



ネットワークマルウェア防御とファイルポリシー

次のトピックでは、ファイル制御、ファイルポリシー、ファイルルール、Advanced Malware Protection (AMP) 、クラウド接続、および動的分析接続の概要を示します。

- ネットワークにおけるマルウェア防御とファイルポリシーについて (1 ページ)
- ファイルポリシーの要件と前提条件 (3 ページ)
- ファイルおよびマルウェア ポリシーのライセンス要件 (3 ページ)
- ファイルポリシーとマルウェア検出のベストプラクティス (4 ページ)
- マルウェア防御の設定方法 (7 ページ)
- マルウェア防御のためのクラウド接続 (13 ページ)
- ファイルポリシーとファイルルール (24 ページ)
- レトロスペクティブな性質の変更 (44 ページ)
- ファイルおよびマルウェアのインスペクションパフォーマンスとストレージのオプション (44 ページ)
- ファイルおよびマルウェアのインスペクションパフォーマンスおよびストレージの調整 (47 ページ)
- (オプション) Secure Endpoint を使用したマルウェア防御 (47 ページ)
- ネットワークマルウェア防御とファイルポリシーの履歴 (53 ページ)

ネットワークにおけるマルウェア防御とファイルポリシーについて

マルウェアを検出してブロックするには、ファイルポリシーを使用します。また、ファイルポリシーを使用して、ファイルタイプごとにトラフィックを検出および制御することもできます。

Firepower の高度なマルウェア防御 (AMP) は、ネットワーク トラフィックでのマルウェアの伝送を検出、キャプチャ、追跡、分析、ロギング、および必要に応じてブロックできます。Secure Firewall Management Center Web インターフェイスでは、この機能はマルウェア防御と

■ ファイルポリシー

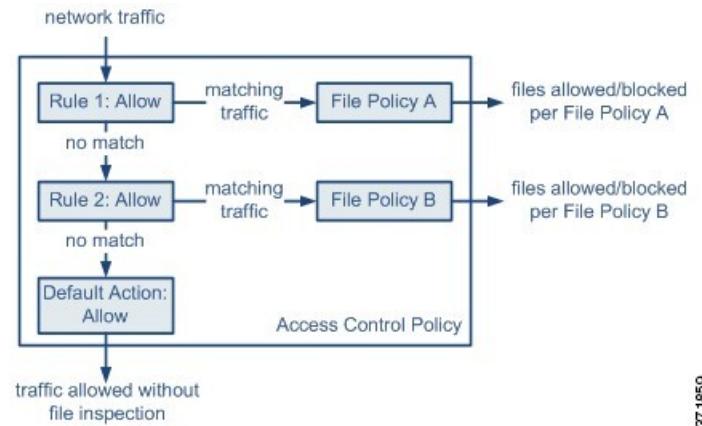
呼ばれ、以前は *AMP for Firepower* とも呼ばれていました。高度なマルウェア防御は、シスコ クラウドからインラインおよび脅威データを展開した管理対象デバイスを使用してマルウェアを特定します。

すべてのアクセス コントロール設定に含まれるネットワーク トラフィックを処理するアクセス コントロールルールとファイルポリシーを関連付けます。

システムがネットワーク上のマルウェアを検出すると、ファイルおよびマルウェアイベントを生成します。ファイルイベントおよびマルウェアイベントのデータを分析するには、Cisco Secure Firewall Management Center アドミニストレーションガイドの「ファイルイベント/マルウェアイベントとネットワーク ファイル トラジェクトリ」の章を参照してください。

ファイルポリシー

ファイルポリシーは、いくつかの設定からなるセットです。システムは全体的なアクセス コントロール設定の一部としてこれを使用して、マルウェア防御とファイル制御を実行できます。この関連付けにより、アクセス コントロールルールの条件と一致するトラフィック内のファイルを通過させる前に、システムは必ずファイルを検査するようになります。次の図のような、オンライン展開での単純なアクセス コントロールポリシーがあるとします。



371859

このポリシーには 2 つのアクセス コントロールルールがあり、両方とも許可アクションを使用し、ファイルポリシーに関連付けられています。このポリシーのデフォルトアクションもまた「トラフィックの許可」ですが、ファイルポリシーインスペクションはありません。このシナリオでは、トラフィックは次のように処理されます。

- Rule 1 に一致するトラフィックは File Policy A で検査されます。
- Rule 1 に一致しないトラフィックは Rule 2 に照らして評価されます。Rule 2 に一致するトラフィックは File Policy B で検査されます。
- どちらのルールにも一致しないトラフィックは許可されます。デフォルトアクションにファイルポリシーを関連付けることはできません。

異なるファイルポリシーを個々のアクセスコントロールルールに関連付けることにより、ネットワークで伝送されるファイルを識別/ブロックする方法をきめ細かく制御できます。

ファイルポリシーの要件と前提条件

モデルのサポート

任意 (Any)

サポートされるドメイン

任意

ユーザの役割

- 管理者
- アクセス管理者

ファイルおよびマルウェアポリシーのライセンス要件

操作内容	必要なライセンス	ファイルルールのアクション
特定のタイプのすべてのファイルをブロックまたは許可します (すべての .exe ファイルをブロックなど)	IPS (Firewall Threat Defense デバイスの場合) 保護 (従来のデバイスの場合)	許可 (Allow)、ブロック (Block)、リセットしてブロック (Block with reset)
マルウェアが含まれているか、または含まれている可能性があると判断した場合に、ファイルを選択的に許可またはブロックします	IPS (Firewall Threat Defense デバイスの場合) 保護 (従来のデバイスの場合) マルウェア防御	マルウェアクラウド ルックアップ (Malware Cloud Lookup)、マルウェアブロック (Block Malware)
ファイルの保存 (Store files)	IPS (Firewall Threat Defense デバイスの場合) 保護 (従来のデバイスの場合) マルウェア防御	[ファイルの保存 (Store Files)] で選択された ファイルルールアクション

マルウェア防御ライセンスの詳細については、次を参照してください。

- Cisco Secure Firewall Management Center アドミニストレーション ガイド のマルウェア防御ライセンス

ファイルポリシーとマルウェア検出のベストプラクティス

以下で説明する項目に加えて、[マルウェア防御の設定方法（7ページ）](#) および参照されているトピックの手順に従ってください。

ファイルルールのベストプラクティス

ファイルルールを設定する場合、次の注意事項と制約事項に注意してください。

- パッシブ展開でファイルをブロックするよう設定されたルールは、一致するファイルをブロックしません。接続ではファイル伝送が続行されるため、接続の開始をログに記録するルールを設定した場合、この接続に関して複数のイベントが記録されることがあります。
- ポリシーには複数のルールを含めることができます。ルールを作成する場合、このルールが以前のルールよりも「優先されている」ことを確認します。
- 動的分析でサポートされているファイルタイプは、他のタイプの分析でサポートされているファイルタイプのサブセットです。各分析タイプでサポートされているファイルタイプを表示するには、ファイルルール設定ページに移動し、[マルウェア ブロック (Block Malware)] アクションを選択して、対象のチェックボックスをオンにします。

システムがすべてのファイルタイプを検査するには、動的分析と他の分析タイプで個別のルール（同じポリシー内）を作成します。

- [マルウェアクラウド ルックアップ (Malware Cloud Lookup)] アクションまたは[マルウェア ブロック (Block Malware)] アクションを使ってファイルルールが設定されている場合、Firewall Management Center が AMP クラウドとの接続を確立できないと、接続が復元されるまで、システムは設定済みルールアクション オプションを実行できません。
- シスコでは、[ファイルブロック (Block Files)] アクションと[マルウェア ブロック (Block Malware)] アクションで[接続のリセット (Reset Connection)] を有効にすることを推奨しています。これにより、ブロックされたアプリケーションセッションがTCP接続リセットまで開いたままになることを防止できます。接続をリセットしない場合、TCP接続が自身をリセットするまで、クライアントセッションが開いたままになります。
- 大量のトラフィックをモニターしている場合、キャプチャしたすべてのファイルを保存したり、動的分析用に送信したりしないでください。そのようにすると、システムパフォーマンスに悪影響が及ぶことがあります。
- システムで検出されるすべてのファイルタイプに対してマルウェア分析を実行できるわけではありません。[アプリケーション プロトコル (Application Protocol)]、[転送の方向

(Direction of Transfer)]、および[アクション (Action)] ドロップダウンリストで値を選択すると、システムはファイルタイプのリストを限定します。

ファイル検出のベストプラクティス

ファイル検出については、次の注意事項と制限事項を考慮してください。

- アダプティブプロファイリングが有効でなければ、アクセスコントロールルールは、AMPを含め、ファイルの制御を実行できません。
- ファイルがアプリケーションプロトコル条件を持つルールに一致する場合、ファイルイベントの生成は、システムがファイルのアプリケーションプロトコルを正常に識別した後に行われます。識別されていないファイルは、ファイルイベントを生成しません。
- FTPは、さまざまなチャネルを介してコマンドおよびデータを転送します。パッシブまたはオンラインタップモードの展開では、FTPデータセッションとその制御セッションからのトラフィックは同じ内部リソースに負荷分散されない場合があります。
- POP3、POP、SMTP、またはIMAPセッションでのすべてのファイル名の合計バイト数が1024を超えると、セッションのファイルイベントでは、ファイル名バッファがいっぱいになった後で検出されたファイルの名前が正しく反映されないことがあります。
- SMTP経由でテキストベースのファイルを送信すると、一部のメールクライアントは改行をCRLF改行文字標準に変換します。MACベースのホストはキャリッジリターン(CR)文字を使用し、UNIX/Linuxベースのホストはラインフィード(LF)文字を使用するので、メールクライアントによる改行変換によってファイルのサイズが変更される場合があります。一部のメールクライアントは、認識できないファイルタイプを処理する際に改行変換を行うようデフォルト設定されていることに注意してください。
- ISOファイルを検出するには、[ファイルおよびマルウェアのインスペクションパフォーマンスとストレージのオプション \(44ページ\)](#)の説明のように、[ファイルタイプを検知する前に検閲するバイト数制限 (Limit the number of bytes inspected when doing file type detection)]オプションを36870を超える値に設定します。
- rar5を含む一部の.rarアーカイブ内の.exeファイルは検出できません。
- ファイルの性質がNeutralの場合、そのファイルの性質は不明です。

ファイルブロッキングのベストプラクティス

ファイルブロッキングについては、次の注意事項と制限事項を考慮してください。

- ファイルの終わりを示すEnd of Fileマークーが検出されない場合、転送プロトコルとは無関係に、そのファイルはマルウェアブロックルールでもカスタム検出リストでもブロックされません。システムは、End of Fileマークーで示されるファイル全体の受信が完了するまでファイルのブロックを待機し、このマークーが検出された後にファイルをブロックします。

■ ファイルブロッキングのベストプラクティス

- FTP ファイル転送で End of File マーカーが最終データ セグメントとは別に伝送される場合、マーカーがブロックされ、ファイル転送失敗がFTP クライアントに表示されますが、実際にはそのファイルは完全にディスクに転送されます。
- [ファイルブロック (Block Files)] アクションおよび[マルウェアブロック (Block Malware)] アクションを持つファイルルールでは、最初のファイル転送試行後 24 時間で検出される、同じファイル、URL、サーバ、クライアントアプリケーションを使った新しいセッションをブロックすることにより、HTTP 経由のファイルダウンロードの自動再開をブロックします。
- まれに、HTTP アップロードセッションからのトラフィックが不適切である場合、システムはトラフィックを正しく再構築できなくなり、トラフィックのブロックやファイルイベントの生成を行いません。
- ファイルブロックルールでブロックされる NetBios-ssn 経由ファイル転送 (SMB ファイル転送など) の場合、宛先ホストでファイルが見つかることがあります。ただし、ダウンロード開始後にファイルがブロックされ、結果としてファイル転送が不完全になるため、そのファイルは使用できません。
- (SMB ファイル転送などの) NetBIOS-ssn 経由で転送されたファイルを検出またはブロックするファイルルールを作成した場合、進行中のファイル転送はシステムにより検査されません。ただし、ファイルポリシーを呼び出すアクセスコントロールポリシーを展開した後に、転送された新しいファイルがシステムにより検査されます。
- SMB には、同じ IP アドレスと異なるポートを持つ複数のパラレルセッションを作成する、マルチチャネルと呼ばれる機能があります。マルチチャネルを使用するトランザクションでは、ファイルのダウンロードはこれらのセッションにわたって多重化され、システムにより単一のファイルとして検査されません。
- 1 つの TCP または SMB セッションで同時に転送されたファイルは検査されません。
- クラスタ環境では、クラスタロールの変更またはデバイス障害が原因で既存の SMB セッションが新しいデバイスに移動されると、進行中のファイル転送のファイルが検査されないことがあります。
- Microsoft Windows システム間での一部の SMB ファイル転送では、迅速なファイル転送のため、非常に大きな TCP ウィンドウ サイズを使用します。このようなファイル転送を検出またはブロックするには、[ネットワーク分析ポリシー (Network Analysis Policy)] > [TCPストリームの設定 (TCP Stream Configuration)] > [トラブルシューティングオプション (Troubleshooting Options)] にある [最大キューイングバイト (Maximum Queued Bytes)] と [最大キューイングセグメント (Maximum Queued Segments)] の値を大きくすることを推奨します。
- Firepower Threat Defense の高可用性を設定したときに、元のアクティブなデバイスがファイルを識別している間にフェールオーバーが発生した場合、ファイルタイプは同期されません。ファイルポリシーでそのファイルタイプがブロックされている場合でも、新しいアクティブなデバイスはファイルをダウンロードします。

