



# 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 \(19 ページ\)](#)
- [ファイルの脅威判定の変更時のアクションの実行 \(22 ページ\)](#)
- [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 \(23 ページ\)](#)

## 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

高度なマルウェア防御は、次によりゼロデイや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に通知する。

この機能はファイルのダウンロードに使用できます。アップロードされたファイル

ファイルレピュテーション サービスはクラウドに存在します。ファイル分析サービスには、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）のオプションがあります。

- 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 AMP 仮想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ビスの設定 \(9 ページ\)](#) 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 Threat Grid アプライアンスから提供されます。 [オンプレミスのファイル分析サーバの設定（10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

脅威判定は、新たな情報に合わせて変更できます。最初にファイルが不明または正常として評価されると、ユーザがこのファイルにアクセスできます。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トランザクションを調査できます。

判定を、「悪意がある」から「正常」に変更できます。

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（19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（22ページ）](#)

## ファイル処理の概要

最初に、ファイルのダウンロード元の Web サイトが Web ベースレピュテーションサービス (WBRS) に対して評価されます。

サイトの Web レピュテーションスコアが「スキャン」に設定される範囲内である場合、アプライアンスはマルウェアについてトランザクションをスキャンすると同時に、ファイルのレピュテーションについてクラウドベースサービスに問い合わせます。(サイトのレピュテーションスコアが「ブロック」の範囲内である場合、トランザクションは適宜に処理され、ファイルをさらに処理する必要はありません)。スキャン中にマルウェアが検出された場合は、ファイルレピュテーションに関係なく、トランザクションがブロックされます。

[[適応型スキャン \(Adaptive Scanning\)](#)] もイネーブルになっている場合は、ファイルレピュテーションの評価とファイル分析が適応型スキャンに含まれます。

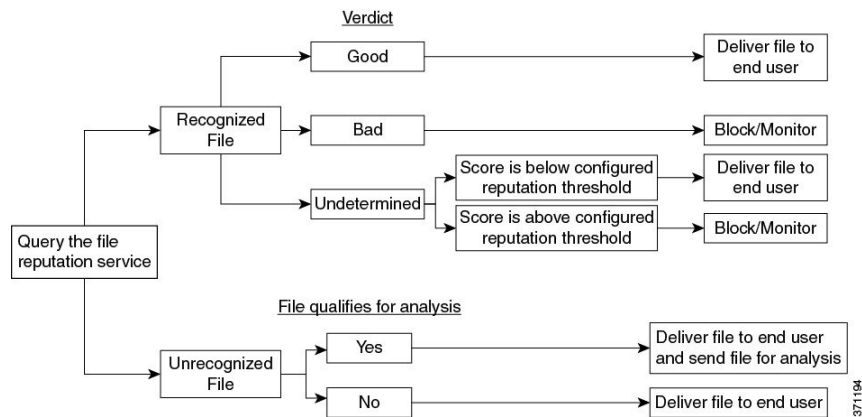
アプライアンスとファイルレピュテーションサービス間の通信は暗号化され、改ざんから保護されます。

ファイルレピュテーションの評価後：

- 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、ファイルはエンドユーザに対して解放されます。

- ファイルレピュテーションサービスから悪意があるという判定が返されると、このようなファイルに対して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、脅威スコアを戻します。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、悪意がある、またはリスクの高いファイルに関するアクセス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、エンドユーザーに解放されます。
- クラウドベースのファイル分析サービスを有効にしており、レピュテーションサービスにそのファイルの情報がなく、そのファイルが分析できるファイルの基準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）は、ファイルは正常と見なされ、任意で分析用に送信されます。
- 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、そのファイルはユーザーに解放されますが、ファイル分析の結果がローカルキャッシュで更新され、そのファイルのインスタンスの以降の評価に使用されます。
- 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: クラウドファイル分析の展開のための高度なマルウェア防御のワークフロー



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 AMP Threat Grid 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大部分のファイルタイプを評価します。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」となっているファイルは脅威の特徴と対比して分析できます。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、

<http://www.cisco.com/c/en/us/support/security/web-security-appliance/products-user-guide-list.html> から入手できます。ファイルのレピュテーションの評価と分析のためにファイルを送信する基準は、随時変更される場合があります。

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。

[セキュリティ サービス (Security Services)] > [マルウェア対策およびレピュテーション (Anti-Malware and Reputation)] ページの [DVS エンジンオブジェクトスキャンの制限 (DVS Engine Object Scanning Limits)] の設定も、ファイルレピュテーションと分析の最大ファイルサイズを決定します。

