マルウェアとファイル アクティビティの分析

防御センター は、システムのファイル インスペクションおよび処理のレコードを、キャプチャされたファイル、ファイル イベント、およびマルウェア イベントとしてログ記録します。

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

ファイル内のマルウェアを検出するために、システムはまずファイル自体を検出する必要があるため、ネットワーク トラフィック内のマルウェア検出/ブロックに基づいてシステムがマルウェア イベントを生成するときには、ファイル イベントも生成します。FireAMP コネクタによって生成されたエンドポイント ベースのマルウェア イベント(FireAMP と FireSIGHT システムの統合(37-8 ページ)を参照)には、対応するファイル イベントがないことに注意してください。同様に、システムがネットワーク トラフィック内でファイルをキャプチャするとき、システムはまずファイルを検出するため、ファイル イベントも生成されます。

防御センター を使用すると、キャプチャされたファイル、ファイル イベント、およびマルウェア イベントを表示、操作、分析して、分析内容を他のユーザに送信できます。Context Explorer、ダッシュボード、イベント ビューア、コンテキスト メニュー、ネットワーク ファイル トラジェクトリ マップ、およびレポート機能を使用することにより、検出、キャプチャ、ブロックされたファイルおよびマルウェアに関してより深く理解できるようになります。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。

DC500 では Malware ライセンスを使用できず、シリーズ 2 デバイスや Blue Coat X-Series 向け Cisco NGIPS では Malware ライセンスを有効にすることもできません。このため、これらのアプライアンスを使用して、マルウェア クラウド ルックアップまたはアーカイブ ファイルの内容に関連するキャプチャされたファイル、ファイル イベント、およびマルウェア イベントを生成/分析することはできません。

詳細については、以下を参照してください。

- ファイル ストレージの操作(40-2 ページ)
- 動的分析の操作(40-5 ページ)
- ファイル イベントの操作(40-8 ページ)

- マルウェア イベントの操作（40-18 ページ）
- キャプチャ ファイルの操作（40-33 ページ）
- ネットワーク ファイル トラジェクトリの操作（40-39 ページ）

この章で説明するデータを生成する、マルウェア防御およびファイル制御アクションを実行するためのシステムの設定の詳細については、マルウェアと禁止されたファイルのブロッキング（37-1 ページ）を参照してください。

ファイル ストレージの操作

ライセンス：Malware

サポートされるデバイス：シリーズ 2 と X-シリーズ を除くすべて

サポートされる防御センター：任意（DC500 を除く）

ファイル ポリシーの設定に基づき、ファイル制御機能を使用して、ファイルの検出およびブロックを行えます。ただし、疑わしいホストまたはネットワークからのファイルや、ネットワーク上の監視対象ホストに送信された大量のファイルについては、さらに分析が必要になる場合があります。ファイル ストレージ機能を使用することにより、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、それら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。

デバイスがトラフィックでファイルを検出すると、そのファイルをキャプチャできます。こうしてコピーが作成され、システムはそれを保存したり動的分析のために送信したりできます。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。詳細については、キャプチャ ファイル ストレージについて（40-3 ページ）を参照してください。
- 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。詳細については、保存されているファイルの別の場所へのダウンロード（40-4 ページ）を参照してください。
- 動的分析のために、キャプチャしたファイルを Collective Security Intelligence クラウドに送信する。詳細については、動的分析の操作（40-5 ページ）を参照してください。

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） 初めて検出されたファイルは、防御センター によるクラウド ルックアップの完了後に性質が割り当てられます。システムはファイル イベントを生成しますが、ファイルに性質が即座に割り当てられない限り、ファイルを保存できません。

以前に検出されていないファイルがブロック マルウェア アクション付きのファイル ルールと一致する場合、後続のクラウド ルックアップによって即座に性質が返されるので、システムはファイルを保存しイベントを生成できるようになります。

以前に検出されていないファイルがマルウェア クラウド ルックアップ アクション付きのファイル ルールと一致する場合、システムはファイル イベントを生成しますが、クラウド ルックアップを実行し性質を返すのに追加の時間を要します。この遅延のため、システムはマルウェア クラウド ルックアップ アクション付きのファイル ルールに一致するファイルがネットワーク上に 2 回目に現れるまで保存することはできません。

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。

- イベント ビューア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。詳細については、キャプチャ ファイルの操作（40-33 ページ）を参照してください。
- 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。詳細については、ネットワーク ファイル トラジェクトリの分析（40-42 ページ）を参照してください。
- 以後の検出時に、ファイルをクリーンまたはマルウェアな性質を持つものとして常に扱うように、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。詳細については、ファイル リストの操作（3-38 ページ）を参照してください。

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性質（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、それをデバイスに適用した後、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、保存する最小ファイル サイズと最大ファイル サイズを制限できます。詳細については、ファイルおよびマルウェアのインスペクション パフォーマンスおよびストレージの調整（18-21 ページ）とファイル ルールの操作（37-20 ページ）を参照してください。

ファイル ストレージには、デバイスに十分なディスク領域が必要です。デバイスのプライマリ ハード ドライブに十分な領域がなく、マルウェア ストレージ パックもインストールされていない場合、デバイスにファイルを保存できません。

注意　シスコ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、『*FireSIGHT システム Malware Storage Pack Guide*』を参照してください。

DC500 で Malware ライセンスを使用したり、シリーズ 2 デバイスや Blue Coat X-Series 向け Cisco NGIPS で Malware ライセンスを有効にすることはできないので、それらのアプライアンスをファイルのキャプチャまたは保存に使用することはできないことに注意してください。

詳細については、以下を参照してください。

- キャプチャ ファイル ストレージについて（40-3 ページ）
- 保存されているファイルの別の場所へのダウンロード（40-4 ページ）

キャプチャ ファイル ストレージについて

ライセンス：Malware

サポートされるデバイス：8000 シリーズ

ファイル ポリシー構成に基づいて、デバイスはハード 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。

注意　シスコ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、『*FireSIGHT システム Malware Storage Pack Guide*』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ようにデバイスを構成する際に、設定された量のプライマリ ハード ドライブのスペースだけがキャプチャ ファイル ストレージに割り当てられます。デバイスにマルウェア ストレージ パックを設置して、ファイルを保存するようにデバイスを構成すると、デバイスは代わりに、マルウェア ストレージ パック全体をキャプチャ ファイルの保存用に割り当てます。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 ファイルがすべて、マルウェア ストレージ パックに移動されます。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。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。

保存したファイルは、システム バックアップ ファイルに含められないことに注意してください。詳細については、バックアップ ファイルの作成（70-2 ページ）を参照してください。

保存されているファイルの別の場所へのダウンロード

ライセンス：Malware

サポートされるデバイス：シリーズ 2 と X-シリーズ を除くすべて

サポートされる防御センター：任意（DC500 を除く）

デバイスがファイルを保存すると、防御センター がそのデバイスと通信でき、しかもファイルが削除されていない限り、そのファイルをダウンロードできます。手動でファイルを分析したり、長期保存や分析のためにローカル ホストにダウンロードしたりできます。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。詳細については、コンテキスト メニューの使用（2-5 ページ）およびサマリー情報（40-42 ページ）を参照してください。

マルウェアによる被害を防ぐために、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、ファイル ダウンロード プロンプトでの確認を無効にできます。確認を再度有効にするには、ファイル設定（71-5 ページ）を参照してください。

注意　シスコは、有害な結果が生じるのを防ぐために、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、ダウンロード先をセキュアに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。

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 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。デフォルトの .zip ファイル パスワードを編集または削除するには、ファイル設定（71-5 ページ）を参照してください。

動的分析の操作

ライセンス：Malware

サポートされるデバイス：シリーズ 2 と X-シリーズ を除くすべて

サポートされる防御センター：任意（DC500 を除く）

クラウドの精度を向上させ、追加のマルウェア分析および脅威識別を提供するために、適格なキャプチャ ファイルを シスコ クラウドに送信して、動的分析を行うことができます。クラウドはテスト環境でそのファイルを実行し、その結果に基づいて、脅威スコアおよび動的分析のサマリー レポートを 防御センター に返します。適格なファイルをクラウドに送信して、Spero 分析を行うこともできます。これは、マルウェア識別を補うために、ファイルの構造を調べます。

動的分析のためのクラウドへのファイル送信は、キャプチャされたファイルのタイプと、アクセス コントロール ポリシーで設定された可能な最小および最大のファイル サイズによって異なります。以下を行うことができます。

- ファイル ルールによって実行可能ファイルに対するマルウェア クラウド ルックアップが行われ、ファイル性質が不明の場合、動的分析用に自動的にファイルを送信できます。
- 保存済みで、サポートされているファイル タイプ（PDF や Microsoft Office ドキュメントなど）の場合、最大で 25 個のファイルを手動で一度に送信できます。

送信されたファイルはクラウドでの分析のためにキューに入れられます。キャプチャ ファイルおよびファイルのトラジェクトリを表示して、ファイルが動的分析のために送信されているかどうかを判別できます。注意すべき点として、動的分析のためにファイルを送信するたびに、最初の分析で結果が生成されていても、クラウドはそのファイルを分析します。

詳細については、ファイル ルールの操作（37-20 ページ）および動的分析のためのファイルの送信（40-6 ページ）を参照してください。

（注） 動的分析に適格なファイル タイプのリストおよび送信可能な最小/最大ファイル サイズに関する更新がないか、システムはクラウドを検査します（一日に 2 回以上行われることはありません）。

クラウドは、サンドボックス環境でファイルを実行することにより、動的な分析を実行します。以下が返されます。

- 脅威スコア：ファイルにマルウェアが含まれている可能性について詳しく示します。
- 動的分析のサマリー レポート：クラウドがその脅威スコアを割り当てた理由について詳しく示します。

ファイル ポリシーの設定に基づき、定義されているしきい値を脅威スコアが超えているファイルを自動的にブロックできます。また、動的分析のサマリー レポートを確認して、マルウェアの識別を向上させたり、検出機能を調整したりできます。

動的分析を補うために、ファイル ルールによって実行可能ファイルにマルウェア クラウド ルックアップが行われる場合に、自動的にファイルを送信して Spero 分析を行うことができます。クラウドは実行可能ファイルの構造（メタデータや見出しの情報を含む）を調べて、ファイルがマルウェアかどうかを識別できます。詳細については、マルウェア防御とファイル制御について（37-2 ページ）を参照してください。

注意すべき点として、DC500 で Malware ライセンスは使用できず、シリーズ 2 デバイスや Blue Coat X-Series 向け Cisco NGIPS で Malware ライセンスを有効にすることもできないため、それらのアプライアンスを使用して、動的分析または Spero 分析のためにファイルを送信することはできません。

（注）　HTTP プロキシ経由で シスコ クラウドにファイルを送信するように、管理対象デバイスを設定できます。物理アプライアンスを設定するには、管理インターフェイスの構成（64-9 ページ）を参照してください。仮想アプライアンスを設定するには、http-proxy（D-37 ページ）を参照してください。Blue Coat X-Series 向け Cisco NGIPS では、プロキシ設定はサポートされていません。

詳細については、以下を参照してください。

- Spero 分析について（40-6 ページ）
- 動的分析のためのファイルの送信（40-6 ページ）
- 脅威スコアおよび動的解析のサマリーの確認（40-7 ページ）

Spero 分析について

ライセンス：Malware

サポートされるデバイス：シリーズ 2 と X-シリーズ を除くすべて

サポートされる防御センター：任意（DC500 を除く）

Spero 分析は SHA256 ハッシュの分析を補うもので、実行可能ファイル内のマルウェアをより正確に識別できます。Spero 分析では、デバイスがファイル構造の特性（メタデータや見出し情報など）を調べます。この情報に基づいて Spero シグニチャを生成した後、デバイスはそれをシスコ 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。Spero シグニチャに基づいて、そのファイルがマルウェアかどうかを Spero エンジンが返します。マルウェアの場合、現時点の性質が不明であれば、システムはマルウェアの性質をファイルに割り当てます。ファイル性質の詳細については、マルウェア防御とファイル制御について（37-2 ページ）を参照してください。

Spero 分析のために実行可能ファイルを送信できるのは、検出時だけなので注意してください。後から手動で送信することはできません。動的分析のためにファイルを送信しなくても、Spero 解析のためにファイルを送信できます。詳細については、ファイル ルールの操作（37-20 ページ）を参照してください。

動的分析のためのファイルの送信

ライセンス：Malware

サポートされるデバイス：シリーズ 2 と X-シリーズ を除くすべて

サポートされる防御センター：任意（DC500 を除く）

イベント ビューアのコンテキスト メニューまたはネットワーク ファイルのトラジェクトリから、動的分析のためにファイルを手動で送信できます。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（たとえば、PDF や Microsoft Office ドキュメントなど）も送信できます。詳細については、コンテキスト メニューの使用（2-5 ページ）とサマリー情報（40-42 ページ）を参照してください。

問題が生じた後で複数のファイルを分析するために、キャプチャ ファイル ビューから一度に最大で 25 個の（特定のタイプの）ファイルをファイル性質に関係なく手動で送信できます。これにより、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。詳細については、キャプチャ ファイルの操作（40-33 ページ）およびワークフロー ページの行の選択（58-40 ページ）を参照してください。