ファイルポリシーのベストプラクティス

ファイルポリシーを設定する場合、次の一般的な注意事項と制約事項に注意してください。

- 1つのファイルポリシーを、[許可 (Allow)]、[インタラクティブブロック (Interactive Block)]、または[リセットしてインタラクティブブロック (Interactive Block with reset)]アクションを含むアクセスコントロールルールに関連付けることができます。
- ただし、アクセスコントロールのデフォルトアクションによって処理されるトラフィックを検査するためにファイルポリシーを使用できないことに注意してください。
- 新しいポリシーの場合、ポリシーが使用中でないことがWebインターフェイスに示されます。使用中のファイルポリシーを編集している場合は、そのファイルポリシーを使用しているアクセスコントロールポリシーの数がWebインターフェイスに示されます。どちらの場合も、テキストをクリックすると[アクセスコントロールポリシー (Access Control Policies)]ページに移動できます。
- ファイルブロッキングが機能するには、アクセスコントロールポリシーに適用するNAPポリシーが保護モードで動作している必要があります（オンラインモードとも呼ばれます）。
- 設定に応じて、システムがファイルを初めて検出したときに、そのファイルを検査してクラウドルックアップの結果を待機するか、または、クラウドルックアップの結果を待機せずにファイルを通過させることができます。
- デフォルトでは、暗号化されたペイロードのファイル検査は無効になっています。これにより、ファイル検査が設定されたアクセス制御ルールに暗号化接続が一致したときの誤検出が減少し、パフォーマンスが向上します。



注目 次のジェネレータID (GID)を持つファイル検査プリプロセッサは、ファイル/マルウェアポリシーに対してデフォルトで有効になっています：GID: 146およびGID: 147。

- [マルウェア (Malware)]アクションまたは[ファイルの保存 (Store Files)]オプションのいずれかを使用するファイルポリシーでアクセスコントロールポリシーをイネーブルにすると、デバイスのコンピューティング能力とシステムパフォーマンスが低下します。

マルウェア防御の設定方法

ここでは、悪意のあるソフトウェアからネットワークを保護するために、システムのセットアップで実行する必要がある手順について説明します。

手順

[ステップ1 マルウェア防御の計画と準備 \(8 ページ\)](#)

[ステップ2 ファイルポリシーの設定 \(10 ページ\)](#)

[ステップ3 アクセスコントロール設定へのファイルポリシーの追加 \(10 ページ\)](#)

[ステップ4 ネットワーク検出ポリシーを設定して、ファイルとマルウェアイベントをネットワーク上のホストと関連付けます。](#)

(ネットワーク検出をオンにするだけでなく、ネットワーク上のホストを検出して組織のネットワークマップを構築するように設定する必要があります。)

[ネットワーク検出ポリシーおよびサブトピックを参照してください。](#)

[ステップ5 管理対象デバイスにポリシーを展開します。](#)

[設定変更の展開を参照してください。](#)

[ステップ6 予想したとおりに悪意のあるファイルを処理していることを確認するためにシステムをテストします。](#)

[ステップ7 マルウェア防御のメンテナンスとモニタリングの設定 \(12 ページ\)](#)

次のタスク

- (オプション) ネットワーク内のマルウェアの検出をさらに強化するには、シスコの Secure Endpoint 製品を導入して統合します。 (オプション) [Secure Endpoint を使用したマルウェア防御 \(47 ページ\)](#) およびサブトピックを参照してください。

- ファイルおよびマルウェアイベントを調査する方法を理解します。

[Cisco Secure Firewall Management Center アドミニストレーションガイド](#)の「File/Malware Events and Network File Trajectory」を参照してください。

マルウェア防御の計画と準備

この手順は、マルウェアを防御するようにシステムを設定するための完全なプロセスの最初の手順です。

手順

[ステップ1 ライセンスを購入してインストールします。](#)

ファイルおよびマルウェアポリシーのライセンス要件（3ページ）および『Cisco Secure Firewall Management Center アドミニストレーションガイド』のライセンスを参照してください。

ステップ2 ファイルポリシーおよびマルウェア防御がアクセスコントロールプランにどのように適合するかを理解します。

[アクセス制御の概要](#)の章を参照してください。

ステップ3 ファイル分析およびマルウェア防御ツールについて理解します。

[ファイルルールアクション](#)（33ページ）およびサブトピックを参照してください。

また、[高度およびアーカイブファイルインスペクションオプション](#)（25ページ）も考慮してください。

ステップ4 マルウェア防御（ファイル分析と動的分析）にパブリッククラウドまたはプライベート（オンプレミス）クラウドを使用するかどうかを決定します。

[マルウェア防御のためのクラウド接続](#)（13ページ）およびサブトピックを参照してください。

ステップ5 マルウェア防御にプライベート（オンプレミス）クラウドを使用する場合は、これらの製品を購入、展開、テストします。

詳細については、シスコのセールス担当者または認定リセラーにお問い合わせください。

ステップ6 選択したクラウドとの通信を許可するようにファイアウォールを設定します。

[Cisco Secure Firewall Management Center アドミニストレーションガイド](#)の「*Security, Internet Access, and Communication Ports*」を参照してください。

ステップ7 Firepowerとマルウェア防御クラウド（パブリックまたはプライベート）の間の接続を設定します（該当する場合）。

- AMPクラウドについては、[AMPオプションの変更](#)（19ページ）を参照してください。
- オンプレミスのSecure Malware Analyticsアプライアンスを展開した場合は、[オンプレミスの動的分析アプライアンスへの接続](#)（21ページ）を参照してください。（パブリックSecure Malware Analyticsクラウドへのアクセスを設定する必要はありません。）

次のタスク

マルウェア防御ワークフローの次の手順に進みます。

[「マルウェア防御の設定方法](#)（7ページ）」を参照してください。

ファイルポリシーの設定

始める前に

マルウェア防御ワークフローで、この時点までのタスクを実行します。

[マルウェア防御の設定方法（7ページ）](#) を参照してください。

手順

ステップ1 ファイルポリシーおよびファイルルールの制限事項を確認します。

[ファイルポリシーとマルウェア検出のベストプラクティス（4ページ）](#) およびサブトピックを参照してください。

ステップ2 ファイルポリシーを作成します。

[ファイルポリシーの作成または編集（24ページ）](#) を参照してください。

ステップ3 ファイルポリシー内にルールを作成します。

[ファイルルール（30ページ）](#) およびサブトピックを参照してください。

ステップ4 詳細オプションを設定します。

[高度およびアーカイブファイルインスペクションオプション（25ページ）](#) を参照してください。

次のタスク

マルウェア防御ワークフローの次の手順に進みます。

[「マルウェア防御の設定方法（7ページ）」](#) を参照してください。

アクセスコントロール設定へのファイルポリシーの追加

アクセスコントロールポリシーは、複数のアクセスコントロールルールをファイルポリシーに関連付けることができます。ファイルインスペクションを許可アクセスコントロールルールまたはインタラクティブブロックアクセスコントロールルールに設定でき、これによって、トラフィックが最終宛先に到達する前に、異なるファイルおよびマルウェアのインスペクションプロファイルをネットワーク上のさまざまなタイプのトラフィックと照合できます。

始める前に

マルウェア防御ワークフローで、この時点までのタスクを実行します。

[マルウェア防御の設定方法（7ページ）](#) を参照してください。

手順

ステップ1 アクセス コントロール ポリシーでファイル ポリシーのガイドラインを確認します。（これらは以前に確認したファイルルールおよびファイルポリシーのガイドラインとは異なります。）

[ファイルインスペクションおよび侵入インスペクションの順序を確認してください。](#)

ステップ2 アクセス コントロール ポリシーとファイル ポリシーを関連付けます。

[マルウェア保護のためのアクセス コントロールルールの設定（11 ページ）](#) を参照してください

ステップ3 管理対象デバイスにアクセス コントロール ポリシーを割り当てます。

[アクセス コントロール ポリシーのターゲット デバイスの設定](#) を参照してください。

次のタスク

マルウェア防御ワークフローの次の手順に進みます。

[「マルウェア防御の設定方法（7 ページ）」](#) を参照してください。

マルウェア保護のためのアクセス コントロール ルールの設定



注意 [ファイルの検出（Detect Files）] または [ファイルのブロック（Block Files）] ルールで [ファイルの保存（Store files）] を有効化/無効化した場合、または [マルウェアクラウドルックアップ（Malware Cloud Lookup）] または [マルウェアブロック（Block Malware）] ファイルルールアクションを分析オプション（[Spero分析またはMSEXE（Spero Analysis or MSEXE）]、[動的分析（Dynamic Analysis）]、または [ローカルマルウェア分析（Local Malware Analysis）]）またはファイルの保存オプション（[マルウェア（Malware）]、[不明（Unknown）]、[正常（Clean）]、または [カスタム（Custom）]）と結合する最初のファイルルールを追加または最後のファイルルールを削除した場合には、設定の変更を展開する際に Snort プロセスが再起動され、一時的にトライフィックのインスペクションが中断されます。この中断中にトライフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトライフィックを処理する方法に応じて異なります。詳細は [Snort の再起動によるトライフィックの動作](#) を参照してください。



(注)

ファイルポリシーがアクセスコントロールルールに含まれている場合、オンライン正規化は自動的に有効になります。詳細については、[オンライン正規化プリプロセッサ](#) を参照してください。

始める前に

- AMP を含むファイル制御をアクセス コントロールルールで実行するためには、[適応型プロファイルの設定](#) で説明されているように、アダプティブ プロファイルを有効（デフォルト状態）にする必要があります。
- このタスクを実行するには、管理者、アクセス管理者、またはネットワーク管理者ユーザーである必要があります。

手順

ステップ1 ([ポリシー (Policy)] > [アクセス制御 (Access Control)] から) アクセス コントロールルールエディタで、[許可 (Allow)]、[インタラクティブブロック (Interactive Block)]、または [リセットしてインタラクティブブロック (Interactive Block with reset)] の [アクション (Action)] を選択します。

ステップ2 (レガシー UI のみ。) [検査 (Inspection)] をクリックします。

ステップ3 アクセスコントロールルールに一致するトラフィックを検査する場合は [ファイルポリシー (File Policy)] を選択し、または一致するトラフィックに対するファイルインスペクションを無効にする場合は [なし (None)] を選択します。

ステップ4 (オプション) [ロギング (Logging)] をクリックし、[ログファイル (Log Files)] チェックボックスをオフにして、一致する接続のファイルまたはマルウェアイベントのロギングを無効にします。

(注)

Cisco では、ファイルイベントおよびマルウェアイベントのロギングを有効のままにすることを推奨しています。

ステップ5 ルールを保存します。

ステップ6 [保存 (Save)] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します[設定変更の展開](#)を参照してください。

関連トピック

[ファイルポリシーの作成または編集](#) (24 ページ)

[Snort 再起動のシナリオ](#)

マルウェア防御のメンテナンスとモニタリングの設定

ネットワークの保護には継続的なメンテナンスが必要不可欠です。

始める前に

マルウェアからネットワークを保護するようにシステムを設定します。

[マルウェア防御の設定方法（7ページ）](#) および参照手順を確認してください。

手順

ステップ1 システムが常に最新かつ効果的に保護されていることを確認します。

[システムの保守：動的分析の対象となるファイルタイプの更新（23ページ）](#) を参照してください。

ステップ2 マルウェア関連のイベントおよびヘルス モニタリングのアラートを設定します。

「*Configuring マルウェア防御 Alerting*」の詳細および以下のモジュールの詳細については、[Cisco Secure Firewall Management Center アドミニストレーション ガイド](#)を参照してください。

- ローカルマルウェア分析 (Local Malware Analysis)
- セキュリティインテリジェンス
- デバイスでの脅威データの更新
- 侵入およびファイルイベント レート
- AMP for Firepower のステータス
- Secure Endpoint のステータス

次のタスク

マルウェア防御ワークフローの「次の項目について」を確認してください。

[「マルウェア防御の設定方法（7ページ）」](#) を参照してください。

マルウェア防御のためのクラウド接続

マルウェアからネットワークを保護するためには、パブリック クラウドまたはプライベート クラウドに接続する必要があります。

AMP クラウド

高度なマルウェア防御 (AMP) クラウドは、ビッグデータ分析や連続分析によりネットワーク上のマルウェアを検出およびブロックするシスコ ホステッド サーバーです。

AMP クラウドは、管理対象デバイスがネットワーク トラフィックから検出した潜在的なマルウェアの性質と、ローカルマルウェア分析とファイルの事前分類のデータ更新を提供します。

AMP クラウド接続の設定

組織で Secure Endpoint を展開し、データをインポートするように Firepower を設定している場合、システムは、スキャンレコード、マルウェア検出、隔離、侵害の兆候 (IOC) など、AMP クラウドからこのデータをインポートします。

シスコでは、既知のマルウェアの脅威についてシスコクラウドからデータを取得するために次のオプションを提供しています。

- **AMP パブリック クラウド**

Secure Firewall Management Center がパブリック シスコクラウドと直接通信します。米国、欧州、アジアに 3 つのパブリック AMP クラウドがあります。

- **AMP プライベート クラウド**

ネットワーク上に展開された AMP プライベート クラウドは、圧縮型、オンプレミス AMP クラウドおよびパブリック AMP クラウドに接続するための匿名プロキシとして機能します。詳細は、[Cisco AMP プライベート クラウド \(16 ページ\)](#) を参照してください。

Secure Endpoint と統合する場合、AMP プライベート クラウドにはいくつかの制限があります。[Secure Endpoint と AMP プライベート クラウド \(50 ページ\)](#) を参照してください。

動的分析クラウド

- **Secure Malware Analytics クラウド**

動的分析の送信に適したファイルを処理し、脅威スコアと動的分析レポートを提供するパブリック クラウド。Firepower は、Secure Malware Analytics 分析で 200 サンプル/日をサポートします。

- **オンプレミス Secure Malware Analytics アプライアンス**

組織のセキュリティポリシーがシステムによるネットワーク外部へのファイルの送信を許可しない場合は、オンプレミスアプライアンスを設定できます。このアプライアンスはパブリック Secure Malware Analytics クラウドには接続しません。

詳細については、[オンプレミスアプライアンスの動的分析 \(Cisco Secure Malware Analytics\) \(21 ページ\)](#) を参照してください。