高度なマルウェア防御が対応しないファイルのダウンロード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](#) (11 ページ)
- [高度なマルウェア防御の問題に関連するアラートの受信の確認](#) (17 ページ)
- [アーカイブまたは圧縮されたファイルの処理](#) (5 ページ)

## アーカイブまたは圧縮されたファイルの処理

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調査するアーカイブファイルおよび圧縮ファイルの詳細については、[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) からリンクされている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)。
- 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)。



---

(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 AMP Threat Grid アプライアンスで分析されたファイルの詳細は、レピュテーションサービスと共有されることはありません。

## 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](#) (6 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](#) (9 ページ)
- [オンプレミスのファイル分析サーバの設定](#) (10 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](#) (11 ページ)
- [\(パブリッククラウドファイル分析サービスのみ\) アプライアンスグループの設定](#) (15 ページ)
- [アクセスポリシーごとのファイルレピュテーションおよび分析サービスのアクションの設定](#) (17 ページ)
- [高度なマルウェア防御の問題に関連するアラートの受信の確認](#) (17 ページ)
- [高度なマルウェア防御機能の集約管理レポートの設定](#) (18 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すべての Web セキュリティ アプライアンスは、インターネットを通じてそれらのサービスに直接接続可能である必要があります (オンプレミスの Cisco AMP Threat Grid アプライアンスを使用するように設定されたファイル分析サービスを除く)。
- 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との通信は、アプライアンスの管理ポート (M1) 経由でルーティングされます。アプライアンスが管理ポートを使用してデータをルーティングしていない場合は、[データインターフェイス経由でのファイルレピュテーションサーバおよびファイル分析サーバへのトラフィックのルーティング](#) (7 ページ) 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。
- 以下のファイアウォールポートが開いている必要があります。

ファイアウォールポート	説明	プロトコル	入力/出力	ホストネーム	アプライアンスのインターフェイス
32137 (デフォルト) または 443	ファイルレピュテーションを取得するためにクラウドサービスにアクセスします。	[TCP]	発信 (Out)	[セキュリティ サービス (Security Services)] > [マルウェア対策とレピュテーション (Anti-Malware and Reputation)] の [詳細設定 (Advanced)] セクション: [ファイルレピュテーションの詳細設定 (Advanced Settings for File Reputation)] の [クラウドサーバプール (Cloud Server Pool)] パラメータで設定された名前。	データポートを介してこのトラフィックをルーティングするようにスタティックルートが設定されていない場合は、管理インターフェイス。
443	ファイル分析のためにクラウドサービスにアクセスします。	[TCP]	発信 (Out)	[セキュリティサービス (Security Services)] > [マルウェア対策とレピュテーション (Anti-Malware and Reputation)] の [詳細設定 (Advanced)] セクション: [ファイル分析の詳細設定 (Advanced Settings for File Analysis)] で設定された名前。	

- ファイルレピュテーション機能を設定する際は、ポート 443 で SSL を使用するかどうかを選択します。

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 \(11 ページ\)](#)

## データインターフェイス経由でのファイルレピュテーションサーバおよびファイル分析サーバへのトラフィックのルーティング

([ネットワーク (Network)] > [インターフェイス (Interfaces)] ページで) アプライアンスの管理ポートがアプライアンス管理サービス専用設定されている場合は、代わりに、データポートを介してファイルレピュテーションおよび分析のトラフィックをルーティングするように、アプライアンスを設定します。

[ネットワーク (Network)] > [ルート (Routes)] ページでデータトラフィックのルートを追加します。一般的な要件と手順については、次を参照してください。 [TCP/IP トラフィックルートの設定](#)