脅威スコアおよび動的解析のサマリーの確認

ライセンス：Malware

サポートされるデバイス：シリーズ 2 と X-シリーズ を除くすべて

サポートされる防御センター：任意（DC500 を除く）

動的分析のためにファイルを送信すると、シスコ クラウドはファイルのシグニチャを分析し、脅威スコアと動的分析のサマリーの両方を返します。これらは、潜在的なマルウェア脅威をより詳しく分析し、検出戦略を調整するのに役立ちます。

脅威スコア

ファイルは、マルウェアである可能性に応じて、脅威スコア レーティングのいずれかに分類されます。

表 40-1　脅威スコア レーティング

脅威スコア	アイコン	評価
低（Low）	●○○○	1 ～ 25
中	●●○○	26 ～ 50
高	●●●○	51 ～ 75
非常に高い	●●●●	76 ～ 100

防御センター は、ファイルの性質と同じ期間、ファイルの脅威スコアをローカルのキャッシュに入れます。これ以降、これらのファイルを検出すると、システムはシスコ クラウドに再度クエリを行う代わりに、キャッシュに入れられた脅威スコアを表示します。ファイル ポリシーの設定に基づき、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、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。詳細については、ファイル ポリシーの作成（37-19 ページ）を参照してください。

動的分析のサマリー

動的分析のサマリーを使用できる場合、脅威スコアのアイコンをクリックすると、それが表示されます。動的分析のサマリーでは、脆弱性調査チーム（VRT）のファイル分析による全体的な脅威スコアの構成するレーティングと、クラウドがそのファイルを実行しようとしたときに開始された他のプロセスについて説明されています。

複数のレポートが存在する場合、このサマリーは、脅威スコアと完全に一致する最新のレポートに基づきます。完全に一致する脅威スコアがない場合、脅威スコアが最も高い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できます。

サマリーには、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ています。各コンポーネントの脅威は、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、VRT の調査結果のリストまで展開できます。

プロセス ツリーには、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、次にエクスプローラが起動し、さらに Java が起動するなど)を識別するのに役立ちます。

リストされている各プロセスには、実際のプロセスを検査するのに使用できるプロセス ID と md5 チェックサムが含まれています。プロセス ツリーには、親プロセスの結果として開始されたプロセスが子ノードとして表示されます。

動的分析のサマリーから [詳細レポートの表示(View Full Report)] をクリックすることにより、VRT の完全な分析を詳述する VRT の分析レポートを表示できます。これには、ファイルの一般情報、検出されたすべてのプロセスのより綿密な説明、ファイル分析の概要、および他の関連情報が含まれています。

ファイル イベントの操作

ライセンス: Protection

システムは、現在適用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。注意すべき点として、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制御ルールのログ設定に関係なく、システムは 防御センター データベースへの関連する接続の終わりも記録します。詳細については、ファイル ポリシーの概要と作成(37-11 ページ)を参照してください。

(注)　ネットワーク トラフィックで検出され、FireSIGHT システム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。これは、システムがファイル内のマルウェアを検出するために、まずそのファイル自体を検出する必要があるためです。エンドポイントベースのマルウェア イベントには、対応するファイル イベントはありません。詳細については、マルウェア イベントの操作(40-18 ページ)およびキャプチャ ファイルの操作(40-33 ページ)を参照してください。

防御センター のイベント ビューアを使用して、ファイル イベントの表示、検索、削除を行えます。さらに、Files Dashboard では、ネットワークで検出されたファイル(マルウェア ファイルを含む)に関する詳細情報を、図やグラフを使って一目で知ることができます。ネットワーク ファイル トラジェクトリでは、個々のファイルの情報とそれらが時間の経過に伴ってネットワークでどのように推移してきたかに関する情報のサマリーが提供されるので、それらのファイルに関してより綿密に知ることができます。ファイルの識別データを使用して、相関ルールをトリガーしたり、レポートを作成したりできます。後者では、定義済みの Files Report テンプレートまたはカスタム レポート テンプレートを使用します。

詳細については、以下を参照してください。

- ファイル イベントの表示（40-9 ページ）
- ファイル イベント テーブルについて（40-10 ページ）
- 地理位置情報の使用（58-24 ページ）
- ファイル イベントの検索（40-14 ページ）

ファイル イベントの表示

ライセンス：Protection

FireSIGHT システムのイベント ビューアでは、分析に関連した情報に応じてイベント ビューを操作するほかに、ファイル イベントをテーブルの形で表示できます。また、個々のファイル イベントに使用可能な情報は、ライセンスなどのさまざまな要因によって異なることに注意してください。詳細については、サービス サブスクリプション（65-8 ページ）を参照してください。

ファイル 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。システムには、ファイル イベント用の以下の定義済みのワークフローが付属しています。

- [ファイル サマリー（File Summary）]（デフォルト）：さまざまなファイル イベントのカテゴリとタイプ、および関連するマルウェア ファイル性質の概要を提供します。
- [ファイルを受信したホスト（Hosts Receiving Files）] および [ファイルを送信したホスト（Hosts Sending Files）]：ファイルを送受信したホストのリストを、それらのファイルの関連するマルウェア性質でグループ化した形で提供します。

（注） ファイル性質は、システムがマルウェア クラウド ルックアップを実行したファイルに関してのみ表示されます。ファイル ルール アクションと評価順序（37-13 ページ）を参照してください。

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。カスタム ワークフローを含む、さまざまなデフォルト ワークフローの指定の詳細については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

FireSIGHT システムは、Unicode（UTF8）文字を使用するファイル名の表示および入力を Web インターフェイスのすべてのエリア（イベント ビューア、イベント検索、ダッシュボード、Context Explorer など）でサポートしています。ただし、PDF 形式で生成したレポートでは Unicode がサポートされないので注意してください。PDF レポートでは、Unicode ファイル名は翻字形式で表示されます。詳細については、レポートの生成と表示（57-29 ページ）を参照してください。また、SMB プロトコルは Unicode ファイル名を印刷可能な文字に変換することにも注意してください。SMB を通して検出した Unicode ファイル名を持つファイルは、印刷不可能な文字の代わりにピリオド（.）とともに表示されます。

イベント ビューアを使用して、以下を行うことができます。

- イベントの検索、ソート、および制限と、表示されるイベントの時間範囲の変更
- 表示される列の指定（テーブル ビューのみ）
- IP アドレスに関連付けられたホスト プロファイル、またはユーザ ID に関連付けられたユーザの詳細およびホスト履歴の表示
- 特定のファイルが検出された接続の表示
- 同じワークフロー内のさまざまなワークフロー ページを使用したイベントの表示

- 別のワークフローを使用したイベントの表示
- 特定の値で制限されるワークフロー内のページからページへのドリルダウン
- 後で同じデータに戻る（存在している場合）ための、現在のページおよび制約のブックマーク
- ファイルに関連付けられたルーティング可能な IP アドレスの送受信の国および大陸の表示
- ファイルのトラジェクトリの表示
- ファイル リストへのファイルの追加、ファイルのダウンロード、動的分析のためのファイルの送信、ファイルの SHA-256 値のフルテキストの表示
- ファイルの動的分析のサマリー レポート（使用可能な場合）の表示
- アーカイブ ファイル内のネストされたファイルの表示
- 現在の制約を使用してレポート テンプレートを作成する
- データベースからのイベントの削除
- IP アドレスのコンテキスト メニューを使用した、ホワイトリストまたはブラックリストへの追加、あるいはファイル イベントに関連付けられたホストまたは IP アドレスに関する他の使用可能な情報の取得

カスタム ワークフローの作成など、イベント ビューアの使用の詳細については、ワークフローの概要と使用（58-1 ページ）を参照してください。

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、イベント ビューアでチェック ボックスを使用してファイルを選択してから、[ジャンプ先（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。詳細については、ワークフロー間のナビゲート（58-41 ページ）を参照してください。

ファイル イベントを表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [ファイル（Files）] > [ファイル イベント（Files Events）] を選択します。

デフォルトのファイル イベントのワークフローの最初のページが表示されます。表示される列の詳細については、ファイル イベント テーブルについて（40-10 ページ）を参照してください。

ファイル イベント テーブルについて

ライセンス：Protection

防御センター は、適用されているファイル ポリシーの設定に従って、監視対象ネットワーク トラフィックで送信されるファイルを管理対象デバイスが検出またはブロックしたときに、ファイル イベントを記録します。

ファイル イベントのテーブル 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。デフォルトでは、ファイル イベントのテーブル ビューにいくつかのフィールドが表示されます。セッション中にフィールドを有効にするには、展開矢印（  ）をクリックして、検索制約を拡張してから、[無効列（Disabled Columns）] の下の列名をクリックします。

個々のファイル イベントに使用可能な情報は、ライセンスなどのさまざまな要因によって異なることに留意してください。たとえば、ファイル制御を行えるのは Protection ライセンスだけですが、Malware ライセンスを使用して、特定のファイル タイプの高度なマルウェア対策を実行したり、ネットワークで転送されたファイルを追跡したりできます。

以下の表は、ファイル イベント フィールドについて説明しています。

表 40-2　ファイル イベント フィールド

フィールド	説明
時刻（Time）	イベントが生成された日時。
アクション（Action）	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。
送信側 IP（Sending IP）	検出されたファイルを送信するホストの IP アドレス。
送信側の国（Sending Country）	検出されたファイルを送信するホストの国。 DC500 防御センター はこの機能をサポートしていないことに注意してください。
受信側 IP（Receiving IP）	検出されたファイルを受信するホストの IP アドレス。
受信側の国（Receiving Country）	検出されたファイルを受信するホストの国。 DC500 防御センター はこの機能をサポートしていないことに注意してください。
送信側のポート（Sending Port）	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。
受信側のポート（Receiving Port）	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。
SSL ステータス（SSL Status）	SSL ルールに関連したアクション、デフォルトのアクション、または暗号化接続をログに記録した復号できないトラフィック アクション。 • [ブロック（Block）] および [リセットしてブロック（Block with reset）] は、ブロックされた暗号化接続を表します。 • [復号（再署名）（Decrypt (Resign)）] は、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（キーの置き換え）（Decrypt (Replace Key)）] は、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された発信接続を表します。 • [復号（既知のキー）（Decrypt (Known Key)）] は、既知の秘密キーを使用して復号された着信接続を表します。 • [デフォルト アクション（Default Action）] は、デフォルト アクションによって接続が処理されたことを示します。 • [復号しない（Do not Decrypt）] は、システムが復号しなかった接続を表します。 システムが暗号化接続を復号できなかった場合は、実行された復号不能のトラフィック アクションと障害の理由が表示されます。たとえば、システムが不明な暗号スイートで暗号化されたトラフィックを検出し、さらにインスペクションを行わずにそのトラフィックを許可した場合、このフィールドには [復号しない（不明な暗号スイート）（Do Not Decrypt (Unknown Cipher Suite)）] が表示されます。 証明書の詳細を表示するにはロック アイコン（  ）をクリックします。詳細については、暗号化接続に関連付けられた証明書の表示（39-34 ページ）を参照してください。
ユーザ（User）	ファイルの宛先のホスト（[受信側 IP（Receiving IP）]）にログインしたユーザ。 ユーザが宛先ホストに関連付けられているため、ユーザがファイルをアップロードしたファイル イベントに、ユーザが関連付けられないことに注意してください。

表 40-2　ファイル イベント フィールド(続き)

フィールド	説明
ファイル名(File Name)	ファイルの名前です。
傾向(Disposition)	以下のファイル性質のいずれかです。 • マルウェア(Malware)は、クラウドでそのファイルがマルウェアとして分類されていること、またはファイルの脅威スコアが、ファイル ポリシーで定義されたマルウェアしきい値を超えていることを示します。 • クリーン(Clean):クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。 • 不明(Unknown):クラウドが性質を割り当てる前にマルウェア クラウド ルックアップが行われたことを示します。ファイルは分類されていません。 • カスタム検出(Custom Detection):ユーザがカスタム検出リストにファイルを追加したことを示します。 • 使用不可(Unavailable)は、防御センター がマルウェア クラウド ルックアップを実行できなかったことを示します。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。 • N/A は、ファイル検出またはファイル ブロック ルールがファイルを処理し、防御センター がマルウェア クラウド ルックアップを行わなかったことを示します。
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(このファイルが以下の結果として検出された場合)。 • [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 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。詳細については、ネットワーク ファイル トラジェクトリの分析(40-42 ページ)を参照してください。
脅威スコア(Threat Score)	そのファイルに関連する最新の脅威スコア: • 低(Low)(●○○○) • 中(Medium)(●●○○) • 高(High)(●●●○) • 非常に高い(Very High)(●●●●) 動的分析のサマリー 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(Type)	ファイルのタイプ(HTML や MSEXE など)。
カテゴリ(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)。

表 40-2　ファイル イベント フィールド(続き)

