



マルウェアと禁止されたファイルのブロッキング

悪意のあるソフトウェア、つまりマルウェアは、複数のルートで組織のネットワークに入る可能性があります。マルウェアの影響を特定して軽減するために、FireSIGHT システムのファイル制御、ネットワーク ファイル トラjectory、および高度なマルウェア防御の各コンポーネントを使用すると、マルウェアやその他の種類のファイルがネットワーク トラフィックで伝送されるのを検出、追跡、保存、分析、および任意でブロックすることができます。また、システムは、アーカイブ ファイル内のネストされたファイルを分析して処理することができます(アーカイブ ファイル形式 .zip または .rar)。

全体的なアクセス コントロール設定の一部として、マルウェア防御とファイル制御を実行するようにシステムを設定できます。作成してアクセス コントロール ルールに関連付けたファイルポリシーは、ルールに一致するネットワーク トラフィックを処理します。そのトラフィックで検出されたファイルをダウンロードした後、ファイルのシグネチャの動的分析用にそのファイルをシスコのマルウェア認識ネットワーク (Collective Security Intelligence クラウドと呼ばれる) に送信することで、そのファイルにマルウェアが含まれるかどうか判断できます。

コンテキスト エクスプローラとダッシュボードは、組織のネットワーク トラフィックで検出されたファイル(マルウェア ファイルを含む)のさまざまな概要表示を提供します。分析のターゲットをさらに絞り込むために、マルウェア ファイルの [ネットワーク ファイル trajectory] ページを使用して、ホスト間での個々の脅威の広がりを時系列で追跡できます。これにより、最も効果的なアウトブレイク制御と防止対策に集中できます。

ファイル ポリシーはどのライセンスでも作成可能ですが、マルウェア防御とファイル制御の一部の操作を行うには、次の表に示すように、ライセンス供与される特定の機能をターゲット デバイスで有効にする必要があります。

表 37-1 侵入インスペクションおよびファイルインスペクションのライセンスおよびアプライアンスの要件

機能	説明	追加する必要があるライセンス	追加先となる Defense Center	それを以下のデバイスで有効にする
侵入防御	侵入およびエクスプロイトを検出し、任意でブロックします	Protection	Any	Any
ファイル制御	ファイル タイプの伝送を検出し、任意でブロックします	Protection	Any	Any
高度なマルウェア防御 (AMP)	マルウェアの伝送を検出、保存、追跡し、任意でブロックします キャプチャしたファイルを シスコクラウドに送信し、マルウェアの分析を行います	Malware	DC500 を除くいずれか	シリーズ 2 と X-シリーズ を除くすべて

また、組織で FireAMP サブスクリプションをご利用の場合、Defense Center はパブリックのシスコクラウドからエンドポイントベースのマルウェア検出データを受信することもできます。Defense Center は、このデータを、ネットワークベースのファイルおよびシステム生成のマルウェアデータとともに提示します。FireAMP データのインポートには、FireAMP サブスクリプションに加えてライセンスは必要ありません。詳細については、[FireAMP 用のクラウド接続の操作 \(37-29 ページ\)](#) を参照してください。

クラウドベースのファイルおよびマルウェア機能については、組織が追加のセキュリティを必要とする場合や、外部接続を制限したい場合に、標準のクラウド接続の代わりに FireAMP プライベートクラウドを使用できます。すべてのファイルおよびマルウェアのクラウド検索、および FireAMP エンドポイントからのイベントデータの収集とリレーは、プライベートクラウドを介して処理されます。プライベートクラウドは、パブリックのシスコクラウドに接続したときに、エンドポイントイベントデータを送信しない匿名化されたプロキシ接続を介してこれらの処理を行います。

詳細については、以下を参照してください。

- [マルウェア防御とファイル制御について \(37-2 ページ\)](#)
- [ファイルポリシーの概要と作成 \(37-11 ページ\)](#)
- [FireAMP 用のクラウド接続の操作 \(37-29 ページ\)](#)

マルウェア防御とファイル制御に関連するイベントデータの評価の詳細については、[マルウェアとファイルアクティビティの分析 \(40-1 ページ\)](#) を参照してください。

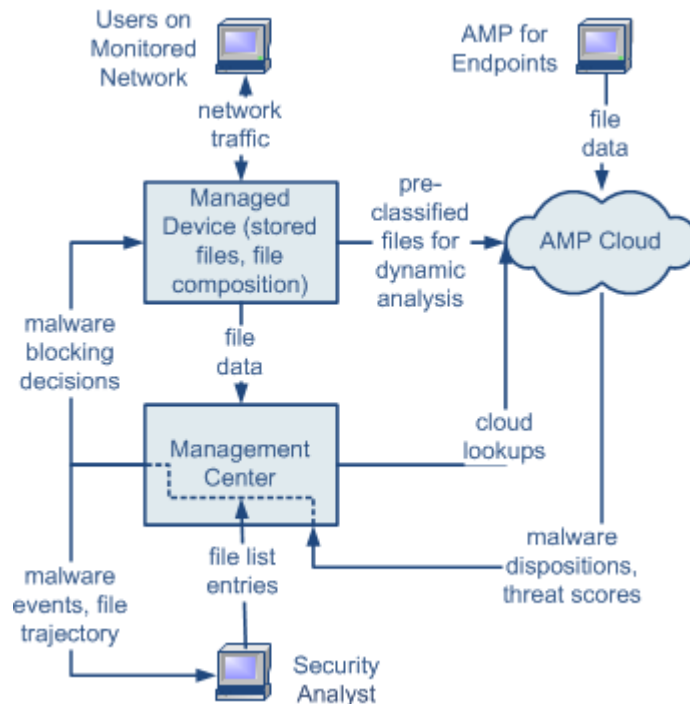
マルウェア防御とファイル制御について

ライセンス: Protection、Malware、またはすべて

サポートされるデバイス: 機能に応じて異なる

サポートされる防御センター: 機能に応じて異なる

高度なマルウェア防御機能を使用すると、次の図に示すように、ネットワークで送信されるマルウェアファイルを検出、保存、追跡、分析、および(オプションで)ブロックするよう FireSIGHT システムを設定できます。



システムは、PDF、Microsoft Office 文書など多数のファイルタイプに潜むマルウェアを検出し、オプションでブロックできます。管理対象デバイスは、特定のアプリケーションプロトコルベースのネットワークトラフィック内で、これらのファイルタイプの伝送をモニタします。対象となるファイルを検出した場合、デバイスはそのファイルのSHA-256ハッシュ値をDefense Centerに送信できます。その後、その情報を使ってマルウェアクラウドルックアップが実行されます。これらの結果に基づき、シスコクラウドはDefense Centerにファイルの性質を返します。

システムがネットワークトラフィック内でファイルを検出すると、デバイスはファイルストレージ機能を使用して、対象となるファイルをハードドライブまたはマルウェアストレージパックに保存できます。性質が不明な実行可能ファイルについては、デバイスでそのファイルを保存するかどうかに関係なく、動的分析のためにファイルを送信できます。クラウドはDefense Centerに次の情報を返します。

- ファイルにマルウェアが含まれている可能性を記述する脅威スコア、および
- クラウドがその脅威スコアを割り当てた理由を詳述する動的分析サマリーレポート。

また、対象となる実行可能ファイルが見つかった場合、デバイスはファイル構造のSpero分析を実行し、結果として得られたSperoシグネチャをクラウドに送信できます。クラウドはこのシグネチャを動的分析の補足情報として使用し、ファイルがマルウェアであるかどうかを判断します。

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、次のようにして、ファイルのSHA-256値をファイルリストに追加できます。

- 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。
- 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。

あるファイルの SHA-256 値がファイル リスト内で検出されると、システムはマルウェア ルックアップの実行もファイルの性質の検査も行わずに、適切なアクションを実行します。ファイルの SHA 値を計算するには、[マルウェア クラウド ルックアップ (Malware Cloud Lookup)] アクションと [マルウェア ブロック (Block Malware)] アクションのどちらか、および一致するファイル タイプを使用して、ファイル ポリシー内のルールを設定する必要があります。ことに注意してください。ファイル ポリシーごとに、クリーン リストまたはカスタム検出リストの使用を有効にできません。ファイル リストの管理の詳細については、[ファイル リストの操作 \(3-38 ページ\)](#) を参照してください。

システムは、通常の圧縮されていないファイルを分析および処理するのと同じ方法で、アーカイブ ファイル (.zip や .rar アーカイブ ファイルなど) 内のネストされたファイルを検査し、ブロックできます。ただし、システムがネストされたファイルをブロックすると、それを含むアーカイブ ファイル全体がブロックされることに注意してください。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。指定したレベルのネストを超えるアーカイブ ファイルをブロックするようにファイル ポリシーを設定できます (最大 3 つのレベルまで)。

また、コンテンツが暗号化されているか、または検査できないアーカイブ ファイルをブロックするようにファイル ポリシーを設定することもできます。アーカイブ ファイルのインスペクションの詳細については、[アーカイブ ファイルのインスペクション オプションの設定 \(37-24 ページ\)](#) を参照してください。

ファイルを検査またはブロックするには、ポリシーを適用する管理対象デバイスで Protection ライセンスを有効にする必要があります。また、ファイルの保存、マルウェア ファイルに関するマルウェア クラウド ルックアップと (オプションの) ブロック操作、動的分析のためのクラウドへのファイル送信、またはファイル リストへのファイルの追加を行うには、それらのデバイスに Malware ライセンスも有効にする必要があります。

ファイルの性質について

システムは、シスコクラウドから返される性質に基づいてファイルの性質を決定します。シスコクラウドから返された情報、ファイル リストへの追加操作、または脅威スコアに応じて、ファイルの性質は次のいずれかになります。

