



ファイルポリシーと AMP for Firepower

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

- [ファイルポリシーと AMP for Firepower について, 1 ページ](#)
- [ファイル制御および Cisco AMP の基本, 2 ページ](#)
- [ファイルポリシー, 9 ページ](#)
- [ファイルルール, 16 ページ](#)
- [クラウド接続, 23 ページ](#)
- [集合型セキュリティインテリジェンス通信の設定, 32 ページ](#)

ファイルポリシーと AMP for Firepower について

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しやすくするため、Firepower システムの *Advanced Malware Protection for Firepower* (AMP for Firepower) の機能によって、ネットワークトラフィックでのマルウェアの伝送を検出、追跡、保存、分析、および必要に応じてブロックできます。

AMP for Firepower およびファイル制御（ファイルにマルウェアが含まれている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制御できる）をアクセス制御設定全体の一部として設定します。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、ローカルマルウェア分析を実行して、ファイルにマルウェアが含まれているかどうかを判断できます。また、ファイルを動的分析のために AMP Threat Grid クラウドに送信して、そのファイルがマルウェアを表しているかどうかを判断できます。

アクティブファイルポリシーのファイルイベント、マルウェアイベント、および取得されたファイルロギングが自動的に有効になります。また、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、システムは関連する接続の終了を Firepower Management 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。

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 トrajjectory (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。



ヒント 組織で AMP for Endpoints を使用している場合は、システムで、AMP for Firepower によって収集されたデータとともにエンドポイントベースのデータをインポートして表示できます。このデータのインポートには、ライセンスは必要ありません。

組織で追加のセキュリティが必要であるか、外部接続を制限する場合は、Cisco AMP プライベートクラウド仮想アプライアンス (AMPv) を使用します。AMPv は個別に AMP for Endpoints イベントを収集し、Firepower Management Center に転送します。

ファイル制御および Cisco AMP の基本

AMP for Firepower

AMP for Firepower では、インライン展開された管理対象デバイスを使用して、ネットワーク上のマルウェアを検出、保存、トラッキング、分析、およびブロックできます。AMP for Firepower は、PDF、Microsoft Office ドキュメントを含め、多くのタイプのマルウェア ファイルをブロックできます。

ファイルの検出と保存

AMP for Firepower により、管理対象デバイスは、特定のファイルタイプの送信のネットワークトラフィックをモニタします。

デバイスが対象のファイルを検出すると、ファイルの SHA-256 ハッシュ値を Firepower Management Center に送信します。Firepower Management Center は、マルウェア クラウドルックアップを実行し、AMP クラウドでファイルの性質をクエリします。デバイスは、ファイルストレージ機能を使用して、ハードドライブまたはマルウェアのストレージパックに対象ファイルを保存できます。イベントビューアのキャプチャファイル情報を表示したり、オフライン分析のためにコピーをダウンロードしたりできます。

ファイル分析

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



- (注) 設定に応じて、システムがファイルを初めて検出したときに、そのファイルを検査してクラウドルックアップの結果を待機するか、または、クラウドルックアップの結果を待機せずにファイルを通過させることができます。

ファイルルールでオプションを有効にするかどうかに基づいて、システムは次の順序でファイルを検査します。

Spero 分析

ファイルが対象の実行可能ファイルの場合、デバイスはファイル構造を分析し、結果として得られた Spero シグネチャを AMP Threat Grid クラウドに送信できます。クラウドは、このシグネチャを使用して、ファイルにマルウェアが含まれるかを判断します。

ローカル マルウェア分析

ローカル マルウェア インспекション エンジンを使用して、デバイスは対象ファイルを調べ、ファイルにマルウェアが含まれる場合、ファイルルールでそのように設定されていればこのファイルをブロックし、マルウェア イベントを生成します。

また、デバイスにより、ファイルプロパティ、組み込みオブジェクト、および可能性のあるマルウェアの詳細情報を含むファイル構成レポートが生成されます。

動的分析

デバイスが、マルウェアの可能性があるととしてファイルを事前分類している場合、デバイスがファイルを保存するかどうかに関係なく、これらのファイルを AMP Threat Grid クラウドまたは AMP Threat Grid オンプレミス アプライアンスに動的分析のために送信します。

AMP Threat Grid クラウドまたはオンプレミスの AMP Threat Grid アプライアンスは、悪意のあるファイルかどうかを判断するためにサンドボックス環境でファイルを実行し、ファイルにマルウェアが含まれる可能性を示す脅威スコアを返します。脅威スコアから、クラウドが脅威スコアを割り当てた理由を詳細に説明する動的分析のサマリー レポートを表示できます。

ファイルとマルウェア イベント、およびキャプチャ ファイル

ファイル分析結果に基づいて、イベントビューアからのキャプチャ ファイル、生成されたマルウェアとファイルイベントを確認できます。使用可能な場合は、ファイルの構成、性質、脅威スコア、動的分析のサマリー レポートを調べ、マルウェア分析をさらに詳細に把握できます。また、ファイルがネットワークをどのように通過するか（ホストを通過するか）を示すマップ、およびさまざまなファイルプロパティを表示する、ネットワーク ファイル トラジェクトリにアクセスできます。

アーカイブ ファイル

システムは、ファイルがアーカイブ（.rar または .zip アーカイブ ファイルなど）の場合、一番外側のアーカイブ ファイル（レベル 0）の下の最大 3 レベルのネストされたファイルを検査できます。ブロックアクションを含むファイルルールにいずれかの個別ファイルが一致する場合は、

その個別ファイルだけでなくアーカイブ全体がブロックされます。また、指定したネストのレベルを超えるアーカイブ、またはそのコンテンツが暗号化されているか検査できないアーカイブも、ブロックされることがあります。

ファイルトラッキング

AMPクラウドにあるファイルの性質が不正確だとわかっている場合、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。

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

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



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

関連トピック

[ファイルリスト](#)

マルウェアの性質

システムは、AMP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。パフォーマンスを改善するために、SHA-256 値に基づいてファイルの性質がシステムですでにわかっている場合、Firepower Management Centerは AMPクラウドでクエリを行う代わりに、キャッシュ済みの性質を使用します。システムは、ファイルの性質に基づいてファイルをブロックすることもできます。アーカイブファイル内にネストされているファイルが1つでもブロックされる場合、システムはアーカイブファイル全体をブロックします。