フィールド	説明
サイズ(KB)(Size (KB))	ファイルのサイズ(KB 単位)。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判別すると、ファイル サイズが計算されずに、このフィールドがブランクになる場合があるので注意してください。
URI	ファイルの送信元の URI(ファイルをダウンロードした URL など)。
アーカイブ名(Archive Name)	ファイルが関連付けられているアーカイブ ファイル(存在する場合)の名前(`archive.zip` など)。アーカイブ ファイルの内容を表示するには、アーカイブ ファイルのイベント ビューア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 コンテンツの表示(View Archive Contents)] をクリックします。詳細については、アーカイブ ファイルの内容の表示(37-26 ページ)を参照してください。
アーカイブ SHA256(Archive SHA256)	ファイルが関連付けられているアーカイブ ファイル(存在する場合)の SHA256 ハッシュ値。
アーカイブ深度(Archive Depth)	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)。たとえば、`1` や `3` など。
アプリケーション プロトコル	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、クライアント、または Web アプリケーション カテゴリまたはタグ(Application Protocol, Client, or 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。表 45-2(45-12 ページ)を参照してください。
クライアント(Client)	ファイルを送信する接続で使用されるクライアント アプリケーション。
Web アプリケーション(Web Application)	HTTP を使用してファイルが送信された場合、接続で検出され、ファイルの送信に使用された Web アプリケーション(コンテンツまたは要求された URL)。
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。詳細については、表 45-2(45-12 ページ)を参照してください。
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。詳細については、表 45-2(45-12 ページ)を参照してください。
メッセージ(Message)	マルウェア性質が変更されたファイル(つまり、レトロスペクティブ マルウェア イベントに関連したファイル)で、性質がいつ、どのように変更されたかに関する情報。
ファイル ポリシー(File Policy)	ファイルを検出したファイル ポリシー。
Device	ファイルを検出したデバイスの名前。
セキュリティ コンテキスト(Security 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。システムがこのフィールドにデータを設定するのは、マルチ コンテキスト モードの ASA FirePOWER デバイスだけです。
メンバー数(Count)	各行の情報に一致するイベントの数。このフィールドが表示されるのは、2 つ以上の同一の行を作成する制限を適用した後です。

ファイル イベントの検索

ライセンス：Protection

防御センター の [検索（Search）] ページを使用して、特定のファイル イベントを検索し、その結果をイベント ビューアで表示できます。また、後で再利用するために検索条件を保存できます。カスタム分析のダッシュボード ウィジェット、レポート テンプレート、カスタム ユーザ ロールでも、保存した検索を使用できます。

覚えておくべき点として、検索結果は、検索するイベントの使用可能なデータに依存します。つまり、使用可能なデータによっては、検索の制約が適用されないことがあります。たとえば、[傾向（Disposition）] および [SHA256] フィールドにデータが入れられるのは、防御センターがマルウェア クラウド ルックアップを実行したファイルに限られます。

一般的な検索構文

システムは、各検索フィールドの横に有効な構文の例を示します。検索条件を入力する場合、次の点に留意してください。

- すべてのフィールドで否定（!）を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「A」または「B」または「C, D, E」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに A または B、または C、D、E のすべてを含むレコードが一致します。
- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク（*）を受け入れます。
- フィールドでその情報を利用できないイベントを示すには、そのフィールドで `n/a` を指定します。フィールドに情報が入力されているイベントを示すには `!n/a` を使用します。
- 特定のデバイス、およびグループ、スタック、またはクラスタ内のデバイスを検索するには、デバイス フィールドを使用します。検索での FireSIGHT システムによるデバイス フィールドの処理方法については、検索でのデバイスの指定（60-7 ページ）を参照してください。
- 検索条件としてオブジェクトを使用するには、検索フィールドの横に表示されるオブジェクトの追加アイコン（ ＋ ）をクリックします。

検索でのオブジェクトの使用など、検索構文の詳細については、イベントの検索（60-1 ページ）を参照してください。

ファイル イベントの特別な検索構文

前述の一般的な検索構文を補うために、以下のリストでは、ファイル イベントの特別な検索構文について説明しています。

送信側/受信側の大陸（Sending/Receiving Continent）

システムは **Sending Continent** または **Receiving Continent** が指定した大陸と一致するすべてのイベントを返します。

送信側/受信側の国（Sending/Receiving Country）

システムは **Sending Country** または **Receiving Country** が指定した国と一致するすべてのイベントを返します。

送信側/受信側の IP（Sending/Receiving IP）

システムは **Sending IP** または **Receiving IP** が指定した IP アドレスと一致するすべてのイベントを返します。

URI または Message

システムは部分一致を実行します。つまり、アスタリスクを使用せずに、フィールドの内容の全部または一部を検索できます。

ファイル ストレージ（File Storage）

以下の 1 つ以上を入力します。

- 保存済み（Stored）は、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。
- 接続で保存済み（Stored in connection）は、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（Failed）は、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。

実行された実際の SSL アクション（The SSL Actual Action taken）

システムが指定したアクションを適用した暗号化されたトラフィックのファイル イベントを表示するには、次のキーワードのいずれかを入力します。

- [復号しない（Do not Decrypt）] は、システムが復号しなかった接続を表します。
- [ブロック（Block）] および [リセットしてブロック（Block with Reset）] は、ブロックされた暗号化接続を表します。
- [復号（既知のキー）（Decrypt (Known Key)）] は、既知の秘密キーを使用して復号された着信接続を表します。
- [復号（キーの置き換え）（Decrypt (Replace Key)）] は、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された発信接続を表します。
- [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。

このカラムは、ファイル イベントのテーブル ビューに表示されません。

SSL 障害の理由（The SSL Failure Reason）

システムが指定された理由で復号化に失敗した暗号化されたトラフィックのファイル イベントを表示するには、次のキーワードのいずれかを入力します。

- 不明
- 不一致（No Match）
- Success

- キャッシュされないセッション(Uncached Session)
- 不明な暗号スイート(Unknown Cipher Suite)
- サポートされていない暗号スイート(Unsupported Cipher Suite)
- サポートされていない SSL バージョン(Unsupported SSL Version)
- SSL 圧縮の使用(SSL Compression Used)
- パッシブ モードで復号できないセッション(Session Undecryptable in Passive Mode)
- ハンドシェイク エラー(Handshake Error)
- 復号化エラー(Decryption Error)
- 保留サーバ名カテゴリ ルックアップ(Pending Server Name Category Lookup)
- 保留共通名カテゴリ ルックアップ(Pending Common Name Category Lookup)
- 内部エラー(Internal Error)
- ネットワーク パラメータを使用できません(Network Parameters Unavailable)
- 無効なサーバ証明書の処理(Invalid Server Certificate Handle)
- サーバ証明書フィンガープリントを使用できません(Server Certificate Fingerprint Unavailable)
- サブジェクト DN をキャッシュできません(Cannot Cache Subject DN)
- 発行元 DN をキャッシュできません(Cannot Cache Issuer DN)
- 不明の SSL バージョン(Unknown SSL Version)
- 外部証明書リストを使用できません(External Certificate List Unavailable)
- 外部証明書フィンガープリントを使用できません(External Certificate Fingerprint Unavailable)
- 内部証明書リストが無効です(Internal Certificate List Invalid)
- 内部証明書リストを使用できません(Internal Certificate List Unavailable)
- 内部証明書を使用できません(Internal Certificate Unavailable)
- 内部証明書フィンガープリントを使用できません(Internal Certificate Fingerprint Unavailable)
- サーバ証明書検証を使用できません(Server Certificate Fingerprint Unavailable)
- サーバ証明書検証エラー(Server Certificate Validation Failure)
- 無効なアクション(Invalid Action)

このカラムは、ファイル イベントのテーブル ビューに表示されません。

SSL 対象国(The SSL Subject Country)

証明書の対象の国に関連付けられている暗号化されたトラフィックのファイル イベントを表示するには、2 文字の ISO 3166-1 アルファ 2 国番号を入力します。

このカラムは、ファイル イベントのテーブル ビューに表示されません。

SSL 発行国(The SSL Issuer Country)

証明書発行者の国に関連付けられている暗号化されたトラフィックのファイル イベントを表示するには、2 文字の ISO 3166-1 アルファ 2 国番号を入力します。

このカラムは、ファイル イベントのテーブル ビューに表示されません。

SSL 証明書のフィンガープリント(SSL Certificate Fingerprint)

その証明書に関連付けられているトラフィックのファイル イベントを表示するには、その証明書の認証に使用される SHA ハッシュ値を入力するか、または貼り付けます。

このカラムは、ファイル イベントのテーブル ビューに表示されません。

SSL 公開キーのフィンガープリント（SSL Public Key Fingerprint）

その証明書に関連付けられているトラフィックのファイル イベントを表示するには、その証明書に含まれている公開キーの認証に使用される SHA ハッシュ値を入力するか、または貼り付けます。

このカラムは、ファイル イベントのテーブル ビューに表示されません。

ファイル イベントを検索するには、以下を行います。

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [検索（Search）] を選択します。

[検索（Search）] ページが表示されます。

手順 2　テーブル ドロップダウン リストから [ファイル イベント（File Events）] を選択します。

ページが適切な制約によって更新されます。

手順 3　次の項に記載されているように、該当するフィールドに検索基準を入力します。

- ファイル イベント テーブルのフィールドの詳細については、ファイル イベント フィールドの表を参照してください。
- ファイル イベントの特別な検索構文については、ファイル イベントの特別な検索構文（40-14 ページ）を参照してください。
- 公開キー証明書に関連するフィールドについては、暗号化接続に関連付けられた証明書の表示（39-34 ページ）を参照してください。

手順 4　必要に応じて検索を保存する場合は、[プライベート（Private）] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　カスタム ユーザ ロールのデータの制限として検索を使用する場合は、必ずプライベート検索として保存する**必要**があります。

手順 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [保存（Save）] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [保存（Save）] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[プライベート（Private）] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。
- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[新規として保存（Save As New）] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [保存（Save）] をクリックします。検索が保存され（[プライベート（Private）] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

手順 6　検索を開始するには、[検索（Search）] ボタンをクリックします。

検索結果は、現在の時刻範囲によって制限されるデフォルトのファイル イベントのワークフローに表示されます。

マルウェア イベントの操作

ライセンス: Malware またはすべて

サポートされるデバイス: 機能に応じて異なる

サポートされる防御センター: 機能に応じて異なる

システムは以下のタイミングでマルウェア イベントを 防御センター データベースに記録します。

- 管理対象デバイスがネットワーク トラフィックでファイルを検出し、そのファイルがマルウェア クラウド ルックアップでマルウェアとして識別された。
- 管理対象デバイスがネットワーク トラフィックでカスタム検出リストに含まれているファイルを検出した。
- ファイルのマルウェア性質が変更されたことをシステムが認識した。これらは、レトロスペクティブ マルウェア イベントと呼ばれます。
- 組織のエンドポイントにインストールされた FireAMP コネクタが脅威を検出し、その脅威を シスコ クラウドに伝えた。

FireAMP マルウェア検出がダウンロード時または実行時にエンドポイントで行われるのに対し、管理対象デバイスはネットワーク トラフィックでファイルを検出するため、これらのマルウェア イベントの情報は異なります。レトロスペクティブ マルウェア イベントには、他のネットワークベースのマルウェア イベントとも、エンドポイントベースのマルウェア イベントとも若干異なるデータが含まれます。

以降の項では、さまざまな種類のマルウェア イベントについて簡単に説明します。マルウェア検出の全体的なプロセスの詳細については、マルウェア防御とファイル制御について（37-2 ページ）を参照してください。

エンドポイントベース（FireAMP）のマルウェア イベント

組織が FireAMP サブスクリプションを持っている場合、各ユーザは自分のコンピュータやモバイル デバイスに FireAMP コネクタをインストールします。これらの軽量のエージェントは シスコ クラウドと通信し、それは防御センターと通信します。FireAMP 用のクラウド接続の操作（37-29 ページ）を参照してください。クラウドは脅威の通知や他の種類の情報（スキャン、隔離、ブロックされた実行、クラウドのリコールのデータなど）を送信できます。防御センター はこの情報をマルウェア イベントとしてデータベースに記録します。

（注）　エンドポイントベースのマルウェア イベントで報告される IP アドレスは、ネットワーク マップに（そして、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、FireAMP コネクタがインストールされている組織内のエンドポイントが、管理対象デバイスによって監視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。

ネットワーク トラフィックに基づくマルウェア イベント

サポートされるデバイス: シリーズ 2 と X-シリーズ を除くすべて

サポートされる防御センター: 任意（DC500 を除く）

Malware ライセンスを使用すると、管理対象デバイスは全体的なアクセス制御設定の一部として、ネットワーク トラフィック内のマルウェアを検出できます。ファイル ポリシーの概要と作成（37-11 ページ）を参照してください。

以下のシナリオでは、マルウェア イベントが生成される可能性があります。

- 管理対象デバイスが一連の特定のファイル タイプのいずれかを検出すると、防御センターはマルウェア クラウド ルックアップを実行します。これにより、ファイル性質として Malware、Clean、または Unknown が 防御センター に返されます。
- 防御センター がクラウドとの接続を確立できない場合や、それ以外でクラウドが使用できない場合、ファイル性質は Unavailable になります。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。
- 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、防御センター はファイル性質として Malware をそのファイルに割り当てます。
- SHA-256 値がカスタム検出リストに保存されているファイルを管理対象デバイスが検出した場合、防御センター はファイル性質としてカスタムム検出(Custom Detection)をそのファイルに割り当てます。
- クリーン リストに含まれているファイルを管理対象デバイスが検出した場合、防御センター はファイル性質として Clean をそのファイルに割り当てます。

