



## 検出イベント

---

以下のトピックでは、ディスカバリ イベントを操作する方法について説明します。

- 検出イベントの要件と前提条件 (1 ページ)
- 検出イベントの検出データとアイデンティティ データ (1 ページ)
- ディスカバリ イベントの統計情報の表示 (3 ページ)
- ディスカバリ パフォーマンス グラフの表示 (6 ページ)
- ディスカバリおよびアイデンティティ ワークフローの使用 (7 ページ)
- 検出イベントの操作の履歴 (73 ページ)

## 検出イベントの要件と前提条件

### モデルのサポート

任意

### サポートされるドメイン

任意

### ユーザの役割

- 管理者
- セキュリティ アナリスト (Security Analyst)

## 検出イベントの検出データとアイデンティティ データ

システムは、モニタ対象のネットワークで検出された変更を表すイベントのテーブルを生成します。このテーブルを使用して、ネットワークのユーザアクティビティを確認し、応答方法を決定できます。ネットワーク検出およびアイデンティティポリシーは、収集するデータ、モニ

## ■ 検出イベントの検出データとアイデンティティ データ

タするネットワークセグメント、およびそのために使用する特定のハードウェアインターフェイスの種類を指定します。

検出およびアイデンティティイベントテーブルを使用して、ネットワークのホスト、アプリケーション、およびユーザに関連付けられている脅威を特定できます。システムには事前定義のワークフローセットが用意されており、これを使用して、システムで生成されるイベントを分析することができます。また、特定のニーズに合った情報のみ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。

分析用にネットワーク検出およびアイデンティティデータを収集し、保存するには、ネットワーク検出およびアイデンティティポリシーを設定する必要があります。アイデンティティポリシーを設定した後、アクセスコントロールポリシーで呼び出して、トラフィックのモニタに使用するデバイスに展開する必要があります。

ネットワーク検出ポリシーは、ホスト、アプリケーション、および権限のないユーザデータを提供します。アイデンティティポリシーは、権限のあるユーザー データを提供します。

次の検出イベントテーブルは、[分析 (Analysis)]>[ホストおよび分析 (Hosts and Analysis)]>[ユーザ (Users)]メニューにあります。

検出イベント テーブル	検出データが入力されましたか。	アイデンティティ データが入力されますか。
ホスト (Hosts)	はい	非対応
ホストの侵害の兆候	はい	非対応
アプリケーション	はい	非対応
アプリケーション詳細 (Application Details)	はい	非対応
サーバ	はい	非対応
ホスト属性 (Host Attributes)	はい	非対応
検出イベント	はい	はい
ユーザの侵害の兆候 (User Indications of Compromise)	はい	はい
アクティブ セッション (Active Sessions)	はい	はい
ユーザ アクティビティ (User Activity)	はい	はい
ユーザー	はい	はい
脆弱性 (Vulnerabilities)	はい	非対応
サードパーティの脆弱性 (Third-Party Vulnerabilities)	はい	非対応

# ディスカバリイベントの統計情報の表示

[ディスカバリ統計情報 (Discovery Statistics) ] ページには、システムで検出されたホスト、イベント、プロトコル、アプリケーションプロトコル、オペレーティングシステムの概要が表示されます。

ページには、最後の 1 時間の統計情報、および累計の統計情報が示されます。特定のデバイス、またはすべてのデバイスについての統計情報を表示することができます。サマリに示されているイベント、サーバー、オペレーティングシステム、またはオペレーティングシステムのベンダーをクリックして、ページ上のエントリに一致するイベントを表示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。

## 手順

**ステップ1** [概要 (Overview) ] > [概要 (Summary) ] > [検出統計 (Discovery Statistics) ] を選択します。

**ステップ2** [デバイスの選択 (Select Device) ] リストから、統計情報を表示するデバイスを選択します。オプションで、Firewall Management Center で管理されるすべてのデバイスの統計情報を表示するには、[すべて (All) ] を選択します。

**ステップ3** 次の選択肢があります。

- [統計情報サマリ (Statistics Summary) ] セクション (4 ページ) で説明されているように、[統計サマリー (Statistics Summary) ] に一般的な統計情報を表示します。
- [イベントの中断 (Event Breakdown) ] で、表示するイベントタイプをクリックします。イベントが1つも表示されない場合は、[時間枠の変更](#)で説明されているように、時間範囲を調整する必要があるかもしれません。
- [プロトコルの中断 (Protocol Breakdown) ] で、検出されたホストによって現在使用されているプロトコルを表示します。
- [アプリケーションプロトコルの中断 (Application Protocol Breakdown) ] で、表示するアプリケーションプロトコルの名前をクリックします。
- [OS の中断 (OS Breakdown) ] で、[OS 名 (OS Name) ] または[OS ベンダー (OS Vendor) ] をクリックします。

## 関連トピック

[\[イベント分類 \(Event Breakdown\) \] セクション \(5 ページ\)](#)

[\[プロトコル分類 \(Protocol Breakdown\) \] セクション \(5 ページ\)](#)

[\[アプリケーションプロトコル分類 \(Application Protocol Breakdown\) \] セクション \(5 ページ\)](#)

## ■ [統計情報サマリ (Statistics Summary) ] セクション

### [OS 分類 (OS Breakdown) ] セクション (6 ページ)

## [統計情報サマリ (Statistics Summary) ] セクション

[統計情報サマリ (Statistics Summary) ] セクションの行の説明は次のとおりです。

### 合計イベント数 (Total Events)

Firewall Management Center に格納されているディスカバリ イベントの合計数。

### 過去 1 時間のイベントの合計 (Total Events Last Hour)

最後の 1 時間に生成されたディスカバリ イベントの合計数。

### 過去 1 日のイベントの合計 (Total Events Last Day)

最後の 1 日に生成されたディスカバリ イベントの合計数。

### アプリケーションプロトコル合計数 (Total Application Protocols)

検出されたホストで実行されているサーバのアプリケーションプロトコルの合計数。

### IP ホストの合計 (Total IP Hosts)

一意の IP アドレスによって特定された検出済みホストの合計数。

### MAC ホストの合計 (Total MAC Hosts)

IP アドレスで特定されない検出済みホストの合計数。

すべてのデバイス、または特定のデバイスのどちらについてのディスカバリ統計情報を参照している場合でも、[MAC ホストの合計 (Total MAC Hosts) ] の統計情報は同じになることに注意してください。これは、管理対象デバイスが IP アドレスに基づいてホストを検出するためです。この統計情報は、他の方法によって識別され、特定の管理対象デバイスに依存しないすべてのホストの合計を表します。

### ルータの合計 (Total Routers)

ルータとして識別された検出ノードの合計数。

### ブリッジの合計 (Total Bridges)

ブリッジとして識別された検出ノードの合計数。

### ホスト制限の使用 (Host Limit Usage)

使用中のホスト制限のパーセンテージ合計。ホストの制限は、Firewall Management Center のモデルによって定義されます。すべての管理対象デバイスについての統計情報を表示している場合は、ホストの使用制限のみが表示されることに注意してください。



(注) ホストの制限に達してホストが削除されると、ディスカバリ データを消去するネットワークマップ上にホストは表示されなくなります。

#### 最後に受け取ったイベント (Last Event Received)

最後のディスカバリ イベントが行われた日付と時間。

#### 最後に受信した接続 (Last Connection Received)

最後の接続が完了した日付と時間。

## [イベント分類 (Event Breakdown) ] セクション

[イベント分類 (Event Breakdown) ] セクションには、データベースに格納されている各イベントタイプの合計数のカウントの他に、ネットワーク検出の各タイプのカウント、および最後の1時間で発生したホスト入力イベントが示されます。

[イベント分類 (Event Breakdown) ] セクションを使用して、ディスカバリ イベントおよびホスト入力イベントの詳細を表示することもできます。

#### 関連トピック

[検出イベントおよびホスト入力イベント \(10 ページ\)](#)

## [プロトコル分類 (Protocol Breakdown) ] セクション

[プロトコル分類 (Protocol Breakdown) ] セクションには、検出されたホストで使用されているプロトコルが示されます。このセクションには、検出されたそれぞれのプロトコル名、プロトコルスタックの「レイヤ」、およびプロトコルを使用して通信しているホストの合計数が表示されます。