ファイルリストへの追加操作の結果、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) : ファイルが AMPクラウドでマルウェアと分類されていること、ローカルマルウェア分析でマルウェアとして識別されたこと、またはファイルの脅威スコアがファイルポリシーに定義されたマルウェアのしきい値を超えたこと示します。
- [クリーン (Clean)] : AMP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) : システムはAMPクラウドでファイルの性質をクエリしましたが、ファイルには性質が割り当てられていませんでした。言い換えると、AMPクラウドがファイルを分類できませんでした。
- 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。
- 利用不可 (Unavailable) : システムがAMPクラウドでクエリを行え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。

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

表 1: 内容に基づくアーカイブファイルの性質

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

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



ヒント

短時間で利用不可 (Unavailable) マルウェア イベントが連続して発生した場合は、Firepower Management Center が AMP クラウドに接続できることを確認してください。

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

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

- クリーン : 4 時間

- 不明：1 時間
- マルウェア：1 時間

このキャッシュに対するクエリで、キャッシュされた性質がタイムアウトになったことが識別された場合、システムは AMP クラウドに新しい性質を再びクエリします。

AMP for Firepower を使用しないファイル制御

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。AMP for Firepower 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 AMP for Firepower とは異なり、AMP 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。

エンドポイント向け AMP

エンドポイント向け AMP は、シスコのエンタープライズクラスの高度なマルウェア防御ソリューションです。高度なマルウェアの発生、高度で継続的な脅威、およびターゲット型攻撃を検出、分析、ブロックします。次の図に、エンドポイント向け AMP を使用した場合の一般的な情報フローを示します。



所属部門がエンドポイント向け AMP を使用している場合、個々のユーザはエンドポイント（つまり、コンピュータやモバイルデバイス）に軽量コネクタをインストールします。コネクタは、ファイルのアップロード、ダウンロード、実行、開く、コピー、移動などの操作を行う際にファイルを検査します。コネクタは AMP クラウドと通信して、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します。

ファイルがマルウェアとして特定された場合、AMP クラウドは特定した脅威の情報を Firepower Management Center に送ります。さらに AMP 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 Firepower Management Center に送信することもできます。Firepower Management 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。

エンドポイント向け AMP は、ホストのセキュリティに感染の疑いがある場合、侵害の兆候 (IOC) を生成することができます。Firepower システムでは、モニタ対象ホストの IOC 情報が表示できます。シスコでは折にふれて、エンドポイントベースのマルウェア イベントに対応する新しい IOC タイプの開発を行っており、システムにより自動的にダウンロードされます。

エンドポイント向け AMP では、マルウェア イベントに基づいて Management Center で開始される修復やアラートを設定できるだけでなく、エンドポイント向け AMP 管理コンソールを使ってマルウェアの影響を軽減することもできます。管理コンソールの堅牢かつ柔軟な Web インターフェイスを使用すると、エンドポイント向け AMP 展開のあらゆる側面を制御し、アウトブレイクのすべての段階を管理できます。次の操作を実行できます。

- 部門全体のためにカスタムマルウェア検出ポリシーとプロファイルを設定し、すべてのユーザのファイルに対してフラッシュ スキャンおよび完全スキャンを実行する
- マルウェア分析の実行：ヒートマップ、詳細なファイル情報、ネットワーク ファイル トラジェクトリ、脅威の根本原因の表示など
- アウトブレイクコントロールのさまざまな要素を設定する：自動検疫、検疫されていない実行可能ファイルの実行を停止するアプリケーションブロッキング、除外リストなど
- カスタム保護の作成、グループポリシーに基づく特定のアプリケーションの実行ブロッキング、およびカスタム ホワイトリストの作成



ヒント エンドポイント向け AMP の詳細については『AMP for Endpoints management console』を参照してください。

AMP for Firepower とエンドポイント向け AMP の比較

Firepower システムは、AMP for Firepower およびエンドポイント向け AMP のどちらのデータも使用できます。

管理対象デバイスはネットワーク トラフィックのマルウェアを検出しますが、エンドポイント向け AMP 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ため、この 2 種類のマルウェア イベントの情報は異なります。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。

別の例としては、ネットワークベースのマルウェア イベントの場合、ユーザ情報は、ネットワーク検出で判別された、マルウェアの送信先であるホストに最後にログインしたユーザを示すこと

が挙げられます。一方、エンドポイント向け AMP で報告されるユーザは、マルウェアが検出されたエンドポイントに現在ログインしているユーザを示します。



(注) 展開によっては、AMP for Endpoints がモニタするエンドポイントは、AMP for Firepower がモニタしているものと同じホストではない場合があります。このため、エンドポイントベースのマルウェア イベントは、ネットワーク マップにホストを追加しません。ただし、システムは IP アドレスおよび MAC アドレスのデータを使用して、AMP for Endpoints の展開から取得した侵害の兆候をモニタ対象のホストにタグ付けします。異なる AMP ソリューションによってモニタされる2つの異なるホストが同じ IP アドレスと MAC アドレスを持っている場合、システムは AMP for Endpoints の IOC をモニタ対象のホストに誤ってタグ付けする場合があります。

次の表に、2つの戦略の違いをまとめます。

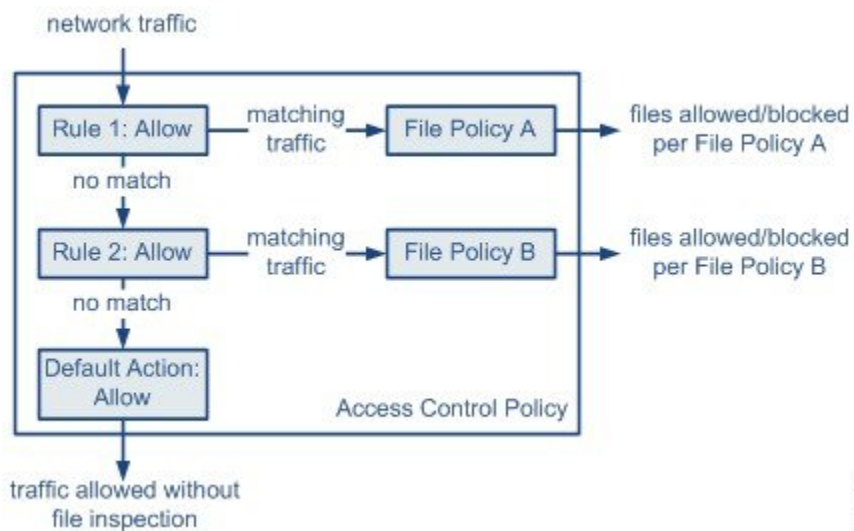
表 2: ネットワークベースとエンドポイントベースの高度なマルウェア防御戦略の比較

