 必要に応じて、「**コメント**」フィールドにコメントを追加できます。
5. 「**保存**」をクリックします。

トピック:

- ユーザ定義リスト エントリの編集
- ユーザ定義リストのエントリの削除

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. 編集するエントリの「構成」列にある「**編集**」アイコンをクリックします。「**Edit Address Location (アドレス位置の編集)**」ダイアログが現れ、既に設定されている、IP アドレスとそのエントリに関するコメントが表示されます。
2. 「**国**」リストで、国を選択します。
3. 「**保存**」をクリックします。
   「**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 1 つ削除するには、以下の手順に従います。

1. エントリの「構成」列にある「**削除**」をクリックするか、エントリのチェックボックスをオンにしたうえで最上部の行にある「**削除**」をクリックします。確認メッセージが表示されます。
2. 「**OK**」をクリックします。

ユーザ定義リストの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するか、最上部ですべてのエントリを選択します。「**削除**」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. 「**保存**」をクリックします。

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できる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。

- **地域 IP フィルタ遮断の詳細を含める** – このオプションを選択すると、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。
- **警告文**
  - 「**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**」をクリックします。
  - 必要に応じて、**警告文**として表示するユーザ定義メッセージを入力します。メッセージは最大 100 文字で、英数字、空白、ピリオド (.)、アンダースコア (_) のみを含めることができます。
- 「**Base64 でエンコードされたロゴ アイコン**」 – このフィールドでは、Base 64 エンコード GIF アイコンを指定して、既定の SonicWall ロゴの代わりに表示することができます。

  ⓘ **補足:** このアイコンが有効であることを確認し、サイズはできるだけ小さくしてください。推奨サイズは 400 x 65 ピクセルです。

- **プレビュー** – クリックすると、ウェブ サイト ページのプレビュー ウィンドウが表示されます。これにより、設定を確認し、必要に応じて変更を加えることができます。
- **既定の遮断ページ** – 遮断メッセージを既定の内容にリセットします。

ウェブ遮断ページの設定を既定値に戻すには、以下の手順に従います。

1. 「**既定の遮断ページ**」をクリックします。
   ⓘ | **重要**:「**Base64 でエンコードされたロゴ アイコン**」フィールドは、空白のままにしておく必要があります。
2. 「**適用**」をクリックします。
3. 「**更新**」をクリックします。ダイアログ ボックスが表示され、更新のスケジュールに関する情報の入力と、変更作成で選択したフィールドの編集が求められます。

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 > 診断**」ページでは、次の複数のツールにアクセスできます。

- 地域 IP キャッシュ統計
- ユーザ定義の国の統計
- 解決された位置の表示
- アドレスの指定に誤りがある場合
- 地域ロケーション サーバ調査を確認する

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**
- **呼び出し回数**
- **検索失敗回数**
- **解決回数**

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

補足: 同様のボットネット ロケーション サーバ調査ツールを「**セキュリティ 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。

地域サーバを調査するには、以下の手順に従います。

1. 「**ポリシー | 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。「**ポリシー | 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**」リンクをクリックしてください。

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。

7

ボット ネット フィルタの設 定

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。また、ウェブ サイト遮断時に送信するユーザ定義メッセージを作成したり、動的ボットネットの HTTP 認証を許可したりできます。このページ上の選択項目の多くには、**情報**アイコンがあり、その上にマウス カーソルを置くと画面にヒントが表示されます。

トピック:

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. 「**ポリシー | 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. 「**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、次の説明に従って、ユーザ定義ボットネット リストを作成します。ユーザ定義ボットネット リストの作成.
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**: ファイアウォールとの双方向の接続すべてをフィルタします。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**」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。

「**ユーザ定義ボットネット リストを有効にする**」が選択されていない場合は、ネットワーク セキュリティ装置上にあるボットネット データベースのみが検索されます。**ステップ 6 に進みます。**

「**ユーザ定義ボットネット リストを有効にする**」を選択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**」リストからアドレス 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。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**」をクリックします。

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 オブジェクトの名前。
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。
構成	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
- 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 リストのエントリの削除

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、次の説明に従って、このリストを有効にする必要があります。「ボットネット フィルタの設定」.

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. 「**ポリシー | 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. 「**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、「適用」をクリックします。
4. 「**ユーザ定義ボットネット リスト**」を選択し、**追加**アイコンを選択します。「**アドレス位置の追加**」ダイアログが表示されます。
5. 「**ボットネット IP アドレス**」リストから、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 位置の追加**」ダイアログが表示されます。
     1. 『*SonicWall SonicOS 7 ポリシー*』の説明に従って、新しいアドレス オブジェクトを制限付きで作成します。許可されている種別は次のとおりです。
        1. **ホスト**
        2. **範囲**
        3. **ネットワーク**
        4. 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 位置の追加**」ダイアログが表示されます。
     『*SonicWall SonicOS 7 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**」をクリックします。

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「**構成**」列にある「**編集**」アイコンを選択します。「**アドレス位置の追加**」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. 「**保存**」をクリックします。

   「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。
2. 確認メッセージが表示されます。
3. 「**確認**」をクリックします。

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. 「**確認**」をクリックします。

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. 「**確認**」をクリックします。

動的 HTTP 認証の設定

SonicOS では、動的ボットネットの設定で HTTP 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、ネットワーク セキュリティ装置は必要な情報を取得します。

動的 HTTP 認証を設定するには、以下の手順に従います。

1. 「**ポリシー | 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**」をクリックします。
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 minutes**（既定）
   - **15 minutes**
   - **1 hour**
   - **24 hours**

