CHAPTER 33

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 トラジェクトリ、および高度なマルウェア対策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。

全体的なアクセス制御設定の一部として、マルウェア対策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*）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。

また、お客様の組織で FireAMP サブスクリプションをご利用の場合、防御センターは、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。防御センターは、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。

コンテキスト エクスプローラとダッシュボードは、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 [network file 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、マルウェア対策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 33-1　ファイルおよびマルウェア検出のライセンス要件

機能	説明	ライセンス
ファイル制御	特定のファイル タイプのネットワーク トラフィック伝送を検出し、（オプションで）ブロックする	Protection
高度なマルウェア対策	ネットワーク トラフィックにおけるマルウェア ファイルおよび指定されたファイルの伝送を検出、保存、追跡、および（オプションで）ブロックする。キャプチャされたファイルを、マルウェア分析のためにシスコ クラウドに送信する。	Malware
FireAMP 統合	組織の FireAMP サブスクリプションを使用して、エンドポイント ベースのマルウェア情報をシスコ クラウドから受信し、この情報を使ってマルウェア ファイルの伝送を追跡する	任意
位置情報	ファイルとマルウェア イベントに関連付けられた送信元と宛先の国やその他の地理情報を検出する	FireSIGHT（詳細情報を得るには GeoDB 更新も必要）

DC500 ではMalware ライセンスを使用できず、シリーズ 2 デバイスで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個別のファイルをキャプチャ、保存、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の伝送経路を表示したりすることはできません。

ファイルとマルウェア クラウドベースの機能に関して、組織で追加のセキュリティが必要な場合や、外部接続を制限する必要がある場合には、標準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。エンドポイント FireAMP からのイベント データの収集とリレー、およびファイルとマルウェア クラウドのルックアップはすべて、プライベート クラウド経由で処理されます。プライベート クラウドが標準シスコ クラウドと通信するときには、匿名化プロキシ接続を経由します。

詳細については、以下を参照してください。

- 「マルウェア対策とファイル制御について」（P.33-3）
- 「ファイル ポリシーの概要と作成」（P.33-10）
- 「FireAMP 用のクラウド接続の操作」（P.33-24）

マルウェア対策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」（P.34-1）を参照してください。

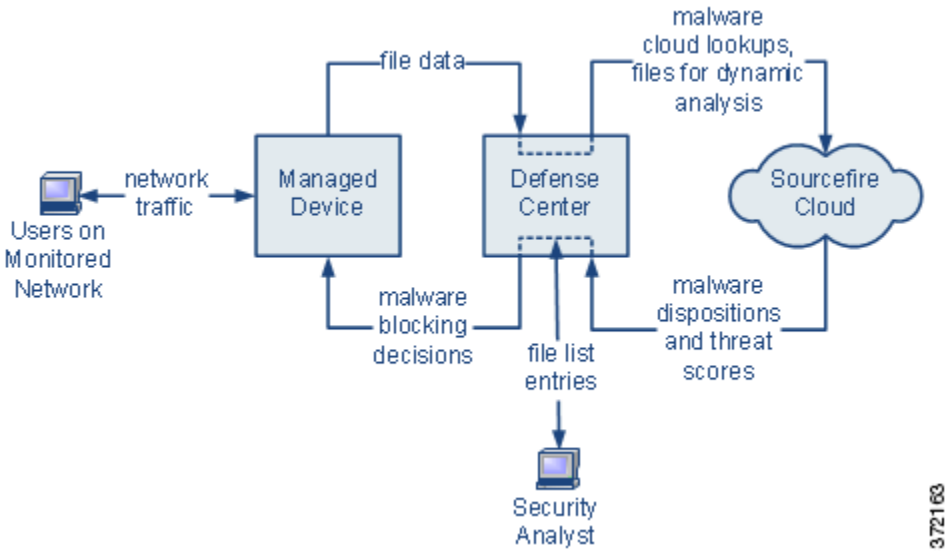
マルウェア対策とファイル制御について

ライセンス：Protection、Malware、または任意

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：機能に応じて異なる

*高度なマルウェア対策*機能を使用すると、次の図に示すように、ネットワークで伝送されるマルウェア 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 タイプの伝送を監視します。該当す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 ハッシュ値を防御センターに送信できます。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 クラウドは防御センター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、該当す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。クラウドは防御センター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概要レポート。