機能	AMP for Firepower	エンドポイント向け AMP
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 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、AMP クラウドとの通信を行うコネクタを使用
ネットワーク トラフィックを検査	管理対象デバイスを通るトラフィック	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	Management Center ベース、および AMP クラウドでの分析	Management Center ベース、およびエンドポイント向け AMP 管理コンソールの追加オプション
マルウェアの影響軽減	ネットワーク トラフィックでのマルウェア ブロックング、Management Center が開始する修復	エンドポイント向け AMP ベースの検疫およびアウトブレイク コントロール オプション、Management Center が開始する修復
生成されるイベント	ファイル イベント、キャプチャされたファイル、マルウェア イベント、およびレトロスペクティブ マルウェア イベント	マルウェア イベント
マルウェア イベントに含まれる情報	基本的なマルウェア イベント情報、および接続データ (IP アドレス、ポート、アプリケーションプロトコル)	詳細なマルウェア イベント情報 (接続データなし)

機能	AMP for Firepower	エンドポイント向け AMP
ネットワーク ファイル トラジェクトリ	Management Center ベース	Management Center ベース、およびエンドポイント向け AMP 管理コンソールの追加オプション
必要なライセンスまたはサブスクリプション	ファイル制御および AMP for Firepower の実行に必要なライセンス	エンドポイント向け AMP サブスクリプション (ライセンスベースではありません)

ファイルポリシー

ファイルポリシーは、いくつかの設定からなるセットです。システムは全体的なアクセス制御設定の一部としてこれを使用して、AMP for Firepower とファイル制御を実行できます。この関連付けにより、アクセスコントロールルールの条件と一致するトラフィック内のファイルを通過させる前に、システムは必ずファイルを検査するようになります。次の図のような、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。

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。

ファイルポリシーの詳細設定

詳細なファイルインスペクションの設定に関する注意事項

ファイルポリシーでは、詳細なオプションを設定して、カスタム検出リストのファイルのブロック、クリーンリストのファイルの許可、およびファイルがマルウェアと見なされる脅威スコアのしきい値の設定を行うことができます。

また、組織のニーズに合わせてアーカイブファイルを検査し、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に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。

アーカイブファイルのインスペクションに関する注意事項

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。



- (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)。

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。

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

ファイルポリシー設定に関する注意事項と制約事項

- 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せん。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。
- 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。

ファイルポリシーの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
Threat (ファイル制御) マルウェア (AMP for Firepower)	Protection (ファイル制御) マルウェア (AMP for Firepower)	任意 (Any)	任意 (Any)	Admin/Access Admin

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

マルチドメイン展開では、編集できる現在のドメインで作成されたポリシーが表示されます。また、編集できない先祖ドメインで作成されたポリシーも表示されます。下位のドメインで作成されたポリシーを表示および編集するには、そのドメインに切り替えます。






(注)

動的分析の対象に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 AMP クラウドをチェックします (多くても 1 日に 1 回)。対象になるファイルタイプのリストが変更された場合、これはファイルポリシーの変更を意味します。このファイルポリシーを使用するアクセスコントロールポリシーがいずれかのデバイスに展開されている場合、そのアクセスコントロールポリシーには失効マークが付けられます。更新したファイルポリシーがデバイスで有効になるには、まず、ポリシーを展開しておく必要があります。

手順

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

ステップ 2 ファイルポリシーを管理します。

- [比較 (Compare)] : [ポリシーの比較 (Compare Policies)] をクリックします ([ポリシーの比較](#) を参照)。
- 作成 : ファイルポリシーを作成するには、[新規ファイルポリシー (New File Policy)] をクリックし、[ファイルポリシーの作成](#), (13 ページ) で説明する手順を実行します。
- コピー : ファイルポリシーをコピーするには、コピーアイコン () をクリックします。
代わりに表示アイコン () が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- 削除 : ファイルポリシーを削除するには、削除アイコン () をクリックし、プロンプトが表示されたら [はい (Yes)] と [OK] をクリックします。

コントロールが淡色表示されている場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。

- 展開：[展開 (Deploy)] をクリックします (設定変更の導入を参照)。
- 編集：既存のファイルポリシーを変更するには、編集アイコン (✎) をクリックします。
- [レポート (Report)]：レポートアイコン (📄) をクリックします (現在のポリシーレポートの生成を参照)。

ファイルポリシーの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
Threat (ファイル制御) マルウェア (AMP for Firepower)	Protection (ファイル制御) マルウェア (AMP for Firepower)	任意 (Any)	任意 (Any)	Admin/Access Admin

手順

- ステップ 1** [ポリシー (Policies)] > [アクセスコントロール (Access Control)] > [マルウェアとファイル (Malware & File)] を選択します。
- 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。
- 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。
- 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)] を入力します。
- ステップ 4** [保存 (Save)] をクリックします。
- ステップ 5** [ファイルルールの作成](#), (21 ページ) の説明に従って、ファイルポリシーに 1 つ以上のルールを追加します。
- ステップ 6** 必要に応じて、[詳細 (Advanced)] タブを選択し、[詳細オプションおよびアーカイブファイル検査オプション](#), (14 ページ) の説明に従って詳細オプションを設定します。
- ステップ 7** ファイルポリシーを保存します。

次の作業

- [ファイル制御およびマルウェア保護のためのアクセスコントロールルール](#)の設定の説明に従って、アクセスコントロールルールにファイルポリシーを追加します。
- 設定変更を展開します。[設定変更の導入](#)を参照してください。

詳細オプションおよびアーカイブファイル検査オプション

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

- [初回ファイル分析 (First Time File Analysis)] : システムで初めて検出するファイル分析のためのファイルを送信します。ファイルは、マルウェアクラウドルックアップと Spero 分析、ローカルマルウェア分析、またはダイナミック分析を実行するように設定されているルールに一致する必要があります。このオプションを無効にすると、初めて検出されたファイルの性質が「不明 (Unknown)」になります。
- [カスタム検出リストを有効にする (Enable Custom Detection List)] : カスタム検出リストにあるファイルをブロックします。
- [クリーンリストを有効にする (Enable Clean List)] : クリーンリストにあるファイルを許可します。
- [ダイナミック分析の脅威スコアに基づいてマルウェアとしてファイルをマークする (Mark files as malware based on dynamic analysis threat score)] : しきい値の脅威スコアを設定します。スコアがしきい値以上のファイルはマルウェアと見なされます。