   ネットワーク セキュリティ装置は、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. 「**プロトコル**」で、ファイルを取得するためにネットワーク セキュリティ装置がバックエンド 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 ファイルのダウンロード先となるサーバの IP アドレスを入力します。

7. 「**ログイン ID**」フィールドに、ネットワーク セキュリティ装置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、ネットワーク セキュリティ装置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、ネットワーク セキュリティ装置がボットネット 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**」をクリックします。

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. 「**ポリシー | 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. 「**ウェブ遮断ページ**」を選択し、「**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**」ボタンをクリックします。
   - **ボットネット フィルタ遮断**ページに表示するユーザ定義メッセージを「**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。

   ⓘ **補足:** 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 ピクセルです。
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**」ボタンをクリックします。警告メッセージが表示されます。
6. 「OK」をクリックします。「**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**」をクリックします。

ボット ネット フィルタ診断の使用

「**ポリシー | セキュリティ サービス > ボットネット フィルタ**」ページでは、次の複数のツールにアクセスできます。

- ボットネット キャッシュ統計
- ボットネットの統計
- 解決されたボットネット位置の表示

- ボットネットサーバ調査を確認する
- アドレスの指定に誤りがある場合

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**
- **呼び出し回数**
- **検索失敗回数**
- **解決回数**

解決されたボット ネット位置の表示

「**診断**」セクションの「**ボットネットの表示**」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 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

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. 「**ポリシー | 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. 「**Go**」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

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、この問題を「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、次のいずれかの操作を行います。

- 「**ポリシー > 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**」にある iマーク のリンクをクリックします。
- 「SonicWall ボットネット IP 状況調査」に移動します。

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**」アイコンをクリックします。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。

8

アプリケーション制御の設定

アプリケーション制御はライセンスされたサービスであり、この機能を使用するには該当するサービスを有効にする必要があります。

「**ポリシー | セキュリティ サービス > アプリケーション制御**」ページでは、種別、アプリケーション、シグネチャを使用してグローバルなアプリケーション制御ポリシーを設定できます。アプリケーションのある種別全体の遮断とログ記録を迅速に有効化したり、個々のアプリケーションや個々のシグネチャを容易に特定して同じ処理を実行したりできます。有効にすると、「**ポリシー | セキュリティサービス > アプリケーション ルール**」ページでポリシーを作成しなくても、種別、アプリケーション、またはシグネチャのグローバルな遮断またはログ記録が行われます。すべてのアプリケーション検知および防御の設定は「**ポリシー | セキュリティサービス > アプリケーション制御**」ページで利用できます。

ⓘ **補足:** 「**ポリシー | セキュリティ サービス > アプリケーション制御 | アプリケーション制御のグローバル設定**」ページで「**アプリケーション制御を有効にする**」が選択されている場合、精密パケット検査 (DPI) に合格したすべてのトラフィックで **Connection Closed Syslog** メッセージに **dpi=1** の Syslog タグが表示されます。DPI を通過しなかったトラフィックでは、**Connection Closed Syslog** メッセージで **dpi=0** と表示されます。Syslog タグ フィールド説明のインデックスの詳細と、SPI タグを説明する Syslog の例については、『*SonicOS ログ イベント管理ガイド*』を参照してください。

このページでは次の設定を使用できます。

- 種別、アプリケーション、またはシグネチャを選択する。
- 遮断またはログ記録、あるいはこれら両方の動作を選択する。
- 動作に含めたり除外したりするユーザ、グループ、または IP アドレス範囲を指定する。
- 制御を執行するスケジュールを設定する。

これらのアプリケーション制御設定はアプリケーション ルール ポリシーとは独立したものですが、ここで使用できる任意の種別、アプリケーション、またはシグネチャでアプリケーション一致オブジェクトを作成して、それらの一致オブジェクトをアプリケーション ルール ポリシーで使用することもできます。詳細については、「*アプリケーション リスト オブジェクトについて*」および「*アプリケーション リスト オブジェクトの設定*」を参照してください。

ⓘ **ビデオ:** アプリケーション制御の設定例を示す情報ビデオがオンラインで提供されています (https://www.sonicwall.com/ja-jp/support/video-tutorials)。

トピック:

- アプリケーション制御ポリシーの作成について
- アプリケーション制御の状況の表示
- アプリケーション制御のグローバル設定について
- アプリケーション制御のグローバル設定の構成
- シグネチャの表示
- プリケーション制御の種別ごとの設定
- アプリケーション制御のアプリケーションごとの設定
- アプリケーション制御のシグネチャごとの設定

アプリケーション制御ポリシーの作成について

「**ポリシー | セキュリティサービス > アプリケーション制御**」ページの設定手法では、特定の種別、アプリケーション、またはシグネチャをきめ細かく制御できます。これには、きめ細かなログ制御や、ユーザ、グループ、または IP アドレス範囲の包含および除外、スケジュールのきめ細かな設定が含まれます。ここでの設定はグローバルなポリシーであり、どんな個別のアプリケーション ルール ポリシーからも独立しています。

このページでは次の設定を使用できます。

- 種別、アプリケーション、またはシグネチャを選択する。
- 遮断またはログ記録、あるいはこれら両方の動作を選択する。
- 動作に含めたり除外したりするユーザ、グループ、または IP アドレス範囲を指定する。
- 制御を執行するスケジュールを設定する。

