SonicOS および SonicOSX 7 キャプチャ ATP

管理ガイド

SONICWALL®

目次

キャプチャ ATP **3**
キャプチャ ATP について 3
ファイルの前処理 4
分析が完了するまでファイルを遮断 4
暗号化接続を使ったファイル送信 4
キャプチャ ATP のフレンドリファイル名表示 4
キャプチャ ATP ライセンスの有効化 5
キャプチャ ATP の有効化 5
「キャプチャ ATP」ページについて 6
基本セットアップ確認リスト 6
帯域幅管理 8
除外 8
ユーザ定義の遮断動作 9
キャプチャ ATPの設定 11
GAV または クラウド ゲートウェイ アンチウイルス の無効化 12

スキャン履歴 **14**
サンプルの送信 14
分析結果の表示 15

SonicWall サポート **17**
このドキュメントについて 18

1

キャプチャ ATP

ⓘ **補足:** SonicOS/X という表記は、その機能が両方の SonicOS および SonicOSX で使用可能なことを示します。

ⓘ **重要:** キャプチャ高度脅威防御（ATP）はゲートウェイ アンチウイルス（GAV）と同様に、ファイアウォールに対するアドオン セキュリティ サービスであり、ファイアウォールで有害ファイルを識別するために使用します。キャプチャ ATP を有効にするには、最初にライセンスを取得し、さらにゲートウェイ アンチウイルス（GAV）と クラウド ゲートウェイ アンチウイルス データベース サービスを有効にする必要があります。キャプチャ ATP のライセンスを取得すると、MySonicWall アカウントでキャプチャ ATP の状況を確認でき、警告と通知を設定して受け取ることができるようになります。

トピック:

- キャプチャ ATP について
- キャプチャ ATP の有効化
- 「キャプチャ ATP」ページについて
- キャプチャ ATP の設定
- GAV またはクラウド アンチウイルスの無効化

キャプチャ ATP について

キャプチャ高度脅威防御（ATP）を追加すると、ファイアウォールは、あるファイルが悪質なものかを識別するため、そのファイルをクラウドに転送できます。クラウドではSonicWall キャプチャ ATP サービスがファイルを分析して、ウイルスなどの有害な要素が含まれるかどうかを確認します。その後、キャプチャ ATP は、結果をファイアウォールに送信します。分析と報告は、ファイルがファイアウォールによって処理されている間にリアルタイムで実行されます。

すべてのファイルは、暗号化された接続を介してキャプチャ ATP クラウドに送信されます。ファイルの分析は数分で完了し、有害であると判定された場合を除き、削除されます。有害ファイルは、暗号化された HTTPS 接続経由で SonicWall Threats Research チームに送信され、詳細に分析されたのち、脅威に関する情報の充実に活用されます。ファイルは、分析以外の用途でそれ以外の場所に転送されることはありません。有害ファイルは、脅威に関する情報に活用した後、受信から 30 日以内に削除されます。

キャプチャ ATP は、ファイル分析報告（脅威報告）を作成して、脅威となる動作に関する詳細な情報を提供します。

ファイアウォールは顧客が保有する施設内にありますが、キャプチャ ATP のサーバとデータベースは SonicWall の施設内にあります。ファイアウォールは、キャプチャ ATP クラウドとの間にセキュアな接続を作成してから、データの転送を開始します。

キャプチャ ATP は、ゲートウェイ アンチウイルス (GAV) および クラウド ゲートウェイ アンチウイルス サービスと連携して動作します。キャプチャ ATP は、GAV によって解析された電子メール ヘッダー情報 (to、cc、bcc) もログ/表示します。

トピック:

- ファイルの前処理
- 分析が完了するまでファイルを遮断
- 暗号化接続を使ったファイル送信
- キャプチャ ATP による分かりやすいファイル名表示
- キャプチャ ATP ライセンスの有効化

ファイルの前処理

キャプチャ ATP に分析のため送信されるすべてのファイルは、最初に GAV で前処理され、有害または無害と判定されます。GAV の設定を使って、GAV とキャプチャ ATP によるスキャンから除外するアドレス オブジェクトを選択または定義することもできます。

前処理で有害または無害と判定されたファイルは、キャプチャ ATP で分析されません。前処理段階でファイルが有害か無害か判定されなかった場合、ファイルは分析のためキャプチャ ATP に送信されます。