AMP および Secure Malware Analytics クラウドへの接続の設定

- [AMP クラウド接続の設定 \(14 ページ\)](#)

- [動的分析接続 \(20 ページ\)](#)

AMP クラウド接続の設定

次のトピックでは、さまざまなシナリオでの AMP クラウド接続の設定について説明します。

- [AMP クラウドの選択 \(15 ページ\)](#)

- [AMP プライベート クラウドへの接続 \(17 ページ\)](#)

- [Firepower と Secure Endpoint の統合 \(50 ページ\)](#)

次のトピックも関連しています。

- [Cisco AMP プライベート クラウド \(16 ページ\)](#)
- [AMP クラウド接続の要件とベストプラクティス \(15 ページ\)](#)
- [AMP クラウドへの接続の管理 \(パブリックまたはプライベート\) \(18 ページ\)](#)

AMP クラウド接続の要件とベストプラクティス

AMP クラウド接続要件

AMP クラウドを設定するには、管理者ユーザーである必要があります。

Firewall Management Center が AMP クラウドと通信できるようにするには、[Cisco Secure Firewall Management Center アドミニストレーション ガイド](#) のセキュリティ、インターネットアクセス、および通信ポートを参照してください。

AMP とハイ アベイラビリティ

高可用性ペアの Firewall Management Center はファイル ポリシーおよび関連する設定を共有しますが、AMP クラウド接続、キャプチャされたファイル、ファイルイベント、マルウェアイベントを共有することはありません。運用の継続性を確保し、検出されたファイルのマルウェア処理が両方の Firewall Management Center で同じであるようにするために、アクティブとスタンバイ両方の Firewall Management Center がクラウドにアクセスできる必要があります。

これらの要件は、パブリック、プライベート両方の AMP クラウドに適用されます。

AMP クラウド接続とマルチテナンシー

マルチドメイン展開では、マルウェア防御接続はグローバル レベルで設定します。各 Firewall Management Center には、マルウェア防御接続を 1 つだけ設定できます。

AMP クラウドの選択

システムでは、デフォルトで米国 (US) AMP パブリッククラウドへの接続が設定され、有効になっています。（この接続は web インターフェイスにマルウェア防御と表示されますが、AMP for Firepower と表示される場合もあります。）マルウェア防御 クラウド接続の削除または無効化はできませんが、地理的に異なる AMP クラウドの切り替え、または AMP プライベート クラウドの接続が設定が可能です。

始める前に

- AMP プライベート クラウドを使用する場合は、このトピックの代わりに[AMP プライベート クラウドへの接続 \(17 ページ\)](#) を参照してください。

- Firepower が Secure Endpoint と統合されていない場合は、AMP クラウド接続を 1 つだけ設定できます。この接続には、**AMP for Networks** または **AMP for Firepower** というラベルが付けられています。
- Secure Endpoint を展開済みで、このアプリケーションを Firepower と統合するために 1 つ以上の AMP クラウドを追加する場合は、[Firepower と Secure Endpoint の統合（50 ページ）](#) を参照してください。
- [AMP クラウド接続の要件とベストプラクティス（15 ページ）](#) を参照してください。

手順

ステップ1 [統合（Integration）]>[AMP]>[AMP管理（AMP Management）]を選択します。

ステップ2 鉛筆をクリックし、既存のクラウド接続を編集します。

ステップ3 [クラウド名（Cloud Name）] ドロップダウンリストから、Secure Firewall Management Center から最も近い地域にあるクラウドを選択します。

APJC はアジア/太平洋/日本/中国です。

ステップ4 [保存（Save）] をクリックします。

次のタスク

- 展開がハイアベイラビリティ構成の場合は、[AMP クラウド接続の要件とベストプラクティス（15 ページ）](#) を参照してください。
- （任意）[AMP オプションの変更（19 ページ）](#)。

Cisco AMP プライベート クラウド

Firewall Management Center は AMP クラウドに接続し、ネットワーク トラフィックで検出されたファイルの判定結果をクエリしたり、レトロスペクティブマルウェアイベントを受信したりします。このクラウドはパブリックまたはプライベートに指定することができます。

部門のプライバシーやセキュリティ保護の観点から、モニター対象ネットワークと AMP クラウドとの間で頻繁にあるいは直接接続することが困難、または不可能な場合があります。このような場合、AMP クラウドの圧縮型、オンプレミスバージョンとして機能するシスコ独自の製品、ユーザーのネットワークと AMP クラウドの安全なメディエータである、Cisco AMP プライベート クラウドを設定できます。Firewall Management Center を AMP プライベート クラウドに接続すると、パブリック AMP クラウドとの既存の直接接続は無効化されます。

AMP プライベート クラウドを介した AMP クラウド ファンルとのすべての接続は、監視対象ネットワークのセキュリティとプライバシーを確保するための匿名プロキシとして機能します。これには、ネットワーク トラフィックで検出されたファイルの判定結果のクエリ、レトロ

スペクティブマルウェアイベントの受信などが含まれます。AMP プライベート クラウドは、エンドポイントデータを外部接続では一切共有しません。



(注) AMP プライベート クラウドは動的分析を実行しません。また、Cisco Collective Security Intelligence (CSI) に依存するその他の機能 (URL フィルタリングやセキュリティインテリジェンス フィルタリングなど) のための脅威インテリジェンスの匿名での取得もサポートしていません。

AMP プライベート クラウド (「AMPv」とも呼ばれる) の詳細については、<https://www.cisco.com/c/en/us/products/security/fireamp-private-cloud-virtual-appliance/index.html> を参照してください。

AMP プライベート クラウドへの接続

始める前に

- AMP のマニュアルの指示に従って、Cisco AMP プライベート クラウドまたはクラウドを設定します。設定時に、プライベート クラウドのホスト名をメモしてください。このホスト名は、Firewall Management Center で接続を設定するときに必要になります。
- Firewall Management Center が AMP プライベート クラウドと通信できることを確認し、プライベート クラウドがインターネットにアクセスし、パブリック AMP クラウドと通信できることを確認します。[Cisco Secure Firewall Management Center アドミニストレーションガイド](#) の「*Security, Internet Access, and Communication Ports*」にあるトピックを参照してください。
- 展開で Secure Endpoint と統合されていない場合は、Firewall Management Center ごとに AMP クラウド接続を 1 つだけ設定できます。この接続には、AMP for Networks または AMP for Firepower というラベルが付けられています。

Secure Endpoint と統合する場合には、複数の Secure Endpoint クラウド接続を設定できます。

手順

ステップ 1 [統合 (Integration)] > [AMP] > [AMP管理 (AMP Management)] を選択します。

ステップ 2 [AMP クラウド接続の追加 (Add AMP Cloud Connection)] をクリックします。

ステップ 3 [クラウド名 (Cloud Name) ドロップダウンリストから [プライベート クラウド (Private Cloud)] を選択します。

ステップ 4 名前を入力します。

この情報は、AMP プライベート クラウドによって生成または送信されるマルウェア イベントに表示されます。

ステップ 5 [ホスト (Host)] フィールドに、プライベート クラウドの設定時に設定したプライベート クラウドのホスト名を入力します。

AMP クラウドへの接続の管理（パブリックまたはプライベート）

- ステップ 6** [証明書アップロードパス（Certificate Upload Path）] フィールドの横にある [参照（Browse）] をクリックして、プライベートクラウドの有効な TLS または SSL 暗号化証明書の場所を参照します。詳細については、AMP プライベートクラウドのマニュアルを参照してください。
- ステップ 7** このプライベートクラウドをマルウェア防御と Secure Endpoint の両方に使用する場合は、[AMP for Firepowerに使用（Use for AMP for Firepower）] チェックボックスをオンにします。マルウェア防御通信を処理する別のプライベートクラウドを設定した場合は、このチェックボックスをオフにすることができます。これが唯一の AMP プライベートクラウド接続の場合は、オフにできません。
- マルチドメイン展開では、このチェックボックスはグローバルドメインにのみ表示されます。各 Firewall Management Center には、マルウェア防御接続を 1 つだけ設定できます。
- ステップ 8** プロキシを使用して AMP プライベートクラウドと通信するには、[接続にプロキシを使用（Use Proxy for Connection）] チェックボックスをオンにします。
- ステップ 9** [登録（Register）] をクリックし、AMP クラウドへの既存の直接接続を無効にすることを確認し、最後に AMP プライベートクラウド管理コンソールを続行して登録を完了することを確認します。
- ステップ 10** 管理コンソールにログインして登録プロセスを完了します。詳細については、AMP プライベートクラウドのマニュアルを参照してください。

次のタスク

高可用性展開では、両方の Management Center で AMP クラウド接続を設定します。これらの設定は同期されません。

AMP クラウドへの接続の管理（パブリックまたはプライベート）

Firewall Management Center を使用して、マルウェア防御や Secure Endpoint またはその両方に使用されるパブリックおよびプライベート AMP クラウドへの接続を管理します。

クラウドからマルウェア関連の情報を受信する必要がなくなった場合は、パブリックまたはプライベート AMP クラウドとの接続を削除します。Secure Endpoint または AMP プライベートクラウド管理コンソールを使用して接続の登録を解除しても、システムから接続を削除することにはならない点に注意してください。登録解除した接続は、Secure Firewall Management Center の Web インターフェイスに障害発生状態で表されます。

また、接続は一時的に無効にすることもできます。クラウド接続を再度有効化すると、クラウドは、無効化されていた期間にキューに保持していたデータを含めて、システムへのデータ送信を再開します。



- 注意** 無効化された接続の場合、プライベート AMP クラウドは、接続を再有効化するまでマルウェアイベントや侵害の兆候などを保存できます。まれに、イベントレートが非常に高い場合や接続が長期間無効になっていた場合など、接続無効中に生成されたすべての情報をクラウドで保存できないことがあります。

マルチドメイン展開では、現在のドメインで作成された接続が表示されます。これは、管理が可能な接続です。また、先祖ドメインで作成した接続も表示されますが、この接続は管理できません。下位ドメインの接続を管理するには、そのドメインに切り替えます。各 Firewall Management Center は、グローバルドメインに属するマルウェア防御接続を1つのみ保持できます。

手順

ステップ1 [統合 (Integration)] > [AMP] > [AMP管理 (AMP Management)] を選択します。

ステップ2 AMP クラウド接続を管理します。

- 削除 : [削除 (Delete)] (trash bin icon) をクリックして、選択内容を確認します。
 - 有効化または無効化 : スライダをクリックして、選択内容を確認します。
-

次のタスク

高可用性展開では、両方の Management Center で AMP クラウド接続を設定します。これらの設定は同期されません。

AMP オプションの変更

手順

ステップ1 [統合 (Integration)] > [その他の統合 (Other Integrations)] を選択します。

ステップ2 クラウドサービスをクリックします。

ステップ3 次のオプションを選択します。

表 1: AMP for Networks のオプション

オプション	説明
ローカルマルウェア検出の自動更新を有効にする (Enable Automatic Local Malware Detection Updates)	ローカルマルウェア検出エンジンは、Ciscoが提供する署名を使用して統計的にファイルを分析し、事前に分類します。このオプションを有効にすると、Firewall Management Center が 30 分ごとに署名の更新を確認します。

オプション	説明
マルウェアイベントの URL を Cisco と共有する (Share URI from Malware Events with Cisco)	ネットワーク トラフィックで検出されたファイルに関する情報を AMP クラウドに送信することができます。この情報には、検出されたファイルに関する URI 情報と SHA-256 ハッシュ値が含まれます。共有はオプトインですが、この情報を Cisco に送信すると、マルウェアを識別して追跡する今後の取り組みに役立ちます。

ステップ4 [保存 (Save)] をクリックします。

動的分析接続

動的分析の要件

動的分析を使用するには、管理者、アクセス管理者、またはネットワーク管理者のユーザーであり、グローバルドメインにいる必要があります。

適切なライセンスを使用して、システムが自動的に Secure Malware Analytics クラウドにアクセスします。

動的分析では、管理対象デバイスがポート 443 から Secure Malware Analytics Cloud またはオンプレミス Secure Malware Analytics Appliance に、直接あるいはプロキシを介してアクセスできる必要があります。

[動的分析の対象となるファイル \(39 ページ\)](#) も参照してください。

オンプレミス Secure Malware Analytics Appliance に接続する場合は、[オンプレミスの動的分析アプライアンスへの接続 \(21 ページ\)](#) の前提条件も参照してください。

デフォルト動的分析接続の表示

デフォルトで、Secure Firewall Management Center は、ファイルの送信やレポートの取得のために、パブリック Secure Malware Analytics Cloud に接続できます。この接続は、設定したり、削除したりすることはできません。

手順

ステップ1 [統合 (Integration)]>[AMP]>[AMPダイナミック分析接続 (Dynamic Analysis Connections)] を選択します。

ステップ2 [編集 (Edit)] (edit icon) をクリックします。

(注)

[統合 (Integration)] > [AMP] > [ダイナミック分析接続 (Dynamic Analysis Connections)] ページの [関連付け (Association)] (🔗) の詳細については、[パブリック クラウドでの動的分析の結果へのアクセスの有効化 \(23 ページ\)](#) を参照してください。

オンプレミスアプライアンスの動的分析 (Cisco Secure Malware Analytics)

組織にパブリックの Secure Malware Analytics クラウドへのファイルの送信に関してプライバシーまたはセキュリティ上の懸念がある場合、オンプレミスの Secure Malware Analytics アプライアンスを展開することができます。このオンプレミスアプライアンスは、パブリッククラウドと同様に適格なファイルをサンドボックス環境で実行し、脅威スコアと動的分析レポートをシステムに返します。ただし、このオンプレミスアプライアンスは、ご使用のネットワークの外部にあるパブリック クラウドや他のすべてのシステムとは通信しません。

オンプレミス Secure Malware Analytics アプライアンスの詳細については、<https://www.cisco.com/c/en/us/products/security/threat-grid/index.html> を参照してください。