## [アプリケーションプロトコル分類 (Application Protocol Breakdown) ] セクション

[アプリケーションプロトコル分類 (Application Protocol Breakdown) ] セクションには、検出されたホストで使用されているアプリケーションプロトコルが示されます。このセクションには、プロトコル名、最後の1時間にアプリケーションプロトコルを実行したホストの合計数、いずれかのポイントでプロトコルの実行が検出されたホストの合計数が表示されます。

[アプリケーションプロトコル分類 (Application Protocol Breakdown) ] セクションではさらに、検出されたプロトコルを使用しているサーバーの詳細を表示することもできます。

#### 関連トピック

[サーバー データ \(35 ページ\)](#)

## [OS 分類 (OS Breakdown) ] セクション

[OS 分類 (OS Breakdown) ] セクションには、監視対象ネットワーク上で稼動しているオペレーティングシステム、およびオペレーティングシステムのベンダー、各オペレーティングシステムを実行しているホストの合計数が示されます。

オペレーティングシステムの名前またはバージョンの値が `unknown` の場合は、オペレーティングシステムまたはそのバージョンが、システムのフィンガープリントの内容と一致しないことを意味します。値が `pending` の場合は、オペレーティングシステムまたはそのバージョンを識別するための十分な情報がシステムで収集されていないことを意味します。

[OS 分類 (OS Breakdown) ] セクションを使用して、検出されたオペレーティングシステムの詳細を表示することができます。

### 関連トピック

[ホストデータ \(19 ページ\)](#)

## ディスカバリパフォーマンス グラフの表示

ディスカバリイベントを使用して、管理対象デバイスのパフォーマンス統計情報を示すグラフを生成することができます。

新しいデータは5分ごとに統計グラフに蓄積されます。したがって、グラフをすばやくリロードしても、次の5分の差分更新が実行されるまでデータは変更されていない場合があります。

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。

### 始める前に

適切なネットワーク検出ポリシーを編集して、アプリケーション、ホスト、およびユーザーを含めます（これは、システムパフォーマンスに影響を与える可能性があります）。[ネットワーク検出ルールの設定](#)および[アクションと検出されるアセット](#)を参照してください。

このタスクを実行するには、管理者ユーザーまたはメンテナンスユーザーである必要があります。

### 手順

**ステップ1** [概要 (Overview) ] > [概要 (Summary) ] > [検出パフォーマンス (Discovery Performance) ] を選択します。

**ステップ2** [デバイスの選択 (Select Device) ] リストから、Firewall Management Center または対象とする管理対象デバイスを選択します。

**ステップ3** [ディスカバリパフォーマンス グラフ タイプ \(7 ページ\)](#) で説明されているように、[グラフの選択 (Select Graph(s)) ] リストから、作成するグラフの種類を選択します。

**ステップ4** [時間範囲の選択 (Select Time Range) ] リストから、グラフに使用する時間範囲を選択します。

ステップ5 [グラフ (Graph)] をクリックして、選択した統計情報をグラフ化します。

## ディスカバリ パフォーマンス グラフ タイプ

次に、使用できるグラフのタイプについて説明します。

### 処理されたイベント数/秒

Data Correlator が 1 秒間に処理するイベントの数を表します。

### 処理された接続数/秒

Data Correlator が 1 秒間に処理する接続の数を表します。

### 生成されたイベント数/秒

システムが 1 秒間に生成するイベントの数を表します。

### メガビット/秒

ディスカバリ プロセスによって 1 秒間に分析されたトラフィック数（メガビット）を表します。

### 平均バイト/パケット

ディスカバリ プロセスによって分析された各パケットに含まれるバイト数の平均を表します。

### キロパケット/秒

ディスカバリ プロセスで 1 秒間に分析されるパケット数を 1000 単位で表します。

## ディスカバリおよびアイデンティティワークフローの使用

Firewall Management Center は、ネットワークで生成されるディスカバリおよびアイデンティティデータの分析で使用できるイベントワークフロー セットを提供します。ワークフローはネットワーク マップとともに、ネットワーク 資産に関する主要な情報源になります。

Firewall Management Center には、ディスカバリおよびアイデンティティデータ、検出されたホストとそのホストの属性、サーバー、アプリケーション、アプリケーションの詳細、脆弱性、ユーザー アクティビティ、ユーザーに関する事前定義されたワークフローが用意されています。ユーザーはカスタム ワークフローを作成することもできます。

## 手順

---

**ステップ1** 事前定義されたワークフローにアクセスするには、以下を実行します。

- ディスカバリとホスト入力データ：[ディスカバリ イベントとホスト入力イベントの表示（17 ページ）](#) を参照してください。
- ホストデータ：[ホストデータの表示（20 ページ）](#) を参照してください。
- ホスト属性データ：[ホスト属性の表示（27 ページ）](#) を参照してください。
- ホストまたはユーザーの侵害の兆候データ：[侵害兆候データの表示と処理（30 ページ）](#) を参照してください。
- サーバー データ：[サーバー データの表示（35 ページ）](#) を参照してください。
- アプリケーションデータ：[アプリケーションデータの表示（39 ページ）](#) を参照してください。
- アプリケーション詳細データ：[アプリケーション詳細データの表示（42 ページ）](#) を参照してください。
- アクティブセッションデータ：[アクティブセッションデータの表示（64 ページ）](#) を参照してください。
- ユーザー データ：[ユーザー データの表示（67 ページ）](#) を参照してください。
- ユーザー アクティビティデータ：[ユーザー アクティビティデータの表示（70 ページ）](#) を参照してください。
- ネットワーク マップ：[ネットワーク マップの表示](#) を参照してください。

**ステップ2** カスタム ワークフローにアクセスするには、[分析 (Analysis)]>[詳細 (Advanced)]>[カスタムワークフロー (Custom Workflows)] を選択します。

**ステップ3** カスタム テーブルに基づいたワークフローにアクセスするには、[分析 (Analysis)]>[詳細 (Advanced)]>[カスタムテーブル (Custom Tables)] を選択します。

**ステップ4** 以下のいずれかのアクションを実行します。これらは、ネットワーク検出ワークフローでアクセスするすべてのページに共通です。

- 列の制約：表示される列を制約するには、非表示にする列の見出しにある[閉じる (Close) ] (X) をクリックします。表示されるポップアップ ウィンドウで、[適用 (Apply) ] をクリックします。

### ヒント

他のカラムを表示または非表示にするには、[適用 (Apply) ] をクリックする前に、該当するチェック ボックスをオンまたはオフにします。無効にした列をビューに戻すには、展開の矢印をクリックして検索の制約を開き、[無効な列 (Disabled Columns) ] の下の列名をクリックします。

- 削除：現在の制約されたビューにある一部またはすべての項目を削除するには、削除する項目の横にあるチェックボックスをオンにし、[削除 (Delete) ]または[すべて削除 (Delete All) ]をクリックします。これらのアイテムが再検出されても、システムのディスカバリ機能が再開されるまで、これらのアイテムは削除されたままになります。

#### 注意

[分析 (Analysis) ]>[ユーザー (Users) ]>[ユーザー (Users) ] [分析 (Analysis) ]>[ユーザー (Users) ] 見出し>[アクティブセッション (Active Sessions) ]ページで非 VPN セッションを削除する前に、そのセッションが実際に閉じられていることを確認します。アクティブなセッションを削除すると、該当するポリシーはデバイス上のセッションを検出できなくなります。そのため、モニターしたり、ブロックしたりするようポリシーが設定されていたとしても、セッションはそれらのアクションを実行しません。

#### (注)

[分析 (Analysis) ]>[ユーザー (Users) ]>[アクティブセッション (Active Sessions) ]ページの VPN セッションに関する詳細については、「リモートアクセス VPN の現在のユーザーの表示」を参照してください。