分析が完了するまでファイルを遮断

HTTP/HTTPS ダウンロードについては、「判定が返ってくるまでファイルのダウンロードを遮断する」というオプションがあります。これは、キャプチャ ATP がファイルを完全に分析し、有害または無害と判定するまで、いっさいのパケットを通過させないというものです。ファイルは、最後のパケットが分析されるまで保留となります。ファイルにマルウェアが含まれる場合、最後のパケットが破棄され、ファイルはブロックされます。脅威報告には、脅威や感染に対処するために必要な情報が記載されています。

暗号化接続を使ったファイル送信

すべてのファイルは、暗号化接続を使用してキャプチャ ATP クラウドに送信されます。SonicWall はこれらのファイルを保存しません。すべてのファイル タイプは、有害、無害の区別なく、一定の期間が過ぎればキャプチャ ATP サーバから削除されます。

SonicWall プライバシー ポリシーは、https://www.mysonicwall.com/muir/privacy で参照できます。

キャプチャ ATP のフレンドリファイル名表示

次の非 HTTP プロトコルに対し、SonicWall Capture Advanced Threat Protection が、スキャン済みファイルをフレンドリファイル名でログに記録します。

• SMTP	• POP3	• FTP
• IMAP	• NetBIOS	

この機能を使用すると、キャプチャ ATP によってスキャンされているファイルとその状況（「**ポリシー > キャプチャ ATP > スキャン履歴**」テーブルやログ メッセージにおいて、これらのプロトコル種別のファイル名について表示される）を簡単に識別できます。フレンドリファイル名には、最大 256 文字を使用できます。

次の要素は解析できません:

- TCP プロトコル ストリームのファイル名情報。
- 単一のネットワーク パケットに含まれていないファイル名。

SonicOS/X の設定は不要です。

キャプチャ ATP ライセンスの有効化

ⓘ **重要:** キャプチャ ATP の実行には ゲートウェイ アンチウイルス サービスが必要です。このサービスもライセンスが有効になっている必要があります。

キャプチャ ATP サービス ライセンスを有効化すると、SonicOS/X の左側にあるナビゲーション パネル（左側のナビゲーション パネル）の「**クライアント強制**」の下に「**キャプチャ ATP**」が表示されます。
補足: キャプチャ ATP サービス ライセンスを有効化してから間もなく キャプチャ ATP が表示されない場合は、「**デバイス | 設定 > ライセンス**」ページの「**同期**」ボタンをクリックしてください。

ライセンスを有効化するには、すべてのサービス ライセンスを表示できる「**デバイス | 設定 > ライセンス**」ページに移動し、キャプチャ ATP のライセンスを開始します。

キャプチャ ATP の有効化

ⓘ **重要:** キャプチャ ATP を有効化する前にゲートウェイ アンチウイルスとクラウド ゲートウェイ アンチウイルスを有効にしてください。

キャプチャ ATP のライセンスは取得済みでもまだサービスを有効化していない場合は、次のメッセージが表示されます。

> キャプチャ ATP は現在動作していません。トラブルシュートは以下の「基本セットアップ確認リスト」をご覧下さい。

無効モードでは「**基本セットアップ確認リスト**」セクションは表示されますが、他のセクションはグレー表示になります。

キャプチャ ATP を有効にするには、以下の手順に従います。

1. 「**ポリシー | キャプチャ ATP > 設定**」に移動します。
2. ゲートウェイ アンチウイルス（GAV）と クラウド ゲートウェイ アンチウイルス を有効にします。
3. また、GAVとクラウド ゲートウェイ アンチウイルスを設定することもできます。この設定はキャプチャ ATP にも適用されます。
4. 「**ポリシー | キャプチャ ATP > 設定**」に移動します。キャプチャ ATP が有効になっていないと、次の警告メッセージが表示されます。

