CHAPTER 14

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

- 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（14-1 ページ）
- ファイル レピュテーション機能と分析機能の設定（14-5 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（14-17 ページ）
- ファイルの脅威判定が変更された場合に実行する操作（14-20 ページ）
- ファイル レピュテーションおよび分析のトラブルシューティング（14-20 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、次のようにして、ゼロデイ攻撃やファイルベースの標的型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で使用できます。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 サービスおよびファイル分析サービスは、パブリック クラウド サービスまたはプライベート クラウド（オンプレミス）サービスとして使用できます。

- 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 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 サーバの設定」セクション（14-8 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」セクション（14-9 ページ）を参照してください。

ファイルの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。当初ファイルが不明または正常と評価され、そのファイルへのアクセスが許可されることがあります。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。脅威の影響を排除する第一歩として、ポイント オブ エントリの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、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（14-4 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（14-17 ページ）
- ファイルの脅威判定が変更された場合に実行する操作（14-20 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（Scan）」に設定されている範囲内である場合、アプライアンスはトランザクションをスキャンしてマルウェアがあるかどうかを確認し、同時にファイルのレピュテーションをクラウドベース サービスに照会します。（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）] も有効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。

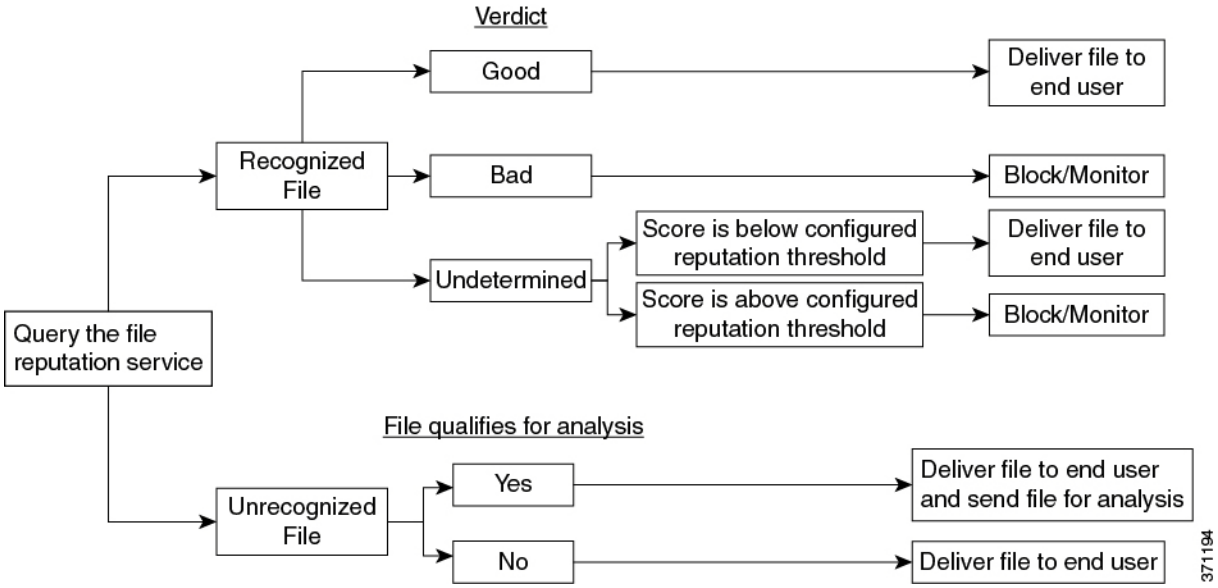
アプライアンスとファイル レピュテーション サービス間の通信は暗号化され、改ざんから保護されます。

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 サービスにとって既知のものであり、正常と判定された場合、ファイルはエンド ユーザにリリースされます。
- ファイル レピュテーション サービスが「悪意がある」という判定を返した場合、は、そのようなファイルに対して指定されているアクションを適用します。
- ファイルがファイル レピュテーション サービスにとって既知のものであるが、最終判定のための情報が不足している場合、レピュテーション サービスは、脅威のフィンガープリントや動作分析など、ファイルの特性に基づいて脅威スコアを返します。このスコアが既定のレピュテーションしきい値に合致している場合や、しきい値を越えている場合、悪意のあるファイル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 サービスにファイルに関する情報がなく、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（14-4 ページ）を参照）、ファイルは正常と見なされ、エンド ユーザにリリースされます。