これらのアプリケーション制御設定はアプリケーション ルール ポリシーとは独立したものですが、この場所または「**オブジェクト | 一致オブジェクト > アドレス**」ページで使用できる任意の種別、アプリケーション、またはシグネチャでアプリケーション一致オブジェクトを作成して、それらの一致オブジェクトをアプリケーション ルール ポリシーで使用することもできます。これにより、アプリケーション ルールで設定できる動作やその他の多様な設定を使用できます。アプリケーション ルールに関するこうしたポリシーベースのユーザ インターフェースの詳細については、「*アプリケーション リスト オブジェクトについて*」を参照してください。

アプリケーション制御の状況の表示

「**アプリケーション制御状況**」の情報は、「**ポリシー | セキュリティサービス > アプリケーション制御**」ページの上部に表示されます。

アプリケーション シグネチャ データベース	アプリケーション シグネチャ データベースがダウンロード済みかどうかを示します。
アプリケーション シグネチャ データベース タイムスタンプ	アプリケーション シグネチャ データベースがダウンロードされた UTC 日時を表示します。 アプリケーション シグネチャ データベースを更新するには、「**更新**」をクリックします。
最終確認	SonicOS がアプリケーション 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を表示します。
アプリケーション シグネチャ データベースの失効日	アプリケーション シグネチャ データベースの有効期限が切れる日を表示します。

「**アプリケーション制御の状況**」セクションは、シグネチャ データベースに関する情報を表示し、データベースを更新できます。

ゾーンごとにアプリケーション制御を有効にするには、「**アプリケーション制御状況**」セクションの上の「補足」に示されている「**オブジェクト | 一致オブジェクト > ゾーン**」ページへのリンクをクリックします。

アプリケーション制御の有効化

アプリケーション制御を使用するには、グローバルに有効にする必要があります。また、アプリケーション トラフィックのあるネットワーク ゾーンで有効にする必要があります。

グローバルなアプリケーション制御の有効化

アプリケーション制御をグローバルに有効にするには、以下の手順に従います。

1. 「**ポリシー | セキュリティ サービス > アプリケーション制御 | アプリケーション制御のグローバル設定**」ページに移動します。
2. 「**アプリケーション制御を有効にする**」を選択します。
3. 「**送信**」をクリックします。

ゾーンごとのアプリケーション制御の有効化

アプリケーション制御をネットワーク ゾーンごとに有効にするには、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。「+ ゾーンの追加」または「構成」をクリックして、目的のゾーンを編集します。「ゾーン設定」ダイアログが表示されます。

2. 「**アプリケーション制御サービスを有効にする**」を選択します。
3. 「**保存**」をクリックします。

> **補足:** あるネットワーク ゾーン内のトラフィックにアプリケーション制御ポリシーが適用されるのは、そのゾーンで「**アプリケーション制御サービスを有効にする**」を選択している場合に限ります。アプリケーション ルール ポリシーは独立しており、ネットワーク ゾーンに対するアプリケーション制御の設定には影響されません。

「**オブジェクト | 一致オブジェクト > ゾーン**」ページでは、アプリケーション制御サービスが有効になっているすべてのゾーンの「**アプリケーション制御**」列に緑色のインジケータが表示されます。

ログとログ フィルタ間隔の設定

すべてのアプリケーションでログを有効にして、冗長フィルタ間隔を指定するには、以下の手順に従います。

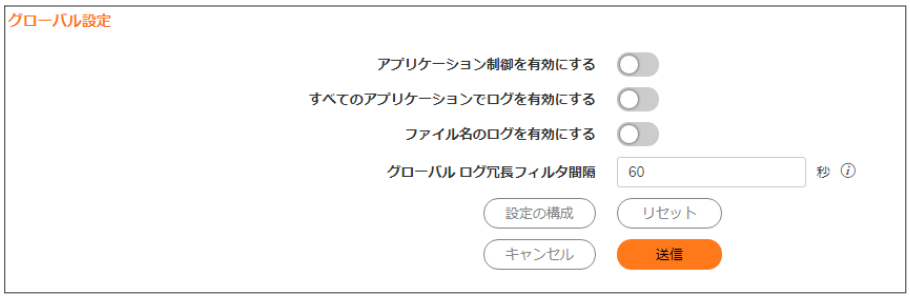
1. 「**ポリシー | セキュリティサービス > アプリケーション制御 | アプリケーション制御のグローバル設定**」ページに移動します。
2. 「**すべてのアプリケーションでログを有効にする**」を選択します。
3. 「**グローバル ログ冗長フィルタ間隔**」フィールドに、グローバル ログ冗長フィルタの間隔を秒数で入力します。範囲は 0～86400 秒で、既定値は **60** 秒です。
4. 「**送信**」をクリックします。

アプリケーション制御ファイル名のログの有効化

アプリケーション制御のプロセス、パケット、またはフローとして明示的に識別されたファイル名または対象URIごとの通知を許可するには、以下の手順に従います。

1. 「**ポリシー | セキュリティサービス > アプリケーション制御 | アプリケーション制御のグローバル設定**」ページに移動します。
2. 「**ファイル名のログを有効にする**」をクリックします。
3. 「**送信**」をクリックします。

アプリケーション制御のグローバル設定の構成



「**ポリシー | セキュリティサービス > アプリケーション制御 | アプリケーション制御のグローバル設定**」ページには、以下のグローバル設定が含まれています。