オンプレミスの動的分析アプライアンスへの接続

ネットワークでオンプレミスの Secure Malware Analytics アプライアンスをインストールする場合は、動的分析接続を設定してファイルを送信し、アプライアンスからレポートを取得できます。オンプレミスのアプライアンスの動的分析接続を設定するには、オンプレミスのアプライアンスに Secure Firewall Management Center を登録します。

始める前に

- オンプレミス Secure Malware Analytics アプライアンスを設定します。

このアプライアンスのドキュメントは、<https://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。

バージョンの要件については、『Cisco Firepower Compatibility Guide』を参照してください。

- Secure Malware Analytics アプライアンスが自己署名公開キー証明書を使用している場合は、Secure Malware Analytics アプライアンスから証明書をダウンロードします。詳細については、Secure Malware Analytics アプライアンスの管理者ガイド参照してください。

認証局 (CA) によって署名された証明書を使用する場合、証明書は次の要件を満たしている必要があります。

- サーバーキーと署名付き証明書を Secure Malware Analytics アプライアンスにインストールする必要があります。Secure Malware Analytics アプライアンスの管理者ガイドのアップロード手順に従います。
- CA のマルチレベル署名チェーンがある場合、Firewall Management Center にアップロードされる単一のファイルに必要なすべての中間証明書とルート証明書が含まれている必要があります。

- すべての証明書は PEM でエンコードされている必要があります。
- ファイルの改行は、DOS ではなく UNIX でなければなりません。
- プロキシを使用してオンプレミスのアプライアンスに接続する場合は、プロキシを設定します。Cisco Secure Firewall Management Center アドミニストレーションガイドの「*Modify Firewall Management Center Management Interfaces*」を参照してください。
- 管理対象デバイスは、ポート 443 で直接またはプロキシを介して Secure Malware Analytics アプライアンスにアクセスできる必要があります。

手順

- ステップ1** [統合 (Integration)]>[AMP]>[AMPダイナミック分析接続 (Dynamic Analysis Connections)] を選択します。
- ステップ2** [新しい接続を追加 (Add New Connection)] をクリックします。
- ステップ3** 名前を入力します。
- ステップ4** [ホスト (Host)] に入力します。
- ステップ5** [証明書のアップロード (Certificate Upload)] の横にある [参照 (Browse)] をクリックして、オンプレミスのアプライアンスの証明書をアップロードします。
- Secure Malware Analytics アプライアンスから自己署名証明書が提示される場合は、そのアプライアンスからダウンロードした証明書をアップロードします。
- Secure Malware Analytics アプライアンスから CA 署名付き証明書が提示される場合は、証明書署名チェーンを含むファイルをアップロードします。
- ステップ6** 設定済みのプロキシを使用して接続を確立する場合は、[使用可能な場合はプロキシを使用する (Use Proxy When Available)] チェックボックスをオンにします。
- ステップ7** [登録 (Register)] をクリックします。
- ステップ8** [はい (Yes)] をクリックして、オンプレミスの Secure Malware Analytics アプライアンスのログインページを表示します。
- ステップ9** オンプレミスの Secure Malware Analytics アプライアンスにユーザー名とパスワードを入力します。
- ステップ10** [サインイン (Sign in)] をクリックします。
- ステップ11** 次の選択肢があります。
- 以前にオンプレミスのアプライアンスに Secure Firewall Management Center を登録した場合は、[戻る (Return)] をクリックします。
 - Secure Firewall Management Center を登録していない場合は、[アクティベーション (Activate)] をクリックします。

パブリック クラウドでの動的分析の結果へのアクセスの有効化

Secure Malware Analytics では、分析されたファイルに関して、Firewall Management Center で使用できるレポートよりもさらに詳細なレポートが提供されます。組織に Secure Malware Analytics Cloud アカウントがある場合、Secure Malware Analytics ポータルに直接アクセスして、管理対象デバイスから分析のために送信されたファイルに関する追加の詳細を表示できます。ただし、プライバシー上の理由から、ファイル分析の詳細は、そのファイルを提出した組織だけが使用できます。そのため、この情報を表示するためには、Firewall Management Center を、管理対象デバイスによって提出されたファイルと関連付ける必要があります。

始める前に

Secure Malware Analytics クラウドのアカウントがあり、アカウントのログイン情報を持ってい る必要があります。

手順

ステップ1 [統合 (Integration)]>[AMP]>[AMPダイナミック分析接続 (Dynamic Analysis Connections)] を選択します。

ステップ2 Secure Malware Analytics クラウドに対応するテーブル行で、[関連付け (Association)] (🔗) をクリックします。

Secure Malware Analytics ポータル ウィンドウが開きます。

ステップ3 Secure Malware Analytics クラウドにサインインします。

ステップ4 [クエリの送信 (Submit Query)] をクリックします。

(注)

[デバイス (Devices)] フィールドのデフォルト値を変更しないでください。

このプロセスで問題が発生した場合は、Secure Malware Analytics 担当者にお問い合わせください。

この変更が有効になるまでに最大で 24 時間かかることがあります。

次のタスク

関連付けが有効化された後、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Viewing Dynamic Analysis Results in the Cisco Cloud」を参照してください。

システムの保守：動的分析の対象となるファイルタイプの更新

動的分析の対象となるファイルタイプのリストは、定期的に更新される（多くても 1 日 1 回）脆弱性データベース (VDB) によって決定されます。管理者ユーザーは、動的分析の対象となるファイルタイプを更新できます。

システムに現在のリストがあることを次のように確認します。

手順

ステップ1 次のいずれかを実行します。

- ・（推奨）Cisco Secure Firewall Management Center アドミニストレーションガイドで説明されている脆弱性データベース更新の自動化を参照してください。
- ・新しいVDBの更新を定期的に確認し、必要に応じて、Cisco Secure Firewall Management Centerアドミニストレーションガイドで説明されているようにVDBを手動で更新します。このオプションを選択した場合は、定期的な通知をスケジュールすることをお勧めします。

ステップ2 ファイルポリシーで[動的分析可能 (Dynamic Analysis Capable)]ファイルタイプカテゴリではなく個々のファイルタイプを指定する場合は、ファイルポリシーを更新して新しくサポートされるファイルタイプを使用します。

ステップ3 対応するファイルタイプのリストが変更されている場合は、管理対象デバイスに展開します。

ファイルポリシーとファイルルール

ファイルポリシーの作成または編集

始める前に

マルウェア保護のポリシーを設定する場合は、[ファイルポリシーの設定 \(10 ページ\)](#) の必要なすべての手順を参照してください。

手順

ステップ1 [ポリシー (Policies)] > [アクセス制御 (Access Control)] 見出し > [マルウェアとファイル (Malware & File)] を選択します。

ステップ2 新しいポリシーを作成するか、既存のポリシーを編集します。

既存のポリシーを編集する場合：代わりに [表示 (View)] (⌚) 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

ヒント

既存のファイルポリシーのコピーを作成するには、[コピー (Copy)] (Cop) をクリックして、表示されるダイアログボックスで新しいポリシーの固有名を入力します。その後、そのコピーを変更できます。

ステップ3 ファイルルールの作成 (42 ページ) の説明に従って、ファイルポリシーに1つ以上のルールを追加します。

ステップ4 必要に応じて、[詳細 (Advanced)] を選択し、高度およびアーカイブファイルインスペクションオプション (25 ページ) の説明に従って詳細オプションを設定します。

ステップ5 ファイルポリシーを保存します。

次のタスク

- マルウェア保護のポリシーを設定する場合は、ファイルポリシーの設定 (10 ページ) の必要なその他の手順を参照してください。
- 該当しない場合は、次のようにになります。
 - アクセスコントロール設定へのファイルポリシーの追加 (10 ページ) の説明に従って、アクセスコントロールルールにファイルポリシーを追加します。
 - 設定変更を展開します設定変更の展開を参照してください。

高度およびアーカイブファイルインスペクションオプション

ファイルポリシーエディタの [詳細設定 (Advanced Settings)] には、次の一般オプションがあります。

- [初回ファイル分析 (First Time File Analysis)] : 最初に検出されたファイルを分析すると同時にAMPクラウドの判定結果を保留にする場合にこのオプションを選択します。ファイルは、マルウェアクラウドルックアップとSpero分析、ローカルマルウェア分析、またはダイナミック分析を実行するように設定されているルールに一致する必要があります。このオプションの選択を解除すると、初めて検出されたファイルの判定結果が[不明 (Unknown)]になります
- [カスタム検出リストを有効にする (Enable Custom Detection List)] : カスタム検出リストにあるファイルをブロックします。
- [クリーンリストを有効にする (Enable Clean List)] : 有効にすると、このポリシーはクリーンリストにあるファイルを許可します。
- [AMPクラウドの判定結果が不明な場合は、脅威スコアに基づいて判定結果をオーバーライドします (If AMP Cloud disposition is Unknown, override disposition based upon threat score)] : オプションを選択します。
- [無効 (Disabled)] を選択すると、システムはAMPクラウドによって提供された判定結果をオーバーライドしません。

■ アーカイブ ファイル

- 脅威スコアのしきい値を設定すると、動的分析スコアがしきい値以下である場合、AMP クラウドの判定が[不明 (Unknown)]のファイルはマルウェアと見なされます。
- しきい値に低い値を選択すると、マルウェアとして扱われるファイルの数が増えます。ファイルポリシーで選択したアクションによっては、その結果、ブロックされるファイルの数が増える可能性があります。
- 数値の脅威スコアの範囲については、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「Threat Scores and Dynamic Analysis Summary Reports」を参照してください。

ファイルポリシーエディタの [詳細設定 (Advanced Settings)] には、次のアーカイブファイル検査オプションがあります。

- [アーカイブを検査する (Inspect Archives)] : アクセスコントロールの詳細設定の [保存する最大ファイルサイズ (Maximum file size to store)] と同じ大きさのアーカイブファイルまで、アーカイブファイルのコンテンツのインスペクションをできるようにします。
- [暗号化されたアーカイブのブロック (Block Encrypted Archives)] : パスワードで保護されたアーカイブをブロックします。
- [検査不可能なアーカイブをブロックする (Block Uninspectable Archives)] : 暗号化以外の理由でシステムが検査できないコンテンツを含むアーカイブファイルをブロックします。これは通常、破損したファイル、または指定した最大アーカイブ深度を超えるファイルに適用されます。
- [最大アーカイブ深度 (Max Archive Depth)] : 指定した深度を超えるネストされたアーカイブファイルをブロックします。トップレベルのアーカイブファイルはこの数で考慮されません。深さは最初にネストされたファイルで 1 から始まります。

アーカイブ ファイル

アーカイブ ファイルとは、.zip や .rar ファイルなどの他のファイルを含むファイルです。

ブロック アクションを含むファイルルールにアーカイブ内のいづれかの個別ファイルが一致する場合は、その個別ファイルだけでなくアーカイブ全体がブロックされます。

アーカイブファイルのインスペクションのオプションについては、高度およびアーカイブファイルインスペクションオプション (25 ページ) を参照してください。

検査可能なアーカイブ ファイル

・ファイル タイプ

検査可能なアーカイブファイルタイプの完全なリストが FMC Web インターフェイスのファイルルール設定ページに表示されます。このページを表示するには、ファイルルールの作成 (42 ページ) を参照してください。

検査可能な格納ファイルが同じページに表示されます。

・ファイル サイズ (File size)

アクセス コントロールの詳細設定の [保存する最大ファイルサイズ (Maximum file size to store)] ファイル ポリシーと同じ大きさのアーカイブ ファイルまで検査できます。

• ネストされたアーカイブ

アーカイブ ファイルには他のアーカイブ ファイルを含められます。その結果、複数のアーカイブ ファイルが含めることができます。ファイルがネストされるレベルは、そのアーカイブ ファイルの深さです。トップレベルのアーカイブ ファイルは深さの数に含まれないことに注意してください。深さは最初にネストされたファイルで 1 から始まります。

システムは、最も外側のアーカイブ ファイル (レベル 0) の下にネストされた最大 3 つのレベルのファイルを検査できます。その深さ (または指定したそれより低い最大深さ) を超えるアーカイブ ファイルをブロックするようファイル ポリシーを設定できます。

最大アーカイブ ファイルの深さ 3 を超えるファイルをブロックしないよう選択した場合、抽出可能な内容と深さ 3 以上でネストされた内容を含むアーカイブ ファイルがモニター対象のトラフィックに現れると、システムは検査可能だったファイルについてのみデータを検査して報告します。

圧縮解除されたファイルに適用できるすべての機能 (動的分析やファイルストレージなど) は、アーカイブ ファイル内のネストされたファイルに使用可能です。

• 暗号化ファイル

コンテンツが暗号化されているか検査できないアーカイブをブロックするように設定できます。

• 検査されないアーカイブ

アーカイブ ファイルを含むトラフィックがセキュリティインテリジェンスのブロックリストまたはブロックしないリストに登録された場合、またはトップレベルのアーカイブ ファイルの SHA-256 値がカスタム検出リストにある場合、システムはアーカイブ ファイルの内容を検査しません。

ネストされたファイルがブロックされた場合、アーカイブ 全体がブロックされます。しかし、ネストされたファイルが許可された場合、アーカイブ は自動的に渡されません (他のネストされたファイルおよび特性による)。

rar5 を含む一部の .rar アーカイブ 内の .Exe ファイルは検出できません。

アーカイブ ファイルの性質

アーカイブ ファイルの性質は、アーカイブ 内部のファイルに割り当てられた性質に基づきます。識別されたマルウェア ファイルを含んでいるすべてのアーカイブ は、マルウェア (Malware) の性質になります。識別されたマルウェア ファイルを含んでいないアーカイブ の場合、不明なファイルが 1 つでも含まれていれば不明 (Unknown) の性質、クリーン ファイルのみが含まれていればクリーン (Clean) の性質になります。