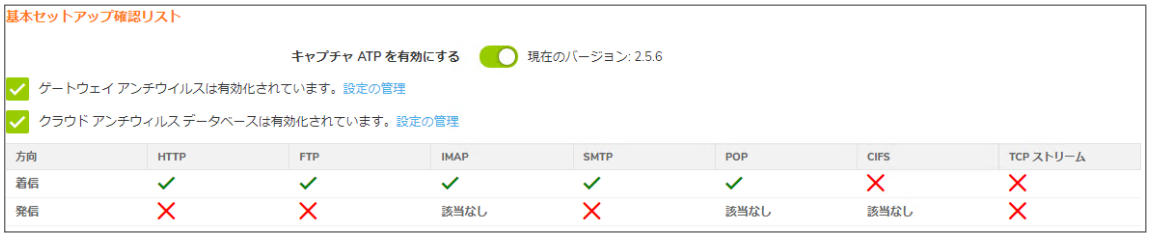
5. 「基本セットアップ確認リスト」セクションの「キャプチャ ATP 購読は <日付> まで有効です。ただしサービスは現在有効化されていません。(有効にする)」で「(有効にする)」をクリックします。警告メッセージが消え、ステータス インジケータが緑色のチェックマークに変わります。

「キャプチャ ATP」ページについて

トピック:

- 基本セットアップ確認リスト
- 帯域幅管理
- 除外
- ユーザ定義の遮断動作

基本セットアップ確認リスト



基本セットアップ確認リスト:

- キャプチャ ATPおよび関連コンポーネント、ゲートウェイ アンチウイルスおよびクラウド ゲートウェイ アンチウイルスの状況を表示します。
- エラーが発生していれば、その状態が表示されます。
- キャプチャ ATP サービスを有効または無効に設定できます。
- GAV、クラウド ゲートウェイ アンチウイルス、およびプロトコル検査を設定できる「**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**」ページへのリンクがあります。
- プロトコル検査の設定と、受信方向と送信方向のどちらが有効化されているかが表形式で表示されます。

ⓘ **補足:** このセクションで表示されるメッセージについては、「キャプチャ ATP 状況」から「プロトコル検査設定」までの表を参照してください。緑色のチェックマークは**有効**を意味し、赤い X マークは**無効**を意味します。

キャプチャ ATP 状況

アイコン	メッセージ	リンク	動作
有効	キャプチャ ATP サービスは、更新日 まで有効です。	無効にする	このリンクをクリックするとキャプチャ ATP がオフに切り替わり、サービスが無効モードになります。この変更を適用するために「**適用**」をクリックする必要はありません。
無効	キャプチャ ATP の購読は 更新日 まで有効ですが、サービスは現在有効ではありません。	有効にする	このリンクをクリックすると、キャプチャ ATP がオンに切り替わり、サービスが有効モードになります。この変更を適用するために「**適用**」をクリックする必要はありません。
無効	キャプチャ ATP の購読は、更新日 に期限切れで終了しました。	更新する	このリンクをクリックすると、MySonicWall に移動してサービスを更新できます。

ゲートウェイ アンチウイルス 状況

アイコン	メッセージ	リンク	動作
有効	ゲートウェイ アンチウイルス は有効です。	設定の管理	このリンクを選択すると、「**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**」ページが表示されます。
無効	キャプチャ ATP が機能するにはゲートウェイ アンチウイルスを有効にしなければなりません。	設定の管理	このリンクを選択すると、「**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**」ページが表示されます。

クラウド ゲートウェイ アンチウイルス データベースの状況

アイコン	メッセージ	リンク	動作
有効	クラウド ゲートウェイ アンチウイルス データベースは有効です。	設定の管理	このリンクを選択すると、「**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**」ページが表示されます。
無効	キャプチャ ATP が機能するにはクラウド ゲートウェイ アンチウイルス データベースを有効にしなければなりません。	設定の管理	このリンクを選択すると、「**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**」ページが表示されます。

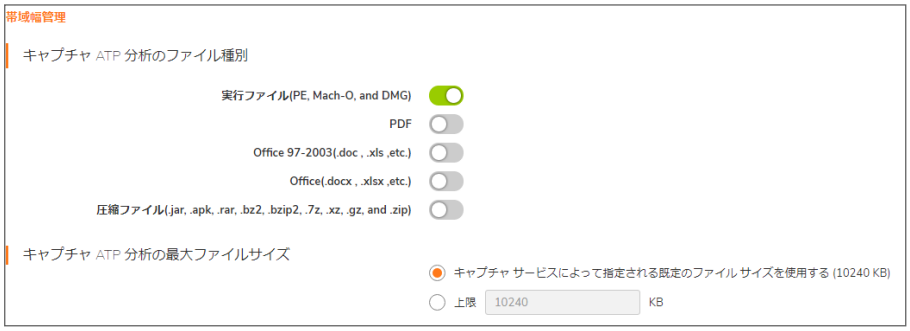
「**検査されるプロトコル**」の表には、「**ポリシー | セキュリティ サービス > ゲートウェイ アンチウイルス**」ページに移動できる「設定の管理」リンクも提供されています。ここでは、HTTP、FTP、IMAP、SMTP、POP、CIFS、TCP ストリームなどのネットワーク トラフィック プロトコルを指定して、検査を有効または無効に設定できます。各プロトコルは、受信トラフィックまたは送信トラフィックを区別して管理できます。