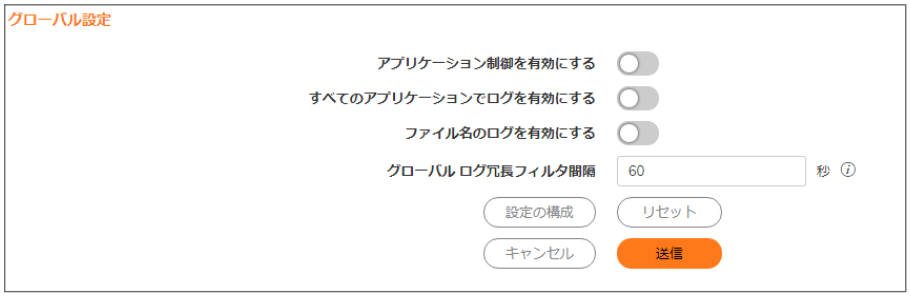
- アプリケーション制御を有効にする
- すべてのアプリケーションでログを有効にする
- ファイル名のログを有効にする
- グローバル ログ冗長フィルタ間隔

アプリケーション制御はライセンスされたサービスであり、この機能を使用するには該当するサービスも有効にする必要があります。アプリケーション制御およびアプリケーション ルール ポリシーのログおよび除外リストを設定したり、ポリシーを工場出荷時のデフォルトにリセットすることもできます。詳細については、「アプリケーション制御のグローバル設定について」を参照してください。

トピック:

- アプリケーション制御の有効化
- ログとログ フィルタ間隔の設定
- アプリケーション制御ファイル名のログの有効化

アプリケーション制御のグローバル設定について



「**ポリシー | セキュリティサービス > アプリケーション制御**」ページには、次のグローバル設定が含まれています。

- **アプリケーション制御を有効にする** – アプリケーション制御はライセンスされたサービスであり、この機能を有効にする必要があります。「**オブジェクト | 一致オブジェクト > ゾーン**」ページからゾーンごとに有効にする必要もあります。
- **すべてのアプリケーションでログを有効にする** – 有効にすると、アプリケーション制御とアプリケーション ルールのポリシーの一致と動作が記録されます。
- **ファイル名のログを有効にする** – 有効にすると、アプリケーション制御がパケットまたはフローを処理するとき明示的に識別した各ファイル名と対象の URI が管理者に通知されます。この通知にはログ メカニズムが利用され、次の方法でいくつかのメッセージ形式の出力を得ることができます。
  - 「**監視 | ログ > システム ログ**」ページの SonicOS イベント ログ。
  - 「**デバイス | ログ > Syslog**」ページの Syslog ビューア。

ⓘ | **補足:** ファイル名のログの詳細については、『*SonicOS ログ管理ガイド*』を参照してください。

- **グローバル ログ冗長フィルタ間隔** – 同じポリシーが複数回発生しても、繰り返しログに記録されない間隔を秒単位で指定します。範囲は 0～99999 秒で、既定値は **60** 秒です。

  グローバル ログ冗長設定は、すべてのアプリケーション制御のイベントに適用されます。ゼロに設定した場合、通過トラフィック内で検知されたポリシーの一致ごとに 1 つのログ エントリが作成されます。その他の値は、同じポリシーでの一致に対するログ エントリ間の最小秒数を指定します。例えば、ログ冗長設定として 10 を指定した場合、それぞれのポリシーの一致に対して 10 秒ごとに 1 つのメッセージが作成されます。ログの冗長性も設定できます。
  - 「**アプリケーション制御ポリシーの編集**」ダイアログで、ポリシーごとに設定します。
  - 「**アプリケーション制御種別の編集**」ダイアログで、種別ごとに設定します。
  - 「**アプリケーション制御アプリケーションの編集**」ダイアログで、アプリケーションごとに設定します。

  それぞれのポリシー設定に対して行われるポリシー単位のログ冗長フィルタ設定は、グローバル ログ冗長フィルタ設定よりも優先されます。

アプリケーション制御詳細設定の構成

トピック:

- アプリケーション制御詳細の種別ごとの設定
- アプリケーション制御詳細のアプリケーションごとの設定
- アプリケーション制御詳細のシグネチャごとの設定
- シグネチャの表示

アプリケーション制御詳細の種別ごとの設定

種別に基づく設定は、「**ポリシー | セキュリティサービス > アプリケーション制御 | シグネチャ**」ページで最も広範囲にわたるポリシー設定の方法です。種別のリストは、「シグネチャ種別」ドロップダウン メニューで使用できます。

アプリケーション制御ポリシーをアプリケーション種別に対して設定するには、以下の手順に従います。

1. 「**ポリシー | セキュリティサービス > アプリケーション制御 | シグネチャ**」ページに移動します。
2. 「**種別**」ドロップダウン メニューからアプリケーション種別を選択します。種別を選択すると、フィールドの右側にある「**構成**」アイコンが有効になります。
3. 「**構成**」をクリックすると、選択した種別の「**アプリケーション制御種別の設定**」ダイアログが表示されます。

