



ファイルレピュテーションフィルタリングとファイル分析

この章は、次の項で構成されています。

- [ファイルレピュテーションフィルタリングとファイル分析の概要](#) (1 ページ)
- [ファイルレピュテーションと分析機能の設定](#) (6 ページ)
- [ファイルレピュテーションおよびファイル分析のレポートとトラッキング](#) (31 ページ)
- [ファイルの脅威判定の変更時のアクションの実行](#) (35 ページ)
- [ファイルレピュテーションと分析のトラブルシューティング](#) (35 ページ)

ファイルレピュテーションフィルタリングとファイル分析の概要

Advanced Malware Protection は、次によりゼロデイや電子メールの添付ファイル内のファイルベースの標的型の脅威から保護します。

- 既知のファイルのレピュテーションを取得する。
- レピュテーション サービスでまだ認識されていない特定のファイルの動作を分析する。
- 新しい情報が利用可能になるのに伴い出現する脅威を常に評価し、脅威と判定されているファイルがネットワークに侵入するとユーザーに通知する。

この機能は着信メッセージと発信メッセージ。

ファイルレピュテーションおよびファイル分析サービスでは、パブリッククラウドまたはプライベートクラウド（オンプレミス）を選択できます。

- プライベートクラウドファイルレピュテーションサービスは Cisco Secure Endpoint プライベートクラウドアプライアンスにより提供され、「プロキシ」モードまたは「エアギャップ」（オンプレミス）モードで動作します。「[オンプレミスのファイルレピュテーションサーバの設定](#) (7 ページ)」を参照してください。

- プライベートクラウドファイル分析サービスは、オンプレミス Cisco AMP マルウェア分析アプライアンスにより提供されます。[オンプレミスのファイル分析サーバの設定 \(8 ページ\)](#) を参照してください。

ファイル脅威判定のアップデート

新しい情報の出現に伴い、脅威の判定は変化します。最初にファイルが不明または正常として評価されると、ファイルは受信者に対して解放されます。新しい情報が利用可能になるのに伴い脅威判定が変更されると、アラートが送信され、ファイルとその新しい判定が [AMP 判定のアップデート (AMP Verdict Updates)] レポートに示されます。脅威の影響に対処する最初の作業として、侵入のきっかけとなったメッセージを調査できます。

判定が「悪意がある」から「正常」に変更されることもあります。

ファイル分析の後でファイルに動的なコンテンツが見つからない場合、判定は「低リスク」です。ファイル分析用にファイルは送信されず、メッセージは電子メールパイプラインを通過します。

アプライアンスが同じファイルの後続インスタンスを処理するときに、更新された結果がただちに適用されます。

判定アップデートのタイミングに関する情報は、ファイル基準のドキュメント ([ファイルレピュテーションおよび分析サービスでサポートされるファイル \(4 ページ\)](#)) を参照) に記載されています。

関連項目

- [ファイルレピュテーションおよびファイル分析のレポートとトラッキング \(31 ページ\)](#)
- [ファイルの脅威判定の変更時のアクションの実行 \(35 ページ\)](#)

ファイル処理の概要

メッセージに対して最終アクションが実行されていない場合は、以前のスキャンエンジンの判定に関係なく、アンチウイルス スキャンの完了直後に、ファイルレピュテーションが評価され、ファイルが分析目的で送信されます。

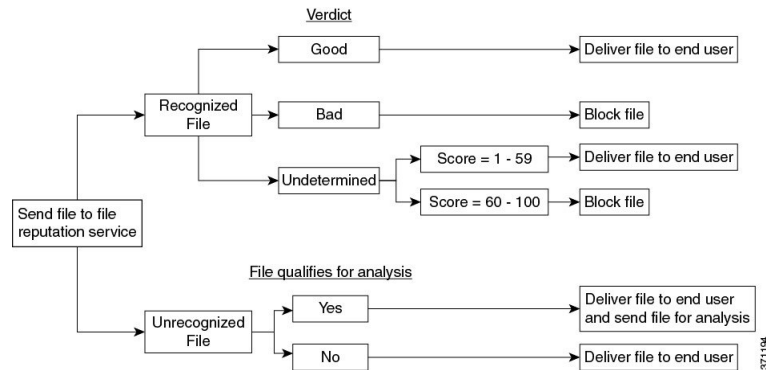


- (注) メッセージの MIME ヘッダーの形式が正しくない場合、ファイルレピュテーション サービスはデフォルトで「スキャン不可」の判定を返します。アプライアンスは、このメッセージからも添付ファイルを抽出しようとします。アプライアンスが添付ファイルを抽出できない場合、判定は「スキャン不可」のままです。アプライアンスが添付ファイルを抽出できる場合は、添付ファイルのファイルレピュテーションが評価されます。添付ファイルが悪意のあるものである場合、判定は「スキャン不可」から「悪意のある」に変わります。

アプライアンスとファイルレピュテーションサービス間の通信は暗号化され、改ざんされないように保護されます。

ファイルレピュテーションの評価後：

- メッセージに添付ファイルが含まれていない場合、ファイルレピュテーションサービスは「スキップ」の判定を返します。
- ファイルがファイルレピュテーションサービスに対して既知であり、正常であると判断された場合、メッセージは引き続きワークキューに残ります。
- ファイルレピュテーションサービスからメッセージの添付ファイルについて悪意があるという判定が返されると、該当するメールポリシーで指定したアクションが、アプライアンスにより適用されます。
- レピュテーションサービスがファイルを認識しているが、決定的な判定を下すための十分な情報がない場合、レピュテーションサービスはファイルの特性（脅威のフィンガープリントや動作分析など）に基づき、レピュテーションスコアを戻します。このスコアが設定されたレピュテーションしきい値を満たすか、または超過した場合、マルウェアが含まれるファイルに関するメールポリシーで設定したアクションがアプライアンスによって適用されます。
- レピュテーションサービスにそのファイルに関する情報がなく、そのファイルが分析の基準を満たしていない場合（[ファイルレピュテーションおよび分析サービスでサポートされるファイル（4 ページ）](#)を参照）、そのファイルは正常と見なされ、メッセージはワークキューに残ります。
- ファイル分析サービスがイネーブルな状態で、レピュテーションサービスにはファイルに関する情報がなく、そのファイルが分析可能なファイルの条件を満たしている場合（[ファイルレピュテーションおよび分析サービスでサポートされるファイル（4 ページ）](#)を参照）、メッセージは隔離され（[分析のために送信した添付ファイルがあるメッセージの隔離（25 ページ）](#)を参照）、ファイルは分析用に送信される可能性があります。添付ファイルが分析のために送信される時、またはファイルが分析のために送信されない場合にメッセージを隔離するようにアプライアンスを設定していない場合、そのメッセージはユーザに解放されます。
- オンプレミスのファイル分析での展開では、レピュテーション評価とファイル分析は同時に実行されます。レピュテーションサービスから判定が返された場合は、その判定が使用されます。これは、レピュテーションサービスにはさまざまなソースからの情報が含まれているためです。レピュテーションサービスがファイルを認識していない場合、ファイル分析の判定が使用されます。
- サーバとの接続がタイムアウトしたためにファイルレピュテーションの判定の情報が利用できない場合、そのファイルはスキャン不可と見なされ、設定されたアクションが適用されます。

図 1: パブリッククラウドファイル分析の展開における **Advanced Malware Protection** ワークフロー

ファイルが分析のために送信される場合：

- 分析用にクラウドに送信される場合、ファイルは HTTPS 経由で送信されます。
- 分析には通常、数分かかりますが、さらに時間がかかることもあります。
- ファイル分析で悪意があるとしてフラグ付けされたファイルが、レピュテーションサービスでは悪意があると識別されない場合があります。ファイルレピュテーションは、1回のファイル分析結果でなく、さまざまな要因によって経時的に決定されます。
- オンプレミスの Cisco Secure Endpoint マルウェア分析アプライアンスを使用して分析されたファイルの結果は、ローカルにキャッシュされます。

判別のアップデートの詳細については、[ファイル脅威判定のアップデート \(2 ページ\)](#) を参照してください。

ファイルレピュテーションおよび分析サービスでサポートされるファイル

レピュテーションサービスはほとんどのタイプのファイルの評価します。ファイルタイプの識別はファイル コンテンツによって行われ、ファイル拡張子には依存していません。

レピュテーションが不明な一部のファイルは、分析して脅威の特性を調べることができます。ファイル分析機能を設定すると、分析するファイルタイプを選択できます。新しいタイプを動的に追加できます。アップロード可能なファイルタイプのリストが変更された場合はアラートを受け取るので、追加されたファイルタイプを選択してアップロードできます。

ファイルレピュテーションおよび分析サービスでサポートされているファイルの詳細は、登録済みのお客様に限り提供しています。評価と分析の対象となるファイルについて詳しくは、『*File Criteria for Advanced Malware Protection Services for Cisco Content Security Products*』を参照してください。このドキュメントは、<https://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html> から入手できます。ファイルレピュテーションの評価基準、および分析用ファイルの送信基準はいつでも変更できます。

このドキュメントにアクセスするには、シスコの顧客アカウントとサポート契約が必要です。登録するには、<https://tools.cisco.com/RPF/register/register.do> にアクセスしてください。

Advanced Malware Protectionが対応しないファイルの配信をブロックするには、ポリシーを設定する必要があります。



(注) どこかのソースからすでに分析用にアップロードしたことのある（着信メールまたは発信メールのいずれかの）ファイルは、再度アップロードされません。このようなファイルの分析結果を表示するには、[ファイル分析（File Analysis）] レポート ページから SHA-256 を検索します。