防御センター は他のコンテキスト データとともに、ファイルの検出と性質のレコードをマルウェア イベントとして記録します。

(注)　ネットワーク トラフィックで検出され、FireSIGHT システム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。これは、ファイル内のマルウェアを検出するために、システムはまずそのファイル自体を検出する必要があるためです。詳細については、ファイル イベントの操作(40-8 ページ)およびキャプチャ ファイルの操作(40-33 ページ)を参照してください。

レトロスペクティブ マルウェア イベント

サポートされるデバイス: シリーズ 3、仮想

サポートされる防御センター: 任意(DC500 を除く)

ネットワーク トラフィックで検出されたマルウェア ファイルの場合、ファイル性質が変わることがあります。たとえば、シスコ クラウドがあるファイルを以前はクリーンであると識別したものの、今はマルウェアとして判断したり、その逆にマルウェアとして識別したファイルが実際にはクリーンだったと判断する場合があります。

前の週にマルウェア ルックアップを実行したファイルのファイル性質が変更された場合、クラウドは 防御センター に通知します。その場合、以下の 2 つが行われます。

- 防御センター が新しいレトロスペクティブ マルウェア イベントを生成します。

  この新しいレトロスペクティブ 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(防御センター 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。
- 防御センター はレトロスペクティブ イベントの関連する SHA-256 ハッシュ値を持つすで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、防御センター 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。新しい性質を除いて、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 Clean に変更された場合に、防御センター がそのマルウェア イベントをマルウェア テーブルから削除することはありません。そうする代わりに、イベントは単に性質の変更を反映します。つまり、性質が Clean のファイルがマルウェア テーブルに含められる場合があり、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。

いずれの場合でも、マルウェア イベントの **Message** に、性質がいつ、どのように変更されたかが示されます。以下に例を示します。

```
Retrospective Event, Mon Oct 1 20:44:00 2012 (UTC), Old Disp: Unknown, New Disp:
Malware
```

マルウェア イベントの使用

防御センター のイベント ビューアを使用して、マルウェア イベントの表示、検索、削除を行えます。さらに、Files Dashboard および Context Explorer では、ネットワークで検出されたファイル（マルウェア ファイルを含む）に関する詳細情報を、図やグラフを使って一目で知ることができます。ネットワーク ファイル トラジェクトリでは、個々のマルウェア ファイルの情報とそれらが時間の経過に伴ってネットワーク内をどのように移動してきたかに関する情報のサマリーが提供されるので、それらのファイルに関してより綿密に知ることができます。マルウェア検出データを使用して、相関ルールをトリガーしたり、レポートを作成したりできます。後者では、定義済みのマルウェア レポート テンプレートかカスタム レポート テンプレートを使用します。

詳細については、以下を参照してください。

- マルウェア イベントの表示（40-20 ページ）
- マルウェア イベント テーブルについて（40-22 ページ）
- マルウェア イベントの検索（40-29 ページ）

マルウェア イベントの表示

ライセンス：Malware またはすべて

FireSIGHT システムのイベント ビューアでは、マルウェア イベントをテーブルの形で表示でき、分析に関連した情報に応じてイベント ビューを操作することもできます。また、個々のマルウェア イベントに使用可能な情報は、ライセンスなどのさまざまな要因によって異なることに注意してください。詳細については、サービス サブスクリプション（65-8 ページ）を参照してください。

マルウェア 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。システムには、マルウェア イベント用の以下の定義済みのワークフローが付属しています。

- *マルウェアの概要（Malware Summary）*（デフォルト）：個々の脅威でグループ化された、検出マルウェアのリストを提供します。
- *マルウェア イベントの概要（Malware Event Summary）*：さまざまなマルウェア イベントのタイプとサブタイプの概要を提供します。
- *マルウェアを受信したホスト（Hosts Receiving Malware）*および*マルウェアを送信したホスト（Hosts Sending Malware）*：マルウェアを送受信したホストのリストを、それらのファイルの関連するマルウェア性質でグループ化した形で提供します。性質はマルウェア クラウド ルックアップまたはマルウェア ブロック ファイル ルールの結果として検出されたファイルに関してのみ表示されるので注意してください。
- *マルウェアを取り込んだアプリケーション（Applications Introducing Malware）*：組織のエンドポイントで検出されたマルウェアにアクセスしたか、そのマルウェアを実行したクライアント アプリケーションのリストを提供します。このリストから、それぞれの親クライアントによってアクセスされる個々のマルウェア ファイルにドリルダウンできます。

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。カスタム ワークフローを含む、さまざまなデフォルト ワークフローの指定の詳細については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

FireSIGHT システムは、Unicode（UTF8）ファイル名の表示および入力を Web インターフェイスのすべてのエリア（イベント ビューア、イベント検索、ダッシュボード、Context Explorer など）でサポートしています。ただし、PDF 形式で生成したレポートでは Unicode がサポートされないので注意してください。PDF レポートでは、Unicode ファイル名は翻字形式で表示されます。詳細については、レポートの生成と表示（57-29 ページ）を参照してください。

イベント ビューアを使用して、以下を行うことができます。

- イベントの検索、ソート、および制限と、表示されるイベントの時間範囲の変更
- 表示される列の指定（テーブル ビューのみ）
- IP アドレスに関連付けられたホスト プロファイル、またはユーザ ID に関連付けられたユーザの詳細およびホスト履歴の表示
- 特定のマルウェアが検出された接続の表示（ネットワークベースのマルウェア イベントのみ）
- 同じワークフロー内のさまざまなワークフロー ページを使用したイベントの表示
- 別のワークフローを使用したイベントの表示
- 特定の値で制限されるワークフロー内のページからページへのドリルダウン
- 後で同じデータに戻る（存在している場合）ための、現在のページおよび制約のブックマーク
- ファイルに関連付けられたルーティング可能 IP アドレスの位置情報の表示
- ファイルのトラジェクトリの表示
- アーカイブ ファイル内のネストされたファイルの表示
- 現在の制約を使用してレポート テンプレートを作成する
- データベースからのイベントの削除
- ファイル リストへのファイルの追加、ファイルのダウンロード、動的分析のためのファイルの送信、ファイルの SHA-256 値のフルテキストの表示
- ファイルの動的分析のサマリー レポート（使用可能な場合）の表示
- IP アドレスのコンテキスト メニューを使用した、ホワイトリストまたはブラックリストへの追加、あるいはマルウェア イベントに関連付けられたホストまたは IP アドレスに関する他の使用可能な情報の取得

シリーズ 2 デバイス、Blue Coat X-Series 向け Cisco NGIPS、および DC500 防御センター は、ネットワークベースのマルウェア防御およびアーカイブ ファイル インスペクションをサポートしていません。これは、表示されるデータに影響を及ぼす場合があるので注意してください。たとえば、シリーズ 2デバイスだけを管理するシリーズ 3防御センターは、エンドポイントベースのマルウェア イベントだけを表示できます。

カスタム ワークフローの作成など、イベント ビューアの使用の詳細については、ワークフローの概要と使用（58-1 ページ）を参照してください。

マルウェア イベントを表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [ファイル（Files）] > [マルウェア イベント（Malware Events）] を選択します。

デフォルトのマルウェア イベントのワークフローの最初のページが表示されます。表示される列の詳細については、マルウェア イベント テーブルについて（40-22 ページ）を参照してください。

マルウェア イベント テーブルについて

ライセンス: Malware またはすべて

サポートされるデバイス: 機能に応じて異なる

サポートされる防御センター: 機能に応じて異なる

組織内のエンドポイントにインストールされた FireAMP コネクタが脅威を検出した場合、または管理対象デバイスがネットワーク トラフィックでファイルを検出し、そのファイルがマルウェア クラウド ルックアップでマルウェアとして識別された場合、システムはマルウェア イベントを防御センター データベースに記録します。また、ファイルのマルウェア性質が変更されたことをシステムが認識した場合、システムはレトロスペクティブ マルウェア イベントを記録します。シリーズ 2 デバイス、Blue Coat X-Series 向け Cisco NGIPS、および DC500 防御センター は、ネットワークベースのマルウェア防御をサポートしていません。これは、表示されるデータに影響を及ぼす場合があるので注意してください。たとえば、シリーズ 2 デバイスだけを管理するシリーズ 3 防御センター は、エンドポイントベースのマルウェア イベントだけを表示できます。詳細については、マルウェア防御とファイル制御について（37-2 ページ）およびマルウェア イベントの操作（40-18 ページ）を参照してください。

マルウェア イベントのテーブル 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。マルウェア イベントのテーブル ビューのいくつかのフィールドは、デフォルトで表示されます。セッション中にフィールドを有効にするには、展開矢印（  ）をクリックして、検索制約を拡張してから、[無効列（Disabled Columns）] の下の列名をクリックします。

すべてのイベントで、すべてのフィールドにデータが入っている訳ではないことに留意してください。マルウェア イベントのタイプが異なれば、含まれる情報も異なる可能性があります。たとえば、FireAMP 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、エンドポイントベースのマルウェア イベントには、ファイル パスや呼び出し元のクライアント アプリケーションに関する情報などが含まれます。対照的に、管理対象デバイスはネットワーク トラフィックでマルウェア ファイルを検出するため、それらに関連したマルウェア イベントには、ファイルを送信するのに使用される接続に関する、ポート、アプリケーション プロトコル、および送信元 IP アドレスの情報が含まれます。

次の表では各マルウェア イベント フィールドがリストされており、マルウェア イベントのタイプに応じて、システムがそのフィールドに情報を表示するかどうかを示しています。DC500 防御センター は、送受信の大陸または国の位置情報をサポートしていないので注意してください。

表 40-3　マルウェア イベント フィールド

フィールド	説明	ネットワーク（Network）	エンドポイント（Endpoint）	クラウドからのレトロスペクティブ
時刻（Time）	イベントが生成された日時。	Yes	Yes	Yes
操作（Action）	ファイルが一致したルールのルール アクションに関連付けられているファイル ルール アクションと、関連するファイル ルール アクションのオプション。	Yes	No	Yes
送信側 IP（Sending IP）	検出されたマルウェアを送信しているホストの IP アドレス。	Yes	No	No

表 40-3　マルウェア イベント フィールド(続き)

フィールド	説明	ネットワーク（Network）	エンドポイント（Endpoint）	クラウドからのレトロスペクティブ
送信側の大陸（Sending Continent）	検出されたマルウェアを送信しているホストがある大陸。	Yes	No	Yes
送信側の国（Sending Country）	検出されたマルウェアを送信しているホストがある国。	Yes	No	No
受信側 IP（Receiving IP）	ネットワークベースのマルウェア イベントの場合、検出されたマルウェアを受信するホストの IP アドレス。 エンドポイントベースのマルウェア イベントの場合、FireAMP コネクタがインストールされていて、マルウェア イベントが発生したエンドポイントの IP アドレス。	Yes	Yes	No
受信側の大陸（Receiving Continent）	検出されたマルウェアを受信しているホストがある大陸。	Yes	No	Yes
受信側の国（Receiving Country）	検出されたマルウェアを受信しているホストがある国。	Yes	No	No
送信側のポート（Sending Port）	管理対象デバイスがマルウェアを検出したトラフィックによって使用されている送信元ポート。	Yes	No	No
受信側のポート（Receiving Port）	管理対象デバイスがマルウェアを検出したトラフィックによって使用されている宛先ポート。	Yes	No	No

表 40-3　マルウェア イベント フィールド(続き)

フィールド	説明	ネットワーク(Network)	エンドポイント(Endpoint)	クラウドからのレトロスペクティブ
SSL ステータス(SSL Status)	SSL ルールに関連したアクション、デフォルトのアクション、または暗号化接続をログに記録した復号できないトラフィック アクション。 • [ブロック(Block)] および [リセットしてブロック(Block with reset)] は、ブロックされた暗号化接続を表します。 • [復号(再署名)(Decrypt (Resign))] は、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(キーの置き換え)(Decrypt (Replace Key))] は、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された発信接続を表します。 • [復号(既知のキー)(Decrypt (Known Key))] は、既知の秘密キーを使用して復号された着信接続を表します。 • [復号しない(Do not Decrypt)] は、システムが復号しなかった接続を表します。 システムが暗号化接続を復号できなかった場合は、実行された復号不能のトラフィック アクションと障害の理由が表示されます。たとえば、システムが不明な暗号スイートで暗号化されたトラフィックを検出し、さらにインスペクションを行わずにそのトラフィックを許可した場合、このフィールドには [復号しない(不明な暗号スイート)(Do Not Decrypt (Unknown Cipher Suite))] が表示されます。 証明書の詳細を表示するにはロック アイコン( )をクリックします。詳細については、暗号化接続に関連付けられた証明書の表示(39-34 ページ)を参照してください。	Yes	No	No
ユーザ(User)	マルウェア イベントが発生したホスト(**受信側 IP**)のユーザ ネットワークベースのマルウェア 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。ユーザが宛先ホストに関連付けられているため、ユーザがマルウェア 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ていません。 エンドポイントベースのマルウェア イベントの場合、FireAMP コネクタがユーザ名を判別します。FireAMP 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。	Yes	Yes	No
イベント タイプ(Event Type)	マルウェア イベントのタイプ。イベント タイプの完全なリストについては、マルウェア イベントのタイプ(40-28 ページ)を参照してください。	Yes	Yes	Yes

