ファイル ポリシーと高度なマルウェア防御

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 ポリシーと高度なマルウェア防御について

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

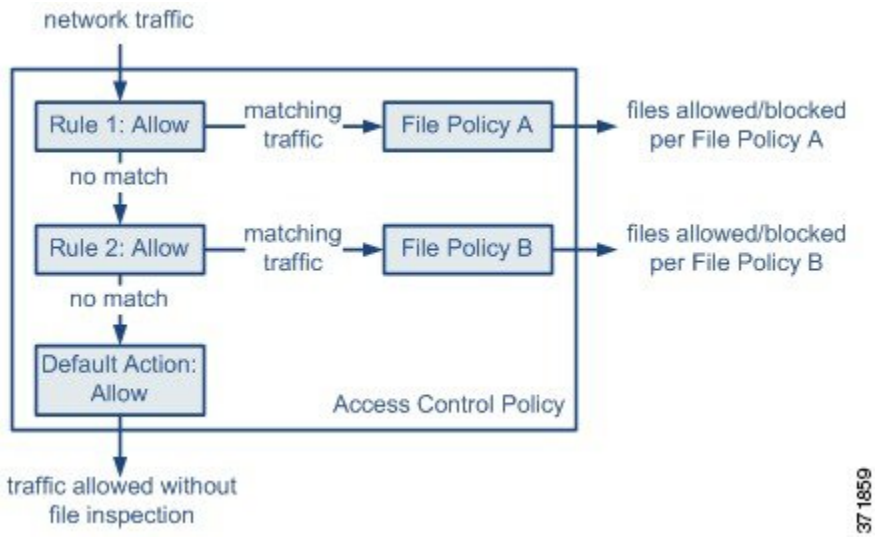
Firepower の高度なマルウェア防御（AMP）は、ネットワーク トラフィックでのマルウェアの伝送を検出、キャプチャ、追跡、分析、ロギング、および必要に応じてブロックできます。Firepower Management Center Web インターフェイスでは、この機能は ネットワーク向け *AMP* と呼ばれ、以前は *AMP for Firepower* とも呼ばれていました。高度なマルウェア防御は、シスコ クラウドからインラインおよび脅威データを展開した管理対象デバイスを使用してマルウェアを特定します。

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

システムがネットワーク上のマルウェアを検出すると、ファイルおよびマルウェア イベントを生成します。ファイルおよびマルウェア イベント データを分析するには、ファイル/マルウェア イベントとネットワーク ファイル トラジェクトリを参照してください。

ファイル ポリシー

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

ファイルおよびマルウェア ポリシーのライセンス要件

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

マルウェアライセンスの詳細については、次を参照してください。

- Firepower Threat Defense デバイスのマルウェア ライセンス
- 従来のデバイスのマルウェア ライセンス

マルウェア防御のベストプラクティス

- マルウェア防御の設定方法 （4 ページ）およびそのサブトピックの手順に従います。
- 手順の前提条件を必ず満たしてください。
- ファイル ポリシーとファイル ルールの注意事項と制限事項 （20 ページ）も参照してください。

マルウェア防御の設定方法

ここでは、悪意のあるソフトウェアからネットワークを保護するために Firepower システムの設定で実行する必要がある手順を説明します。

手順

ステップ 1 マルウェア防御の計画と準備 （4 ページ）

ステップ 2 ファイル ポリシーの設定 （6 ページ）

ステップ 3 アクセス コントロール設定へのファイル ポリシーの追加 （6 ページ）

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

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

ネットワーク検出ポリシーおよびサブトピックを参照してください。

ステップ 5 管理対象デバイスにポリシーを展開します。

設定変更の展開を参照してください。

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

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

次のタスク

- （任意）ネットワーク内のマルウェアの検出をさらに強化するには、シスコの AMP for Endpoints 製品を導入して統合します。（オプション）AMP for Endpoints を使用したマルウェア防御 （44 ページ）およびサブトピックを参照してください。
- ファイルおよびマルウェア イベントを調査する方法を理解します。

  ファイル/マルウェア イベントとネットワーク ファイル トラジェクトリを参照してください。

マルウェア防御の計画と準備

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

手順

ステップ 1 ライセンスを購入してインストールします。

ファイルおよびマルウェア ポリシーのライセンス要件 （3 ページ）およびFirepower システムのライセンスを参照してください。

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

侵入ポリシーとファイル ポリシーを使用したアクセス制御の章を参照してください。

ステップ 3 ファイル分析およびマルウェア防御ツールについて理解します。

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

また、 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 （24 ページ）も考慮してください。

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

マルウェア防御のためのクラウド接続（8 ページ）およびサブトピックを参照してください。

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

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

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

セキュリティ、インターネット アクセス、および通信ポートを参照してください。

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

- AMP クラウドについては、AMP オプションの変更 （14 ページ）を参照してください。
- オンプレミスの Cisco Threat Grid アプライアンスを展開した場合は、オンプレミスの動的分析アプライアンスへの接続（16 ページ）を参照してください。（パブリック Threat Grid クラウドへのアクセスに設定は必要ありません。）