関連項目

- [ファイルレピュテーションと分析サービスの有効化と設定（9 ページ）](#)
- [Advanced Malware Protection の問題に関するアラートの確実な受信（29 ページ）](#)
- [アーカイブファイルまたは圧縮ファイルの処理（5 ページ）](#)

アーカイブファイルまたは圧縮ファイルの処理

ファイルが圧縮またはアーカイブされている場合：

- 圧縮ファイルまたはアーカイブファイルのレピュテーションが評価されます。

ファイル形式を含めて、検査対象となるアーカイブファイルや圧縮ファイルについて詳しくは、[ファイルレピュテーションおよび分析サービスでサポートされるファイル（4 ページ）](#) の情報を参照してください。

このシナリオでは、次のようになります。

- 抽出されたファイルのいずれかが悪意のあるファイルである場合、ファイルレピュテーションサービスは、その圧縮/アーカイブファイルに対して「悪意がある（Malicious）」という判定を返します。
- 圧縮/アーカイブファイルが悪意のあるファイルであり、抽出されたすべてのファイルが正常である場合、ファイルレピュテーションサービスは、圧縮/アーカイブファイルに対して「悪意がある（Malicious）」という判定を返します。
- 抽出されたファイルのいくつかの判定が「不明（unknown）」である場合、それらの抽出ファイルは、状況に応じて、分析のために送信されます（そのように設定されており、ファイルタイプがファイル分析でサポートされている場合）。
- 抽出されたファイルまたは添付ファイルのいくつかの判定が「低リスク（low risk）」である場合、そのファイルはファイル分析に送信されません。
- 圧縮/アーカイブファイルの圧縮解除中にファイルの抽出に失敗した場合、ファイルレピュテーションサービスは、圧縮/アーカイブファイルに対して「スキャン不可（Unscannable）」という判定を返します。ただし、抽出されたファイルの1つが悪意のあるファイルである場合、ファイルレピュテーションサービスは、圧縮/アーカイブファイルに対して「悪意がある（Malicious）」という判定を返します（「悪意がある

(Malicious)」という判定は「スキャン不可 (Unscannable)」よりも順位が高くなります)。

- アーカイブまたは圧縮ファイルは、次のシナリオではスキャン不可として処理されます。
 - データ圧縮率が 20 を超える。
 - アーカイブ ファイルに 5 を超えるレベルのネストが含まれる。
 - アーカイブ ファイルに 200 を超える子ファイルが含まれる。
 - アーカイブ ファイルのサイズが 50 MB を超える。
 - アーカイブファイルがパスワードで保護されているか、または読み取り不可である。



(注) セキュア MIME タイプの抽出ファイル (テキストやプレーンテキストなど) のレピュテーションは、評価されません。

クラウドに送信される情報のプライバシー

- クラウド内のレピュテーション サービスには、ファイルを一意に識別する SHA のみが送信されます。ファイル自体は送信されません。
- クラウド内のファイル分析サービスを使用している場合、ファイルが分析の要件を満たしていれば、ファイル自体がクラウドに送信されます。
- 分析用にクラウドに送信されて「悪意がある」と判定されたすべてのファイルに関する情報は、レピュテーション データベースに追加されます。この情報は他のデータと共にレピュテーション スコアを決定するために使用されます。

オンプレミスの Cisco Secure Endpoint マルウェア分析アプライアンスで分析されたファイルの情報は、レピュテーションサービスと共有されません。

FIPS Compliance

ファイルレピュテーション スキャンおよびファイル分析は、FIPS に準拠しています。

ファイルレピュテーションと分析機能の設定

- [ファイルレピュテーションと分析サービスとの通信の要件 \(7 ページ\)](#)
- [オンプレミスのファイルレピュテーションサーバの設定 \(7 ページ\)](#)
- [オンプレミスのファイル分析サーバの設定 \(8 ページ\)](#)
- [ファイルレピュテーションと分析サービスの有効化と設定](#)

- (パブリッククラウドファイル分析サービスのみ) アプライアンスグループの設定 (19 ページ)
- ファイルレピュテーションスキャンおよびファイル分析のメールポリシーの設定 (22 ページ)
- 分析のために送信した添付ファイルがあるメッセージの隔離 (25 ページ)
- ファイル分析隔離の使用 (26 ページ)
- 中央集中型のファイル分析の隔離 (28 ページ)
- ファイルレピュテーションと分析の X ヘッダー (29 ページ)
- ドロップされたメッセージまたは添付ファイルに関する通知のエンドユーザーへの送信 (29 ページ)
- 高度なマルウェア防御とクラスタ (29 ページ)
- Advanced Malware Protection の問題に関するアラートの確実な受信 (29 ページ)
- Advanced Malware Protection 機能の集約管理レポートの設定 (31 ページ)

ファイルレピュテーションと分析サービスとの通信の要件

- これらのサービスを使用する E メールセキュリティ アプライアンスはすべて (オンプレミスの Cisco Secure Endpoint マルウェア分析 アプライアンスを使用するよう設定されたファイル分析サービスは除く)、インターネット経由で直接サービスに接続する必要があります。
- デフォルトでは、ファイルレピュテーションおよび分析サービスを参照してください。
- デフォルトでは、ファイルレピュテーションとクラウドベースの分析サービスとの通信は、デフォルトゲートウェイに関連付けられているインターフェイス経由でルーティングされます。トラフィックを異なるインターフェイス経由でルーティングするには、[セキュリティサービス (Security Services)] > [ファイルレピュテーションと分析 (File Reputation and Analysis)] ページの [詳細設定 (Advanced)] セクションで、各アドレスにスタティックルートを作成します。
- 開く必要があるファイアウォールポートの詳細については、[ファイアウォール情報](#) 章を参照してください。

オンプレミスのファイルレピュテーションサーバの設定

プライベートクラウドのファイル分析サーバとして Cisco Secure Endpoint プライベートクラウド アプライアンスを使用する場合は、以下のように設定します。

- FireAMP プライベートクラウドのインストールおよび設定に関するガイドを含む、Cisco Advanced Malware Protection 仮想プライベートクラウド アプライアンスのドキュメント

は、
<http://www.cisco.com/c/en/us/support/security/fireamp-private-cloud-virtual-appliance/tsd-products-support-series-home.html>
 から取得できます。

この項目に記載されているタスクはこのドキュメントを参照して実行します。

AMP 仮想プライベートクラウドアプライアンスのヘルプリンクを使用して、その他のドキュメントも入手できます。

- 「プロキシ」モードまたは「エアギャップ」（オンプレミス）モードでの Cisco Secure Endpoint プライベートクラウドアプライアンスを設定および構成します。
- Cisco Secure Endpoint プライベートクラウドアプライアンスのソフトウェアバージョンが、電子メールゲートウェイと Cisco Secure Endpoint アプライアンスの統合を可能にするバージョン 3.8.1 以降であることを確認します。
- Cisco Secure Endpoint プライベートクラウドの SSL 証明書をそのアプライアンスにダウンロードして、この電子メールゲートウェイにアップロードします。



(注) オンプレミスのファイルレピュテーションサーバーを設定した後に、この E メールセキュリティアプライアンスからこのサーバーへの接続を設定します。以下[ファイルレピュテーションと分析サービスの有効化と設定（9 ページ）](#)のステップ 6 を参照してください。

オンプレミスのファイル分析サーバの設定

Cisco Secure Endpoint マルウェア分析アプライアンスをプライベートクラウドのファイル分析サーバーとして使用する場合：

- 『Cisco Secure Endpoint Malware Analytics Appliance Setup and Configuration Guide』および『Cisco Secure Endpoint Malware Analytics Appliance Administration Guide』を入手してください。Cisco Secure Endpoint マルウェア分析アプライアンスのドキュメントは、<http://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides%20-list.html> から入手できます。

この項目に記載されているタスクはこのドキュメントを参照して実行します。

追加のドキュメントは、Cisco Secure Endpoint マルウェア分析アプライアンスのヘルプリンクから入手できます。

アドミニストレーションガイドで、次のすべての情報を検索します：他の Cisco アプライアンス、CSA、Cisco Sandbox API、ESA、および Cisco E メールセキュリティアプライアンス、との統合。

- Cisco Secure Endpoint マルウェア分析アプライアンスを設定および構成します。
- 必要に応じて、Cisco Secure Endpoint マルウェア分析アプライアンスのソフトウェアバージョンをバージョン 1.2.1 に更新します。これにより、Cisco E メールセキュリティアプライアンスとの統合がサポートされます。

バージョン番号を確認し更新を実行する方法については、AMP マルウェア分析のドキュメントを参照してください。

- アプライアンスがネットワーク上で相互に通信できることを確認します。Cisco E メールセキュリティ アプライアンスは、Cisco Secure Endpoint マルウェア分析アプライアンスの正常な (CLEAN) インターフェイスに接続可能である必要があります。
- 自己署名証明書を展開する場合は、E メールセキュリティ アプライアンスで使用される Cisco Secure Endpoint マルウェア分析アプライアンスから自己署名 SSL 証明書を生成しません。SSL 証明書をダウンロードする手順については、Cisco Secure Endpoint マルウェア分析アプライアンスの管理者ガイドを参照してください。CN として Cisco Secure Endpoint マルウェア分析アプライアンスのホスト名がある証明書を生成してください。Cisco Secure Endpoint マルウェア分析アプライアンスからのデフォルトの証明書は機能しません。
- マルウェア分析アプライアンスへの E メールセキュリティ アプライアンスの登録は、「[ファイルレピュテーションと分析サービスの有効化と設定](#)」で説明したように、ファイル分析の構成を送信したときに自動的に実行されます。ただし、同じ手順に記載されているように、登録をアクティブ化する必要があります。