4. この種別のアプリケーションを遮断するには、「**遮断**」ドロップダウン メニューで「**有効**」を選択します。
5. この種別のアプリケーションが検出されたときにログ エントリを作成するには、「**ログ**」ドロップダウン リストで「**有効**」を選択します。
6. 選択した遮断やログ記録の動作の対象を特定のユーザまたはユーザのグループに設定するには、「**包含するユーザ/グループ**」ドロップダウン メニューからユーザ グループまたは個々のユーザを選択します。「**すべて**」を選択すると、このポリシーがすべてのユーザに適用されます。
7. 選択した遮断やログ記録の動作の対象から特定のユーザまたはユーザのグループを除外するには、「**除外するユーザ/グループ**」ドロップダウン メニューからユーザ グループまたは個々のユーザを選択します。「**なし**」を選択すると、このポリシーがすべてのユーザに適用されます。
8. 選択した遮断やログ記録の動作の対象を特定の IP アドレスまたはアドレス範囲に設定するには、「**包含する IP アドレス範囲**」ドロップダウン メニューからアドレス グループまたはアドレス オブジェクトを選択します。「**すべて**」を選択すると、このポリシーがすべての IP アドレスに適用されます。
9. 選択した遮断やログ記録の動作の対象から特定の IP アドレスまたはアドレス範囲を除外するには、「**除外する IP アドレス範囲**」ドロップダウン メニューからアドレス グループまたはアドレス オブジェクトを選択します。「**なし**」を選択すると、このポリシーがすべての IP アドレスに適用されます。
10. このポリシーを特定の曜日や特定の時間だけ有効にするには、「**スケジュール**」ドロップダウン メニューから次のスケジュールのいずれかを選択します。

スケジュール オプション

スケジュール	ポリシーを有効にする期間
常に有効	常時。このオプションは、既定では選択されています。
勤務時間	月曜日から金曜日の午前 8:00 から午後 5:00 まで。
M-T-W-T-F 08:00 to 17:00	月曜日から金曜日の午前 8:00 から午後 5:00 まで（「**勤務時間**」と同じ）。
時間外	月曜日から金曜日の午後 5:00 から翌午前 8:00 まで。
M-T-W-T-F 00:00 to 08:00	月曜日から金曜日の深夜 0:00 から午前 8:00 まで。
M-T-W-T-F 17:00 to 24:00	月曜日から金曜日の午後 5:00 から深夜 0:00 まで。
SU-SA 00:00 to 24:00	日曜日から土曜日まで毎日 24 時間（「**常に有効**」と同じ）。
週末時間	金曜日の午後 5:00 から月曜日の午前 8:00 まで。
AppFlow 報告時間	AppFlow 報告が設定されている時間。
SU-M-T-W-TH-F-S 00:00 to 24:00	日曜日から土曜日まで毎日 24 時間（「**常に有効**」と同じ）。
TSR 報告時間	TSR 報告が設定されている時間。

11. 既定では、「**グローバル設定を使用する**」オプションが選択されており、既定値の **60** 秒を変更できません（フィールドは淡色表示になっています）。繰り返し発生するイベントのログ エントリ間隔を変更するには:
    a. 「**グローバル設定を使用する**」チェックボックスをオフにします。フィールドが使用可能になります。
    b. 「**ログ冗長フィルタ**」フィールドに間隔を秒数で入力します。最小秒数は 0（間隔なし）、最大秒数は 999999、既定値は **0** です。
12. 「**OK**」をクリックします。

アプリケーション制御詳細のアプリケーションごとの設定

アプリケーションに基づく設定は、「**ポリシー | セキュリティサービス > アプリケーション制御 | シグネチャ**」ページでの中間レベルのポリシー設定であり、種別に基づくレベルとシグネチャに基づくレベルの中間に位置付けられます。

この設定方法では、同じ種別内の他のアプリケーションに影響を及ぼすことなく単一のアプリケーションのシグネチャに対してのみポリシーを執行する場合に、そのアプリケーションに特定のポリシー ルールを作成できます。

アプリケーション制御ポリシーを特定のアプリケーションに対して設定するには、以下の手順に従います。

1. 「**ポリシー | セキュリティサービス > アプリケーション制御 | シグネチャ**」ページに移動します。
2. 「**アプリケーション**」ドロップダウン メニューからアプリケーションを選択します（種別を選択しなかった場合は、選択したアプリケーションの種別に変わります）。アプリケーションを選択すると、フィールドの右側に「**設定**」ボタンが表示されます。

3. 「**設定**」をクリックして、選択したアプリケーションの「**アプリケーション制御シグネチャの設定**」ダイアログを表示します。

ⓘ **ヒント:** アプリケーションの「**遮断**」設定が「**種別を選択してください**」に設定されている場合:
カテゴリ設定がアプリケーションの設定を上書きしないようにするには、必要に応じて「**遮断**」の設定を「**有効**」または「**無効**」に変更し、このダイアログで必要な値を選択します。

このダイアログの上部にあるフィールド「**アプリケーション種別**」および「**アプリケーション名**」は編集できません。他の設定パラメータには、アプリケーションが属する種別の現在の設定が既定で設定されます。種別の設定に対するこの関係を 1 つ以上のフィールドで維持するには、それらのフィールドでのこうした選択をそのままにしておきます。