次のタスク

マルウェア防御ワークフローの次の手順に進みます。

マルウェア防御の設定方法 （4 ページ）を参照してください。

ファイル ポリシーの設定

始める前に

マルウェア防御ワークフローで、この時点までのタスクを実行します。

マルウェア防御の設定方法 （4 ページ）を参照してください。

手順

ステップ 1 ファイル ポリシーおよびファイル ルールの制限事項を確認します。

ファイル ポリシーとファイル ルールの注意事項と制限事項 （20 ページ）およびサブトピックを参照してください。

ステップ 2 ファイル ポリシーを作成します。

ファイル ポリシーの作成 （23 ページ）を参照してください。

ステップ 3 ファイル ポリシー内にルールを作成します。

ファイル ルール （30 ページ）およびサブトピックを参照してください。

ステップ 4 詳細オプションを設定します。

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 （24 ページ）を参照してください。

次のタスク

マルウェア防御ワークフローの次の手順に進みます。

マルウェア防御の設定方法 （4 ページ）を参照してください。

アクセス コントロール設定へのファイル ポリシーの追加

始める前に

マルウェア防御ワークフローで、この時点までのタスクを実行します。

マルウェア防御の設定方法 （4 ページ）を参照してください。

手順

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

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

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

マルウェア保護のためのアクセス コントロール ルールの設定を参照してください

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

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

次のタスク

マルウェア防御ワークフローの次の手順に進みます。

マルウェア防御の設定方法 （4 ページ）を参照してください。

マルウェア防御のメンテナンスとモニタリングの設定

ネットワークの保護には継続的なメンテナンスが必要不可欠です。

始める前に

マルウェアからネットワークを保護するようにシステムを設定します。

マルウェア防御の設定方法 （4 ページ）および参照手順を確認してください。

手順

ステップ 1 システムが常に最新かつ効果的に保護されていることを確認します。

システムの保守：動的分析の対象となるファイル タイプの更新 （19 ページ）を参照してください。

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

次のモジュールについては、ヘルス モニタリングのネットワーク向け AMP アラートの設定を参照してください。

- ローカル マルウェア分析（Local Malware Analysis）
- Security Intelligence
- デバイスでの脅威データの更新
- 侵入およびファイル イベント レート
- AMP for Firepower のステータス

- AMP for Endpoint のステータス

次のタスク

マルウェア防御ワークフローの「次の項目について」を確認してください。

マルウェア防御の設定方法 （4 ページ）を参照してください。

マルウェア防御のためのクラウド接続

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

AMP クラウド

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

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

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

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

- **AMP パブリック クラウド**

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

- **AMP プライベート クラウド**

  ネットワーク上に展開された AMP プライベート クラウドは、圧縮型、オンプレミス AMP クラウドおよびパブリック AMP クラウドに接続するための匿名プロキシとして機能します。詳細は、Cisco AMP プライベート クラウド （11 ページ）を参照してください。

  AMP for Endpoints と統合する場合、AMP プライベート クラウドにはいくつかの制限があります。AMP for Endpoints と AMP プライベート クラウド （47 ページ）を参照してください。

動的分析クラウド

- **Cisco Threat Grid クラウド**

動的分析の送信に適したファイルを処理し、脅威スコアと動的分析レポートを提供するパブリック クラウド。

- **オンプレミス Cisco Threat Grid アプライアンス**

  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、オンプレミスアプライアンスを設定できます。このアプライアンスはパブリック Cisco Threat Grid クラウドには接続しません。

  詳細については、オンプレミス アプライアンスの動的分析（Cisco Threat Grid） （16 ページ）を参照してください。

AMP および Threat Grid クラウドへの接続の設定

- AMP クラウド接続の設定 （9 ページ）
- 動的分析接続 （15 ページ）

AMP クラウド接続の設定

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

- AMP クラウドの選択 （10 ページ）
- AMP プライベート クラウドへの接続 （12 ページ）
- Firepower と AMP for Endpoints の統合 （47 ページ）

次のトピックも関連しています。

- Cisco AMP プライベート クラウド （11 ページ）
- AMP クラウド接続の要件とガイドライン （9 ページ）
- AMP クラウドへの接続の管理（パブリックまたはプライベート） （13 ページ）

AMP クラウド接続の要件とガイドライン

AMP クラウド接続要件

FMC が AMP クラウドと通信できるようにするには、セキュリティ、インターネット アクセス、および通信ポートのトピックを参照してください。

AMP の通信にレガシー ポートを使用するには 通信ポートの要件 を参照してください。

AMP とハイ アベイラビリティ

ハイ アベイラビリティ ペアの Firepower Management Center はファイル ポリシーおよび関連する設定を共有しますが、クラウド接続、キャプチャされたファイル、ファイルイベント、マルウェアイベントを共有することはありません。運用の継続性を確保し、検出されたファイルの

マルウェア処理が両方の Firepower Management Center で同じであるようにするためには、アクティブとスタンバイ両方の Firepower Management Center がクラウドにアクセスできる必要があります。

ハイ アベイラビリティの設定では、Firepower Management Center のアクティブ インスタンスとスタンバイ インスタンスで AMP クラウド接続を個別に設定する必要があります。これらの設定は同期されません。

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

AMP クラウド接続とマルチテナンシー

マルチドメイン展開では、ネットワーク向け AMP 接続はグローバル レベルでのみ設定します。各 Firepower Management Center には、ネットワーク向け AMP 接続を 1 つだけ設定できます。

AMP クラウドの選択

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）	任意（Any）	Admin

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

始める前に

- AMP プライベート クラウドを使用する場合は、このトピックの代わりにAMP プライベート クラウドへの接続 （12 ページ）を参照してください。
- Firepower が AMP for Endpoints と統合されていない場合は、AMP クラウド接続を 1 つだけ設定できます。この接続には、**AMP for Networks** または **AMP for Firepower** というラベルが付けられています。
- AMP for Endpoints を展開し、このアプリケーションを Firepower と統合するために 1 つ以上の AMP クラウドを追加する場合は、Firepower と AMP for Endpoints の統合 （47 ページ）を参照してください。
- AMP クラウド接続の要件とガイドライン （9 ページ）を参照してください。

手順

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

ステップ 2 鉛筆アイコンをクリックし、既存のクラウド接続を編集します。

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

APJC はアジア/太平洋/日本/中国です。

ステップ 4 [保存（Save）] をクリックします。

次のタスク

- 展開がハイ アベイラビリティ構成の場合は、AMP クラウド接続の要件とガイドライン （9 ページ）を参照してください。
- （任意）AMP オプションの変更 （14 ページ）。

Cisco AMP プライベート クラウド

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。このクラウドはパブリックまたはプライベートに指定することができます。

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

AMP プライベート クラウドを介した AMP クラウド ファネルとのすべての接続は、監視対象ネットワークのセキュリティとプライバシーを確保するための匿名プロキシとして機能します。これには、ネットワーク トラフィックで検出されたファイルの判定結果のクエリ、レトロスペクティブ マルウェア イベントの受信などが含まれます。AMP プライベート クラウドは、エンドポイント データを外部接続では一切共有しません。

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

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

AMP プライベート クラウドへの接続

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（ネットワーク向け AMP ） 任意（AMP for Endpoints）	マルウェア（ネットワーク向け AMP ） 任意（AMP for Endpoints）	任意（Any）	任意（Any）	Admin