ファイルレピュテーションと分析サービスの有効化と設定

始める前に

- ファイルレピュテーションサービスとファイル分析サービスの機能キーを取得して、このアプライアンスに転送します。
- [ファイルレピュテーションと分析サービスとの通信の要件 \(7 ページ\)](#) を満たします。
- [更新 (Updates)] ページで設定したアップデートサーバへの接続を確認します。
- Cisco Secure Endpoint プライベートクラウドアプライアンスをプライベートクラウドのファイルレピュテーションサーバとして使用する場合は、[オンプレミスのファイルレピュテーションサーバの設定 \(7 ページ\)](#) を参照してください。
- Cisco Secure Endpoint マルウェア分析アプライアンスをプライベートクラウドのファイル分析サーバとして使用する場合は、[オンプレミスのファイル分析サーバの設定 \(8 ページ\)](#) を参照してください。

手順

-
- ステップ 1** [セキュリティサービス (Security Services)]>[ファイルレピュテーションと分析 (File Reputation and Analysis)] を選択します。
 - ステップ 2** [グローバル設定を編集 (Edit Global Settings)] をクリックします。
 - ステップ 3** [ファイルレピュテーションフィルタを有効にする (Enable File Reputation Filtering)] をクリックし、必要に応じて [ファイル分析を有効にする (Enable File Analysis)] をクリックします。

- [ファイルレピュテーションフィルタを有効にする (Enable File Reputation Filtering)] をオンにする場合、[ファイルレピュテーションサーバ (File Reputation Server)] セクションを設定するために (ステップ 6)、外部パブリックレピュテーションクラウドサーバの URL を入力するか、プライベートレピュテーションクラウドサーバの接続情報を入力する必要があります。
- 同様に、[ファイル分析を有効にする (Enable File Analysis)] をオンにする場合、[ファイル分析サーバの URL (File Analysis Server URL)] セクションを設定するために (ステップ 7)、外部クラウドサーバの URL を入力するか、プライベート分析クラウドの接続情報を入力する必要があります。

(注) 新しいファイルタイプがアップグレード後に追加される場合がありますが、デフォルトでは有効になっていません。ファイル分析を有効にしており、新しいファイルタイプを分析に含めることが必要な場合には、それらを有効にする必要があります。

ステップ 4 ライセンス契約が表示された場合は、それに同意します。

ステップ 5 [ファイル分析 (File Analysis)] セクションで、適切なファイルグループ (たとえば、「Microsoft Documents」) からファイル分析のために送信する必要があるファイルタイプを選択します。

サポートされるファイルタイプについては、次のドキュメントの説明を参照してください。
[ファイルレピュテーションおよび分析サービスでサポートされるファイル \(4 ページ\)](#)

(注) シスコは、ゼロデイの脅威を阻止するために、潜在的な悪意のあるファイルタイプを定期的にチェックしています。新しい脅威が特定されると、アップデートサーバを介してファイルタイプなどの詳細がアプライアンスに送信されます。[その他の潜在的な悪意のあるファイルタイプ (Other potentially malicious file types)] オプションを選択して、この機能を有効にします。この機能を有効にすると、アプライアンスは選択したファイルタイプに加えて分析用のファイルタイプを送信します。

ステップ 6 [ファイルレピュテーションの詳細設定 (Advanced Settings for File Reputation)] パネルを展開し、必要に応じて以下のオプションを調整します。

| オプション | 説明 |
|--|--|
| ファイルレピュテーションサーバ (File Reputation Server) | <p>パブリックレピュテーションクラウドサーバまたはプライベートレピュテーションクラウドクラウドのホスト名を選択します。</p> <p>プライベートレピュテーションクラウドを選択する場合は、次の情報を入力します。</p> <ul style="list-style-type: none"> • [コンソールのホスト名 (Console Hostname)] - Cisco Secure Endpoint プライベートクラウドアプライアンスのコンソールのホスト名。 • [アクティベーションコード (Activation Code)] - Cisco Secure Endpoint プライベートクラウドアプライアンスのアクティベーションコード。 <p>コンソールのホスト名とアクティベーションコードを取得する方法の詳細については、Cisco Secure Endpoint プライベートクラウドのドキュメントを参照してください。</p> <p>(注) ファイルレピュテーションのSSL通信を実行するには、CLI コマンド certconfig>CERTAUTHORITY>CUSTOM、または Web インターフェイスの [ネットワーク (Network)]>[証明書 (カスタム認証局) (Certificates (Custom Certificate Authorities))] のいずれかを使用して、AMP オンプレミスレピュテーションサーバー CA 証明書をこの電子メールゲートウェイの証明書ストアに追加する必要があります。この証明書は、Cisco Secure Endpoint プライベートクラウドアプライアンスから取得します ([統合 (Integrations)]>[Eメールセキュリティアプライアンス (Email Security Appliance)]>[バージョン15.0以降 (Version 15.0 and above)]>[SSL構成 (SSL Configuration)]>[ダウンロード (download)])。</p> |
| Cisco Secure Endpoint コンソールの統合 | <p>[電子メールゲートウェイを Cisco Secure Endpoint に登録 (Register the Email Gateway with Secure Endpoint)] をクリックして、電子メールゲートウェイを Cisco Secure Endpoint コンソールと統合します。詳細な手順については、電子メールゲートウェイと Cisco Secure Endpoint コンソールの統合 (16 ページ) を参照してください。</p> |
| ハートビート間隔 (Heartbeat Interval) | <p>レトロスペクティブなイベントを確認するための ping の送信頻度 (分単位)。</p> |
| クエリータイムアウト (Query Timeout) | <p>レピュテーションクエリーがタイムアウトになるまでの経過秒数。</p> |
| 処理のタイムアウト (Processing Timeout) | <p>ファイルの処理がタイムアウトになるまでの経過秒数。</p> |

| オプション | 説明 |
|---|--|
| ファイルレピュテーションクライアントID (File Reputation Client ID) | ファイルレピュテーションサーバ上のこのアプライアンスのクライアントID (読み取り専用) |
| ファイルレトロスペクティブ (File Retrospective) | メッセージ受信者に配信されなかった、ドロップ、または隔離されたメッセージに関するレトロスペクティブ判定アラートを抑制するには、[レトロスペクティブ判定アラートの抑制 (Suppress the retrospective verdict alerts)] をオンにします。 |

(注) このセクションの他の設定は、シスコのサポートのガイダンスなしに変更しないでください。

ステップ7 ファイル分析にクラウドサービスを使用する場合は、[ファイル分析の詳細設定 (Advanced Settings for File Analysis)] パネルを展開し、必要に応じて次のオプションを調整します。

| オプション | 説明 |
|---|----|
| ファイル分析サーバの URL (File Analysis Server URL) | |

| オプション | 説明 |
|-------|--|
| | <p>外部クラウドサーバの名前（URL）、または[プライベート分析クラウド（Private analysis cloud）]を選択します。</p> <p>外部クラウドサーバを指定する場合、アプライアンスに物理的に近いサーバを選択します。新たに使用可能になったサーバは、標準の更新プロセスを使用して、このリストに定期的に追加されます。</p> <p>ファイル分析にオンプレミス Cisco Secure Endpoint マルウェア分析アプライアンスを使用するプライベート分析クラウドを選択し、次の情報を入力します。</p> <ul style="list-style-type: none"> • [TG サーバー（TG Servers）]：スタンドアロンの、またはクラスタ化された Cisco Secure Endpoint マルウェア分析アプライアンスの IPv4 アドレスまたはホスト名を入力します。最大7つの Cisco Secure Endpoint マルウェア分析アプライアンスを追加できます。 <ul style="list-style-type: none"> （注） シリアル番号は、スタンドアロンまたはクラスタ化された Cisco Secure Endpoint マルウェア分析アプライアンスの追加順序を示しています。アプライアンスの優先順位を示すものではありません。 （注） 1つのインスタンスにスタンドアロンサーバとクラスタサーバを追加することはできません。スタンドアロンまたはクラスタのいずれかにする必要があります。 <p>1つのインスタンスに追加できるスタンドアロンサーバは1台のみです。クラスタモードの場合は7台までサーバを追加できますが、すべてのサーバが同じクラスタに属している必要があります。複数のクラスタを追加することはできません。</p> • [認証局（Certificate Authority）]：[シスコのデフォルト認証局を使用する（Use Cisco Default Certificate Authority）]または[アップロードした認証局を使用する（Use Uploaded Certificate Authority）]を選択します。 <p>[アップロードした認証局を使用する（Use Uploaded Certificate Authority）]を選択する場合、[参照（Browse）]をクリックし、このアプライアンスとプライベートクラウドアプライアンスとの間の暗号化通信に使用する有効な証明書ファイルをアップロードします。これは、プライベートクラウドサーバで使用される証明書と同じである必要があります。</p> <p>（注） ファイル分析のためにアプライアンスで Cisco Secure Endpoint マルウェア分析ポータルを設定している場合は、Cisco Secure Endpoint マルウェア分析ポータル</p> |

| オプション | 説明 |
|--|---|
| | <p>(https://panacea.threatgrid.eu など) にアクセスし、ファイル分析用に送信されたファイルを表示および追跡できます。Cisco Secure Endpoint マルウェア分析ポータルにアクセスする方法については、Cisco TAC にお問い合わせください。</p> |
| <p>プロキシの設定</p> | <p>ファイル分析用アップストリームプロキシとして設定済みの、同じファイルレピュテーショントンネルプロキシを使用するには、[ファイルレピュテーションプロキシを使用する (Use File Reputation Proxy)] チェックボックスをオンにします。</p> <p>別のアップストリームプロキシを設定するには、[ファイルレピュテーションプロキシを使用する (Use File Reputation Proxy)] チェックボックスをオフにして、適切な [サーバ (Server)]、[ポート (Port)]、[ユーザ名 (Username)]、および [パスワード (Passphrase)] の情報を入力します。</p> |
| <p>ファイル分析クライアント ID (File Analysis Client ID)</p> | <p>ファイル分析サーバ上のこのアプライアンスのクライアント ID (読み取り専用)</p> |