しきい値に低い値を選択すると、マルウェアとして扱われるファイルの数が増えます。ファイルポリシーで選択したアクションによっては、その結果、ブロックされるファイルの数が増える可能性があります。

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

- [アーカイブを検査する (Inspect Archives)] : アーカイブファイルの内容を検査します。



注意 [アーカイブを検査する (Inspect Archives)] を有効化または無効化すると設定の変更を展開すると Snort プロセスが再起動され、一時的にトラフィックのインスペクションが中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、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® の再起動によるトラフィックの動作](#)を参照してください。

- [暗号化されているアーカイブをブロックする (Block Encrypted Archives)] : 暗号化されている内容を含むアーカイブファイルをブロックします。

- [検査できないアーカイブをブロックする (Block Uninspectable Archives)] : 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します。これは、通常、破損したファイル、または指定されているアーカイブの最大の深さを超えるファイルに適用されます。
- [アーカイブの最大の深さ (Max Archive Depth)] : 指定されている深さを超えてネストされているアーカイブをブロックします。最上位のアーカイブファイルはこの数に含まれず、深さは最初のネストファイルを 1 として始まります。

関連トピック

[Snort® の再起動シナリオ](#)

ファイルポリシーの編集

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
Threat (ファイル制御) マルウェア (AMP for Firepower)	Protection (ファイル制御) マルウェア (AMP for Firepower)	任意 (Any)	任意 (Any)	Admin/Access Admin

手順

- ステップ 1** [ポリシー (Policies)] > [アクセス コントロール (Access Control)] > [マルウェアとファイル (Malware & File)] を選択します。
- ステップ 2** 編集するファイルポリシーの横にある編集アイコン (✎) をクリックします。代わりに表示アイコン (🔍) が表示される場合、設定は先祖ドメインに属しており、設定を変更する権限がありません。
- ステップ 3** 次の選択肢があります。
 - [ファイルルールの追加 (Add File Rule)] を選択して、ファイルルールを追加します。詳細については、[ファイルルール, \(16 ページ\)](#) を参照してください。
 - 既存のファイルルールの横にある編集アイコン (✎) をクリックします。
 - [詳細オプションおよびアーカイブ ファイル検査オプション, \(14 ページ\)](#) の説明に従って詳細オプションを設定します。

- (注) ファイルポリシーエディタに、現在編集集中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表示されます。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。

次の作業

- 設定変更を展開します。[設定変更の導入](#)を参照してください。

ファイルルール

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

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
- 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
- ローカルマルウェア分析、Spero 分析、または動的分析のために、キャプチャしたファイルを送信する。

さらに、ファイルポリシーによって以下を実行できます。

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

ファイルルールのコンポーネント

表 3: ファイルルールのコンポーネント

ファイルルールのコンポーネント	説明
アプリケーションプロトコル	<p>システムは、FTP、HTTP、SMTP、IMAP、POP3、および NetBIOS-ssn (SMB) を介して伝送されるファイルを検出し、検査できます。デフォルトの [任意 (Any)] は、HTTP、SMTP、IMAP、POP3、FTP、および NetBIOS-ssn (SMB) トラフィック内のファイルを検出します。パフォーマンスを向上させるには、ファイルルールごとに、これらのアプリケーションプロトコルのうち 1 つだけでファイルを検出するよう限定できます。</p>
転送の方向	<p>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。</p> <p>ヒント [任意 (Any)] を使用すると、ユーザが送信しているか受信しているかには関係なく、多数のアプリケーションプロトコルを介したファイルが検出されます。</p>
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、ShockWaveFlash (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) 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>選択したアクションに応じて、システムでファイルを保存するか、ファイルに対して Spero 分析、ローカルマルウェア分析、または動的分析を実行するかを設定できます。[ブロック (Block)] アクションを選択すると、システムでブロックされた接続をリセットするかどうかを設定できます。</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。</p>

ファイルルールアクションと評価順序

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。ファイルルールを使用すると、ロギング、ブロック、またはマルウェアスキャンの対象となるファイルタイプを詳細に制御できます。

各ファイルルールには、ルールの条件に一致するトラフィックがシステムによってどのように処理されるかを決定する1つのアクションが関連付けられます。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。（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。

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

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

ファイルルールアクションに応じて、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、管理対象デバイスに取得したファイルを保存するオプション、ファイルでマルウェアをローカルで分析するオプション、取得したファイルを動的分析および Spero 分析のために AMP

クラウドに送信するオプション、および後で送信するためにクラウドに現在送信できないファイルを保存するオプションを設定できます。

表 4: ファイルルールアクション

ファイルルールアクションのオプション	ファイルのブロックが可能か	マルウェアのブロックが可能か	ファイルの検出が可能か	マルウェアクラウドロックアップが可能か
MSEXE 用の Spero 分析 (Spero Analysis for MSEXE)	No	はい: 実行可能 ファイルを送信できます	No	はい: 実行可能 ファイルを送信できます
動的分析 (Dynamic Analysis)	No	はい: 不明なファイルの性質の実行可能ファイルを送信できます	No	はい: 不明なファイルの性質の実行可能ファイルを送信できます
容量処理 (Capacity Handling)	No	Yes	No	Yes
ローカルマルウェア分析 (Local Malware Analysis)	No	Yes	No	Yes
接続のリセット (Reset Connection)	はい (推奨)	はい (推奨)	No	No
ファイルの保存 (Store files)	はい: 一致するすべてのファイルを保存できます	はい: 選択したファイルの性質に一致するファイルタイプを保存できます	はい: 一致するすべてのファイルを保存できます	はい: 選択したファイルの性質に一致するファイルタイプを保存できます

