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

次のトピックでは、ファイル/マルウェア イベント、ローカル マルウェア分析、動的分析、キャプチャされたファイル、およびネットワーク ファイル トラジェクトリの概要を示します。

ファイル イベント/マルウェア イベントとネットワーク ファイル トラジェクトリについて

ファイル ポリシーは、一致したトラフィックのファイル イベントおよびマルウェア イベントを自動的に生成し、キャプチャされたファイルの情報をログに記録します。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。このデータを分析して、悪影響に対処したり、将来の攻撃をブロックしたりすることができます。

ファイル分析結果に基づいて、キャプチャされたファイル、生成されたマルウェアとファイルイベントを、[分析（Analysis）]>[ファイル（Files）] メニューで使用可能なページの表を使用して確認することができます。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。

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ラジェクトリ（network file trajectory）]（さまざまなファイル プロパティに加え、ファイルがどのようにネットワークを通過し、ホスト間で渡されてきたかを示すマップ）を使用して、ホスト間での個々の脅威の広がりを時系列で追跡できます。これにより、最も効果的なアウトブレイク制御と防止対策に集中できます。

ファイル ルールでローカル マルウェア分析または動的分析を設定すると、システムによってルールに一致するファイルが事前分類され、ファイル構成レポートが生成されます。

組織で *AMP for Endpoints* が展開されていて、その展開が Firepower Management Center と統合されている場合は、その製品により、スキャン、マルウェア検出、および検疫のレコードと侵害の兆候（IOC）をインポートすることもできます。このデータは、ネットワーク上のマルウェアの全体像をより完全に把握するために、Firepower によって収集されたイベントデータとともに表示されます。

コンテキスト エクスプローラ、およびレポート機能を使用すると、検出/キャプチャ/ブロックされたファイルとマルウェアについてより詳しく理解できます。また、イベントを使用して相関ポリシー違反をトリガーしたり、電子メール、SMTP、または syslog によるアラートを発行したりすることもできます。

（注） マルウェアを検出し、ファイル イベントおよびマルウェア イベントを生成するようにシステムを設定するには、ファイル ポリシーと高度なマルウェア防御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

Firepower Management Center は、さまざまなタイプのファイルおよびマルウェア イベントをログに記録できます。個々のイベントに関する情報は、イベントの生成方法と生成理由に応じて異なります。

- ファイルイベントとは、Firepower システム（ネットワーク向け AMP）によって検出されたマルウェアを含むファイルを意味します。ファイル イベントには、AMP for Endpoints 関連のフィールドは含まれません。
- マルウェア イベントとは、ネットワーク向け AMP または AMP for Endpoints によって検出されたマルウェアを意味します。また、マルウェア イベントは、スキャンや検疫など、AMP for Endpoints の導入からの脅威以外のデータを記録できます。
- レトロスペクティブ マルウェア イベントとは、性質（ファイルがマルウェアかどうか）が変更された、ネットワーク向け AMP によって検出されたファイルを意味します。

（注）

- ネットワーク向け AMP によってマルウェアとして識別されたファイルは、ファイル イベントとマルウェア イベントの両方を生成します。エンドポイント向けの AMP によって生成されたマルウェア イベントは対応するファイル イベントを持っていません。
- NetBIOS-ssn（SMB）トラフィックの検査によって生成されるファイル イベントは、即座には接続イベントを生成しません。これは、クライアントとサーバが持続的接続を確立するためです。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。
- Firepower システムでは、Unicode（UTF-8）文字を使用するファイル名の表示および入力がサポートされます。ただし、Unicode のファイル名は PDF レポートに変換された形式で表示されます。また、SMB プロトコルによって、ファイル名の印刷不能な文字がピリオドに置き換えられます。

ファイル イベントおよびマルウェア イベントの種類

ファイル イベント

システムは、現在展開されているファイル ポリシーのルールに従って、管理対象デバイスがネットワーク トラフィック内のファイルを検出またはブロックしたときに生成されたファイル イベントを記録します。

システムがファイル イベントを生成する際に、呼び出しを行うアクセス コントロール ルールのログ設定に関係なく、システムは Firepower Management Center データベースへの関連する接続の終わりも記録します。

マルウェア イベント（Malware Events）

Firepower システム（特に ネットワーク向け AMP の機能）は、全体的なアクセス コントロール設定の一部としてネットワーク トラフィック内のマルウェアを検出すると、マルウェア イベントを生成します。マルウェアイベントには、結果として生じたイベントの性質や、いつどこでどのようにしてマルウェアが検出されたかに関するコンテキスト データが含まれます。

表 *1*: でのマルウェア イベントの生成シナリオ

システムがファイルを検出し、次の状態になった場合	性質
AMP クラウドにファイルの性質についてクエリを行い（マルウェア クラウド ルックアップを実行）、クエリに成功した場合	マルウェア、クリーン、または不明
AMP クライドにクエリを行ったものの、接続を確立できないか、他の理由でクライドが利用可能でない場合	応対不可 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。

システムがファイルを検出し、次の状態になった場合	性質
ファイルに関連付けられている脅威スコアが、ファイルを検出したファイル ポリシーで定義されたマルウェアしきい値の脅威スコアを超えた場合、またはローカルマルウェア分析でマルウェアが識別された場合	マルウェア
ファイルがカスタム検出リストに設定されている場合（手動でマルウェアとしてマークされている場合）	カスタム検出
ファイルがクリーン リストに設定されている場合（手動でクリーンとしてマークされている場合）	クリーン

レトロスペクティブ マルウェア イベント

ネットワーク トラフィックで検出されたマルウェアの場合、性質が変わることがあります。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。先週クエリしたファイルの性質が変わると、AMP クラウドがシステムに通知します。その場合、以下の 2 つが行われます。

- Firepower Management Centerが新しい遡及的マルウェア イベントを生成します。

  この新しい遡及的マルウェア イベントは、前の週に検出され、同じ SHA-256 ハッシュ値を持つ同じすべてのファイルの性質変更を表します。そのため、これらのイベントには限られた情報（Firepower Management Centerに性質変更が通知された日時、新しい性質、ファイルの SHA-256 ハッシュ値、および脅威名）が含まれます。IP アドレスや他のコンテキスト情報は含まれません。

- Firepower Management Centerは遡及的イベントの関連する SHA-256 ハッシュ値を持つ既に検出済みのファイルのファイル性質を変更します。

  ファイルの性質が Malware に変更されると、Firepower Management Centerは新しいマルウェア イベントをデータベースに記録します。新しい性質を除き、この新しいマルウェア イベントの情報は、ファイルが最初に検出されたときに生成されたファイルイベントのものと同じです。

  ファイルの性質が [クリーン（Clean）] に変更された場合、Firepower Management Center はそのマルウェアイベントを削除しません。代わりに、イベントに性質の変更が反映されます。つまり、マルウェア テーブルには性質が [クリーン（Clean）] のファイルが含められることがありますが、それはそのファイルが最初マルウェアと識別されていた場合だけです。マルウェアとして識別されたことのないファイルは、ファイルのテーブルにのみ含められます。

エンドポイント向け AMP によって生成されたマルウェア イベント

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。コネクタでは、アップロード、ダウンロード、実行、オープン、コピー、移動などのときにファイルを検査できます。検査対象のファイルにマルウェアが含まれるかどうかを判断するために、これらのコネクタは AMP クラウドと通信します。

ファイルがマルウェアとして識別された場合、AMP クラウドは脅威の特定情報を 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。

（注） エンドポイント向け AMP によって生成されたマルウェア イベントで報告される IP アドレスは、ネットワーク マップに（および監視対象ネットワークにも）含まれない場合もあります。展開、コンプライアンスのレベル、およびその他の要因によっては、AMP for Endpoints によってモニタされる組織内のエンドポイントが、ネットワーク向け AMP によってモニタされているものと同じホストではない可能性があります。

AMP for Endpoints を使用したマルウェア イベント分析

組織で Cisco AMP for Endpoints を導入している場合は、次のことができます。

- AMP for Endpoints によって検出されたマルウェア イベントを、AMP for Networks によって検出されたイベントとともに Firepower Management Center のイベント ページに表示するようにシステムを設定できます。
- AMP パブリック クラウドを使用している場合は、AMP for Endpoints の特定の SHA に関するファイル トラジェクトリやその他の情報を表示できます。

上記の機能を設定するには、Firepower と AMP for Endpoints の統合を参照してください。

AMP for Endpoints からのイベントデータ

組織でマルウェア防御のために AMP for Endpoints を導入している場合は、AMP for Endpoints からのファイルデータおよびマルウェア データを使用した作業を FMC 上で行えるようにシステムを設定できます。

ただし、AMP for Endpoints からのファイル データおよびマルウェア データと ネットワーク向け AMP （Firepower システムを使用したマルウェア防御）のファイル データおよびマルウェア データとの相違点に注意する必要があります。

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、エンドポイントの AMP によって検出されたマルウェア 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。

その他にも、ネットワークベースの AMP によって検出されたマルウェア イベント（「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） 展開に応じて、AMP for Endpoints によってモニタされるエンドポイントは AMP for Networks でモニタされるものと同じホストにならない場合があります。このため、エンドポイント向け AMP によって生成されたマルウェア 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、マルウェア ライセンスを使用する場合に Firepower によって生成されるイベントデータと、AMP for Endpoints によって生成されるイベントデータの違いを要約します。

表 *2 : AMP* 製品間のデータの相違点の要約

機能	ネットワーク向け AMP	エンドポイント向け AMP
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。