「**検査されるプロトコル**」の下の表には、各プロトコルの現在の検査設定が方向別に示されます（以下を参照）。「プロトコル検査設定」.

プロトコル検査設定

アイコン	メッセージ
有効	プロトコルは検査されます。
無効	プロトコルは検査されません。
該当なし	検査がこのプロトコルのこの方向には適用が不可能であることを意味します。

帯域幅管理



「**帯域幅管理**」セクションでは、キャプチャ ATP に送信できるファイルのタイプを選択し、送信できるファイルの最大サイズを指定することができます。また、検査から除外するアドレス オブジェクトも指定できます。

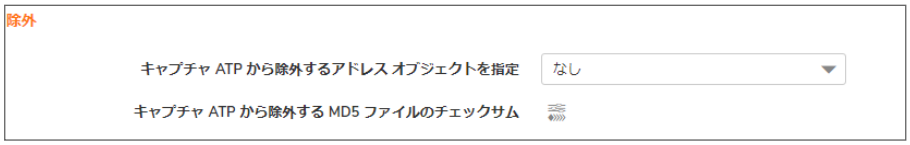
既定では、「**実行ファイル (PE、Mach-O、および DMG)**」ファイル タイプのみが有効です。

最大ファイル サイズの既定のオプションは、「**キャプチャ サービスによって指定される既定のファイル サイズを使用する (10240 KB)**」です。このオプションを選択すると、ファイル サイズは 10 MB に制限されます。

「**キロバイトに制限する**」を選択すると、個別の値を入力できます。この値は、0 ではなく、なおかつ既定の制限値より大きくない数値でなければなりません。

除外

「**除外**」セクションでは、キャプチャ ATP からアドレス オブジェクトや MD5 ハッシュ関数を除外することができます。



「**キャプチャ ATP から除外するアドレス オブジェクトを指定**」を使用する場合は、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たり、新しいアドレス オブジェクトを作成することもできます。選択したアドレス オブジェクトのメンバーは、キャプチャ ATP サービスによる検査から除外されます。

アドレス オブジェクトを除外するには

1. アドレス オブジェクトをドロップダウン メニューから選択するか、新しく作成します。
2. 「**適用**」をクリックします。

MD5 ファイルを除外するには

1. 「**MD5 除外リストの設定**」をクリックします。「**MD5 除外の設定**」ダイアログが表示されます。

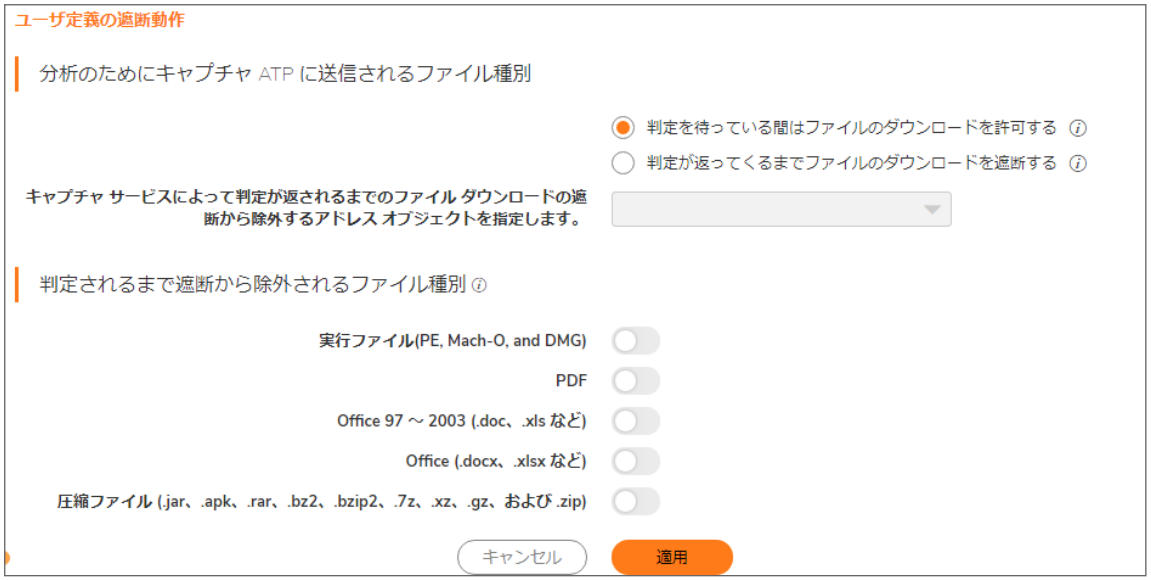
2. 除外する 16 進数 32 桁のハッシュ関数を追加します。
3. 「**保存**」をクリックします。