- クラウドベースのファイル分析サービスが有効になっており、レピュテーション サービスに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（14-4 ページ）を参照）、ファイルは正常と見なされ、任意に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 サービスにとってファイルが未知のものである場合、そのファイルはユーザにリリースされますが、ファイル分析の結果はローカル キャッシュで更新され、ファイルの以降のインスタンスの評価に使用されます。
- サービスとの接続がタイムアウトしたため、ファイル レピュテーションまたはファイル分析の判定情報を利用できない場合、そのファイルは正常と見なされ、エンドユーザにリリースされます。

図 14-1　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 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「悪意がある」と見なされないことがあります。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、ファイルの脅威判定のアップデート（14-2 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ていないファイルのダウンロードをブロックするように、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 レピュテーションおよび分析サービスの有効化と設定（14-10 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（14-16 ページ）
- アーカイブまたは圧縮ファイルの処理（14-4 ページ）

アーカイブ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。
- 圧縮またはアーカイブ ファイルが圧縮解除され、すべての抽出された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（14-4 ページ）からリンクされている情報を参照してください。

この場合のシナリオは次のとおりです。

- 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（`text/plain` 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」と判定されたあらゆるファイルの情報が、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情報は、レピュテーション サービスと共有されません。

ファイル レピュテーション機能と分析機能の設定

- ファイル レピュテーション サービスおよび分析サービスと通信するための要件（14-6 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（14-8 ページ）
- オンプレミスのファイル分析サーバの設定（14-9 ページ）
- ファイル レピュテーションおよび分析サービスの有効化と設定（14-10 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（14-14 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（14-15 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（14-16 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（14-16 ページ）

ファイル レピュテーション サービスおよび分析サービスと通信するための要件

- これらのサービスを使用するすべての Web セキュリティ アプライアンスが、インターネット経由で直接サービスに接続できなければなりません（オンプレミスのアプライアンスを使用するよう設定されているファイル レピュテーション サービスとファイル分析サービスは除く）。
- 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、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データ インターフェイスを介したトラフィックのルーティング（14-7 ページ）を参照してください。
- 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）]、[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	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 レピュテーションおよび分析サービスの有効化と設定（14-10 ページ）

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データ インターフェイスを介した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に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。全般的な要件と手順については、TCP/IP トラフィック ルートの設定(2-26 ページ)を参照してください。

接続先	宛先ネットワーク	ゲートウェイ
ファイル レピュテーション サービス	[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)] 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)] 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。 [ファイル レピュテーション サーバ(File Reputation Server)] の [プライベート クラウド(Private Cloud)] を選択する場合は、[サーバ(Server)] のホスト名または IP アドレスを入力し、有効な [公開キー(Public Key)] を指定します。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。	データ ポートのゲートウェイの IP アドレス。

接続先	宛先ネットワーク	ゲートウェイ
ファイル分析サービス	• [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）] 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）] 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。 [ファイル分析サーバ（File Analysis Server）] の [プライベート クラウド（Private Cloud）] を選択する場合は、[サーバ（Server）] の URL を入力し、有効な [認証局（Certificate Authority）] を指定します。 • [ファイル分析クライアント ID（File Analysis Client ID）] は、ファイル分析サーバにおける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）。	データ ポートのゲートウェイの IP アドレス。

関連項目

- TCP/IP トラフィック ルートの設定（2-26 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

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。

- 『*Installation and Configuration of FireAMP Private Cloud*』ガイドなど、Cisco Advanced Malware Protection 仮想プライベート クラウド アプライアンスに関するドキュメントは、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 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 2.2 であることを確認します。これにより、Cisco Web セキュリティ アプライアンス と統合できるようになります。
- 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。
- この Web セキュリティ アプライアンスにアップロードするために、アプライアンスに AMP 仮想プライベート クラウドの証明書とキーをダウンロードします。

(注)　オンプレミスのファイル レピュテーション サーバを設定したら、この Web セキュリティ アプライアンスからサーバへの接続を設定します(手順 7(「ファイル レピュテーションおよび分析サービスの有効化と設定」セクション(14-10 ページ))を参照)。

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、以下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/tsd-products-support-series-home.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。

  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、他の Cisco 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 アプライアンスのソフトウェアをバージョン 1.2.1 に更新します。これにより、Cisco Web Security Appliance 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 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 Security Appliance は、AMP Threat Grid アプライアンスの CLEAN インターフェイスに接続できなければなりません。
- 自己署名証明書を展開する場合は、Web Security Appliance 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として CN を含む証明書が生成されたことを確認します。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。
- ファイル分析用の設定を送信すると、Threat Grid アプライアンスへの Web Security Appliance の登録が自動的に実行されます(ファイル レピュテーションおよび分析サービスの有効化と設定(14-10 ページ)を参照)。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ら、この Web Security Appliance からサーバへの接続を設定します(「ファイル レピュテーションおよび分析サービスの有効化と設定」セクション(14-10 ページ)の手順 8 を参照)。