ファイルポリシーの注意事項と制約事項

ファイルルール設定に関する注意事項と制約事項

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

ファイル検出に関する注意事項と制約事項

- ファイルがアプリケーションプロトコル条件を持つルールに一致する場合、ファイルイベントの生成は、システムがファイルのアプリケーションプロトコルを正常に識別した後に行われます。識別されていないファイルは、ファイルイベントを生成しません。
- FTP は、さまざまなチャン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内部リソースに負荷分散されない場合があります。
- POP3、POP、SMTP、または IMAP セッションでのすべてのファイル名の合計バイト数が 1024 を超えると、セッションのファイルイベントでは、ファイル名バッファがいっぱいになった後で検出されたファイルの名前が正しく反映されないことがあります。
- SMTP 経由でテキストベースのファイルを送信すると、一部のメールクライアントは改行を CRLF 改行文字標準に変換します。MAC ベースのホストはキャリッジリターン (CR) 文字を使用し、UNIX/Linux ベースのホストはラインフィード (LF) 文字を使用するので、メールクライアントによる改行変換によってファイルのサイズが変更される場合があります。一

部のメールクライアントは、認識できないファイルタイプを処理する際に改行変換を行うようデフォルト設定されていることに注意してください。

ファイルブロックに関する注意事項と制約事項

- 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。
- [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展開前に開始された、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。

ファイルルールの作成

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
Threat (ファイル制御)	Protection (ファイル制御)	任意 (Any)	任意 (Any)	Admin/Access Admin
Malware (AMP for Firepower)	Malware (AMP for Firepower)			

**注意**

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

手順

- ステップ 1** ファイルポリシーエディタで、[ファイルルールの追加 (Add File Rule)] をクリックします。
- ステップ 2** [ファイルルールのコンポーネント](#), (17 ページ) の説明に従って、[アプリケーションプロトコル (Application Protocol)] および [転送の宛先 (Direction of Transfer)] を選択します。
- ステップ 3** [ファイルタイプ (File Types)] を 1 つ以上選択します。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。
- 1 つ以上の [ファイルタイプカテゴリ (File Type Categories)] を選択し、[選択したカテゴリのすべてのタイプ (All types in selected Categories)] をクリックします。
 - 名前または説明でファイルタイプを検索します。たとえば、Microsoft Windows 固有のファイルのリストを表示するには、[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。
- ステップ 4** [ファイルルールアクションと評価順序](#), (18 ページ) の説明に従って、ファイルルールの [アクション (Action)] を選択します。
- ステップ 5** 選択したアクションに応じて、以下を実行するかどうかを設定します。
- ファイルのブロック後に接続をリセットする
 - 一致するファイルを保存する
 - Spero 分析を有効にする
 - ローカルマルウェア分析を有効にする
 - ダイナミック分析およびキャパシティの処理を有効にする

ファイルルールアクションと評価順序, (18 ページ) の説明を参照してください。

ステップ 6 [追加 (Add)] をクリックします。

ステップ 7 [保存 (Save)] をクリックしてポリシーを保存します。

次の作業

- 設定変更を展開します。設定変更の導入を参照してください。

関連トピック

[Snort® の再起動シナリオ](#)

クラウド接続

Firepower システムでは Cisco Advanced Malware Protection (AMP) を実施するため、次のパブリッククラウドベースのサーバへの接続を行います。

- AMP クラウド : AMP for Firepower のマルウェア判定結果と更新、エンドポイント向け AMP のスキャンレコード、マルウェア検出、検疫、侵害の兆候 (IOC) を取得できます。
- AMP Threat Grid クラウド : AMP for Firepower ダイナミック分析に利用可能なファイルの送信、脅威スコアやダイナミック分析レポートの取得ができます。

部門のプライバシー、セキュリティ保護のニーズに応じて、プライベートクラウドサーバを導入することもできます。

- AMP プライベートクラウド仮想アプライアンス (AMPv) は、圧縮型、オンプレミス AMP クラウドとして機能します。
- AMP Threat Grid アプライアンスはパブリック AMP Threat Grid クラウドとは連絡しないオンプレミス AMP Threat Grid クラウドとして機能します。

AMP クラウド接続

高度なマルウェア防御 (AMP) クラウドは、ビッグデータ分析や連続分析によりネットワーク上のマルウェアを検出およびブロックするシスコホステッドサーバです。次の 2 つのシスコ AMP ソリューションはどちらも AMP クラウドを使用します。

- AMP for Firepower は、管理対象デバイスがネットワークトラフィックから検出した潜在的なマルウェアの性質を取得し、ローカルマルウェア分析とファイルの事前分類の更新を取得するために AMP クラウドを使用します。
- エンドポイント向け AMP は、シスコのエンタープライズクラスの AMP ソリューションです。ユーザはそれぞれ、AMP クラウドと通信するコンピュータやモバイルデバイスに軽量

コネクタをインストールします。次に Firepower Management Center がスキャン、マルウェア検出、隔離、および侵害の兆候 (IOC) のレコードをインポートします。

展開によっては、AMP for Endpoints がモニタするエンドポイントは、AMP for Firepower がモニタしているものと同じホストではない場合があります。このため、エンドポイントベースのマルウェアイベントは、ネットワーク マップにホストを追加しません。ただし、システムは IP アドレスおよび MAC アドレスのデータを使用して、AMP for Endpoints の展開から取得した侵害の兆候をモニタ対象のホストにタグ付けします。異なる AMP ソリューションによってモニタされる2つの異なるホストが同じ IP アドレスと MAC アドレスを持っている場合、システムは AMP for Endpoints の IOC をモニタ対象のホストに誤ってタグ付けする場合があります。

[AMP 管理 (AMP Management)] ページ ([AMP] > [AMP 管理 (AMP Management)]) で AMP クラウドとの接続を管理します。AMP for Firepower では、デフォルトで米国 (US) AMP パブリッククラウドへの接続が設定され、有効になっています。AMP for Firepower クラウド接続の削除や無効化はできませんが、欧州連合 (EU) および米国 (US) AMP クラウドの切り替え、またはプライベートクラウド (AMPv) の接続の設定が可能です。

エンドポイントに独自の FireAMP 接続を追加するには、FireAMP ポータルのアカウントが必要です。ポータルに登録されていないエンドポイント向け AMP 接続では、AMP for Firepower は無効になりません。

AMP クラウド接続要件

- AMP for Networks : パブリックまたはプライベートいずれの AMP クラウドを使用しているも、ポート 443 を使って AMP for Networks のマルウェアクラウドルックアップを行います。Firepower Management Center からの通信を行うため、このポートをアウトバウンドに開く必要があります。
- エンドポイント向け AMP : 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。Firepower Management Center との通信を行うため、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、Firepower Management Center はインターネットに直接アクセスする必要があります。デフォルトの正常性ポリシーに含まれる AMP ステータス モニタは、Firepower Management 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 AMP ポータルを使って接続が登録解除された場合に警告を出します。