表 40-3　マルウェア イベント フィールド(続き)

フィールド	説明	ネットワーク(Network)	エンドポイント(Endpoint)	クラウドからのレトロスペクティブ
イベント サブタイプ(Event Subtype)	マルウェア検出につながった FireAMP アクション(Create、Execute、Move、または Scan など)。	No	Yes	No
脅威名(Threat Name)	検出されたマルウェアの名前。	Yes	Yes	Yes
ファイル名(File Name)	マルウェア ファイルの名前。	Yes	Yes	No
ファイル性質(File Disposition)	以下のファイル性質のいずれかです。 • マルウェア(Malware)は、クラウドでそのファイルがマルウェアとして分類されていること、またはファイルの脅威スコアが、ファイル ポリシーで定義されたマルウェアしきい値を超えていることを示します。 • クリーン(Clean):クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。 • 不明(Unknown):クラウドが性質を割り当てる前にマルウェア クラウド ルックアップが行われたことを示します。ファイルは分類されていません。 • カスタム検出(Custom Detection):ユーザがカスタム検出リストにファイルを追加したことを示します。 • 使用不可(Unavailable)は、防御センターがマルウェア クラウド ルックアップを実行できなかったことを示します。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。 Clean 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 Clean に変更された場合だけです。レトロスペクティブ マルウェア イベント(40-19 ページ)を参照してください。	Yes	No	Yes
ファイル SHA256(File 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。詳細については、ネットワーク ファイル トラジェクトリの分析(40-42 ページ)を参照してください。	Yes	Yes	Yes

表 40-3　マルウェア イベント フィールド(続き)

フィールド	説明	ネットワーク(Network)	エンドポイント(Endpoint)	クラウドからのレトロスペクティブ
脅威スコア(Threat Score)	そのファイルに関連する最新の脅威スコア: • 低(Low)(●○○○) • 中(Medium)(●●○○) • 高(High)(●●●○) • 非常に高い(Very High)(●●●●) 動的分析のサマリー 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。	Yes	No	No
ファイル パス(File Path)	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)。	No	Yes	No
ファイル タイプ(File Type)	マルウェア ファイルのファイル タイプ(HTML や MSEXE など)。	Yes	Yes	No
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)。	Yes	Yes	No
ファイルのタイムスタンプ(File Timestamp)	マルウェア ファイルが作成された日時。	No	Yes	No
ファイル サイズ(File Size)(KB)	マルウェア ファイルのサイズ(KB 単位)。	Yes	Yes	No
ファイル URI(File URI)	マルウェア ファイルの送信元の URI(ファイルをダウンロードした URL など)。	Yes	No	No
アーカイブ名(Archive Name)	マルウェア ファイルが関連付けられているアーカイブ ファイル(存在する場合)の名前(archive.zip など)。	Yes	Yes	No
アーカイブ SHA256(Archive SHA256)	マルウェア ファイルが関連付けられているアーカイブ ファイル(存在する場合)の SHA256 ハッシュ値。アーカイブ ファイルの内容を表示するには、そのアーカイブ ファイルのイベント ビューア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 コンテンツの表示(View Archive Contents)] をクリックします。詳細については、アーカイブ ファイルの内容の表示 (37-26 ページ)を参照してください。	Yes	Yes	No
アーカイブ深度(Archive Depth)	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)。たとえば、1 や 3 など。	Yes	Yes	No
アプリケーション ファイル名(Application File Name)	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**。	No	Yes	No

表 40-3　マルウェア イベント フィールド(続き)

フィールド	説明	ネットワーク(Network)	エンドポイント(Endpoint)	クラウドからのレトロスペクティブ
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、FireAMP 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。	No	Yes	No
アプリケーション プロトコル(Application Protocol)	管理対象デバイスがマルウェア 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。	Yes	No	No
アプリケーション プロトコル、クライアント、または Web アプリケーション カテゴリまたはタグ(Application Protocol, Client, or Web Application Category or Tag)	アプリケーションの機能を理解するうえで役立つ、アプリケーションの特性を示す基準。表 45-2(45-12 ページ)を参照してください。	Yes	No	Yes
クライアント(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。	Yes	No	Yes
Web アプリケーション(Web Application)	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。	Yes	No	Yes
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害の痕跡(IOC)をトリガーしたかどうか。エンドポイントベースのマルウェア検出が IOC ルールをトリガーした場合、タイプ `FireAMP IOC` で、完全なマルウェア イベントが生成されます。IOC の詳細については、侵害の兆候(痕跡)について(45-22 ページ)を参照してください。	Yes	Yes	Yes
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。詳細については、表 45-2(45-12 ページ)を参照してください。	Yes	No	Yes
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。詳細については、表 45-2(45-12 ページ)を参照してください。	Yes	No	Yes

表 40-3　マルウェア イベント フィールド(続き)

フィールド	説明	ネットワーク(Network)	エンドポイント(Endpoint)	クラウドからのレトロスペクティブ
ディテクタ(Detector)	マルウェアを識別した FireAMP ディテクタ(ClamAV、Spero、SHA など)。	No	Yes	No
メッセージ(Message)	マルウェア イベントに関連する追加情報。 ネットワークベースのマルウェア イベントの場合、このフィールドにデータが入れられるのは、性質が変更されたファイルだけです。レトロスペクティブ マルウェア イベント(40-19 ページ)を参照してください。	Yes	Yes	No
FireAMP Cloud	イベントが発信された FireAMP クラウドの名前。	No	Yes	No
Device	ネットワークベースのマルウェア イベントの場合、マルウェア ファイルを検出したデバイスの名前。 エンドポイントベースのマルウェア イベントおよびクラウドによって生成されるレトロスペクティブ マルウェア イベントの場合、防御センター の名前。	Yes	Yes	Yes
セキュリティ コンテキスト(Security 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。システムがこのフィールドにデータを設定するのは、マルチ コンテキスト モードの ASA FirePOWER デバイスだけです。	Yes	Yes	Yes
メンバー数(Count)	各行の情報に一致するイベントの数。このフィールドが表示されるのは、2 つ以上の同一の行を作成する制限を適用した後です。	適用対象外	適用対象外	適用対象外

マルウェア イベントのタイプ

ライセンス: Malware またはすべて

サポートされるデバイス: 機能に応じて異なる

サポートされる防御センター: 機能に応じて異なる

ネットワークベースのマルウェア イベントの場合、イベントのタイプは以下のいずれかになります。

- ファイル転送中に検出された脅威(Threat Detected in Network File Transfer)
- ファイル転送中に検出された脅威(レトロスペクティブ)(Threat Detected in Network File Transfer (retrospective))

エンドポイントベースのマルウェア イベントは、以下のタイプのいずれかになります。

- ブロックされた実行(Blocked Execution)
- 隔離のクラウド リコール(Cloud Recall Quarantine)
- 隔離のクラウド リコールの試みに失敗(Cloud Recall Quarantine Attempt Failed)
- 隔離のクラウド リコールの開始(Cloud Recall Quarantine Started)
- クラウド リコールを隔離から復元(Cloud Recall Restore from Quarantine)
- クラウド リコールの隔離からの復元に失敗(Cloud Recall Restore from Quarantine Failed)

- クラウド リコールの隔離からの復元が開始（Cloud Recall Restore from Quarantine Started）
- FireAMP IOC
- 隔離エラー（Quarantine Failure）
- 隔離されたアイテムが復元された（Quarantined Item Restored）
- 隔離の復元に失敗（Quarantine Restore Failed）
- 隔離の復元が開始（Quarantine Restore Started）
- スキャン完了、検出なし（Scan Completed, No Detections）
- スキャン完了、検出あり（Scan Completed With Detections）
- スキャンに失敗（Scan Failed）
- スキャンが開始（Scan Started）
- Threat Detected
- 検出された脅威が実行中（Threat Detected in Exclusion）
- 検疫された脅威（Threat Quarantined）

ファイルのトラジェクトリ マップにマルウェア イベントが含まれている場合、イベントのタイプは、ファイル転送中に検出された脅威（Threat Detected in Network File Transfer）、ファイル転送中に検出された脅威（レトロスペクティブ）（Threat Detected in Network File Transfer (retrospective)）、検出された脅威（Threat Detected）、検出された脅威が実行中（Threat Detected in Exclusion）、検疫された脅威（Threat Quarantined）のいずれかになります。詳細については、ネットワーク ファイル トラジェクトリの操作（40-39 ページ）を参照してください。

シリーズ 2 デバイス、Blue Coat X-Series 向け Cisco NGIPS、および DC500 防御センター は、ネットワークベースのマルウェア防御をサポートしていません。これは、表示されるデータに影響を及ぼす場合があるので注意してください。たとえば、シリーズ 2 デバイスだけを管理するシリーズ 3 防御センターは、エンドポイントベースのマルウェア イベントだけを表示できます。

マルウェア イベントの検索

ライセンス：Malware またはすべて

防御センター の [検索（Search）] ページを使用して、特定のマルウェア イベントを検索し、その結果をイベント ビューアで表示できます。また、後で再利用するために検索条件を保存できます。カスタム分析のダッシュボード ウィジェット、レポート テンプレート、カスタム ユーザ ロールでも、保存した検索を使用できます。

サンプルとしてシステムに付属している検索には、[保存済み検索（Saved Searches）] リストで (シスコ) というラベルが付いています。

覚えておくべき点として、検索結果は、検索するイベントの使用可能なデータに依存します。つまり、使用可能なデータによっては、検索の制約が適用されないことがあります。たとえば、エンドポイントベースのマルウェア イベントは、ネットワーク トラフィックを検査する管理対象デバイスの結果として生成されないため、接続情報（ポート、アプリケーション プロトコルなど）は含まれません。

一般的な検索構文

システムは、各検索フィールドの横に有効な構文の例を示します。検索条件を入力する場合、次の点に留意してください。

- すべてのフィールドで否定(!)を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。
  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、`A, B, "C, D, E"` を検索すると、指定したフィールドに「`A`」または「`B`」または「`C, D, E`」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、`A, B, "C, D, E"` をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに `A` または `B`、または `C`、`D`、`E` のすべてを含むレコードが一致します。
- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク(*)を受け入れます。
- フィールドでその情報を利用できないイベントを示すには、そのフィールドで `n/a` を指定します。フィールドに情報が入力されているイベントを示すには `!n/a` を使用します。
- 特定のデバイス、およびグループ、スタック、またはクラスタ内のデバイスを検索するには、デバイス フィールドを使用します。検索での FireSIGHT システムによるデバイス フィールドの処理方法については、検索でのデバイスの指定(60-7 ページ)を参照してください。
- 検索条件としてオブジェクトを使用するには、検索フィールドの横に表示されるオブジェクトの追加アイコン(+)をクリックします。

検索でのオブジェクトの使用など、検索構文の詳細については、イベントの検索(60-1 ページ)を参照してください。

マルウェア イベントの特別な検索構文

前述の一般的な検索構文を補うために、以下のリストでは、マルウェア イベントの特別な検索構文について説明しています。

送信側/受信側の IP(Sending/Receiving IP)

システムは **Sending IP** または **Receiving IP** が指定した IP アドレスと一致するすべてのイベントを返します。

イベント タイプ(Event Type)

特定のマルウェア イベント タイプのイベントを検索する場合(マルウェア イベントのタイプ(40-28 ページ)を参照)、イベント タイプを引用符で囲みます(`"Scan Completed With Detection"` など)。そうしないと、システムは部分一致を実行します。つまり、同じストリングで引用符を使用しない場合、システムは次のタイプのイベントを返します。

- スキャン完了、検出なし(`Scan Completed, No Detections`)
- スキャン完了、検出あり(`Scan Completed With Detection`)

イニシエータ/レスポンダの大陸（Initiator/Responder Continent）

システムは **Initiator Continent** または **Responder Continent** が指定した大陸と一致するすべてのイベントを返します。

イニシエータ/レスポンダの国（Initiator/Responder Country）

システムは、**Initiator Country** または **Responder Country** が、指定した国に一致するすべてのイベントを返します。

URI または Message

システムは部分一致を実行します。つまり、アスタリスクを使用せずに、フィールドの内容の全部または一部を検索できます。

実行された実際の SSL アクション（The SSL Actual Action taken）

システムが指定したアクションを適用した暗号化されたトラフィックのマルウェア イベントを表示するには、次のキーワードのいずれかを入力します。

- [復号しない(Do not Decrypt)] は、システムが復号しなかった接続を表します。
- [ブロック（Block）] および [リセットしてブロック（Block with Reset）] は、ブロックされた暗号化接続を表します。
- [復号（既知のキー）（Decrypt (Known Key)）] は、既知の秘密キーを使用して復号された着信接続を表します。
- [復号（キーの置き換え）（Decrypt (Replace Key)）] は、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された発信接続を表します。
- [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。