- ステップ 8** (任意) ファイルレピュテーション判定結果の値にキャッシュ有効期限を設定する場合は、[キャッシュ設定 (Cache Settings)] パネルを展開します。
- ステップ 9** 許容されるファイル分析スコアの上限を設定するには、[しきい値の設定 (Threshold Settings)] パネルを展開します。スコアがこのしきい値を超えた場合は、ファイルが感染していることを示しています。次のいずれかのオプションを選択します。
- クラウドサービスの値を使用 (95) (Use value from Cloud Service (60))
 - [カスタム値の入力 (Enter Custom Value)] : デフォルトでは 95 に設定されます。
- ステップ 10** 変更を送信し、保存します。
- ステップ 11** オンプレミスの Cisco Secure Endpoint マルウェア分析アプライアンスを使用している場合は、Cisco Secure Endpoint マルウェア分析アプライアンスでこのアプライアンスのアカウントをアクティブ化します。
- 「ユーザー」アカウントをアクティブ化するための詳細な手順は、Cisco Secure Endpoint マルウェア分析のドキュメントで説明しています。
- a) ページセクションの下部に表示されたファイル分析クライアント ID を書き留めます。ここにはアクティブ化する「ユーザ」が表示されます。
 - b) Cisco Secure Endpoint マルウェア分析アプライアンスにサインインします。
 - c) [ようこそ... (Welcome...)] > [ユーザの管理 (Manage Users)] を選択し、[ユーザの詳細 (User Details)] に移動します。

- d) Eメールセキュリティ アプライアンスのファイル分析クライアント ID に基づいて「ユーザー」アカウントを見つけます。
- e) アプライアンスの「ユーザ」アカウントをアクティブにします。

電子メールゲートウェイと Cisco Secure Endpoint コンソールの統合

お使いのアプライアンスを Cisco Secure Endpoint コンソールと統合すると、Cisco Secure Endpoint コンソールで以下のアクションを実行できます。

- シンプル カスタム検出リストを作成する。
- シンプル カスタム検出リストに新しい悪意のあるファイル SHA を追加する。
- アプリケーション許可リストを作成する。
- アプリケーション許可トリストに新しいファイル SHA を追加する。
- カスタム ポリシーを作成する。
- カスタムポリシーにシンプルカスタム検出リストおよびアプリケーション許可リストを関連付ける。
- カスタム グループを作成する。
- カスタム グループにカスタム ポリシーを関連付ける。
- 登録済みのアプライアンスをデフォルトのグループからカスタム グループに移動する。
- 特定のファイル SHA のファイル トラジェクトリの詳細を表示する。

アプライアンスを Cisco Secure Endpoint コンソールと統合するには、アプライアンスをコンソールに登録する必要があります。

統合後に、ファイル SHA がファイル レピュテーション サーバーに送信されると、ファイル SHA に対してファイル レピュテーション サーバーから得られた判定は、Cisco Secure Endpoint コンソールの同じファイル SHA に対してすでに利用可能な判定により上書きされます。

ファイル SHA がすでにグローバルに悪意のあるものとしてマークされている場合、Cisco Secure Endpoint コンソールで同じファイル SHA をブロックリストに追加すると、ファイルの判定結果は「悪意のあるもの」になります。

[高度なマルウェア防御レポート (Advanced Malware Protection report)] ページには、新しいセクション、[カテゴリ別受信マルウェアファイル (Incoming Malware Files by Category)] があります。このセクションには、Cisco Secure Endpoint コンソールから受信されたブロックリストに登録されているファイル SHA の割合が、[カスタム検出 (Custom Detection)] として表示されます。ブロックリストに登録されているファイル SHA の脅威名は、レポートの [受信したマルウェア脅威ファイル (Incoming Malware Threat Files)] セクションに [シンプルカスタム検出 (Simple Custom Detection)] として表示されます。レポートの [詳細 (More Details)] セクシ

のリンクをクリックすると、Cisco Secure Endpoint コンソールでのブロックリストに登録されているファイル SHA のファイルトラジェクトリ詳細を表示できます。

始める前に

Cisco Secure Endpoint コンソールの管理アクセス権を伴うユーザーアカウントがあることを確認してください。Cisco Secure Endpoint コンソールのユーザーアカウントを作成する方法の詳細については、Cisco TAC にお問い合わせください。

(クラスタ化された構成の場合) クラスタ化された構成では、ログインしている電子メールゲートウェイを Cisco Secure Endpoint コンソールにのみ登録できます。電子メールゲートウェイを Cisco Secure Endpoint コンソールにスタンドアロンモードですでに登録している場合は、電子メールゲートウェイをクラスタに参加させる前に手動で登録を解除してください。

ファイルレピュテーションフィルタリングが有効化され、設定されていることを確認してください。ファイルレピュテーションフィルタリングを有効にして設定する方法については、「[ファイルレピュテーションと分析サービスの有効化と設定](#)」を参照してください。

手順

ステップ 1 [セキュリティサービス (Security Services)]>[ファイルレピュテーションと分析 (File Reputation and Analysis)] を選択します。

ステップ 2 [グローバル設定を編集 (Edit Global Settings)] をクリックします。

ステップ 3 Web インターフェイスの [ファイルレピュテーションとファイル分析 (File Reputation and File Analysis)] ページで、[ファイルレピュテーション (File Reputation)] の [詳細設定 (Advanced Settings)] パネルにある [Cisco Secure Endpoint へのアプライアンスの登録 (Register Appliance with Cisco Secure Endpoint)] をクリックします。

[Cisco Secure Endpoint へのアプライアンスの登録 (Register Appliance with Cisco Secure Endpoint)] をクリックすると、Cisco Secure Endpoint コンソールのログインページが表示されます。

ステップ 4 ご使用のユーザーログイン情報で、Cisco Secure Endpoint コンソールにログインします。

ステップ 5 Cisco Secure Endpoint の認証ページで [許可 (Allow)] をクリックして、アプライアンスを登録します。

[許可 (Allow)] をクリックすると登録が完了し、アプライアンスの [ファイルレピュテーションと分析 (File Reputation and Analysis)] ページにリダイレクトされます。[Cisco Secure Endpoint コンソールの統合 (Cisco Secure Endpoint Console Integration)] フィールドに、お使いのアプライアンスの名前が表示されます。アプライアンス名は、Cisco Secure Endpoint コンソールページでアプライアンス設定をカスタマイズする際に使用できます。

次のタスク

- Cisco Secure Endpoint コンソールページの [アカウント (Accounts)]>[アプリケーション (Applications)] セクションに移動すると、アプライアンスが Cisco Secure Endpoint コン

ソールに登録されているかどうかを確認できます。アプライアンス名は、Cisco Secure Endpoint コンソールページの [アプリケーション (Applications)] セクションに表示されません。

- 登録されたアプライアンスは、デフォルトのポリシー（ネットワークポリシー）が関連付けられたデフォルトのグループ（監査グループ）に追加されます。デフォルトポリシーには、ブロックリストまたは許可リストに追加されるファイルSHAが含まれています。Cisco Secure Endpoint の設定をお使いのアプライアンス用にカスタマイズして、ブロックリストまたは許可リストに追加されている独自のファイル SHA を追加する場合は、<https://console.amp.cisco.com/docs> で Cisco Secure Endpoint のユーザーマニュアルを参照してください。
- [ファイルレピュテーション設定 (File Reputation Settings)] ページの [ファイルレピュテーションクライアント ID (File Reputation Client ID)] の値と、Cisco Secure Endpoint コンソールポータルで登録したアプライアンスの [デバイス GUID (Device GUID)] の値が同じであることを確認します。値が異なっていると、アプライアンスと Cisco Secure Endpoint の統合が、マシンレベルまたはクラスタレベルで正しく機能しません。Cisco Secure Endpoint 機能を使用するには、アプライアンスを登録解除して登録しなおす必要があります。
- アプライアンス接続を Cisco Secure Endpoint コンソールから登録解除するには、アプライアンスの [ファイルレピュテーション (File Reputation)] セクションの [詳細設定 (Advanced Settings)] で [登録解除 (Deregister)] をクリックするか、または <https://console.amp.cisco.com/> で Cisco Secure Endpoint コンソールページにアクセスする必要があります。詳細については、<https://console.amp.cisco.com/docs> で Cisco Secure Endpoint ユーザーマニュアルを参照してください。