- マルウェア (Malware): クラウドでそのファイルがマルウェアとして分類されていること、またはファイルの脅威スコアが、ファイル ポリシーで定義されたマルウェアしきい値を超えていることを示します。
- クリーン (Clean): クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。
- 不明 (Unknown): クラウドが性質を割り当てる前にマルウェア クラウド ルックアップが行われたことを示します。クラウドはそのファイルをまだ分類していません。
- カスタム検出 (Custom Detection): ユーザがカスタム検出リストにファイルを追加したことを示します。
- 使用不可 (Unavailable): Defense Center がマルウェア クラウド ルックアップを実行できなかったことを示します。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。



ヒント

高速連続で複数の使用不可 (Unavailable) なマルウェア イベントが発生した場合は、クラウド接続およびポート設定を確認してください。詳細については、[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 \(E-1 ページ\)](#) を参照してください。

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。[コンテンツごとのアーカイブ ファイルの性質](#)に、アーカイブに含まれるファイルのさまざまな組み合わせによって決定されるアーカイブ ファイルの性質を示します。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、いずれかの不明なファイルが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。アーカイブ ファイルのインスペクションの詳細については、[アーカイブ ファイルのインスペクション オプションの設定 \(37-24 ページ\)](#)を参照してください。他のファイルと同様に、アーカイブ ファイルには、その性質に関する条件が適用される場合、カスタム検出 (Custom Detection) または使用不可 (Unavailable) の性質が割り当てられる場合があります。

表 37-2 コンテンツごとのアーカイブ 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
不明	1 つ以上	Any	0
クリーン (Clean)	0	1 つ以上	0
マルウェア (Malware)	Any	Any	1 つ以上

ファイルの性質に基づき、ファイルをブロックするか、ファイルのアップロードまたはダウンロードを許可するよう、Defense Center が管理対象デバイスに指示します。アーカイブ ファイル内のネストされたファイルがブロックされている場合は、システムはアーカイブ ファイル全体をブロックすることに注意してください。パフォーマンスを改善させるために、SHA-256 値に基づくファイルの性質がシステムですでにわかっている場合、Defense Center はシスコクラウドに照会する代わりに、キャッシュ済みの性質を使用します。

ファイルの性質は変更される可能性があることに注意してください。たとえば、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。あるファイルに関するマルウェア ルックアップを先週実行した後、そのファイルの性質が変更された場合は、クラウドが Defense Center に通知を送ります。これにより、そのファイルの伝送が次回検出されたときにシステムは適切なアクションを実行できます。変更されたファイルの性質は、レトロスペクティブな性質と呼ばれます。

マルウェア クラウド ルックアップから戻されたファイルの性質、およびそれに関連する脅威スコアには、存続可能時間 (TTL) 値が割り当てられます。ファイルの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

キャッシュに照らしたマルウェア クラウド ルックアップの結果、キャッシュ済み性質がタイムアウトになったことが識別されると、システムはファイルの性質を判別するために新しいルックアップを実行します。

ファイル制御について

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、[ファイル制御機能](#)により防御網を広げることができます。マルウェア防御の場合と同様に、管理対象デバイスはネットワークトラフィック内で特定のファイルタイプの伝送をモニタし、そのファイルをブロックまたは許可します。

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。ファイル制御はマルウェア防御とは異なり、シスコクラウドへの照会を必要としないことに注意してください。

キャプチャされたファイル、ファイルイベント、およびマルウェア イベントを分析に使用する

ファイルが転送またはブロックされると、システムはマルウェア イベントやファイル イベントを生成します。また、システムは、管理対象デバイスでキャプチャされたファイルの情報を収集します。Defense Center の Web インターフェイスを使用して、これらのイベントと情報を表示することができます。また、Context Explorer とダッシュボードには、組織で検出されたファイル (マルウェア ファイルを含む) のさまざまなタイプの概要が表示されます。

分析ターゲットをさらに絞り込むために、ネットワーク ファイル トラジェクトリ機能を使用すると、個々のファイルの伝送パスを追跡できます。ファイルのトラジェクトリ ページには、ファイルの概要情報、ホスト間のファイル伝送 (ブロックされた伝送も含む) を示すグラフィカルマップ、およびそれらのファイルの検出/ブロックに関連するマルウェア イベントまたはファイル イベントが表示されます。

DC500 では Malware ライセンスを使用できず、シリーズ 2 デバイスまたは Blue Coat X-Series 向け Cisco NGIPS で Malware ライセンスを有効にすることもできないので、これらのアプライアンスを使用して個別のファイルをキャプチャまたはブロックしたり、動的分析用にファイルを送信したり、マルウェアクラウドルックアップの対象となるファイル トラジェクトリを表示したりすることはできないことに注意してください。

詳細については、次の項を参照してください。

- [マルウェア防御とファイル制御の設定 \(37-6 ページ\)](#)
- [マルウェア防御とファイル制御に基づくイベントのロギング \(37-7 ページ\)](#)
- [FireAMP と FireSIGHT システムの統合 \(37-8 ページ\)](#)
- [ネットワークベースの AMP とエンドポイント ベースの FireAMP の比較 \(37-9 ページ\)](#)
- [ネットワーク ファイル トラジェクトリの操作 \(40-39 ページ\)](#)

マルウェア防御とファイル制御の設定

ライセンス: Protection または Malware

サポートされるデバイス: 機能に応じて異なる

サポートされる防御センター: 機能に応じて異なる

ファイルポリシーをアクセス コントロールルールに関連付けることで、全体的なアクセス コントロール設定の一部として、マルウェア防御とファイル制御を設定します。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。

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。

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
- マルウェア ファイルの性質に基づいてファイルをブロックする
- ファイルをキャプチャしてデバイスに保存する
- キャプチャされたファイルを動的分析のために送信する

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

単純な例として、ユーザによる実行可能ファイルのダウンロードをブロックするファイル ポリシーを導入できます。別の例として、ダウンロードされた PDF でマルウェアを検査し、見つかった場合はそれをブロックできます。ファイル ポリシーについて、およびファイル ポリシーとアクセス コントロール ルールとの関連付けについての詳細は、[ファイル ポリシーの概要と作成 \(37-11 ページ\)](#) および [侵入防御パフォーマンスの調整 \(18-10 ページ\)](#) を参照してください。

DC500 では Malware ライセンスを使用できないため、このアプライアンスを使用して、ネットワークベースのマルウェア防御やアーカイブ ファイルの内容の検査を行うファイル ポリシーを適用することはできません。同様に、シリーズ 2 デバイスまたは Blue Coat X-Series 向け Cisco NGIPS では Malware ライセンスを有効にできないため、ネットワークベースのマルウェア防御やアーカイブ ファイルの内容の検査を行うファイル ポリシーをこれらのアプライアンスに適用することはできません。

マルウェア防御とファイル制御に基づくイベントのロギング

ライセンス:Protection または Malware

サポートされるデバイス:機能に応じて異なる

サポートされる防御センター:機能に応じて異なる

Defense Center は、システムのファイル インспекションおよび処理のレコードを、キャプチャされたファイル、ファイル イベント、およびマルウェア イベントとしてログ記録します。

- キャプチャされたファイルは、システムがキャプチャしたファイル。
- ファイル イベントは、システムがネットワーク トラフィック内で検出した(およびオプションでブロックした)ファイルを表します。
- マルウェア イベントは、システムがネットワーク トラフィック内で検出した(およびオプションでブロックした)マルウェア ファイルを表します。
- レトロスペクティブ マルウェア イベント:性質がマルウェア ファイルから変更されたファイル。

ファイル内のマルウェアを検出するために、システムはまずファイル自体を検出する必要があります。そのため、ネットワークトラフィック内のマルウェア検出/ブロックに基づいてシステムがマルウェアイベントを生成するときには、ファイルイベントも生成します。FireAMP コネクタによって生成されたエンドポイントベースのマルウェアイベント([FireAMP と FireSIGHT システムの統合 \(37-8 ページ\)](#))を参照)には、対応するファイルイベントがないことに注意してください。同様に、システムがネットワークトラフィック内でファイルをキャプチャするとき、システムはまずファイルを検出するため、ファイルイベントも生成されます。

Defense Center を使用すると、キャプチャされたファイル、ファイルイベント、およびマルウェアイベントを表示、操作、分析して、分析内容を他のユーザに送信できます。Context Explorer、ダッシュボード、イベントビューア、ネットワークファイルトラジェクトリマップ、およびレポート機能を使用すると、検出/キャプチャ/ブロックされたファイルとマルウェアについてより詳しく理解できます。また、イベントを使用して相関ポリシー違反をトリガーしたり、電子メール、SMTP、または syslog によるアラートを発行したりすることもできます。ファイルイベントとマルウェアイベントの詳細については、[ファイルイベントの操作 \(40-8 ページ\)](#) および [マルウェアイベントの操作 \(40-18 ページ\)](#) を参照してください。

DC500 では Malware ライセンスを使用できず、シリーズ 2 デバイスまたは Blue Coat X-Series 向け Cisco NGIPS では Malware ライセンスを有効にすることもできません。このため、これらのアプライアンスを使用して、マルウェアクラウドルックアップまたはアーカイブファイルの内容に関連するキャプチャされたファイル、ファイルイベント、およびマルウェアイベントを生成/分析することはできません。

FireAMP と FireSIGHT システムの統合

ライセンス:任意 (Any)

FireAMP は、シスコが提供するエンタープライズ向けの高度なマルウェア分析/対策ソリューションです。高度なマルウェアの発生、高度な持続的脅威、および標的を絞った攻撃を検出、把握、ブロックします。

組織で FireAMP サブスクリプションをご利用の場合、個々のユーザはエンドポイント(コンピュータとモバイルデバイス)に FireAMP コネクタをインストールします。FireAMP コネクタはさまざまな機能を備えた軽量エージェントです。特に、アップロード、ダウンロード、実行、オープン、コピー、移動などの際にファイルを検査する機能があります。検査対象の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、これらのコネクタはシスコクラウドと通信します。

ファイルがマルウェアとして識別された場合、クラウドは脅威の特定に関する情報を Defense Center に送ります。さらに、クラウドは、スキャン、検疫、実行のブロック、クラウドリコールなど、他の種類のデータを Defense Center に送信することもできます。Defense Center はこれらの情報をマルウェアイベントとしてログに記録します。