接続先	宛先ネットワーク	ゲートウェイ
<p>ファイルレピュテーションサービス</p>	<p>[セキュリティサービス (Security Services) ] &gt; [マルウェア対策とレピュテーション (Anti-Malware and Reputation) ] の [詳細設定 (Advanced) ] セクション &gt; [ファイルレピュテーションの詳細設定 (Advanced Settings for File Reputation) ] セクションで、 [ファイルレピュテーションサーバ (File Reputation Server) ] にファイルレピュテーションサーバの名前 (URL) を指定し、 [クラウドドメイン (Cloud Domain) ] にクラウドサーバプールのクラウドドメインを指定します。</p> <p>ファイルレピュテーションサーバのプライベートクラウドを選択する場合は、サーバのホスト名または IP アドレスを入力し、有効な公開キー指定します。これは、プライベートクラウドアプライアンスで使用されるキーと同じである必要があります。</p> <p>[セキュリティサービス (Security Services) ] &gt; [マルウェア対策とレピュテーション (Anti-Malware and Reputation) ] の [詳細設定 (Advanced) ] セクション : [ファイルレピュテーションの詳細設定 (Advanced Settings for File Reputation) ] で設定されているクラウドサーバプールのホスト名。</p>	<p>データポートのゲートウェイの IP アドレス。</p>



接続先	宛先ネットワーク	ゲートウェイ
<p>ファイル分析サービス</p>	<ul style="list-style-type: none"> <li>• [セキュリティサービス (Security Services) ] &gt; [マルウェア対策とレピュテーション (Anti-Malware and Reputation) ] の [詳細設定 (Advanced) ] セクション &gt; [ファイルレピュテーションの詳細設定 (Advanced Settings for File Reputation) ] セクションの [ファイル分析サーバ (File Analysis Server) ] に、ファイル分析サーバの名前 (URL) を指定します。</li> </ul> <p>ファイル分析サーバのプライベートクラウドを選択する場合は、サーバ URL と有効な認証局を指定します。</p> <ul style="list-style-type: none"> <li>• ファイル分析クライアント ID は、ファイル分析サーバでのこのアプライアンスのクライアント ID です (読み取り専用)。</li> </ul> <p>[セキュリティサービス (Security Services) ]、[マルウェア対策とレピュテーション (Anti-Malware and Reputation) ] の [詳細設定 (Advanced) ] セクション: [ファイル分析の詳細設定 (Advanced Settings for File Analysis) ] で設定されているファイル分析サーバのホスト名。</p>	<p>データポートのゲートウェイの IP アドレス。</p>

関連項目

- [TCP/IP トラフィック ルートの設定](#)

## 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 AMP 仮想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> [英語] 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 AMP仮想プライベートアプライアンスを設定および構成します。
- Cisco AMP仮想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、Cisco Webセキュリティアプライアンスとの統合を可能にするバージョン2.2であることを確認します。
- AMP仮想プライベートクラウドの証明書およびキーをこのアプライアンスにダウンロードして、このWebセキュリティアプライアンス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を設定した後に、このWebセキュリティアプライアンスからこのサーバへの接続を設定します。以下のステップ6を参照してください。[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（11ページ）](#)

## オンプレミスのファイル分析サーバの設定

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

- 『Cisco AMP Threat Grid Appliance Setup and Configuration Guide』および『Cisco AMP Threat Grid Appliance Administration Guide』を入手します。Cisco AMP Threat Grid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%20list.html> [\[英語\]](#) 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。

AMP Threat Gridアプライアンスのヘルプリンクからその他のドキュメントも入手できます。

管理ガイドでは、別のシスコアプライアンスとの統合、CSA、Cisco Sandbox API、WSA、Webセキュリティアプライアンスなどに関する情報を提供しています。

- Cisco AMP Threat Gridアプライアンスをセットアップし、設定します。
- 必要に応じて、Cisco AMP Threat GridアプライアンスソフトウェアをCisco Webセキュリティアプライアンスとの統合をサポートするバージョン1.2.1へ更新します。

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 Threat Grid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 Webセキュリティアプライアンスは、AMP Threat Grid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、Webセキュリティアプライアンスで使用されるCisco AMP Threat Gridアプライアンスから自己署名SSL証明書を生成します。SSL証明書とキー

をダウンロードする手順については、AMP Threat Grid アプライアンスの管理者ガイドを参照してください。AMP Threat Grid アプライアンスのホスト名を CN として持つ証明書を生成してください。AMP Threat Grid アプライアンスのデフォルトの証明書は機能しません。

- Threat Grid アプライアンスへの Web 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 \(11 ページ\)](#) で説明したようにファイル分析の設定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。



- (注) オンプレミスのファイル分析サーバを設定した後に、この Web セキュリティ アプライアンスからこのサーバへの接続を設定します。以下のステップ 7 を参照してください。[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 \(11 ページ\)](#)