始める前に

- AMP のマニュアルの指示に従って、Cisco AMP プライベート クラウドまたはクラウドを設定します。設定時に、プライベート クラウドのホスト名をメモしてください。このホスト名は、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 AMP プライベート クラウドと通信できることを確認し、プライベート クラウドがインターネットにアクセスし、パブリック AMP クラウドと通信できることを確認します。セキュリティ、インターネット アクセス、および通信ポートのトピックを参照してください。
- 展開で AMP for Endpoints と統合されていない場合は、Firepower Management Center ごとに AMP クラウド接続を 1 つだけ設定できます。この接続には、**AMP for Networks** または **AMP for Firepower** というラベルが付けられています。

  AMP for Endpoints と統合する場合は、複数の AMP for Endpoints クラウド接続を設定できます。

手順

ステップ 1 **[AMP]** > **[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、AMP プライベート クラウドによって生成または送信されるマルウェア イベントに表示されます。

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

ステップ 6 [証明書アップロードパス（Certificate Upload Path）] フィールドの横にある [参照（Browse）] をクリックして、プライベート クラウドの有効な TLS または SSL 暗号化証明書の場所を参照します。詳細については、AMP プライベート クラウドのマニュアルを参照してください。

ステップ 7 このプライベート クラウドを ネットワーク向け AMP と AMP for Endpoints の両方に使用する場合は、[AMP for Firepowerに使用（Use for AMP for Firepower）] チェックボックスをオンにします。

ネットワーク向け AMP 通信を処理する別のプライベート クラウドを設定した場合は、このチェックボックスをオフにすることができます。これが唯一の AMP プライベート クラウド接続の場合は、オフにできません。

マルチドメイン展開では、このチェックボックスはグローバル ドメインにのみ表示されます。各 Firepower Management Center には、ネットワーク向け AMP 接続を 1 つだけ設定できます。

ステップ 8 プロキシを使用して AMP プライベート クラウドと通信するには、[接続にプロキシを使用（Use Proxy for Connection）] チェックボックスをオンにします。

ステップ 9 [登録（Register）] をクリックし、AMP クラウドへの既存の直接接続を無効にすることを確認し、最後に AMP プライベート クラウド管理コンソールを続行して登録を完了することを確認します。

ステップ 10 管理コンソールにログインして登録プロセスを完了します。詳細については、AMP プライベート クラウドのマニュアルを参照してください。

次のタスク

ハイ アベイラビリティの設定では、Firepower Management Center のアクティブ インスタンスとスタンバイ インスタンスで AMP クラウド接続を個別に設定する必要があります。これらの設定は同期されません。

AMP クラウドへの接続の管理（パブリックまたはプライベート）

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（ネットワーク向け AMP ） 任意（AMP for Endpoints）	マルウェア（ネットワーク向け AMP ） 任意（AMP for Endpoints）	任意（Any）	任意（Any）	Admin

Firepower Management Center を使用して、ネットワーク向け AMP や AMP for Endpoints またはその両方に使用されるパブリックおよびプライベート AMP クラウドへの接続を管理します。

クラウドからマルウェア関連の情報を受信する必要がなくなった場合は、パブリックまたはプライベート AMP クラウドとの接続を削除します。AMP for Endpoints または AMP プライベート クラウド管理コンソールを使用して接続の登録を解除しても、システムから接続を削除することにはならない点に注意してください。登録解除した接続は、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 無効化された接続の場合、プライベート AMP クラウドは、接続を再有効化するまでマルウェア イベントや侵害の兆候などを保存できます。まれに、イベント レートが非常に高い場合や接続が長期間無効になっていた場合など、接続無効中に生成されたすべての情報をクラウドで保存できないことがあります。

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

手順

ステップ 1 **[AMP]** > **[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。

次のタスク

ハイ アベイラビリティの設定では、Firepower Management Center のアクティブ インスタンスとスタンバイ インスタンスで AMP クラウド接続を個別に設定する必要があります。これらの設定は同期されません。

AMP オプションの変更

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）	任意（Any）	Admin

手順

ステップ 1 **[System]** > **[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 次のオプションを選択します。

表 *1 : AMP for Networks* のオプション

オプション	説明
ローカル マルウェア検出の自動更新を有効にする（Enable Automatic Local Malware Detection Updates）	ローカルマルウェア検出エンジンは、Cisco が提供する署名を使用して統計的にファイルを分析し、事前に分類します。このオプションを有効にすると、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 ネットワーク向け AMP に使用する（Use Legacy Port 32137 for AMP for Networks）	デフォルトでは、Firepower はポート 443/HTTPS を使用して AMP パブリック クラウドまたはプライベート クラウドと通信し、ファイルの性質データを取得します。このオプションは、システムによるポート 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。 FMC がプロキシ設定で設定されている場合、このオプションはグレー表示されます。

ステップ 4 [保存（Save）] をクリックします。

動的分析接続

動的分析の要件

適切なライセンスを使用すると、Firepower システムが Cisco Threat Grid パブリック クラウドに自動的にアクセスします。

動的分析では、管理対象デバイスがポート 443 から Cisco Threat Grid パブリック クラウドまたはオンプレミス Cisco 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。

動的分析の対象となるファイル （39 ページ）も参照してください。

オンプレミス Threat Grid アプライアンスに接続する場合は、オンプレミスの動的分析アプライアンスへの接続 （16 ページ）の前提条件も参照してください。

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 Cisco 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]** > **[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。

（注） **[AMP]** > **[ダイナミック分析接続（Dynamic Analysis Connections）]** ページの  ボタンの詳細については、パブリック クラウドでの動的分析の結果へのアクセスの有効化（18 ページ）を参照してください。

オンプレミス アプライアンスの動的分析（Cisco Threat Grid）

組織にパブリックの Cisco 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 Cisco 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格なファイルをサンドボックス環境で実行し、脅威スコアと動的分析レポートを 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。

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

オンプレミスの動的分析アプライアンスへの接続

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 Cisco 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。

始める前に

- オンプレミスの Cisco Threat Grid アプライアンスを設定します。『*Cisco Threat Grid Appliance Setup and Configuration Guide*』を参照してください。

  このアプライアンスのドキュメントは、https://www.cisco.com/c/en/us/support/security/amp-threat-grid-appliances/tsd-products-support-series-home.html から入手できます。
- ログインに使用する公開キー証明書を Cisco 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 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。
- 管理対象デバイスは、ポート 443 で Cisco Threat Grid アプライアンスへの直接またはプロキシを介したアクセスが必要です。