このカラムは、マルウェア イベントのテーブル ビューに表示されません。

SSL 障害の理由（The SSL Failure Reason）

システムが指定された理由で復号化に失敗した暗号化トラフィックのマルウェア イベントを表示するには、次のキーワードのいずれかを入力します。

- 不明
- 不一致(No Match)
- Success
- キャッシュされないセッション(Uncached Session)
- 不明な暗号スイート(Unknown Cipher Suite)
- サポートされていない暗号スイート(Unsupported Cipher Suite)
- サポートされていない SSL バージョン(Unsupported SSL Version)
- SSL 圧縮の使用(SSL Compression Used)
- パッシブ モードで復号できないセッション(Session Undecryptable in Passive Mode)
- ハンドシェイク エラー(Handshake Error)
- 復号化エラー(Decryption Error)
- 保留サーバ名カテゴリ ルックアップ(Pending Server Name Category Lookup)
- 保留共通名カテゴリ ルックアップ(Pending Common Name Category Lookup)
- 内部エラー(Internal Error)
- ネットワーク パラメータを使用できません(Network Parameters Unavailable)
- 無効なサーバ証明書の処理(Invalid Server Certificate Handle)

- サーバ証明書フィンガープリントを使用できません(Server Certificate Fingerprint Unavailable)
- サブジェクト DN をキャッシュできません(Cannot Cache Subject DN)
- 発行元 DN をキャッシュできません(Cannot Cache Issuer DN)
- 不明の SSL バージョン(Unknown SSL Version)
- 外部証明書リストを使用できません(External Certificate List Unavailable)
- 外部証明書フィンガープリントを使用できません(External Certificate Fingerprint Unavailable)
- 内部証明書リストが無効です(Internal Certificate List Invalid)
- 内部証明書リストを使用できません(Internal Certificate List Unavailable)
- 内部証明書を使用できません(Internal Certificate Unavailable)
- 内部証明書フィンガープリントを使用できません(Internal Certificate Fingerprint Unavailable)
- サーバ証明書検証を使用できません(Server Certificate Fingerprint Unavailable)
- サーバ証明書検証エラー(Server Certificate Validation Failure)
- 無効なアクション(Invalid Action)

このカラムは、マルウェア イベントのテーブル ビューに表示されません。

SSL 対象国(The SSL Subject Country)

証明書サブジェクトの国に関連付けられている暗号化されたトラフィックのマルウェア イベントを表示するには、2 文字の ISO 3166-1 アルファ 2 国番号を入力します。

このカラムは、マルウェア イベントのテーブル ビューに表示されません。

SSL 発行国(The SSL Issuer Country)

証明書発行者の国に関連付けられている暗号化されたトラフィックを表示するには、2 文字の ISO 3166-1 アルファ 2 国番号を入力します。

このカラムは、マルウェア イベントのテーブル ビューに表示されません。

SSL 証明書のフィンガープリント(SSL Certificate Fingerprint)

証明書に関連付けられているトラフィックを表示するには、その証明書の認証に使用される SHA ハッシュ値を入力するか、または貼り付けます。

このカラムは、マルウェア イベントのテーブル ビューに表示されません。

SSL 公開キーのフィンガープリント(SSL Public Key Fingerprint)

証明書に関連付けられているトラフィックを表示するには、その証明書に含まれている公開キーの認証に使用される SHA ハッシュ値を入力するか、または貼り付けます。

このカラムは、マルウェア イベントのテーブル ビューに表示されません。

マルウェア イベントを検索するには、以下を行います。

アクセス: Admin/Any Security Analyst

手順 1　[分析(Analysis)] > [検索(Search)] を選択します。

[検索(Search)] ページが表示されます。

手順 2　テーブル ドロップダウン リストから [マルウェア イベント(Malware Events)] を選択します。

ページが適切な制約によって更新されます。

手順 3　次の項に記載されているように、該当するフィールドに検索基準を入力します。

- マルウェア イベント テーブルのフィールドの詳細については、マルウェア イベント フィールドの表を参照してください。
- マルウェア イベントの特別な検索構文については、マルウェア イベントの特別な検索構文（40-30 ページ）を参照してください。
- 公開キー証明書に関連するフィールドについては、暗号化接続に関連付けられた証明書の表示（39-34 ページ）を参照してください。

手順 4　必要に応じて検索を保存する場合は、[プライベート（Private）] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。または、すべてのユーザに対し検索を保存するにはこのチェックボックスをオフのままにします。

ヒント　カスタム ユーザ ロールのデータの制限として検索を使用する場合は、**必ず**プライベート検索として保存する必要があります。

手順 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [保存（Save）] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [保存（Save）] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[プライベート（Private）] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。
- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[新規として保存（Save As New）] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [保存（Save）] をクリックします。検索が保存され（[プライベート（Private）] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

手順 6　検索を開始するには、[検索（Search）] ボタンをクリックします。

検索結果は、現在の時刻範囲によって制限されるデフォルトのマルウェア イベントのワークフローに表示されます。

キャプチャ ファイルの操作

ライセンス：Malware

サポートされるデバイス：シリーズ 2 と X-シリーズ を除くすべて

サポートされる防御センター：任意（DC500 を除く）

システムは、現在適用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キャプチャしたときに記録を行います。イベント ビューアから、キャプチャ ファイルに関連した情報（SHA-256 値に関連した最新のファイル名、ファイルの性質および脅威スコア、ファイル ストレージのステータス、アーカイブ インスペクションのステータス、ファイルが動的分析のために手動で送信されたかなど）を表示できます。

(注)　マルウェアはキャプチャされる前に検出される必要があるため、マルウェアを含むデバイスでキャプチャされたファイルは、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。詳細については、ファイル イベントの操作（40-8 ページ）およびマルウェア イベントの操作（40-18 ページ）を参照してください。

防御センター のイベント ビューアを使用して、キャプチャされたファイルの表示および検索を行ったり、キャプチャされたファイルを動的分析のために送信したりできます。さらに、Files Dashboard では、ネットワークで検出されたファイル（マルウェア ファイルを含む）に関する詳細情報を、図やグラフを使って一目で知ることができます。

詳細については、以下を参照してください。

- キャプチャ ファイルの表示（40-34 ページ）
- キャプチャ ファイル テーブルについて（40-35 ページ）
- キャプチャ ファイルの検索（40-37 ページ）

キャプチャ ファイルの表示

ライセンス：Malware

FireSIGHT システム のイベント ビューアでは、キャプチャ イベントをテーブルの形で表示したり、分析に関連した情報に応じてイベント ビューを操作したりすることができます。

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。システムには、キャプチャ ファイル用の以下の定義済みのワークフローが付属しています。

- *キャプチャ ファイルの概要（Captured File Summary）*（デフォルト）：タイプ、カテゴリ、および脅威スコアに基づく、キャプチャ ファイルの概要を提供します。
- *動的解析のステータス（Dynamic Analysis Status）*：動的分析のために送信したかどうかに基づいて、キャプチャ ファイルのカウントを提供します。

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。カスタム ワークフローを含む、さまざまなデフォルト ワークフローの指定の詳細については、イベント ビュー設定の設定（71-3 ページ）を参照してください。

FireSIGHT システムは、Unicode（UTF8）ファイル名の表示および入力を Web インターフェイスのすべてのエリア（イベント ビューア、イベント検索、ダッシュボード、Context Explorer など）でサポートしています。ただし、PDF 形式で生成したレポートでは Unicode がサポートされないので注意してください。PDF レポートでは、Unicode ファイル名は翻字形式で表示されます。詳細については、レポートの生成と表示（57-29 ページ）を参照してください。

イベント ビューアを使用して、以下を行うことができます。

- イベントの検索、ソート、および制限と、表示されるイベントの時間範囲の変更
- 表示される列の指定（テーブル ビューのみ）
- 同じワークフロー内のさまざまなワークフロー ページを使用したイベントの表示
- 別のワークフローを使用したイベントの表示
- 特定の値で制限されるワークフロー内のページからページへのドリルダウン
- 後で同じデータに戻る（存在している場合）ための、現在のページおよび制約のブックマーク
- ファイルのトラジェクトリの表示

- アーカイブ ファイルの内容とインスペクションのステータスの表示
- ファイル リストへのファイルの追加、ファイルのダウンロード、動的分析のためのファイルの送信、ファイルの SHA-256 値のフルテキストの表示
- ファイルの動的分析のサマリー レポート（使用可能な場合）の表示
- 動的分析のための最大 25 個のファイルの送信
- 現在の制約を使用してレポート テンプレートを作成する

シリーズ 2 デバイス、Blue Coat X-Series 向け Cisco NGIPS、および DC500 防御センター は、ネットワークベースのマルウェア防御およびアーカイブ ファイル インスペクションをサポートしていません。これは、表示されるデータに影響を及ぼす場合があるので注意してください。たとえば、シリーズ 2デバイスだけを管理するシリーズ 3防御センターは、キャプチャ ファイルを表示できません。

カスタム ワークフローの作成など、イベント ビューアの使用の詳細については、ワークフローの概要と使用（58-1 ページ）を参照してください。

ファイル イベントを表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [ファイル（Files）] > [キャプチャ済みファイル（Captured Files）] を選択します。

デフォルトのファイル イベントのワークフローの最初のページが表示されます。表示される列の詳細については、キャプチャ ファイル テーブルについて（40-35 ページ）を参照してください。

キャプチャ ファイル テーブルについて

ライセンス：Malware

防御センター は、適用されているファイル ポリシーの設定に従って、監視されているネットワーク トラフィックで送信されるファイルを管理対象デバイスがキャプチャしたときに記録を行います。

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。キャプチャ ファイルのテーブル ビューのいくつかのフィールドは、デフォルトで表示されます。セッション中にフィールドを有効にするには、展開矢印（  ）をクリックして、検索制約を拡張してから、[無効列（Disabled Columns）] の下の列名をクリックします。以下の表は、キャプチャ ファイル フィールドについて説明しています。

表 40-4　キャプチャ ファイル フィールド

フィールド	説明
最終更新時刻（Last Changed）	このファイルに関連した情報が最後に更新された時刻。
ファイル名（File Name）	ファイルの SHA-256 ハッシュ値に関連した、最後に検出されたファイル名。

表 40-4　キャプチャ ファイル フィールド(続き)

フィールド	説明
傾向(Disposition)	以下のファイル性質のいずれかです。 • マルウェア(Malware)は、クラウドでそのファイルがマルウェアとして分類されていること、またはファイルの脅威スコアが、ファイル ポリシーで定義されたマルウェアしきい値を超えていることを示します。 • クリーン(Clean):クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。 • 不明(Unknown):クラウドが性質を割り当てる前にマルウェア クラウド ルックアップが行われたことを示します。ファイルは分類されていません。 • カスタム検出(Custom Detection):ユーザがカスタム検出リストにファイルを追加したことを示します。 • 使用不可(Unavailable)は、防御センター がマルウェア クラウド ルックアップを実行できなかったことを示します。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。 • N/A は、ファイル検出またはファイル ブロック ルールがファイルを処理し、防御センターがマルウェア クラウド ルックアップを行わなかったことを示します。
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。詳細については、ネットワーク ファイル トラジェクトリの分析(40-42 ページ)を参照してください。
脅威スコア(Threat Score)	そのファイルに関連する最新の脅威スコア: • 低(Low)(●○○○) • 中(Medium)(●●○○) • 高(High)(●●●○) • 非常に高い(Very High)(●●●●) 動的分析のサマリー 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(Type)	ファイルのタイプ(HTML や MSEXE など)。
カテゴリ(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)。
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。

表 40-4　キャプチャ ファイル フィールド(続き)

フィールド	説明
アーカイブ インスペクション ステータス(Archive Inspection Status)	アーカイブ ファイルでの、アーカイブ インスペクションのステータス: • [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ています。ファイルが再びシステムを通過する場合、完全な情報が使用可能になります。 • [抽出済み(Extracted)] は、システムがアーカイブの内容を抽出し、検査できたことを示しています。 • [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、許可された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ています。 • [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ています。 • [検査不能(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、そのイベント ビューア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 コンテンツの表示(View Archive Contents)] を選択します。詳細については、アーカイブ ファイルのインスペクション オプションの設定 (37-24 ページ)を参照してください。
分析ステータス(Analysis Status)	ファイルが動的分析のために送信されているかどうか。
最終送信日時(Last Sent)	ファイルが動的分析のためにクラウドに最後に送信された時刻。

キャプチャ ファイルの検索

ライセンス: Malware

防御センター の [検索(Search)] ページを使用して、特定のキャプチャ ファイルを検索し、その結果をイベント ビューアで表示できます。また、後で再利用するために検索条件を保存できます。カスタム分析のダッシュボード ウィジェット、レポート テンプレート、カスタム ユーザ ロールでも、保存した検索を使用できます。

覚えておくべき点として、検索結果は、検索するイベントの使用可能なデータに依存します。つまり、使用可能なデータによっては、検索の制約が適用されないことがあります。たとえば、ファイルが動的分析のために送信されていない場合は、関連する脅威スコアがない場合があります。

一般的な検索構文

システムは、各検索フィールドの横に有効な構文の例を示します。検索条件を入力する場合、次の点に留意してください。

- すべてのフィールドで否定(!)を使用できます。
- すべてのフィールドで検索値のカンマ区切りリストを使用できます。指定したフィールドにリストされた値のいずれかを含むレコードは、その検索条件に一致します。
- すべてのフィールドで、引用符で囲んだカンマ区切りリストを検索値として使用できます。