## 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

### 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。アプライアンスへの機能キーの追加については、[機能キーの使用](#)を参照してください。
- [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 \(6 ページ\)](#) を満たします。
- ファイルレピュテーションおよび分析サービスにデータ ネットワーク インターフェイスを使用する場合は、アプライアンスでデータ ネットワーク インターフェイスがイネーブルになっていることを確認します。参照先 [ネットワーク インターフェイスのイネーブル化または変更](#)
- [アップグレードおよびサービス アップデートの設定](#) 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 AMP 仮想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 \(9 ページ\)](#) を参照してください。
- Cisco AMP Threat Grid 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 \(10 ページ\)](#) を参照してください。

**ステップ 1** [セキュリティサービス (Security Services) ] > [マルウェア対策とレピュテーション (Anti-Malware and Reputation) ] 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。

**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
クラウドドメイン (Cloud Domain)	ファイルレピュテーションクエリーに使用するドメインの名前。
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"> <li>• [サーバ (Server)] : Cisco AMP 仮想プライベートクラウドアプライアンスのホスト名または IP アドレス。</li> <li>• [公開キー (Public Key)] : 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公開キーを入力します。これは、プライベートクラウドサーバで使用されるキーと同じである必要があります。このアプライアンス上のキーファイルの位置を指定して、[ファイルのアップロード (Upload File)] をクリックします。</li> </ul> <p>(注) 事前にサーバからこのアプライアンスにキーファイルをダウンロードしておく必要があります。</p>
着信サービス一覧 (Routing Table)	高度なマルウェア防御サービスで使用されるルーティングテーブル。アプライアンスのネットワークインターフェイスタイプ (管理またはデータ) に関連付けられています。アプライアンスで管理インターフェイスと 1 つ以上のデータインターフェイスがイネーブルになっている場合は、[管理 (Management)] または [データ (Data)] を選択できます。

オプション	説明
ファイルレピュテーション用のSSL通信 (SSL Communication for File Reputation)	<p>デフォルトポート (32137) ではなくポート443で通信するには、[SSL (ポート443) の使用 (Use SSL (Port 443))] をオンにします。サーバへのSSHアクセスを有効にする方法については、Cisco AMP 仮想プライベートクラウドアプライアンスのユーザガイドを参照してください。</p> <p>(注) ポート32137でSSL通信を行うには、ファイアウォールでこのポートを開く必要があります。</p> <p>このオプションを使用すると、ファイルレピュテーションサービスとの通信用にアップストリームプロキシを設定できます。オンにする場合、[サーバ (Server)]、[ユーザ名 (Username)]、[パスフレーズ (Passphrase)] に適切な情報を入力します。</p> <p>[SSL (ポート443) の使用 (Use SSL (Port 443))] がオンにされている場合、[証明書検証の緩和 (Relax Certificate Validation)] もオンにすると、(トンネルプロキシサーバの証明書に信頼できるルート認証局の署名がない場合に) 標準の証明書検証をスキップできます。たとえば信頼できる内部トンネルプロキシサーバの自己署名証明書を使用している場合は、このオプションをオンにします。</p> <p>(注) [ファイルレピュテーションの詳細設定 (Advanced Settings for File Reputation)] の [ファイルレピュテーションのSSL通信 (SSL Communication for File Reputation)] セクションで [SSL (ポート443) の使用 (Use SSL (Port 443))] をオンにした場合、Web インターフェイスの [ネットワーク (Network)] &gt; [証明書 (カスタム認証局) (Certificates (Custom Certificate Authorities))] を使用して AMP オンプレミスレピュテーションサーバCA証明書を追加する必要があります。この証明書をサーバから取得します ([設定 (Configuration)] &gt; [SSL] &gt; [クラウドサーバ (Cloud server)] &gt; [ダウンロード (download)] ) 。</p>
ハートビート間隔 (Heartbeat Interval)	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)。
レピュテーションしきい値 (Reputation Threshold)	<p>許容されるファイルレピュテーションスコアの上限。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。</p> <ul style="list-style-type: none"> <li>• クラウドサービスの値を使用 (60) (Use value from Cloud Service (60))</li> <li>• [カスタム値の入力 (Enter Custom Value)] : デフォルトでは 60 に設定されます。</li> </ul>
クエリータイムアウト (Query Timeout)	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。
処理のタイムアウト (Processing Timeout)	ファイルの処理がタイムアウトになるまでの経過秒数。

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)