また、該当す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スペロ分析を実行し、結果として得られたスペロ 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** アクションと**マルウェア ブロック** 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る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す。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」（P.5-37）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。

- マルウェアは、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。
- クリーンは、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。
- 不明は、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。
- カスタム検出は、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。
- 使用不可は、防御センターがマルウェア 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。

ヒント　最近のいくつかのマルウェア イベントで使用不可の性質が示されている場合は、クラウド接続と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」（P.E-1）を参照してください。

ファイルの性質に基づき、ファイルをブロックするか、ファイルのダウンロード/アップロードを許可するよう、防御センターが管理対象デバイスに指示します。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、防御センターはシスコ 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、クラウドが防御センターに通知を送りま

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。マルウェア対策の場合と同様に、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 タイプの伝送を監視し、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対策とは異なり、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。防御センターの 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、コンテキスト エクスプローラ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、個々のファイルの転送パスを追跡できます。ファイルの伝搬経路ページには、ファイルの概要情報、ホスト間のファイル転送（ブロックされた転送も含む）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 デバイスで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、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伝送経路を表示したりすることはできません。

詳細については、次の項を参照してください。

- 「マルウェア対策とファイル制御の設定」（P.33-6）
- 「マルウェア対策とファイル制御に基づくイベントのロギング」（P.33-6）
- 「FireAMP と FireSIGHT システムの統合」（P.33-7）
- 「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」（P.33-8）
- 「ネットワーク ファイル トラジェクトリの操作」（P.34-31）

マルウェア対策とファイル制御の設定

ライセンス：Protection または Malware

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：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、全体的なアクセス制御設定の一部として、マルウェア対策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 ポリシーには、親アクセス コントロール ポリシーと同様に、各ルールの条件に一致するファイルの処理方法を決定するルールがいくつか含まれています。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 ポリシーでは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

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」（P.33-10）および「許可されたトラフィックに対するファイル インスペクションと侵入インスペクションの実行」（P.14-35）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対策を行うファイル 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対策を行うファイル 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。

マルウェア対策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

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：機能に応じて異なる

防御センターは、システムでのファイル インスペクション レコードをログに記録し、次に示す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 イベントとしての処理を記録します。

- *キャプチャされたファイル*は、システムでキャプチャされたファイルを表します。
- *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（さらに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（さらに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。
- *遡及的マルウェア イベント*は、マルウェア ファイルの性質が変更されたファイルを表します。

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るため、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」（P.33-7）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。

防御センターを使用すると、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伝達できます。コンテキスト エクスプローラ、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」（P.34-8）および「マルウェア イベントの操作」（P.34-14）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 デバイスで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、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

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。

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*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、クラウドは脅威の識別情報を防御センターに送ります。さらにクラウドは、スキャン、検疫、実行のブロッキング、クラウド リコールなど、他の種類のデータを防御センターに送ることもできます。防御センター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防御センター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
- アウトブレイク制御のさまざまな局面を設定する：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 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」（P.33-8）に、シスコ製品ファミリで使用可能なマルウェア対策戦略の比較を示します。
- 「FireAMP 用のクラウド接続の操作」（P.33-24）では、防御センターとシスコ クラウドの間の通信を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。