手順

ステップ 1 **[AMP]** > **[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 Cisco 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 Cisco 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。

パブリック クラウドでの動的分析の結果へのアクセスの有効化

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

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

始める前に

Cisco Threat Grid パブリック クラウドにアカウントがあること、およびアカウントのクレデンシャルを持っている必要があります。

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 Cisco Threat Grid パブリック クラウドに対応するテーブル行で、 をクリックします。

Cisco Threat Grid ポータル ウィンドウが開きます。

ステップ 3 Cisco Threat Grid パブリック クラウドにサインインします。

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

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

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

この変更が有効になるまでに最大で 24 時間かかることがあります。

次のタスク

関連付けが有効化された後、Cisco Threat Grid パブリック クラウドの動的分析結果の表示を参照してください。

システムの保守：動的分析の対象となるファイル タイプの更新

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）	グローバルだけ	Admin

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

システムに現在のリストがあることを次のように確認します。

手順

ステップ 1 次のいずれかを実行します。

- （推奨）参照します 脆弱性データベースの更新の自動化
- 新しい VDB の更新を定期的に確認し、必要に応じて脆弱性データベース（VDB）の手動による更新を確認します。

  このオプションを選択した場合は、定期的な通知をスケジュールすることをお勧めします。

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

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

シスコ クラウド

Firepower System ではシスコの Collective Security Intelligence（CSI）クラウドを使用して、ファイルのリスクを評価し、URL カテゴリとレピュテーションを取得するために使用する脅威インテリジェンス データを取得します。適正なライセンスがあれば ネットワーク向け AMP および URL フィルタリングの機能の通信オプションを指定できます。

その他の情報：

- **高度なマルウェア防御**

  パブリック クラウドはデフォルトで設定されています。変更を加えるには、AMP オプションの変更 （14 ページ）を参照してください。

- **URL フィルタリング**

  詳細については、次を参照してください。

  - URL フィルタリング オプション
  - カテゴリとレピュテーションを使用した URL フィルタリングの有効化

ファイル ポリシーとファイル ルール

ファイル ポリシーとファイル ルールの注意事項と制限事項

ファイル ルール設定の注意事項と制限事項

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

  システムがすべてのファイルタイプを検査するには、動的分析と他の分析タイプで個別のルール（同じポリシー内）を作成します。
- [マルウェア クラウドルックアップ（Malware Cloud Lookup）] アクションまたは [マルウェア ブロック（Block Malware）] アクションを使ってファイル ルールが設定されている場合、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

- アダプティブ プロファイリングが有効でなければ、アクセス コントロール ルールは、AMP を含め、ファイルの制御を実行できません。
- ファイルがアプリケーション プロトコル条件を持つルールに一致する場合、ファイル イベントの生成は、システムがファイルのアプリケーションプロトコルを正常に識別した後に行われます。識別されていないファイルは、ファイル イベントを生成しません。
- FTP は、さまざまなチャネルを介してコマンドおよびデータを転送します。パッシブまたはインライン 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。
- ISO ファイルを検出するには、ファイルおよびマルウェアのインスペクション パフォーマンスとストレージのオプション の説明のように、[ファイルタイプを検知する前に検閲するバイト数制限（Limit the number of bytes inspected when doing file type detection）] オプションを 36870 を超える値に設定します。

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** ルールでブロックされるNetBios-ssn経由ファイル転送（SMBファイル転送など）の場合、宛先ホストでファイルが見つかることがあります。ただし、ダウンロード開始後にファイルがブロックされ、結果としてファイル転送が不完全になるため、そのファイルは使用できません。
- （SMBファイル転送などの）NetBIOS-ssn経由で転送されたファイルを検出またはブロックするファイルルールを作成した場合、進行中のファイル転送はシステムにより検査されません。ただし、ファイル ポリシーを呼び出すアクセス コントロール ポリシーを展開した後に、転送された新しいファイルがシステムにより検査されます。
- SMBには、同じIPアドレスと異なるポートを持つ複数のパラレル セッションを作成する、マルチチャネルと呼ばれる機能があります。マルチチャネルを使用するトランザクションでは、ファイルのダウンロードはこれらのセッションにわたって多重化され、システムにより単一のファイルとして検査されません。
- 1つのTCPまたはSMBセッションで同時に転送されたファイルは検査されません。
- クラスタ環境では、クラスタ ロールの変更またはデバイス障害が原因で既存のSMBセッションが新しいデバイスに移動されると、進行中のファイル転送のファイルが検査されないことがあります。
- Microsoft Windowsシステム間での一部のSMBファイル転送では、迅速なファイル転送のため、非常に大きなTCPウィンドウ サイズを使用します。このようなファイル転送を検出またはブロックするには、[ネットワーク分析ポリシー（Network Analysis Policy）] の [TCPストリームの設定（TCP Stream Configuration）] タブの [トラブルシューティング オプション（Troubleshooting Options）] にある [最大キューイング バイト（Maximum Queued Bytes）] と [最大キューイング セグメント（Maximum Queued Segments）] **の**値を大きくすることを推奨します。
- Firepower Threat Defenseのハイ アベイラビリティを設定したときに、元のアクティブなデバイスがファイルを識別している間にフェイル オーバーが発生した場合、ファイル タイプは同期されません。ファイル ポリシーでそのファイル タイプがブロックされている場合でも、新しいアクティブ デバイスはファイルをダウンロードします。

ファイル ポリシーの一般的な注意事項と制限事項

- ただし、アクセス コントロールのデフォルト アクションによって処理されるトラフィックを検査するためにファイル ポリシーを使用**できない**ことに注意してください。
- 新しいポリシーの場合、ポリシーが使用中でないことがWebインターフェイスに示されます。使用中のファイル ポリシーを編集している場合は、そのファイル ポリシーを使用しているアクセス コントロール ポリシーの数がWebインターフェイスに示されます。ど

ちらの場合も、テキストをクリックすると[アクセス コントロール ポリシー（Access Control Policies）] ページに移動できます。

- 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 ファイル転送をブロックし、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。
- 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 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**）
脅威（ファイル制御） マルウェア（ネットワーク向け AMP ）	Protection（ファイル制御） マルウェア（ネットワーク向け AMP ）	任意（Any）	任意（Any）	Admin/Access Admin

