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

高度なマルウェア防御は、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 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 （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 （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 （30 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 （34 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、アンチウィルス 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。

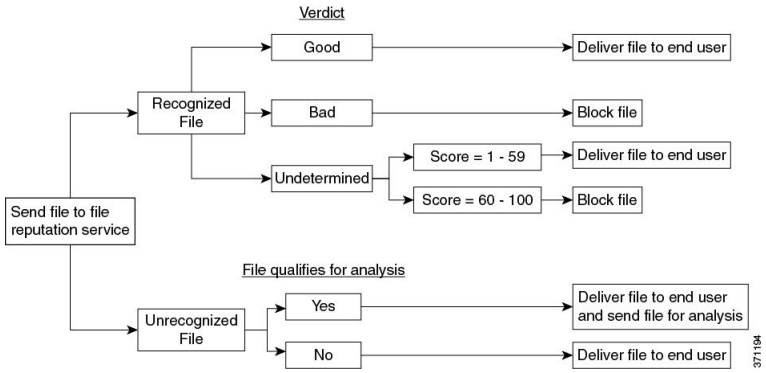
（注） メッセージの MIME ヘッダーの形式が正しくない場合、ファイル レピュテーション サービスはデフォルトで「スキャン不可」の判定を返します。アプライアンスは、このメッセージからも添付ファイルを抽出しようとします。アプライアンスが添付ファイルを抽出できない場合、判定は「スキャン不可」のままです。アプライアンスが添付ファイルを抽出できる場合は、添付ファイルのファイル レピュテーションが評価されます。添付ファイルが悪意のあるものである場合、判定は「スキャン不可」から「悪意のある」に変わります。

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 （24 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とき、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高度なマルウェア防御ワーク 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、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。

高度なマルウェア防御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）
- 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 （28 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 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

- これらのサービスを使用するすべてのは、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 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（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（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）] セクションで設定された名前。	

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 E メール 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 E メール セキュリティ アプライアンスにアップロードします。
- E メール セキュリティ アプライアンスで信頼されているルート認証局がトンネル プロキシ サーバの証明書に署名していない場合は、[ルート証明書（Root Certificate）] オプションを使用して標準の検証をスキップします。

（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 E メール 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

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%20-list.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、ESA、E メール 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 E メール 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 E メール 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、E メール 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 Thread 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 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 （9 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。

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 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 （8 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 （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、アップデータ 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
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（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。
AMP for Endpoints コンソールの統合	お使いのアプライアンスを AMP for Endpoints コンソールと統合するには、[アプライアンスのAMP for Endpointsコンソールへの登録（Register the Appliance with AMP for Endpoints）] をクリックします。詳細な手順については、アプライアンスと AMP for Endpoints コンソールとの統合 （16 ページ）を参照してください。

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、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)）] 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）] > [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。
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）

オプション	説明
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
	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 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。 • [TG サーバ（TG Servers）]：スタンドアロンの、またはクラスタ化された Cisco AMP Threat Grid 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 AMP Threat Grid アプライアンスを追加することができます。 （注） 通し番号は、スタンドアロンの、またはクラスタ化された Cisco AMP Threat Grid 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 AMP Threat Grid ポータルを設定している場合は、Cisco AMP Threat Grid 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

オプション	説明
	きます。Cisco AMP Threat Grid 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。
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。

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 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) 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。

アプライアンスと AMP for Endpoints コンソールとの統合

お使いのアプライアンスを AMP for Endpoints コンソールと統合すると、AMP for Endpoints コンソールで以下の操作を実行できます。

- 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 AMP for Endpoints 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 サーバから得られた判定は、AMP for Endpoints コンソールの同じファイル SHA に対してすでに入手できる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、AMP for Endpoints 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、AMP for Endpoints から受信されたブラックリスト登録済みのファイル SHA の割合が、[カスタム検出（Custom Detection）] として表示されます。ブラックリスト 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）] セクションのリンクをクリックすると、AMP for Endpoints コンソールでのブラックリスト追加ファイル 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

AMP for Endpoints コンソールの管理アクセス権を伴うユーザ アカウントがあることを確認してください。AMP for Endpoints コンソールのユーザ 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。

[クラスタ化された設定の場合]クラスタ化された設定では、ログインしているアプライアンスを AMP for Endpoints コンソールにのみ登録できます。アプライアンスを AMP for Endpoints 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、アプライアンス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化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 （9 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 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 [AMP for Endpointsへのアプライアンスの登録（Register Appliance with AMP for Endpoints）] をクリックします。

[AMP for Endpointsへのアプライアンスの登録（Register Appliance with AMP for Endpoints）] をクリックすると、AMP for Endpoints 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 クレデンシャルで、AMP for Endpoints コンソール にログインします。

ステップ 5 AMP for Endpoints 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。[AMP for Endpoints コンソールの統合（AMP for Endpoints 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、AMP for Endpoints のコンソール 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

次の手順：

- [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 AMP for Endpoints 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、AMP for Endpoints 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す。
- 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。AMP for Endpoints 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、独自のブロックリストまたは許可リストに追加されているファイル SHA を追加する場合は、https://console.amp.cisco.com/docs で AMP for Endpoints のユーザ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、AMP for Endpoints 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」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 AMP for Endpoints 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。AMP for Endpoints 機能を使用するには、アプライアンスの登録を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 AMP for Endpoints 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 AMP for Endpoints のコンソール ページ（https://console.amp.cisco.com/）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 AMP for Endpoints のユーザ 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 サーバを別のデータ センターに変更すると、アプライアンスは AMP for Endpoints 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 サーバに選択された同じデータ センターを使用して、アプライアンスを AMP for Endpoints 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 サーバを変更すると、ログインしているアプライアンスは自動的に AMP for Endpoints 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 サーバ用に選択したものと同じデータセンターを使用して、すべてのアプライアンスを AMP for Endpoints 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 AMP for Endpoints 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 Thread 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。

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 [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 3 [今すぐグループ化（Group Now）] 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

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 [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、**[アプライアンスの表示（View Appliances）]** 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

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。

（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

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を指定します。

ユーザ	情報
ローカル ユーザ（Local Users）	ローカルユーザのリストには、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（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 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。

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。 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）	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 （35 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 （34 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電子メール 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 （30 ページ）
- #unique_844
- 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 （33 ページ）
- メッセージ 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 （33 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

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
高度なマルウェア対策（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 [着信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
[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。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。
高度なマルウェア防御レピュテーション	高度なマルウェア防御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、[]列はアプライアンス 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高度なマルウェア防御機能について

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
  - メッセージ全体に対する高度なマルウェア防御の最終判定
  - マルウェアが検出された添付ファイル

- 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。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

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、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、組織外のアカウントからテスト 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。[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。

解決方法

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。
- 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 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 （9 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）。