(注) ファイルレピュテーションサーバーを別のデータセンターに変更すると、電子メールゲートウェイは Cisco Secure Endpoint コンソールから自動的に登録解除されます。ファイルレピュテーションサーバーに選択された同じデータセンターを使用して、電子メールゲートウェイを Cisco Secure Endpoint コンソールに再登録する必要があります。



(注) クラスタレベルでファイルレピュテーションサーバーを変更すると、ログインしている電子メールゲートウェイは自動的に Cisco Secure Endpoint コンソールから登録解除されます。クラスタ内の他のすべてのマシンの登録を解除してください。ファイルレピュテーションサーバーに選択された同じデータセンターを使用してすべての電子メールゲートウェイを Cisco Secure Endpoint コンソールに再登録する必要があります。



- (注) (クラスタ構成の場合) : [ファイルレピュテーションとファイル分析 (File Reputation and File Analysis)]構成設定をあるクラスタレベルから別のクラスタレベルに移動する予定がある場合は、最初に Cisco Secure Endpoint コンソールからログインしている電子メールゲートウェイの登録を解除する必要があります。 [ファイルレピュテーションとファイル分析 (File Reputation and File Analysis)]構成設定を新しいクラスタレベルに移動した後、電子メールゲートウェイを Cisco Secure Endpoint コンソールに再登録する必要があります。



- (注) 悪意のあるファイル SHA がクリーンと判定される場合、そのファイル SHA が Cisco Secure Endpoint コンソールで許可リストに追加されていないか確認する必要があります。

重要：ファイル分析設定に必要な変更

新しいパブリック クラウド ファイル分析サービスを使用する場合は、次の説明を読み、データセンターの分離を維持するようにしてください。

- 既存のアプライアンスのグループ化情報は、新しいファイル分析サーバには保存されません。新しいファイル分析サーバでアプライアンスを再グループ化する必要があります。
- ファイル分析隔離エリアに隔離されたメッセージは、保存期間が経過するまで保存されません。隔離エリアでの保存期間が経過すると、メッセージはファイル分析隔離エリアから解放され、AMP エンジンによって再スキャンされます。その後、ファイルは分析のために新しいファイル分析サーバにアップロードされますが、メッセージがもう一度ファイル分析隔離エリアに送信されることはありません。

詳細については、

<http://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/products-installation-guides-list.html> から Cisco AMP マルウェア分析のマニュアルを参照してください。

(パブリック クラウド ファイル分析サービスのみ) アプライアンスグループの設定

組織のすべてのコンテンツ セキュリティ アプライアンスで、組織内の任意のアプライアンスから分析用に送信されるファイルに関するクラウド内の分析結果の詳細が表示されるようにするには、すべてのアプライアンスを同じアプライアンスグループに結合する必要があります。マシンレベルまたはクラスタレベルでアプライアンスのグループを設定できます。

始める前に

- クラスタ内のすべてのマシンが動作していることを確認します。
- 地域の設定済みファイル分析サーバーに接続していて、サーバーが動作していることを確認します。



- (注) オンプレミスの仮想Eメールゲートウェイに「クラウド管理機能」キーが含まれていないライセンスキーファイルをロードした場合でも、スマートライセンスアカウントIDを使用して脅威グループファイル分析の自動登録を実行できます。

手順

- ステップ1** [セキュリティサービス (Security Services)]>[ファイルレピュテーションと分析 (File Reputation and Analysis)] を選択します。
- ステップ2** [ここをクリックしてファイル分析用電子メールゲートウェイレポートをグループ化または表示 (Click here to group or view Email Gateway for File Analysis reporting)] オプションをクリックして、アプライアンスグループを作成します。
- ステップ3** (電子メールゲートウェイでスマートライセンスが無効になっている場合に適用) [アプライアンスID/名前 (Appliance ID/Name)] フィールドにグループIDを手動で入力し、[今すぐグループ化 (Group Now)] をクリックします。

または

(電子メールゲートウェイでスマートライセンスが有効になっている場合に適用) システムによりスマートアカウントIDがグループIDとして自動的に登録され、[アプライアンスグループID/名前 (Appliance Group ID/Name)] フィールドに表示されます。

注:

- アプライアンスは1つのグループだけに属することができます。
- マシンはいつでもグループに追加できます。
- マシンレベルまたはクラスタレベルでアプライアンスのグループを設定できます。
- これがグループに追加されている最初のアプライアンスである場合、グループにわかりやすいIDを指定します。このIDは大文字と小文字が区別され、スペースを含めることはできません。
- アプライアンスグループIDは、分析用にアップロードしたファイルのデータを共有するすべてのアプライアンスで同じである必要があります。ただし、IDはグループ内の以降のアプライアンスでは検証されません。
- アプライアンスグループIDを更新すると、変更はすぐに有効になります。確定は必要ありません。
- グループ内のすべてのアプライアンスがクラウド内の同じファイル分析サーバーを使用するように設定する必要があります。
- スマートライセンスが有効になっている場合、アプライアンスはスマートアカウントIDを使用してグループ化されます。

ファイル分析レポートのアプライアンスグループ名の更新

手順

-
- ステップ 1** [セキュリティサービス (Security Services)]>[ファイルレピュテーションと分析 (File Reputation and Analysis)] を選択します。
- ステップ 2** [ここをクリックしてファイル分析用電子メールゲートウェイレポートをグループ化または表示 (Click here to group or view Email Gateway for File Analysis reporting)] オプションをクリックします。
- ステップ 3** [ファイル分析レポートのアプライアンスのグループ化 (Appliance Grouping for File Analysis Reporting)] ページで [グループの変更 (Change Group)] をクリックします。
- (注) CLI で `ampconfig > setgroup` サブコマンドを使用してグループ ID を変更することもできます。
- ステップ 4** [アプライアンスグループID/名前 (Appliance Group ID/Name)] フィールドに名前または ID を入力し、[今すぐグループ化 (Group Now)] をクリックします。
- (注) 特定のグループ内のすべてのアプライアンスのグループ名を個別に更新する必要があります。
-

分析グループ内のアプライアンスの確認

手順

-
- ステップ 1** [セキュリティサービス (Security Services)]>[ファイルレピュテーションと分析 (File Reputation and Analysis)] を選択します。
- ステップ 2** [ここをクリックしてファイル分析用電子メールゲートウェイレポートをグループ化または表示 (Click here to group or view Email Gateway for File Analysis reporting)] オプションをクリックします。
- ステップ 3** [アプライアンスの表示 (View Appliance)] をクリックして、特定のファイル分析グループに追加されたアプライアンスを表示します。
-

ファイル分析グループ化に関するアラートの表示

以下の表では、ファイル分析レポートのためのアプライアンスのグループ化に関して生成されるシステムアラート、アラートの説明、アラートの重大度を記載します。

| コンポーネント/アラート名 | メッセージと説明 | パラメータ |
|-----------------------|---|-------------|
| AMP.ENGINE.ALERT.WARN | <p>アラートテキスト：ファイル分析グループ名を Cisco Threat Grid サーバーに登録できませんでした。Cisco TAC に連絡して、サポートを受けてください。</p> <p>アラートレベル：警告 (WARNING)。</p> <p>説明：電子メールゲートウェイが、スマートアカウント ID を使用したアプライアンスグループ名の Cisco Threat Grid サーバーへの登録に失敗すると、アラートが送信されません。</p> | パラメータ：失敗の理由 |

ファイルレピュテーションスキャンおよびファイル分析のメールポリシーの設定

手順

-
- ステップ 1** [メールポリシー (Mail Policies)] > [受信メールポリシー (Incoming Mail Policies)] または [メールポリシー (Mail Policies)] > [送信メールポリシー (Outgoing Mail Policies)] を選択します (どちらか該当するほう)。
- ステップ 2** 変更するメールポリシーの [高度なマルウェア防御 (Advanced Malware Protection)] カラム内のリンクをクリックします。
- ステップ 3** オプションを選択します。
- オンプレミスの Cisco AMP Threat Grid アプライアンスがなく、機密上の理由などからクラウドにファイルを送信したくない場合は、[ファイル分析を有効にする (Enable File Analysis)] をオフにします。
 - 添付ファイルがスキャン不可であると見なされる場合にアプライアンスが実行するアクションを選択します。アプライアンスが以下の理由でファイルをスキャンできない場合、添付ファイルはスキャン不能とみなされます。
 - **メッセージエラー：**
 - パスワードで保護されたアーカイブまたは圧縮ファイル
 - RFC 違反のあるメッセージ。

- 200 を超える子ファイルを含むメッセージ
- 5 回以上ネストされた子ファイルを含むメッセージ
- 抽出が失敗したメッセージ
- **レート制限**：アプライアンスがファイルのアップロード制限に達したために、ファイル分析サーバによってスキャンされていないファイル。
- **AMP サービスが使用不可**：
 - ファイルレピュテーションサービスが使用不可
 - ファイル分析サービスが使用不可
 - ファイルレピュテーションクエリーのタイムアウト
 - ファイルアップロードクエリーのタイムアウト
- AMP エンジンによってスキャンされないメッセージに対する、次のいずれかのメッセージ処理アクションを設定できます。
 - メッセージのドロップ
 - メッセージをそのまま配信
 - ポリシー隔離へのメッセージの送信
- メッセージを配信する場合は、次の追加の操作を選択します。
 - 元のメッセージをアーカイブするかどうか。アーカイブされたメッセージは、アプライアンスの `amparchive` ディレクトリに保管されます。事前設定された AMP アーカイブ (`amparchive`) ログサブスクリプションが必要です。
 - メッセージの件名を変更して（例：[WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]）エンドユーザーに警告するかどうか。
 - 管理者が細かく制御できるようにするために、カスタムヘッダーを追加するかどうか。
 - メッセージの受信者を変更して、メッセージが別のアドレスに送信されるようするかどうか。[はい (Yes)] をクリックして、新しい受信者のアドレスを入力します。
 - スキャンできないメッセージを代替の宛先ホストに送信するかどうか。[はい (Yes)] をクリックして代替 IP アドレスまたはホスト名を入力します。
- ポリシー隔離にメッセージを送信する場合は、次の追加の操作を選択します。
 - ドロップダウンリストからポリシー隔離を選択するかどうか。隔離のフラグが立てられている場合、メッセージは電子メールパイプラインの最後に到達すると隔離に置かれ、電子メールパイプラインの他のすべてのエンジンによってスキャンされます。