AMP の通信にレガシー ポートを使用するには [集合型セキュリティ インテリジェンスの通信設定オプション](#)、(32 ページ) を参照してください。

AMP クラウド接続とマルチテナンシー

マルチドメイン導入環境では、AMP for Firepower 接続はグローバル レベルでのみ設定します。各 Firepower Management Center で可能な AMP for Firepower 接続数は 1 接続のみです。エンドポイント向け AMP 接続は、どのドメイン レベルでも設定可能です。ただし、各接続にそれぞれ個別のエンドポイント向け AMP アカウントを使用する必要があります。たとえば、MSSP の各クライアントは、それぞれ独自のエンドポイント向け AMP を展開している場合があります。



注意

特にリーフドメインに重複する IP スペースがある場合、エンドポイント向け AMP 接続はリーフレベルのみで設定することを強く推奨します。複数のサブドメインに同じ IP-MAC アドレスペアを持つホストが存在する場合、誤ったリーフドメインにエンドポイントベースのマルウェアイベントを保存したり、誤ったホストに IOC を関連付けたりする可能性があります。

AMP for Endpoints クラウド接続の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin

組織で AMP for Endpoints が展開されると、脅威の識別、侵害の兆候 (IOC)、およびその他のマルウェア関連の情報を AMP クラウドからシステムにインポートできます。AMP for Firepower 接続がすでに設定されている場合にも、AMP for Endpoints 接続を設定する必要があります。



注意

マルチドメイン展開では、特にリーフドメインに重複する IP スペースがある場合は、AMP for Endpoints 接続をリーフレベルのみで設定することを強くお勧めします。複数のサブドメインに同じ IP-MAC アドレスペアを持つホストがある場合、システムが誤ったリーフドメインにエンドポイントベースのマルウェアイベントを保存したり、誤ったホストに IOC を関連付けたりする可能性があります。

はじめる前に

- Firepower Management Center を工場出荷時の初期状態に復元した後、または以前のバージョンに戻した後 AMP クラウドに接続している場合は、AMP for Endpoints 管理コンソールを使用して以前の接続を削除します。

手順

- ステップ 1 [AMP] > [AMP 管理 (AMP Management)] を選択します。
- ステップ 2 [AMP クラウド接続の作成 (Create AMP Cloud Connection)] をクリックします。
- ステップ 3 [クラウド名 (Cloud Name)] ドロップダウンリストから、使用するクラウドを選択します。
 - 欧州連合 AMP クラウドの場合、[EU クラウド (EU Cloud)] を選択します。
 - 米国 AMP クラウドの場合、[US クラウド (US Cloud)] を選択します。
 - AMPv の場合、[プライベートクラウド (Private Cloud)] を選択し、[Cisco AMP プライベートクラウド](#)、(26 ページ) の説明に従って続行します。

- ステップ 4** このクラウドを AMP for Firepower と AMP for Endpoints に使用する場合は、[AMP for Firepower に使用 (Use for AMP for Firepower)] チェックボックスをオンにします。マルチドメイン展開では、このチェックボックスはグローバルドメインにのみ表示されます。各 Firepower Management Center には、AMP for Firepower 接続を 1 つだけ設定できます。
- ステップ 5** [登録 (Register)] をクリックします。回転状態のアイコンは、たとえば、Firepower Management Center で接続を設定した後、AMP for Endpoints 管理コンソールの使用を許可する前に、接続が保留中であることを示します。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。
- ステップ 6** AMP for Endpoints 管理コンソールを続行することを確認し、管理コンソールにログインします。
- ステップ 7** 管理コンソールを使用して、AMP for Endpoints データを Firepower Management Center に送信することを AMP クラウドに許可します。
- ステップ 8** 受信するデータを制限する場合は、情報を受け取る組織内の特定のグループを選択します。デフォルトでは、AMP クラウドはすべてのグループのデータを送信します。グループを管理するには、AMP for Endpoints 管理コンソールで [管理 (Management)] > [グループ (Groups)] を選択します。詳細については、管理コンソールのオンラインヘルプを参照してください。
- ステップ 9** [許可 (Allow)] をクリックして接続を有効にして、データの転送を開始します。[拒否 (Deny)] をクリックすると Firepower Management Center に戻りますが、接続には拒否マークが付きます。接続を拒否/許可しないまま AMP for Endpoints 管理コンソールの [アプリケーション (Applications)] ページから別のページに移動した場合、Firepower Management Center の Web インターフェイスでは接続に保留中のマークが付きます。これらのいずれの状況でも、ヘルスマニタは失敗した接続のアラートを生成しません。後で AMP クラウドに接続するには、失敗した接続または保留中の接続を削除してから再作成します。
- AMP for Endpoints 接続の登録が未完了であっても、AMP for Firepower 接続は無効になりません。

Cisco AMP プライベートクラウド

Cisco AMP プライベートクラウド仮想アプライアンス (AMPv) を構成することで、ネットワーク上の AMP エンドポイント データを収集することができます。AMPv は、AMP クラウドの圧縮型、オンプレミスバージョンとして機能する、シスコ独自の仮想マシンです。

エンドポイント向け AMP のすべてのコネクタが AMPv にデータを送信し、AMPv は Firepower Management Center にデータを転送します。AMPv は、エンドポイントデータを外部接続では一切共有しません。Firepower Management Center は AMP クラウドに接続し、ネットワークトラフィックで検出されたファイルの判定結果をクエリしたり、レトロスペクティブマルウェアイベントを受信したりします。

各プライベートクラウドは、エンドポイント向け AMP コネクタを最大 10,000 までサポート可能で、複数のプライベートクラウドを設定できます。

[AMP 管理 (AMP Management)] ページ ([AMP]>[AMP 管理 (AMP Management)]) を使って、Firepower Management Center から AMPv との接続を制御します。



(注) AMP for Firepower のコンポーネントであるダイナミック分析では、管理対象デバイスがポート 443 から AMP Threat Grid クラウドまたはオンプレミス AMP Threat Grid アプライアンスに、直接あるいはプロキシを介してアクセスできる必要があります。AMPv はダイナミック分析をサポートしていません。また、シスコ集合型セキュリティインテリジェンス (CSI) に依存するその他の機能 (URL フィルタリングやセキュリティインテリジェンス フィルタリングなど) のための脅威インテリジェンスの匿名での取得もサポートしていません。