カスタムリストを使用したファイル性質のオーバーライド

表 2: 内容に基づくアーカイブファイルの性質

アーカイブファイルの性質	不明なファイルの数	クリーンファイルの数	マルウェアファイルの数
Unknown	1つ以上	任意	0
Clean	[0]	1つ以上	[0]
Malware	すべて	すべて	1つ以上

他のファイルと同様に、アーカイブファイルにも、該当する性質に関する条件が適用される場合はカスタム検出 (Custom Detection) または利用不可 (Unavailable) の性質が割り当てられます。

アーカイブの内容と詳細の表示

アーカイブファイルの内容を検査するようにファイルポリシーが設定されている場合は、[分析 (Analysis)] > [ファイル (Files)] メニューのページにあるコンテキストメニューおよびネットワークファイルトラジェクトリビュアを使用して、アーカイブファイルがファイルイベント、マルウェアイベントに現れた場合、またはキャプチャされたファイルとして現れた場合に、アーカイブ内のファイルに関する情報を表示できます。

アーカイブのすべてのファイルコンテンツは表形式でリストされます。そのリストには、名前、SHA-256ハッシュ値、タイプ、カテゴリ、およびアーカイブの深さといった関連情報の概略が含まれています。ネットワークファイルトラジェクトリアイコンはファイルごとに表示されます。そのアイコンをクリックすることで、特定のファイルに関する詳細な情報を表示することができます。

カスタムリストを使用したファイル性質のオーバーライド

AMP クラウドにあるファイルの性質が不正確だとわかっている場合、クラウドから性質を上書きするファイルの SHA-256 値をファイルリストに追加できます。

- AMP クラウドがクリーンの性質を割り当てた場合と同じ方法でファイルを扱うには、クリーンリストにファイルを追加します。
- AMP クラウドがマルウェアの性質を割り当てた場合と同じ方法でファイルを扱うには、カスタム検出リストにファイルを追加します。

これ以降に検出された場合、デバイスでは、ファイルの性質を再評価せずに許可またはブロックできます。ファイルポリシーに応じてクリーンリストまたはカスタム検出リストを使用できます。



(注)

ファイルの SHA-256 値を計算するには、マルウェアクラウドルックアップを実行するか、一致ファイルでマルウェアをブロックするルールをファイルポリシーで設定する必要があります。

Firepower でのファイルリストの使用の詳細については、[ファイルリスト](#)を参照してください。

または、該当する場合は[Secure Endpoint からの一元的なファイルリスト \(29 ページ\)](#) を参照します。

Secure Endpoint からの一元的なファイルリスト

組織で Secure Endpoint を展開している場合、Firepower は AMP クラウドにファイルの性質を照会するときに、Secure Endpoint で作成されたブロックリストおよび許可リストを使用できます。

要件：

- 組織で AMP パブリック クラウドを使用している必要がある。
- 組織で Secure Endpoint を導入している。
- [Firepower と Secure Endpoint の統合 \(50 ページ\)](#) の手順を使用して、システムを Secure Endpoint に登録している。

これらのリストを作成して展開するには、Secure Endpoint のマニュアルまたはオンラインヘルプを参照してください。



(注) Firepower で作成されたファイルリストは、Secure Endpoint で作成されたファイルリストをオーバーライドします。

ファイルポリシーの管理

[ファイルポリシー (File Policies)] ページには、既存のファイルポリシーが最終更新日とともに表示されます。このページは、ファイルポリシーの管理に使用できます。



(注) 動的分析の対象となるファイルタイプのリストが更新されたかどうか検査するために、システムは更新をチェックします（多くても 1 日に 1 回）。対象になるファイルタイプのリストが変更された場合、これはファイルポリシーの変更を意味します。このファイルポリシーを使用するアクセスコントロールポリシーがいずれかのデバイスに展開されている場合、そのアクセスコントロールポリシーには失効マークが付けられます。更新したファイルポリシーがデバイスで有効になるには、まず、ポリシーを展開しておく必要があります。 [システムの保守：動的分析の対象となるファイルタイプの更新 \(23 ページ\)](#) を参照してください。

手順

ステップ1 [ポリシー (Policies)] > [アクセス制御 (Access Control)] 見出し > [マルウェアとファイル (Malware & File)] を選択します。

ステップ2 ファイルポリシーを管理します。

- ・[比較 (Compare)] : [ポリシーの比較 (Compare Policies)] をクリックします（「[ポリシーの比較](#)」を参照）。
- ・作成：ファイルポリシーを作成するには、[新規ファイルポリシー (New File Policy)] をクリックし、[ファイルポリシーの作成または編集 \(24 ページ\)](#) で説明する手順を実行します。
- ・コピー：ファイルポリシーをコピーするには、[コピー (Copy)] (F5) をクリックします。
代わりに [表示 (View)] (F1) 表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ・削除：ファイルポリシーを削除するには、[削除 (Delete)] (Shift+Delete) をクリックし、プロンプトが表示されたら [はい (Yes)] と [OK] をクリックします。
コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ・[展開 (Deploy)] : [展開 (Deploy)] > [展開 (Deployment)] をクリックします（[設定変更の展開](#) を参照）。
- ・編集：既存のファイルポリシーを変更するには、[編集 (Edit)] (F6) をクリックします。
- ・レポート：[レポート (Report)] (F7) をクリックします（[現在のポリシーレポートの生成](#) を参照）。

ファイルルール

ファイルのポリシーには、その親であるアクセスコントロールポリシーと同様に、各ルールの条件に一致したファイルをシステムがどのように処理するかを決定するルールが含まれています。ファイルタイプ、アプリケーションプロトコル、転送方向の違いに応じて異なるアクションを実行する別個のファイルルールを設定できます。

たとえば、あるファイルがルールに一致する場合、ルールで以下を実行できます。

- ・単純なファイルタイプ照合に基づいてファイルを許可またはブロックする
- ・性質に基づいてファイルをブロックする（悪意があることを示す評価の有無に関係なく）

- デバイスにファイルを保存する（詳細については、[キャプチャされたファイルとファイルストレージ（39 ページ）](#) を参照してください）
- ローカルマルウェア分析、Spero 分析、または動的分析のために、保存（キャプチャ）したファイルを送信する

さらに、ファイルポリシーによって以下を実行できます。

- クリーンリストまたはカスタム検出リストのエントリに基づいて、ファイルがクリーンまたはマルウェアである場合と同じ方法で自動的にファイルを扱う
- ファイルの脅威スコアが、設定可能なしきい値を超えた場合、マルウェアと同じ方法でファイルを扱う
- アーカイブファイル（.zip や .rar など）の内容を検査する
- アーカイブファイルの内容が暗号化されている場合、アーカイブのネスト レベルが最大 レベル指定値より深い場合、あるいはその反対で検査できない場合、アーカイブファイルをブロックする

ファイルルールのコンポーネント

表 3: ファイルルールのコンポーネント

ファイルルールのコンポーネント	説明
アプリケーションプロトコル	システムは、FTP、HTTP、SMTP、IMAP、POP3、および NetBIOS-ssn (SMB) を介して伝送されるファイルを検出し、検査できます。デフォルトの [任意 (Any)] は、HTTP、SMTP、IMAP、POP3、FTP、および NetBIOS-ssn (SMB) トライフィック内のファイルを検出します。パフォーマンスを向上させるには、ファイルルールごとに、これらのアプリケーションプロトコルのうち 1 つだけでファイルを検出するよう限定できます。
転送の方向	ダウンロードされるファイルに対して、FTP、HTTP、IMAP、POP3、および NetBIOS-ssn (SMB) の着信トライフィックを検査できます。アップロードされるファイルに対しては、FTP、HTTP、SMTP、および NetBIOS-ssn (SMB) の発信トライフィックを検査できます。 ヒント [任意 (Any)] を使用すると、ユーザが送信しているか受信しているかには関係なく、多数のアプリケーションプロトコルを介したファイルが検出されます。

■ ファイルルールのコンポーネント

ファイルルールのコンポーネント	説明
ファイルのカテゴリとタイプ	<p>システムは、さまざまなタイプのファイルを検出できます。これらのファイルタイプは、マルチメディア (swf, mp3)、実行可能ファイル (exe, torrent)、PDFなどの基本的なカテゴリにグループ分けされます。個々のファイルタイプを検出したり、ファイルタイプカテゴリ全体を検出したりするよう、ファイルルールを設定できます。</p> <p>たとえば、すべてのマルチメディアファイルをロックしたり、ShockWave Flash (swf) ファイルのみをロックしたりできます。または、ユーザが BitTorrent (torrent) ファイルをダウンロードしたときにアラートを出すよう、システムを設定できます。</p> <p>実行可能ファイルには、マクロとスクリプトを実行できるファイルタイプが含まれていることに注意してください。マルウェアが含まれている可能性があるためです。</p> <p>システムで検査可能なファイルタイプのリストについては、[ポリシー (Policies)] > [アクセス制御 (Access Control)] > [マルウェアとファイル (Malware & File)] を選択して、一時的な新しいファイルポリシーを作成してから、[ルールの追加 (Add Rule)] をクリックします。ファイルタイプカテゴリを選択すると、システムが検査できるファイルタイプが [ファイルタイプ (File Types)] リストに表示されます。</p> <p>(注) 頻繁にトリガーされるファイルルールは、システムパフォーマンスに影響を与える可能性があります。たとえば、HTTP トラフィックでマルチメディアファイルを検出しようとすると (たとえば YouTube は多量の Flash コンテンツを伝送します)、膨大な数のイベントが生成される可能性があります。</p>
ファイルルールアクション	<p>ファイルルールのアクションによって、ルールの条件に一致したトランザクションをシステムが処理する方法が決定されます。</p> <p>選択したアクションに応じて、システムでファイルを保存するか、ファイルに対して Spero 分析、ローカルマルウェア分析、または動的分析を実行するかを設定できます。[ブロック (Block)] アクションを選択すると、システムでブロックされた接続をリセットするかどうかも設定できます。</p> <p>これらのアクションおよびオプションの説明については、ファイルルールアクション (33 ページ) を参照してください。</p> <p>ファイルルールは数値上の順番ではなく、ルールアクションの順番で評価されます。詳細については、「ファイルルールアクション: 評価順序 (41 ページ)」を参照してください。</p>

ファイルルールアクション

ファイルルールを使用すると、ロギング、ブロック、またはマルウェアスキャンの対象となるファイルタイプを詳細に制御できます。各ファイルルールには、ルールの条件に一致するトラフィックがシステムによってどのように処理されるかを決定する1つのアクションが関連付けられます。効果を発揮するには、ファイルポリシーに1つ以上のルールが含まれている必要があります。1つのファイルポリシー内に、ファイルタイプ、アプリケーションプロトコル、転送方向の違いに応じて異なるアクションを実行する別々のルールを使用できます。

ファイルルールアクション

- [ファイル検出 (Detect Files)] ルールを使用すると、ファイルの伝送を許可しながら、特定のファイルタイプの検出をデータベースに記録できます。
- ファイルブロックルールを使用すると、特定のファイルタイプをブロックできます。ファイル転送がブロックされたときに接続をリセットするオプション、およびキャプチャされたファイルを管理対象デバイスに保存するオプションを設定できます。
- [マルウェアクラウドルックアップ (Malware Cloud Lookup)] ルールを使用すると、ネットワークを通過するファイルの性質を取得して記録したうえでその伝送を許可できます。
- [マルウェアブロック (Block Malware)] ルールを使用すると、特定のファイルタイプのSHA-256ハッシュ値を計算した後、AMPクラウドを照会して、ネットワークを通過するファイルにマルウェアが含まれているかどうかを判断し、脅威を示すファイルをブロックできます。

ファイルルールアクションのオプション

選択したアクションに応じて、さまざまなオプションがあります。

ファイルルールアクションのオプション	ファイルのブロックが可能か	マルウェアのブロックが可能か	ファイルの検出が可能か	マルウェアクラウドルックアップが可能か
MSEXЕ用のSpero分析* (Spero Analysis* for MSEXЕ)	No	はい：実行可能 ファイルを送信できます	No	はい：実行可能 ファイルを送信できます
動的分析* (Dynamic Analysis*)	No	はい：不明なファイルの性質の実行可能ファイルを送信できます	No	はい：不明なファイルの性質の実行可能ファイルを送信できます
容量処理 (Capacity Handling)	×	○	×	○

■ マルウェア防御オプション（ファイルルールアクション）

ファイルルールアクションのオプション	ファイルのブロックが可能か	マルウェアのブロックが可能か	ファイルの検出が可能か	マルウェアクラウドルックアップが可能か
ローカルマルウェア分析 (Local Malware Analysis)	×	○	×	○
接続のリセット (Reset Connection)	はい（推奨）	はい（推奨）	×	×
ファイルの保存 (Store files)	はい：一致するすべてのファイルを保存できます	はい：選択したファイルの性質に一致するファイルタイプを保存できます	はい：一致するすべてのファイルを保存できます	はい：選択したファイルの性質に一致するファイルタイプを保存できます

* これらのオプションの詳細については、[マルウェア防御オプション（ファイルルールアクション）（34 ページ）](#) およびそのサブトピックを参照してください。



注意 [ファイルの検出 (Detect Files)] または [ファイルのブロック (Block Files)] ルールで [ファイルの保存 (Store files)] を有効化または無効化、または [マルウェアクラウドルックアップ (Malware Cloud Lookup)] または [マルウェアブロック (Block Malware)] ファイルルールアクションを分析オプション ([Spero 分析または MSEXE (Spero Analysis or MSEXE)]、[動的分析 (Dynamic Analysis)]、または [ローカルマルウェア分析 (Local Malware Analysis)]) またはファイルの保存オプション ([マルウェア (Malware)]、[不明 (Unknown)]、[正常 (Clean)]、または [カスタム (Custom)]) と結合する最初のファイルルールを追加または最後のファイルルールを削除すると、設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細は[Snort の再起動によるトラフィックの動作](#)を参照してください。