関連項目

Firepower と AMP for Endpoints の統合

ファイルおよびマルウェア イベントのワークフローの使用

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数	サポートされるドメイン数	アクセス
機能に応じて異なる	機能に応じて異なる	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

次の手順を使用して、テーブル内のファイルおよびマルウェア イベントを表示し、分析に関連する情報に基づいてイベント ビューを操作します。イベントにアクセスしたときに表示されるページは、ワークフローによって異なります。ワークフローは、大まかなビューから詳細なビューに移動してイベントを評価するために使用できる、一連のページです。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

次のいずれかを実行します。

- **[Analysis]** > **[Files]** > **[File Events]**
- **[Analysis]** > **[Files]** > **[Malware Events]**

ヒント イベントのテーブル ビューでは、一部のフィールドがデフォルトで非表示にされています。イベント ビューに非表示フィールドを表示するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のフィールド名をクリックします。

ヒント 特定のファイルが検出された接続をすぐに表示するには、テーブルでチェックボックスを使用してファイルを選択してから、[ジャンプ（Jump to）] ドロップダウン リストで [接続イベント（Connections Events）] を選択します。

ヒント オプションを表示するには、テーブル内の項目を右クリックします（オプションが表示されない列もあります）。

関連トピック

ファイルおよびマルウェア イベント フィールド （7 ページ）
定義済みファイルのワークフロー
定義済みマルウェアのワークフロー
イベント ビュー設定の設定

ファイルおよびマルウェア イベント フィールド

ワークフローを使用して表示および検索できるマルウェア イベントには、このセクションにリストするフィールドがあります。個別のイベントで利用可能な情報は、いつ、どのように生成されたかによって異なることに注意してください。

（注） ネットワーク向けAMP によってマルウェアとして識別されたファイルは、ファイルイベントとマルウェア イベントの両方を生成します。エンドポイント向け AMP によって生成されたマルウェア イベントには対応するファイル イベントはありません。また、ファイル イベントにはエンドポイント向け AMP 関連のフィールドはありません。

syslog メッセージにはメッセージに初期値が入力され、たとえば、レトロスペクティブな判定などでFMC Webインターフェイスの同等なフィールドが更新されたとしても更新されません。

[アクション（Action）]（syslog：FileAction）

ファイルを検出したファイル ポリシー ルールに関連したアクション、および関連するファイル アクション オプション。

AMP クラウド（AMP Cloud）

AMP for Endpoints イベントが発信された AMP クラウドの名前。

アプリケーション ファイル名（Application File Name）

AMP for Endpoints 検出が行われたときに、マルウェア ファイルにアクセスしていたクライアントアプリケーション。これらのアプリケーションはネットワーク検出またはアプリケーション制御とは関係**ありません**。

アプリケーション ファイル SHA256（Application File SHA256）

検出が行われたときに、AMP for Endpoints で検出された、または隔離されたファイルにアクセスした親ファイルの SHA-256 のハッシュ値。

[アプリケーション プロトコル（Application Protocol）]（syslog：ApplicationProtocol）

管理対象デバイスがファイルを検出したトラフィックで使用されるアプリケーションプロトコル。

アプリケーション プロトコル カテゴリまたはタグ（Application Protocol Category or Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

[アプリケーションのリスク（Application Risk）]

接続で検出されたアプリケーション トラフィックに関連するリスク：Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、関連するリスクがあります。このフィールドでは、それらのうち最も高いものが表示されます。

[アーカイブの深さ（Archive Depth）]（syslog：ArchiveDepth）

アーカイブ ファイル内でファイルがネストされたレベル（存在する場合）。

[アーカイブ名（Archive Name）]（syslog：ArchiveFileName）

マルウェア ファイルが含まれていたアーカイブ ファイル（ある場合）の名前。

アーカイブ ファイルの内容を表示するには、[分析（Analysis）] >[ファイル（Files）] にある、アーカイブ ファイルの一覧が表示されるいずれかのテーブルに移動し、アーカイブ ファイルのテーブルの行を右クリックしてコンテキスト メニューを開いてから、[アーカイブの内容の表示（View Archive Contents）] をクリックします。

[SHA256 のアーカイブ（Archive SHA256）]（syslog：ArchiveSHA256）

マルウェア ファイルを含むアーカイブ ファイル（ある場合）の SHA-256 ハッシュ値。

アーカイブ ファイルの内容を表示するには、[分析（Analysis）]>[ファイル（Files）] にある、アーカイブ ファイルの一覧が表示されるいずれかのテーブルに移動し、アーカイブ ファイルのテーブルの行を右クリックしてコンテキスト メニューを開いてから、[アーカイブの内容の表示（View Archive Contents）] をクリックします。

ArchiveFileStatus（syslog のみ）

調査中のアーカイブのステータス。次のいずれかの値になります。

- [保留中（Pending）]：アーカイブは調査中です
- [取得済み（Extracted）]：調査が問題なく正常に実行されました
- [失敗（Failed）]：システムのリソース不足のため調査に失敗しました。
- [深度の超過（Depth Exceeded）]：調査は正常に実行されましたが、アーカイブがネストされた調査の深度を超過しました
- [暗号化（Encrypted）]：部分的に正常に実行されましたが、アーカイブが暗号化されているか、暗号化されたアーカイブが含まれています
- [調査できませんでした（Not Inspectable）]：部分的に正常に実行されましたが、ファイルは形式が不正であるか破損しています

ビジネスとの関連性（Business Relevance）

接続で検出されたアプリケーション トラフィックに関連するビジネス関連性：Very High、High、Medium、Low、または Very Low。接続で検出されたアプリケーションのタイプごとに、関連するビジネスとの関連性があります。このフィールドでは、それらのうち最も低いもの（関連が最も低い）が表示されます。

カテゴリ（Category）/ファイル タイプ カテゴリ（File Type Category）

ファイルタイプの一般的なカテゴリ（Office ドキュメント、アーカイブ、マルチメディア、実行可能ファイル、PDF ファイル、エンコード ファイル、グラフィック、システム ファイルなど）。

[クライアント（Client）]（syslog：Client）

1 つのホストで実行され、ファイルを送信するためにサーバに依存するクライアント アプリケーション。

クライアント カテゴリまたはタグ（Client Category or Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

（Syslog のみ）

ある接続と別の同時接続を区別するカウンタ。このフィールドは、それ自体には意味がありません。

[Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定のファイルまたはマルウェアイベントに関連付けられた接続イベントを一意に識別できます。

（Syslog のみ）

接続イベントを処理した Snort インスタンス。このフィールドは、それ自体には意味がありません。

[Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定のファイルまたはマルウェアイベントに関連付けられた接続イベントを一意に識別できます。

メンバー数（Count）

複数の同じ行を作成する制約を適用した後の、各行の情報に一致するイベントの数。

検出名（Detection Name）

検出されたマルウェアの名前。

ディテクタ（Detector）

マルウェアを識別した AMP for Endpoints ディテクタ（ClamAV、Spero、SHA など）。

Device

ネットワーク向け AMP によって生成されたファイル イベントとマルウェア イベントの場合は、ファイルを検出したデバイスの名前。

エンドポイント向け AMP によって生成されたマルウェア イベントと AMP クラウドによって生成されたレトロスペクティブ マルウェア イベントの場合は、Firepower Management Center の名前。

[後処理/ファイルの後処理（Disposition / File Disposition）]（syslog：SHA_Disposition）

ファイルの性質：

マルウェア（Malware）

AMP クラウドでそのファイルがマルウェアとして分類された、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、またはファイル ポリシーで定義されたマルウェアしきい値をファイルの脅威スコアが超えたことを示します。

[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。クリーンのファイルがマルウェア テーブルに含められるのは、そのファイルがクリーンに変更された場合だけです。

[不明（Unknown）]

システムが AMP クラウドに問い合わせましたが、ファイルの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正しく分類していませんでした。

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。

[応対不可（Unavailable）]

システムがAMPクラウドに問い合わせできなかったことを示します。この性質に関するイベントが、わずかながら存在する可能性があります。これは予期された動作です。

[該当なし（N/A）]

[ファイル検出（Detect Files）] または [ファイル ブロック（Block Files）] ルールがファイルを処理し、Firepower Management Center が AMP クラウドに問い合わせなかったことを示します。

ファイルの後処理は、システムが AMP クラウドにクエリを実行したファイルについてのみ表示されます。

syslog フィールドには最初の後処理のみが反映されます。レトロスペクティブな判定を反映するようには更新されません。

ドメイン

ネットワーク向け AMP によって生成されたファイル イベントとマルウェア イベントの場合は、ファイルを検出したデバイスのドメイン。エンドポイント向け AMP によって生成されたマルウェア イベントおよびAMP クラウドによって生成される遡及的マルウェア イベントの場合、イベントを報告した AMP クラウド接続に関連付けられたドメイン。

This field is only present if you have ever configured the Firepower Management Center for multitenancy.

