CHAPTER 32

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、ASA FirePOWER モジュールのファイル制御、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。

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。

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 ASA FirePOWER モジュールで有効にする必要があります。

表 32-1　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	追加する必要のあるライセンス
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
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
高度なマルウェア防御（AMP）	マルウェアの伝送を検出、追跡し、任意でブロックします	マルウェア

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（32-1 ページ）
- ファイル ポリシーの概要と作成（32-4 ページ）

マルウェア防御とファイル制御について

ライセンス：Protection、マルウェア、またはすべて

*高度なマルウェア防御*機能を使用すると、ネットワークで伝送されるマルウェア ファイルを検出、追跡、分析、およびオプションでブロックするよう ASA FirePOWER モジュールを設定できます。

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。ASA FirePOWER モジュールは、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。ASA FirePOWER モジュールは該当するファイルを検出します。次に、ASA FirePOWER モジュールはファイルの SHA-256 ハッシュ値を使用して*マルウェア クラウド ルックアップ*を実行します。これらの結果に基づき、シスコ クラウドは ASA FirePOWER モジュールにファイルの性質を返します。

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。

ファイルを検査またはブロックするには、ASA FirePOWER モジュールで 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 リストへのファイルの追加を行うにはマルウェア ライセンスを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）：ASA FirePOWER モジュールがマルウェア 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（D-1 ページ）を参照してください。

ファイルの性質に基づき、ASA FirePOWER モジュールはファイルをブロックするか、またはファイルのアップロード/ダウンロードをブロックするよう、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、アプライアンスは 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 ASA FirePOWER モジュールに通知を送ります。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。性質には次の TTL 値が割り当てられます。

- クリーン（Clean）：4 時間
- 不明（Unknown）：1 時間
- マルウェア（Malware）：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、ASA FirePOWER モジュールはネットワーク 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。

マルウェア防御とファイル制御の設定

ライセンス：Protectionまたはマルウェア

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
- 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

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。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（32-4 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基づくイベントのロギング

ライセンス：Protectionまたはマルウェア

ASA FirePOWER モジュールは、システムのファイル インスペク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。

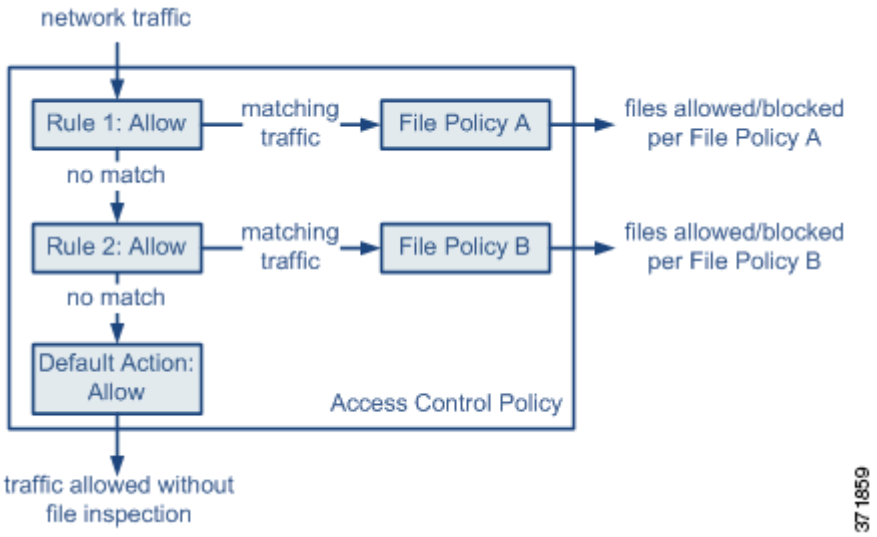
- *ファイル イベント*は、システムがネットワーク トラフィック内で検出した（およびオプションでブロックした）ファイルを表します。
- *マルウェア イベント*は、システムがネットワーク トラフィック内で検出した（およびオプションでブロックした）マルウェア ファイルを表します。
- *レトロスペクティブ マルウェア イベント*：性質がマルウェア ファイルから変更されたファイル。

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。

ファイル ポリシーの概要と作成

ライセンス：Protectionまたはマルウェア

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。



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
- 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

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（10-2 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 32-2　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 32-2　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	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。 **（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。

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（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、およびキャプチャされたファイルを ASA FirePOWER モジュールに保存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 32-3　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 ブロック（Block Files）	はい（推奨）
マルウェア ブロック（Block Malware）	はい（推奨）
ファイル検出（Detect Files）	いいえ
マルウェア クラウド ルックアップ（Malware Cloud Lookup）	いいえ

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 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。
- 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。
- 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、ASA FirePOWER モジュール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。

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（32-6 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。モジュール 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 32-4　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（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）	接続のリセット（Reset Connection）	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、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）		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ます。
任意	任意	ファイル検出（Detect Files）	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。

ASA FirePOWER モジュールでは、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。

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。

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。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。

ASA FirePOWER モジュール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SNMP 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。

インターネット アクセス

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。ASA FirePOWER モジュールでこのポート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

[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。

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ないことに注意してください。

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（32-10 ページ）
- ファイル ルールの操作（32-11 ページ）
- 2 つのファイル ポリシーの比較（32-14 ページ）

ファイル ポリシーの作成

ライセンス：Protectionまたはマルウェア

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。

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：

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [ファイル（Files）] の順に選択します。

[ファイル ポリシー（File Policies）] ページが表示されます。

ステップ 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モジュール 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 ポリシーの数がモジュール 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 ポリシーの開始（4-1 ページ）を参照）。

ステップ 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。

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(32-11 ページ)を参照してください。

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([一般(General)])の設定(32-13 ページ)を参照してください。

ステップ 6　[ASA FirePOWER 変更の保存(Store ASA FirePOWER Changes)] 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またはマルウェア

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。

ファイル ルールを作成する方法:

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [ファイル(Files)] の順に選択します。

[ファイル ポリシー(File Policies)] ページが表示されます。

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、[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(32-10 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。

ステップ 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。

ステップ 4　ドロップダウンリストから、[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。

ステップ 5　ドロップダウンリストから [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。

ステップ 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、[接続のリセット（Reset Connection）] チェックボックスをクリアします。

（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（32-6 ページ）を参照してください。

ステップ 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。

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。

ステップ 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。

ステップ 9　[ASA FirePOWER 変更の保存（Store ASA FirePOWER Changes）] 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：マルウェア

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。

表 32-5　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
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）

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。

ステップ 1　[設定（Configuration）] > [ASA FirePOWER 設定（ASA FirePOWER Configuration）] > [ポリシー（Policies）] > [ファイル（Files）] の順に選択します。

[ファイル ポリシー（File Policies）] ページが表示されます。

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。

[ファイル ポリシー ルール（File Policy Rules）] ページが表示されます。

ステップ 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。

ステップ 4　ファイル ポリシーの詳細オプション（[一般（General）]）の表に示されているようにオプションを変更します。

ステップ 5　[ASA FirePOWER 変更の保存（Store ASA FirePOWER Changes）] 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:

ステップ 1　[設定(Configuration)] > [ASA FirePOWER 設定(ASA FirePOWER Configuration)] > [ポリシー(Policies)] > [ファイル(Files)] の順に選択します。

[ファイル ポリシー(File Policies)] ページが表示されます。

ステップ 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。

ステップ 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。

ステップ 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。

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。

オプションで、[比較レポート(Comparison Report)] をクリックして、ファイル ポリシー比較レポートを生成します。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ます。