FireAMP 展開を使用すると、マルウェアイベントに基づいて Defense Center で開始される修復やアラート発行を設定できることに加えて、FireAMP ポータル(<http://amp.sourcefire.com/>)を使ってマルウェアの影響を軽減することもできます。ポータルに備わっている堅牢かつ柔軟な Web インターフェイスを使用すると、FireAMP 展開のすべての局面を制御し、アウトブレイクのすべての段階を管理できます。次の操作を実行できます。

- 組織全体のためのカスタム マルウェア検出ポリシーとプロファイルの設定、およびすべてのユーザのファイルに対するフラッシュ スキャンと完全スキャンの実行
- 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局面の設定: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 ブロック、除外リストなど
- カスタム防御の作成、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ク、およびカスタム ホワイトリストの作成

詳細については、次の項を参照してください。

- [ネットワークベースの AMP とエンドポイント ベースの FireAMP の比較\(37-9 ページ\)](#)に、シスコ製品ファミリで使用可能なマルウェア防御戦略の比較を示します。
- [FireAMP 用のクラウド接続の操作\(37-29 ページ\)](#)では、Defense Center とシスコ クラウドの間の通信を直接確立する方法、または FireAMP プライベート クラウド接続によって確立する方法を説明します。



ヒント

FireAMP の詳細については、FireAMP ポータルのオンライン ヘルプを参照してください。

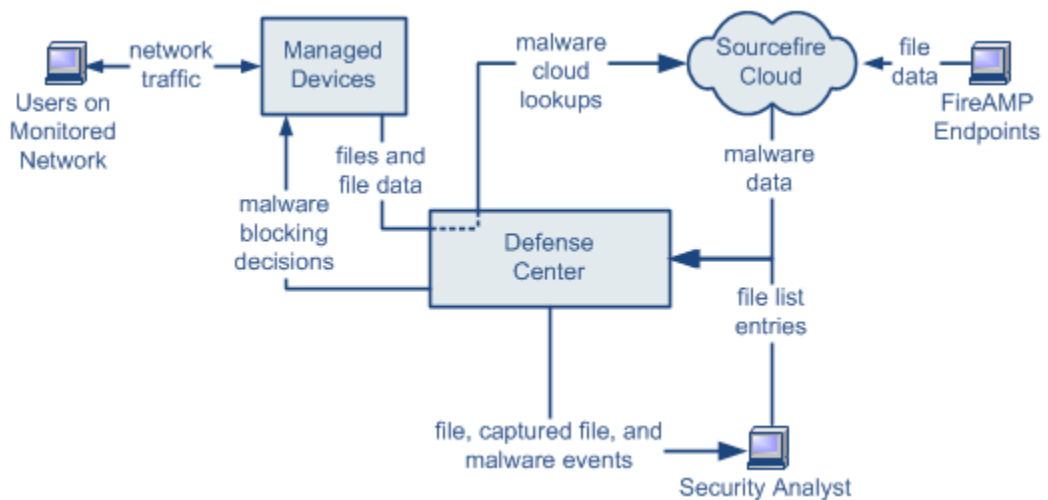
ネットワークベースの AMP とエンドポイント ベースの FireAMP の比較

ライセンス:Malware またはすべて

サポートされるデバイス:機能に応じて異なる

サポートされる防御センター:機能に応じて異なる

ネットワークベースの高度なマルウェア防御戦略と、エンドポイント ベースの FireAMP 戦略の両方からのデータを Defense Center でどのように使用できるかを次の図に示します。



のマルウェア検出はダウンロード時または実行時にエンドポイントで行われるのに対し、管理対象デバイスはネットワーク トラフィック内でマルウェアを検出するため、この2種類のマルウェア イベントの情報が異なることに注意してください。たとえば、エンドポイント ベースのマルウェア イベントには、ファイルパス、呼び出し元クライアント アプリケーションなどの情報が含まれるのに対して、ネットワーク トラフィックでのマルウェア検出には、ファイルの送信に使用された接続のポート、アプリケーション プロトコル、発信元 IP アドレス情報が含まれます。

別の例として、ネットワークベースのマルウェア イベントにおけるユーザ情報は、ネットワーク検出で判別されたマルウェア宛先ホストに最後にログインしたユーザを表します。一方、FireAMP で報告されるユーザは、ローカル コネクタで判別されるマルウェア検出場所のエンドポイントに現在ログインしているユーザを表します。



(注)

エンドポイント ベースのマルウェア イベントで報告された IP アドレスは、組織のネットワーク マップに含まれない可能性があり、モニタ対象のネットワークにも含まれない可能性があります。展開方法、ネットワーク アーキテクチャ、コンプライアンス レベル、その他の要因により、コネクタがインストールされているエンドポイントは、管理対象デバイスによってモニタされるのと同じホストでない可能性があります。

DC500 では Malware ライセンスを使用できず、シリーズ 2 デバイスまたは Blue Coat X-Series 向け Cisco NGIPS で Malware ライセンスを有効にすることもできません。したがって、これらのアプライアンスを使用して個別のファイルをキャプチャ/ブロックしたり、動的分析用にファイルを送信したり、アーカイブ ファイルの内容を検査したり、マルウェア クラウドルックアップの対象となるファイルのトラジェクトリを表示したりすることはできません。

次の表に、2 つの戦略の違いをまとめます。

表 37-3 ネットワークベースとエンドポイント ベースのマルウェア防御戦略の比較

機能	ネットワークベース	エンドポイント ベース (FireAMP)
ファイルタイプの検出とブロックングの方法 (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クングの方法	ネットワーク トラフィックで、アクセス制御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で、シスコクラウドとの通信を行うインストール済みコネクタを使用
検査されるネットワーク トラフィック	管理対象デバイスを通るトラフィック	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
マルウェア分析の選択肢	Defense Center ベース、およびクラウドでの分析	Defense Center ベース、および FireAMP ポータルでの追加のオプション
マルウェアの影響軽減	ネットワーク トラフィックでのマルウェア ブロックング、Defense Center が開始する修復	FireAMP ベースの検疫およびアウトブレイク制御オプション、Defense 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	Defense Center ベース	Defense Center ベース、および FireAMP ポータルでの追加のオプション
必要なライセンスまたはサブスクリプション	ファイル制御を実行するには Protection ライセンス、マルウェア防御を実行するには Malware ライセンス	FireAMP サブスクリプション (ライセンスベースではない)

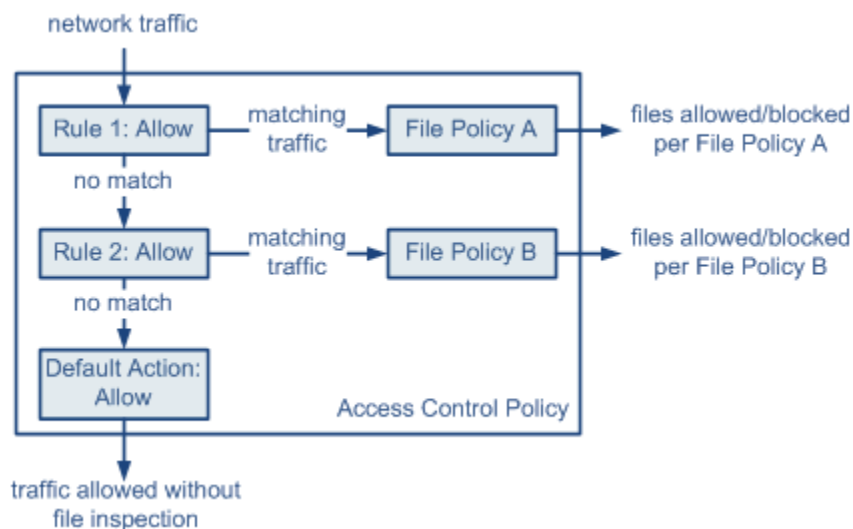
ファイルポリシーの概要と作成

ライセンス:Protection または Malware

サポートされるデバイス:機能に応じて異なる

サポートされる防御センター:機能に応じて異なる

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、高度なマルウェア防御とファイル制御を実行できます。次の図のような、イ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ります。



37-1859

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。

- ルール1に一致するトラフィックはファイルポリシーAで検査されます。
- ルール1に一致しないトラフィックはルール2に照らして評価されます。ルール2に一致するトラフィックはファイルポリシー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。

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。

ファイルがルールに一致すると、ルールは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
- マルウェアファイルの性質に基づいてファイルをブロックする
- キャプチャされたファイルをデバイスに保存する
- キャプチャされたファイルを動的分析のために送信する

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

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。その後、システムはそのファイル ポリシーを使用して、アクセス コントロール ルールの条件を満たすネットワーク トラフィックを検査します。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。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。詳細については、[許可されたトラフィックに対する侵入およびマルウェアの有無のインスペクション\(18-2 ページ\)](#)を参照してください。

ファイル ルール

ファイル ポリシーの中でファイル ルールを設定します。次の表に、ファイル ルールのコンポーネントを示します。

表 37-4 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。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) の発信トラフィックを検査できます。

表 37-4 ファイルルールのコンポーネント(続き)

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、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。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ブロックしたり、ShockWave Flash (swf) ファイルのみをブ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> 注意 ファイルタイプまたはファイルカテゴリを追加または削除すると、変更を適用したときに一時的にトラフィックが中断され、Snort プロセスが再起動されます。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、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort の再開によるトラフィックへの影響 (1-9 ページ) を参照してください。</p> <p> 注意 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 (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フィックをシステムが処理する方法が決定されます。</p> <p>(注) 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。詳細は、次の項 ファイルルールアクションと評価順序 を参照してください。</p>

ファイルルールアクションと評価順序

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。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設定できます。複数のルールアクションは、以下のようなルールアクション順になります。

- [ファイルブロック (Block Files)] 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。
- [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、クラウドルックアッププロセスを使用して、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。