DstIP（syslog のみ）

接続に応答したホストの IP アドレス。これは、FileDirection フィールドの値によってファイルの送信者または受信者の IP アドレスとなる場合があります。

FileDirection が **`Upload`** の場合、これはファイル受信者の IP アドレスです。

FileDirection が **`Download`** の場合、これはファイル送信者の IP アドレスです。

SrcIP も参照してください。

DstPort（syslog のみ）

DstIP で説明されている接続で使用されるポート。

イベント サブタイプ（Event Subtype）

マルウェア検出につながった AMP for Endpoints アクション（[作成（Create）]、[実行（Execute）]、[移動（Move）]、[スキャン（Scan）] など）。

イベント タイプ（Event Type）

マルウェア イベントのサブタイプ。

[ファイル名（File Name）]（syslog：FileName）

ファイルの名前。

ファイル パス（File Path）

AMP for Endpoints によって検出されたマルウェア ファイルのファイル パス（ファイル名を含まない）。

[ファイル ポリシー（File Policy）]（syslog：FilePolicy）

ファイルを検出したファイル ポリシー。

[ファイル ストレージ/保存済み（File Storage / Stored）]（syslog：FileStorageStatus）

イベントに関連付けられたファイルのストレージ ステータス：

保存（Stored）

関連するファイルが現在保存されているすべてのイベントを返します。

関連保存（Stored in connection）

関連するファイルが現在保存されているかどうかに関係なく、関連するファイルをシステムがキャプチャおよび保存したすべてのイベントを返します。

失敗しました（Failed）

関連するファイルをシステムが保存できなかったすべてのイベントを返します。

syslog フィールドには、初期のステータスのみが含まれています。これらのステータスは変更後のステータスを反映するようには更新されません。

ファイルのタイムスタンプ（File Timestamp）

AMP for Endpoints が検出したマルウェア ファイルが作成された日時。

FileDirection（syslog のみ）

接続中にファイルがダウンロードされたか、またはアップロードされたか。値は次のとおりです。

- Download：ファイルは DstIP から SrcIP に転送されました。
- Upload：ファイルは SrcIP から DstIP に転送されました。

FileSandboxStatus（syslog のみ）

ファイルが動的分析のために送信されたかとその場合のステータスを示します。

（Syslog のみ）

システムが最初のパケットを検出した時間。

[Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定のファイルまたはマルウェアイベントに関連付けられた接続イベントを一意に識別できます。

FirstPacketSecond（syslog のみ）

ファイルのダウンロード フローまたはアップロード フローが開始された時刻。

イベントが発生した時刻がメッセージ ヘッダーのタイムスタンプにキャプチャされます。

HTTP 応答コード（HTTP Response Code）

ファイルの転送時にクライアントの HTTP 要求に応じて送信される HTTP ステータス コード。

IOC

マルウェア イベントが、接続に関与したホストに対する侵入の痕跡（IOC）をトリガーしたかどうか。AMP for Endpoints データが IOC ルールをトリガーした場合、タイプ AMP IOC で、完全なマルウェア イベントが生成されます。

メッセージ（Message）

マルウェア イベントに関連付けられる追加情報。ファイル イベントおよびネットワーク向け AMP によって生成されたマルウェア イベントでは、このフィールドは、後処理が変更された、つまり関連付けられたレトロスペクティブ イベントがあるファイルに対してのみ入力されます。

Protocol（syslog のみ）

接続に使用されたプロトコル（TCP や UDP など）。

受信側の大陸（Receiving Continent）

ファイルを受信するホストの大陸。

受信側の国（Receiving Country）

ファイルを受信するホストの国。

受信側 IP（Receiving IP）

FMC の Web インターフェイスでは、次のようになります。

ファイルイベントおよびネットワーク向け AMP によって生成されたマルウェア イベントの場合、ファイルを受信するホストの IP アドレス。

エンドポイント向け AMP によって生成されたマルウェアのイベントの場合、コネクタがイベントを報告したエンドポイントの IP アドレス。

同等な syslog については（ネットワーク向け AMP のみ）、 **DstIP** と **SrcIP** を参照してください。

受信側のポート（Receiving Port）

FMC の Web インターフェイスでは、次のようになります。

ファイルが検出されたトラフィックによって使用される宛先ポート。

Syslog と同等なものについては、**DstIP** および **SrcIP** と **DstPort** および **SrcPort** を参照してください。

[セキュリティ コンテキスト（Security Context）]（syslog：Context）

トラフィックが通過した仮想ファイアウォール グループを識別するメタデータ。複数のコンテキスト モードで実行している 1 台以上の ASA FirePOWER デバイスを管理する場合、システムはこのフィールドのみを表示します。

送信側の大陸（Sending Continent）

ファイルを送信するホストの大陸。

送信側の国（Sending Country）

ファイルを送信するホストの国。

送信側 IP（Sending IP）

FMC の Web インターフェイス：ファイルを送信するホストの IP アドレス。

同等な syslog については、 **DstIP** と **SrcIP** を参照してください。

送信側のポート（Sending Port）

FMC の Web インターフェイスでは、次のようになります。

ファイルが検出されたトラフィックによって使用される送信元ポート。

同等な syslog については、**DstIP** および **SrcIP** と **DstPort** および **SrcPort** を参照してください。

（Syslog のみ）

イベントを生成した Firepower デバイスの一意の識別子。

[Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、特定のファイルまたはマルウェアイベントに関連付けられた接続イベントを一意に識別できます。

[SHA256/ファイル SHA256/（SHA256/File SHA256）]（syslog：FileSHA256）

ファイルの SHA-256 ハッシュ値。

SHA256 値を得るには、ファイルが次のいずれかによって処理されている必要があります。

- [ファイルの保存（Store files）] が有効になっているファイル検出ファイル ルール。
- [ファイルの保存（Store files）] が有効になっているファイル ブロック ファイル ルール。
- マルウェア クラウド ルックアップ ファイル ルール
- マルウェア ブロック ファイル ルール
- AMP for Endpoints

また、この列には最後に検出されたファイルイベントおよびファイルの後処理を表し、ネットワーク ファイル トラジェクトリにリンクするネットワーク ファイル トラジェクトリ アイコンも表示されます。

[サイズ（KB）/ファイル サイズ（KB）（Size (KB) / File Size (KB)）]（syslog：FileSize）

FMC の Web インターフェイス：ファイルのサイズ（バイト単位）。

In syslog messages: The size of the file, in bytes.

ファイルが完全に受信される前にシステムがファイルのタイプを特定した場合は、ファイルサイズが計算されない場合があります。この状況では、このフィールドは空白です。

SperoDisposition(Syslog のみ)

SPERO 署名がファイル分析で使用されたかどうかを示します。有効な値：

- ファイルで実行された Spero の検出
- ファイルで実行されなかった Spero の検出

SrcIP（syslog のみ）

接続を開始したホストの IP アドレス。これは、FileDirection フィールドの値によってファイルの送信者または受信者の IP アドレスとなる場合があります。

FileDirection が **`Upload`** の場合、これはファイル送信者の IP アドレスです。

FileDirection が **`Download`** の場合、これはファイル受信者の IP アドレスです。

DstIP も参照してください。

SrcPort（syslog のみ）

SrcIP で説明されている接続で使用されるポート。

[SSL の実際のアクション（SSL Actual Action）]（syslog：SSLActualAction）

システムが暗号化されたトラフィックに適用したアクション。

[ブロック（Block）] または [リセットしてブロック（Block with reset）]

ブロックされた暗号化接続を表します。

[復号（再署名）（Decrypt (Resign)）]

再署名サーバ証明書を使用して復号された発信接続を表します。

[復号（キーの交換）（Decrypt (Replace Key)）]

置き換えられた公開キーと自己署名サーバ証明書を使用して復号化された発信接続を表します。

[復号（既知のキー）（Decrypt (Known Key)）]

既知の秘密キーを使用して復号化された着信接続を表します。

[デフォルトアクション（Default Action）]

接続がデフォルト アクションによって処理されたことを示します。

[復号しない（Do not Decrypt）]

システムが復号化しなかった接続を表します。

フィールド値は、検索ワークフロー ページの [SSL ステータス（SSL Status）] フィールドに表示されます。

[SSL 証明書情報（SSL Certificate Information）]

トラフィックを暗号化するための公開キー証明書に保存される次の情報：

- サブジェクト/発行元共通名（Subject/Issuer Common Name）
- サブジェクト/発行元組織（Subject/Issuer Organization）
- サブジェクト/発行元組織単位（Subject/Issuer Organization Unit）
- 有効期間（Not Valid Before/After）
- シリアル番号（Serial Number）、証明書フィンガープリント（Certificate Fingerprint）
- 公開キー フィンガープリント（Public Key Fingerprint）

syslog の場合は、**SSLCertificate** を参照してください。

[SSL 失敗の理由（SSL Failure Reason）]（syslog：SSLFlowStatus）

システムが暗号化されたトラフィックの復号化に失敗した理由。

- 不明
- No Match
- Success
- Uncached Session
- 不明な暗号スイート
- サポートされていない暗号スイート
- Unsupported SSL Version
- SSL Compression Used
- Session Undecryptable in Passive Mode
- Handshake Error
- Decryption Error
- Pending Server Name Category Lookup
- Pending Common Name Category Lookup
- Internal Error
- Network Parameters Unavailable
- Invalid Server Certificate Handle
- Server Certificate Fingerprint Unavailable
- Cannot Cache Subject DN
- Cannot Cache Issuer DN
- Unknown SSL Version
- External Certificate List Unavailable
- External Certificate Fingerprint Unavailable
- Internal Certificate List Invalid
- Internal Certificate List Unavailable
- Internal Certificate Unavailable
- Internal Certificate Fingerprint Unavailable
- Server Certificate Validation Unavailable
- Server Certificate Validation Failure
- 無効なアクション（Invalid Action）

フィールド値は、検索ワークフローのページの [SSL ステータス（SSL Status）] フィールドに表示されます。

SSL ステータス（SSL Status）

暗号化接続をログに記録した [SSL の実際のアクション（SSL Actual Action）]（SSL ルール、デフォルトのアクション、または復号化できないトラフィック アクション）に関連付けられているアクション。ロック アイコン（  ）は、TLS/SSL 証明書の詳細にリンクしています。証明書を利用できない場合（たとえば、TLS/SSL ハンドシェイク エラーにより接続がブロックされる場合）、ロック アイコンはグレー表示になります。