さらにファイルを追加するには、

1. ハッシュ関数ごとにステップ 2 と 3 を繰り返します。
2. 「**保存**」をクリックします。
3. 「**適用**」をクリックします。

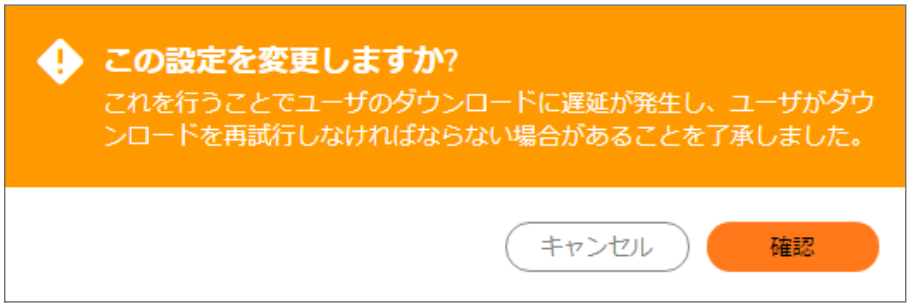
ユーザ定義の遮断動作

「**ユーザ定義の遮断動作**」セクションでは、「**判定が返ってくるまでファイルのダウンロードを遮断する**」機能を選択できます。



既定のオプションは、「**判定を待っている間はファイルのダウンロードを許可する**」です。この設定を使うと、キャプチャ サービスがファイルの有害要素を分析している間も、ファイルのダウンロードは遅延なく許可されます。キャプチャ サービスの分析でファイルが有害と判定されたかどうかは、電子メールのアラートで通知するように設定したり、ファイアウォールのログをチェックして確認することができます。

「**判定が返ってくるまでファイルのダウンロードを遮断する**」機能は、厳格な制御が望ましい状況でのみ使用してください。この機能をオンにすると、警告のダイアログが表示されます。



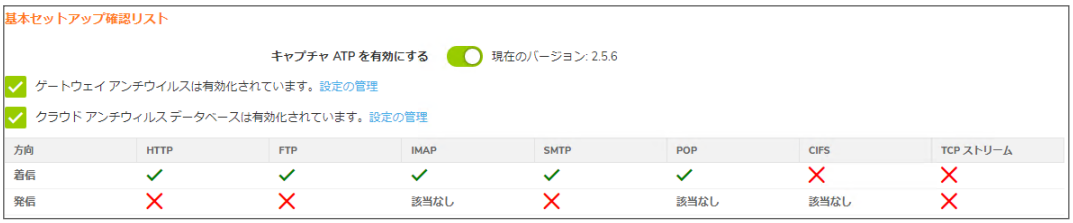
「**判定が返ってくるまでファイルのダウンロードを遮断する**」機能が有効になると、他のオプションが使用可能になります。次の選択が可能です。

- 「**キャプチャ サービスから判定が返ってくるまでファイルのダウンロードが遮断されないよう除外するアドレス オブジェクトを選択する**」から、アドレス オブジェクトを選択します。既定は「**なし**」です。
- 「**キャプチャ サービスから判定が返ってくるまでファイルのダウンロードが遮断されないよう除外するファイル種別を指定する**」から ファイル種別を選択します。
    - **実行ファイル (PE、Mach-O、および DMG)**
    - **PDF**
    - **Office 97-2003 (.doc、.xls など)**
    - **Office (.docx、.xlsx など)**
    - **圧縮ファイル (.jar、.apk、.rar、.gz、および .zip)**