- [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伝送を許可しながら、クラウドルックアップに基づいてそのファイルのマルウェアの性質をログに記録できます。
- [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。



注意

[ファイル検出 (Detect Files)] または [マルウェアブロック (Block Malware)] に関するファイルルールアクションを変更するか、[ファイルの保存 (Store Files)] を有効または無効にすると、アクセスコントロールポリシーを適用するときにトラフィックのインスペクションが一時的に中断され、Snort プロセスが再起動されます。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、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。Snort の再開によるトラフィックへの影響(1-9 ページ)を参照してください。

ファイルルールアクションごとに、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、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、およびキャプチャされたファイルを動的分析と Spero 分析のためクラウドに送信するオプションを設定できます。次の表に、各ファイルアクションで使用可能なオプションの詳細を示します。

表 37-5 ファイルルールアクション

アクション	接続をリセットするか	ファイルを保存するか	動的分析をするか	MSEXE 用の Spero 分析をするか
ファイルブロック (Block Files)	はい (Yes) (推奨)	はい: 一致するすべてのファイルを保存できます	No	No
マルウェアブロック (Block Malware)	はい (Yes) (推奨)	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: 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	はい: 実行可能ファイルを送信できます
ファイル検出 (Detect Files)	No	はい: 一致するすべてのファイルを保存できます	No	No
マルウェアクラウドルックアップ (Malware Cloud Lookup)	No	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: 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	はい: 実行可能ファイルを送信できます

ファイルとマルウェアの検出、キャプチャ、およびブロックに関する注意事項と制約事項

ファイルとマルウェアの検出、キャプチャ、およびブロックの動作に関して、以下の詳細および制限に注意してください。

- ファイルの終わりを示す End of File マーカ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 (Block Malware)] 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 マーカ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、このマーカーが検出された後にファイルをブロックします。
- 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送信される場合、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。

- 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。パッシブまたはインライン 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 Snort に負荷分散されない場合があります。
- 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 に関する [マルウェア ブロック (Block Malware)] ルールを持つファイル ポリシーを使用するアクセス コントロール ポリシーでは、[インライン時にドロップ (Drop when Inline)] を無効にした侵入ポリシーをデフォルト アクションに設定した場合、システムはルールに一致するファイルやマルウェアの検出でイベントを生成しますが、ファイルをドロップしません。FTP ファイア転送をブロックし、ファイル ポリシーを選択するアクセス コントロール ポリシーのデフォルト アクションとして侵入ポリシーを使用するには、[インライン時にドロップ (Drop when Inline)] を有効にした侵入ポリシーを選択する必要があります。
- [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 (Block Files)] 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) NetBIOS-ssn 経由で転送される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、ファイル ポリシーを呼び出すアクセス コントロール ポリシーの適用前に開始された、確立済み TCP または SMB セッションで転送されるファイルに対しては、検査が行われません。このため、これらのファイルは検出/ブロックされません。
- 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継続されるため、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。
- 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 ベースのホストは改行 (CR) 文字を使用し、UNIX/Linux ベースのホストは改行 (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。
- 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。

- [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、Defense Center がクラウドとの接続を確立できないと、クラウド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。
- 大量のトラフィックをモニタしている場合、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。



(注) ファイルがセッションで検出されブロックされるまで、セッションからのパケットは侵入インスペクションの対象になります。

ファイルルールの評価例

番号順にルールが評価されるアクセスコントロールポリシーとは異なり、ファイルポリシーでは **ファイルルールアクションと評価順序 (37-13 ページ)** に従ってファイルが処理されます。つまり、(優先度の高い順に) 単純なブロック、次にマルウェアインスペクションとブロック、さらにその次に単純な検出とロギングとなります。例として、1 つのファイルポリシー内に、PDF ファイルを処理する 4 つのルールがあるとします。Web インターフェイスで表示される順序に関係なく、これらのルールは次の順序で評価されます。

表 37-6 ファイルルールの評価順序の例

アプリケーションプロトコル	方向 (Direction)	アクション	アクションのオプション	結果
SMTP	アップロード (Upload)	ファイルブロック (Block Files)	接続のリセット (Reset Connection)	ユーザが電子メールで PDF ファイルを送信することをブロックし、接続をリセットします。
FTP	ダウンロード (Download)	マルウェアブロック (Block Malware)	不明な性質のファイルを保存、接続のリセット	ファイル転送を介したマルウェア PDF ファイルのダウンロードをブロックし、不明なファイルの性質を持つファイルをデバイスに保存して、接続をリセットします。
POP3 IMAP	ダウンロード (Download)	マルウェアクラウドルックアップ (Malware Cloud Lookup)	不明な性質のファイルを保存、動的分析	電子メールで受信された PDF ファイルに対してマルウェア検査を行い、不明なファイルの性質を持つファイルをデバイスに保存します。動的分析用に、シスコクラウドにファイルを送信します。
Any	Any	ファイル検出 (Detect Files)	none	ユーザが Web 上で (つまり HTTP 経由で) PDF ファイルを表示すると、それを検出してログに記録しますが、トラフィックは許可します。

Defense Center では、矛盾するファイルルールを示すために警告アイコン (⚠) を使用しています。警告アイコンの上にポインタを置くと詳細が表示されます。

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ないことに注意してください。[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。

DC500 では Malware ライセンスを使用できないため、[マルウェア ブロック (Block Malware)] アクションや [マルウェア クラウドルックアップ (Malware Cloud Lookup)] アクションを使用するファイルルールを作成したり、それらのアクションを行うルールを含むファイルポリシーを適用するためにこのアプライアンスを使用したりできないことに注意してください。同様に、シリーズ 2 デバイスまたは Blue Coat X-Series 向け Cisco NGIPS では Malware ライセンスを有効にできないため、これらのアクションを行うルールを含むファイルポリシーをこのアプライアンスに適用することはできません。

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 イベントおよびアラートのロギング

ファイルポリシーをアクセスコントロールルールに関連付けると、一致するトラフィックに関するファイル イベントとマルウェア イベントのロギングが自動的に有効になります。また、ファイルをキャプチャ/保存するようファイルポリシーが設定されている場合、ファイルがキャプチャされると、キャプチャされたファイルのロギングも自動的に有効になります。ファイルを検査するときに、システムは次のタイプのイベントを生成できます。

- **ファイル イベント:** 検出またはブロックされたファイル、および検出されたマルウェア ファイルを表します
- **マルウェア イベント:** 検出されたマルウェア ファイルを表します
- **レトロスペクティブ マルウェア イベント:** 以前に検出されたファイルに関する「マルウェア」ファイルの性質が変更された場合に、生成されます

ファイルポリシーでファイル イベントまたはマルウェア イベントが生成されるか、ファイルがキャプチャされると、システムは(起動元のアクセスコントロールルールにおけるロギング設定とは無関係に)関連する接続の終了を Defense Center データベースに自動的に記録します。



(注)

NetBIOS-ssn(SMB) トラフィックのインスペクションによって生成されるファイル イベントは、即座には接続イベントを生成しません。これは、クライアントとサーバが持続的接続を確立するためです。システムはクライアントまたはサーバがセッションを終了した後に接続イベントを生成します。

これらの接続イベントごとに、

- [ファイル (Files)] フィールドには、接続で検出されたファイル数(マルウェア ファイルを含む)を示すアイコン(📁)が含まれます。このアイコンをクリックすると、それらのファイルのリスト、およびマルウェア ファイルの性質が表示されます。
- [理由 (Reason)] フィールドには、接続イベントがログに記録された理由が示されます。これはファイルルールアクションに応じて次のように異なります。
- **ファイル モニタ (File Monitor):** [ファイル検出 (Detect Files)] ルールおよび [マルウェア クラウドルックアップ (Malware Cloud Lookup)] ファイルルールの場合、およびクリーン リスト内のファイルの場合
- **ファイル ブロック (File Block):** [ファイル ブロック (Block Files)] ルールまたは [マルウェア ブロック (Block Malware)] ファイルルールの場合
- **ファイル カスタム検出 (File Custom Detection):** カスタム検出リストにあるファイルをシステムが検出した場合
- **ファイル 復帰許可 (File Resume Allow):** ファイル送信がはじめに [ファイル ブロック (Block Files)] ルールまたは [マルウェア ブロック (Block Malware)] ファイルルールによってブロックされた場合。ファイルを許可する新しいアクセスコントロールポリシーが適用された後、HTTP セッションが自動的に再開しました。

- ファイル復帰ブロック (File Resume Block): ファイル送信がはじめに [ファイル検出 (Detect Files)] ルールまたは [マルウェア クラウドルックアップ (Malware Cloud Lookup)] ファイルルールによって許可された場合、ファイルをブロックする新しいアクセス コントロール ポリシーが適用された後、HTTP セッションが自動的に停止しました。
- ファイルやマルウェアがブロックされた接続では、[アクション (Action)] が [ブロック (Block)] になります。

Defense Center の Web インターフェイスを使用すると、FireSIGHT システムで生成されるすべての種類のイベントと同様に、ファイル イベントとマルウェア イベントを表示、操作、および分析できます。また、マルウェア イベントを使用して関連ポリシー違反をトリガーしたり、電子メール、SMTP、または syslog によるアラートを発行したりすることもできます。



(注)

さらに、組織の FireAMP サブスクリプションを使用して、Defense Center でマルウェア イベントを受信することもできます。これらのマルウェア イベントはダウンロード時または実行時にエンドポイントで生成されるため、その情報はネットワークベースのマルウェア イベントの情報とは異なります。

接続イベント、ファイル イベント、マルウェア イベント、およびそれらのログの詳細については、以下を参照してください。

- [ネットワークトラフィックの接続のログ \(38-1 ページ\)](#)
- [ファイル イベントの操作 \(40-8 ページ\)](#)
- [マルウェア イベントの操作 \(40-18 ページ\)](#)
- [接続およびセキュリティ インテリジェンスのデータについて \(39-2 ページ\)](#)