始める前に

マルウェア保護のポリシーを設定する場合は、ファイル ポリシーの設定 （6 ページ）を参照してください。

手順

ステップ 1 **[Policies]** > **[Access Control]** > **[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 （42 ページ）の説明に従って、ファイル ポリシーに 1 つ以上のルールを追加します。

ステップ 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 （24 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。

次のタスク

- マルウェア保護のポリシーを設定する場合は、ファイル ポリシーの設定 （6 ページ）を参照してください。
- 該当しない場合は、次のようになります。
  - マルウェア保護のためのアクセス コントロール ルールの設定の説明に従って、アクセス コントロール ルールにファイル ポリシーを追加します。
  - 設定変更を展開します。設定変更の展開を参照してください。

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）]：最初に表示された（不明な）ファイルを保存し、ローカルで分析すると同時に AMP クラウドでの処理を保留にする場合にこのオプションを選択します。ファイルは、マルウェア クラウド ルックアップと Spero 分析、ローカル マルウェア分析、またはダイナミック分析を実行するように設定されているルールに一致する必要があります。ストレージと処理リソースを節約するには、このオプションの選択を解除します。このオプションの選択を解除すると、初めて検出されたファイルは「不明（Unknown）」とマークされます。
- [カスタム検出リストを有効にする（Enable Custom Detection List）]：カスタム検出リストにあるファイルをブロックします。
- [クリーンリストを有効にする（Enable Clean List）]：有効にすると、このポリシーはクリーン リストにあるファイルを許可します。
- [脅威スコアに基づいてAMPクラウド判定結果を上書きする（Override AMP Cloud Disposition Based upon 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）]：アクセス コントロールの詳細設定の [保存する最大ファイルサイズ（Maximum file size to store）] と同じ大きさのアーカイブ ファイルまで、アーカイブ ファイルのコンテンツのインスペクションをできるようにします。
- [暗号化されたアーカイブをブロックする（Block Encrypted Archives）]：暗号化されたコンテンツを含むアーカイブ ファイルをブロックします。
- [検査不可能なアーカイブをブロックする（Block Uninspectable Archives）]：暗号化以外の理由でシステムが検査できないコンテンツを含むアーカイブ ファイルをブロックします。これは通常、破損したファイル、または指定した最大アーカイブ深度を超えるファイルに適用されます。
- **[最大アーカイブ深度（Max Archive Depth）]**：指定した深度を超えるネストされたアーカイブ ファイルをブロックします。トップレベルのアーカイブ ファイルはこの数で考慮されません。深さは最初にネストされたファイルで 1 から始まります。

アーカイブ ファイル

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

ブロック アクションを含むファイル ルールにアーカイブ内のい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。

アーカイブ ファイルのインスペクションのオプションについては、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 （24 ページ）を参照してください。

検査可能なアーカイブ ファイル

- **ファイル タイプ**

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

  検査可能な格納ファイルが同じページに表示されます。

- **ファイルサイズ（File size）**

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

- **ネストされたアーカイブ**

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

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

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

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

- **暗号化ファイル**

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

- **検査されないアーカイブ**

  アーカイブ ファイルを含むトラフィックがセキュリティ インテリジェンス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 ファイルの性質

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

表 *2:* 内容に基づくアーカイブ ファイルの性質

アーカイブ ファイルの性質	不明なファイルの数	クリーン ファイルの数	マルウェア ファイルの数
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	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。

アーカイブの内容と詳細の表示

アーカイブ ファイルの内容を検査するようにファイル ポリシーが設定されている場合は、[分析（Analysis）] > [ファイル（Files）] メニューのページにあるコンテキスト メニューおよびネットワーク ファイル トラジェクトリ ビューアを使用して、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。

カスタム リストを使用したファイル性質のオーバーライド

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

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

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

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

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

または、該当する場合はAMP for Endpoints からの一元的なファイル リスト （27 ページ）を参照します。

AMP for Endpoints からの一元的なファイル リスト

組織で AMP for Endpoints を展開している場合、Firepower は AMP クラウドにファイルの性質を照会するときに、AMP for Endpoints で作成されたブラックリストおよびホワイトリストを使用できます。

要件：

- 組織で AMP パブリック クラウドを使用している必要がある。
- 組織で AMP for Endpoints を展開している。
- Firepower と AMP for Endpoints の統合 （47 ページ）の手順を使用して、Firepower システムを AMP for Endpoints に登録している。

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

（注） AMP for Endpoints で作成された Firepower オーバーライド ファイル リストで作成されたファイル リスト。

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）
脅威（ファイル制御） マルウェア（ネットワーク向け AMP）	Protection（ファイル制御） マルウェア（ネットワーク向け AMP）	任意（Any）	任意（Any）	Admin/Access Admin

手順

ステップ 1 **[Policies]** > **[Access Control]** > **[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 （30 ページ）を参照してください。
- 既存のファイル ルールを編集するには、その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 （24 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。

次のタスク

- 設定変更を展開します。設定変更の展開を参照してください。

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）
脅威（ファイル制御） マルウェア（ネットワーク向け AMP ）	Protection（ファイル制御） マルウェア（ネットワーク向け AMP ）	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） 動的分析の対象となるファイルタイプのリストが更新されたかどうか検査するために、システムは更新をチェックします（多くても1日に1回）。対象になるファイルタイプのリストが変更された場合、これはファイル ポリシーの変更を意味します。このファイル ポリシーを使用するアクセス コントロール ポリシーがいずれかのデバイスに展開されている場合、そのアクセス コントロール ポリシーには失効マークが付けられます。更新したファイル ポリシーがデバイスで有効になるには、まず、ポリシーを展開しておく必要があります。システムの保守：動的分析の対象となるファイル タイプの更新 （19 ページ）を参照してください。

手順

ステップ 1 **[Policies]** > **[Access Control]** > **[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 （23 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（設定変更の展開 を参照）。
- 編集：既存のファイル ポリシーを変更するには、編集アイコン（）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 ルール

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

たとえば、あるファイルがルールに一致する場合、ルールで以下を実行できます。

- 単純なファイル タイプ照合に基づいてファイルを許可またはブロックする
- 性質に基づいてファイルをブロックする（悪意があることを示す評価の有無に関係なく）
- デバイスにファイルを保存する（詳細については、キャプチャされたファイルとファイル ストレージ （40 ページ）を参照してください）
- ローカル マルウェア分析、Spero 分析、または動的分析のために、保存（キャプチャ）したファイルを送信する