AMPv への接続

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
マルウェア (AMP for Firepower) 任意 (AMP for Endpoints)	マルウェア (AMP for Firepower) 任意 (AMP for Endpoints)	任意 (Any)	任意 (Any)	Admin

はじめる前に

- AMPv のマニュアルの指示に従って、Cisco AMP プライベートクラウドまたはクラウドを設定します。設定時に、プライベートクラウドのホスト名をメモしてください。このホスト名は、後で Firepower Management Center で接続を設定するときに必要になります。
- Firepower Management Center が AMPv と通信できることを確認し、AMPv がインターネットにアクセスでき、AMP クラウドと通信できることを確認します。

手順

- ステップ 1** [AMP]>[AMP 管理 (AMP Management)] を選択します。
- ステップ 2** [AMP クラウド接続の作成 (Create AMP Cloud Connection)] をクリックします。
- ステップ 3** [クラウド名 (Cloud Name)] ドロップダウンリストから [プライベートクラウド (Private Cloud)] を選択します。
- ステップ 4** 名前を入力します。
この情報は、AMPv によって生成または送信されるマルウェア イベントに表示されます。

- ステップ 5** [ホスト (Host)] フィールドに、AMPv の設定時に設定したプライベートクラウドのホスト名を入力します。
- ステップ 6** [証明書アップロードパス (Certificate Upload Path)] フィールドの横にある [参照 (Browse)] をクリックして、AMPv の有効な TLS または SSL 暗号化証明書の場所を参照します。詳細については、AMPv のマニュアルを参照してください。
- ステップ 7** このプライベートクラウドを AMP for Firepower および AMP for Endpoints に使用する場合は、[AMP for Firepower に使用 (Use for AMP for Firepower)] チェックボックスをオンにします。AMP for Firepower 通信を処理する別のプライベートクラウドを設定した場合は、このチェックボックスをオフにすることができます。これが唯一の AMPv 接続の場合は、オフにできません。マルチドメイン展開では、このチェックボックスはグローバルドメインにのみ表示されます。各 Firepower Management Center には、AMP for Firepower 接続を 1 つだけ設定できます。
- ステップ 8** プロキシを使用して AMPv と通信するには、[接続にプロキシを使用 (Use Proxy for Connection)] チェックボックスをオンにします。
- ステップ 9** [登録 (Register)] をクリックし、AMP クラウドへの既存の直接接続を無効にすることを確認し、最後に AMPv 管理コンソールを続行して登録を完了することを確認します。
- ステップ 10** 管理コンソールにログインして登録プロセスを完了します。手順の詳細については、AMPv のマニュアルを参照してください。

AMP クラウドおよび AMPv 接続の管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
マルウェア (AMP for Firepower) 任意 (AMP for Endpoints)	マルウェア (AMP for Firepower) 任意 (AMP for Endpoints)	任意 (Any)	任意 (Any)	Admin

クラウドからマルウェア関連の情報を受信する必要がなくなったら、Firepower Management Center を使用して AMP クラウドまたは AMPv 接続を削除します。AMP for Endpoints または AMPv 管理コンソールを使用して接続の登録を解除しても、システムから接続を削除することにはならない点に注意してください。登録解除した接続は、Firepower Management Center の Web インターフェイスに障害発生状態で表されます。

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

**注意**

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

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

手順

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

ステップ 2 AMP クラウド接続を管理します。

- 削除：削除アイコン (🗑️) をクリックして、選択内容を確認します。
- 有効化または無効化：スライダをクリックして、選択内容を確認します。

動的分析接続

AMP Threat Grid クラウドでは、ファイルがサンドボックス環境で実行されます。AMP for Firepower ではクラウドを使用して、動的分析送信ファイルの脅威スコアと動的分析レポートを取得します。適切なライセンスを使用して、システムが自動的にクラウドにアクセスします。

組織のセキュリティ ポリシーが Firepower システムによるネットワーク外部へのファイルの送信を許可しない場合は、オンプレミスの AMP Threat Grid アプライアンスを設定できます。詳細については、『Cisco AMP Threat Grid Appliance Setup and Configuration Guide』を参照してください。

Firepower Management Center の [ダイナミック分析接続 (Dynamic Analysis Connections)] ページ ([AMP]>[ダイナミック分析接続 (Dynamic Analysis Connections)]) を使用して、AMP Threat Grid クラウドへのパブリック動的分析接続およびオンプレミスの AMP Threat Grid アプライアンスへのプライベート動的分析接続を管理します。

デフォルトの動的分析接続の表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
マルウェア	マルウェア	任意 (Any)	グローバルだけ	Admin/Access Admin/Network Admin

デフォルトで、Firepower Management Center は、ファイルを送信したり、レポートを取得したりするために、パブリック AMP Threat Grid クラウドに接続できます。この接続は、設定したり、削除したりすることはできません。

手順

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

ステップ 2 編集アイコン (✎) をクリックします。

Threat Grid のオンプレミス アプライアンス

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

1 台のオンプレミス AMP Threat Grid アプライアンスを Firepower Management Center に接続できません。詳細については、『Cisco AMP Threat Grid アプライアンス セットアップおよび構成ガイド』を参照してください。

このオンプレミスアプライアンスへの動的分析接続を設定した場合、システムではパブリックの AMP クラウドを使用してマルウェアクラウドルックアップを実行し、またファイルが以前に動的分析用に送信されていないことを確認します。

システムでは、パブリック レポートの取得に AMP クラウドへのデフォルトのパブリック動的分析接続も使用します。オンプレミスアプライアンスがファイル用の動的分析レポートを生成しなかった場合、システムはこの動的分析レポートについてパブリックの AMP クラウドに問い合わせます。組織がファイルを送信していない限り、表示できるのは、限られたデータが含まれた、スクラビング処理が実行されたレポートだけです。

オンプレミスの動的分析接続の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
マルウェア	マルウェア	任意 (Any)	グローバルだけ	Admin/Access Admin/Network Admin

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

はじめる前に

- オンプレミスの AMP Threat Grid アプライアンスを設定します。『*Cisco AMP Threat Grid Appliance Setup and Configuration Guide*』を参照してください。
- ログインに使用する公開キー証明書を AMP Threat Grid アプライアンスからオンプレミスのアプライアンスにダウンロードします。『*Cisco AMP Threat Grid Appliance Administrator's Guide*』を参照してください。
- プロキシを使用してオンプレミスのアプライアンスに接続する場合は、プロキシを設定します。[Firepower Management Center 管理インターフェイスの設定](#)を参照してください。