- 元のメッセージをアーカイブするかどうか。アーカイブされたメッセージは、アプライアンスの `amparchive` ディレクトリに保管されます。事前設定された AMP アーカイブ (`amparchive`) ログサブスクリプションが必要です。
 - メッセージの件名を変更して (例: [WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]) エンドユーザーに警告するかどうか。
 - 管理者が細かく制御できるようにするために、カスタム ヘッダーを追加するかどうか。
- 添付ファイルが悪意のあるファイルであると見なされる場合に AsyncOS が実行する必要があるアクションを選択します。次のことを選択します。
 - メッセージを配信するか、またはドロップするか。
 - 元のメッセージをアーカイブするかどうか。アーカイブされたメッセージは、アプライアンスの `amparchive` ディレクトリに保管されます。事前設定された AMP アーカイブ (`amparchive`) ログサブスクリプションが必要です。
 - マルウェア添付ファイルを削除した後で、メッセージを配信するかどうか。
 - メッセージの件名を変更して (例: [WARNING: MALWARE DETECTED IN ATTACHMENT(S)]) エンドユーザーに警告するかどうか。
 - 管理者が細かく制御できるようにするために、カスタム ヘッダーを追加するかどうか。
 - メッセージの受信者を変更して、メッセージが別のアドレスに送信されるようするかどうか。[はい (Yes)] をクリックして、新しい受信者のアドレスを入力します。
 - 悪意のあるメッセージを代替の宛先ホストに送信するかどうか。[はい (Yes)] をクリックして代替 IP アドレスまたはホスト名を入力します。
 - ファイル分析のために添付ファイルを送信する場合は、AsyncOS が実行すべきアクションを選択します次のことを選択します。
 - メッセージを配信するか、または隔離するか。
 - 元のメッセージをアーカイブするかどうか。アーカイブされたメッセージは、アプライアンスの `amparchive` ディレクトリに保管されます。事前設定された AMP アーカイブ (`amparchive`) ログサブスクリプションが必要です。
 - メッセージの件名を変更して (例: [WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]) エンドユーザーに警告するかどうか。
 - 管理者が細かく制御できるようにするために、カスタム ヘッダーを追加するかどうか。
 - メッセージの受信者を変更して、メッセージが別のアドレスに送信されるようするかどうか。[はい (Yes)] をクリックして、新しい受信者のアドレスを入力します。

- ファイル分析のために送信されるメッセージを代替の宛先ホストに送信するかどうか。[はい (Yes)] をクリックして代替 IP アドレスまたはホスト名を入力します。
- (着信メールポリシーの場合のみ) 脅威の判定が「悪意がある」に変更された時点でエンドユーザーに送信されるメッセージに対して実行する修復アクションを設定します。[メールボックス自動修復の有効化 (Enable Mailbox Auto Remediation)] をオンにして、以下のいずれかのアクションを選択します。
 - [電子メールアドレスに転送 (Forward to an email address)]。指定したユーザ (たとえば、電子メール管理者など) に悪意のある添付ファイルを転送する場合は、このオプションを選択します。
 - メッセージを削除します。悪意のある添付ファイルをエンドユーザーのメールボックスから完全に削除する場合は、このオプションを選択します。
 - [指定した電子メールアドレスに転送してメッセージを削除 (Forward to an email address and delete the message)]。指定したユーザ (たとえば、電子メール管理者など) に悪意のある添付ファイルを転送して、悪意のある添付ファイルをエンドユーザーのメールボックスから完全に削除する場合は、このオプションを選択します。

(注) Office 365 サービスでは特定のフォルダからのメッセージの削除をサポートしていないため、それらのフォルダ ([削除済みアイテム (Deleted Items)] など) からメッセージを削除することはできません。

重要 [メールボックス自動修復 (Mailbox Auto Remediation)] の設定を確定する前に、 [メールボックスでのメッセージの修復](#) を確認します。

ステップ 4 変更を送信し、保存します。

分析のために送信した添付ファイルがあるメッセージの隔離

分析用に送信されたファイルをただちにワークキューにリリースする代わりに、隔離するようにアプライアンスを設定できます。隔離されたメッセージとそれらの添付ファイルは、隔離からの解放時に脅威について再スキャンされます。ファイル分析結果がレピュテーションスキャナで使用できるようになった後にメッセージが解放された場合は、特定された脅威は再スキャン中に補足されます。

手順

ステップ 1 [メール ポリシー (Mail Policies)] > [受信メール ポリシー (Incoming Mail Policies)] または [メール ポリシー (Mail Policies)] > [送信メールポリシー (Outgoing Mail Policies)] を選択します (どちらか該当するほう)。

ステップ2 変更するメールポリシーの [高度なマルウェア防御 (Advanced Malware Protection)] カラム内のリンクをクリックします。

ステップ3 [ファイル分析が保留中のメッセージ (Messages with File Analysis Pending)] セクションで、[メッセージに適用するアクション (Action Applied to Message)] ドロップダウンから [隔離 (Quarantine)] を選択します。

隔離されたメッセージはファイル分析隔離エリアに保存されます。 [ファイル分析隔離の使用 \(26 ページ\)](#) を参照してください。

ステップ4 (任意) [ファイル分析が保留中のメッセージ (Messages with File Analysis Pending)] セクションで、以下のオプションを選択します。

- 元のメッセージをアーカイブするかどうか。アーカイブされたメッセージは、アプライアンスの `amparchive` ディレクトリに保管されます。事前設定された AMP アーカイブ (`amparchive`) ログ サブスクリプションが必要です。
- メッセージの件名を変更して (例: [WARNING: ATTACHMENT(S) MAY CONTAIN MALWARE]) エンドユーザーに警告するかどうか。
- アプライアンスからの最終メッセージの配信中にファイル分析の判定が保留された場合、添付ファイルをドロップするかどうかを選択できます。デフォルトのオプションは [いいえ (No)] です。
- 管理者が細かく制御できるようにするために、カスタム ヘッダーを追加するかどうか。

(注) ステップ4で説明した上記のアクションが適用されるのは、メッセージが隔離エリアからリリースされるときだけです。メッセージが隔離エリアに送信されるときには適用されません。

- 元のメッセージのアーカイブ。
- メッセージ件名の変更。
- カスタム ヘッダーの追加。

ステップ5 変更を送信し、保存します。

次のタスク

関連項目

[ファイル分析隔離の使用 \(26 ページ\)](#)

ファイル分析隔離の使用

- [ファイル分析隔離の設定の編集 \(27 ページ\)](#)
- [ファイル分析隔離領域内のメッセージの手動処理 \(28 ページ\)](#)

ファイル分析隔離の設定の編集

手順

- ステップ 1** [モニタ (Monitor)]>[ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択します。
- ステップ 2** [ファイル分析 (File Analysis)] 隔離リンクをクリックします。
- ステップ 3** 保留期間を指定します。
デフォルトの 1 時間から変更することはお勧めしません。
- ステップ 4** 保留期間経過後に AsyncOS が実行する必要があるデフォルトのアクションを指定します。
- ステップ 5** 隔離ディスクに空き領域がなくなった場合でも、指定した保持期間前にその隔離内のメッセージが処理されなくなるように設定するには、[容量オーバーフロー時にメッセージにデフォルトのアクションを適用して容量を解放します (Free up space by applying default action on messages upon space overflow)] の選択を解除します。
- ステップ 6** デフォルトのアクションとして [リリース (Release)] を選択する場合は、保留期間が経過する前にリリースされるメッセージに適用する追加のアクションを任意で指定できます。

| オプション | 情報 |
|--------------------------------|--|
| 件名の変更 (Modify Subject) | 追加するテキストを入力し、そのテキストを元の件名の前と後ろのどちらに追加するかを選択します。 たとえば、受信者にマルウェアが添付されている可能性があるメッセージであることを警告します。 (注) 非 ASCII 文字を含む件名を正しく表示するために、件名は RFC 2047 に従って表記されている必要があります。 |
| [X-Header の追加 (Add X-Header)] | X-Header にはメッセージに対して実行されたアクションを記録できます。この情報は、特定のメッセージが配信された理由についての照会を処理するときなどに役立ちます。 名前と値を入力します。 例： Name = Inappropriate-release-early Value = True |
| 添付ファイルを除去 (Strip Attachments) | 添付ファイルを削除することで、メッセージに添付されたマルウェアから保護します。 |

- ステップ 7** この隔離へのアクセスを付与するユーザーを指定します。

| ユーザー | 情報 |
|---|---|
| ローカルユーザー (Local Users) | ローカルユーザーのリストには、隔離にアクセスできるロールを持つユーザだけが含まれます。 すべての管理者は隔離に完全なアクセス権限を持つため、リストでは管理者が除外されます。 |
| 外部認証されたユーザー (Externally Authenticated Users) | 外部認証を設定しておく必要があります。 |
| カスタムユーザーロール (Custom User Roles) | このオプションは、隔離へのアクセス権限を持つ少なくとも1つのカスタムユーザーロールを作成している場合にのみ表示されます。 |