(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 6** 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)	<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 AMP Threat Grid 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"> <li>• [サーバ (Server) ] : オンプレミス プライベート分析クラウドサーバの URL。</li> <li>• [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。</li> </ul> <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>
ファイル分析クライアント ID (File Analysis Client ID)	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)

**ステップ 7** (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 8** 変更を送信し、保存します。

**ステップ 9** オンプレミスの Cisco AMP Threat Grid アプライアンスを使用している場合は、AMP Threat Grid 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にします。

「ユーザ」アカウントをアクティブにするための完全な手順は、AMP Threat Grid 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) AMP Threat Grid 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) Web 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 に応じた「ユーザ」アカウントを指定します。
- 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。

## 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 Threat Grid 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。



- (注) マシンレベルでアプライアンスのグループを設定できます。アプライアンスのグループは、クラスタ レベルで設定することはできません。

**ステップ 1** [セキュリティサービス (Security Services)] > [マルウェア対策とレピュテーション (Anti-Malware and Reputation)] を選択します。

**ステップ 2** [ファイル分析クラウドレポートのためのアプライアンスのグループ化 (Appliance Grouping for File Analysis Cloud Reporting)] セクションで、ファイル分析クラウドレポート グループ ID を入力します。

- 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。
- 指定した 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 は以降のグループ アプライアンスでは検証されません。
- 不正なグループ ID を入力したか、または他の何らかの理由でグループ ID を変更する必要がある場合は、Cisco TAC に問い合わせる必要があります。
- この変更はすぐに反映されます。コミットする必要はありません。
- 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を使用するように設定する必要があります。
- 1 つのアプライアンスは、1 つのグループだけに属することができます。
- いつでもグループにマシンを追加できますが、追加できるのは一度のみです。

**ステップ 3** [アプライアンスをグループに追加 (Add Appliance to Group)] をクリックします。

## 分析グループ内のアプライアンスの確認

**ステップ 1** [セキュリティサービス (Security Services)] > [マルウェア対策とレピュテーション (Anti-Malware and Reputation)] を選択します。

**ステップ 2** [ファイル分析クラウドレポートの用のアプライアンスのグループ化 (Appliance Grouping for File Analysis Cloud Reporting)] セクションで、[グループ内のアプライアンスの表示 (View Appliances in Group)] をクリックします。

**ステップ 3** 特定のアプライアンスのファイル分析クライアント ID を表示するには、以下の場所を参照します。

アプライアンス	ファイル分析クライアント ID の場所
E メール セキュリティ アプライアンス	[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 [ファイル分析の詳細設定 (Advanced Settings for File Analysis)] セクション
Web セキュリティ アプライアンス	[セキュリティ サービス (Security Services)] > [マルウェア対策とレピュテーション (Anti-Malware and Reputation)] ページの [ファイル分析の詳細設定 (Advanced Settings for File Analysis)] セクション



アプライアンス	ファイル分析クライアント ID の場所
セキュリティ管理アプライアンス	[管理アプライアンス (Management Appliance) ]>[集約管理サービス (Centralized Services) ]>[セキュリティアプライアンス (Security Appliances) ] ページの下部

## アクセスポリシーごとのファイルレピュテーションおよび分析サービスのアクションの設定

- ステップ 1** [Web セキュリティ マネージャ (Web Security Manager) ]>[アクセス ポリシー (Access Policies) ] を選択します。
- ステップ 2** テーブルの [マルウェア対策とレピュテーション (Anti-Malware and Reputation) ] 列にあるポリシーのリンクをクリックします。
- ステップ 3** [高度なマルウェア防御設定 (Advanced Malware Protection Settings) ] セクションで、[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を有効にする (Enable File Reputation Filtering and File Analysis) ] を選択します。
- ファイル分析がグローバルにイネーブルになっていない場合は、ファイルレピュテーションフィルタリングだけが表示されます。
- ステップ 4** [悪意のある既知の高リスク ファイル (Known Malicious and High-Risk Files) ] に対してアクション ([モニタ (Monitor) ] または [ブロック (Block) ]) を選択します。
- デフォルトは [モニタ (Monitor) ] です。
- ステップ 5** 変更を送信し、保存します。