#### (注)

サードパーティの場合とは異なり、シスコの脆弱性は削除できません。ただし、確認済みとしてマークすることはできます。

- ドリルダウン：ワークフローの次のページにドリルダウンするには、[ドリルダウンページの使用](#)を参照してください。
- 現在のページを移動する：現在のワークフロー ページ内を移動するには、[ワークフロー ページのナビゲーション ツール](#)を参照してください。
- ワークフロー内で移動する：現在の制約を維持しながら現在のワークフローのページ間で移動するには、ワークフロー ページの左上にある該当するページリンクをクリックします。
- 他のワークフローに移動する：関連するイベントを調べるために、他のイベントビューに移動するには、[ワークフロー間のナビゲーション](#)を参照してください。
- データのソート：ワークフローでデータをソートするには、カラムのタイトルをクリックします。ソート順を逆にするには、カラムのタイトルをもう一度クリックします。
- ホストプロファイルの表示：IP アドレスのホストプロファイルを表示するには、[ホストプロファイル (Host Profile) ]をクリックします。アクティブな侵害の兆候 (IOC) タグのあるホストの場合は、IP アドレスの横に表示される [侵害を受けたホスト (Compromised Host) ] をクリックします。
- ユーザー プロファイル：ユーザー ID 情報を表示するには、[ユーザーID (User Identity) ] の隣に表示される [ユーザー (User) ] アイコン、または IOC に関連付けられているユーザーの場合は [レッドユーザー (Red User) ] をクリックします。 の表示

## ■ 検出イベントおよびホスト入力イベント

### 関連トピック

[ワークフローの使用](#)

[Firewall Management Center データベースからのデータの消去](#)

## 検出イベントおよびホスト入力イベント

システムは検出イベントを生成します。このイベントは、監視対象ネットワークセグメントにおける変更の詳細をやり取りします。新しく検出されたネットワーク機能に対しては、新しいイベントが生成され、以前に認識されたネットワークアセットにおける何らかの変更に対しては、変更のイベントが生成されます。

最初のネットワーク検出のフェーズ中に、システムは各ホスト、および各ホスト上での稼動が検出された TCP または UDP サーバについて、新しいイベントを生成します。必要に応じて、エクスポートされた NetFlow レコードを使用してこれらの新しいホストおよびサーバのイベントを生成するよう、システムを設定することができます。

またシステムは、検出された各ホスト上で稼動しているネットワーク、トランスポート、およびアプリケーションプロトコルのそれぞれに対して新しいイベントを生成します。設定されている検出ルールでアプリケーションプロトコルの検出を無効にして、NetFlow エクスポートをモニターできますが、管理対象デバイスをモニターするよう設定された検出ルールではできません。NetFlow以外の検出ルールでホストまたはユーザの検出を有効にすると、アプリケーションが自動的に検出されます。

最初のネットワークマッピングが完了すると、続けてシステムは変更イベントを生成し、ネットワークの変更を記録します。変更イベントは、以前に検出されたアセットの設定が変更されるたびに生成されます。

検出イベントが生成されると、データベースに記録されます。Firewall Management Center の Web インターフェイスを使用して、検出イベントを表示、検索、および削除できます。また、相關ルールで検出イベントを使用することもできます。ユーザが指定する他の基準だけでなく、生成される検出イベントのタイプに基づいて、相關ルールを作成することができます。相關ルールは相關ポリシーで使用され、ネットワークトラフィックが基準を満たしたときに、修復、syslog、SNMP、および電子メールアラートの応答を起動します。

ホスト入力機能を使用して、ネットワークマップにデータを追加することができます。オペレーティングシステムの情報を追加、修正、または削除することができますが、この場合、システムは対象のホストに対する情報の更新を停止します。アプリケーションプロトコル、クライアント、サーバ、およびホストの属性を手動で追加、変更、または削除することも、脆弱性の情報を変更することもできます。この処理を行う場合、システムはホスト入力機能を生成します。

## ディスカバリ イベントタイプ

ネットワーク検出ポリシーにシステムが記録するディスカバリイベントのタイプを設定できます。ディスカバリイベントのテーブルを表示すると、[イベント (Event)] カラムにイベントタイプが表示されます。次に、ディスカバリイベントタイプについて説明します。

## ホストの追加 MAC の検出

このイベントは、以前に検出したホストに対してシステムが新しい MAC アドレスを検出したときに生成されます。

このイベントは多くの場合、ルータを通じてトラフィックを渡すホストをシステムが検出したときに生成されます。それぞれのホストには 1 つの IP アドレスがありますが、これらの IP アドレスはすべて、ルータに関連付けられている MAC アドレスを持っているように見えます。システムは IP アドレスに関連付けられている実際の MAC アドレスを検出すると、ホストプロファイル内でその MAC アドレスを太字で表示し、イベントビューのイベント説明に「ARP/DHCP detected」のメッセージを表示します。

## クライアントタイムアウト

このイベントは、非アクティブであるという理由で、システムがデータベースからクライアントをドロップしたときに生成されます。

## クライアント更新

このイベントは、HTTP トラフィック内でシステムがペイロード（つまり音声やビデオ、Web メールなどの特別なタイプのコンテンツ）を検出したときに生成されます。

## DHCP : IP アドレスの変更

このイベントは、DHCP アドレスの割り当てによってホスト IP アドレスが変わったことがシステムで検出された場合に生成されます。

## DHCP : IP アドレスの再割り当て

このイベントは、ホストが IP アドレスを再利用するとき、つまり他の物理ホストが以前に使用した IP アドレスを、別のホストが DHCP の IP アドレス割り当てによって取得した場合に生成されます。

## Hops Change

このイベントは、ホストと、そのホストを検出するデバイス間でシステムがネットワーク ホップ数の変更を検出した場合に生成されます。これは次のような場合に発生します。

- デバイスがさまざまなルータを介してホストのトラフィックを監視しており、ホストの場所についてより適切な決定ができる場合。
- デバイスがホストから ARP 送信を検出し、ホストがローカルセグメント上にあることを示している場合。

## ホスト削除 : ホスト制限に到達

このイベントは、Firewall Management Center 上でホストの制限を超えて、のネットワーク マップから監視対象のホストが削除されたときに生成されます。

## ■ ディスカバリ イベントタイプ

### ホスト ドロップ : ホスト制限に到達

このイベントは、Firewall Management Center上でホストの制限に達して新しいホストがドロップされたときに生成されます。このイベントとの相違点として、前述のイベントでは、ホストの制限に達したときに古いホストがネットワーク マップから削除されます。

ホストの制限に達したときに新しいホストをドロップするには、[ポリシー (Policies)]>[ネットワーク検出 (Network Discovery)]>[詳細 (Advanced)]を選択し、[ホストの制限に達した場合 (When Host Limit Reached)]を[ホストをドロップ (Drop hosts)]に設定します。

### ホスト IOC 設定

このイベントは、ホストに対してIOC（侵害の痕跡）が設定され、アラートが生成されたときに生成されます。

### ホスト タイムアウト

このイベントは、ネットワーク検出ポリシーで定義された間隔内でホストがトラフィックを生成しなかったために、ネットワークマップからホストがドロップされたときに生成されます。個々のホストのIP アドレスと MAC アドレスはそれぞれタイムアウトになることに注意してください。関連付けられているアドレスがすべてタイムアウトになるまで、ホストはネットワーク マップから消えません。

ネットワーク検出ポリシーで監視するネットワークを変更する場合は、ネットワークマップから古いホストを手動で削除して、それらのホストがホストの制限に不利に作用しないようにします。

### ネットワーク デバイスへのホスト タイプの変更

このイベントは、システムが、検出されたホストが実際はネットワークデバイスであったことを認識したときに生成されます。

### アイデンティティ競合

このイベントは、システムが、新しいサーバーまたはオペレーティングシステムに対する現行のアクティブなアイデンティティと競合する、そのサーバーまたはオペレーティングシステムのアイデンティティを検出したときに生成されます。

より新しいアクティブなアイデンティティデータを取得するためにホストを再スキャンして、アイデンティティの競合を解決する場合は、Identity Conflict イベントを使用して Nmap の修復をトリガーできます。

### アイデンティティ タイムアウト

このイベントは、アクティブなソースからのサーバーまたはオペレーティング システムの ID データがタイムアウトしたときに生成されます。

より新しいアクティブなアイデンティティデータを取得するために、ホストを再スキャンしてアイデンティティデータをリフレッシュする場合は、Identity Conflict イベントを使用して Nmap の修復をトリガーできます。