キャプチャ ATPの設 定

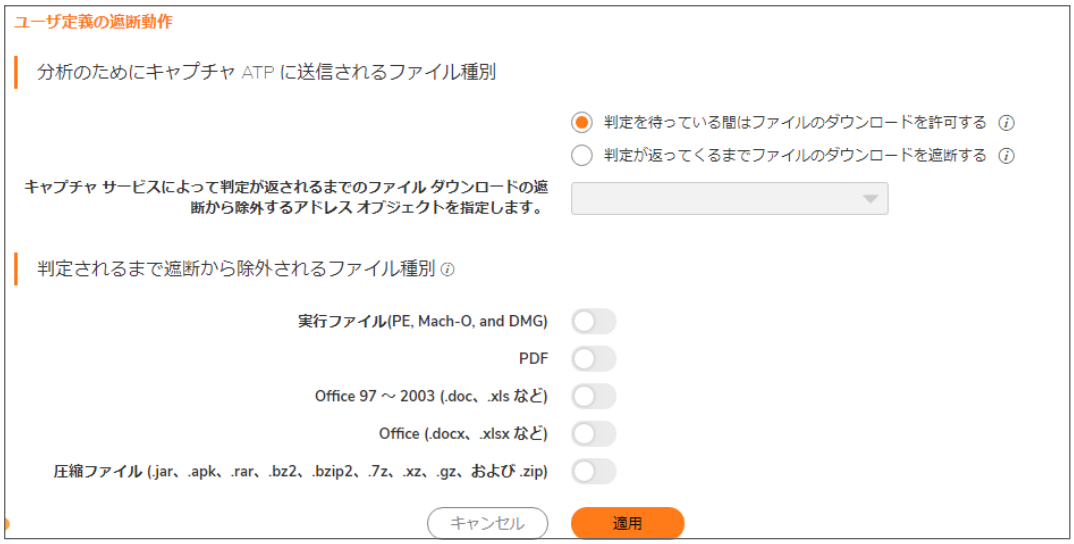
キャプチャ ATP のオプションを設定するには、以下の手順に従います。

1. 「**ポリシー | キャプチャ ATP > 設定**」に移動します。



2. キャプチャ ATP、GAV、クラウド ゲートウェイ アンチウイルス データベース、関連するプロトコルが有効化されていることを確認します。
3. 「**帯域幅管理**」セクションでキャプチャ ATP の分析対象とするファイル タイプを選択します。既定では、「**実行ファイル (PE、Mach-O、および DMG)**」のみが有効です。

4. 既定では、「**キャプチャ サービスによって指定される既定のファイル サイズを使用する (10240 KB)**」が選択されています。このサイズを変更するには、「**KB に制限する**」フィールドに 1 から 10240 までの値を入力します。
5. 必要に応じて、「**キャプチャ ATP から除外するアドレス オブジェクトを指定**」ドロップダウン メニューからアドレス オブジェクトを選択してキャプチャ ATP からアドレス オブジェクトを除外することもできます。
6. 必要に応じて、「**MD5 除外リスト設定**」をクリックして「**MD5 除外設定**」ダイアログを表示し、MD5 チェックサムに基づいてファイルを除外することもできます。
    a. 「**MD5 除外リスト**」フィールドに 16 進数 32 桁のハッシュを追加します。
    b. 「**保存**」をクリックします。
    c. 除外するファイルごとにステップ a とステップ b を繰り返します。
    d. 「**保存**」をクリックします。
7. HTTP/HTTPS ファイルを分析する場合は、「**ユーザ定義の遮断動作**」セクションで、分析が完了するまですべてのファイルを遮断するかどうかを指定できます。