システムが暗号化接続を復号できなかった場合は、[SSL の実際の動作（SSL Actual Action）]（実行された復号不能のトラフィック アクション）と、[SSL 失敗理由（SSL Failure Reason）] が表示されます。たとえば、不明な暗号スイートによって暗号化されたトラフィックをシステムが検出し、それ以上のインスペクションをせずにこれを許可した場合、このフィールドには [Do Not Decrypt (Unknown Cipher Suite)] が表示されます。

このフィールドを検索する場合は、[SSL の実際の動作（SSL Actual Action）] と [SSL 失敗理由（SSL Failure Reason）] の 1 つ以上の値を入力し、システムが処理した、または復号に失敗した暗号化トラフィックを表示します。

[SSL 件名/発行者の国（SSL Subject/Issuer Country）]

暗号化証明書に関連付けられた件名または発行元国の 2 文字の ISO 3166-1 alpha-2 国番号。

SSLCertificate（syslog のみ）

TLS/SSL サーバの証明書のフィンガープリント。

[脅威の名前（Threat Name）]（syslog：ThreatName）

検出されたマルウェアの名前。

[脅威スコア（Threat Score）]（syslog：ThreatScore）

このファイルに関連付けられている最新の脅威スコア。これは、動的分析中に観察された悪意がある可能性がある動作に基づいた 0 ～ 100 の値です。

脅威スコア アイコンは、[動的分析要約（Dynamic Analysis Summary）] レポートにリンクされています。

時刻（Time）

イベントが生成された日時。このフィールドは検索できません。

syslog メッセージでは、 **FirstPacketSecond** を参照してください。

[タイプ/ファイル タイプ（Type/File Type）]（syslog：FileType）

ファイルのタイプ（HTML や MSEXE など）。

[URI/ファイルURI（URI/File URI）]（syslog：URI）

ファイル トランザクションに関連付けられている接続のURI。たとえば、ユーザがファイルをダウンロードした URL など。

[ユーザ（User）]（syslog：User）

FMC の Web インターフェイスでは、次のようになります。

イベントが発生したホストに関連付られているユーザ名（**Receiving IP**）。

syslog メッセージでは、次のようになります。

ファイルをダウンロードした内部ホストに関連付けられているユーザ名。

ファイルイベントおよびネットワーク向けAMPによって生成されたマルウェア イベントの場合、このユーザはネットワーク検出によって判別されます。ユーザは宛先ホストに関連付けられているため、内部ホストがマルウェア ファイルをアップロードしたマルウェア イベントにユーザは関連付けられません。

エンドポイント向け AMP によって生成されたマルウェア イベントの場合、エンドポイント向け AMP がユーザ名を判別します。これらのユーザをユーザ検出または制御に関連付けることは**できません**。それらは [ユーザ（Users）] テーブルに含まれず、それらのユーザの詳細を表示することもできません。

[Web アプリケーション（Web Application）]（syslog：WebApplication）

接続で検出されたHTTPトラフィックについて、内容を表すまたはURLを要求したアプリケーション。

Web アプリケーションのカテゴリまたはタグ（Web Application Category or Tag）

アプリケーションの機能を理解するのに役立つ、アプリケーションの特性を示す基準。

マルウェア イベントのサブタイプ

次の表に、マルウェア イベントのサブタイプ、そのサブタイプは AMP for Networks によって生成されたマルウェア イベント（「ネットワークベースのマルウェア イベント」）または AMP for Endpoints によって生成されたマルウェア イベント（「エンドポイントベースのマルウェア イベント」）のどちらに該当するか、また、そのサブタイプを使用してネットワーク ファイル トラジェクトリが構築されるかどうかを一覧で示します。

表 *3*：マルウェア イベントのタイプ

マルウェア イベントのサブタイプ/検索値	ネットワーク向け AMP	エンドポイント向け AMP	ファイル トラジェクトリ
ネットワーク ファイル転送時に検出された脅威（Threat Detected in Network File Transfer）	はい	いいえ	はい

マルウェア イベントのサブタイプ/検索値	ネットワーク向け **AMP**	エンドポイント向け **AMP**	ファイル トラジェクトリ
ネットワーク ファイル転送時に検出された脅威（遡及的）（Threat Detected in Network File Transfer (retrospective)）	はい	いいえ	はい
検出された脅威（Threat Detected）	いいえ	はい	はい
除外項目内で検出された脅威（Threat Detected in Exclusion）	いいえ	はい	はい
検疫された脅威（Threat Quarantined）	いいえ	はい	はい
AMP IOC（侵害の兆候）（AMP IOC (Indications of compromise)）	いいえ	はい	いいえ（No）
ブロックされた実行（Blocked Execution）	いいえ	はい	いいえ（No）
隔離のクラウドリコール（Cloud Recall Quarantine）	いいえ	はい	いいえ（No）
隔離のクラウドリコールの試行に失敗（Cloud Recall Quarantine Attempt Failed）	いいえ	はい	いいえ（No）
隔離のクラウドリコールの開始（Cloud Recall Quarantine Started）	いいえ	はい	いいえ（No）
隔離からのクラウドリコールの復元（Cloud Recall Restore from Quarantine）	いいえ	はい	いいえ（No）
隔離からのクラウドリコールの復元に失敗（Cloud Recall Restore from Quarantine Failed）	いいえ	はい	いいえ（No）

マルウェア イベントのサブタイプ/検索値	ネットワーク向け AMP	エンドポイント向け AMP	ファイル トラジェクトリ
隔離からのクラウドリコールの復元の開始（Cloud Recall Restore from Quarantine Started）	いいえ	はい	いいえ（No）
隔離エラー（Quarantine Failure）	いいえ	はい	いいえ（No）
隔離されたアイテムの復元（Quarantined Item Restored）	いいえ	はい	いいえ（No）
隔離の復元に失敗（Quarantine Restore Failed）	いいえ	はい	いいえ（No）
隔離の復元の開始（Quarantine Restore Started）	いいえ	はい	いいえ（No）
スキャン完了、検出なし（Scan Completed, No Detections）	いいえ	はい	いいえ（No）
スキャンが検出ありで完了（Scan Completed With Detections）	いいえ	はい	いいえ（No）
スキャンに失敗（Scan Failed）	いいえ	はい	いいえ（No）
スキャン開始（Scan Started）	いいえ	はい	いいえ（No）

ファイルおよびマルウェア イベント フィールドで利用可能な情報

次の表に、システムが各ファイルおよびマルウェア イベント フィールドの情報を表示するかどうかを示します。

組織で AMP for Endpoints が導入されていて、その製品を Firepower 展開と統合している場合は、次のようになります。

- エンドポイント向け AMP の展開からインポートされたマルウェア イベントと侵害の兆候（IOC）には、コンテキスト接続情報は含まれていませんが、ダウンロード時または実行時に取得された情報（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）が含まれています。
- ファイル イベント テーブル ビューには、エンドポイント向け AMP 関連のフィールドは表示されません。

表 *4:* ファイルおよびマルウェア イベント フィールドで利用可能な情報

フィールド	ファイル イベント	**Firepower** システムによって検出されたマルウェア イベント	**Firepower** システムによって検出されたレトロスペクティブイベント	**AMP for Endpoints** によって検出されたマルウェア イベント
Action	はい	はい	はい	いいえ（No）
AMP クラウド（AMP Cloud）	いいえ	いいえ	いいえ	はい
アプリケーションファイル名（Application File Name）	いいえ	いいえ	いいえ	はい
アプリケーションファイル SHA256（Application File SHA256）	いいえ	いいえ	いいえ	はい
アプリケーションプロトコル	はい	はい	いいえ	いいえ
アプリケーションプロトコルカテゴリまたはタグ（Application Protocol Category or Tag）	はい	はい	はい	いいえ（No）
Application Risk	はい	はい	はい	いいえ（No）
アーカイブ深度（Archive Depth）	はい	はい	いいえ	はい
アーカイブ名（Archive Name）	はい	はい	いいえ	はい
アーカイブ SHA256（Archive SHA256）	はい	はい	いいえ	はい
ビジネス関連性	はい	はい	はい	いいえ（No）
カテゴリ/ファイル タイプ カテゴリ（Category / File Type Category）	はい	はい	いいえ	はい
クライアント	はい	はい	はい	いいえ（No）

フィールド	ファイル イベント	**Firepower** システムによって検出されたマルウェア イベント	**Firepower** システムによって検出されたレトロスペクティブイベント	**AMP for Endpoints** によって検出されたマルウェア イベント
クライアントカテゴリまたはタグ（Client Category or Tag）	はい	はい	はい	いいえ（No）
Count	はい	はい	はい	はい
検出名（Detection Name）	いいえ	はい	いいえ	いいえ
ディテクタ（Detector）	いいえ	いいえ	いいえ	はい
デバイス	はい	はい	はい	はい
性質/ファイル性質（Disposition / File Disposition）	はい	はい	はい	いいえ（No）
ドメイン（Domain）	はい	はい	はい	はい
イベント サブタイプ（Event Subtype）	いいえ	いいえ	いいえ	はい
イベント タイプ（Event Type）	いいえ	はい	はい	はい
ファイル名（File Name）	はい	はい	いいえ	はい
ファイル パス（File Path）	いいえ	いいえ	いいえ	はい
ファイル ポリシー（File Policy）	はい	いいえ	いいえ	いいえ
ファイルのタイムスタンプ（File Timestamp）	いいえ	いいえ	いいえ	はい
HTTP 応答コード（HTTP Response Code）	はい	はい	いいえ	いいえ