## MAC 情報の変更

このイベントは、特定の MAC アドレスまたは TTL 値に関連付けられている情報で、システムが変更を検出したときに生成されます。

このイベントは多くの場合、ルータを通じてトライフィックを渡すホストをシステムが検出したときに発生します。それぞれのホストには 1 つの IP アドレスがありますが、これらの IP アドレスはすべて、ルータに関連付けられている MAC アドレスを持っているように見えます。システムは IP アドレスに関連付けられている実際の MAC アドレスを検出すると、ホストプロファイル内でその MAC アドレスを太字で表示し、イベントビューのイベント説明に

「ARP/DHCP detected」のメッセージを表示します。TTL は変わる可能性がありますが、これはトライフィックが複数のルータを通じて渡される可能性があるためです。また、システムがホストの実際の MAC アドレスを検出した場合も TTL が変わることもあります。

## NETBIOS 名の変更

このイベントは、システムがホストの NetBIOS 名に対する変更を検出したときに生成されます。このイベントは、NetBIOS プロトコルを使用するホストに対してのみ生成されます。

## 新しいクライアント

このイベントは、システムが新しいクライアントを検出したときに生成されます。



(注) 分析用にクライアントデータを収集および格納するには、ネットワーク検出ポリシーのディスカバリー ルールでアプリケーションの検出が有効になっていることを確認します。

## 新しいホスト

このイベントは、システムがネットワーク上で稼動している新しいホストを検出したときに生成されます。

このイベントは、デバイスが新しいホストを含む NetFlow データを処理するときも生成できます。この状況でイベントを生成するには、NetFlow データを管理するネットワーク検出ルールでホストを検出するように設定します。

## 新しいネットワーク プロトコル

このイベントは、ホストが新しいネットワーク プロトコル (IP、ARP など) と通信していることをシステムが検出したときに生成されます。

## 新しい OS

このイベントは、システムがホストの新しいオペレーティングシステムを検出した、またはホストのオペレーティング システムで変更を検出したときに生成されます。

## ■ ディスカバリイベントタイプ

### 新しいTCPポート

このイベントは、ホスト上でアクティブな新しいTCPサーバーポート（SMTPまたはWebサービスで使用されているポートなど）をシステムが検出したときに生成されます。このイベントは、アプリケーションプロトコル、またはアプリケーションプロトコルに関連付けられているサーバーの識別には使用されません。情報は、TCP Server Information Updateイベントで伝送されます。

このイベントは、デバイスがネットワークマップにすでに存在しないモニター対象ネットワーク上のサーバーを含むNetFlowデータを処理するときも生成できます。この状況でイベントを生成するには、NetFlowデータを管理するネットワーク検出ルールでアプリケーションを検出するように設定します。

### 新しいトランスポートプロトコル

このイベントは、ホストが新しいトランスポートプロトコル（TCP、UDPなど）と通信していることをシステムが検出したときに生成されます。

### 新しいUDPポート

このイベントは、システムが、ホスト上で稼動している新しいUDPサーバーポートを検出したときに生成されます。

このイベントは、デバイスがネットワークマップにすでに存在しないモニター対象ネットワーク上のサーバーを含むNetFlowデータを処理するときも生成できます。この状況でイベントを生成するには、NetFlowデータを管理するネットワーク検出ルールでアプリケーションを検出するように設定します。

### TCPポートクローズ

このイベントは、システムが、ホスト上でTCPポートがクローズしたことを検出したときに生成されます。

### TCPポートタイムアウト

このイベントは、システムのネットワーク検出ポリシーに定義された間隔内で、システムがTCPポートからアクティビティを検出しなかつたときに生成されます。

### TCPサーバー情報の更新

このイベントは、ホスト上で稼動しており、すでに検出されているTCPサーバーでシステムが変更を検出したときに生成されます。

このイベントは、TCPサーバーが更新されたときに生成される場合があります。

### UDPポートクローズ

このイベントは、システムが、ホスト上でUDPポートがクローズしたことを検出したときに生成されます。

### UDP ポート タイムアウト

このイベントは、ネットワーク検出ポリシーに定義された間隔内で、システムが UDP ポートからアクティビティを検出しなかったときに生成されます。

### UDP サーバー情報の更新

このイベントは、ホスト上で稼動しており、すでに検出されている UDP サーバーでシステムが変更を検出したときに生成されます。

このイベントは、UDP サーバーが更新されたときに生成される場合があります。

### VLAN タグ情報の更新

このイベントは、システムが、VLAN タグ内でホストに起因する変更を検出したときに生成されます。

#### 関連トピック

[ホスト入力イベント タイプ](#) (15 ページ)

## ホスト入力イベント タイプ

ディスカバリイベントのテーブルを表示すると、[イベント (Event)] カラムにイベント タイプが表示されます。

ユーザーが（手動でホストを追加するなどの）特定のアクションを実行したときに生成されるホスト入力イベントとは異なり、ディスカバリイベントは、システムが、監視対象ネットワークで変更を検出したとき（以前は検出されなかったホストでトラフィックを検出した場合など）に生成されます。

ネットワーク検出ポリシーを変更して、システムが記録するホスト入力イベントのタイプを設定できます。

さまざまなタイプのホスト入力イベントが提示する情報を理解すると、どのイベントを記録およびアラートの対象にするか、相関ポリシーでこれらのアラートをどのように使用するかを効率よく判断できるようになります。また、イベントタイプの名前がわからると、より効率のよいイベント検索を作成するうえで役に立ちます。次に、ホスト入力イベントのさまざまなタイプについて説明します。

#### クライアントの追加 (Add Client)

このイベントは、ユーザーがクライアントを追加したときに生成されます。

#### ホストの追加 (Add Host)

このイベントは、ユーザーがホストを追加したときに生成されます。

#### プロトコルの追加 (Add Protocol)

このイベントは、ユーザーがプロトコルを追加したときに生成されます。

## ■ ホスト入力イベントタイプ

### スキャン結果の追加 (Add Scan Result)

このイベントは、システムがNmapスキャンの結果をホストに追加したときに生成されます。

### ポートの追加 (Add Port)

このイベントは、ユーザーがサーバーポートを追加したときに生成されます。

### クライアントの削除 (Delete Client)

このイベントは、ユーザーがシステムからクライアントを削除したときに生成されます。

### ホスト/ネットワークの削除 (Delete Host/Network)

このイベントは、ユーザーがシステムからIPアドレスまたはサブネットを削除したときに生成されます。

### プロトコルの削除 (Delete Protocol)

このイベントは、ユーザーがシステムからプロトコルを削除したときに生成されます。

### ポートの削除 (Delete Port)

このイベントは、ユーザーがシステムからサーバーポートまたはサーバーポートのグループを削除したときに生成されます。

### Host Attribute Add

このイベントは、ユーザが新しいホスト属性を作成したときに生成されます。

### Host Attribute Delete

このイベントは、ユーザーが、ユーザー定義のホスト属性を削除したときに生成されます。

### ホスト属性値の削除 (Host Attribute Delete Value)

このイベントは、ユーザーが、ホスト属性に割り当てられている値を削除したときに生成されます。

### ホスト属性値の設定 (Host Attribute Set Value)

このイベントは、ユーザーがホストに対してホスト属性値を設定したときに生成されます。

### Host Attribute Update

このイベントは、ユーザーが、ユーザー定義のホスト属性の定義を変更したときに生成されます。

### ホスト重要度の設定（Set Host Criticality）

このイベントは、ユーザーがホストに対してホストの重要度の値を設定した、または変更したときに生成されます。

### オペレーティング システム定義の設定（Set Operating System Definition）

このイベントは、ユーザーがホストに対してオペレーティング システムを設定したときに生成されます。

### サーバー定義の設定（Set Server Definition）

このイベントは、ユーザーがサーバーに対してベンダーおよびバージョンの定義を設定したときに生成されます。

### Set Vulnerability Impact Qualification

このイベントは、脆弱性の影響の認定が設定されたときに生成されます。

脆弱性が、影響の認定に対する使用でグローバル レベルで無効になったとき、または脆弱性がグローバル レベルで有効になったときに、このイベントが生成されます。

### 脆弱性を無効に設定（Vulnerability Set Invalid）

このイベントは、ユーザーが1つ以上の脆弱性を無効にした（または確認した）ときに生成されます。

### 脆弱性を有効に設定（Vulnerability Set Valid）

このイベントは、ユーザーが、以前に無効であるとマークされた脆弱性を有効にしたときに生成されます。

#### 関連トピック

[ディスカバリ イベント タイプ](#) (10 ページ)