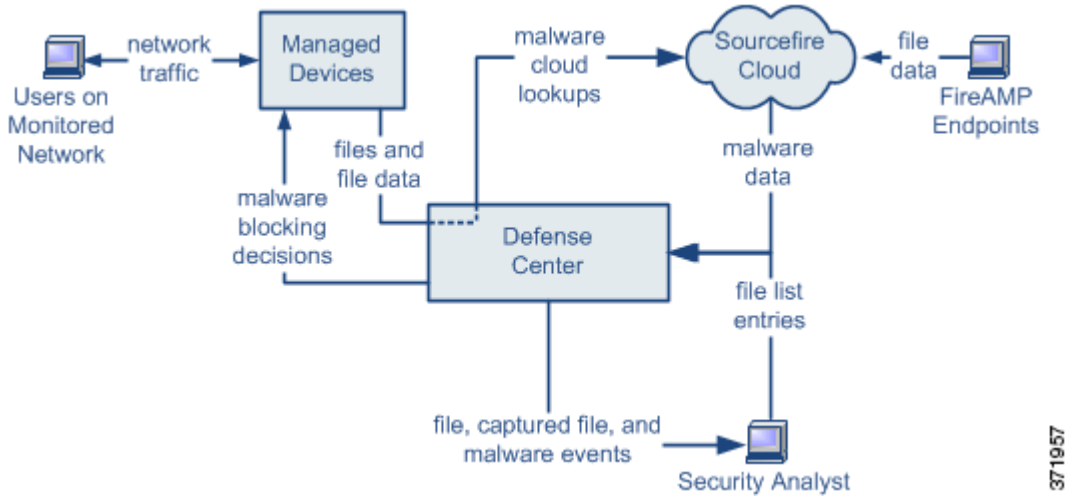
ネットワークベースの AMP とエンドポイント ベースの FireAMP の比較

ライセンス：Malwareまたは任意

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：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対策戦略と、エンドポイント ベースの FireAMP 戦略の両方からのデータを防御センターでどのように使用できるかを次の図に示します。



FireAMP 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、ファイル伝送に使われた接続のポート、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、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伝送経路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 33-3　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対策戦略の比較

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	サポートされていません
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します）
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	防御センター ベース、およびクラウドでの分析	防御センター 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 ブロッキング、防御センターが開始する修復	FireAMP ベースの検疫およびアウトブレイク制御オプション、防御センターが開始する修復
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 イベント内の情報	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）

表 33-3　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対策戦略の比較 （続き）

機能	ネットワークベース	エンドポイント ベース （FireAMP）
ネットワーク ファイル トラジェクトリ	防御センター ベース	防御センター 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、マルウェア対策を実行するには 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）

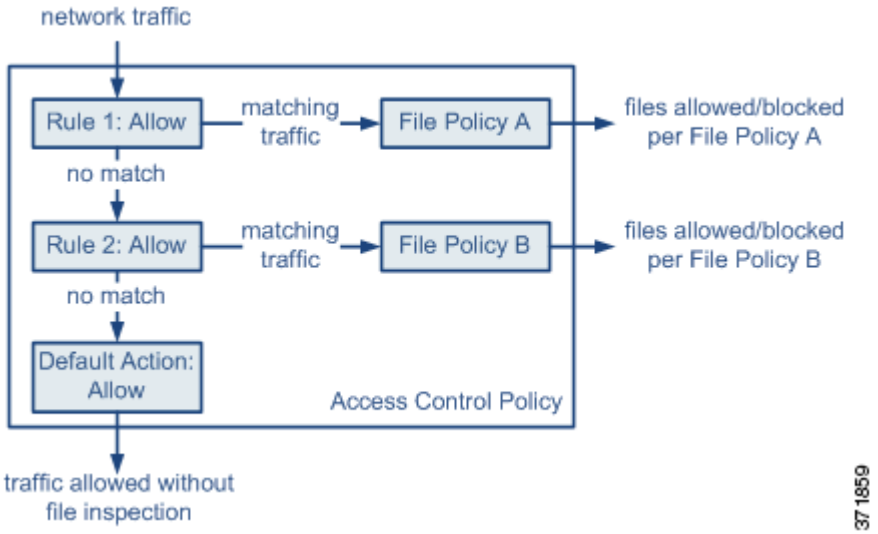
ファイル ポリシーの概要と作成

ライセンス：Protection または Malware

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：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制御設定の一部としてこれを使用して、高度なマルウェア対策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 ポリシーがあるとします。



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 ポリシーには、親アクセス コントロール ポリシーと同様に、各ルールの条件に一致するファイルの処理方法を決定するルールがいくつか含まれています。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
- 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 ポリシーでは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