マルウェア防御オプション（ファイルルールアクション）

システムでは、ファイルにマルウェアが含まれるかどうかを判断するために、ファイルインスペクションと分析のいくつかの方法が適用されます。

ファイルルールでオプションを有効にするオプションに応じて、システムは次のツールと順序でファイルを検査します。

1. [Spero 分析（37 ページ）](#) および [AMP クラウドのルックアップ（37 ページ）](#)
2. [ローカルマルウェア分析（Local Malware Analysis）（37 ページ）](#)

3. 動的分析 (Dynamic Analysis) (38 ページ)

これらのツールの比較については、[マルウェア防御のオプションの比較 \(35 ページ\)](#) を参照してください。

(該当する場合は、そのファイルタイプに基づいてすべてのファイルをブロックすることができます。詳細については、[ファイルタイプによるすべてのファイルのブロック \(41 ページ\)](#) を参照してください)。

(オプション) [Secure Endpoint を使用したマルウェア防御 \(47 ページ\)](#) およびサブトピックからシスコの Secure Endpoint 製品に関する情報も参照してください。

マルウェア防御のオプションの比較

次の表では、各タイプのファイル分析の利点と欠点、および各マルウェア防御方法によってファイルの性質が決定される方法について説明します。

分析タイプ	利点	制限事項	マルウェアの特定
Spero 分析	実行可能ファイルの構造分析。Spero シグネチャを分析のために AMP クラウドに送信します。	ローカルマルウェア分析または動的分析よりも詳細度が低くなります。実行可能ファイル専用です。	マルウェアの特定がポジティブの場合にのみ、性質が [不明 (Unknown)] から [マルウェア (Malware)] に変更されます。
ローカルマルウェア分析 (Local Malware Analysis)	動的分析より消費するリソースが少なく、特に検出されたマルウェアが一般的な場合は結果がより迅速に返されます。	動的分析よりも結果の詳細度が低くなります。	マルウェアの特定がポジティブの場合にのみ、性質が [不明 (Unknown)] から [マルウェア (Malware)] に変更されます。
動的分析* (Dynamic Analysis*)	を使用した不明なファイルの詳細な分析 Secure Malware Analytics	対象ファイルはパブリッククラウドまたはオンプレミスアプライアンスにアップロードされます。分析の完了には少し時間がかかります	脅威スコアによってファイルの悪意の度合いが決定されます。性質はファイルポリシーに設定されている脅威スコアしきい値に基づいている場合があります。
Spero 分析とローカルマルウェア分析	AMP クラウドのリソースを使用してマルウェアを特定しながら、ローカルマルウェア分析と動的分析を設定するよりも少ないリソースを消費します。	動的分析、Spero 分析よりも詳細度が低くなります。実行可能ファイル専用です。	マルウェアの特定がポジティブの場合にのみ、性質が [不明 (Unknown)] から [マルウェア (Malware)] に変更されます。

マルウェア防御のオプションの比較

分析タイプ	利点	制限事項	マルウェアの特定
Spero 分析と動的分析	ファイルおよび Spero シグネチャの送信時に AMP クラウドの全機能を使用します	ローカルマルウェア分析を使用する場合よりも結果の取得に時間がかかります	マルウェアの可能性があるとして事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。ファイルポリシーで設定されている脅威スコアしきい値に基づいて、および Spero 分析でマルウェアが特定された場合は、性質が [不明 (Unknown)] から [マルウェア (Malware)] に変更されます。
ローカルマルウェア分析と動的分析	両方のタイプのファイル分析を使用することで詳細な結果が得られます	どちらか一方の場合よりも消費するリソースが多くなります	マルウェアの可能性があるとして事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。ローカルマルウェア分析でマルウェアが特定された場合、またはファイルポリシーで設定されている脅威スコアしきい値に基づいて、性質が [不明 (Unknown)] から [マルウェア (Malware)] に変更されます。
Spero 分析、ローカルマルウェア分析、および動的分析	詳細結果	3つすべてのタイプのファイル分析を実行するため消費するリソースが最も多くなります	マルウェアの可能性があるとして事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。Spero 分析またはローカルマルウェア分析でマルウェアが特定された場合、またはファイルポリシーで設定されている脅威スコアしきい値に基づいて、性質が [不明 (Unknown)] から [マルウェア (Malware)] に変更されます。

分析タイプ	利点	制限事項	マルウェアの特定
(指定されたファイルタイプのすべてのファイルの送信をロック)	マルウェア防御のライセンスは必要ありません (このオプションは技術的なマルウェア防御オプションではありません。)	正規ファイルもロックされます	(分析は実行されません。)



(注) 事前分類はファイルの性質を決定するものではありません。ファイルが動的分析の対象であるかどうかを判断する要因の 1 つにすぎません。

Spero 分析

Spero 分析では、実行可能なファイルのファイル構造の特性（メタデータやヘッダー情報など）を調べます。この情報に基づいて Spero シグネチャを生成した後、ファイルが対象の実行可能なファイルである場合、デバイスはそれを AMP クラウド内の Spero ヒューリスティックエンジンに送信します。Spero シグネチャに基づいて、そのファイルがマルウェアかどうかを Spero エンジンが決定します。また、ファイルを AMP クラウドに送信することなく、Spero 分析用に送信するようにルールを設定することもできます。

Spero 分析用にファイルを手動で送信することはできません。

AMP クラウドのロックアップ

高度なマルウェア防御を使用した評価の対象となるファイルの場合、Firewall Management Center はマルウェアクラウドロックアップを実行し、その SHA-256 ハッシュ値に基づいてファイルの性質を AMP クラウドに照会します。

パフォーマンスを改善するために、システムはクラウドから返される性質をキャッシュ化し、AMP クラウドでクエリを実行する代わりに、既知のファイルのキャッシュ済みの性質を使用します。このキャッシュの詳細については、[キャッシュ済み性質の有効期間（38 ページ）](#) を参照してください。

ローカルマルウェア分析（*Local Malware Analysis*）

ローカルマルウェア分析では、管理対象デバイスで Talos インテリジェンスグループから提供される検出ルールを使用して、実行可能ファイル、PDF、Office 文書、およびその他のタイプのファイルで最も一般的なタイプのマルウェアの有無をローカルで検査することができます。ローカル分析では AMP クラウドにクエリを実行せず、ファイルも実行しないため、ローカルマルウェア分析では時間とシステムリソースが節約できます。

システムはローカルマルウェアによってマルウェアを識別すると、その既存のファイルの性質を [不明 (Unknown)] から [マルウェア (Malware)] に更新します。その上で、システムは新しいマルウェアイベントを生成します。システムはマルウェアを識別しなかったとしても、

■ キャッシュ済み性質の有効期間

ファイルの性質を [不明 (Unknown)] から [正常 (Clean)] に更新することはしません。ローカルマルウェア分析を実行した後、システムはファイル情報 (SHA-256 ハッシュ値、タイムスタンプ、ファイルの性質など) をキャッシュに入れて、特定の期間内にそのファイルを再度検出した場合に再び分析を行わなくともマルウェアを識別できるようにします。このキャッシュの詳細については、[キャッシュ済み性質の有効期間 \(38 ページ\)](#) を参照してください。

ローカルマルウェア分析では、Secure Malware Analytics クラウドとの通信を確立する必要はありません。ただし、ファイルをダイナミック分析用にクラウドに送信するため、また、アップデートをローカルマルウェア分析ルールセットにダウンロードするために、クラウドとの通信を設定する必要があります。

キャッシュ済み性質の有効期間

AMP クラウドのクエリから返された、脅威スコアに関連付けられた性質、およびローカルマルウェア分析によって割り当てられた性質には、存続可能時間 (TTL) が設定されます。性質が更新されないまま、TTL 値で指定された期間にわたって保持された後は、キャッシュ情報が消去されます。性質および関連する脅威スコアには次の TTL 値が割り当てられます。

- クリーン : 4 時間
- 不明 : 1 時間
- マルウェア : 1 時間

このキャッシュに対するクエリで、キャッシュされた性質がタイムアウトになったことが識別された場合、システムはローカルマルウェア分析データベースおよび AMP クラウドに新しい性質を再びクエリします。

動的分析 (Dynamic Analysis)

Secure Malware Analytics (以前の Threat Grid) 、シスコのファイル分析、および脅威インテリジェンスプラットフォームを使用して動的分析用ファイルを自動的に送信するようにファイルポリシーを設定できます。

デバイスは、デバイスがファイルを保存するかどうかに関係なく、適格なファイルを Secure Malware Analytics (指定したいずれかのパブリック クラウドまたはオンプレミスアプライアンス) に送信します。

Secure Malware Analytics 悪意のあるファイルかどうかを判断するためにサンドボックス環境でファイルを実行してファイルの動作を分析し、ファイルにマルウェアが含まれる可能性を示す脅威スコアを返します。脅威スコアから、脅威スコアを割り当てた理由が含まれる動的分析のサマリーレポートを表示できます。また、Secure Malware Analytics では、組織が送信したファイルの詳細レポートを表示したり、組織が送信しなかったファイルのデータが限定されたスクーリング処理レポートを表示したりすることもできます。

Cisco Secure Malware Analytics の詳細については、<https://www.cisco.com/c/en/us/products/security/threat-grid/index.html> を参照してください。

動的分析を実行するようにシステムを設定するには、[動的分析接続 \(20 ページ\)](#) のトピックを参照してください。

動的分析の対象となるファイル

動的分析用ファイルの対象は、次の条件によって異なります。

- ファイルタイプ
- ファイル サイズ
- ファイルルールのアクション

さらに、次のパターンがあります。

- システムは設定したファイルルールに一致するファイルのみを送信します。
- 分析用の送信時にファイルのマルウェア クラウド ルックアップの性質が不明または使用不可になっている必要があります。
- システムは潜在的なマルウェアとしてファイルを事前分類する必要があります。

動的分析とキャパシティ処理

キャパシティ処理を使用すると、デバイスがクラウドと通信できない場合、または送信の最大数に達した場合に、システムがクラウドにファイルを一時的に送信できないと、動的分析の対象となるファイルを一時的に保存することができます。システムは、妨害状態が経過すると保存したファイルを送信します。

一部のデバイスはデバイスのハードドライブまたはマルウェアストレージパックにファイルを保存できます。 [マルウェアストレージパック \(40 ページ\)](#) も参照してください。

キャプチャされたファイルとファイルストレージ

ファイルストレージ機能を使用すると、選択したファイル（トライフィックで検出された）をキャプチャして、ファイルのコピーをデバイスのハードドライブかマルウェアストレージパック（インストールされている場合）に自動的に保存できます。

デバイスがファイルをキャプチャした後に、以下の選択肢があります。

- 後で分析するために、キャプチャしたファイルをデバイスのハードドライブに保存する。
- さらに手動で分析したりアーカイブしたりするために、保存したファイルをローカルコンピュータにダウンロードする。
- AMP クラウド ルックアップまたは動的分析の対象となるキャプチャファイルを手動で送信します。

注意すべき点として、デバイスがファイルを保存した後は、以後それを検出しても、デバイスが引き続きそれを保存していれば、そのファイルを再度キャプチャすることはありません。



(注)

ファイルがネットワーク上で初めて検出された際には、ファイルの検出を表すファイルイベントを生成できます。ただし、ファイルルールがマルウェアクラウドルックアップを行う場合は、システムがAMPクラウドにクエリを行い、判定結果が返るまで、より多く時間を要します。この遅延により、システムはネットワークでこのファイルが2回目に検出され、ファイルの判定結果を即座に判断できるまでは、このファイルを保存できません。

システムがファイルをキャプチャするか保存するかに関わらず、以下が可能です。

- [分析 (Analysis)] > [ファイル (Files)] > [キャプチャされたファイル (Captured Files)] からのキャプチャされたファイルに関する情報（動的分析のためにファイルが保存されたのか送信されたかどうか、ファイルの性質、脅威スコアなど）を確認することにより、ネットワーク上で検出されたマルウェアの潜在的な脅威について迅速に検討する。
- ファイルのトラジェクトリを表示して、ネットワークのトラバースの仕方およびコピーを保持しているホストを判別する。
- ファイルをクリーンリストまたはカスタム検出リストに追加することで、以後の検出時には常に、クリーンまたはマルウェアの判定結果を持つファイルとして扱う。

ファイルポリシーでファイルルールを設定して、特定のタイプまたは特定のファイル判定結果（使用できる場合）のファイルをキャプチャして保存します。ファイルポリシーをアクセスコントロールポリシーと関連付けて、それをデバイスに展開した後、トラフィック内の一致ファイルが検出され、保存されます。また、保存するファイルサイズの最小値と最大値を設定できます。

システムバックアップに保存ファイルは含まれません。

キャプチャしたファイル情報は、[分析 (Analysis)] > [ファイル (Files)] > [キャプチャしたファイル (Captured Files)] で表示し、コピーをオフライン分析用にダウンロードすることができます。

マルウェアストレージパック

ファイルポリシー構成によっては、デバイスがハードドライブにかなりの量のファイルデータを保存することができます。デバイスにマルウェアストレージパックを設置できます。システムがファイルをマルウェアストレージパックに保存することにより、イベントおよび設定ファイルを保存するために、プライマリハードドライブにより多くのスペースを確保できます。システムは定期的に古いファイルを削除します。デバイスのプライマリハードドライブに使用可能な領域が十分でなく、マルウェアストレージパックも設置されていない場合、ファイルを保存することはできません。



注意

シスコから供給されたハードドライブ以外はデバイスに取り付けないでください。サポートされていないハードドライブを取り付けると、デバイスが破損する可能性があります。マルウェアストレージパックキットは、シスコからのみ購入できます。マルウェアストレージパックのサポートが必要な場合は、サポートにお問い合わせください。

マルウェアストレージパックが設置されていない場合、ファイルを保存するデバイスを設定すると、プライマリハードドライブのスペースの特定の部分がキャプチャファイルストレージに割り当てられます。ダイナミック分析用に一時的にファイルに保存するよう容量処理を設定すると、システムはファイルをクラウドに再送信できるようになるまで、同じハードドライブ割り当てを使用してそれらのファイルを保存します。