  - 値を 1 つのみ含むことができるフィールドの場合、検索条件に一致するのは、指定したフィールドに引用符内の文字列と同じ文字列が含まれるレコードです。たとえば、A, B, "C, D, E" を検索すると、指定したフィールドに「A」または「B」または「C, D, E」を含むレコードが一致します。これにより、使用できる値にカンマを含むフィールドでの一致が可能です。
  - 同時に複数の値を含むことができるフィールドの場合、引用符で囲んだカンマ区切りリスト内のすべての値が指定したフィールドに含まれるレコードが検索条件に一致します。
  - 同時に複数の値を含むことができるフィールドについては、引用符で囲んだカンマ区切りリストだけでなく、単一の値も検索条件に使用することができます。たとえば、A, B, "C, D, E" をこれらの文字の 1 つまたは複数を含むことができるフィールドで検索すると、指定したフィールドに A または B、または C、D、E のすべてを含むレコードが一致します。
- 検索により、すべてのフィールドに対して指定した検索条件と一致するレコードのみが返されます。
- 多くのフィールドでは、ワイルドカードとして 1 つ以上のアスタリスク(*)を受け入れます。
- フィールドでその情報を利用できないイベントを示すには、そのフィールドで n/a を指定します。フィールドに情報が入力されているイベントを示すには !n/a を使用します。
- 検索条件としてオブジェクトを使用するには、検索フィールドの横に表示されるオブジェクトの追加アイコン(+)をクリックします。

検索でのオブジェクトの使用など、検索構文の詳細については、イベントの検索(60-1 ページ)を参照してください。

キャプチャ ファイルの特別な検索構文

前述の一般的な検索構文を補うために、以下の表では、キャプチャ ファイルの特別な検索構文について説明しています。

表 40-5　キャプチャ ファイルの特別な検索構文

検索条件	特別な構文
ストレージ ステータス(Storage Status)	以下の 1 つ以上を指定してください。 • ファイル保存済み(File Stored):デバイスに保存されたすべてのキャプチャ ファイルを返します • ファイル保存不能(Unable to Store File):デバイスに保存されなかったすべてのキャプチャ ファイルを返します
動的分析ステータス(Dynamic Analysis Status)	以下の 1 つ以上を指定してください。 • 分析用に送信済み(Sent for Analysis):動的分析のためにキューに入れられたすべてのキャプチャ ファイルを返します • 分析用に未送信(Not Sent for Analysis):動的分析のために送信されなかったすべてのキャプチャ ファイルを返します • 分析完了(Analysis Complete):動的分析のために送信されず、脅威スコアおよび動的分析のサマリー レポートを受け取った、すべてのキャプチャ ファイルを返します • 以前に分析済み(Previously Analyzed):動的分析のために再度送信しようとした、キャッシュに入れられた脅威スコアを持つすべてのファイルを返します • 失敗(分析タイムアウト)(Failure (Analysis Timeout)):クラウドがまだ結果を返していない動的分析のために送信されたすべてのキャプチャ ファイルを返します • 失敗(ネットワークの問題)(Failure (Network Issue)):ネットワーク接続の障害のために動的分析に送信できなかったすべてのファイルを返します • 失敗(ファイル実行不能)(Failure (Cannot Run File)):クラウドがテスト環境で実行できなかった動的分析のために送信されたすべてのファイルを返します

キャプチャ ファイルを検索するには、以下を行います。

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [検索（Search）] を選択します。

[検索（Search）] ページが表示されます。

手順 2　テーブル ドロップダウン リストから [キャプチャ済みファイル（Captured Files）] を選択します。

ページが適切な制約によって更新されます。

手順 3　該当するフィールドに検索基準を入力します。

キャプチャ ファイル テーブルのフィールドの詳細については、キャプチャ ファイル フィールドの表を参照してください。

手順 4　必要に応じて検索を保存する場合は、[プライベート（Private）] チェックボックスをオンにしてプライベートとして検索を保存すると、本人だけがアクセスできるようになります。本人のみではなくすべてのユーザを対象にする場合は、このチェックボックスをオフのままにして検索を保存します。

ヒント　カスタム ユーザ ロールのデータの制限として検索を使用する場合は、必ずプライベート検索として保存する**必要**があります。

手順 5　必要に応じて、後で再度使用する検索を保存できます。次の選択肢があります。

- [保存（Save）] をクリックして、検索条件を保存します。

  新しい検索の場合、ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [保存（Save）] をクリックします。保存済みの既存の検索で新しい条件を保存する場合、プロンプトは表示されません。検索が保存され（[プライベート（Private）] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

- 新しい検索を保存するか、以前保存した検索を変更して作成した検索に名前を割り当てるには、[新規として保存（Save As New）] をクリックします。

  ダイアログボックスに検索の名前を要求するプロンプトが表示されます。一意の検索名を入力して [保存（Save）] をクリックします。検索が保存され（[プライベート（Private）] を選択した場合は本人のアカウントでのみ閲覧可能）、後で実行できます。

手順 6　検索を開始するには、[検索（Search）] ボタンをクリックします。

検索結果は、現在の時刻範囲によって制限されるデフォルトのキャプチャ イベントのワークフローに表示されます。

ネットワーク ファイル トラジェクトリの操作

ライセンス：Malware またはすべて

サポートされるデバイス：機能に応じて異なる

サポートされる防御センター：機能に応じて異なる

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。このマップを使用して、どのホストがマルウェアを転送した可能性があるか、またどのホストにリスクがあるかを判別したり、ファイル転送の傾向を観察したりできます。

トラジェクトリ マップは、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示します。マップの作成に使用されるデータは、ネットワークベースのマルウェア イベント（システムがマルウェア クラウド ルックアップを実行してマルウェア性質を返したファイル イベント）から取得される場合も、マルウェアの検出およびブロックに関連した特定のエンドポイントベースのマルウェア イベント（Threat Detected または Threat Quarantined イベント タイプ）から取得される場合もあります。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。

システムがマルウェア クラウド ルックアップを実行できるファイル タイプの伝送を追跡できます。ファイルのトラジェクトリに直接アクセスするには、[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（[分析（Analysis）] > [ファイル（Files）] > [ネットワーク ファイル トラジェクトリ（Network File Trajectory）]）を使用して、特定のファイルを見つけることができます。さらに、侵入を分析して、関連するファイルのトラジェクトリを確認する場合、接続、ファイル、マルウェア イベントの Context Explorer、ダッシュボード、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。

単一のトランジェクトリ マップが表示するデータは、アプライアンスに適用されるライセンスによって異なります。次の表は、さまざまな種類のファイル トランジェクトリを追跡するのに必要なライセンスをリストしています。

表 40-6　ネットワーク ファイル トランジェクトリのライセンス要件

表示対象	必要なライセンス
ネットワークベースのファイルおよびマルウェア トラジェクトリ	Malware
エンドポイントベースの脅威および隔離の追跡	任意（FireAMP サブスクリプションが必要）

詳細については、マルウェア防御とファイル制御について（37-2 ページ）を参照してください。

注意すべき点として、DC500 で Malware ライセンスは使用できず、シリーズ 2 デバイスや Blue Coat X-Series 向け Cisco NGIPS で Malware ライセンスを有効にすることもできないため、それらのアプライアンスを使用して、個々のファイルのキャプチャ/保存/ブロック、動的分析のためのファイルの送信、アーカイブ ファイルの内容の表示、マルウェア クラウド ルックアップを行うファイルのファイル トラジェクトリの表示を行うことはできません。ただし、エンドポイントベースの脅威および隔離の追跡のためにファイル トラジェクトリを表示することは可能です。

詳細については、次の項を参照してください。

- ネットワーク ファイル トラジェクトリの確認（40-40 ページ）
- ネットワーク ファイル トラジェクトリの分析（40-42 ページ）

ネットワーク ファイル トラジェクトリの確認

ライセンス：Malware またはすべて

サポートされるデバイス：機能に応じて異なる

サポートされる防御センター：機能に応じて異なる

キャプチャされたファイル、イベント イベント、およびマルウェア イベントを確認する際に、Context Explorer、適切に設定されたダッシュボード ウィジェット、さまざまなイベント ビューからファイルのトラジェクトリ マップを表示できます。また、最後に表示されたネットワーク ファイル トラジェクトリおよび最後に検出されたマルウェアを [ネットワーク ファイル トラジェクトリ リスト(Network File Trajectory List)] ページから確認することもできます。

詳細については、次の項を参照してください。

- [上位ファイル名(Top File Names)] グラフの表示(56-27 ページ)
- Context Explorer データのドリルダウン(56-41 ページ)
- Custom Analysis ウィジェットについて(55-13 ページ)
- アーカイブ ファイルのインスペクション オプションの設定(37-24 ページ)
- ファイル イベント テーブルについて(40-10 ページ)
- マルウェア イベント テーブルについて(40-22 ページ)
- キャプチャ ファイル テーブルについて(40-35 ページ)
- 接続イベントとセキュリティ インテリジェンス イベントで利用可能な情報(39-12 ページ)
- ネットワーク ファイル トラジェクトリへのアクセス(40-41 ページ)

ネットワーク ファイル トラジェクトリへのアクセス

ライセンス: Malware またはすべて

サポートされるデバイス: 機能に応じて異なる

サポートされる防御センター: 機能に応じて異なる

[ネットワーク ファイル トラジェクトリ リスト(Network File Trajectory List)] ページを使用して、最新の検出されたマルウェアを分析するため、または特定の脅威を追跡するために、ある SHA256 ハッシュ値を持つファイルを見つけることができます。

このページには、ネットワークで最後に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表示できます。フィールドの詳細については、ファイル イベント テーブルについて(40-10 ページ)を参照してください。

また、このページに含まれる検索ボックスを使用して、SHA256 ハッシュ値またはファイル名に基づくか、ファイルを送信または受信するホストの IP アドレスで、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ら、[ファイル SHA256(File SHA256)] 値をクリックして詳細なトラジェクトリ マップを表示できます。詳細については、ネットワーク ファイル トラジェクトリの分析(40-42 ページ)を参照してください。

FireSIGHT システムは、Unicode(UTF8)ファイル名の表示および入力を Web インターフェイスのすべてのエリア(イベント ビューア、イベント検索、ダッシュボード、Context Explorer など)でサポートしています。ただし、PDF 形式で生成したレポートでは Unicode がサポートされないので注意してください。PDF レポートでは、Unicode ファイル名は翻字形式で表示されます。詳細については、レポートの生成と表示(57-29 ページ)を参照してください。

注意すべき点として、DC500 で Malware ライセンスは使用できず、シリーズ 2 デバイスや Blue Coat X-Series 向け Cisco NGIPS で Malware ライセンスを有効にすることもできないため、それらのアプライアンスを使用して、マルウェア クラウド ルックアップを行うファイルのファイル トラジェクトリを表示することはできません。

[ネットワーク ファイル トラジェクトリ リスト(Network File Trajectory List)] ページからファイルを見つけるには、以下を行います。

アクセス:任意(Any)

手順 1　[分析(Analysis)] > [ファイル(Files)] > [ネットワーク ファイル トラジェクトリ(Network File Trajectory)] を選択します。

[ネットワーク ファイル トラジェクトリ リスト(Network File Trajectory List)] ページが表示され、最近表示したファイルと最近のマルウェアのリストが示されます。

手順 2　オプションで、追跡するファイルの完全な SHA256 ハッシュ値、ホスト IP アドレス、ファイル名を検索フィールドに入力して、Enter を押すこともできます。

[クエリ結果(Query Results)] ページが表示され、検索に一致するすべてのファイルがリストされます。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。

ネットワーク ファイル トラジェクトリの分析

ライセンス: Malware またはすべて

サポートされるデバイス:機能に応じて異なる

サポートされる防御センター:機能に応じて異なる

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、ネットワークを介してファイルを追跡できます。ファイルのトラジェクトリは、ファイルに関するサマリー情報を提供し、時間の経過に伴うデータ ポイントをグラフにしたマップを表示します。また、データ ポイントに関係したイベント データをテーブルにリストします。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、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。

注意すべき点として、DC500 で Malware ライセンスは使用できず、シリーズ 2 デバイスや Blue Coat X-Series 向け Cisco NGIPS で Malware ライセンスを有効にすることもできないため、それらのアプライアンスを使用して、マルウェア クラウド ルックアップを行うファイルのファイル トラジェクトリを表示することはできません。

詳細については、次の項を参照してください。

- サマリー情報(40-42 ページ)
- トラジェクトリ マップ(40-45 ページ)
- [イベント(Events)] テーブル(40-48 ページ)

サマリー情報

ライセンス: Malware またはすべて

サポートされるデバイス:機能に応じて異なる

サポートされる防御センター:機能に応じて異なる

ファイルのトラジェクトリ ページには、ファイルに関する基本的な情報（ファイル識別情報、ネットワーク上でファイルが最初に発見された時間および最後に発見された時間、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。