1 つのファイル ポリシーを、**許可**、**インタラクティブ ブロック**、または **リセット付きインタラクティブ ブロック** 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。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。つまり、このような関連付けを行うと、アクセス コントロール ルールの条件に一致するトラフィックを通過させる前に、システムはファイル ポリシーを使ってトラフィックを検査するようになります。

なお、インタラクティブ ブロックされたトラフィックに対してファイル インスペクションを実行できるのは、ユーザが警告を迂回し、クリックして、最初に要求されたサイトに進んだ場合のみであることに注意してください。そうでない場合、ファイル インスペクションや侵入インスペクションが行われずに接続が拒否されます（「ルール アクションについて」（P.14-6）および「HTTP 応答ページの追加」（P.13-12）を参照してください）。

同じアクセス コントロール ポリシーで、個々のアクセス コントロール ルールにさまざまなファイル ポリシーを関連付けることができます。これにより、さまざまなファイル/マルウェア検出プロファイルを、ネットワーク上のさまざまなタイプのトラフィックに照合させることができます。ただし、アクセス制御のデフォルト 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。

また、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対策を行うファイル 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対策を行うファイル 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。

ファイル ポリシーと侵入ポリシーのインタラクション

ファイル ポリシーと侵入ポリシーの両方をアクセス コントロール ルールに関連付けることができます。その場合、2 つのポリシーの相互作用により、トラフィックの検査方法が変化する可能性があることに注意してください。

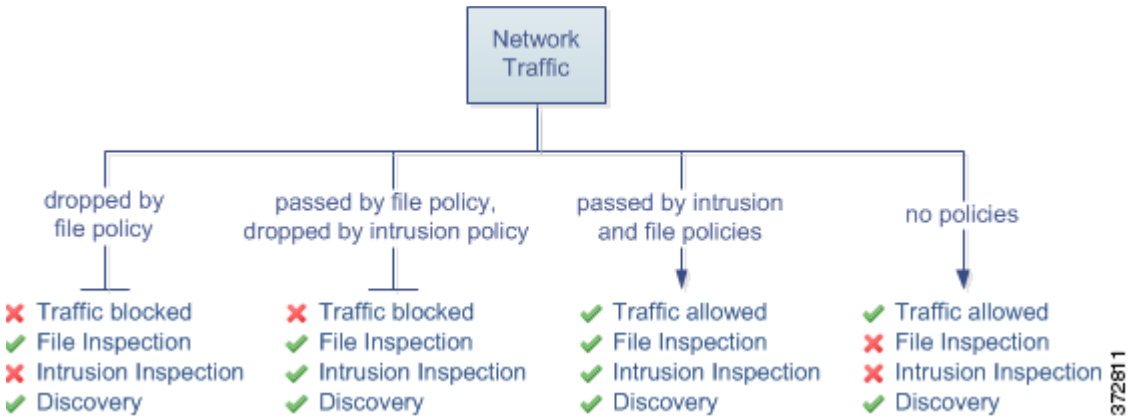
ファイル インスペクションは侵入ポリシー検査の前に行われます。つまり、ファイル ポリシーでブロックされたファイルに対して、システムは侵入の検査を行いません。ファイル ポリシー内では、タイプによる単純なブロックの方が、マルウェア インスペクションおよびブロックよりも優先されます。

たとえば、アクセス コントロール ルールで定義された特定のネットワーク トラフィックを正常に許可するシナリオを考えてください。ただし、予防措置として、実行可能ファイルのダウンロードをブロックし、ダウンロードされた PDF のマルウェア インスペクションを行って検出された場合はブロックし、トラフィックに対して侵入インスペクションを実行する必要があるとします。そこで、すべてのトラフィックに一致し、侵入ポリシーとファイル ポリシーの両方に関連付けられているルールを含む 1 つのアクセス コントロール ポリシーを作成します。ファイル ポリシーの中に、ダウンロードされた PDF を照合する、「ファイルのブロック」アクションを持つルールを含めます。さらに、ダウンロードされた実行可能ファイルを照合する、「マルウェアのブロック」アクションを持つ別のルールも含めます。このポリシーを適用した後は、次のようになります。