さらに、ファイル ポリシーによって以下を実行できます。

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

ファイル ルールのコンポーネント

表 *3*: ファイル ルールのコンポーネント

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

ファイル ルールのコンポーネント	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。 システムで検査可能なファイル タイプのリストについては、[ポリシー（Policies）] > [アクセス制御（Access Control）] > [マルウェアとファイル（Malware & File）] を選択して、一時的な新しいファイル ポリシーを作成してから、[ルールの追加（Add Rule）] をクリックします。ファイル タイプ カテゴリを選択すると、システムが検査できるファイル タイプが [ファイルタイプ（File Types）] リストに表示されます。 （注） 頻繁にトリガーされるファイル ルールは、システム パフォーマンスに影響を与える可能性があります。たとえば、HTTP トラフィックでマルチメディア ファイルを検出しようとすると（たとえば YouTube は多量の Flash コンテンツを伝送します）、膨大な数のイベントが生成される可能性があります。

ファイル ルールのコンポーネント	説明
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。 選択したアクションに応じて、システムでファイルを保存するか、ファイルに対してSpero分析、ローカルマルウェア分析、または動的分析を実行するかを設定できます。[ブロック（Block）]アクションを選択すると、システムでブロックされた接続をリセットするかどうかも設定できます。 これらのアクションおよびオプションの説明については、ファイル ルール アクション （33 ページ）を参照してください。 ファイルルールは数値上の順番ではなく、ルールアクションの順番で評価されます。詳細については、ファイルルール アクション：評価順序 （42 ページ）を参照してください。

ファイル ルール アクション

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

ファイル ルール アクション

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

ファイル ルール アクションのオプション

選択したアクションに応じて、さまざまなオプションがあります。

ファイル ルール アクションのオプション	ファイルのブロックが可能か	マルウェアのブロックが可能か	ファイルの検出が可能か	マルウェア クラウド ルックアップが可能か
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	可
ローカル マルウェア分析（Local Malware Analysis）	No	Yes	No	可
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

* これらのオプションの詳細については、マルウェア防御オプション（ファイル ルール アクション） （35 ページ）およびそのサブトピックを参照してください。

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

マルウェア防御オプション（ファイル ルール アクション）

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

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

1. Spero 分析 （38 ページ）およびAMP クラウドのルックアップ （38 ページ）
2. ローカル マルウェア分析（Local Malware Analysis） （38 ページ）
3. 動的分析（Dynamic Analysis） （39 ページ）

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

（該当する場合は、そのファイル タイプに基づいてすべてのファイルをブロックすることもできます。詳細については、ファイル タイプによるすべてのファイルのブロック （42 ページ）を参照してください）。

（オプション）AMP for Endpoints を使用したマルウェア防御 （44 ページ）およびサブトピックからシスコの AMP for Endpoints 製品に関する情報も参照してください。

マルウェア防御のオプションの比較

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

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

分析タイプ	利点	制限事項	マルウェアの特定
ローカルマルウェア分析と動的分析	両方のタイプのファイル分析を使用することで詳細な結果が得られます	どちらか一方の場合よりも消費するリソースが多くなります	マルウェアの可能性があるとして事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。ローカル マルウェア分析でマルウェアが特定された場合、またはファイル ポリシーで設定されている脅威スコアしきい値に基づいて、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。
Spero 分析、ローカルマルウェア分析、および動的分析	詳細結果	3 つすべてのタイプのファイル分析を実行するため消費するリソースが最も多くなります	マルウェアの可能性があるとして事前分類されているファイルの場合、動的分析の結果に基づいて脅威スコアが変更されます。Spero 分析またはローカル マルウェア分析でマルウェアが特定された場合、またはファイル ポリシーで設定されている脅威スコアしきい値に基づいて、性質が [不明（Unknown）] から [マルウェア（Malware）] に変更されます。
（指定されたファイル タイプのすべてのファイルの送信をブロック）	マルウェア ライセンスは必要ありません （このオプションは技術的なマルウェア防御オプションではありません。）	正規ファイルもブロックされます	（分析は実行されません。）

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

Spero 分析

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

Spero 分析用にファイルを手動で送信することはできません。

AMP クラウドのルックアップ

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

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

ローカル マルウェア分析（*Local Malware Analysis*）

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

システムはローカルマルウェアによってマルウェアを識別すると、その既存のファイルの性質を [不明（Unknown）] から [マルウェア（Malware）] に更新します。その上で、システムは新しいマルウェア イベントを生成します。システムはマルウェアを識別しなかったとしても、ファイルの性質を [不明（Unknown）] から [正常（Clean）] に更新することはしません。ローカル マルウェア分析を実行した後、システムはファイル情報（SHA-256 ハッシュ値、タイムスタンプ、ファイルの性質など）をキャッシュに入れて、特定の期間内にそのファイルを再度検出した場合に再び分析を行わなくてもマルウェアを識別できるようにします。このキャッシュの詳細ついては、キャッシュ済み性質の有効期間 （38 ページ）を参照してください。

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

キャッシュ済み性質の有効期間

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

- クリーン：4 時間
- 不明：1 時間
- マルウェア：1 時間

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

動的分析（*Dynamic Analysis*）

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

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

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

必要に応じて、脅威スコアに基づいて AMP クラウド ファイルの性質を上書きするようにファイル ポリシーを設定することができます。

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

動的分析を実行するようにシステムを設定するには、動的分析接続 （15 ページ）のトピックを参照してください。

動的分析の対象となるファイル

動的分析用ファイルの対象は、次の条件によって異なります。

- ファイル タイプ
- ファイル サイズ
- ファイル ルールのアクション

さらに、次のパターンがあります。

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

- システムは潜在的なマルウェアとしてファイルを事前分類する必要があります。

動的分析とキャパシティ処理

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

8000 シリーズ デバイスの場合：デバイスはそのハード ドライブまたはマルウェア ストレージ パックにファイルを保存できます。マルウェア ストレージ パック（8000 シリーズ デバイスのみ）（41 ページ）も参照してください。