## ディスカバリ イベントとホスト入力イベントの表示

ディスカバリ イベントワークフローでは、ディスカバリ イベントとホスト入力イベント両方からのデータを表示できます。ユーザーは検索する情報に応じてイベントビューを操作することができます。

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。

ユーザーがイベントにアクセスするときに表示されるページは、使用するワークフローによって異なります。ユーザーは事前定義のワークフローを使用できますが、これにはディスカバリ イベントのテーブル ビューと、ホスト ビューの最終ページが含まれています。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。

## ■ ディスカバリ イベントのフィールド

### 手順

**ステップ1** [分析 (Analysis)] > [ホスト (Hosts)] 見出し > [検出イベント (Discovery Events)] を選択します。

**ステップ2** 次の選択肢があります。

- ・[時間枠の変更](#)の説明に従って、時間範囲を調整します。

(注)

イベントビューを時間によって制約している場合は、（グローバルかイベントに特有かに関係なく）アプライアンスに設定されている時間枠の範囲外に生成されたイベントがイベントビューに表示されることがあります。アプライアンスに対してスライドする時間枠を設定した場合でも、この状況が発生することがあります。

- ・[(ワークフローの切り替え) ((switch workflow))] をクリックしてカスタムワークフローを含む別のワークフローを使用します。
- ・基本的なワークフロー操作を実行します ([ディスカバリおよびアイデンティティワークフローの使用 \(7ページ\)](#) を参照)。
- ・テーブルのカラムの内容について詳しく調べます ([ディスカバリ イベントのフィールド \(18ページ\)](#) を参照)。

### 関連トピック

[ディスカバリおよびアイデンティティ ワークフローの使用 \(7ページ\)](#)

## ディスカバリ イベントのフィールド

以下に、ディスカバリ イベント テーブルで表示および検索できるフィールドについて説明します。

### 時刻 (Time)

システムがイベントを生成した時間。

### イベント

ディスカバリ イベント タイプまたはホスト入力イベント タイプ。

### [IPアドレス (IP Address)]

イベントに関連するホストに関連付けられている IP アドレス。

### ユーザー (User)

イベントが生成される前に、イベントに関係するホストに最後にログインしたユーザ。権限のあるユーザの後に、権限のないユーザのみがログインした場合、権限のあるユーザが次にログインするまで、権限のあるユーザが現行のユーザとして保持されます。

### [MAC アドレス (MAC Address) ]

ディスカバリイベントをトリガーとして使用したネットワーク トライフィックが使用する NIC の MAC アドレス。この MAC アドレスは、イベントに関連するホストの実際の MAC アドレスであるか、またはトライフィックが通過したネットワークデバイスの MAC アドレスになります。

### [MAC ベンダー (MAC Vendor) ]

ディスカバリイベントをトリガーとして使用したネットワーク トライフィックが使用する NIC の MAC ハードウェアベンダー。

### [ポート (Port) ]

イベントをトリガーとして使用したトライフィックが使用するポート（該当する場合）。

#### 説明

テキストによるイベントの説明。

#### ドメイン

ホストを検出したデバイスのドメイン。このフィールドは、マルチテナントのためにFirewall Management Center を設定したことがある場合に表示されます。

#### デバイス

イベントを生成した管理対象デバイスの名前。NetFlow データに基づいた新しいホストおよび新しいサーバーのイベントの場合、これはそのデータを処理した管理対象デバイスになります。

#### 関連トピック

[イベントの検索](#)

## ホストデータ

システムがホストを検出し、ホストプロファイルを作成するためにホストに関する情報を収集したときに、イベントが生成されます。Firewall Management Center Web インターフェイスを使用して、ホストを表示、検索、および削除できます。

ホストの表示中に、選択したホストに基づいてトライフィックのプロファイル、およびコンプライアンスのallowリストを作成できます。また、（ビジネスの重要度を設定する）ホストの重要度の値などのホスト属性をホストグループに割り当てることもできます。その後で、相関ル

## ホストデータの表示

ルおよびポリシーの中でこれらの重要度の値、allowリスト、およびトラフィックプロファイルを使用できます。

システムは、エクスポートされたNetFlowレコードからネットワークマップにホストを追加できますが、これらのホストに使用できる情報は限られます ([NetFlowデータと管理対象デバイスデータの違い](#)を参照)。

## ホストデータの表示

Firewall Management Centerを使用して、システムが検出したホストのテーブルを表示することができます。ここでユーザーは、検索する情報に応じてビューを操作できます。

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。

ユーザーがホストにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローは両方とも、ホストビューで終了しますが、これにはユーザーの制約を満たすすべてのホストのホストプロファイルが含まれています。また、特定のニーズを満たす情報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。

### 手順

---

**ステップ1** 次のように、ホストデータにアクセスします。

- 事前定義されたワークフローを使用する場合、[分析 (Analysis)] > [ホスト (Hosts)] 見出し > [ホスト (Hosts)] を選択します。
- ホストのテーブルビューが含まれないカスタムワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow))] をクリックして [ホスト (Hosts)] を選択します。

**ステップ2** 次の選択肢があります。

- [(ワークフローの切り替え) ((switch workflow))] をクリックしてカスタムワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します ([ディスカバリおよびアイデンティティワークフローの使用 \(7ページ\)](#) を参照)。
- テーブルのカラムの内容について詳しく調べます ([ホストデータフィールド \(21ページ\)](#) を参照)。
- 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)。
- ホスト属性を特定のホストに割り当てます ([選択したホストのホスト属性の設定 \(29ページ\)](#) を参照)。
- 特定のホストのトラフィックプロファイルを作成します ([選択したホストのトラフィックプロファイルの作成 \(25ページ\)](#) を参照)。

- 特定のホストに基づいて、コンプライアンスの allow リストを作成します（[選択したホストに基づいたコンプライアンスの許可リストの作成（26 ページ）](#) を参照）。

## ホストデータフィールド

システムはホストを検出したときに、そのホストに関するデータを収集します。そのデータには、ホストの IP アドレス、ホストが実行しているオペレーティングシステムなどが含むことができます。ユーザーは、ホストのテーブルビューでこれらの情報の一部を表示することができます。

ホストテーブルで表示および検索できるフィールドの説明が続きます。

### 前回の検出 (Last Seen)

システムによっていずれかのホストの IP アドレスが最後に検出された日付と時間。[前回の検出 (Last Seen)] の値は、ホストの IP アドレスに対してシステムが新しいホストイベントを生成したときだけでなく、少なくともユーザーがネットワーク検出ポリシーに設定した更新間隔の頻度で更新されます。

ホスト入力機能を使用して、オペレーティングシステムのデータを更新しているホストでは、Last Seen の値は、そのデータが最初に追加された日付と時間を表します。

### IP Address

ホストに関連付けられている IP アドレス。

### MAC Address

ホストが検出した NIC の MAC アドレス。

[MAC Address] フィールドは、[Hosts] ワークフローの [Table View of Hosts] に表示されます。以下のものに対して [MAC Address] フィールドを追加できます。

- Hosts テーブルのフィールドが含まれているカスタム テーブル
- [ホスト (Hosts) ] テーブルに基づいたカスタム ワークフローのドリルダウンページ

### MAC Vendor

ホストが検出した NIC の MAC ハードウェアベンダー。

[MAC Vendor] フィールドは、[Hosts] ワークフローの [Table View of Hosts] に表示されます。以下のものに対して [MAC Vendor] フィールドを追加できます。

- Hosts テーブルのフィールドが含まれているカスタム テーブル
- [ホスト (Hosts) ] テーブルに基づいたカスタム ワークフローのドリルダウンページ

このフィールドを検索する場合は、`virtual_mac_vendor` を入力して、仮想ホストに関するイベントを照合します。

## ホストデータ フィールド

### 現在のユーザー（Current User）

ホストに現在ログインしているユーザーの ID（ユーザー名）。

権限のないユーザーがホストにログインすると、そのログインはユーザーおよびホストの履歴に記録されることに注意してください。権限のあるユーザーがホストに関連付けられていない場合、権限のないユーザーがそのホストの現行ユーザーとなることが可能ですが。ただし、権限のあるユーザーがホストにログインした後は、権限のある別のユーザーがログインした場合のみ、現行ユーザーが変わります。また、権限のないユーザーがホストの現行ユーザーである場合、そのユーザーを使用してユーザー制御を行うことはできません。