- まず、システムはファイル ポリシーで指定された単純なタイプ マッチングに基づいてすべての PDF ファイルのダウンロードをブロックします。これはすぐにブロックされるため、これらのファイルは、マルウェア ルックアップの対象にも侵入インスペクションの対象にもなりません。
- 次に、システムは、ネットワーク上のホストにダウンロードされた実行可能ファイルに対するマルウェア クラウド ルックアップを実行します。マルウェア ファイルの性質を持つ実行可能ファイルはすべてブロックされ、侵入インスペクションの対象にはなりません。
- 最後に、システムはアクセス コントロール ルールに関連付けられている侵入ポリシーを使用して、ファイル ポリシーでブロックされなかったファイルを含む残りのトラフィック全体を検査します。

以下の図は、「許可」アクセス コントロール ルール、またはユーザ によりバイパスされた「インタラクティブ ブロック」アクセス コントロール ルールのどちらかの条件を満たすトラフィックに対して実行されるインスペクションの種類を示しています。単純化のために、侵入/ファイル ポリシーの両方が 1 つのアクセス コントロール ルールに関連付けられている（またはどちらも関連付けられていない）状態でのトラフィック フローを図に示しています。ただし、どちらか 1 つだけを設定することも可能です。ファイル ポリシーがない場合、トラフィック フローは侵入ポリシーによって決定されます。侵入ポリシーがない場合、トラフィック フローはファイル ポリシーによって決定されます。

トラフィックが侵入/ファイル ポリシーによって検査またはドロップされるかどうかに関わらず、システムはネットワーク検出を使ってそれを検査できます（「ネットワーク検出の概要」（P.35-1）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 33-4　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、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。
ファイルのカテゴリとタイプ	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。 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。 **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。
ファイル ルール アクション	ファイル ルール アクションは、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します。 **(注)**　複数のファイル ルールは（数値順ではなく）ルール アクション順に評価されます。詳細については、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。

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* 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* 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まず判断し、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* 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* 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。

各ファイル 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スペロ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 33-5　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 用のスペロ分析をするか
ファイル ブロック	はい（推奨）	はい：一致するすべてのファイルを保存できます	いいえ	いいえ
マルウェア ブロック	はい（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	いいえ	はい：一致するすべてのファイルを保存できます	いいえ	いいえ
マルウェア クラウド ルックアップ	いいえ	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、およびブロッキング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、およびブロッキングの動作に関して、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** 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時点で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。
- FTP データ セッションと制御セッションからのトラフィックが同じ Snort にロードバランスされない場合、その FTP セッション内のファイルは、**ファイル ブロック** アクションや**マルウェア ブロック** アクションを持つファイル ルールでも、カスタム検出リストでもブロックされない可能性があります。セッションに対してファイル イベントが生成される必要があります。
- FTP に関する**マルウェア ブロック** 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、[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、[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** アクションおよび **マルウェア ブロック** 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）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。
- 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。
- Mac または Linux ベースのホストが、SMTP 経由で Mozilla Thunderbird を使ってテキスト ベースのファイルをアップロードしたり、IMAP または POP 経由でテキスト ベースのファイルをダウンロードしたりする場合、そのファイルがファイル ルールでキャプチャされると、キャプチャされたファイル サイズが実際のファイル サイズと異なる場合があります。Mac ベースのホストは CR 改行文字を使用し、Linux ベースのホストは LF 改行文字を使用します。Thunderbird は、テキスト ベース ファイル内の CR と LF を CRLF 改行文字に置き換えます。
- シスコでは、**ファイル ブロック** アクションと **マルウェア ブロック** アクションで**接続のリセット**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** アクションまたは **マルウェア ブロック** 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、防御センター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。

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」（P.33-14）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。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 33-6　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	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	ファイル ブロック	接続のリセット	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	マルウェア ブロック	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	マルウェア クラウド ルックアップ	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。
任意	任意	ファイル検出	なし	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。

防御センターでは、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。[Application Protocol]、[Direction of Transfer]、および [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 アクションやマルウェア クラウド ルックアップ 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防御センター データベースに自動的に記録します。