## 高度なマルウェア防御の問題に関連するアラートの受信の確認

高度なマルウェア防御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 (Type)	重大度 (Severity)
オンプレミス (プライベートクラウド) の Cisco AMP Threat Grid への接続をセットアップし、以下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。 <a href="#">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 (11 ページ)</a>	マルウェア対策 (Anti-Malware)	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。	マルウェア対策 (Anti-Malware)	警告
クラウドサービスとの通信が確立されました。	マルウェア対策 (Anti-Malware)	情報 (Info)
		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。	マルウェア対策 (Anti-Malware)	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。	マルウェア対策 (Anti-Malware)	情報 (Info)
一部のファイルタイプの分析を一時的に利用できません。	マルウェア対策 (Anti-Malware)	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。	マルウェア対策 (Anti-Malware)	情報 (Info)

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 \(23 ページ\)](#)
- [ファイルの脅威判定の変更時のアクションの実行 \(22 ページ\)](#)

## 高度なマルウェア防御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ガイドの **Web レポーティング** の章の高度なマルウェア防御に関するセクションで、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 \(19 ページ\)](#)
- [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 \(20 ページ\)](#)
- [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 \(21 ページ\)](#)
- [Web トラッキング機能と高度なマルウェア防御機能について \(21 ページ\)](#)

## 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)。組織のマルウェア インスタンスに関連付けられたファイル名を特定するには、[レポート (Reporting)] > [高度なマルウェア防御 (Advanced Malware Protection)] を選択し、テーブルの SHA-256 リンクをクリックします。関連付けられたファイル名が詳細ページに表示されます。

## 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
[高度なマルウェア防御 (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>各 SHA にアクセスしようとしたユーザ、およびその SHA-256 に関連付けられたファイル名を表示するには、テーブルの SHA-256 リンクをクリックします。</p> <p>[マルウェア脅威ファイルの詳細 (Malware Threat File Details) ] レポートページの下部にあるリンクをクリックすると、レポート用に選択された時間範囲に関係なく使用可能な最大時間範囲内に検出された、Web トラッキング内のファイルのすべてのインスタンスが表示されます。</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>(注) 圧縮/アーカイブファイルから抽出したファイルの1つが悪意のあるファイルである場合は、圧縮/アーカイブファイルのSHA値だけが[高度なマルウェア防御 (Advanced Malware Protection) ] レポートに含まれます。</p>
[高度なマルウェア防御 (Advanced Malware Protection) ] におけるファイル分析	<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。</p> <p>Cisco AMP Threat Grid アプライアンスでホワイトリスティングされたファイルは、「正常 (clean) 」として表示されます。ホワイトリストについては、AMP Threat Grid のオンラインヘルプを参照してください。</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およびスコアを含む詳細な分析結果が表示されます。</p> <p>また、分析を実行した AMP Threat Grid アプライアンスまたはクラウドサーバで SHA に関する追加の詳細を直接表示するには、SHA を検索するか、またはファイル分析の詳細ページ下部にある Cisco AMP Threat Grid リンクをクリックします。</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>

レポート	説明
[高度なマルウェア防御 (Advanced Malware Protection) ]の判定の更新	<p>このアプライアンスにより処理されており、かつトランザクションが処理された時点以降に判定が変更されたファイルの一覧を示します。この状況の詳細については、<a href="#">ファイル脅威判定のアップデート (2 ページ)</a> 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>SHA-256 リンクをクリックすると、レポート用に選択された時間範囲に関係なく、使用可能な最大時間範囲において、この SHA-256 が含まれたすべてのトランザクションの Web トラッキング結果が表示されます。</p> <p>(レポートで選択されている時間範囲に関係なく) 設定可能な最大時間範囲内において特定の SHA-256 を含む影響を受けるすべてのトランザクションを表示するには、[マルウェア脅威ファイル (Malware Threat Files) ] ページ下部の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、[高度なマルウェア防御でブロック (Blocked by Advanced Malware Protection) ]列はアプライアンス レポートに表示されません。追加カラムを表示するには、テーブルの下の [列 (Columns) ]リンクをクリックします。

[ユーザの場所別のレポート (Report by User Location) ]に [高度なマルウェア防御 (Advanced Malware Protection) ]タブが含まれています。

## Web トラッキング機能と高度なマルウェア防御機能について

Web 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 [マルウェア脅威 (Malware Threat) ]エリアの [マルウェア カテゴリでフィルタ (Filter by Malware Category) ] オプションで [既知の悪意のある、リスクが高いファイル (Known Malicious and High-Risk Files) ] を選択します。
- Web 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正常であると判断され、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、正常の判定のみがトラッキング結果に表示されます。