### Host Criticality

ホストに割り当てられている、ユーザー指定の重要度の値。

### NetBIOS 名（NetBIOS Name）

ホストの NetBIOS 名。NetBIOS プロトコルを実行しているホストにのみ、NetBIOS 名があります。

### VLAN ID

ホストが使用する VLAN ID。

### ホップ（Hops）

ホストを検出したデバイスからホストへのネットワークのホップ数。

### ホストタイプ（Host Type）

ホストのタイプ。ホスト、モバイルデバイス、jailbroken モバイルデバイス、ルータ、ブリッジ、NAT デバイス、ロードバランサのいずれかにできます。

ネットワーク デバイスを区別するためにシステムでは次の方法を使用します。

- Cisco Discovery Protocol (CDP) メッセージの分析。ネットワークのデバイスおよびそれらのタイプ (Cisco デバイスのみ) を特定できます。
- スパニングツリープロトコル (STP) の検出。デバイスをスイッチまたはブリッジとして識別します。
- 同じ MAC アドレスを使用している複数のホストの検出。MAC アドレスを、ルータに属しているものとして識別します。
- クライアント側からの TTL 値の変更、または通常のブート時間よりも頻繁に変更されている TTL 値の検出。この検出では、NAT デバイスとロードバランサを識別します。

デバイスがネットワーク デバイスとして識別されない場合は、ホストとして分類されます。

このフィールドを検索するときは、!host と入力してすべてのネットワーク デバイスを検索します。

### ハードウェア (Hardware)

モバイルデバイスのハードウェアプラットフォーム。

### OS

次のいずれかです。

- ホスト上で検出されたオペレーティングシステム（名前、ベンダー、およびバージョン）、またはNmapかホスト入力機能を使用して更新されたオペレーティングシステム。
- オペレーティングシステムが既知のフィンガープリントに一致しない場合はunknown
- オペレーティングシステムを識別するための十分な情報がシステムで収集されていない場合はpending

システムが複数のアイデンティティを検出した場合は、これらのアイデンティティはカンマ区切りリストで表示されます。

このフィールドは、ダッシュボード上で[カスタム分析 (Custom Analysis) ] ウィジェットからホストイベントビューを起動したときに表示されます。また、これは[ホスト (Hosts) ] テーブルに基づいたカスタムテーブルのフィールドオプションです。

このフィールドを検索するときは、n/aと入力して、オペレーティングシステムがまだ識別されていないホストを含めます。

### OS競合 (OS Conflict)

このフィールドは検索専用です。

### OSベンダー (OS Vendor)

次のいずれかです。

- ホストで検出されたオペレーティングシステムのベンダー、またはNmapかホスト入力機能を使用して更新されたオペレーティングシステムのベンダー。
- オペレーティングシステムが既知のフィンガープリントに一致しない場合はunknown
- オペレーティングシステムを識別するための十分な情報がシステムで収集されていない場合はpending

システムが複数のベンダーを検出した場合は、これらのベンダーはカンマ区切りリストで表示されます。

このフィールドを検索するときは、n/aと入力して、オペレーティングシステムがまだ識別されていないホストを含めます。

### OS名 (OS Name)

次のいずれかです。

## ■ ホストデータ フィールド

- ホスト上で検出されたオペレーティングシステム、またはNmapかホスト入力機能を使用して更新されたオペレーティングシステム。
- オペレーティングシステムが既知のフィンガープリントに一致しない場合は `unknown`
- オペレーティングシステムを識別するための十分な情報がシステムで収集されていない場合は `pending`

システムが複数の名前を検出した場合は、これらの名前はカンマ区切りリストで表示されます。

このフィールドを検索するときは、`n/a`と入力して、オペレーティングシステムがまだ識別されていないホストを含めます。

### OS バージョン (OS Version)

次のいずれかです。

- ホストで検出されたオペレーティングシステムのバージョン、またはNmapかホスト入力機能を使用して更新されたオペレーティングシステムのバージョン。
- オペレーティングシステムが既知のフィンガープリントに一致しない場合は `unknown`
- オペレーティングシステムを識別するための十分な情報がシステムで収集されていない場合は `pending`

システムが複数のバージョンを検出した場合は、これらのバージョンはカンマ区切りリストで表示されます。

このフィールドを検索するときは、`n/a`と入力して、オペレーティングシステムがまだ識別されていないホストを含めます。

### ソースタイプ (Source Type)

ホストのオペレーティングシステムのアイデンティティを確立するために使用されるソースのタイプは次のとおりです。

- [ユーザー (User) ] : `user_name`
- [アプリケーション (Application) ] : `app_name`
- スキャナ : `scanner_type` (ネットワーク検出の設定を介して追加された Nmap またはスキャナ)
- システムによって検出されたオペレーティングシステムの場合は `Firepower`

システムでは、オペレーティングシステムのアイデンティティを判断するために、複数のソースのデータを統合することができます。

### 信頼性 (Confidence)

次のいずれかです。

- システムで検出されたホストについて、ホスト上で稼動しているオペレーティングシステムのアイデンティティ内にシステムが保持している信頼度（パーセンテージ）。
- 100%（ホスト入力機能やNmapスキャナなどのアクティブなソースによって識別されたオペレーティングシステムの場合）。
- unknown（システムがオペレーティングシステムのアイデンティティを特定できないホスト、およびNetFlowデータに基づいてネットワークマップに追加されたホストの場合）。

このフィールドを検索するときは、n/aと入力して、NetFlowデータに基づいてネットワークマップに追加されたホストを含めます。

#### 注記（Notes）

[注記（Notes）] ホスト属性の、ユーザー定義のコンテンツ。

#### ドメイン（Domain）

ホストに関連付けられているドメイン。このフィールドは、マルチテナンシーのためにFirewall Management Centerを設定したことがある場合に表示されます。

#### Device

トラフィックを検出した管理対象デバイスか、NetFlowまたはホスト入力データを処理したデバイスのいずれか。

このフィールドが空白の場合は、次のいずれかの条件を満たします。

- ホストがデバイスによってネットワークマップに追加されたが、このデバイスは、ホストが存在しているネットワークに対してネットワーク検出ポリシーに定義されているとおりに明示的に監視していない。
- ホストの入力機能を使用してホストが追加されたが、システムによって検出されていない。

#### メンバー数（Count）

各行に表示される情報と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のみです。

#### 関連トピック

[イベントの検索](#)

[オペレーティングシステムのアイデンティティの競合](#)

## 選択したホストのトラフィック プロファイルの作成

トラフィックプロファイルは、指定した期間に収集された接続データに基づいた、ネットワーク上のトラフィックのプロファイルです。トラフィック プロファイルを作成した後、正常なネットワーク トラフィックを表すと想定されるプロファイルに照らして新しいトラフィックを評価することにより、異常なネットワーク トラフィックを検出できます。

## 選択したホストに基づいたコンプライアンスの許可リストの作成

[ホスト (Hosts) ] ページを使用して、指定するホストグループのトラフィックプロファイルを作成できます。トラフィックプロファイルは、指定したホストのいずれかが発信元ホストである、検出された接続に基づいています。ソートおよび検索機能を使用して、プロファイルを作成するホストを分離することができます。

### 始める前に

このタスクを実行するには、管理者ユーザーである必要があります。

### 手順

---

**ステップ1** ホストワークフローのテーブルビューで、トラフィックプロファイルを作成するホストの隣にあるチェックボックスをオンにします。

**ステップ2** ページの下部で [トラフィックプロファイルの作成 (Create Traffic Profile) ] をクリックします。

**ステップ3** 特別なニーズに応じて、トラフィックプロファイルを変更し、保存します。

---

### 関連トピック

[トラフィックプロファイルの概要](#)

## 選択したホストに基づいたコンプライアンスの許可リストの作成

コンプライアンスのallowリストでは、ネットワーク上で許可されるオペレーティングシステム、クライアント、ネットワーク、トранSPORT、またはアプリケーションプロトコルを指定することができます。