ファイル レピュテーションおよび分析サービスの有効化と設定

はじめる前に

- 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詳しくは、機能キーの使用（22-4 ページ）を参照してください。
- ファイル レピュテーション サービスおよび分析サービスと通信するための要件（14-6 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。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（2-22 ページ）を参照してください。
- アップグレードおよびサービス アップデートの設定の変更（22-37 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。
- 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 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、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（14-8 ページ）を参照してください。
- 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、オンプレミスのファイル分析サーバの設定（14-9 ページ）を参照してください。

手順 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。

手順 2　[有効（Enable）] をクリックします。

手順 3　ライセンス契約に同意します。

手順 4　[グローバル設定を編集（Edit Global Settings）] をクリックします。

手順 5　[ファイル レピュテーションを有効にする（Enable File Reputation）] [ファイル レピュテーション フィルタリングを有効にする（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 レピュテーションを有効にする（Enable File Reputation][ファイル レピュテーション フィルタリングを有効にする（Enable File Reputation Filtering）] をオンにした場合は、外部パブリック レピュテーション クラウド サーバの URL を選択するか、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して、[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必要があります（手順 7）。
- 同様に、[ファイル分析を有効にする（Enable File Analysis）] をオンにした場合は、外部クラウド サーバの URL またはプライベート分析クラウドの接続情報を入力して、[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必要があります（手順 8）。

手順 6　[ファイル分析（File Analysis）] セクションの [ファイル タイプ（File Types）] で、分析用にクラウドに送信するファイル 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、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（14-4 ページ）のドキュメントの説明を参照してください。

手順 7　[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）	パブリック レピュテーション クラウド サーバのホスト名、または [プライベート レピュテーション クラウド（Private reputation cloud）] を選択します。 [プライベート レピュテーション クラウド（Private reputation cloud）] を選択した場合は、次の情報を入力します。 • [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。 • [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。 **（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。
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）	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。 **（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。 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。 [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。 **（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)）] をオンにした場合は、Web インターフェイスで [ネットワーク（Network）] > [証明書の管理（Certificate Management）] を使用して、このアプライアンスの証明書ストアに 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）] > [SSL] > [クラウド サーバ（Cloud server）] > [ダウンロード（download）]）。
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）	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。 • **クラウド サービスの値を使用（60）（Use value from Cloud Service (60)）** • [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。
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。

オプション	説明
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。
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。

手順 8　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）	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。 外部クラウド サーバを指定する場合は、アプライアンスに物理的に最も近いサーバを選択します。定期的に標準の更新プロセスを使用することにより、新たに利用可能になったサーバがこのリストに追加されます。 ファイル分析にオンプレミスの Cisco AMP Threat Grid アプライアンスを使用するには、[プライベート分析クラウド（Private analysis cloud）] を選択し、次の情報を入力します。 • [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。 • [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。 [アップロードした認証局を使用する（Use Uploaded Certificate Authority）] を選択した場合は、[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。
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）。

手順 9　変更を送信し、保存します。

手順 10　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. セクションの下部に表示される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 Security Appliance のファイル分析クライアント ID に基づいて「ユーザ」アカウントを検索します。

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。

（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。

はじめる前に

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。

手順 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。

手順 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。

手順 3　[グループにアプライアンスを追加（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を確認する

手順 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。

手順 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、[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。

手順 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	[ファイル分析の詳細設定（Advanced Settings for File Analysis）] セクション（[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）
Web Security Appliance	[ファイル分析の詳細設定（Advanced Settings for File Analysis）] セクション（[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）
Security Management Appliance	[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

手順 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。

手順 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。

手順 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。

手順 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。

手順 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、ファイル レピュテーションおよび分析サービスの有効化と設定（14-10 ページ）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（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）
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 サーバまたは分析サーバへの接続の失敗に関するアラート（14-21 ページ）
- ファイルの脅威判定が変更された場合に実行する操作（14-20 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