クリーンな添付ファイルおよびスキャンできない添付ファイルの情報は表示されません。検索結果の [ブロック - AMP (Block - AMP)] は、ファイルのレピュテーション判定が原因でトランザクションがブロックされたことを意味します。

トラッキングの詳細に表示される [AMP 脅威スコア (AMP Threat Score)] は、ファイルを明確に判定できないときにクラウドレピュテーションサービスが提示するベストエフォート型のスコアです。この場合のスコアは 1 ~ 100 です (AMP 判定が返された場合、またはスコアがゼロの場合は [AMP 脅威スコア (AMP Threat Score)] を無視してください)。アプライアンスはこのスコアをしきい値スコア ([セキュリティサービス (Security Services)] > [マルウェア対策とレピュテーション (Anti-Malware and Reputation)] ページで設定) と比較して、実行するアクションを決定します。デフォルトでは、スコアが 60 ~ 100 の場合に悪意のあるファイルと見なされます。デフォルトのしきい値スコアを変更することはお勧めしません。WBRスコアはファイルのダウンロード元となったサイトのレピュテーションです。このスコアはファイルレピュテーションとは関係ありません。

- 判定のアップデートは [AMP 判定のアップデート (AMP Verdict Updates)] レポートでのみ使用できます。Web トラッキングの元のトランザクションの詳細は、判定の変更によって更新されません。特定のファイルに関連するトランザクションを確認するには、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)] > [ファイル分析 (File Analysis)] を選択し、ファイルで検索する SHA-256 を入力するか、または Web トラッキングの詳細で SHA-256 リンクをクリックします。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、Web 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

- ステップ 1** [AMP 判定のアップデート (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。エンドユーザーに対してアクセスが許可されていたファイルに関連するすべてのトランザクションの Web 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ファイルのダウンロード元 Web サイト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 \(Log Files\) \(23 ページ\)](#)
- [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 \(23 ページ\)](#)
- [API キーのエラー \(オンプレミスのファイル分析\) \(24 ページ\)](#)
- [ファイルが予想どおりにアップロードされない \(24 ページ\)](#)
- [クラウド内のファイル分析の詳細が完全でない \(25 ページ\)](#)
- [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 \(25 ページ\)](#)

### ログ ファイル (Log Files)

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高度なマルウェア防御に関する情報は、アクセスログまたはAMPエンジンのログに記録されます。詳細については、ログによるシステムアクティビティのモニタリングに関する章を参照してください。

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。

- 0 : レピュテーションサービスがファイルを認識しています。分析目的で送信しないでください。
- 1 : 送信します
- 2 : レピュテーションサービスがファイルを認識しています。分析目的で送信しないでください。

### 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）。

#### ソリューション

- [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（6 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 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）] > [マルウェア対策とレピュテーション（Anti-Malware and Reputation）] を選択します。[高度なマルウェア防御サービス（Advanced Malware Protection Services）] セクションの [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 Web セキュリティ アプライアンスを AMP Threat Grid サーバに接続できない場合は、API キーのアラートを受信します。

#### ソリューション

このエラーは、AMP Threat Grid サーバのホスト名を変更し、AMP Threat Grid サーバ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 Threat Grid アプライアンスから新しい証明書を生成します。
- Web 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 Threat Grid 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 Threat Grid 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（11 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。

#### ソリューション

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。
- [セキュリティ サービス (Security Services) ] > [マルチウェア対策とレピュテーション (Anti-Malware and Reputation) ] ページの [DVS エンジン オブジェクト スキャンの制限 (DVS Engine Object Scanning Limits) ] ページで設定した最大ファイルサイズの制限を確認します。この制限は、高度なマルウェア防御機能に適用されます。

## クラウド内のファイル分析の詳細が完全でない

### 問題

パブリック クラウド内の完全なファイル分析結果は、組織のその他の Web セキュリティ アプライアンスからアップロードされたファイルでは取得できません。

### ソリューション

ファイルの分析結果データを共有するすべてのアプライアンスをグループ化してください。[\(パブリッククラウドファイル分析サービスのみ\) アプライアンスグループの設定 \(15ページ\)](#) を参照してください。この設定は、グループの各アプライアンスで実行する必要があります。

## 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。

### ソリューション

このアラートは、サポートされているファイルタイプが変更された場合、または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する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に選択した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、ユーザによるアクションは必要ありません。
- アプライアンスがたとえば AsyncOS のアップグレードの一環として再起動している。

■ 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