インターネットアクセスとハイアベイラビリティ

システムはポート 443 を使用して、ネットワークベース AMP 用のマルウェア クラウドルックアップを実行します。Defense Center でこのポートをアウトバウンドに開く必要があります。

ハイアベイラビリティペアの Defense 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、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性質が両方の Defense Center で同じであるようにするためには、プライマリとセカンダリ両方の Defense Center がクラウドにアクセスできなければなりません。

また、動的分析のためにクラウドにファイルを送信するには、デバイスでポート 443 をアウトバウンドに開く必要があります。



(注)

FireAMP プライベートクラウドには、シスコのパブリッククラウド接続と同じオープンポートを必要とし、同じハイアベイラビリティ制限事項があることに注意してください。

ファイルポリシーの管理

[ファイルポリシー (File Policies)] ページ ([ポリシー (Policies)] > [ファイル (Files)]) でファイルポリシーの作成、編集、削除、および比較を行います。ここには既存のファイルポリシーのリストと、それらの最終更新日が表示されます。

ファイルポリシーの適用アイコン(☑)をクリックするとダイアログボックスが表示され、そ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示された後、[アクセスコントロールポリシー (Access Control Policy)] ページにリダイレクトされます。これは、ファイルポリシーが親アクセスコントロールポリシーの一部と見なされ、ファイルポリシーを単独で適用できないためです。新しいファイルポリシーを使用したり、既存のファイルポリシーの変更内容を適用したりするには、親アクセスコントロールポリシーを適用/再適用する必要があります。

次の点に注意してください。

- 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、システムはクラウドに照会します(多くても1日に1回)。対象と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適用されている場合、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。更新されたファイルポリシーをデバイスに適用するには、親アクセスコントロールポリシーを再適用する必要があります。
- 保存済みまたは適用済みのアクセスコントロールポリシーで使われているファイルポリシーは削除できません。

ファイルポリシーの管理の詳細については、次の項を参照してください。

- [ファイルポリシーの作成\(37-19 ページ\)](#)
- [ファイルルールの操作\(37-20 ページ\)](#)
- [2つのファイルポリシーの比較\(37-28 ページ\)](#)

ファイルポリシーの作成

ライセンス:Protection または Malware

サポートされるデバイス:機能に応じて異なる

サポートされる防御センター:機能に応じて異なる

ファイルポリシーを作成して、その中でルールを設定すると、それをアクセスコントロールポリシーで使用できるようになります。

DC500 では Malware ライセンスを使用できないため、[マルウェアブロック (Block Malware)] アクションや [マルウェアクラウドルックアップ (Malware Cloud Lookup)] アクションを使用するファイルルールを作成したり、それらのアクションを行うルールを含むファイルポリシーを適用するためにこのアプライアンスを使用したりできないことに注意してください。同様に、シリーズ 2 デバイスまたは Blue Coat X-Series 向け Cisco NGIPS では Malware ライセンスを有効にできないため、これらのアクションを行うルールを含むファイルポリシーをこのアプライアンスに適用することはできません。



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、コピーアイコン(📄)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。

ファイル ポリシーを作成する方法:

アクセス:Admin/Access Admin

-
- 手順 1** [ポリシー (Policies)] > [ファイル (Files)] を選択します。
[ファイル ポリシー (File Policies)] ページが表示されます。
- 手順 2** [新しいファイル ポリシー (New File Policy)] をクリックします。
[新しいファイル ポリシー (New File Policy)] ダイアログ ボックスが表示されます。
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([アクセス コントロール ポリシーの準備 \(12-1 ページ\)](#)を参照)。
- 手順 3** 新しいポリシーの [名前 (Name)] とオプションの [説明 (Description)] を入力してから、[保存 (Save)] をクリックします。
[ファイル ポリシー ルール (File Policy Rules)] タブが表示されます。
- 手順 4** ファイル ポリシーに 1 つ以上のルールを追加します。
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。ファイル ルールの追加については、[ファイル ルールの操作 \(37-20 ページ\)](#)を参照してください。
DC500 では Malware ライセンスを使用できないため、[マルウェア ブロック (Block Malware)] アクションや [マルウェア クラウドルックアップ (Malware Cloud Lookup)] アクションを使用するファイル ルールを作成したり、それらのアクションを行うルールを含むファイル ポリシーを適用するためにこのアプライアンスを使用したりできません。同様に、シリーズ 2 デバイスまたは Blue Coat X-Series 向け Cisco NGIPS では Malware ライセンスを有効にできないため、これらのアクションを行うルールを含むファイル ポリシーをこのアプライアンスに適用することはできません。
- 手順 5** 詳細オプションを設定します。詳細については、[ファイル ポリシーの詳細オプション \(\[一般 \(General\)\]\) の設定 \(37-23 ページ\)](#)と[アーカイブ ファイルのインスペクション オプションの設定 \(37-24 ページ\)](#)を参照してください。
- 手順 6** [保存 (Save)] をクリックします。
新しいポリシーを使用するには、アクセス コントロール ルールにファイル ポリシーを追加してから、アクセス コントロール ポリシーを適用する必要があります。既存のファイル ポリシーを編集している場合は、そのファイル ポリシーを使用するすべてのアクセス コントロール ポリシーを再適用する必要があります。
-

ファイル ルールの操作

ライセンス:Protection または Malware

サポートされるデバイス:機能に応じて異なる

サポートされる防御センター:機能に応じて異なる

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。新しいファイルポリシーを作成するとき、または既存のポリシーを編集するときに表示される [ファイルポリシールール (File Policy Rules)] ページで、ルールを作成、編集、および削除します。このページには、ポリシー内のすべてのルールがリストされ、各ルールの基本的な特性も示されます。

また、このページでは、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の数も通知されます。この通知をクリックすると、親ポリシーのリストが表示され、オプションで [アクセスコントロールポリシー (Access Control Policies)] ページに進むことができます。



注意

ファイルタイプまたはファイルカテゴリを追加または削除したり、[ファイル検出 (Detect Files)] または [マルウェアブロック (Block Malware)] に関するファイルルールアクションを変更したり、[ファイルの保存 (Store Files)] を有効または無効にしたりすると、アクセスコントロールポリシーを適用するときにトラフィックのインスペクションが一時的に中断され、Snort プロセスが再起動されます。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、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、[Snort の再開によるトラフィックへの影響 \(1-9 ページ\)](#) を参照してください。

ファイルルールを作成する方法:

アクセス: Admin/Access Admin

- 手順 1 [ポリシー (Policies)] > [ファイル (Files)] を選択します。
[ファイルポリシー (File Policies)] ページが表示されます。
- 手順 2 次の選択肢があります。
 - 新しいポリシーにルールを追加するには、[新しいファイルポリシー (New File Policy)] をクリックして、新しいポリシーを作成します ([ファイルポリシーの作成 \(37-19 ページ\)](#) を参照)。
 - 既存のポリシーにルールを追加するには、ポリシーの横にある編集アイコン (✎) をクリックします。
- 手順 3 表示される [ファイルポリシールール (File Policy Rules)] ページで、[ファイルルールの追加 (Add File Rule)] をクリックします。
[ファイルルールの追加 (Add File Rule)] ダイアログボックスが表示されます。
- 手順 4 [アプリケーションプロトコル (Application Protocol)] を選択します。
デフォルトの [任意 (Any)] は、HTTP、SMTP、IMAP、POP3、FTP、および NetBIOS-ssn (SMB) トラフィック内のファイルを検出します。
- 手順 5 [転送の方向 (Direction of Transfer)] を選択します。
ダウンロードされるファイルに関して、以下のタイプの着信トラフィックを検査できます。
 - HTTP
 - IMAP
 - POP3
 - FTP
 - NetBIOS-ssn (SMB)

アップロードされるファイルに関して、以下のタイプの発信トラフィックを検査できます。

- HTTP
- FTP
- SMTP
- NetBIOS-ssn(SMB)

[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。

手順 6 ファイル ルールの [アクション (Action)] を選択します。詳細については、[ファイル ルール アクション](#)の表を参照してください。

[ファイル ブロック (Block Files)] または [マルウェア ブロック (Block Malware)] を選択すると、[接続のリセット (Reset Connection)] がデフォルトで有効になります。ファイル転送のブロックが発生した接続をリセットしないようにするには、このオプションをクリアします。



(注)

シスコでは、[接続のリセット (Reset Connection)] を有効のままにしておく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。

ファイル ルールのアクションの詳細については、[ファイル ルール アクションと評価順序 \(37-13 ページ\)](#)を参照してください。

DC500 では Malware ライセンスを使用できないため、[マルウェア ブロック (Block Malware)] アクションや [マルウェア クラウドルックアップ (Malware Cloud Lookup)] アクションを使用するファイル ルールを作成したり、それらのアクションを行うルールを含むファイル ポリシーを適用するためにこのアプライアンスを使用したりできないことに注意してください。同様に、シリーズ 2 デバイスまたは Blue Coat X-Series 向け Cisco NGIPS では Malware ライセンスを有効にできないため、これらのアクションを行うルールを含むファイル ポリシーをこのアプライアンスに適用することはできません。

手順 7 [ファイル タイプ (File Types)] を 1 つ以上選択します。複数のファイル タイプを選択するには、Shift キーと Ctrl キーを使用します。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。

- [ファイル タイプ カテゴリ (File Type Categories)] を 1 つ以上選択します。
- 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、[名前および説明の検索 (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。

ファイル ルールで使用できるファイル タイプは、[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)] での選択内容に応じて変化します。

たとえば、[転送の方向 (Direction of Transfer)] で [ダウンロード (Download)] を選択すると、ファイル イベントが過剰になることを防止するために、[グラフィック (Graphics)] カテゴリから [GIF]、[PNG]、[JPEG]、[TIFF]、および [ICO] が削除されます。