[ホスト (Hosts) ] ページを使用して、ユーザーが指定するホストグループのホストプロファイルに基づいて、コンプライアンスのallowリストを作成することができます。ソートおよび検索機能を使用して、allowリストの作成に使用するホストを分離することができます。

### 始める前に

このタスクを実行するには、管理者ユーザーである必要があります。

### 手順

---

**ステップ1** ホストワークフローのテーブルビューで、allowリストを作成するホストの隣にあるチェックボックスをオンにします。

**ステップ2** ページの下部で [許可リスト (Allow List) の作成 (Create White List) ] をクリックします。

**ステップ3** 特別なニーズに応じて、allowリストを変更し、保存します。

## 関連トピック

[コンプライアンス許可リストの概要](#)

# ホスト属性データ

Firepower システムは、検出したホストに関する情報を収集し、その情報を使用してホストプロファイルを作成します。ただし、ネットワーク上のホストについて、アナリストに提供する追加情報が存在する場合があります。ユーザは、ホストプロファイルにメモを追加する、ホストのビジネス重要度を設定する、選択する他の情報を提供する、といったことが可能です。それぞれの情報は、ホスト属性と呼ばれます。

ホストプロファイルの認定でホスト属性を使用することができます。これにより、トラフィックプロファイルの作成中に収集するデータを制約し、相關ルールをトリガーする条件を制限することができます。相關ルールに応じて属性値を設定することもできます。

## 関連トピック

[ホスト属性の表示 \(27 ページ\)](#)

[セット属性修復の設定](#)

## ホスト属性の表示

Firewall Management Center を使用して、システムで検出されたホストのテーブル、およびそのホスト属性を表示することができます。ここでユーザーは、検索する情報に応じてビューを操作できます。

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。

ユーザーがホスト属性にアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフロー（検出されたすべてのホスト、およびそのホストの属性が記載されているホスト属性のテーブルビューが含まれており、ホストビューページで終了するワークフロー）を使用することができます。このワークフローには、制約を満たすすべてのホストについて 1 つのホストプロファイルが含まれています。

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。

## 手順

**ステップ1** 次のように、ホスト属性データにアクセスします。

- 事前定義されたワークフローを使用する場合、[分析 (Analysis)] > [ホスト (Hosts)] 見出し > [ホスト属性 (Host Attributes)] を選択します。
- ホスト属性のテーブルビューが含まれないカスタムワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow))] をクリックして [属性 (Attributes)] を選択します。

## ホスト属性データ フィールド

**ステップ2** 次の選択肢があります。

- ・[(ワークフローの切り替え) ((switch workflow)) ]をクリックしてカスタムワークフローを含む別のワークフローを使用します。
  - ・基本的なワークフロー操作を実行します ([ディスカバリおよびアイデンティティワークフローの使用 \(7ページ\)](#) を参照)。
  - ・テーブルのカラムの内容について詳しく調べます ([ホスト属性データ フィールド \(28ページ\)](#) を参照)。
  - ・ホスト属性を特定のホストに割り当てます ([選択したホストのホスト属性の設定 \(29ページ\)](#) を参照)。
- 

## ホスト属性データ フィールド

ホスト属性テーブルには、MAC アドレスでのみ識別されるホストは表示されないことに注意してください。

ホスト属性テーブルで表示および検索できるフィールドの説明が続きます。

### [IPアドレス (IP Address) ]

ホストに関連付けられている IP アドレス。

### 現在のユーザー (Current User)

ホストに現在ログインしているユーザーの ID (ユーザー名)。

権限のないユーザーがホストにログインすると、そのログインはユーザーおよびホストの履歴に記録されることに注意してください。権限のあるユーザーがホストに関連付けられていない場合、権限のないユーザーがそのホストの現行ユーザーとなることが可能ですが。ただし、権限のあるユーザーがホストにログインした後は、権限のある別のユーザーがログインした場合のみ、現行ユーザーが変わります。また、権限のないユーザーがホストの現行ユーザーである場合、そのユーザーを使用してユーザー制御を行うことはできません。

### Host Criticality

ユーザが割り当てた、企業にとってのホストの重要度。ホストの重要度を相関ルールおよびポリシーで使用して、イベントに関するホストの重要度に対して、ポリシー違反および違反の応答を作成することができます。ホストの重要度に[低 (Low) ]、[中 (Medium) ]、[高 (High) ]、または[なし (None) ]を割り当てることができます。

### 注記 (Notes)

他のアナリストに提示する、ホストに関する情報。

コンプライアンス allow リストの属性を含む、ユーザー定義のホスト属性 (**Any user-defined host attribute, including those for compliance allow lists**)

ユーザー定義のホスト属性の値。ホスト属性テーブルには、ユーザ定義のそれぞれのホスト属性のフィールドが含まれています。

#### ドメイン (Domain)

ホストに関連付けられているドメイン。このフィールドは、マルチテナントのためにFirewall Management Center を設定したことがある場合に表示されます。

#### メンバー数 (Count)

各行に表示される情報と一致するイベントの数。[カウント (Count) ] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

#### 関連トピック

[イベントの検索](#)

## 選択したホストのホスト属性の設定

ホストワークフローから、事前定義済のホスト属性とユーザー定義のホスト属性を設定できます。

### 手順

---

**ステップ1** ホストワークフローで、ホスト属性を追加するホストの横にあるチェックボックスをオンにします。

#### ヒント

ソート機能と検索機能を使用して、特別な属性を割り当てるホストを分離することができます。

**ステップ2** ページの下部にある [属性の設定 (Set Attributes) ] をクリックします。

**ステップ3** 必要に応じて、選択したホストに対してホストの重要度を設定します。[なし (None) ]、[低 (Low) ]、[中 (Medium) ]、または[高 (High) ]を選択できます。

**ステップ4** 必要に応じて、テキストボックスで、選択したホストのホストプロファイルにメモを追加します。

**ステップ5** 必要に応じて、自分で設定したユーザ定義のホストの属性を設定します。

**ステップ6** [保存 (Save) ] をクリックします。

---

## 侵害の兆候データ

システムは、モニタリング対象のネットワーク上でホストが悪意のある手段によって侵害されている可能性があるかどうかを判断するために、ホストに関連付けられているさまざまなタイプのデータ（侵入イベント、セキュリティインテリジェンス、接続イベント、ファイルまたはマルウェアイベント）との関連性を示します。イベントデータの特定の組み合わせと頻度は、影響を受けたホストの侵害の痕跡（IOC）タグをトリガーとして使用します。このようなホストのIPアドレスは侵害を受けているホストの赤いアイコンでイベントビューに表示されます。

ホストが侵害されている可能性があると識別された場合、その侵害に関連付けられているユーザーにもタグが付けられます。そのようなユーザーは、赤色のユーザーアイコンでイベントビューに表示されます。

マルウェアが含まれているファイルが300秒以内にIOCというタグが付けられて再度表示される場合は、別のIOCは生成されません。同じファイルが300秒以上経つから表示された場合は、新しいIOCが生成されます。

侵害の兆候としてイベントにタグを付けるように設定するには、Cisco Secure Firewall Management Centerデバイス構成ガイドの「Enabling Indications of Compromise Rules」を参照してください。

### 関連トピック

[サーバーのアイデンティティの編集](#)

## 侵害兆候データの表示と処理

Firewall Management Centerを使用して、侵害の兆候（IOC）を示すテーブルを表示できます。検索する情報に応じてイベントビューを操作します。

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。

表示されるページは、使用するワークフローによって異なります。事前定義のIOCワークフローはプロファイルビューで終了しますが、これには、制約を満たすすべてのホストまたはユーザーのホストプロファイルまたはユーザープロファイルが含まれています。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。

### 始める前に

- システムで侵害の兆候（IOC）を検出してタグを付けるには、ネットワーク検出ポリシーのIOC機能をアクティブにして、少なくとも1つのIOCルールを有効にする必要があります。『Cisco Secure Firewall Management Centerデバイス構成ガイド』の「侵害の兆候ルールの有効化」を参照してください。
- アクティブなアイデンティティポリシーでユーザーが認識される必要があります。