ステップ 8 変更を送信し、保存します。

ファイル分析隔離領域内のメッセージの手動処理

手順

ステップ 1 [モニタ (Monitor)] > [ポリシー、ウイルスおよびアウトブレイク隔離 (Policy, Virus, and Outbreak Quarantines)] を選択します。

ステップ 2 表のファイル分析隔離の行で、[メッセージ (Messages)] 列の青い番号をクリックします。

ステップ 3 要件に応じて、メッセージに以下のアクションを実行します。

- 削除 (Delete)
- リリース
- 隔離からのリリースの遅延
- 指定した電子メールアドレスにメッセージのコピーを送信

中央集中型のファイル分析の隔離

中央集中型ファイル分析の隔離の詳細については、『Cisco Email Security Appliance Guide』の章「Centralized Policy, Virus and Outbreak Quarantine」を参照してください。

ファイルレピュテーションと分析の X ヘッダー

Xヘッダーを使用して、メッセージ処理ステップのアクションと結果でメッセージをマークできます。メールポリシーでメッセージに X ヘッダーをタグ付けし、次にコンテンツフィルタを使用して、これらのメッセージの処理オプションと最終アクションを選択します。

値では大文字/小文字が区別されます。

| ヘッダー名 | 有効な値（大文字と小文字を区別） | 説明 |
|------------------------|---|--|
| X-Amp-Result | 正常 (Clean) 悪意のある (Malicious) スキャン不可 (Unscannable) | ファイルレピュテーションサービスにより処理されたメッセージに適用される判定。 |
| X-Amp-Original-Verdict | file unknown verdict unknown | レピュテーションしきい値に基づく調整の前の判定。このヘッダーは、元の判定が有効な値のいずれかである場合にだけ存在します。 |
| X-Amp-File-Uploaded | true false | メッセージに添付されたファイルが分析目的で送信されている場合、このヘッダーは「true」です。 |

ドロップされたメッセージまたは添付ファイルに関する通知のエンドユーザーへの送信

疑わしい添付ファイルまたはその親メッセージが、ファイルレピュテーションスキャンに基づいてドロップされる場合に、エンドユーザーに対して通知を送信するには、Xヘッダーまたはカスタムヘッダーとコンテンツフィルタを使用します。

高度なマルウェア防御とクラスタ

一元管理を使用する場合、クラスタ、グループ、およびマシンの各レベルで、高度なマルウェア防御とメールポリシーをイネーブルにできます。

ライセンスキーはマシンレベルで追加する必要があります。

アプライアンスグループをクラスタレベルで設定しないでください。

Advanced Malware Protection の問題に関するアラートの確実な受信

Advanced Malware Protectionに関連するアラートを送信するようにアプライアンスが設定されていることを確認します。

以下の場合にアラートを受信します。

| アラートの説明 | タイプ | 重大度 |
|---|------------------------------------|-------------|
| オンプレミス（プライベートクラウド）の Cisco Secure Endpoint マルウェア分析アプリケーションへの接続をセットアップし、 ファイルレピュテーションと分析サービスの有効化と設定 に説明されているようにアカウントをアクティブ化する必要があります。 | マルウェア対策 | 警告 |
| 機能キーが期限切れになりました | (すべての機能に対する標準) | |
| ファイルレピュテーションまたはファイル分析サービスに到達できません。 | ウイルス対策および AMP (Anti-Virus and AMP) | 警告 |
| クラウドサービスとの通信が確立されました。 | ウイルス対策および AMP (Anti-Virus and AMP) | 情報 (Info) |
| レピュテーションおよび分析エンジンがウォッチドッグサービスにより再起動される | ウイルス対策および AMP (Anti-Virus and AMP) | 情報 (Info) |
| ファイルレピュテーションの判定が変更されました。 | ウイルス対策および AMP (Anti-Virus and AMP) | 情報 (Info) |
| 分析用に送信できるファイルタイプが変更された。新しいファイルタイプのアップロードをイネーブルにできます。 | ウイルス対策および AMP (Anti-Virus and AMP) | 情報 (Info) |
| 一部のファイルタイプの分析が一時的に利用できません。 | ウイルス対策および AMP (Anti-Virus and AMP) | 警告 |
| サポートされているすべてのファイルタイプの分析が一時停止後に復旧されます。 | ウイルス対策および AMP (Anti-Virus and AMP) | 情報 (Info) |
| 無効なファイル分析サービスキーです。このエラーを修正するには、Cisco TAC にファイル分析 ID の詳細を連絡する必要があります。 | AMP | エラー (Error) |

関連項目

- [ファイルレピュテーションサーバまたはファイル分析サーバへの接続失敗に関する各種アラート \(36 ページ\)](#)
- [ファイルの脅威判定の変更時のアクションの実行 \(35 ページ\)](#)

Advanced Malware Protection 機能の集約管理レポートの設定

セキュリティ管理アプライアンスでレポートを集約管理する場合は、管理アプライアンスに関するオンラインヘルプまたはユーザーガイドのEメールレポートのトピックの「Advanced Malware Protection」セクションで、重要な設定要件を確認してください。

ファイルレピュテーションおよびファイル分析のレポートとトラッキング

- [SHA-256 ハッシュによるファイルの識別 \(31 ページ\)](#)
- [ファイルレピュテーションとファイル分析レポートのページ \(32 ページ\)](#)
- [その他のレポートでのファイルレピュテーションフィルタデータの表示 \(34 ページ\)](#)
- [メッセージトラッキング機能と Advanced Malware Protection 機能について \(34 ページ\)](#)

SHA-256 ハッシュによるファイルの識別

ファイル名は簡単に変更できるため、アプライアンスはセキュアハッシュアルゴリズム (SHA-256) を使用して各ファイルの ID を生成します。アプライアンスが名前の異なる同じファイル进行处理する場合、すべてのインスタンスが同じ SHA-256 として認識されます。複数のアプライアンスが同じファイル进行处理する場合、ファイルのすべてのインスタンスには同じ SHA-256 ID があります。

ほとんどのレポートでは、ファイルはその SHA-256 値でリストされます (短縮形式

ファイルレピュテーションとファイル分析レポートのページ

| レポート | 説明 |
|-----------------------------|--|
| Advanced Malware Protection | <p>ファイルレピュテーションサービスによって特定されたファイルベースの脅威を示します。</p> <p>判定が変更されたファイルについては、[AMP 判定のアップデート (AMP Verdict Updates)] レポートを参照してください。これらの判定は、[高度なマルウェア防御 (Advanced Malware Protection)] レポートに反映されません。</p> <p>圧縮ファイルまたはアーカイブ済みファイルから悪意のあるファイルが抽出された場合、圧縮ファイルまたはアーカイブ済みファイルの SHA 値のみが [高度なマルウェア防御 (Advanced Malware Protection)] レポートに含まれます。</p> <p>[カテゴリ別受信マルウェアファイル (Incoming Malware Files by Category)] セクションは、[カスタム検出 (Custom Detection)] に分類される、AMP for Endpoints コンソールから受信したブロックリストに登録されたファイル SHA の割合を示しています。</p> <p>AMP for Endpoints コンソールから取得されるブロックリストに登録されているファイル SHA の脅威名は、レポートの [受信したマルウェア脅威ファイル (Incoming Malware Threat Files)] セクションで [シンプルカスタム検出 (Simple Custom Detection)] として表示されます。</p> <p>レポートの [詳細 (More Details)] セクションでリンクをクリックすると、AMP for Endpoints コンソールでのブロックリストに登録されているファイル SHA のファイルトラジェクトリ詳細を表示できます。</p> <p>[リスク低 (Low Risk)] 判定の詳細をレポートの [AMP により渡された受信ファイル (Incoming Files Handed by AMP)] セクションに表示できます。</p> |

| レポート | 説明 |
|--|---|
| <p>Advanced Malware Protection [ファイル分析 (File Analysis)]</p> | <p>分析用に送信された各ファイルの時間と判定（または中間判定）を表示します。SMA アプライアンスは 30 分ごとに WSA で分析結果をチェックします。</p> <p>1000 を超えるファイル分析結果を表示するには、データを .csv ファイルとしてエクスポートします。</p> <p>ドリルダウンすると、各ファイルの脅威の特性を含む詳細な分析結果が表示されます。</p> <p>SHA に関するその他の情報を検索するか、またはファイル分析詳細ページの下部のリンクをクリックして、ファイルを分析したサーバに関する追加の詳細を表示することもできます。</p> <p>(注) 圧縮/アーカイブ ファイルから抽出したファイルが分析用に送信される場合は、それらの抽出ファイルの SHA 値だけが [ファイル分析 (File Analysis)] レポートに含まれます。</p> |
| <p>Advanced Malware Protection レピュテーション</p> | <p>Advanced Malware Protection は対象を絞ったゼロデイ脅威に焦点を当てるため、集約データでより詳細な情報が提供されると、脅威の判定が変わる可能性があります。</p> <p>[AMP レピュテーション (AMP Reputation)] レポートには、このアプライアンスで処理され、メッセージ受信後に判定が変わったファイルが表示されます。この状況の詳細については、ファイル脅威判定のアップデート (2 ページ) を参照してください。</p> <p>1000 を超える判定アップデートを表示するには、データを .csv ファイルとしてエクスポートします。</p> <p>1 つの SHA-256 に対して判定が複数回変わった場合は、判定履歴ではなく最新の判定のみがこのレポートに表示されます。</p> <p>使用可能な最大時間範囲内（レポートに選択された時間範囲に関係なく）に特定の SHA-256 の影響を受けるすべてのメッセージを表示するには、SHA-256 リンクをクリックします。</p> |