手順

- ステップ 1 [AMP] > [ダイナミック分析接続 (Dynamic Analysis Connections)] を選択します。
- ステップ 2 [新しい接続を追加 (Add New Connection)] をクリックします。
- ステップ 3 名前を入力します。
- ステップ 4 [ホスト URL (Host URL)] を入力します。
- ステップ 5 [証明書のアップロード (Certificate Upload)] の横にある [参照 (Browse)] をクリックして、オンプレミスのアプライアンスとの接続を確立するために使用する公開キー証明書をアップロードします。
- ステップ 6 設定されているプロキシを使用して接続を確立する場合は、[可能な場合はプロキシを使用 (Use Proxy When Available)] を選択します。
- ステップ 7 [登録 (Register)] をクリックします。
- ステップ 8 [はい (Yes)] をクリックして、オンプレミスの AMP Threat Grid アプライアンスのログイン ページを表示します。
- ステップ 9 オンプレミスの AMP Threat Grid アプライアンスにユーザ名とパスワードを入力します。
- ステップ 10 [サインイン (Sign in)] をクリックします。
- ステップ 11 次の選択肢があります。
 - 以前にオンプレミスのアプライアンスに Firepower Management Center を登録した場合は、[戻る (Return)] をクリックします。
 - Firepower Management Center を登録していない場合は、[アクティブ化 (Activate)] をクリックします。

集合型セキュリティ インテリジェンス通信の設定

Firepower システムは、レピュテーション、リスク、脅威インテリジェンスに関して、シスコ集合型セキュリティ インテリジェンス (CSI) を使用します。適正なライセンスがあれば、URL フィルタリングおよび AMP for Firepower 機能の通信オプションを指定できます。

集合型セキュリティ インテリジェンスの通信設定オプション

Enable URL Filtering

Web サイトの一般的な分類、カテゴリ、リスク レベル、またはレピュテーションに基づくトラフィックのフィルタリングを可能にします。URL フィルタリングライセンスが自動的に追加されるようにして、[URL フィルタリングを有効にする (Enable URL Filtering)] および [自動更新を

有効にする (Enable Automatic Updates)]を有効にします。URL フィルタリングは、他の URL フィルタリング オプションを選択する前に有効にする必要があります。

URL フィルタリングを有効にする場合は、URL フィルタリングが最後に有効になってから経過した時間に応じて、または URL フィルタリングを今回初めて有効にするかどうかに応じて、Firepower Management Center が Cisco CSI から URL データを取得します。

メモリの制約上、一部のモデルでは、小規模でそれほど細分化されていないカテゴリとレピュテーションによって URL フィルタリングが実行されます。たとえば、親 URL のサブサイトがそれぞれ異なる URL カテゴリとレピュテーションを持っている場合、一部のデバイスでは、すべてのサブサイトに対して親 URL のデータが使用されます。具体的な例として、システムは google.com カテゴリとレピュテーションを使用して mail.google.com を評価します。

メモリが少ないデバイスには、7100 ファミリーと次の ASA モデルが含まれます：ASA5506-X、ASA5506H-X、ASA5506W-X、ASA5508-X、ASA5512-X、ASA5515-X、ASA5516-X、ASA5525-X。NGIPSv で、カテゴリおよびレピュテーションベースの URL フィルタリングを実行するための正しいメモリ量を割り当てる方法について、詳しくは *Firepower System Virtual Installation Guide* を参照してください。

自動更新を有効にする (Enable Automatic Updates)

Firepower Management Center で展開環境の URL データが自動的に更新されるようにします。一般的に、URL データは 1 日 1 回更新されますが、自動更新を有効にすると、30 分ごとに Firepower Management Center が確認するようになります。通常、毎日の更新は小規模ですが、最終更新日から 5 日を超えると、帯域幅によっては新しい URL データのダウンロードに最長 20 分かかる場合があります。その後、更新自体を実行するのに最長で 30 分かかることがあります。

システムが外部リソースと通信するタイミングを厳格に制御する必要がある場合は、自動更新を無効にし、代わりにスケジューラを使用します。



(注) Cisco では、自動更新を有効にするか、またはスケジューラを使用して更新をスケジュールすることを推奨しています。[今すぐ更新する (Update Now)]をクリックして手動でオンデマンド更新を実行できますが、プロセスを自動化すると、最新の関連データを使用できるようになります。更新がすでに進行中である場合は、オンデマンド更新を開始できません。

不明 URL を Cisco CSI に問い合わせる (Query Cisco CSI for Unknown URL)

カテゴリとレピュテーションがローカルデータセットにない Web サイトをユーザが閲覧するとき URL が脅威インテリジェンス評価のために送信されるようにします。プライバシー上の理由などで未分類の URL を送信したくない場合は、このオプションを無効にしてください。

未分類の URL への接続は、カテゴリまたはレピュテーションベースの URL 条件を含むルールに一致しません。URL に手動でカテゴリやレピュテーションを割り当てることはできません。

ローカル マルウェア検出の自動更新を有効にする (Enable Automatic Local Malware Detection Updates)

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

マルウェア イベントの URL を Cisco と共有する (Share URI from Malware Events with Cisco)

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

レガシー ポート 32137 を AMP for Firepower に使用する (Use Legacy Port 32137 for AMP for Firepower)

デフォルトでは、AMP for Firepower はポート 443/HTTPS を使用して AMP クラウド（または AMPv）と通信します。このオプションは、AMP for Firepower によるポート 32137 の使用を許可します。システムを以前のバージョンから更新する場合は、このオプションを有効にすることができます。

関連トピック

[通信ポートの要件](#)

集合型セキュリティ インテリジェンスとの通信の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
URL フィルタリング (URL フィルタリング)	URL フィルタリング (URL フィルタリング)	任意 (Any)	任意 (Any)	Admin
マルウェア (AMP for Firepower)	マルウェア (AMP for Firepower)			

手順

-
- ステップ 1 [システム (System)] > [統合 (Integration)] を選択します。
 - ステップ 2 [Cisco CSI] タブをクリックします。
 - ステップ 3 [集合型セキュリティ インテリジェンスの通信設定オプション](#), (32 ページ) の説明に従って Cisco CSI 通信を設定します。
 - ステップ 4 [保存 (Save)] をクリックします。
-