4. このアプリケーションを遮断するには、「**遮断**」ドロップダウン メニューで「**有効**」を選択します。
5. このアプリケーションが検出されたときにログ エントリを作成するには、「**ログ**」ドロップダウン メニューで「**有効**」を選択します。
6. 選択した遮断やログ記録の動作の対象を特定のユーザまたはユーザのグループに設定するには、「**包含するユーザ/グループ**」ドロップダウン メニューからユーザ グループまたは個々のユーザを選択します。「**すべて**」を選択すると、このポリシーがすべてのユーザに適用されます。
7. 選択した遮断やログ記録の動作の対象から特定のユーザまたはユーザのグループを除外するには、「**除外するユーザ/グループ**」ドロップダウン メニューからユーザ グループまたはユーザを選択します。「**なし**」を選択すると、このポリシーがすべてのユーザに適用されます。
8. 選択した遮断やログ記録の動作の対象を特定の IP アドレスまたはアドレス範囲に設定するには、「**包含する IP アドレス範囲**」ドロップダウン メニューから「**アドレス グループ**」または「**アドレス オブジェクト**」を選択します。「**すべて**」を選択すると、このポリシーがすべての IP アドレスに適用されます。
9. 選択した遮断やログ記録の動作の対象から特定の IP アドレスまたはアドレス範囲を除外するには、「**除外する IP アドレス範囲**」ドロップダウン メニューから「**アドレス グループ**」または「**アドレス オブジェクト**」を選択します。「**なし**」を選択すると、このポリシーがすべての IP アドレスに適用されます。
10. このポリシーを特定の曜日や特定の時間だけ有効にするには、「**スケジュール**」ドロップダウン メニューからスケジュールのいずれかを選択します。スケジュールのリストについては、「**スケジュール オプション**」を参照してください。アプリケーション制御詳細の種別ごとの設定.
11. 既定では、「**ログ冗長フィルタ**」の「**種別設定を使用する**」オプションが選択されています。このフィールドは淡色表示になっていて変更できません。繰り返し発生するイベントのログ エントリ間隔を変更するには:
    a. 「**グローバル設定を使用する**」チェックボックスを無効にします。フィールドが使用可能になります。
    b. 「**ログ冗長フィルタ**」フィールドに間隔を秒数で入力します。最小秒数は 0 (間隔なし)、最大秒数は 999999、既定値は 0 です。

12. 「**OK**」をクリックします。

アプリケーション制御詳細のシグネチャごとの設定

シグネチャに基づく設定は、「**ポリシー | セキュリティサービス > アプリケーション制御 | シグネチャ**」ページで最も具体的なレベルのポリシー設定です。

特定のシグネチャに基づくポリシーを設定すると、同じアプリケーションの他のシグネチャに影響を及ぼすことなく個々のシグネチャに対してポリシーを設定できます。

アプリケーション制御ポリシーを特定のシグネチャに対して設定するには、以下の手順に従います。

1. 「**ポリシー | セキュリティサービス > アプリケーション制御 | シグネチャ**」ページに移動します。
2. 「**シグネチャ**」ドロップダウン メニューで シグネチャ を選択します。

   ⓘ **ヒント:** 必要に応じて、「**種別**」ドロップダウン メニューまたは「**アプリケーション**」ドロップダウン メニューからカテゴリを選択して、表示されるシグネチャの数を減らします。

   ⓘ **ヒント:** シグネチャのシグネチャ ID がわかっている場合は、ツールバーの「**シグネチャ ID の検索**」アイコンをクリックし、シグネチャ ID を入力します。
3. 設定するシグネチャの行にある「**設定**」をクリックします。「**アプリケーション制御シグネチャの設定**」ダイアログが表示されます。

ⓘ **ヒント:** シグネチャの「**遮断**」設定が「**アプリケーション設定を使用する**」に設定されている場合: アプリケーション設定がシグネチャの設定を上書きしないようにするには、必要に応じて「**遮断**」の設定を「**有効**」または「**無効**」に変更し、このダイアログで必要な値を選択します。

このダイアログの上部にあるフィールドは編集できません。これらのフィールドには、「**シグネチャ種別**」、「**シグネチャ名**」、「**シグネチャ ID**」、「**アプリケーション ID**」、「**優先順位**」、このシグネチャが属する種別およびアプリケーションのトラフィックの「**方向**」の値が表示されます。

ⓘ **ヒント:** アプリケーション情報を編集するには、「**アプリケーション ID**」フィールドの横にある**編集**アイコンを選択します。「**アプリケーション制御アプリケーションの設定**」ダイアログが表示されます。このダイアログの設定については、「アプリケーション制御のアプリケーションごとの設定」を参照してください。

シグネチャに対する他の設定には、シグネチャが属するアプリケーションの現在の設定が使用されます。アプリケーションの設定に対するこの関係を 1 つ以上のフィールドで維持するには、それらのフィールドでのこうした選択をそのままにしておきます。

4. このシグネチャを遮断するには、「**遮断**」ドロップダウン メニューで「**有効**」を選択します。
5. このシグネチャが検出されたときにログ エントリを作成するには、「**ログ**」ドロップダウン メニューで「**有効**」を選択します。
6. 選択した遮断やログ記録の動作の対象を特定のユーザまたはユーザのグループに設定するには、「**包含するユーザ/グループ**」ドロップダウン メニューからユーザ グループまたは個々のユーザを選択します。「**すべて**」を選択すると、このポリシーがすべてのユーザに適用されます。
7. 選択した遮断やログ記録の動作の対象から特定のユーザまたはユーザのグループを除外するには、「**除外するユーザ/グループ**」ドロップダウン メニューからユーザ グループまたは個々のユーザを選択します。