既定では、「**判定を待っている間はファイルのダウンロードを許可する**」が選択されます。

ⓘ **重要:**「**判定が返ってくるまでファイルのダウンロードを遮断する**」機能は、厳格な制御が望ましい状況でのみ使用してください。

この機能をオンにすると、警告のダイアログが表示されます。

次のオプションがあります。

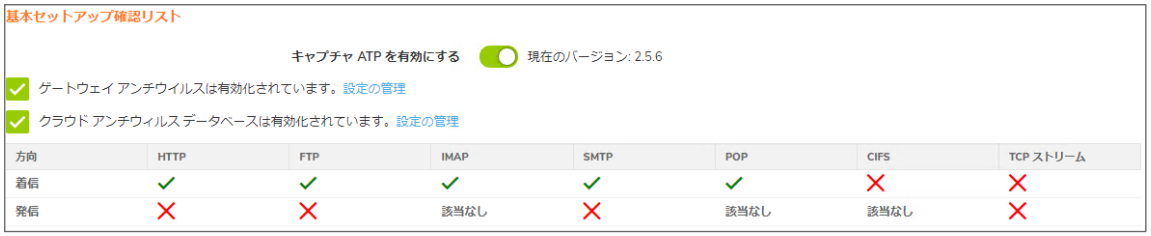
- 「**同意し、この設定を適用します**」ボタンをクリックすると、「**判定が返ってくるまでファイルのダウンロードを遮断する**」オプションが有効になります。変更を反映するには、「**適用**」をクリックする必要もあります。
- 「この設定を**適用しません**」リンクを選択すると、ダイアログが閉じられ、「**判定を待っている間はファイルのダウンロードを許可する**」はオンの状態のままとなります。

8. 「**適用**」をクリックします。

GAV または クラウド ゲートウェイ アンチウイルスの無効化

「**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**」ページでゲートウェイ アンチウイルスまたはクラウド ゲートウェイ アンチウイルス サービスのチェック ボックスをオフすると、各サービスを無効にすることができます。キャプチャ ATP が有効なときにどちらかのサービスを無効にすると、キャプチャ ATP も無効になることを警告するメッセージがポップアップで表示されます。

ゲートウェイ アンチウイルス または クラウド ゲートウェイ アンチウイルス が無効になっている場合、キャプチャ ATP は動作を停止します。例えば、ゲートウェイ アンチウイルスが有効ではないと、「**ポリシー | キャプチャ ATP > 設定**」ページに「**キャプチャ ATP が機能するには、ゲートウェイ アンチウイルスを有効にしなければなりません。**」というメッセージと「設定の管理」リンクが表示されます。このリンクを選択すると、「**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**」ページに移動し、GAV を有効化できます。


基本セットアップ確認リスト
キャプチャ ATP を有効にする
現在のバージョン: 2.5.6
ゲートウェイ アンチウイルスは有効化されています。設定の管理
クラウド アンチウィルス データベースは有効化されています。設定の管理
方向
HTTP
FTP
IMAP
SMTP
POP
CIFS
TCP ストリーム
着信
発信
該当なし
該当なし
該当なし

2

スキャン履歴

キャプチャ ATP の「**スキャン履歴**」ページは、「**ポリシー | キャプチャ ATP > スキャン履歴**」にあり、スキャンと分析が終わったすべてのファイルの一覧を表示します。検索結果をフィルタして絞り込むことで、前月、前週、最新 24 時間、または最新 1 時間のスキャンを表示できます。特定の文字列を検索することもできます。その場合、このページにはその文字列を含む項目のみが表示されます。ユーザ定義の期間を使用して一定の範囲のスキャン インスタンスを表示したり、「**列選択**」の表示をカスタマイズします。

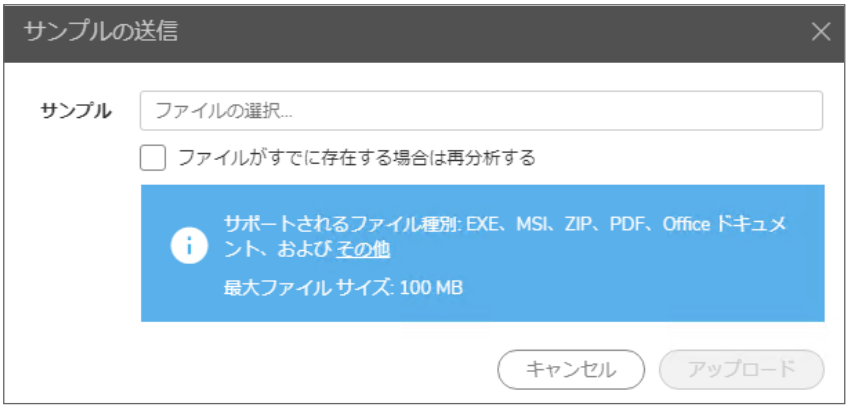
サンプルの送信

「**サンプルの送信**」オプションを使用すると、サポートされているファイルを参照し、分析のために送信してスキャンできます。サポートされているファイルは、.EXE、.MSI、.ZIP、.APK、.PE ファイルなどで、最大ファイル サイズは 10240 KB です。