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。

次の表では、サマリー情報フィールドについて説明されています。

表 40-7　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（Name）]	説明
ファイル SHA256（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 SHA256 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。 ファイルのダウンロード アイコン（ ）をクリックすると、ファイルがローカル コンピュータにダウンロードされます。プロンプトが出力されたら、ファイルをダウンロードすることを確認します。ファイルを保存するには、ブラウザのプロンプトに従います。ファイルをダウンロードできない場合、このアイコンはグレー表示されます。 **注意**　シスコは、有害な結果が生じるのを防ぐために、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、ダウンロード先をセキュアに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。
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 SHA256 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。
ファイル タイプ（File Type）	ファイルのタイプ（`HTML` や `MSEXE` など）。
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）。
親アプリケーション（Parent Application）	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**。 このフィールドは、エンドポイントベースのマルウェア イベントにだけ表示されます。
最初の確認日時（First Seen）	管理対象デバイスまたは FireAMP コネクタがファイルを最初に検出した時刻と、そのファイルを最初にアップロードしたホストの IP アドレス。

表 40-7　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(続き)

[名前(Name)]	説明
最終表示(Last Seen)	管理対象デバイスまたは FireAMP コネクタがファイルを最後に検出した時刻と、そのファイルを最後にアップロードしたホストの IP アドレス。
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。
送受信ホスト数(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、[送受信ホスト数の内訳(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。
送受信ホスト数の内訳(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。
現在の性質(Current Disposition)	以下のファイル性質のいずれかです。 • マルウェア(Malware)は、クラウドでそのファイルがマルウェアとして分類されていること、またはファイルの脅威スコアが、ファイル ポリシーで定義されたマルウェアしきい値を超えていることを示します。 • クリーン(Clean):クラウドでそのファイルがクリーンとして分類されているか、ユーザがファイルをクリーン リストに追加したことを示します。 • 不明(Unknown):クラウドが性質を割り当てる前にマルウェア クラウド ルックアップが行われたことを示します。ファイルは分類されていません。 • カスタム検出(Custom Detection):ユーザがカスタム検出リストにファイルを追加したことを示します。 • 使用不可(Unavailable)は、防御センター がマルウェア クラウド ルックアップを実行できなかったことを示します。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。 • N/A は、ファイル検出またはファイル ブロック ルールがファイルを処理し、防御センター がマルウェア クラウド ルックアップを行わなかったことを示します。 クリーン リストまたはカスタム検出リストに対してファイルの追加や削除を行うには、編集アイコン( )をクリックします。 このフィールドは、ネットワークベースのマルウェア イベントにだけ表示されます。
アーカイブ コンテンツ(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。[アーカイブ コンテンツ(Archive Contents)] ウィンドウでコンテンツ ファイルの情報を表示するには、表示アイコン( )をクリックします。 アーカイブ ファイルのインスペクションの詳細については、アーカイブ ファイルのインスペクション オプションの設定(37-24 ページ)を参照してください。
脅威名(Threat Name)	ファイルに関連付けられたマルウェア脅威の名前。 このフィールドは、エンドポイントベースのマルウェア イベントにだけ表示されます。

表 40-7　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(続き)

[名前(Name)]	説明
脅威スコア(Threat Score)	ファイルの脅威スコア: • 低(Low)(●○○○) • 中(Medium)(●●○○) • 高(High)(●●●○) • 非常に高い(Very High)(●●●●) 動的分析のサマリー 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。 その脅威スコアのすべてのキャプチャ ファイルを表示するには、脅威スコア リンクをクリックします。 動的分析のためにクラウドにファイルを送信するには、クラウド アイコン(☁)をクリックします。ファイルを送信できない場合、またはクラウドに接続できない場合は、このアイコンはグレーで表示されます。

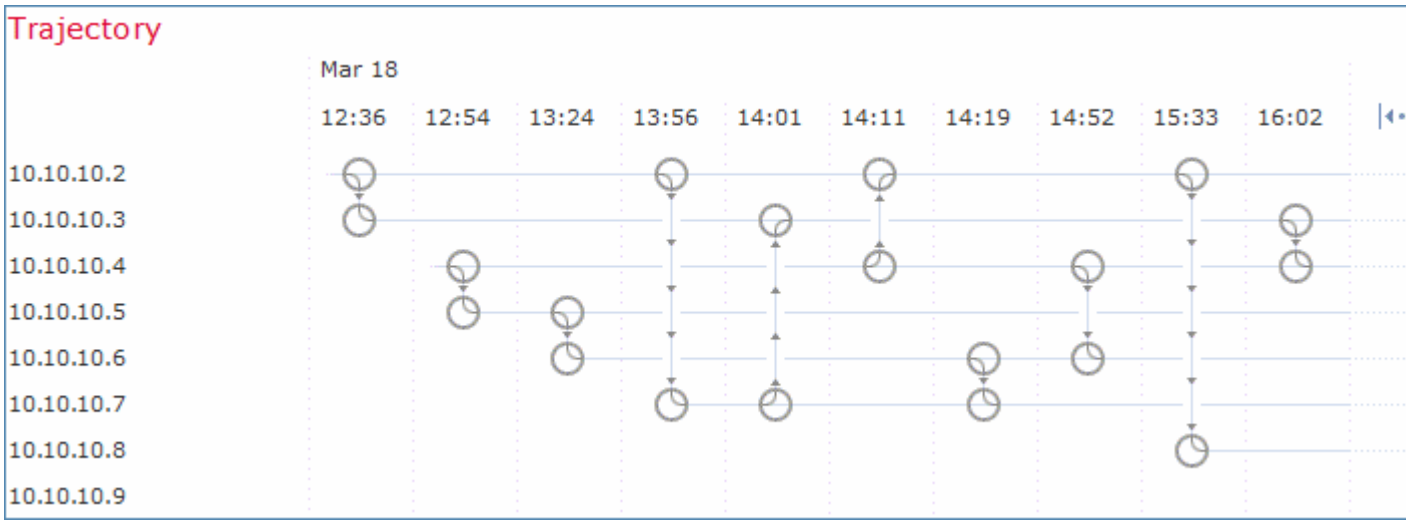
トラジェクトリ マップ

ライセンス: Malware またはすべて

サポートされるデバイス:機能に応じて異なる

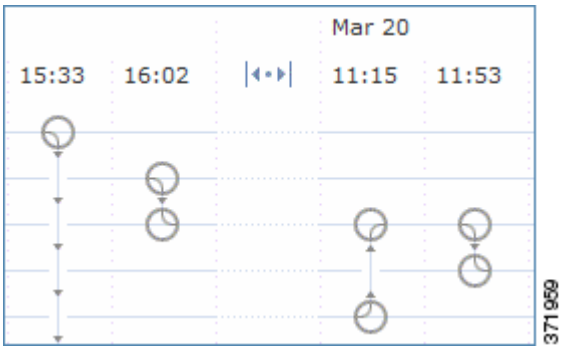
サポートされる防御センター:機能に応じて異なる

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。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レトロスペクティブ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。次の図は、トラジェクトリ マップの例を示しています。



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、レトロスペクティブ 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 SHA256 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。次の図では、イベントが省略され、矢印アイコンが示されています。

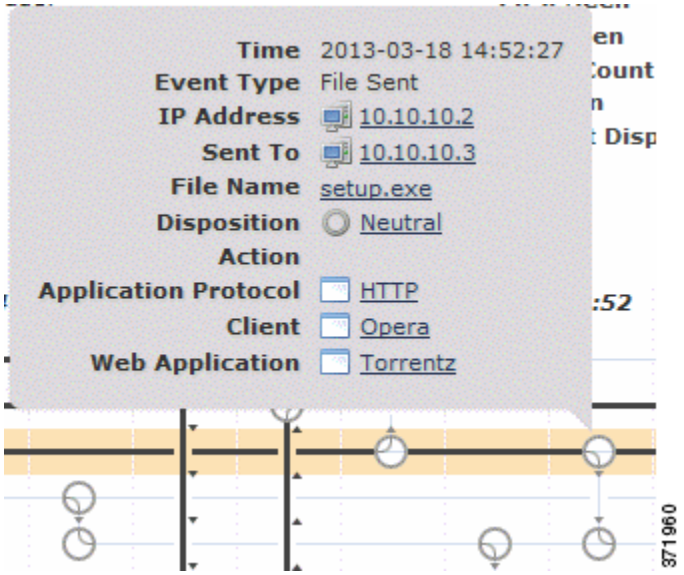


矢印アイコン（|◂•▸|）をクリックすると、[ファイル サマリー（File Summary）] イベント ビューで示されているすべてのイベントが表示されます。デフォルトの [ファイル イベント（File Events）] ワークフローの最初のページが新しいウィンドウで開き、ファイル タイプに基づいて制限されて、すべての余分のイベントが表示されます。エンドポイントベースのマルウェア イベントが表示されない場合、[マルウェア イベント（Malware Events）] テーブルに切り替えて、それらを表示する必要があります。

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。

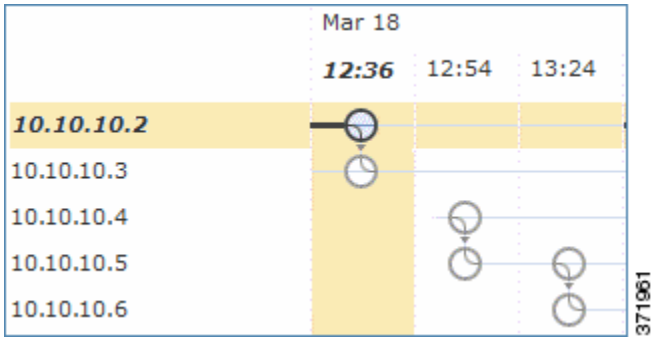
エンドポイントベースのマルウェア イベントには 1 つアイコンが含まれます。レトロスペクティブ イベントでは、ファイルで検出された各ホストのコラムにアイコンが表示されます。ファイル転送イベントでは、縦線でつながれた 2 つのアイコン（ファイル送信アイコンとファイル受信アイコン）が常に含まれます。矢印は、送信側から受信側へのファイル転送方向を示します。

イベント アイコン（◔）上にポインタを移動させると、イベント アイコンのサマリー情報を表示できます。表示されるサマリー情報は、[イベント（Events）] テーブルに表示される情報と一致しています。次の図は、イベント アイコンのサマリー情報を示しています。



イベントのサマリー情報のリンクをクリックすると、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、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。[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開きクリックした基準値と一致するすべてのファイル イベントが表示されます。

IP アドレスが関係するファイル イベントが最初に発生した時点を見つけるには、そのアドレスをクリックします。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。[イベント(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。次の図は、IP アドレスをクリックした後にパスが強調表示されている様子を示しています。

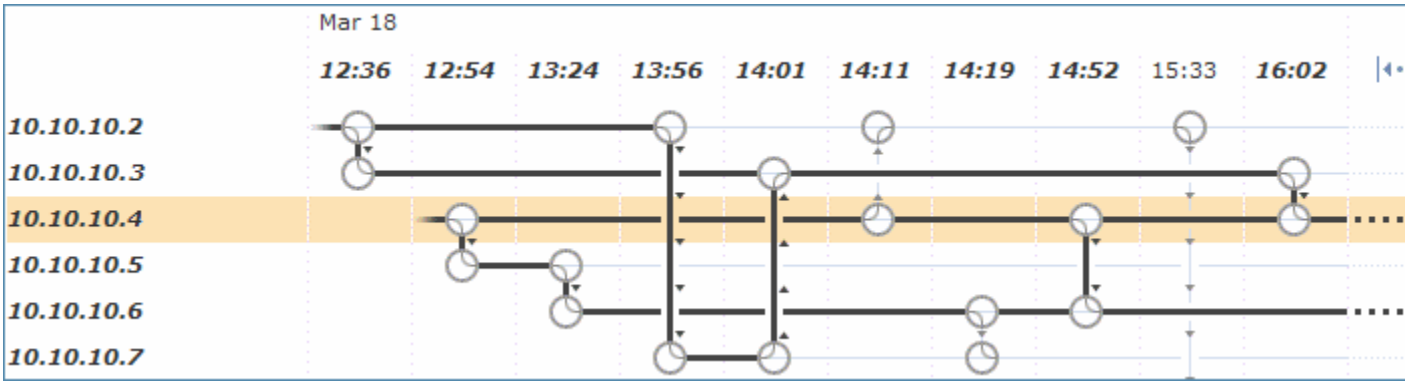


ネットワークを介したファイルの進行状況を追跡するために、データ ポイントをクリックして、選択したデータ ポイントに関連するすべてのデータ ポイントを含むパスを強調表示できます。これには、次のタイプのイベントに関連付けられたデータ ポイントが含まれます。

- 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
- 関連付けられている IP アドレスが関係する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 アドレスが関係する場合、その他方の IP アドレスが関係するエンドポイントベースのマルウェア イベント

次の図は、イベント アイコンをクリックした後でパスが強調表示されている様子を示しています。



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。[イベント（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。

[イベント（Events）] テーブル

ライセンス：Malware またはすべて

サポートされるデバイス：機能に応じて異なる

サポートされる防御センター：機能に応じて異なる

[イベント（Events）] テーブルには、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。列見出しをクリックすると、イベントを昇順または降順でソートできます。テーブル行を選択して、マップ内のデータ ポイントを強調表示できます。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。フィールドの詳細については、ファイル イベント テーブルについて（40-10 ページ）を参照してください。