デバイスにマルウェアストレージパックを設置してファイルストレージまたは容量処理を設定すると、デバイスはマルウェアストレージパック全体をこれらのファイルの保存用として割り当てます。デバイスは、マルウェアストレージパックに他の情報を保存することはできません。

キャプチャファイルストレージに割り当てられたスペースがいっぱいになると、システムは割り当てられたスペースがシステム定義しきい値に達するまで、保管されている古いファイルを削除します。保存されていたファイルの数によっては、システムがファイルを削除した後、ディスク使用率がかなり減る場合があります。

マルウェアストレージパックを設置する時点で、デバイスがすでにファイルを保存している場合、次にデバイスを再起動したときに、プライマリハードドライブに保存されていたキャプチャファイルまたは容量処理ファイルはすべて、マルウェアストレージパックに移動します。それ以降デバイスが保存するファイルはすべて、マルウェアストレージパックに保存されます。

FirepowerデバイスでMSPを使用する詳細については、「[Firepowerハードウェア設置ガイド](#)」を参照してください。

ファイルタイプによるすべてのファイルのブロック

マルウェアファイル伝送のブロックに加えて、マルウェアを含むかどうかにかかわらず、特定のタイプのすべてのファイルをブロックする必要がある場合は、それを実行できます。

システムでマルウェアを検出できるすべてのファイルタイプだけでなく、さらに多数のファイルタイプに対するファイル制御がサポートされています。これらのファイルタイプは、マルチメディア (swf、mp3)、実行可能ファイル (exe、トレント)、PDFなどの基本的なカテゴリにグループ分けされます。

タイプに基づいてすべてのファイルをブロックする方法は、技術的にはマルウェア防御機能ではないため、マルウェア防御ライセンスは不要で、AMPクラウドにクエリは実行されません。

ファイルルールアクション：評価順序

ファイルポリシーには、状況に応じて異なるアクションを持つ複数のルールが含まれる可能性があります。複数のルールを特定の状況に適用できる場合、このトピックで説明する評価順序が適用されます。通常、（優先度の高い順に）単純なブロッキング、次にマルウェアインスペクションとブロッキング、さらにその次に単純な検出とロギングとなります。

ファイルルールアクションの優先度は次のとおりです。

- ファイルブロック (*Block Files*)
- マルウェアブロック (*Block Malware*)
- マルウェアクラウドルックアップ (*Malware Cloud Lookup*)

■ ファイルルールの作成

- ファイル検出 (Detect Files)

設定されている場合、TID は、アクションの優先順位付けに影響を与えます。詳細については、「[Threat Intelligence Director-Firewall Management Center のアクションの優先順位付け](#)」を参照してください。

ファイルルールの作成



注意 [ファイルの検出 (Detect Files)] または [ファイルのブロック (Block Files)] ルールで [ファイルの保存 (Store files)] を有効化または無効化、または [マルウェアクラウドルックアップ (Malware Cloud Lookup)] または [マルウェアブロック (Block Malware)] ファイルルールアクションを分析オプション ([Spero 分析または MSEXE (Spero Analysis or MSEXE)]、[動的分析 (Dynamic Analysis)]、または [ローカルマルウェア分析 (Local Malware Analysis)]) またはファイルの保存オプション ([マルウェア (Malware)]、[不明 (Unknown)]、[正常 (Clean)]、または [カスタム (Custom)]) と結合する最初のファイルルールを追加または最後のファイルルールを削除すると、設定の変更を展開する際に Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細は [Snort の再起動によるトラフィックの動作](#) を参照してください。

始める前に

マルウェア保護のルールを設定する場合は、[ファイルポリシーの設定 \(10 ページ\)](#) を参照してください。

手順

ステップ1 [ポリシー (Policies)] > [アクセス制御 (Access Control)] > [マルウェアとファイル (Malware & File)] を選択します。

ステップ2 編集アイコンをクリックして、既存のファイルポリシーを変更します。

ステップ3 ファイルポリシーエディタで、[ルールの追加 (Add Rule)] をクリックします。

ステップ4 [ファイルルールのコンポーネント \(31 ページ\)](#) の説明に従って、[アプリケーションプロトコル (Application Protocol)] および [転送の宛先 (Direction of Transfer)] を選択します。

ステップ5 [ファイルタイプ (File Types)] を 1 つ以上選択します。

表示されるファイルタイプは、選択したアプリケーションプロトコル、転送の方向、およびアクションによって異なります。

ファイルタイプのリストを、次のようにフィルタ処理できます。

- 1 つ以上の [ファイルタイプカテゴリ (File Type Categories)] を選択し、[選択したカテゴリのすべてのタイプ (All types in selected Categories)] をクリックします。

- 名前または説明でファイルタイプを検索します。たとえば、Microsoft Windows固有のファイルのリストを表示するには、[Search name and description] フィールドに **Windows** と入力します。

ヒント

ファイルタイプの上にポインタを移動すると、説明が表示されます。

ステップ6 [ファイルルールアクション：評価順序（41 ページ）](#) を確認し、[ファイルルールアクション（33 ページ）](#) の説明に従ってファイルルール [アクション (Action)] を選択します。

利用可能なアクションは、インストールしたライセンスによって異なります。 [ファイルおよびマルウェアポリシーのライセンス要件（3 ページ）](#) を参照してください。

ステップ7 選択したアクションに応じて、以下のオプションを設定します。

- ファイルのブロック後に接続をリセットする
- ルールに一致するファイルを保存する
- Spero 分析を有効にする*
- ローカルマルウェア分析を有効にする*
- 動的分析およびキャパシティ処理を有効にする

* これらのオプションの詳細については、[ファイルルールアクション（33 ページ）](#) と [マルウェア防御オプション（ファイルルールアクション）（34 ページ）](#) およびそのサブトピックを参照してください。

ステップ8 [追加 (Add)] をクリックします。

ステップ9 [保存 (Save)] をクリックして、ポリシーを保存します。

次のタスク

- マルウェア保護のポリシーを設定する場合は、[ファイルポリシーの設定（10 ページ）](#) を参照してください。
- 設定変更を展開します [設定変更の展開](#) を参照してください。

マルウェア防御のためのアクセス制御ルールのロギング

システムはファイルポリシーの設定に従って禁止されたファイル（マルウェアを含む）を検出すると、イベントを Secure Firewall Management Center データベースに自動的にロギングします。ログファイルまたはマルウェアイベントが必要ない場合は、アクセスコントロールルールごとにこのロギングを無効にできます。

レトロスペクティブな性質の変更

また、システムは、呼び出し元のアクセスコントロールルールのロギング設定にかかわらず、関連付けられた接続の終了を Secure Firewall Management Center データベースにロギングします。

レトロスペクティブな性質の変更

ファイルの性質は変更される可能性があります。たとえば、新しい情報が見つかると、AMP クラウドによる判定の結果、以前はクリーンであると考えられていたファイルが今はマルウェアとして識別されるようになったり、その逆、つまりマルウェアと識別されたファイルが実際にはクリーンであったりする可能性があります。過去1週間にクエリを行ったファイルの性質が変更された場合、AMP クラウドはシステムに通知して、システムが次回そのファイルの送信を検出した際に自動的にアクションをとれるようにします。変更された性質は、レトロスペクティブな性質と呼ばれます。

ファイルおよびマルウェアのインスペクションパフォーマンスとストレージのオプション

ファイルサイズを増やすと、システムのパフォーマンスに影響を与える可能性があります。

表 4: アクセスコントロール ファイルおよびマルウェア防御の詳細オプション

フィールド	説明	ガイドラインと制限
ファイルタイプを検知する前に検閲するバイト数制限 (Limit the number of bytes inspected when doing file type detection)	ファイルタイプを検出するときに検査するバイト数を指定します。	0 ~ 4294967295 (4 GB) 0 にすると制限が解除されます。 デフォルト値は、TCP パケットの最大セグメントサイズ (1460 バイト) です。ほとんどの場合、システムは最初のパケットによって、一般的なファイルタイプを特定できます。 ISO ファイルを検出するには、36870 よりも大きい値を入力します。

フィールド	説明	ガイドラインと制限
ファイルを許可するのにかかるマルウェアブロックのクラウドルックアップの制限時間 (秒) (Allow file if cloud lookup for Block Malware takes longer than (seconds))	マルウェアクラウドルックアップの実行中に、システムが [マルウェアブロック (Block Malware)] ルールに一致し、性質がキャッシュに入っていないファイルの最後のバイトを保持する期間を指定します。システムが性質を取得する前にこの期間が満了すると、ファイルが渡されます。「使用不可」の性質はキャッシュに入れられません。	0 ~ 30 秒 サポートに連絡することなく、このオプションを 0 に設定しないでください。 シスコは、接続の障害によってトライックのブロックを防ぐために、デフォルト値を使用することをお勧めします。
SHA-256ハッシュ値を計算するファイルの上限サイズ (バイト) (Do not calculate SHA-256 hash values for files larger than (in bytes))	システムが特定のサイズを超えるファイルを保管すること、ファイルでマルウェアクラウドルックアップを実行すること、またはカスタム検出リストに追加されたファイルをブロックすることを防止します。	0 ~ 4294967295 (4 GB) 0 にすると制限が解除されます。 この値は、[保存する最大ファイルサイズ (バイト) (Maximum file size to store (bytes))] および [動的分析テストの最大ファイルサイズ (バイト) (Maximum file size for dynamic analysis testing (bytes))] の値以上に設定する必要があります。
[高度なファイルインスペクションと保存のための最小ファイル サイズ (バイト) (Minimum file size for advanced file inspection and storage (bytes))]	これらの設定は以下を指定します。 <ul style="list-style-type: none">次のディテクタを使用してシステムが検査できるファイルサイズ：<ul style="list-style-type: none">Spero 分析サンドボクシングと事前分類ローカルマルウェア分析/ClamAVアーカイブインスペクションシステムがファイルルールを使用して保存できるファイルサイズ。	0 ~ 10485760 (10MB) 0 にするとファイルストレージが無効になります。 [保存する最大ファイルサイズ (バイト) (Maximum file size to store (bytes))] および [SHA-256ハッシュ値を計算するファイルの上限サイズ (バイト) (Do not calculate SHA-256 hash values for files larger than (in bytes))] の値以下に設定する必要があります。
[高度なファイルインスペクションと保存のための最大ファイル サイズ (Minimum file size for advanced file inspection and storage (bytes))]		0 ~ 10485760 (10MB) 0 にするとファイルストレージが無効になります。 [保存する最小ファイルサイズ (バイト) (Minimum file size to store (bytes))] の値以上、および [SHA-256ハッシュ値を計算するファイルの上限サイズ (バイト) (Do not calculate SHA-256 hash values for files larger than (in bytes))] の値以下に設定する必要があります。

■ ファイルおよびマルウェアのインスペクションパフォーマンスとストレージのオプション

フィールド	説明	ガイドラインと制限
ダイナミック分析の最小ファイルサイズ (バイト) (Minimum file size for dynamic analysis testing (bytes))	システムが AMP クラウドに動的分析対象として送信できるファイルの最小サイズを指定します。	0 ~ 10485760 (10 MB) [動的分析テストの最大ファイルサイズ (バイト) (Maximum file size for dynamic analysis testing (bytes))] および [SHA-256ハッシュ値を計算するファイルの上限サイズ (バイト) (Do not calculate SHA-256 hash values for files larger than (in bytes))] の値以下に設定する必要があります。 動的分析のファイルサイズは、ファイル分析の最小および最大設定で定義された制限内のサイズにする必要があります。 システムは AMP クラウドをチェックして、送信可能なファイルの最小サイズが更新されているかどうかを調べます (最大で 1 日 1 回)。新しい最小サイズが現在の値より大きい場合、現在の値が新しい最小サイズに更新され、ポリシーは古いポリシーとしてマークされます。
ダイナミック分析の最大ファイルサイズ(バイト) (Maximum file size for dynamic analysis testing (bytes))	システムが AMP クラウドに動的分析対象として送信できるファイルの最大サイズを指定します。	0 ~ 10485760 (10 MB) [動的分析の最小ファイルサイズ (バイト) (Minimum file size for dynamic analysis testing (bytes))] の値以上、[SHA-256ハッシュ値を計算するファイルの上限サイズ (バイト) (Do not calculate SHA-256 hash values for files larger than (in bytes))] の値以下に設定する必要があります。 動的分析のファイルサイズは、ファイル分析の最小および最大設定で定義された制限内のサイズにする必要があります。 システムは AMP クラウドをチェックして、送信可能なファイルの最大サイズが更新されているかどうかを調べます (最大で 1 日 1 回)。新しい最大サイズが現在の値より小さい場合、現在の値が新しい最大サイズに更新され、ポリシーは古いポリシーとしてマークされます。

ファイルおよびマルウェアのインスペクションパフォーマンスおよびストレージの調整

このタスクを実行するには、管理者、アクセス管理者、またはネットワーク管理者ユーザーである必要があります。

手順

ステップ1 アクセスコントロールポリシー エディタで、[詳細設定 (Advanced Settings)] をクリックします。

ステップ2 [ファイルおよびマルウェアの設定 (Files and Malware Settings)] の横にある [編集 (Edit)] (✎) をクリックします。

代わりに [表示 (View)] (👁) が表示される場合、設定は先祖ポリシーから継承されており、設定を変更する権限がありません。設定がロック解除されている場合は、[Inherit from base policy] をオフにして、編集を有効にします。

ステップ3 [ファイルおよびマルウェアのインスペクションパフォーマンスとストレージのオプション \(44 ページ\)](#) で説明されている任意のオプションを設定します。