「**なし**」を選択すると、このポリシーがすべてのユーザに適用されます。

8. 選択した遮断やログ記録の動作の対象を特定の IP アドレスまたはアドレス範囲に設定するには、「**包含する IP アドレス範囲**」ドロップダウン メニューから「**アドレス グループ**」または「**アドレス オブジェクト**」を選択します。「**すべて**」を選択すると、このポリシーがすべての IP アドレスに適用されます。
9. 選択した遮断やログ記録の動作の対象から特定の IP アドレスまたはアドレス範囲を除外するには、「**除外する IP アドレス範囲**」ドロップダウン メニューから「**アドレス グループ**」または「**アドレス オブジェクト**」を選択します。「**なし**」を選択すると、このポリシーがすべての IP アドレスに適用されます。
10. このポリシーを特定の曜日や特定の時間だけ有効にするには、「**スケジュール**」ドロップダウン メニューからスケジュールのいずれかを選択します。スケジュールのリストについては、「**スケジュール オプション**」を参照してください。アプリケーション制御詳細の種別ごとの設定.
11. 既定では、「**ログ冗長フィルタ**」の「**種別設定を使用する**」オプションが選択されています。このフィールドは淡色表示になっていて変更できません。繰り返し発生するイベントのログ エントリ間隔を変更するには:
    a. 「**グローバル設定を使用する**」チェックボックスをオフにします。フィールドが使用可能になります。
    b. 「**ログ冗長フィルタ**」フィールドに間隔を秒数で入力します。最小秒数は **0**（間隔なし）、最大秒数は **999999**、既定値は **0** です。
12. シグネチャに関する詳細な情報を確認するには、シグネチャページにあるシグネチャ名をクリックします。
13. 「OK」をクリックします。

シグネチャの表示

「**ポリシー | セキュリティサービス > アプリケーション制御 | シグネチャ**」の表示は、さまざまな「**表示方法**」オプション（「**シグネチャ**」、「**アプリケーション**」、「**種別**」など）によって変更できます。

表示形式	オプション	表示対象
種別	**すべて**（既定）	すべての種別とそのシグネチャ アプリケーション
	個々の種別	指定した種別のシグネチャ アプリケーション
アプリケーション	**すべて**（既定）	指定した種別に関連付けられているすべてのシグネチャ アプリケーション
表示方法	**シグネチャ**	指定した種別に関連付けられているすべてのシグネチャ アプリケーションとアプリケーションに関連付けられているシグネチャ
	アプリケーション（既定）	指定した種別に関連付けられているすべてのシグネチャ アプリケーション

表示形式	オプション	表示対象
	種別	「種別」表示形式で指定した種別

「**シグネチャ ID の検索**」アイコンをクリックした後、「**シグネチャ ID の検索**」フィールドに ID を入力して、特定のシグネチャの「**アプリケーション制御シグネチャの設定**」ダイアログを表示することもできます。

「**アプリケーション名**」または「**シグネチャ名**」の青色のエントリをクリックすると、「**アプリケーション シグネチャ詳細**」ダイアログが表示されます。

トピック:

- すべての種別とすべてのアプリケーションをアプリケーションごとに表示
- すべての種別とすべてのアプリケーションをシグネチャごとに表示
- すべての種別とすべてのアプリケーションを種別ごとに表示
- 1 つの種別のみ表示
- 1 つのアプリケーションのみ表示
- シグネチャ アプリケーションの詳細の表示
- アプリケーション シグネチャの詳細の表示

すべての種別とすべてのアプリケーションをアプリケーションごとに表示

「**アプリケーション制御詳細**」テーブルに表示される列の説明については、「すべての種別とすべてのアプリケーションをシグネチャごとに表示」を参照してください。

すべての種 別 とすべてのアプリケーションをシグネチャごとに表 示

#	種別	アプリケーション	シグネチャ名	ID	リスク	方向	その他の情報
1	IM	Skype	Login over TCP	1	脅威	送信, サーバ	
2	P2P	Winny	Login	3	中	両方	
3	P2P	eMule	Obfuscated Protocol	4	中	送信, サーバ	
4	PROXY-ACCESS	Encrypted Key Exchange	TCP Random Encryption(Skype,UltraSurf,E	5	中	両方	
5	PROXY-ACCESS	Non-SSL traffic over SSL port	Traffic Anomaly Detection	6	中	送信, サーバ	
6	PROXY-ACCESS	Encrypted Key Exchange	UDP Random Encryption(UltraSurf)	7	中	受信, 両方	
7	MULTIMEDIA	Flash Video (FLV)	Download 1	58	中	受信, クライアント	
8	MULTIMEDIA	Flash Video (FLV)	Download 2	59	中	受信, クライアント	
9	P2P	BitTorrent Protocol	UDP Activity 1 [Reqs SID 5]	63	脅威	両方	
10	P2P	BitTorrent Protocol	UDP Activity 3 [Reqs SID 5]	66	脅威	両方	
11	WEB-CONFERENCING	Tlen	Chat Server HTTPS Response	69	中	受信, クライアント	
12	WEB-CONFERENCING	Tlen	Chat Server HTTP Reponse	70	中	受信, クライアント	

種別	選択したシグネチャ種別またはすべてのシグネチャ種別の名前 すべてのシグネチャ アプリケーションは、同じ種別見出し（「APP-UPDATE」など）でグループ化されます。
アプリケーション	種別内の各シグネチャ アプリケーションの名前。
名前	シグネチャ名。
ID	シグネチャ ID。
遮断	種別またはアプリケーションが遮断されているかどうかを示します。遮断が有効な場合、この列には**有効アイコン**が表示されます。種別の行には「**既定**」という語が表示される場合があります。
ログ	種別またはアプリケーションがログ記録されているかどうかを示します。ログ記録が有効な場合、この列には**有効アイコン**が表示されます。
方向	トラフィックの方向: **受信** / **送信** / **両方** **受信、クライアント** / **送信、クライアント** / **双方向、クライアント** **受信、サーバ** / **送信、サーバ** / **双方向、サーバ** **受信、クライアント、サーバ** / **送信、クライアント、サーバ** / **双方向、クライアント、サーバ**
コメント	種別またはシグネチャ アプリケーションに以下を設定していない場合、この列は空白になります。 • **ユーザ**アイコン – ユーザ/グループの包含/除外設定。 • **情報**アイコン – IP アドレスの包含/除外設定。 • **時計**アイコン –「**常に有効**」以外のスケジュール。
構成	シグネチャ アプリケーションの設定を変更するためのダイアログを表示する**編集**アイコン。