他のすべてのデバイス：デバイスはハード ドライブにファイルを保存します。

キャプチャされたファイルとファイル ストレージ

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

デバイスがファイルをキャプチャした後に、以下の選択肢があります。

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

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

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

システムがファイルをキャプチャするか保存するかに関わらず、以下が可能です。

- [分析（Analysis）] > [ファイル（Files）] > [キャプチャされたファイル（Captured Files）] からのキャプチャされたファイルに関する情報（動的分析のためにファイルが保存されたのか送信されたかどうか、ファイルの性質、脅威スコアなど）を確認することにより、ネットワーク上で検出されたマルウェアの潜在的な脅威について迅速に検討する。
- ファイルのトラジェクトリを表示して、ネットワークのトラバースの仕方およびコピーを保持しているホストを判別する。

- ファイルをクリーン リストまたはカスタム検出リストに追加することで、以後の検出時には常に、クリーンまたはマルウェアの判定結果を持つファイルとして扱う。

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

システム バックアップに保存ファイルは含まれません。

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

マルウェア ストレージ パック（8000 シリーズ デバイスのみ）

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

注意 Cisco から供給されたハード ドライブ以外はデバイスに取り付けないでください。サポートされていないハード ドライブを取り付けると、デバイスが破損する可能性があります。マルウェア ストレージ パック キットは、シスコから**のみ**購入でき、8000 シリーズ デバイスで**のみ**使用できます。マルウェア ストレージ パックのサポートが必要な場合は、サポートにお問い合わせください。詳細については、*Firepower* システム マルウェア ストレージ パック ガイドを参照してください。

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

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

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

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

ファイル タイプによるすべてのファイルのブロック

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

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

タイプに基づいてすべてのファイルをブロックすることは、技術的にはマルウェア防御機能ではありません。マルウェア ライセンスは不要であり、AMP クラウドにクエリしません。

ファイル ルール アクション：評価順序

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

ファイル ルール アクションの優先度は次のとおりです。

- ファイル ブロック（*Block Files*）
- マルウェア ブロック（*Block Malware*）
- マルウェア クラウド ルックアップ（*Malware Cloud Lookup*）
- ファイル検出（*Detect Files*）

設定されている場合、TID は、アクションの優先順位付けに影響を与えます。詳細については、TID-Firepower Management Center のアクションの優先順位付けを参照してください。

ファイル ルールの作成

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**）
脅威（ファイル制御） マルウェア（ネットワーク向け AMP）	Protection（ファイル制御） マルウェア（ネットワーク向け AMP）	任意（Any）	任意（Any）	Admin/Access Admin

⚠

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

始める前に

マルウェア保護のルールを設定する場合は、ファイル ポリシーの設定 （6 ページ）を参照してください。

手順

ステップ 1 ファイル ポリシー 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 （31 ページ）の説明に従って、[アプリケーション プロトコル（Application Protocol）] および [転送の宛先（Direction of Transfer）] を選択します。

ステップ 3 [ファイル タイプ（File Types）] を 1 つ以上選択します。

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

ファイル タイプのリストを、次のようにフィルタ処理できます。

- 1 つ以上の [ファイル タイプ カテゴリ（File Type Categories）] を選択し、[選択したカテゴリのすべてのタイプ（All types in selected Categories）] をクリックします。
- 名前または説明でファイル タイプを検索します。たとえば、Microsoft Windows 固有のファイルのリストを表示するには、[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：評価順序 （42 ページ）を確認し、ファイル ルール アクション （33 ページ）の説明に従ってファイル ルール [アクション（Action）] を選択します。

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

ステップ 5 選択したアクションに応じて、以下のオプションを設定します。

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

* これらのオプションの詳細については、ファイル ルール アクション （33 ページ）とマルウェア防御オプション（ファイル ルール アクション） （35 ページ）およびそのサブトピックを参照してください。

ステップ 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。

次のタスク

- マルウェア保護のポリシーを設定する場合は、ファイル ポリシーの設定 （6 ページ）を参照してください。
- 設定変更を展開します。設定変更の展開を参照してください。

レトロスペクティブな性質の変更

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

（オプション）AMP for Endpoints を使用したマルウェア防御

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

AMP for Endpoints はシスコのエンタープライズクラスの高度なマルウェア防御ソリューションです。個別ユーザのエンドポイント（コンピュータやモバイルデバイス）で軽量コネクタとし

て実行し、高度なマルウェアの発生、高度で継続的な脅威、およびターゲット型攻撃を検出、分析、ブロックします。

AMP for Endpoints の利点は次のとおりです。

- 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
- AMP for Endpoints 管理コンソールを使用してマルウェアの影響を軽減する。管理コンソールの堅牢かつ柔軟な Web インターフェイスを使用すると、エンドポイント向け 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。

AMP for Endpoints の詳細については、次の項目を参照してください。

- https://www.cisco.com/c/en/us/products/security/amp-for-endpoints/index.html。
- AMP for Endpoints 管理コンソールのオンライン ヘルプ。
- AMP for Endpoints のマニュアル入手先：http://docs.amp.cisco.com。

マルウェア防御の比較：Firepower と AMP for Endpoints

表 *4*：製品の検出による高度なマルウェア保護の違い

機能	Firepower Malware Protection（ネットワーク向け AMP）	AMP for Endpoints
ファイルタイプの検出とブロッキングの方法（ファイル制御）	ネットワーク トラフィックでアクセス コントロール ポリシーとファイル ポリシーを使用	未サポート
マルウェアの検出とブロッキングの方法	ネットワーク トラフィックでアクセス コントロール ポリシーとファイル ポリシーを使用	個々のエンドポイント（エンドユーザ コンピュータとモバイルデバイス）で AMP クラウドとの通信を行うコネクタを使用
ネットワーク トラフィックを検査	管理対象デバイスを通過するトラフィック	なし（エンドポイントにインストールされたコネクタがファイルを直接検査する）

機能	Firepower Malware Protection（ネットワーク向け AMP）	AMP for Endpoints
マルウェアインテリジェンスのデータソース	AMP クラウド（パブリックまたはプライベート）	AMP クラウド（パブリックまたはプライベート）
マルウェア検出の堅牢性	限定されたファイル タイプ	すべてのファイル タイプ
マルウェア分析の選択肢	FMC ベース、および AMP クラウドでの分析	FMC 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 ブロッキング、FMC 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、FMC が開始する修復
生成されるイベント	ファイルイベント、キャプチャされたファイル、マルウェアイベント、およびレトロスペクティブ マルウェア イベント	マルウェア イベント
マルウェア イベントに含まれる情報	基本的なマルウェアイベント情報、および接続データ（IP アドレス、ポート、アプリケーション プロトコル）	詳細なマルウェアイベント情報（接続データなし）
ネットワーク ファイル トラジェクトリ	FMC ベース	FMC と AMP for Endpoints の管理コンソールには、それぞれネットワーク ファイル トラジェクトリがあります。いずれも使用可能です。
必要なライセンスまたはサブスクリプション	とファイル制御の実行に必要なライセンス ネットワーク向け AMP	AMP for Endpoints サブスクリプション。FMC への AMP for Endpoints データの取り込みに必要なライセンスはありません。