送信できる最大ファイル サイズを制限するには、「**ポリシー | キャプチャ ATP > 設定**」ページの「**帯域幅管理**」を使用します。0 から、ライセンス マネージャによって設定された最大サイズ (10240 KB) まで、任意の数値を入力できます。ゼロ (0) を入力するのは、ファイル サイズを無制限にすることを意味しますが、これは推奨されません。

分析のためにファイルを キャプチャ ATP に送信するには、次の手順に従います。

1. 「**ポリシー | キャプチャ ATP > スキャン履歴**」ページに移動します。
2. 「**サンプルの送信**」アイコンをクリックします。
   「**サンプルの送信**」ダイアログが表示されます。



3. 「**ファイルの選択...**」フィールドをクリックし、送信するファイルを参照します。
4. 以前にスキャンしたファイルを再送信する場合は、「**ファイルがすでに存在する場合は再分析する**」オプションをクリックします。
5. 「**アップロード**」をクリックします。
6. 少ししてから、「**再表示**」をクリックします。ファイルが「**スキャン履歴**」ページに表示されることを確認します。

分析結果の表示

スキャンされたファイルの詳細な結果を表示するには、次の手順に従います。

1. 「**ポリシー | キャプチャ ATP > スキャン履歴**」ページに移動します。
2. 「**スキャン履歴**」ページには、次の列があります。
   - **特性**: このファイルの分析結果は、「**無害**」または「**有害**」です。
   - **ファイル名**: スキャンされたファイルのファイル名を一覧に示します。
   - **ファイル ハッシュ**: 一方向ダイジェスト関数によって処理された入力バイト数から計算された固定長値。
   - **種別**: 分析されたファイルの種別 (実行可能ファイル、zip ファイルなど)。
   - **日付/時刻**: 分析のためにファイルが送信された時刻。
   - **送信元**: ファイル送信元のIPアドレス。
   - **送信先**: ファイル送信先のIPアドレス。

   結果の詳細表示で、スキャン レポートをクリックしてそのファイルのスキャン レポートを開始できます。
3. そのファイルの「**特性**」チェック マークをクリックします。そのファイルの詳細な分析結果が表示されます。

4. 結果を閉じるには、「**特性**」チェック マークをもう一度クリックします。

3

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 および SonicOSX キャプチャ ATP 管理ガイド
更新日 – 2021 年 3 月
ソフトウェア バージョン – 7
232-005435-00 Rev B

Copyright © 2021 SonicWall Inc. All rights reserved.

本文書の情報は SonicWall およびその関連会社の製品に関して提供されています。明示的または暗示的、禁反言にかかわらず、知的財産権に対するいかなるライセンスも、本文書または製品の販売に関して付与されないものとします。本製品のライセンス契約で定義される契約条件で明示的に規定される場合を除き、SONICWALL および/またはその関連会社は一切の責任を負わず、商品性、特定目的への適合性、あるいは権利を侵害しないことの暗示的な保証を含む（ただしこれに限定されない）、製品に関する明示的、暗示的、または法定的な責任を放棄します。いかなる場合においても、SONICWALL および/またはその関連会社が事前にこのような損害の可能性を認識していた場合でも、SONICWALL および/またはその関連会社は、本文書の使用または使用できないことから生じる、直接的、間接的、結果的、懲罰的、特殊的、または付随的な損害（利益の損失、事業の中断、または情報の損失を含むが、これに限定されない）について一切の責任を負わないものとします。SonicWall および/またはその関連会社は、本書の内容に関する正確性または完全性についていかなる表明または保証も行いません。また、事前の通知なく、いつでも仕様および製品説明を変更する権利を留保し、本書に記載されている情報を更新する義務を負わないものとします。

詳細については、次のサイトを参照してください。https://www.sonicwall.com/ja-jp/legal

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