フィールド	ファイル イベント	Firepower システムによって検出されたマルウェア イベント	Firepower システムによって検出されたレトロスペクティブイベント	AMP for Endpoints によって検出されたマルウェア イベント
IOC（侵害の兆候）（IOC (Indication of Compromise)）	いいえ	はい	はい	はい
メッセージ（Message）	はい	はい	いいえ	はい
受信側の大陸（Receiving Continent）	はい	はい	はい	いいえ（No）
受信側の国（Receiving Country）	はい	はい	いいえ	いいえ
受信側 IP（Receiving IP）	はい	はい	いいえ	はい
受信側のポート（Receiving Port）	はい	はい	いいえ	いいえ
セキュリティ コンテキスト（Security Context）	はい	はい	はい	はい
送信側の大陸（Sending Continent）	はい	はい	はい	いいえ（No）
送信側の国（Sending Country）	はい	はい	いいえ	いいえ
送信側 IP（Sending IP）	はい	はい	いいえ	いいえ
送信側のポート（Sending Port）	はい	はい	いいえ	いいえ
SHA256/ファイル SHA256（SHA256 / File SHA256）	はい	はい	はい	はい
サイズ（KB）/ファイルサイズ（KB）（Size (KB) / File Size (KB)）	はい	はい	いいえ	はい

フィールド	ファイル イベント	**Firepower** システムによって検出されたマルウェア イベント	**Firepower** システムによって検出されたレトロスペクティブイベント	**AMP for Endpoints** によって検出されたマルウェア イベント
SSL の実際のアクション（SSL Actual Action）（検索のみ）	はい	はい	いいえ	いいえ
SSL 証明書情報（SSL Certificate Information）（検索のみ）	はい	はい	いいえ	いいえ
SSL 障害の理由（SSL Failure Reason）（検索のみ）	はい	はい	いいえ	いいえ
SSL Status	はい	はい	いいえ	いいえ
SSL 件名/発行者の国（SSL Subject/Issuer Country）（検索のみ）	はい	はい	いいえ	いいえ
ファイル ストレージ/保存済み（File Storage / Stored）（検索のみ）	はい	はい	いいえ	いいえ
脅威名（Threat Name）	いいえ	はい	はい	はい
脅威スコア（Threat Score）	はい	はい	いいえ	いいえ
時刻	はい	はい	はい	はい
タイプ/ファイル タイプ（Type / File Type）	はい	はい	いいえ	はい
URI/ファイル URI（URI / File URI）	はい	はい	いいえ	いいえ
ユーザ（User）	はい	はい	いいえ	はい
Web アプリケーション	はい	はい	はい	いいえ（No）
Web アプリケーション カテゴリまたはタグ（Web Application Category or Tag）	はい	はい	はい	いいえ（No）

分析されたファイルに関する詳細の表示

ヒント　追加のオプションを表示するには、イベント ページのテーブルでファイルの SHA を右クリックします。詳細については、Webベースのリソースを使用したイベントの調査を参照してください。

ファイル構成レポート

ローカルマルウェアの分析または動的分析を設定すると、ファイルの分析後にファイル構成レポートが生成されます。このレポートを使用して、ファイルをさらに分析し、ファイルにマルウェアが組み込まれているかどうかを判断することができます。

ファイル構成レポートでは、ファイルのプロパティ、ファイルに組み込まれているオブジェクト、および検出されたウイルスが示されます。また、ファイル構成レポートでは、そのファイルタイプに固有の追加情報が示される場合があります。保存されているファイルのプルーニング時に、関連ファイル構成レポートもプルーニングされます。

ファイル構成の情報を表示するには、ネットワーク ファイル トラジェクトリの使用 （41 ページ）を参照してください。

AMP プライベート クラウドでのファイルの詳細の表示

AMP プライベート クラウドを導入している場合は、プライベート クラウドで分析されたファイルに関する追加の詳細を表示できます。

詳細については、お使いのプライベート クラウドのマニュアルを参照してください。

AMP プライベート クラウドのコンソールに直接サインインします。

脅威スコアと動的分析のサマリ レポート

脅威スコア

表 *5:* 脅威スコア レーティング

脅威スコア	アイコン
Low	
Medium	

脅威スコア	アイコン
High	
Very High	

Firepower Management Center は、ファイルの性質と同じ期間だけ、ファイルの脅威スコアをキャッシュに入れます。これらのファイルが後から検出されると、Cisco Threat Grid クラウドまたは Cisco Threat Grid オンプレミス アプライアンスにもう一度クエリが実行される代わりに、キャッシュされた脅威スコアが表示されます。ファイルの脅威スコアが、定義済みのマルウェアしきい値の脅威スコアを超える場合は、そのファイルにマルウェアの性質を自動的に割り当てることができます。

動的分析のサマリ

動的分析のサマリが生成可能な場合、脅威スコアアイコンをクリックすると、サマリが表示されます。複数のレポートが存在する場合、このサマリは、脅威スコアと完全に一致する最新のレポートに基づいて生成されます。完全に一致する脅威スコアがない場合、最も高い脅威スコアに関するレポートが表示されます。複数のレポートがある場合は、脅威スコアを選択して、それぞれのレポートを表示することができます。

サマリには、脅威スコアを構成する各コンポーネントの脅威がリストされます。各コンポーネントの脅威を展開すると、そのコンポーネントの脅威に関連するプロセスだけでなく、AMP クラウドの調査結果もリストされます。

プロセス ツリーには、Cisco Threat Grid クラウドがファイルを実行しようとしたときに開始されたプロセスが示されています。これは、マルウェアを含むファイルが、想定外のプロセスやシステム リソースへアクセスしようとしているかどうか（たとえば、Word ドキュメントを実行すると、Microsoft Word が開き、次に Internet Explorer が起動し、さらに Java Runtime Environment が実行されるなど）を識別するのに役立ちます。

リストされる各プロセスには、実際のプロセスを検査するのに使用できるプロセス ID が含まれます。プロセス ツリー内の子ノードは、親プロセスの結果として開始されたプロセスを表します。

動的分析のサマリから [完全なレポートを表示（View Full Report）] をクリックすることにより、AMP クラウドの完全な分析を詳述する完全版分析レポートを表示できます。レポートには、ファイルの一般情報、検出されたすべてのプロセスの詳細な説明、ファイル分析の概要、およびその他の関連情報が含まれます。

Cisco Threat Grid パブリック クラウドの動的分析結果の表示

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数	サポートされるドメイン数	アクセス（Access）
マルウェア	マルウェア	いずれか（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。

始める前に

Firepower Management Center を Cisco Threat Grid パブリック クラウド アカウントに関連付けます。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を参照してください。

ステップ 1 Threat Grid ドキュメントで提供されるアドレスで、Cisco Threat Grid パブリック クラウドのポータルにアクセスします。

ステップ 2 このタスクへの前提条件で関連付けを作成するために使用したアカウントの資格情報を使用してログインします。

ステップ 3 組織によって送信されたファイルを表示するか、SHA を使用して特定のファイルを検索します。

不明な点がありましたら、Threat Grid ドキュメントを参照してください。

キャプチャされたファイル ワークフローの使用

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数	サポートされるドメイン数	アクセス
機能に応じて異なる	機能に応じて異なる	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

管理対象デバイスは、ネットワーク トラフィックで検出されたファイルをキャプチャすると、イベントをログに記録します。

（注） デバイスがマルウェアを含むファイルをキャプチャすると、デバイスは、ファイルを検出した場合はファイル イベント、マルウェアを識別した場合はマルウェア イベントの 2 種類のイベントを生成します。

次の手順を使用して、テーブル内のキャプチャ ファイルの一覧を表示し、分析に関連する情報に基づいてイベント ビューを操作します。キャプチャ ファイルにアクセスしたときに表示されるページは、ワークフローによって異なります。ワークフローは、大まかなビューから詳細なビューに移動してイベントを評価するために使用できる、一連のページです。また、特定のニーズを満たす情報だけを表示するカスタム ワークフローを作成することもできます。

ファイル ポリシーの更新など設定を変更した後に、システムがファイルを再キャプチャする場合、そのファイルの既存の情報が更新されます。

たとえば、[マルウェア クラウド ルックアップ（Malware Cloud Lookup）] アクションを使用してファイルをキャプチャするようにファイル ポリシーを設定した場合、システムはそのファイルと一緒にファイル処理と脅威スコアを保存します。その後、ファイル ポリシーを更新し、新しい [ファイルの検出（Detect Files）] アクションのためにシステムが同じファイルを再キャプチャすると、システムはファイルの [最終変更時刻（Last Changed）] の値を更新します。ただし、別のマルウェア クラウド ルックアップを実行しなかったとしても、システムは既存の処理や脅威スコアを削除しません。

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

[Analysis] > **[Files]** > **[Captured Files]** を選択します。

ヒント イベントのテーブル ビューでは、一部のフィールドがデフォルトで非表示にされています。イベント ビューに非表示フィールドを表示するには、検索制約を展開し、[無効にされたカラム（Disabled Columns）] の下のフィールド名をクリックします。

関連トピック

キャプチャされたファイルのフィールド （29 ページ）
定義済みキャプチャ ファイルのワークフロー
イベント ビュー設定の設定

キャプチャされたファイルのフィールド

キャプチャされたファイルのテーブル ビューは、定義済みファイル イベントのワークフローの最後のページであり、カスタム ワークフローに追加できます。このテーブル ビューには、ファイル テーブルの各フィールドの列が含まれます。

このテーブルを検索する場合、検索結果は、検索対象のイベントで使用可能なデータによって決まることに留意してください。使用可能なデータによって、検索の制約が適用されないことがあります。たとえば、ダイナミック分析のためにファイルが送信されていない場合は、関連する脅威スコアがない可能性があります。