Firepower と AMP for Endpoints の統合について

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

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

Firepower と AMP for Endpoints の統合の利点

AMP for Endpoints 展開を Firepower システムに統合すると、次のような利点があります。

- AMP for Endpoints で設定する中央集中型ブラックリストおよびホワイトリストによって、Firepower から AMP クラウドに送信されるファイル SHA の判定が決まります。

  AMP for Endpoints からの一元的なファイル リスト （27 ページ）を参照してください。

- システムは AMP for Endpoints によって検出されたマルウェア イベントを Firepower Management Center にインポートできるため、Firepower システムによって生成されたマルウェア イベントとともにこれらのイベントを管理できます。これらのイベントでインポートされたデータには、スキャン、マルウェア検出、隔離、ブロックされた実行、クラウドの呼び出し、およびモニタするホストに対して FMC が表示する侵害の兆候（IOC）が含まれます。

  詳細については、AMP for Endpoints を使用したマルウェア イベント分析を参照してください。

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

  詳細は、AMP for Endpoints コンソールでのイベント データの使用を参照してください。

重要 Cisco AMP プライベート クラウドを使用する場合は、AMP for Endpoints と AMP プライベート クラウド （47 ページ）の制限事項を参照してください。

AMP for Endpoints と AMP プライベート クラウド

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

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

AMP プライベート クラウドを使用する場合、次の統合機能は使用できません。AMP for Endpoints で設定されたブラックリストとホワイトリストの使用、Firepower から生成されたマルウェア イベントの AMP for Endpoints での表示。

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

Firepower と AMP for Endpoints の統合

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

組織がシスコの AMP for Endpoints 製品を展開している場合は、そのアプリケーションを Firepower と統合し、Firepower と AMP for Endpoints の統合の利点 （46 ページ）で説明されている利点を実現できます。

AMP for Endpoints と統合する場合、ネットワーク向け AMP （AMP for Firepower）接続がすでに設定されていても、AMP for Endpoints 接続を設定する必要があります。複数の AMP for Endpoints クラウド接続を設定できます。

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向けの AMP が生成したマルウェア 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。

ただし、AMP for Endpoints 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 AMP for Endpoints 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） AMP for Endpoints 接続が正しく登録されていなくても、ネットワーク向け AMP は影響を受けません。

始める前に

- 展開で Cisco AMP プライベートクラウドを使用している場合AMP for Endpoints と AMP プライベート クラウド （47 ページ）は、の制限事項を参照してください。
- ネットワークで AMP for Endpoints が設定されていて、正しく機能している必要があります。
- Firepower Management Center 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。
- FMC および AMP for Endpoints が相互に通信できることを確認します。セキュリティ、インターネット アクセス、および通信ポートのトピックを参照してください。
- 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に 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。
- この手順中に AMP for Endpoints コンソールにログインするには、AMP for Endpoints クレデンシャルが必要です。

手順

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

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

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

- Firepower Management Center の地理的な場所に最も近い AMP クラウド。

  APJC はアジア/太平洋/日本/中国です。

- AMP プライベート クラウド（AMPv）の場合、[プライベートクラウド（Private Cloud）] を選択し、Cisco AMP プライベート クラウド （11 ページ）の手順に進みます。

ステップ 4 このクラウドを ネットワーク向け AMP と AMP for Endpoints の両方に使用する場合は、[AMP for Firepowerに使用（Use for AMP for Firepower）] チェックボックスをオンにします。

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

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、ネットワーク向け AMP 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 FMC が受信するデータを制限する場合は、情報を受け取る組織内の特定のグループを選択します。

デフォルトでは、AMP クラウドはすべてのグループのデータを送信します。グループを管理するには、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 モ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、ネットワーク向け AMP 接続は無効になりません。

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

a) **[AMP]** > **[AMP Management]** ページで、[Cisco AMP ソリューション タイプ（Cisco AMP Solution Type）] 列に **`AMP for Endpoints`** が含まれている [クラウド名（Cloud Name）] をクリックします。

b) 表示される AMP for Endpoints コンソール ウィンドウで、[アカウント（Accounts）] > [アプリケーション（Applications）] を選択します。

c) Firepower Management Center が一覧に含まれていることを確認します。

d) AMP for Endpoints コンソール ウィンドウで、[管理（Manage）] > [コンピュータ（Computers）] を選択します。

e) Firepower Management Center が一覧に含まれていることを確認します。

次のタスク

- AMP for Endpoints コンソール ウィンドウで、必要に応じて設定を行います。たとえば、管理センターのグループ メンバーシップの定義や、ポリシーの割り当てを行います。詳細については、AMP for Endpoints のオンライン ヘルプまたはその他のドキュメントを参照してください。
- ハイ アベイラビリティの設定では、Firepower Management Center のアクティブ インスタンスとスタンバイ インスタンスで AMP クラウド接続を個別に設定する必要があります。これらの設定は同期されません。
- デフォルトのヘルス ポリシーは、Firepower Management Center から AMP for Endpoints への最初の接続が成功した後で接続できなくなった場合、または AMP ポータルを使って接続が登録解除された場合に警告を出します。

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

ファイルとマルウェアの履歴の章

機能	バージョン（Version）	詳細
章の再構成	再発行されたすべてのバージョンに適用されます	混乱を避けるため、この章の内容が再構成されました。 ファイル/マルウェア イベントとネットワーク ファイル トラジェクトリの章との間で一部の内容の移動がありました。
URLフィルタリング情報を新しいURLフィルタリングの章に移動しました。	6.3	URLフィルタリングのクラウド通信の設定に関する情報を新しい URL フィルタリングの章に移動しました。章内の Cisco CSI のトピックの構成に関連する変更を加えました。