その他のレポートでのファイルレピュテーションフィルタ データの表示

該当する場合は、ファイルレピュテーションおよびファイル分析のデータを他のレポートでも使用できます。デフォルトでは、[]列は適用可能なレポートに表示されません。追加列を表示するには、テーブルの下の [列 (Columns)] リンクをクリックします。

メッセージトラッキング機能と Advanced Malware Protection 機能について

メッセージトラッキングでファイル脅威情報を検索するときには、以下の点に注意してください。

- ファイルレピュテーションサービスにより検出された悪意のあるファイルを検索するには、Web メッセージトラッキングの [詳細設定 (Advanced)] セクションの [メッセージイベント (Message Event)] オプションで [高度なマルウェア防御反応ポジティブ (Advanced Malware Protection Positive)] を選択します。
- メッセージトラッキングには、ファイルレピュテーション処理に関する情報と、トランザクションメッセージの処理時点で戻された元のファイルレピュテーション判定だけが含まれます。たとえば最初にファイルがクリーンであると判断され、その後、判定のアップデートでそのファイルが悪質であると判断された場合、クリーンの判定のみがトラッキング結果に表示されます。

メッセージトラッキングの詳細の [処理詳細 (Action Details)] セクションには、以下の情報が表示されます。

- メッセージの各添付ファイルの SHA-256
- メッセージ全体での最終的な Advanced Malware Protection 判定。
- マルウェアが検出された添付ファイル
- 判定の更新は [AMP 判定の更新 (AMP Verdict Updates)] レポートだけに表示されます。メッセージトラッキングの元のメッセージの詳細は、判定の変更によって更新されません。特定の添付ファイルが含まれているメッセージを確認するには、判定アップデートレポートで SHA-256 リンクをクリックします。
- 分析結果や分析用にファイルが送信済みかどうかといった、ファイル分析に関する情報は [ファイル分析 (File Analysis)] レポートにのみ表示されます。

分析済みファイルのその他の情報は、クラウドまたはオンプレミスのファイル分析サーバーから入手できます。ファイルについて使用可能なすべてのファイル分析情報を確認するには、[レポート (Reporting)] [モニタリング (Monitor)] > [ファイル分析 (File Analysis)] を選択し、ファイルで検索する SHA-256 を入力します。ファイル分析サービスによってソースのファイルが分析されると、その詳細を表示できます。分析されたファイルの結果だけが表示されます。

分析目的で送信されたファイルの後続インスタンスがアプライアンスにより処理される場合、これらのインスタンスは、メッセージトラッキング検索結果に表示されます。

ファイルの脅威判定の変更時のアクションの実行

手順

- ステップ 1** [AMP 判定の更新 (AMP Verdict updates)] レポートを表示します。
- ステップ 2** 該当する SHA-256 リンクをクリックします。ファイルを含むメッセージのトラッキングデータが表示されます。
- ステップ 3** トラッキングデータを使用して、侵害された可能性があるユーザと、違反に関連するファイルの名前やなどの情報を特定します。
- ステップ 4** ファイルの脅威の動作を詳細に把握するために、[ファイル分析 (File Analysis)] レポートを検証して、この SHA-256 が分析用に送信されたかどうかを確認します。

次のタスク

関連項目

[ファイル脅威判定のアップデート \(2 ページ\)](#)

ファイルレピュテーションと分析のトラブルシューティング

- [ログ ファイル \(35 ページ\)](#)
- [トレースの使用 \(36 ページ\)](#)
- [ファイルレピュテーションサーバまたはファイル分析サーバへの接続失敗に関する各種アラート \(36 ページ\)](#)
- [API キーのエラー \(オンプレミスのファイル分析\) \(37 ページ\)](#)
- [ファイルが予想どおりにアップロードされない \(38 ページ\)](#)
- [分析のために送信できるファイルタイプに関するアラート \(38 ページ\)](#)

ログ ファイル

ログの説明：

- AMP と amp は、ファイルレピュテーションサービスまたはエンジンを示しています。
- Retrospective は判定のアップデートを示しています。

- VRT と sandboxing はファイル分析サービスを示しています。

ファイル分析を含む Advanced Malware Protectionに関する情報は、または AMP エンジンのログ。

ファイルレピュテーションフィルタリングおよび分析のイベントは、AMP エンジンログとメールログに記録されます。

ログメッセージ「ファイルレピュテーションクエリーに対する受信応答 (Response received for file reputation query)」の「アップロードアクション (upload action)」の値は以下のようになります。

- 1: 送信。(1: SEND.) この場合、ファイル分析のためにファイルを送信する必要があります。
- 2: 送信しない。(2: DON'T SEND.) この場合は、ファイル分析用にファイルを送信しません。
- 3: メタデータのみを送信。(3: SEND ONLY METADATA.) この場合、ファイル分析のためにファイル全体ではなく、メタデータのみを送信します。
- 0: アクションなし。(0: NO ACTION.) この場合、他のアクションは不要です。

メールログの「処理 (Disposition)」の値は、以下のようになります。

- 1: マルウェアが検出されない、または正常であると推測される (正常として処理)
- 2: 正常
- 3: マルウェア

「Spyname」は脅威の名前です。

トレースの使用

ファイルレピュテーションフィルタおよび分析機能ではトレースは使用できません。代わりに、組織外のアカントからテストメッセージを送信します。

ファイルレピュテーションサーバまたはファイル分析サーバへの接続失敗に関する各種アラート

問題

ファイルレピュテーションサービスまたは分析サービスへの接続の失敗に関するアラートをいくつか受信した。(単一のアラートは一時的な問題のみを示していることがあります。)

解決方法

- [ファイルレピュテーションと分析サービスとの通信の要件 \(7 ページ\)](#) に記載されている要件を満たしていることを確認します。

- アプライアンスとクラウドサービスとの通信を妨げている可能性があるネットワークの問題を確認します。
- [クエリー タイムアウト (Query Timeout)] の値を大きくします。

[セキュリティサービス (Security Services)] [ファイルレピュテーションと分析 (File Reputation and Analysis)] を選択します。の [詳細設定 (Advanced settings)] エリアの [クエリタイムアウト (Query Timeout)] の値。

API キーのエラー（オンプレミスのファイル分析）

問題

ファイル分析レポートの詳細を表示しようとした場合や、分析用ファイルをアップロードするのに E メールセキュリティ アプライアンスが Cisco Secure Endpoint マルウェア分析サーバーに接続できない場合、API キーのアラートを受信します。

解決方法

このエラーは、Cisco Secure Endpoint マルウェア分析サーバーのホスト名を変更し、Cisco Secure Endpoint マルウェア分析サーバーの自己署名証明書を使用する場合に発生します。また、他の状況でも発生する可能性があります。この問題を解決するには、次の手順を実行します。

- 新しいホスト名がある AMP マルウェア分析アプライアンスから新しい証明書を生成します。
- E メールセキュリティ アプライアンスに新しい証明書をアップロードします。
- AMP マルウェア分析アプライアンスの API キーをリセットします。手順については、AMP マルウェア分析アプライアンスのオンラインヘルプを参照してください。

関連項目

- [ファイルレピュテーションと分析サービスの有効化と設定](#)

API キーエラー（パブリッククラウドファイル分析）

問題

ファイル分析レポート用にアプライアンスを表示またはグループ化しようとした場合や、分析用ファイルをアップロードするのに電子メールゲートウェイが Cisco Threat Grid サーバーに接続できない場合、API キーのアラートが送信されます。

解決方法

このエラーは、Cisco Threat Grid サーバーに到達できない場合に発生する可能性があります。次のことを確認して、もう一度接続してみてください。

- 地域の正しい Threat Grid サーバーに接続していること。
- Threat Grid サーバーが現在動作していること。

関連項目

- (パブリッククラウドファイル分析サービスのみ) [アプライアンスグループの設定 \(19ページ\)](#)

ファイルが予想どおりにアップロードされない

問題

ファイルが予想どおりに評価または分析されていません。アラートまたは明らかなエラーはありません。

解決方法

以下の点に注意してください。

- ファイルが他のアプライアンスによる分析用に送信されているために、すでにファイル分析サーバ、またはそのファイルを処理するアプライアンスのキャッシュに存在している可能性があります。

分析のために送信できるファイルタイプに関するアラート

問題

ファイル分析のために送信できるファイルタイプに関する重大度情報のアラートを受け取れません。

解決方法

このアラートは、サポート対象のファイルタイプが変更された場合や、アプライアンスがサポート対象のファイルタイプを確認した場合に送信されます。これは、以下の場合に発生する可能性があります。

- 自分または別の管理者が分析用に選択されているファイルタイプを変更した。
- サポート対象のファイルタイプがクラウドサービスでの可用性に基づいて一時的に変更された。この場合、アプライアンスで選択されたファイルタイプのサポートは可能な限り迅速に復旧されます。どちらのプロセスも動的であり、ユーザによる操作は必要ありません。
- アプライアンスが再起動した (たとえば、AsyncOS のアップグレードの一環として) 。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。