注　NetBIOS-ssn（SMB）トラフィックの検査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。クライアントまたはサーバがセッションを終了した後、システムは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、

- [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。
- [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。
- [File Monitor]：ファイル検出ルールおよびマルウェア クラウド ルックアップ 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
- [File Block]：ファイル ブロック ルールまたはマルウェア ブロック ルールの場合
- [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
- [File Resume Allow]：ファイル ブロック ルールまたはマルウェア ブロック ルールによってファイル伝送が最初に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。
- [File Resume Block]：ファイル検出ルールまたはマルウェア クラウド ルックアップ ルールによってファイル伝送が最初に許可された場合。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、[Action] が [Block] になります。

防御センターの 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。

注　さらに、組織の FireAMP サブスクリプションを使用して、防御センターでマルウェア 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、およびそれらのロギングの詳細については、以下を参照してください。

- 「接続、ファイル、マルウェアに関する情報のロギング」（P.14-39）
- 「ファイル イベントの操作」（P.34-8）
- 「マルウェア イベントの操作」（P.34-14）
- 「接続データについて」（P.16-2）

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。防御センター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 ペアの防御センターはファイル 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。継続的な運用を維持し、検出されるファイルのマルウェアの性質が両方の防御センターで必ず同じになるようにするには、プライマリとセカンダリの両方の防御センターからクラウドにアクセスできる必要があります。

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。

ファイル ポリシーの管理

[File Policies] ページ（Policies > 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、[Access Control] 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」（P.33-19）
- 「ファイル ルールの操作」（P.33-20）
- 「2 つのファイル ポリシーの比較」（P.33-23）

ファイル ポリシーの作成

ライセンス：Protection または Malware

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：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 アクションやマルウェア クラウド ルックアップ 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

ステップ 1　[Policies] > [Files] を選択します。

[File Policies] ページが表示されます。

ステップ 2　[New File Policy] をクリックします。

[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 [Access Control Policies] ページに移動できます（「アクセス コントロール ポリシーの管理」（P.13-31）を参照）。

ステップ 3　新しいポリシーの [Name] とオプションの [Description] を入力してから、[Save] をクリックします。

[File Policy Rules] タブが表示されます。

ステップ 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」（P.33-20）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 アクションやマルウェア クラウド ルックアップ 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。

ステップ 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の設定」（P.33-22）を参照してください。

ステップ 6　[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

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：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 [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 [Access Control Policies] ページに進むことができます。

ファイル ルールを作成する方法：

アクセス：Admin/Access Admin

ステップ 1　[Policies] > [Files] を選択します。

[File Policies] ページが表示されます。

ステップ 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、[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」（P.33-19）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。

ステップ 3　表示される [File Policy Rules] ページで、[Add File Rule] をクリックします。

[Add File Rule] ダイアログ ボックスが表示されます。

ステップ 4　[Application Protocol] を選択します。

デフォルトの [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。

ステップ 5　[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）

[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。

ステップ 6　ファイル ルールの [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。

[Block Files] または [Block Malware] を選択すると、接続のリセットを示す [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、[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」（P.33-14）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 アクションやマルウェア クラウド ルックアップ 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。

ステップ 7　[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。

- [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、[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、[Application Protocol] 、[Direction of Transfer] 、および [Action] での選択内容に応じて変化します。

たとえば、[Direction of Transfer] で [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、[Graphics] カテゴリから [GIF]、[PNG]、[JPEG]、[TIFF]、および [ICO] が削除されます。

ステップ 8　選択したファイル タイプを [Selected Files Categories and Types] リストに追加します。

- [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 [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 [All types in selected Categories] をクリックしてから、[Add] をクリックするか、選択項目を [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。

ステップ 9　[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の設定

ライセンス：Malware

サポート対象デバイス：機能に応じて異なる

サポート対象防御センター：機能に応じて異なる

表 33-7　ファイル ポリシーの詳細オプション

フィールド	説明	デフォルト値
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。	enabled
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。	enabled
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、[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（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。