ステップ4 [OK] をクリックします。

ステップ5 [保存 (Save)] をクリックして、ポリシーを保存します。

次のタスク

- 設定変更を展開します [設定変更の展開](#) を参照してください。

(オプション) **Secure Endpoint** を使用したマルウェア防御

シスコの Secure Endpoint は、システムから提供され、Firepower 展開と統合し、マルウェア防御を補完できる個別のマルウェア防御製品です。

Secure Endpoint はシスコのエンタープライズクラスの高度なマルウェア防御ソリューションです。個別ユーザーのエンドポイント（コンピュータやモバイルデバイス）で軽量コネクタとして実行し、高度なマルウェアの発生、高度で継続的な脅威、およびターゲット型攻撃を検出、分析、ブロックします。

Secure Endpoint の利点を次に示します。

マルウェア防御の比較 : Firepower と Secure Endpoint

- ・部門全体のためにカスタム マルウェア検出ポリシーとプロファイルを設定し、すべてのユーザーのファイルに対してフラッシュスキャンおよび完全スキャンを実行する
- ・マルウェア分析の実行：ヒートマップ、詳細なファイル情報、ネットワーク ファイルトラジェクトリ、脅威の根本原因の表示など
- ・アウトブレイクコントロールのさまざまな要素を設定する：自動検疫、検疫されていない実行可能ファイルの実行を停止するアプリケーションブロッキング、除外リストなど
- ・カスタム保護の作成、グループポリシーに基づく特定のアプリケーションの実行ブロッキング、およびカスタムの許可されたアプリケーションリストの作成
- ・Secure Endpoint 管理コンソールを使用してマルウェアの影響を軽減する。管理コンソールの堅牢かつ柔軟な Web インターフェイスを使用すると、エンドポイント向け Secure Endpoint 展開のあらゆる側面を制御し、アウトブレイクのすべての段階を管理できます。

Secure Endpoint の詳細については、次を参照してください。

- ・<https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/index.html>。
- ・Secure Endpoint 管理コンソールのオンライン ヘルプ。
- ・Secure Endpoint のドキュメントは <http://docs.amp.cisco.com>で入手できます。

マルウェア防御の比較 : Firepower と Secure Endpoint

表 5: 製品の検出による高度なマルウェア保護の違い

機能	Firepower Malware Protection (マルウェア防御)	Secure Endpoint
ファイルタイプの検出とブロッキングの方法 (ファイル制御)	ネットワーク トラフィックでアクセス コントロール ポリシーとファイル ポリシーを使用	未サポート
マルウェアの検出とブロッキングの方法	ネットワーク トラフィックでアクセス コントロール ポリシーとファイル ポリシーを使用	個々のエンドポイント (エンドユーザー コンピュータとモバイルデバイス) で AMP クラウドとの通信を行うコネクタを使用
ネットワーク トラフィックを検査	管理対象デバイスを通過するトラフィック	なし (エンドポイントにインストールされたコネクタがファイルを直接検査する)
マルウェア インテリジェンスのデータソース	AMP クラウド (パブリックまたはプライベート)	AMP クラウド (パブリックまたはプライベート)
マルウェア検出の堅牢性	限定されたファイルタイプ	すべてのファイルタイプ

機能	Firepower Malware Protection (マルウェア防御)	Secure Endpoint
マルウェア分析の選択肢	Firewall Management Center ベース、および AMP クラウドでの分析	Firewall Management Center ベース、および Secure Endpoint 管理コンソールの追加オプション
マルウェアの影響軽減	ネットワーク トライフィックでのマルウェア ブロック、Firewall Management Center が開始する修復	Secure Endpoint ベースの検疫およびアウトブレイク コントロール オプション、Firewall Management Center が開始する修復
生成されるイベント	ファイルイベント、キャプチャされたファイル、マルウェアイベント、およびレトロスペクティブ マルウェア イベント	マルウェア イベント
マルウェア イベントに含まれる情報	基本的なマルウェア イベント情報、および接続データ (IP アドレス、ポート、アプリケーション プロトコル)	詳細なマルウェア イベント情報 (接続データなし)
ネットワーク ファイル トラジェクトリ	Firewall Management Center ベース	Firewall Management Center と Secure Endpoint の管理コンソールには、それぞれネットワーク ファイル トラジェクトリがあります。いずれも使用可能です。
必要なライセンスまたはサブスクリプション	とファイル制御の実行に必要なライセンス マルウェア防御	Secure Endpoint サブスクリプション Firewall Management Center への Secure Endpoint データの取り込みに必要なライセンスはありません。

Firepower と Secure Endpoint の統合について

組織で Secure Endpoint が導入されている場合、必要に応じてその製品を Firepower 展開と統合できます。

Secure Endpoint との統合に専用の Firepower ライセンスは必要ありません。

Firepower と Secure Endpoint の統合の利点

Secure Endpoint 展開をシステムに統合すると、次のような利点があります。

- Secure Endpoint で設定する中央集中型のブロックされたアプリケーションおよび許可されたアプリケーションによって、Firepower から AMP クラウドに送信されるファイル SHA の判定が決まります。
「[Secure Endpoint からの一元的なファイル リスト \(29 ページ\)](#)」を参照してください。
- システムは Secure Endpoint によって検出されたマルウェア イベントを Secure Firewall Management Center にインポートできるため、システムによって生成されたマルウェア イ

イベントとともにこれらのイベントを管理できます。これらのイベントでインポートされたデータには、スキャン、マルウェア検出、隔離、ブロックされた実行、クラウドの呼び出し、およびモニターするホストに対して Firewall Management Center が表示する侵害の兆候 (IOC) が含まれます。

詳細については、*Secure Endpoint*を使用したマルウェアイベント分析 ([Cisco Secure Firewall Management Center アドミニストレーションガイド](#)) を参照してください。

- Secure Endpoint コンソールでは、ファイルの軌跡およびその他の詳細を表示できます。

詳細については、*Secure Endpoint* コンソールでのイベントデータの使用 ([Cisco Secure Firewall Management Center アドミニストレーションガイド](#)) を参照してください。



重要 Cisco AMP プライベート クラウドを使用する場合は、[Secure Endpoint と AMP プライベート クラウド \(50 ページ\)](#) の制限事項を参照してください。

Secure Endpoint と AMP プライベート クラウド

ネットワーク上の Secure Endpoint データを収集するように Cisco AMP プライベート クラウドを設定した場合、すべての Secure Endpoint コネクタはプライベート クラウドにデータを送信します。そのデータは Secure Firewall Management Center に転送されます。プライベート クラウドは、エンドポイントデータを外部接続では一切共有しません。

組織で AMP プライベート クラウドを展開している場合、プライベート クラウドを介した AMP クラウド ファンルとのすべての接続は、監視対象ネットワークのセキュリティとプライバシーを確保するための匿名プロキシとして機能します。これには Secure Endpoint データのインポートが含まれます。プライベート クラウドは、エンドポイントデータを外部接続では一切共有しません。

AMP プライベート クラウドを使用する場合、次の統合機能は使用できません。

- Secure Endpoint で設定された、ブロックされたアプリケーションと許可されたアプリケーションのリストの使用。（これらのリストは、ファイルをブロックまたは許可するために使用されます。）
- Firepower から生成されたマルウェアイベントの Secure Endpoint での可視性。

必要なキャパシティをサポートするように複数のプライベート クラウドを設定できます。

Firepower と Secure Endpoint の統合

組織がシスコの Secure Endpoint 製品を展開している場合は、そのアプリケーションを Firepower と統合し、[Firepower と Secure Endpoint の統合の利点 \(49 ページ\)](#) で説明されている利点を実現できます。

Secure Endpoint と統合する場合、マルウェア防御 (AMP for Firepower) 接続がすでに設定されていても、Secure Endpoint 接続を設定する必要があります。複数の Secure Endpoint クラウド接続を設定できます。



(注) Secure Endpoint 接続が正しく登録されていなくても、マルウェア防御は影響を受けません。

始める前に

- このタスクを実行するには、管理者ユーザーである必要があります。
- 展開で Cisco AMP プライベートクラウドを使用している場合 [Secure Endpoint と AMP プライベートクラウド \(50 ページ\)](#) は、の制限事項を参照してください。
- ネットワークで Secure Endpoint が設定されていて、正しく機能している必要があります。
- Firewall Management Center はインターネットにアクセスできる必要があります。
- Firewall Management Center と Secure Endpoint が相互に通信できることを確認します。Cisco Secure Firewall Management Center アドミニストレーションガイドの「Security, Internet Access, and Communication Ports」にあるトピックを参照してください。
- Firewall Management Center を工場出荷時の初期状態に復元した後、または以前のバージョンに戻した後に AMP クラウドに接続している場合は、Secure Endpoint 管理コンソールを使用して以前の接続を削除します。
- この手順中に Secure Endpoint コンソールにログインするには、Secure Endpoint クレデンシャルが必要です。

手順

ステップ1 [統合 (Integration)] > [AMP] > [AMP管理 (AMP Management)] を選択します。

ステップ2 [AMP クラウド接続の追加 (Add AMP Cloud Connection)] をクリックします。

ステップ3 [クラウド名 (Cloud Name)] ドロップダウンリストから、使用するクラウドを選択します。

- Firewall Management Center の地理的な場所に最も近い AMP クラウド。
- APJC** はアジア/太平洋/日本/中国です。
- AMP プライベート クラウド (AMPv) の場合、[プライベート クラウド (Private Cloud)] を選択し、[Cisco AMP プライベート クラウド \(16 ページ\)](#) の手順に進みます。

ステップ4 このクラウドをマルウェア防御と Secure Endpoint の両方に使用する場合は、[AMP for Firepower に使用 (Use for AMP for Firepower)] チェックボックスをオンにします。

マルウェア防御 (AMP for Firepower) 通信を処理する別のクラウドを設定した場合は、このチェックボックスをオフにすることができます。これが唯一の AMP 接続の場合は、オフにできません。

ステップ5 [登録 (Register)] をクリックします。

[回転状態 (Spinning state)] () アイコンは、たとえば、Firewall Management Center で接続を設定した後、Secure Endpoint 管理コンソールの使用を許可する前に、接続が保留中であることを示します。[拒否 (Denied)] (-) アイコンは、クラウドが接続を拒否したこと、または他の理由で接続が失敗したことを示します。

ステップ 6 Secure Endpoint 管理コンソールを続行することを確認し、管理コンソールにログインします。

ステップ 7 管理コンソールを使用して、Secure Endpoint データを Firewall Management Center に送信することを AMP クラウドに許可します。

ステップ 8 Firewall Management Center が受信するデータを制限する場合は、情報を受け取る組織内の特定のグループを選択します。

デフォルトでは、AMP クラウドはすべてのグループのデータを送信します。グループを管理するには、Secure Endpoint 管理コンソールで [管理 (Management)] > [グループ (Groups)] を選択します。詳細については、管理コンソールのオンラインヘルプを参照してください。

ステップ 9 [許可 (Allow)] をクリックして接続を有効にして、データの転送を開始します。

[拒否 (Deny)] をクリックすると Firewall Management Center に戻りますが、接続には拒否マークが付きます。接続を拒否/許可しないまま Secure Endpoint 管理コンソールの [アプリケーション (Applications)] ページから別のページに移動した場合、Firewall Management Center の Web インターフェイスでは接続に保留中のマークが付きます。これらのいずれの状況でも、ヘルスモニターは失敗した接続のアラートを生成しません。後で AMP クラウドに接続するには、失敗した接続または保留中の接続を削除してから再作成します。

Secure Endpoint 接続の登録が未完了であっても、マルウェア防御 接続は無効なりません。

ステップ 10 接続が正しく設定されていることを確認するには、次の手順を実行します。

- [統合 (Integration)] > [AMP] > [AMP 管理 (AMP Management)] ページで、[Cisco AMP ソリューションタイプ (Cisco AMP Solution Type)] 列に Secure Endpoint が含まれている [クラウド名 (Cloud Name)] をクリックします。
- 表示される Secure Endpoint コンソール ウィンドウで、[アカウント (Accounts)] > [アプリケーション (Applications)] を選択します。
- Firewall Management Center が一覧に含まれていることを確認します。
- Secure Endpoint コンソール ウィンドウで、[管理 (Manage)] > [コンピュータ (Computers)] を選択します。
- Firewall Management Center が一覧に含まれていることを確認します。

次のタスク

- Secure Endpoint コンソール ウィンドウで、必要に応じて設定を行います。たとえば、管理センターのグループメンバーシップの定義や、ポリシーの割り当てを行います。詳細については、Secure Endpoint のオンラインヘルプまたはその他のドキュメントを参照してください。
- 高可用性展開では、両方の Management Center で AMP クラウド接続を設定します。これらの設定は同期されません。

- デフォルトのヘルス ポリシーは、Firewall Management Center から Secure Endpoint ポータルへの最初の接続が成功した後で接続できなくなった場合、または AMP ポータルを使って接続が登録解除された場合に警告を出します。

[システム (System)]>[ヘルス (Health)]>[ポリシー (Policy)] の Secure Endpoint ステータス モニターが有効になっていていることを確認します。

ネットワークマルウェア防御とファイルポリシーの履歴

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
AMP クラウドとの通信	7.0	任意 (Any)	<p>レガシーポート 32137 は、AMP パブリッククラウドまたはプライベートクラウドとの通信でサポートされなくなりました。</p> <p>新規/変更された画面 : [システム (System)]>[統合 (Integration)]>[クラウドサービス (Cloud Services)] ページの [ネットワーク用 AMP にレガシーポート 32137 を使用 (Use Legacy Port 32137 for AMP for Networks)] オプションは使用できなくなりました。</p>
章の再構成	変更は 6.4 で行われましたが、再発行されたすべてのバージョンに適用されます	任意 (Any)	<p>混乱を避けるため、この章の内容が再構成されました。</p> <p>一部のコンテンツは、Cisco Secure Firewall Management Center アドミニストレーション ガイドの「File/Malware Events and Network File Trajectory」の章との間で交換されました。</p>
URL フィルタリング情報を新しい URL フィルタリングの章に移動しました。	6.3	任意 (Any)	URL フィルタリングのクラウド通信の設定に関する情報を新しい URL フィルタリングの章に移動しました。章内の Cisco CSI のトピックの構成に関連する変更を加えました。

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。