すべての種別とすべてのアプリケーションを種別ごとに表示

「**アプリケーション制御詳細**」テーブルに表示される列の説明については、「すべての種別とすべてのアプリケーションをシグネチャごとに表示」を参照してください。

1 つの種別のみ表示

#	種別	アプリケーション	シグネチャ名	ID	リスク	方向	その他の情報
1	GAMING	QuakeLive	Browsing Activity 1	628	低	送信, サーバ	
2	GAMING	Blizzard Entertainment	DNS Query battle.net	858	低	送信, 両方	
3	GAMING	QQGame	DNS Query qqgame.store.qq.com	874	警戒	送信, 両方	
4	GAMING	PokerStars	HTTPS Activity	893	低	受信, クライアント	
5	GAMING	PokerStars	HTTP Activity	894	低	送信, サーバ	
6	GAMING	EuroPoker	SSL Traffic	899	警戒	受信, クライアント	
7	GAMING	Zynga Texas Holdem	Client Activity 1	902	低	送信, サーバ	
8	GAMING	QQGame	HTTP Activity 1	906	低	送信, サーバ	
9	GAMING	Yahoo! Games	Browsing Activity	990	低	送信, サーバ	
10	GAMING	Second Life	SSL Connections	1166	低	受信, クライアント	
11	GAMING	Ragnarok Online	Browsing Activity	1655	低	送信, サーバ	
12	GAMING	Barafranca (Omerta)	Browsing Activity 1	1933	低	送信, サーバ	

「**シグネチャ**」テーブルの表示を 1 つの種別のシグネチャ アプリケーションのみに限定するには、以下のいずれかを実行します。

- 「**種別**」ドロップダウン メニューで、「**GAMING**」(上の図の場合) などの種別を選択します。

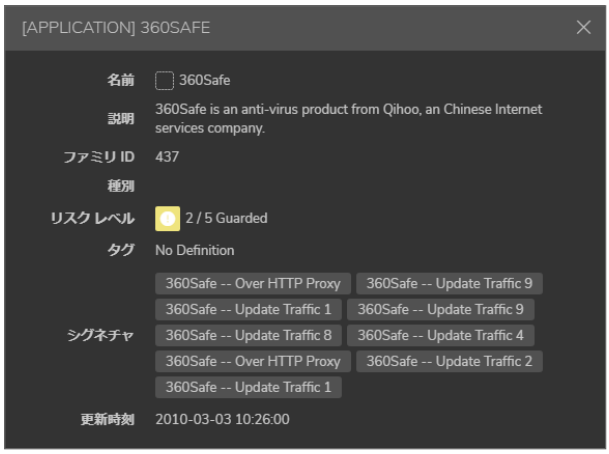
1 つのアプリケーションのみ表示

「**シグネチャ**」テーブルの表示を 1 つのアプリケーションのシグネチャのみに限定するには、「**アプリケーション**」ドロップダウン メニューからアプリケーションを選択します。「**シグネチャ**」テーブルに表示される列の説明については、「すべての種別とすべてのアプリケーションをシグネチャごとに表示」を参照してください。

#	種別	アプリケーション	シグネチャ名	ID	リスク	方向	その他の情報
1	APP-UPDATE	360Safe	Update Traffic 1	1197	低	送信, サーバ	
2	APP-UPDATE	360Safe	Update Traffic 2	1199	低	送信, 両方	
3	APP-UPDATE	360Safe	Update Traffic 4	1201	警戒	両方	
4	APP-UPDATE	360Safe	Over HTTP Proxy	5600	警戒	送信, サーバ	
5	APP-UPDATE	360Safe	Update Traffic 8	6539	警戒	受信, クライアント	
6	APP-UPDATE	360Safe	Update Traffic 9	6540	警戒	送信, サーバ	

シグネチャ アプリケーションの詳 細 の表 示

シグネチャ アプリケーションの詳細を表示するには、シグネチャ アプリケーションの名前（青色）をクリックします。「アプリケーションの詳細」ポップアップ ダイアログが表示されます。



ファミリ ID	ファミリ ID。
種別	シグネチャ アプリケーションの種別（APP-UPDATE、P2P、GAMING など）。
リスク	各シグネチャのリスクのレベル: • **低** • **警戒** • **中** • **高** • **深刻**

シグネチャ ID（Sig ID）をクリックすると、そのシグネチャの「SonicALERT」ページが表示されます。

アプリケーション シグネチャの詳細の表示

シグネチャ アプリケーションの詳細を表示するには、青色の「**シグネチャ名**」をクリックします。「**アプリケーション シグネチャ詳細**」ポップアップ ダイアログが表示されます。

種別	シグネチャ アプリケーションの種別（「**APP-UPDATE**」、「**GAMING**」など）。
アプリケーション	シグネチャ アプリケーションの名前。
リスク レベル	リスク レベル: • **低** • **中** • **高**
脅威度	シグネチャの脅威度: • **低** • **警戒** • **中** • **高** • **深刻**

9

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。
- 次のサイトにアクセスする https://mysonicwall.com。
- 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 セキュリティ サービス 管理ガイド
更新日 – 2021 年 1 月
ソフトウェア バージョン – 7
232-005448-10 Rev B

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