表 *6*: キャプチャされたファイルのフィールド

フィールド	説明
アーカイブ検査ステータス（Archive Inspection Status）	アーカイブ ファイルのアーカイブ検査ステータスであり、次のいずれかになります。 • [保留中（Pending）] は、システムがアーカイブ ファイルとその内容をまだ検査していることを示します。ファイルが再びシステムを通過すると、完全な情報が使用可能になります。 • [抽出済み（Extracted）] は、アーカイブの内容を抽出し、検査できたことを示します。 • [失敗（Failed）] は、まれなケースですが、システムが抽出を処理できない場合に発生します。 • [深さ超過（Depth Exceeded）] は、許可されている最大深さを超えるネストされたアーカイブ ファイルがアーカイブに含まれていることを示します。 • [暗号化（Encrypted）] は、アーカイブ ファイルの内容が暗号化されていて、検査できなかったことを示します。 • [検査不可（Not Inspectable）] は、システムがアーカイブの内容を抽出して検査しなかったことを示しています。このステータスの主な理由としては、ポリシー ルール アクション、ポリシー設定、破損ファイルの 3 つがあります。 アーカイブ ファイルの内容を表示するには、表で該当の行を右クリックしてコンテキスト メニューを開いてから、[アーカイブの内容の表示（View Archive Contents）] を選択します。
カテゴリ	ファイル タイプの一般的なカテゴリ（Office ドキュメント、アーカイブ、マルチメディア、実行可能ファイル、PDF ファイル、エンコード ファイル、グラフィック、システム ファイルなど）。
検出名（Detection Name）	検出されたマルウェアの名前。

フィールド	説明
傾向（Disposition）	ファイルの ネットワーク向け AMP での性質： • [マルウェア（Malware）] は、ファイルがローカルのマルウェア分析でマルウェアとして認識され、クラウドでマルウェアとして分類されていること、または、ファイルの脅威スコアが、ファイル ポリシーで定義されたマルウェアしきい値を超えていることを示します。 • [クリーン（Clean）] は、ファイルが AMP クラウドでクリーンとして分類されていること、または、ファイルをユーザがクリーン リストに追加したことを示します。 • [不明（Unknown）] は、システムが AMP クラウドに問い合わせましたが、ファイルの傾向が割り当てられていないこと、つまり、ファイルが AMP クラウドで正しく分類されていないことを示します。 • [カスタム検出（Custom Detection）] は、ファイルをユーザがカスタム検出リストに追加したことを示します。 • [使用不可（Unavailable）] は、システムが AMP クラウドに問い合わせできなかったことを示します。この性質を持つイベントはごくわずかである可能性があります。これは予期された動作です。 • [N/A] は、[ファイルを検出する（Detect Files）] または [ファイルをブロックする（Block Files）] ルールによってファイルが処理され、Firepower Management Center が AMP クラウドに問い合わせなかったことを示します。
ドメイン（Domain）	キャプチャされたファイルが検出されたドメイン。 This field is only present if you have ever configured the Firepower Management Center for multitenancy.

フィールド	説明
動的分析ステータス（Dynamic Analysis Status）	

フィールド	説明
	ファイルが動的分析のために送信されたかどうかを示すものであり、次の値のうちの 1 つ以上が表示されます。 • [分析完了（Analysis Complete）]：ファイルがダイナミック分析のために送信され、脅威スコアおよびダイナミック分析のサマリー レポートを受け取りました。 • [処理予定の容量（Capacity Handled）]：送信できなかったため、ファイルが保存されました。 • [処理予定の容量（ネットワークの問題）（Capacity Handled (Network Issue)）]：ネットワーク接続の問題が原因で送信できなかったため、ファイルが保存されました。 • [処理予定の容量（レート制限）（Capacity Handled (Rate Limit)）]：最大数に達したことが原因で送信できなかったため、ファイルが保存されました。 • [非アクティブなデバイス（Device Not Activated）]：デバイスがオンプレミスの Cisco Threat Grid アプライアンスでアクティブになっていないため、ファイルが送信されません。このステータスが表示された場合は、サポート担当に連絡してください。 • [失敗（分析タイムアウト）（Failure (Analysis Timeout)）]：ファイルが送信されましたが、まだAMPから結果が返されていません。 • [失敗（ファイル実行不可）（Failure (Cannot Run File)）]：ファイルが送信されましたが、AMP クラウドがテスト環境でファイルを実行できませんでした。 • [失敗（ネットワークの問題）（Failure (Network Issue)）]：ネットワーク接続の問題のため、ファイルが送信されませんでした。 • [分析のための送信なし（Not Sent for Analysis）]：ファイルが送信されませんでした。 • [疑わしくないファイル（分析のための送信なし）（Not Suspicious (Not Sent For Analysis)）]：ファイルがマルウェアではないものとして事前に分類されています。 • [以前に分析済み（Previously Analyzed）]：キャッシュされた脅威スコアがあるファイルをユーザが再び送信しようとしました。 • [分析のために送信（Sent for Analysis）]：ファイルが

フィールド	説明
	マルウェアとして事前に分類されており、ダイナミック分析のためにキューに入れられました。
ダイナミック分析ステータスの変更（Dynamic Analysis Status Changed）	前回、ファイルのダイナミック分析のステータスが変更された日時。
ファイル名	ファイルの SHA-256 ハッシュ値に関連付けられているものとして最後に検出されたファイル名。
前回の変更（Last Changed）	このファイルに関連する情報が最後に更新された時刻。
最終送信日時（Last Sent）	ファイルが動的分析のために AMP クラウドに最後に送信された時刻。
ローカル マルウェア分析ステータス（Local Malware Analysis Status）	ローカル マルウェア分析が実行されたかどうかを示すものであり、次のいずれかになります。 • [分析完了（Analysis Complete）]：ローカル マルウェア分析を使用してファイルが検査され、事前に分類されました。 • [分析失敗（Analysis Failed）]：ローカルマルウェア分析を使用してファイルを検査しようとし、失敗しました。 • [手動による要求の送信（Manual Request Submitted）]：ユーザがローカル マルウェア分析のためにファイルを送信しました。 • [分析なし（Not Analyzed）]：システムでローカル マルウェア分析を使用してファイルが検査されませんでした。
SHA256	ファイルの SHA-256 ハッシュ値と、最後に検出されたファイルイベントおよびファイル性質を表すネットワーク ファイル トラジェクトリ アイコン。ネットワーク ファイル トラジェクトリを表示するには、トラジェクトリ アイコンをクリックします。
ストレージ ステータス（Storage Status）	ファイルが管理対象デバイスに保存されているかどうかを示し、次のいずれかになります。 • ファイル保存済み（File Stored） • 保存なし（性質分析の保留）（Not Stored (Disposition Was Pending)）

フィールド	説明
脅威スコア（Threat Score）	このファイルに関連付けられている最新の脅威スコア。 ダイナミック分析のサマリー レポートを表示するには、脅威スコア アイコンをクリックします。
タイプ	ファイルのタイプ（HTML や MSEXE など）。

保存されているファイルのダウンロード

デバイスによって保存されたファイルは、Firepower Management Center がそのデバイスと通信可能であり、ファイルが削除されていない限り、長期間保存し分析するためにローカル ホストにダウンロードし、手動でファイルを分析できます。関連ファイル イベント、マルウェア イベント、キャプチャ ファイル ビュー、またはファイルのトラジェクトリからファイルをダウンロードできます。

マルウェアによる被害を防ぐため、デフォルトでは、ファイルのダウンロードのたびに確認を行う必要があります。ただし、この確認は [ユーザ設定（User Preferences）] で無効にすることもできます。

性質が使用不可のファイルにはマルウェアが含まれている可能性があるため、ファイルをダウンロードすると、システムはまずそのファイルを .zip パッケージにアーカイブします。.zip ファイル名には、ファイルの性質とファイル タイプ（存在する場合）さらに SHA-256 ハッシュ値が含まれます。誤って解凍してしまわないように、.zip ファイルをパスワードで保護できます。.zip ファイルのデフォルト パスワードは、[ユーザ設定（User Preferences）] で編集または削除できます。

⚠

注意 シスコでは、有害な結果が発生することがあるため、マルウェアをダウンロード**しない**ように強くお勧めします。ファイルをダウンロードする際は、マルウェアが含まれている可能性があるので注意してください。ファイルをダウンロードする前に、ダウンロード先を保護するために必要な予防措置を行っていることを確認します。

分析用ファイルの手動での送信

分析用ファイルを手動で送信すると、システムはローカル分析を実行してから、それらのファイルを動的分析対象としてクラウドに送信します。ただし、ローカル分析がファイル ポリシーで有効になっておらず、分析用のファイルを手動で送信する場合は、ファイルが動的分析用としてしか送信されません。

実行可能ファイルの他に、自動送信に適格ではないファイル タイプ（.swf、.jar など）も送信できます。これにより、ファイルの性質に関わらず、さまざまなファイルをより迅速に分析し、問題の正確な原因を突き止めることができます。

（注） 動的分析に適格なファイル タイプのリストと送信可能な最小および最大のファイル サイズに関して更新がないか、システムは AMP クラウドを検査します（この検査は、一日に 1 回だけ行われます）。

分析用ファイルを送信する方法は、状況により、次の 2 種類があります。

始める前に

分析用にキャプチャしたファイルを手動で送信するには、ファイルを保存するように1つまたは複数のファイル ルールを設定する必要があります。詳細については、ファイル ポリシーと高度なマルウェア防御を参照してください。

