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

Advanced Malware Protection 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 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 （10 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 （11 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、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。

判定が「悪意がある」から「正常」に変更されることもあります。

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 （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 （27 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、同時にクラウドベース サービスに対してファイルのレピュテーションを照会します。（サイトのレピュテーション スコアが「ブロック（Block）」範囲内である場合、トランザクションはブロックされるため、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ると、ファイルのレピュテーションに関係なくトランザクションはブロックされます。

適応型スキャンもイネーブルになっている場合は、ファイル レピュテーション評価とファイル分析は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。

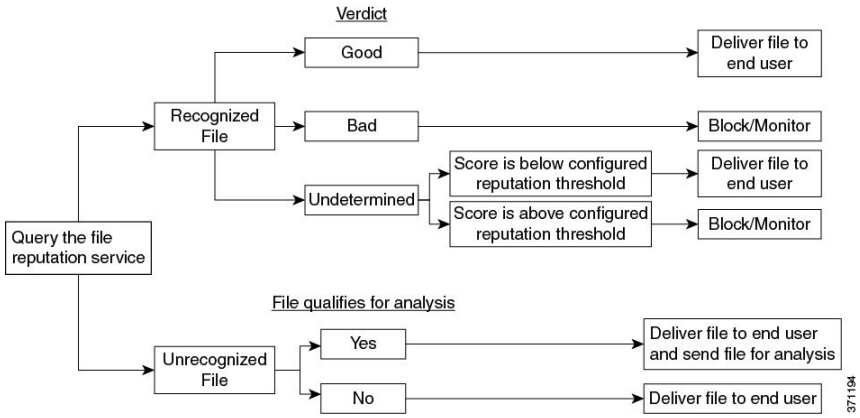
ファイル レピュテーションの評価後：

- 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。

低リスク ファイル

当初ファイルが不明で動的コンテンツを含まないと評価された場合、アプライアンスはそのファイルを事前分類エンジンに送信し、事前分類エンジンで低リスクに指定されます。このファイルは分析用にアップロードされません。キャッシュの有効期限内に同じファイルにアクセスした場合、改めて低リスクと評価され、分析用にアップロードされることはありません。キャッシュ タイムアウトの後、同じファイルにもう一度アクセスすると、不明、低リスクと順を追って評価されます。このプロセスは低リスク ファイルに対して繰り返されます。これらの低リスク ファイルはアップロードされないため、ファイル分析レポートには含められません。

図 *1:* 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、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 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。

[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。

Advanced Malware Protection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 （12 ページ）
- Advanced Malware Protection の問題に関するアラートの確実な受信 （21 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。
- 選択されたファイルの種類によっては、圧縮ファイルまたはアーカイブ ファイルは圧縮解除され、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、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）。

- 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。

ファイル レピュテーションと分析機能の設定

- （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）
- 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 （21 ページ）
- Advanced Malware Protection の問題に関するアラートの確実な受信 （21 ページ）
- Advanced Malware Protection 機能の集約管理レポートの設定 （22 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 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できる必要があります。
- 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 （8 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 インターフェイス
32137（デフォルト）または 443	ファイル レピュテーション取得のためのクラウド サービスへのアクセス。	TCP	発信	[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。	管理（データポート経由で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る場合を除く）。
443	ファイル分析のためのクラウド サービスへのアクセス。	TCP	発信	[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ときに、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

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、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
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。 [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）] で設定されているクラウド サーバ プールのホスト名。	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。 • 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）。 [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。	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

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ーとして 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 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 AMP 仮想プライベート クラウド アプライアンスを設定および構成します。
- Cisco 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 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そのアプライアンスにダウンロードして、この 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 からこのサーバーへの接続を設定します。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 （12 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。

  Administration Guide 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）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 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 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、 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 証明書を生成します。SSL 証明書とキー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 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ーを設定した後に、このからこのサーバーへの接続を設定します。『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』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

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詳しくは、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 （7 ページ）を満たします。
- ファイル レピュテーションと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ー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 （10 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ー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 （11 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。

（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）

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
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。

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）	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。 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。 • [サーバー（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）	Advanced Malware Protection サービスに使用する（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る）ルーティングテーブル。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。サーバーへの 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ー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、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)）] 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 証明書をこのアプライアンスに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）。
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。
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 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
	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、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。 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。 • [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。 （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。 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。 • [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。 （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（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

オプション	説明
	わせください。
プロキシの設定	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。 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 [パスフレーズ（Passphrase）] の情報を入力します。
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）

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。

（注） [しきい値設定（Threshold Settings）] オプションは、[レピュテーションしきい値（Reputation Threshold）] ではなく [ファイル分析しきい値（File Analysis Threshold）] として分類されるようになりました。

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) 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。

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す。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。

（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 （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。
- スマートライセンシング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。

ステップ 3 [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。
- 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 4 [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
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、ファイル レピュテーション フィルタだけが提供されます。

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 [モニタリング（Monitor）] です。

ステップ 5 変更を送信し、保存します。

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（Type）	重大度（Severity）
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ライアンス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。	マルウェア対策	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	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	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	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。	マルウェア対策	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	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 （28 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 （27 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 Web レポーティングのトピックの「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

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
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。 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。 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。 [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。 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。 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。 [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。

レポート	説明
Advanced Malware Protection [ファイル分析（File Analysis）]	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。 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、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。 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。 （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。
Advanced Malware Protection レピュテーション	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。 [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。 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。 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。

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。

[ユーザーの場所別のレポート（Report by User Location）] には [高度なマルウェア防御（Advanced Malware Protection）] タブがあります。

Web トラッキング機能と Advanced Malware Protection 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。

  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、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の変更は推奨されません。WBRS スコアは、ファイルのダウンロード元サイトのレピュテーションであり、ファイル レピュテーションとは関係ありません。
- 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。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。エンドユーザ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 （28 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 （28 ページ）
- API キーのエラー（オンプレミスのファイル分析） （29 ページ）
- ファイルが予想どおりにアップロードされない （29 ページ）
- クラウド内のファイル分析の詳細が完全でない （29 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 （30 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、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トピック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。

- 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。

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）] > [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 が AMP 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、 AMP マルウェア分析サーバのホスト名を変更し、 AMP 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。
- 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

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。
- [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 Advanced Malware Protection 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。

解決方法

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 （19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す。

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。