- 手順 8 選択したファイルタイプを [選択済みのファイル カテゴリとタイプ (Selected Files Categories and Types)] リストに追加します。
- [追加 (Add)] をクリックすると、選択したファイルタイプがルールに追加されます。
 - 1 つ以上のファイルタイプを [選択済みのファイル カテゴリとタイプ (Selected Files Categories and Types)] リストの中にドラッグアンドドロップします。
 - カテゴリを選択して [選択済みカテゴリにあるすべてのタイプ (All types in selected Categories)] をクリックしてから、[追加 (Add)] をクリックするか、選択項目を [選択済みのファイル カテゴリとタイプ (Selected Files Categories and Types)] リストの中にドラッグアンドドロップします。
- 手順 9 [保存 (Save)] をクリックします。
- ファイルルールがポリシーに追加されます。既存のファイルポリシーを編集している場合、変更内容を有効にするには、そのファイルポリシーを使用するすべてのアクセスコントロールポリシーを再適用する必要があります。

ファイルポリシーの詳細オプション ([一般 (General)]) の設定

ライセンス: Malware

サポートされるデバイス: 機能に応じて異なる

サポートされる防御センター: 機能に応じて異なる

ファイルポリシーでは、[一般 (General)] セクションにある以下の詳細オプションを設定できます。アーカイブファイルインスペクションの詳細オプションについては、[アーカイブファイルのインスペクションオプションの設定 \(37-24 ページ\)](#) を参照してください。

表 37-7 ファイルポリシーの詳細オプション ([一般 (General)])

フィールド	説明	デフォルト値 (Default Value)
カスタム検知リストを有効にする (Enable Custom Detection List)	これを選択すると、カスタム検出リストにあるファイルが検出されたときに、そのファイルをブロックします。	有効 (enabled)
クリーンリストを有効にする (Enable Clean List)	これを選択すると、クリーンリストにあるファイルが検出されたときに、そのファイルを許可します。	有効 (enabled)
動的分析脅威スコアに基づいたマルウェアとしてのファイルのマーク (Mark files as malware based on dynamic analysis threat score)	しきい値を選択すると、そのスコア以上の脅威スコアを持つファイルが自動的にマルウェアと同じ方法で扱われます。これを無効にするには、[無効 (Disabled)] を選択します。 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数が増えることに注意してください。ファイルポリシーで選択したアクションによっては、この結果として、ブロックされるファイル数が増える可能性があります。	非常に高い (Very High) (76 以上)

DC500 では Malware ライセンスを使用できないため、これらの設定を使用/変更できないことに注意してください。同様に、シリーズ 2 デバイスまたは Blue Coat X-Series 向け Cisco NGIPS で Malware ライセンスを有効にすることはできないため、これらの設定を有効にしたファイルポリシーを適用することはできません。

ファイル ポリシーの詳細オプション([一般(General)])を設定するには、次の手順を実行します。
アクセス:Admin/Access Admin

-
- 手順 1 [ポリシー(Policies)] > [ファイル(Files)] を選択します。
[ファイル ポリシー(File Policies)] ページが表示されます。
- 手順 2 編集するポリシーの横にある編集アイコン(✎)をクリックします。
[ファイル ポリシー ルール(File Policy Rules)] ページが表示されます。
- 手順 3 [詳細設定(Advanced)] タブを選択します。
[詳細設定(Advanced)] タブが表示されます。
- 手順 4 [一般(General)] セクションで、[ファイル ポリシーの詳細オプション\(\[一般\(General\)\]\)](#)の表に示すように、オプションを変更します。
- 手順 5 [保存(Save)] をクリックします。
編集したファイル ポリシーを使用するすべてのアクセス コントロール ポリシーを再適用する必要があります。
-

アーカイブ ファイルのインスペクション オプションの設定

ライセンス:Malware

サポートされるデバイス:すべて(シリーズ 2 または X-シリーズ を除く)

サポートされる防御センター:DC500 を除くいずれか

アーカイブ ファイル(.zip または .rar など)は多くの場合、モニタ対象トラフィックで現れます。正当な情報を圧縮して転送するための便利な方法にすぎないものもあれば、マルウェアや他の望ましくないファイルを隠そうとするものもあります。組織のニーズに合わせてアーカイブ ファイルを分析し、必要に応じてブロックできるように、アーカイブ ファイルの内容を検査するようファイル ポリシーを設定できます。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。コンテキスト メニューを使用して、イベント ビューアまたはファイル トラジェクトリ ビューアからアーカイブ ファイルの内容を表示できます。詳細については、[項 **アーカイブ ファイルの内容の表示** \(37-26 ページ\)](#)を参照してください。




(注) 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 インテリジェンスによってブラック リスト登録またはホワイトリスト登録された場合、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ラックリスト登録された場合、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ホワイトリスト登録された場合、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)。詳細については、[グローバル ホワイトリストおよびブラックリストの操作\(3-7 ページ\)](#)を参照してください。

一部のアーカイブ ファイルには、追加のアーカイブ ファイル(など)が含まれています。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で考慮さ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。システムでは、ネストされたアーカイブ ファイルを最大 3 レベルまでしか検査できませんが、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。ネストされたアーカイブをさらに制限する場合は、2 または 1 のより低い最大ファイル深さを設定するオプションがあります。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。

アーカイブ ファイルは、それに含まれているファイルの性質に基づいてファイルの性質を取得します。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、いずれかの不明なファイルが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。ファイルの性質の詳細については、[ファイルの性質について\(37-4 ページ\)](#)を参照してください。

次の表に、ファイル ポリシーで設定できるアーカイブ ファイルのインスペクション オプションを示します。

表 37-8 アーカイブファイルのインスペクションオプション

フィールド	説明	デフォルト値(Default Value)
アーカイブの検査(Inspect Archives)	<p>アーカイブ ファイルの内容を検査する場合に選択します。このオプションがオフの場合、下のオプションはグレー表示となり使用できません。</p> <p> 注意 アーカイブ ファイルのインスペクションを有効または無効にすると、変更を適用するときにトラフィックのインスペクションが一時的に中断され、Snort プロセスが再起動されます。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、管理対象デバイスのモデルおよびトラフィックの処理方法に応じて異なります。詳細については、Snort の再開によるトラフィックへの影響(1-9 ページ)を参照してください。</p>	無効
暗号化されたアーカイブをブロック(Block Encrypted Archives)	暗号化された内容があるアーカイブ ファイルをブロックする場合に選択します。	無効
検査不可のアーカイブをブロック(Block Uninspectable Archives)	システムが暗号化以外の理由で検査できない内容を含むアーカイブ ファイルをブロックする場合に選択します(これは通常、何らかの理由で破損したファイル、または指定した最大アーカイブの深さを超えるファイルに適用されます)。	[有効 (Enabled)]
アーカイブの最大深度(Max Archive Depth)	ネストされたアーカイブ ファイルの最大深さを指定します。この深さを超えるアーカイブ ファイルはブロックされます。値は 1、2、または 3 にしてください。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。	2

アーカイブ ファイルのインスペクション オプションを設定するには、次の手順を実行します。
 アクセス:Admin/Access Admin

-
- 手順 1 [ポリシー (Policies)] > [ファイル (Files)] を選択します。
 [ファイル ポリシー (File Policies)] ページが表示されます。
- 手順 2 編集するポリシーの横にある編集アイコン(✎)をクリックします。
 [ファイル ポリシー ルール (File Policy Rules)] ページが表示されます。
- 手順 3 [詳細設定 (Advanced)] タブを選択します。
 [詳細設定 (Advanced)] タブが表示されます。
- 手順 4 [アーカイブ ファイルのインスペクション (Archive File Inspection)] セクションで、[アーカイブ ファイルのインスペクション オプション](#)に示すように、オプションを変更します。
- 手順 5 [保存 (Save)] をクリックします。
 編集したファイル ポリシーを使用するすべてのアクセス コントロール ポリシーを再適用する必要があります。
-

アーカイブ ファイルの内容の表示

ライセンス:Malware

サポートされるデバイス:すべて(シリーズ 2 または X-シリーズ を除く)

サポートされる防御センター:DC500 を除くいずれか

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、イベント ビューアのコンテキスト メニューおよびネットワーク ファイル トラジェクトリ ビューアを使用して、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。

詳細については、以下を参照してください。

- [コンテキスト メニューの使用\(2-5 ページ\)](#)
- [ファイル イベントの表示\(40-9 ページ\)](#)
- [マルウェア イベントの表示\(40-20 ページ\)](#)
- [キャプチャ ファイルの表示\(40-34 ページ\)](#)
- [ネットワーク ファイル トラジェクトリの確認\(40-40 ページ\)](#)

[アーカイブ コンテンツ (Archive Contents)] ウィンドウは 2 つの方法で表示できます。対象となるアーカイブ ファイルを右クリックして、コンテキスト メニューから [アーカイブ コンテンツの表示 (View Archive Contents)] を選択することでイベント ビューアから表示するか、または [アーカイブ コンテンツ (Archive Contents)] の下の表示アイコン(🔍)をクリックして、アーカイブ ファイルのファイル トラジェクトリ ビューアから表示します。いずれの場合も、表示されるウィンドウは同じです。次の図は、[アーカイブ コンテンツ (Archive Contents)] ウィンドウの例を示しています。

Archive Contents

Archive Name	慮る.zip			
Archive SHA256	cf264a33...bacc27a3			
Last Inspected	2014-04-03 12:15:33			
File Name	SHA256	Type	Category	Depth
INVALID_BINARY_DETECT...	Offba5e0...8ce35df7	MSEXE	Executables	1
t1.exe	2fdce4c9...6823ae87	MSEXE	Executables	1
t2.zip	d935cb63...8244a4f3	ZIP	Archive	1
sample.pdf	25163cdd...2c6834ca	PDF	PDF files	2

Close

373591

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、ネットワーク トラジェクトリ機能を使用した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。