高度なファイル ポリシー オプションを設定する方法：

アクセス：Admin/Access Admin

ステップ 1　[Policies] > [Files] を選択します。

[File Policies] ページが表示されます。

ステップ 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。

[File Policy Rule] ページが表示されます。

ステップ 3　[Advanced] タブを選択します。

[Advanced] タブが表示されます。

ステップ 4　「ファイル ポリシーの詳細オプション」の表に示すようにオプションを変更します。

ステップ 5　[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。

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かめたり、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 つのポリシー間の違いは次のように強調表示されます。

- 青は、強調表示されている設定項目が 2 つのポリシー間で異なっていることを示し、異なっている部分は赤のテキストで表示されます。
- グリーンは、強調表示されている設定項目が一方のポリシーに含まれ、もう一方のポリシーには含まれないことを示します。

[Previous] と [Next] をクリックすると、前後の相違箇所に移動できます。左右両側の間にある両方向矢印アイコン（ ）が移動し、[Difference] 番号が調整されて、どの相違箇所を表示しているか識別できるようになります。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

ステップ 1　[Policies] > [Files] を選択します。

[File Policies] ページが表示されます。

ステップ 2　[Compare Policies] をクリックします。

[Select Comparison] ダイアログ ボックスが表示されます。

ステップ 3　[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、[Running Configuration] または [Other Policy] を選択します。この 2 つのオプションの違いは、[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。
- 同じポリシーのバージョン間を比較するには、[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。

ステップ 4　選択した比較タイプに応じて、次の選択肢があります。

- 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 [Policy A] または [Target/Running Configuration A] のどちらかと、[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 [Policy] を選択してから、2 つのリビジョン [Revision A] と [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。

ステップ 5　[OK] をクリックします。

比較ビューが表示されます。

ステップ 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 [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、ポップアップ ウィンドウにレポートが表示されることがあります。あるいは、レポートをコンピュータに保存するよう求められることもあります。

FireAMP 用のクラウド接続の操作

ライセンス：任意

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、さらにクラウドが防御センターと通信します。クラウドに接続するよう防御センターを設定した後、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 イベントとして防御センター データベースに保存されます。詳細については、「マルウェア対策とファイル制御について」（P.33-3）を参照してください。

展開内のそれぞれの防御センターは、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 クラウドに接続します。防御センターで、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、防御センターはインターネットに直接アクセスできる必要があります。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、防御センター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 ペアのメンバ間では**共有されません**。継続的な運用を維持するには、プライマリとセカンダリの両方の防御センターをクラウドに接続してください。

クラウド接続の管理

防御センターの [FireAMP Management] ページ（[FireAMP] > [FireAMP 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、防御センター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」（P.33-25）
- 「クラウド接続の削除または無効化」（P.33-26）

シスコ クラウド接続の作成

ライセンス：任意

防御センターとシスコ 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防御センターを設定します。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。

出荷時の初期状態に復元された防御センター、またはクラウドへの登録中に取り消された防御センターを再登録するには、再び登録する前に FireAMP に接続し、防御センター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：Admin

ステップ 1　[FireAMP] > [AMP Management] を選択します。

[FireAMP Management] ページが表示されます。

ステップ 2　[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。

ステップ 3　[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 Cloud] を選択します。
- 米国クラウドの場合、[US Cloud] を選択します。

ステップ 4　[Register] をクリックします。

ステップ 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 [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 イベントを防御センターに送信することを承認します。

ステップ 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、防御センター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。

ステップ 7　[Allow] をクリックします。

防御センターの [FireAMP Management] ページに戻ります。接続が有効になり、防御センター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、[Deny] をクリックした場合にも防御センターに戻りますが、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、防御センターの 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**。あと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。

クラウド接続の削除または無効化

ライセンス：任意

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 クラウド接続を削除します。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（防御センターの 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、防御センター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。

防御センター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：Admin

ステップ 1　[FireAMP 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、クラウドは防御センター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。

防御センターを使用してクラウド接続を削除する方法：

アクセス：Admin

ステップ 1　[FireAMP Managemenet] 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、クラウドは防御センターへのイベントの送信を停止します。