Security Management Appliance でレポートを集約管理する場合は、使用している管理アプライアンスのオンライン ヘルプまたはユーザ ガイドを参照し、「Web レポート」の章の「高度なマルウェア防御」に関する項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（14-17 ページ）
- [ファイルレピュテーション（File Reputation）] および [ファイル分析（File Analysis）] レポート ページ（14-17 ページ）
- 他のレポートのファイル レピュテーション フィルタリング データの表示（14-18 ページ）
- Web トラッキング機能および高度なマルウェア防御機能について（14-19 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ことから、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識別子を生成します。アプライアンスが名前の異なる同じファイルを処理する場合、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を処理する場合、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、ファイルがその SHA-256 値（短縮形式）別に表示されます。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（File Reputation）] および [ファイル分析（File Analysis）] レポート ページ

レポート	説明
高度なマルウェア防御（Advanced Malware Protection）	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。 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。 [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。 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。 （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。

レポート	説明
[高度なマルウェア防御（Advanced Malware Protection）] におけるファイル分析	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。 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。 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。 ドリルダウンすると、詳細な分析結果（各ファイルの脅威の特性やスコアなど）が表示されます。 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。 （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。
高度なマルウェア防御判定の更新（Advanced Malware Protection Verdict Updates）	このアプライアンスで処理され、トランザクションの処理後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、ファイルの脅威判定のアップデート（14-2 ページ）を参照してください。 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。 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。 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内にこの 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。 （レポートに対して指定した時間範囲に関係なく）使用可能な最大時間範囲内で、特定の SHA-256 の影響を受けたすべてのトランザクションを表示するには、[マルウェアの脅威ファイル（Malware Threat Files）] ページの下部にあるリンクをクリックします。

他のレポートのファイル レピュテーション フィルタリング 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。レポートによっては、[高度なマルウェア防御でブロック（Blocked by Advanced Malware Protection）] 列がデフォルトで非表示になっている場合があります。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 トラッキング機能および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の脅威情報を検索する場合は、次の点に注意してください。

- ファイル レピュテーション サービスで検出された悪意のあるファイルを検索するには、Web トラッキングの [詳細設定（Advanced）] セクションで、[マルウェアの脅威（Malware Threat）] 領域の [マルウェアカテゴリ別フィルタ（Filter by Malware Category）] オプションに対して、[悪意のある既知の高リスク 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、トランザクションの処理時に返された元のファイル レピュテーション判定のみが含まれます。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。

  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により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。WBRS 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、判定が変更されても更新されません。特定のファイルに関連するトランザクションを表示するには、判定のアップデート レポートで SHA-256 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。ファイルの使用可能なファイル分析情報を表示するには、[レポート（Reporting）] > [ファイル分析（File Analysis）] を選択して、ファイルを検索する SHA-256 を入力します。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。

  分析用に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で処理されると、それらのインスタンスは Web トラッキングの検索結果に表示されます。

ファイルの脅威判定が変更された場合に実行する操作

手順 1　[AMP 判定のアップデート（AMP Verdict updates）] レポートを表示します。

手順 2　該当する SHA-256 リンクをクリックし、エンド ユーザがアクセスを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 データを表示します。

手順 3　トラッキング データを使用して、侵害を受けた可能性があるユーザ、漏えいに関連する情報（ファイル名など）、およびファイルのダウンロード元の Web サイトを特定します。

手順 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。

関連項目

- ファイルの脅威判定のアップデート（14-2 ページ）

ファイル レピュテーションおよび分析のトラブルシューティング

- ログ ファイル（14-20 ページ）
- ファイル レピュテーション サーバまたは分析サーバへの接続の失敗に関するアラート（14-21 ページ）
- API キーのエラー（オンプレミスのファイル分析）（14-21 ページ）
- ファイルが期待どおりにアップロードされない（14-21 ページ）
- クラウドでファイル分析詳細が不完全（14-22 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（14-22 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高度なマルウェア防御に関する情報は、[アクセス ログ（Access Logs）] 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 サーバまたは分析サーバへの接続の失敗に関するアラート

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)。

解決策

- ファイル レピュテーション サービスおよび分析サービスと通信するための要件(14-6 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)] > [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 [クエリータイムアウト(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の表示を試みた場合や、Web Security Appliance が分析用ファイルのアップロードために AMP Threat Grid サーバに接続できない場合は、API キー アラートを受信します。

解決策　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。
- 新しい証明書を Web Security Appliance に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 レピュテーションおよび分析サービスの有効化と設定(14-10 ページ)

ファイルが期待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。

解決策　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。

クラウドでファイル分析詳細が不完全

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、組織内の他のWeb Security Appliance からアップロードされたファイルでは使用できません。

解決策　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 (14-14 ページ)を参照してください。この設定は、グループ内のアプライアンスごとに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す。

解決策　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。