イベント ビューアからアーカイブされたファイルの内容を表示するには、次の手順を実行します。

アクセス: Admin/Access Admin

- 手順 1** 選択したイベント ビューアに移動します。次の 3 つのオプションがあります。
- マルウェア イベントの場合は、[分析 (Analysis)] > [ファイル (Files)] > [マルウェア イベント (Malware Events)] を選択します。
 - ファイル イベントの場合は、[分析 (Analysis)] > [ファイル (Files)] > [ファイル イベント (File Events)] を選択します。
 - キャプチャされたファイルの場合は、[分析 (Analysis)] > [ファイル (Files)] > [キャプチャされたファイル (Captured Files)] を選択します。
- デフォルトのイベント ワークフローの最初のページが表示されます。
- 手順 2** 検査するアーカイブ ファイルが表示されるテーブルの行を右クリックします。コンテキスト メニューが表示されます。
- 手順 3** コンテキスト メニューから、[アーカイブ コンテンツの表示 (View Archive Contents)] をクリックします。
- [アーカイブ コンテンツ (Archive Contents)] ウィンドウが表示されます。

ファイル トrajェクトリ ビューアからアーカイブされたファイルの内容を表示するには、次の手順を実行します。

アクセス:Admin/Access Admin

-
- 手順 1 [分析 (Analysis)] > [ファイル (Files)] > [ネットワーク ファイル トrajェクトリ (Network File Trajectory)] を選択します。
[ネットワーク ファイル トrajェクトリ リスト (Network File Trajectory List)] ページが表示されます。
- 手順 2 検査するアーカイブ ファイルのファイル トrajェクトリ アイコン(📁)をクリックします。
そのファイルのファイル トrajェクトリ ページが表示されます。
- 手順 3 [アーカイブ コンテンツ (Archive Contents)] の下で、表示アイコン(🔍)をクリックします。
[アーカイブ コンテンツ (Archive Contents)] ウィンドウが表示されます。
-

2 つのファイル ポリシーの比較

ライセンス:Protection

変更後のポリシーが組織の標準に準拠することを確認したり、システム パフォーマンスを最適化したりする目的で、任意の 2 つのファイル ポリシー間の違いや、同じポリシーの 2 つのリビジョン間の違いを調べることができます。

ファイル ポリシーの比較ビューには、2 つのポリシーまたはリビジョンが並んで表示され、各ポリシー名の横には最終変更時刻と最後に変更したユーザが表示されます。2 つのポリシー間の差異は、次のように強調表示されます。

- 青色は強調表示された設定が 2 つのポリシーで異なることを示し、差異は赤色で示されます。
- 緑色は強調表示された設定が一方のポリシーには存在するが、他方には存在しないことを示します。

[前へ (Previous)] と [次へ (Next)] をクリックすると、前後の相違箇所に移動できます。左側と右側の間にある二重矢印アイコン(↔)が移動し、表示している違いを示す [差異 (Difference)] 番号が変わります。オプションで、ファイル ポリシーの比較レポートを生成できます。これは PDF 版の比較ビューです。

2 つのファイル ポリシーを比較する方法:

アクセス:Admin/Access Admin

-
- 手順 1 [ポリシー (Policies)] > [ファイル (Files)] を選択します。
[ファイル ポリシー (File Policies)] ページが表示されます。
- 手順 2 [ポリシーの比較 (Compare Policies)] をクリックします。
[比較の選択 (Select Comparison)] ダイアログ ボックスが表示されます。

- 手順 3 [比較対象 (Compare Against)] ドロップダウン リストから、比較するタイプを次のように選択します。
- 2 つの異なるポリシーを比較するには、[実行中の設定 (Running Configuration)] または [他のポリシー (Other Policy)] を選択します。この 2 つのオプションの違いは、[実行中の設定 (Running Configuration)] を選択した場合、現在適用されている一連のファイル ポリシーの中からのみ、比較対象の 1 つを選択できます。
 - 同じポリシーの複数のバージョンを比較するには、[その他のリビジョン (Other Revision)] を選択します。
- ダイアログ ボックスの表示が更新され、比較オプションが示されます。
- 手順 4 選択した比較タイプに応じて、次のような選択肢があります。
- 2 つの異なるポリシーを比較する場合、比較対象のポリシーとして [ポリシー A (Policy A)] または [ターゲット/実行中の設定 A (Target/Running Configuration A)] のどちらかと、[ポリシー B (Policy B)] とを選択します。
 - 同じポリシーのバージョン間を比較する場合、対象の [ポリシー (Policy)] を選択してから、2 つのリビジョン [リビジョン A (Revision A)] と [リビジョン B (Revision B)] を選択します。リビジョンは、日付とユーザ名別にリストされます。
- 手順 5 [OK] をクリックします。
- 比較ビューが表示されます。
- 手順 6 必要に応じて、アクセス コントロール ポリシー比較レポートを生成するには [比較レポート (Comparison Report)] をクリックします。
- 比較レポートが表示されます。ブラウザの設定によっては、レポートがポップアップ ウィンドウで表示されるか、コンピュータにレポートを保存するようにプロンプトが出されることがあります。

FireAMP 用のクラウド接続の操作

ライセンス:任意 (Any)

FireAMP は、シスコが提供するエンタープライズ向けの高度なマルウェア分析/対策ソリューションです。お客様の組織で FireAMP サブスクリプションをご利用の場合、個々のユーザは自分のコンピュータやモバイル デバイスに FireAMP コネクタをインストールします。これらの軽量エージェントはシスコクラウドと通信し、さらにクラウドが Defense Center と通信します。クラウドに接続するよう Defense Center を設定した後、スキャン、マルウェア検出、および検疫のレコードを受信できるようになります。レコードは、マルウェア イベントとして Defense Center データベースに保存されます。詳細については、[マルウェア防御とファイル制御について \(37-2 ページ\)](#)を参照してください。

組織のセキュリティ ポリシーで従来型クラウド サーバ接続の使用が許可されていない場合、シスコのプライベート オンプレミス クラウド ソリューションである FireAMP プライベート クラウドを入手して設定できます。これは、圧縮された、パブリックのシスコクラウドのローカルバージョンとして機能する仮想マシンです。この場合、データとアクション (FireAMP コネクタからのイベント、ファイルの性質ルックアップ、レトロスペクティブ イベントなど) は、通常の方法でクラウド接続を経由する代わりに、組織のプライベート クラウドへのローカル接続によって処理されます。(ファイルの性質ルックアップなどのために) 外部クラウドへの接続が必要になったとき、プライベート クラウドは、Defense Center とパブリックのシスコクラウドとの間の匿名化されたプロキシとして機能します。プライベート クラウドでは、エンドポイント イベント データは外部接続で共有されません。プライベート クラウドの構成方法の詳細については、[FireAMP プライベート クラウドの操作 \(37-33 ページ\)](#)を参照してください。



(注) プライベート クラウドは、動的分析をサポートしていません。

また、FireAMP コネクタがインストールされたホストでは、侵害の兆候 (IOC) タグを生成できません。これは、エンドポイント ベースのマルウェア検出アクティビティにより、あるホストでセキュリティ侵害が発生した可能性が示唆されたとき、そのホストに関して生成されます。Defense Center からホストのエンドポイント IOC 情報を表示するには、そのホストは Defense Center のネットワーク マップに表示される必要があります。シスコ ではエンドポイント ベースのマルウェア イベントに関する新しい IOC タイプが開発される場合があります。システムは、シスコクラウドからこれを自動的にダウンロードします。侵害の兆候の詳細については、[侵害の兆候 \(痕跡\) について \(45-22 ページ\)](#) および [エンドポイント ベースのマルウェア イベント IOC タイプ \(45-23 ページ\)](#) を参照してください。

展開内のそれぞれの Defense Center は、シスコクラウドに接続できます。デフォルトで、クラウドは組織内のすべてのグループに関するマルウェア イベントを送信しますが、接続を設定するときにグループごとに制限できます。

インターネットアクセスとハイアベイラビリティ

エンドポイント ベースのマルウェア イベントを受信するために、システムはポート 443/HTTPS を使用してシスコクラウド (パブリックまたはプライベート) に接続します。Defense Center で、このポートをインバウンドとアウトバウンドの両方に開く必要があります。また、Defense Center はインターネットへのダイレクトアクセスを必要とします。デフォルトのヘルスポリシーに含まれる FireAMP ステータス モニタは、Defense Center からクラウド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 FireAMP 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。

エンドポイント ベースのマルウェア イベントを受信するクラウド接続は、ハイアベイラビリティ ペアのメンバー間では共有されません。運用の継続性を確保するには、プライマリとセカンダリの両方の Defense Center をクラウドに接続してください。

クラウド接続の管理

Defense Center の [AMP 管理 (AMP Management)] ページ ([AMP] > [AMP 管理 (AMP Management)]) を使用すると、シスコクラウドまたはプライベートクラウドへの接続の表示と作成、およびそれらの接続の無効化と削除を行うことができます。

回転する状態アイコンは、接続が保留中であることを示します。たとえば、Defense Center で接続の設定がすでに完了した後、FireAMP ポータルを使って接続を承認しなければならない場合です。失敗または拒否を示すアイコン (❗) 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。



ヒント

いずれかのクラウド名をクリックすると、FireAMP ポータルが新しいブラウザ ウィンドウで開きます。

詳細については、以下を参照してください。

- [シスコクラウド接続の作成 \(37-31 ページ\)](#)
- [クラウド接続の削除または無効化 \(37-32 ページ\)](#)
- [FireAMP プライベートクラウドの操作 \(37-33 ページ\)](#)

シスコクラウド接続の作成

ライセンス:任意(Any)

Defense Center とシスコクラウドの間の接続の作成は、2 段階からなるプロセスです。まず、クラウドに接続するよう Defense Center を設定します。次に、FireAMP ポータルにログインして接続を承認します。FireAMP サブスクリプションがない場合は、登録プロセスを完了できません。

デフォルトでは、ネットワークベース AMP で有効になっている米国のパブリッククラウドに接続しています。この接続はファイルポリシーでのファイルルックアップに使用されます。

工場出荷時の初期状態に復元された Defense Center、またはクラウドへの登録中に取り消された Defense Center を再登録するには、再登録する前に FireAMP に接続し、Defense Center を削除する必要があります。