ステップ 1 1 つの分析用ファイルを送信する場合：

a) 次のいずれかを選択します。

- **[分析（Analysis）] > [ファイル（Files）] > [ファイルイベント（File Events）]**
- **[分析（Analysis）] > [ファイル（Files）] > [マルウェアイベント（Malware Events）]**
- **[分析（Analysis）] > [ファイル（Files）] > [キャプチャファイル（Captured Files）]**

b) <イベント タイプまたはファイル> の [テーブルビュー（Table View）] をクリックします。

c) テーブル内のファイルを右クリックし、[ファイルの分析（Analyze file）] を選択します。

ステップ 2 複数のキャプチャした分析用ファイルを送信する場合（一度に最大 25 ファイル）：

a) [分析（Analysis）] > [ファイル（Files）] > [キャプチャファイル（Captured Files）] を選択します。

b) 分析する各ファイルの横にあるチェック ボックスをオンにします。

c) [Analyze（分析）] をクリックします。

ネットワーク ファイル トラジェクトリ

ネットワーク ファイルのトラジェクトリ機能は、ネットワーク全体でホストがどのようにファイル（マルウェア ファイルを含む）を転送したかをマッピングします。トラジェクトリは、ファイル転送データ、ファイルの性質、ファイル転送がブロックされたかどうか、ファイルが隔離されたかどうかをグラフに示します。これにより、マルウェアを転送したおそれのあるホストおよびユーザやリスクがあるホストがどれであるかを判定したり、ファイル転送の傾向を観測したりできます。

AMP クラウドで性質が割り当てられているファイルであれば、どのファイルの送信でも追跡できます。システムは、ネットワーク向け AMP と AMP for Endpoints の両方によるマルウェアの検出およびブロック情報を使用して、トラジェクトリを作成します。

最近検出されたマルウェアおよび分析済みトラジェクトリ

[ネットワーク ファイル トラジェクトリ リスト（Network File Trajectory List）] ページには、ネットワークで最近検出されたマルウェアと最後に表示したトラジェクトリ マップのファイルが表示されます。これらのリストから、ネットワークで各ファイルが最後に発見されたのはいつか、ファイルのSHA-256のハッシュ値、名前、タイプ、現在のファイルの性質、内容（アーカイブ ファイルの場合）、ファイルに関連付けられたイベント数を確認できます。

また、このページに含まれる検索ボックスを使用して、SHA-256ハッシュ値またはファイル名を基準に、あるいはファイルを送信または受信するホストの IP アドレスによってファイルを見つけることができます。ファイルを見つけた後、[ファイル SHA256（File SHA256）] 値をクリックすると詳細なトラジェクトリ マップが表示されます。

ネットワーク ファイル トラジェクトリの詳細ビュー

詳細なネットワーク ファイル トラジェクトリを表示して、ネットワーク全体でファイルを追跡できます。ファイルの SHA 256 値を検索するか、[ネットワーク ファイル トラジェクトリ（Network File Trajectory）] リスト内の [ファイルの SHA 256（File SHA 256）] リンクをクリックして、そのファイルに関する詳細を表示します。

ネットワーク ファイル トラジェクトリの詳細ページには、3 つの部分があります。

- サマリー情報：ファイルのトラジェクトリ ページには、ファイルに関するサマリー情報（ファイル識別情報、ネットワーク上でファイルが最初に表示された時間および最後に表示された時間と表示したユーザ、ファイルに関連したイベントおよびホストの数、ファイルの現在の性質など）が表示されます。このセクションから、管理対象デバイスがファイルを保存した場合に、そのファイルをローカルにダウンロードしたり、ファイルを動的分析用に送信したり、ファイルをファイル リストに追加したりできます。
- トラジェクトリー マップ：ファイルのトラジェクトリ マップは、ネットワークで最初に検出された時点から直近までファイルを視覚的に追跡します。このマップは、ホストがファイルを転送または受信した時点、ファイルを転送した頻度、ファイルがブロックまたは隔離された時点を示します。データ ポイント間の縦線は、ホスト間のファイル転送を表します。データ ポイントをつなぐ横棒は、時間の経過に応じたホストのファイルアクティビティを示します。

  また、そのファイルでファイルイベントが発生した頻度や、システムがファイルに性質または遡及的性質を割り当てた時点についても示します。マップでデータ ポイントを選択し、ホストがそのファイルを転送した最初のインスタンスに遡るパスを強調表示できます。また、このパスは、ファイルの送信側または受信側としてホストが関与する各オカレンスと交差します。このパスにより、関与するユーザが識別されます。
- 関連イベント：[イベント（Events）] テーブルに、マップ内の各データ ポイントに関するイベント情報がリストされます。テーブルおよびマップを使用して、特定のファイルイベント、このファイルを転送または受信したネットワーク上のホストとユーザ、マップ内の関連するイベント、選択した値で制限されたテーブル内の他の関連するイベントを特定することができます。

ネットワーク ファイル トラジェクトリのサマリー情報

次の概要情報は、ネットワーク ファイル トラジェクトリのリストに表示されるファイルの詳細ページの上部に表示されます。

ヒント 関連するファイルイベントを表示するには、フィールド値のリンクをクリックします。ファイルイベントのデフォルトのワークフローの最初のページが新しいウィンドウで開き、選択した値を含むすべてのファイル イベントも表示されます。

表 7:ネットワーク ファイル トラジェクトリのサマリー情報フィールド

名前	説明
コンテンツのアーカイブ（Archive Contents）	検査されたアーカイブ ファイルで、アーカイブに含まれているファイルの数。
現在の性質（Current Disposition）	次のいずれかのネットワーク向けAMP ファイルの性質です。 • [マルウェア（Malware）]：AMP クラウドでそのファイルがマルウェア、マルウェアによって識別されるローカルマルウェア分析として分類されていること、またはファイルの脅威スコアが、ファイル ポリシーで定義されたマルウェアしきい値を超えていることを示します。 • [クリーン（Clean）]：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）]：システムが AMP クラウドに問い合わせましたが、ファイルの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正しく分類していませんでした。 • 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。 • [該当なし（N/A）]：[ファイル検出（Detect Files）] または [ファイル ブロック（Block Files）] ルールがファイルを処理し、Firepower Management Center がAMPクラウドに問い合わせなかったことを示します。

名前	説明
検出名（Detection Name）	ローカル マルウェア分析によって検出されたマルウェアの名前。
イベント カウント（Event Count）	ファイルに関連付けられたネットワークで発見されたイベントの数、検出されたイベントの数が 250 を超える場合は、マップに表示されるイベントの数。
ファイル カテゴリ（File Category）	ファイル タイプの一般的なカテゴリ（`Office Documents` や `System Files` など）。
ファイル名（File Names）	ネットワーク上で発見された、イベントに関連したファイルの名前。 複数のファイル名が SHA-256 ハッシュ値に関連付けられている場合、最後に検出されたファイル名がリストされます。[詳細（more）] をクリックすると、これが展開されて、残りのファイル名が表示されます。
File SHA256	ファイルの SHA-256 ハッシュ値。 デフォルトで、ハッシュは簡略化された形式で表示されます。完全なハッシュ値を表示するには、その上にポインタを移動させます。複数の SHA-256 ハッシュ値がファイル名に関連付けられている場合、リンクの上にポインタを移動されると、すべてのハッシュ値が表示されます。
[ファイル サイズ（File Size）（KB）]	ファイルのサイズ（KB 単位）。
ファイル タイプ（File Type）	ファイルのタイプ（`HTML` や `MSEXE` など）。
最初の確認日時（First Seen）	ネットワーク向け AMP または AMP for Endpoints による初めてのファイル検出に加えて、ファイルを初めてアップロードしたホストの IP アドレス、および関与するユーザの識別情報。
最終表示（Last Seen）	ネットワーク向け AMP または AMP for Endpoints による最新のファイル検出に加えて、ファイルを最後にダウンロードしたホストの IP アドレス、および関与するユーザの識別情報。
親アプリケーション（Parent Application）	エンドポイント向け AMP による検出が行われたときに、マルウェア ファイルにアクセスしていたクライアント アプリケーション。これらのアプリケーションはネットワーク検出またはアプリケーション制御とは関係**ありません**。

名前	説明
表示日（Seen On）	ファイルを送信または受信したホストの数。1 つのホストが 1 つのファイルのアップロードおよびダウンロードを時を異にして行う場合があるため、ホストの合計数が、[Seen On Breakdown] フィールドの送信側の総数と受信側の総数の合計と一致しないことがあります。
Seen On Breakdown	ファイルを送信したホストの数とファイルを受信したホストの数。
脅威名（Threat Name）	エンドポイント向け AMP によって検出されたマルウェアに関連付けられている脅威の名前。
脅威スコア（Threat Score）	ファイルの脅威スコア。

ネットワーク ファイル トラジェクトリ マップと関連イベント リスト

ファイル トラジェクトリ マップの Y 軸には、ファイルと対話したすべてのホストの IP アドレスがリストされます。IP アドレスは、システムがそのホストでファイルを最初に検出した時点に基づいて降順でリストされます。各行には、その IP アドレスに関連付けられたすべてのイベント（単一のファイル イベント、ファイル転送、遡及的イベント）が含まれます。X 軸には、システムが各イベントを検出した日時が含まれます。タイムスタンプは時間順にリストされます。複数のイベントが 1 分以内に発生する場合、すべてが同じ列内にリストされます。マップを左右および上下にスクロールして、イベントおよび IP アドレスをさらに表示できます。