FireAMP 用のシスコクラウド接続を作成する方法:

アクセス:管理

-
- 手順 1 [AMP (AMP)] > [AMP 管理 (AMP Management)] を選択します。
[AMP 管理 (AMP Management)] ページが表示されます。
 - 手順 2 [FireAMP 接続の作成 (Create FireAMP Connection)] をクリックします。
[Create FireAMP Connection] ダイアログ ボックスが表示されます。
 - 手順 3 [クラウド名 (Cloud Name)] ドロップダウン ボックスから、使用するクラウドを選択します。
 - 欧州連合クラウドの場合、[EU クラウド (EU Cloud)] を選択します。
 - 米国クラウドの場合、[US クラウド (US Cloud)] を選択します。
 - プライベートクラウドの場合、[プライベートクラウド (Private Cloud)] を選択し、[FireAMP プライベートクラウドの操作 \(37-33 ページ\)](#) に示されている追加の手順に従います。
 - 手順 4 [登録 (Register)] をクリックします。
 - 手順 5 FireAMP ポータルに移動してもよいことを確認し、ポータルにログインします。
ポータルの [アプリケーション (Applications)] ページが表示されます。このページを使用して、シスコクラウドがマルウェア イベントを Defense Center に送信することを承認します。
 - 手順 6 オプションで、マルウェア イベントの受信対象となる組織内の特定のグループを選択できます。
受信するイベントを制限する必要がある場合にのみ、グループを選択してください。デフォルトで、Defense Center はすべてのグループに関するマルウェア イベントを受信します。



ヒント グループを管理するには、FireAMP ポータルで [Management] > [Groups] を選択します。詳細については、ポータルのオンライン ヘルプを参照してください。

-
- 手順 7 [許可 (Allow)] をクリックします。
Defense Center の [FireAMP Management] ページに戻ります。接続が有効になり、Defense Center はクラウドからマルウェア イベントを受信し始めます。

なお、[拒否 (Deny)] をクリックした場合にも Defense Center に戻りますが、クラウド接続には拒否マークが付きます。同様に、接続を拒否/許可しないまま FireAMP ポータルの [Applications] ページから別のページに移動した場合、Defense 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。どちらの場合も、ヘルス モニタはアラートを出しません。後で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する必要があります。

エンドポイント ベース FireAMP 接続の登録が完了していない場合、ネットワークベース AMP 接続は無効になりません。

クラウド接続の削除または無効化

ライセンス:任意 (Any)

クラウドからマルウェア イベントを受信する必要がなくなった場合は、シスコクラウド接続またはプライベートクラウド接続を削除します。ネットワークベース AMP で有効なクラウド接続は削除できません。

一時的に特定の接続でのマルウェア イベント受信を停止するには、接続を削除するのではなく、接続を無効にすることができます。その場合、接続が再び有効にされるまでクラウドはイベントを保存し、有効になった後、保存済みイベントがクラウドから送信されます。



注意

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イベントをクラウドで保存できないことがあります。

なお (Defense Center の Web インターフェイスではなく) FireAMP ポータルを使用して接続の登録を解除すると、イベント送信が停止しますが、Defense Center からは接続が削除されないことに注意してください。登録解除された接続は [FireAMP Management] ページで失敗状態として表示され、それを削除する必要があります。

Defense Center を使用してクラウド接続を有効または無効にする方法:

アクセス:管理

手順 1 [AMP 管理 (AMP Management)] ページで、削除する接続の横のスライダをクリックしてから、接続を有効または無効にすることを確認します。

接続を有効にすると、クラウドは Defense Center にイベントを送信し始めます。このとき、接続が無効だった間に発生したイベントも送信されます。クラウドは、無効化された接続のイベントを送信しません。

Defense Center を使用してクラウド接続を削除する方法:

アクセス:管理

手順 1 [AMP 管理 (AMP Management)] ページで、削除する接続の横の削除アイコン(🗑️)をクリックしてから、接続の削除を確認します。

接続が削除され、クラウドは Defense Center へのイベントの送信を停止します。

FireAMP プライベートクラウドの操作

ライセンス:任意(Any)

組織のプライバシーやセキュリティ上の理由で、モニタ対象ネットワークと外部クラウドサーバとの間で頻繁に接続することが困難、または不可能な場合があります。この場合、FireAMP プライベートクラウドを入手して設定することができます。これはシスコ独自の仮想マシンであり、ネットワークとシスコ FireAMP クラウドの間のセキュアなメディアータとして機能します。多くのアプライアンスからの識別可能な接続の代わりに、パブリックの外部シスコクラウドへのすべての必要な接続が一括してプライベートクラウド経由で流れます。プライベートクラウドは匿名化されたプロキシとして動作することで、モニタ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します。各プライベートクラウドは、最大で 10,000 個のコネクタをサポートできます。組織の必要に応じて、ネットワーク上に複数のプライベートクラウドを設定できます。

FireAMP プライベートクラウドは、クラウドベースによるファイルの性質ルックアップ処理、エンドポイントベースの FireAMP イベント取得、およびレトロスペクティブマルウェアイベント生成を処理します。パブリッククラウドの代わりに機能するプライベートクラウドは、FireAMP コネクタのエンドポイントからマルウェアイベントを収集して、それらを Defense Center に送信します。匿名化されたプロキシプライベートクラウド接続を介して、(ファイルの性質や SHA-256 値などを判別するための)パブリックのシスコクラウドへの照会だけが、ネットワークから発信されます。エンドポイントイベントデータは、ネットワークから発信されません。

クラウドベースのファイル機能およびマルウェア機能の詳細については、以下を参照してください。

- [マルウェア防御とファイル制御について\(37-2 ページ\)](#)
- [FireAMP と FireSIGHT システムの統合\(37-8 ページ\)](#)
- [動的分析の操作\(40-5 ページ\)](#)
- [エンドポイントベース\(FireAMP\)のマルウェア イベント\(40-18 ページ\)](#)
- [レトロスペクティブマルウェア イベント\(40-19 ページ\)](#)

本ドキュメンテーション、およびプライベートクラウドでサポートされる機能に関する他のドキュメンテーションで「クラウド」または「シスコクラウド」に言及する場合、特に明記されない限り、プライベートクラウドを介した接続も当てはまります。プライベートクラウドは標準のクラウド接続と同じオープンポートを必要とし、同じハイアベイラビリティ制限事項があります。



(注)

FireAMP プライベートクラウドは、マルウェア関連およびファイル関連のクラウドベース機能のみをサポートします。クラウド接続を使用するその他の FireSIGHT システム機能(URL フィルタリングやセキュリティインテリジェンスなど)はサポートされません。また、プライベートクラウドは動的分析機能をサポートしませんが、プライベートクラウドを使用して、シスコがすでに動的に分析したファイルの脅威スコアを取得できます。

Defense Center と FireAMP プライベートクラウドの間の接続を作成するには、まず FireAMP プライベートクラウドを設定する必要があります(サポートサイトで入手可能な『*FireAMP Private Cloud Administration Portal User Guide*』の手順に従います)。この設定中に、[FireAMP コンソール(FireAMP Console)] フィールドに表示されるプライベートクラウドホスト名を必ずメモしておいてください。プライベートクラウドを Defense Center に接続するために、このホスト名が必要になります。プライベートクラウドが正常に設定されると、設定済みのパブリッククラウド接続がある場合はそれがすべて自動的に無効化されることに注意してください。

Defense Center と FireAMP プライベート クラウドの間の接続を作成する方法:

アクセス:管理

-
- 手順 1 [AMP(AMP)] > [AMP 管理(AMP Management)] を選択します。
[AMP 管理(AMP Management)] ページが表示されます。
 - 手順 2 [FireAMP 接続の作成(Create FireAMP Connection)] をクリックします。
[Create FireAMP Connection] ダイアログ ボックスが表示されます。
 - 手順 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。
追加のフィールドがダイアログボックスに表示されます。
 - 手順 4 [名前(Name)] フィールドに、プライベート クラウド接続の名前を入力します。この名前は、マルウェア イベントを表示したときに FireAMP クラウド イベント フィールドに表示されます。
 - 手順 5 [ホスト(Host)] フィールドに、プライベート クラウドのホスト名を入力します。これは、FireAMP プライベート クラウド仮想マシンを設定したときに [FireAMP コンソール(FireAMP Console)] フィールドに表示されたものです。
 - 手順 6 [証明書アップロードパス(Certificate Upload Path)] フィールドで、プライベート クラウドの有効な TLS または SSL 暗号化証明書情報の場所を参照します。詳細については、『*FireAMP Private Cloud Administration Portal User Guide*』を参照してください。
 - 手順 7 モニタ対象ネットワーク用に複数のプライベート クラウドが設定されている場合、どのプライベート クラウドでネットワークベースのマルウェア ルックアップを処理するかを決定するには、[ネットワーク AMP に使用(Use For NetworkAMP)] チェックボックスをオンまたはオフにします。1 つのプライベート クラウドだけが設定されている場合、デフォルトでチェックボックスがオンになり、オフにすることはできません。
 - 手順 8 Defense Center で設定されたプロキシ接続があり、そのプロキシ接続をプライベート クラウドに使用する場合は、[接続にプロキシを使用(Use Proxy for Connection)] チェックボックスを選択します。このオプションが選択されていない場合、プライベート クラウドはその通信に設定されたプロキシを使用しません。
 - 手順 9 [登録(Register)] をクリックします。
ダイアログボックスが表示され、プライベート クラウド設定を作成すると設定済みのすべてのパブリック クラウド接続が無効になることが通知されます。
 - 手順 10 [Yes] をクリックします。
FireAMP ポータルに移動してもよいことを確認し、ポータルにログインします。
 - 手順 11 プライベート クラウド情報がシステムによって処理され、設定を完了するために FireAMP サイトにリダイレクトされます。詳細な手順については、『*FireAMP Private Cloud Administration Portal User Guide*』を参照してください。
-