マップには、ファイルの SHA-256 ハッシュに関連した最大 250 のイベントが表示されます。イベントが 250 を超える場合、マップには最初の 10 個が表示され、余分のイベントは省略されて矢印アイコン（  ）が示されます。その後ろに、マップは残りの 240 個のイベントを表示します。

デフォルトの [File Events（ファイル イベント）] ワークフローの最初のページが新しいウィンドウで開き、ファイル タイプに基づいて制限されて、すべての余分のイベントが表示されます。エンドポイント向け AMP によって生成されたマルウェア イベントが表示されない場合、[マルウェア イベント（Malware Events）] テーブルに切り替えてそれらを表示する必要があります。

各データ ポイントは、イベントの他にファイル性質を表しています。マップの下の凡例を参照してください。たとえば、[マルウェア ブロック（Malware Block）] イベント アイコンは、[悪意のある性質（Malicious Disposition）] アイコンと [ブロック イベント（Block Event）] アイコンを結合したものです。

エンドポイント向け AMP によって生成されたマルウェア イベント（「エンドポイントベースのマルウェア イベント」）には 1 つのアイコンが含まれています。レトロスペクティブ イベントでは、ファイルで検出された各ホストのコラムにアイコンが表示されます。ファイル転送イベントでは、縦線でつながれた 2 つのアイコン（ファイル送信アイコンとファイル受信アイコン）が常に含まれます。矢印は、送信側から受信側へのファイル転送方向を示します。

ネットワークを介したファイルの進行状況を追跡するために、データ ポイントをクリックして、選択したデータ ポイントに関連するすべてのデータ ポイントを含むパスを強調表示できます。これには、次のタイプのイベントに関連付けられたデータ ポイントが含まれます。

- 関連付けられている IP アドレスが送信側または受信側だったファイル転送
- 関連付けられた IP アドレスを含めて、エンドポイント向け AMP によって生成されたマルウェア イベント（「エンドポイントベースのマルウェア イベント」）
- 別の IP アドレスが関係する場合、その関連する IP アドレスが送信側または受信側であったすべてのファイル転送
- 別の IP アドレスが関係していた場合、その他方の IP アドレスが関係するエンドポイント向け AMP によって生成されたマルウェア イベント（「エンドポイントベースのマルウェア イベント」）

強調表示されたデータ ポイントに関連付けられたすべての IP アドレスとタイムスタンプも強調表示されます。[Events] テーブルの対応するイベントも強調表示されます。省略されたイベントがパスに含まれている場合、そのパス自体が点線で強調表示されます。省略されたイベントがパスを交差している場合がありますが、マップに表示されません。

ネットワーク ファイル トラジェクトリの使用

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数	サポートされるドメイン数	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）	いずれか（Any）	いずれか（Any）	Admin/Any Security Analyst

マルチドメイン展開環境では、現在のドメインと子孫ドメインのデータを表示することができます。上位レベルのドメインまたは兄弟ドメインのデータを表示することはできません。

ヒント 組織で AMP for Endpoints を導入している場合、その製品にはネットワーク ファイル トラジェクトリ機能もあります。FMC から AMP for Endpoints にピボットするには、AMP for Endpoints コンソールでのイベント データの使用 （43 ページ）を参照してください。AMP for Endpoints のファイル トラジェクトリ機能の詳細については、AMP for Endpoints のマニュアルを参照してください。

ステップ 1 **[Analysis]** > **[Files]** > **[Network File Trajectory]**を選択します。

ヒント また、ファイル情報を使用して、コンテキスト エクスプローラ、ダッシュボード、またはイベント ビューからファイルのトラジェクトリにアクセスできます。

ステップ 2 リストの [ファイル SHA 256（File SHA 256）] リンクをクリックします。

ステップ 3 オプションで、追跡するファイルの完全な SHA-256 ハッシュ値、ホスト IP アドレス、またはファイル名を検索フィールドに入力して、Enter を押します。

ヒント 1 つの結果だけが一致する場合、そのファイルの [ネットワーク ファイル トラジェクトリ（Network File Trajectory）] ページが表示されます。

ステップ 4 [サマリー情報（Summary Information）] セクションでは、以下を実行できます。

- ファイル リストにファイルを追加する：クリーン リストまたはカスタム検出リストにファイルを追加したり、ファイルを削除したりするには、編集アイコン（  ）をクリックします。
- ファイルをダウンロードする：ファイルをダウンロードするには、ファイルのダウンロード アイコン（  ）をクリックし、プロンプトが表示されたら、ファイルをダウンロードすることを確認します。ファイルをダウンロードできない場合、このアイコンは淡色表示されます。
- レポートする：脅威スコア アイコンをクリックすると、動的分析サマリー レポートが表示されます。
- 動的分析のために送信する：AMP クラウド アイコン（  ）をクリックすると、動的分析のためにファイルを送信できます。ファイルを送信できない場合、または AMP クラウドに接続できない場合は、このアイコンは淡色表示されます。
- アーカイブの内容を表示する：アーカイブ ファイルの内容に関する情報を表示するには、表示アイコン（  ）をクリックします。
- ファイル構成を表示する：ファイルの構成を表示するには、ファイル リスト アイコン（  ）をクリックします。システムがファイル構成レポートを生成していなければ、このアイコンは淡色表示されます。
- 同じ脅威スコアでキャプチャされたファイルを表示する：脅威スコア リンクをクリックすると、その脅威スコアでキャプチャされたすべてのファイルが表示されます。

（注） シスコでは、有害な結果が発生することがあるため、マルウェアをダウンロード**しない**ように強くお勧めします。ファイルをダウンロードする際は、マルウェアが含まれている可能性があるので注意してください。ファイルをダウンロードする前に、ダウンロード先を保護するために必要な予防措置を行っていることを確認します。

ステップ 5 トラジェクトリ マップでは、以下を実行できます。

- 最初のインスタンスを見つける：IP アドレスをクリックして、IP アドレスが含まれる、最初に発生したファイル イベントを見つけます。これにより、そのデータ ポイントへのパスが強調表示され、その最初のファイル イベントに関連した仲介ファイル イベントと IP アドレスがあればそれも強調表示されます。[Events] テーブルの対応するイベントも強調表示されます。そのデータ ポイントが現在表示されていない場合、表示されるまでマップがスクロールされます。
- 追跡する：データ ポイントをクリックすると、選択したデータ ポイントに関連するすべてのデータ ポイントが含まれるパスが強調表示されます。これにより、ネットワークを介してファイルの進捗を追跡できます。

- 非表示のイベントを表示する：矢印アイコンをクリックすると、[ファイル サマリー（File Summary）] イベント ビューに表示されていないすべてのイベントが表示されます。
- ファイルの一致イベントを表示する：イベントアイコン（）の上にポインタを合わせると、イベントのサマリー情報が表示されます。いずれかのイベント サマリー情報リンクをクリックすると、デフォルトの [ファイル イベント（File Events）] ワークフローの最初のページが新しいウィンドウで開き、そのファイル タイプのすべての余分のイベントが表示されます。[ファイル サマリー（File Summary）] イベント ビューが新しいウィンドウで表示され、クリックした条件値に一致するすべてのファイル イベントが表示されます。

ステップ 6 [イベント（Events）] テーブルでは、以下を実行できます。

- 強調表示：テーブル行を選択すると、マップ上のデータ ポイントが強調表示されます。選択したファイル イベントが現在表示されていない場合、表示されるまでマップがスクロールされます。
- ソート：カラム見出しをクリックすると、昇順または降順で情報をソートできます。

AMP for Endpoints コンソールでのイベント データの使用

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数	サポートされるドメイン数	アクセス
いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）	Admin

組織で AMP for Endpoints を導入している場合は、AMP for Endpoints コンソールでマルウェア イベント データを表示して、当該アプリケーションのグローバル ネットワーク ファイル トラジェクトリ ツールを使用することができます。

ヒント AMP for Endpoints とそのコンソールの使用については、コンソールのオンライン ヘルプや、その他のドキュメンテーションを参照してください。 https://www.cisco.com/c/en/us/support/security/fireamp-endpoints/tsd-products-support-series-home.html

Firepower Management Center から AMP for Endpoints コンソールにアクセスするには、次のいずれかを実行します。

始める前に

- AMP for Endpoints への接続が設定され（Firepower と AMP for Endpoints の統合 を参照してください）、Firepower Management Center が AMP クラウドに接続可能になっている必要があります。
- AMP for Endpoints のクレデンシャルが必要になります。

- FMC のマルウェア イベントからピボットする場合は、AMP for Endpoints のコンテキストクロス起動オプションが適切に有効になっていることを確認します。Webベースのリソースを使用したイベントの調査の各トピックを参照してください。

ステップ 1 方法 1：

a) **[AMP]** > **[AMP Management]**を選択します。

b) テーブルでクラウド名をクリックします。

ステップ 2 方法 2：

a) [Analysis（分析）] > [ファイル（Files）] にあるテーブルで、マルウェア イベントに移動します。

b) ファイル SHA を右クリックし、[AMP for Endpoints] オプションを選択します。

ファイルおよびマルウェアイベントとネットワークファイル トラジェクトリの履歴

機能	バージョン	詳細
Syslog の接続イベントの固有識別子	6.4.0.4	syslog の [Sensor UUID]、[First Packet Time]、[Connection Instance ID]、および [Connection Counter] フィールドの情報を総合すると、接続イベントを一意に識別できます。これらのフィールドは、ファイルおよびマルウェアイベントの syslog に含まれます。
syslog を介してファイルイベントおよびマルウェア イベントを送信する機能	6.4	この章のフィールドの説明は、syslog メッセージに含まれるフィールドを指しています。 設定情報については、ファイルとマルウェア イベントの syslog の設定場所を参照してください。