### 手順

---

**ステップ1** Webインターフェイスのどの場所のニーズを満たす情報があるかを特定します。

侵害兆候データを表示または処理するには、次の場所を使用できます。

- ・イベントビューア ([分析 (Analysis)] メニューの下)：接続、セキュリティインテリジェンス、侵入、マルウェアや IOC 検出のイベントビューでそのイベントが IOC をトリガーしたかどうかを表示します。IOC ルールをトリガーする、Secure Endpoint によって生成されたマルウェアイベントは、イベントタイプが AMP IOC であり、侵害を指定するイベントサブタイプと一緒に表示されることに注意してください。
- ・ダッシュボード：ダッシュボードでは、サマリーダッシュボードの [脅威 (Threats)] に、ホスト別とユーザー別の IOC タグがデフォルトで表示されます。カスタム分析ウィジェットは IOC データに基づくプリセットを提供します。
- ・コンテキストエクスプローラ：コンテキストエクスプローラの [侵害の兆候 (Indications of Compromise)] セクションに、IOC カテゴリ別のホストとホスト別の IOC カテゴリのグラフが表示されます。
- ・[ネットワークマップ (Network Map)] ページ：[分析 (Analysis)] > [ホスト (Hosts)] > [ネットワークマップ (Network Map)] にある [侵害の兆候 (Indications of Compromise)] には、侵害されている可能性があるネットワーク上のホストが侵害のタイプと IP アドレス別にグループ分けして示されます。
- ・[ネットワーク ファイル トラジェクトリ (Network File Trajectory)] 詳細ページ：[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)] の下に一覧表示されているファイルの詳細ページでは、ネットワークの侵害の兆候を追跡できます。
- ・[ホストの侵害の兆候 (Host Indications of Compromise)] ページ：[分析 (Analysis)] > [ホスト (Hosts)] メニューの下の [ホストの侵害の兆候 (Host Indications of Compromise)] ページには、モニタ対象ホストの一覧が IOC タグ別にグループ分けされて表示されます。このページのワークフローを使ってデータをドリルダウンできます。
- ・[ユーザの侵害の兆候 (User Indications of Compromise)] ページ：[分析 (Analysis)] > [ユーザ (Users)] メニューの下の [ユーザの侵害の兆候 (User Indications of Compromise)] ページには、IOC の可能性があるイベントに関連付けられているユーザの一覧が IOC タグ別にグループ分けされて表示されます。このページのワークフローを使ってデータをドリルダウンできます。
- ・ホストプロファイルページ：侵害されている可能性があるホストのホストプロファイルには、そのホストに関連付けられているすべての IOC タグが表示され、IOC タグの解決と IOC ルール状態の設定ができます。
- ・ユーザプロファイルページ：IOC の可能性があるイベントに関連付けられているユーザのユーザプロファイルには、そのユーザに関連付けられているすべての IOC タグが表示され、IOC タグの解決と IOC ルール状態の設定ができます (Firewall Management Center の Web インターフェイスでは、ユーザープロファイルは「ユーザーイデンティティ (User Identity)」とラベルが付けられています)。

**ステップ2** 必要に応じて、次のうちのいずれかを実行し、この手順の残りのステップを使用します。

## 侵害兆候データの表示と処理

オプション	説明
ホストの IOC を調べるには、 以下を実行します。	<ul style="list-style-type: none"> <li>事前定義されたワークフローを使用する場合、[分析 (Analysis)] &gt; [ホスト (Hosts)] 見出し &gt; [侵害の兆候 (Indications of Compromise)] を選択します。</li> <li>ホスト IOC のテーブルビューが含まれないカスタムワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow))] をクリックして [ホストの侵害の兆候 (Host Indications of Compromise)] を選択します。</li> </ul>
ユーザーに関連付けられている IOC を調べるには、以下を実行します。	<ul style="list-style-type: none"> <li>事前定義されたワークフローを使用する場合、[分析 (Analysis)] &gt; [ユーザー (Users)] &gt; [侵害の兆候 (Indications of Compromise)] を選択します。</li> <li>ユーザー IOC のテーブルビューが含まれないカスタムワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow))] をクリックして [ユーザーの侵害の兆候 (User Indications of Compromise)] を選択します。</li> </ul>

### ステップ3 次の選択肢があります。

- [(ワークフローの切り替え) ((switch workflow))] をクリックしてカスタムワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します ([ディスカバリおよびアイデンティティワークフローの使用 \(7ページ\)](#) を参照)。
- テーブルのカラムの内容について詳しく調べます ([侵害の兆候データフィールド \(33ページ\)](#) を参照)。
- [ホストの侵害の兆候 (Host Indications of Compromise)] ページ : [IPアドレス (IP Address)] 列にある [侵害を受けたホスト (Compromised Host)] をクリックして、侵害を受けたホストのホストプロファイルを表示します。
- [ユーザーの侵害の兆候 (User Indications of Compromise)] : [ユーザー (User)] 列の [赤色のユーザー (Red User)] をクリックして、侵害に関連付けられているユーザープロファイルを表示します。
- IOCイベントに解決済みとマークして、リストに表示されないようにします。これを実行するには、編集する IOC イベントの横にあるチェックボックスをオンにして、[解決済みとマークを付ける (Mark Resolved)] をクリックします。
- [最初の確認日時 (First Seen)] または [前回の検出 (Last Seen)] 列にある [表示 (View)] (ocular icon) をクリックして、IOC をトリガーしたイベントの詳細を表示します。
- その他のオプションを表示するには、テーブル内の値を右クリックします。

## 侵害の兆候データ フィールド

以下は、ホストまたはユーザの IOC（侵害の兆候）テーブル内のフィールドです。すべての IOC 関連のテーブルにすべてのフィールドが含まれているわけではありません。

### IP アドレス (IP Address) (ホストの IOC データを表示する場合)

IOC をトリガーとして使用したホストに関連付けられている IP アドレス。

### ユーザ (User) (ユーザの IOC データを表示する場合)

IOC をトリガーしたイベントに関連付けられているユーザのユーザ名、レルム、および認証ソース。

### カテゴリ (Category)

Malware Executed や Impact 1 Attack など、示された侵害のタイプの簡単な説明。

### イベントタイプ (Event Type)

特定の IOC に関連付けられている識別子で、トリガーとして使用したイベントを参照します。

### 説明

侵害される可能性のあるホストへの影響の説明 ([このホストはリモート制御下にある可能性があります (This host may be under remote control) ] や [このホスト上でマルウェアが実行されました (Malware has been executed on this host) ] など)。

### 最初の確認日時/最新の確認日時 (First Seen/Last Seen)

IOC をトリガーとして使用したイベントが発生した最初（または最新）の日付と時刻。

### ドメイン (Domain)

IOC をトリガーとして使用したホストのドメイン。このフィールドは、マルチテナントのために Firewall Management Center を設定したことがある場合に表示されます。

### 関連トピック

[イベントの検索](#)

## 単一ホストまたはユーザにおける侵害の兆候のルール状態の編集

ネットワーク検出ポリシーで有効になっている場合、侵害の兆候ルールは監視対象ネットワーク内のすべてのホストと、そのネットワーク上の IOC イベントに関連付けられている権限のあるユーザーに適用されます。個々のホストまたはユーザのルールを無効にして、無用な IOC タグを回避できます（たとえば、DNS サーバに対する IOC タグが表示されないようにできます）。適用可能なネットワーク検出ポリシーでルールを無効にすると、特定のホストまたはユーザに対して有効にすることできません。特定のホストに対してルールを無効にしても、同じイベントに関与するユーザーのタグ付けには影響がなく、その逆もまた同じです。

## 侵害の兆候のタグのソース イベントの表示

### 手順

- ステップ1 ホストまたはユーザ プロファイルの [侵害の兆候 (Indications of Compromise) ] セクションに移動します。
- ステップ2 [ルール状態の編集 (Edit Rule States) ] をクリックします。
- ステップ3 ルールの [有効 (Enabled) ] 列で、スライダをクリックしてこれを有効または無効にします。
- ステップ4 [保存 (Save) ] をクリックします。

## 侵害の兆候のタグのソース イベントの表示

ホストプロファイルやユーザー プロファイルの [侵害の兆候 (Indications of Compromise) ] セクションを使用して、IOC タグをトリガーしたイベントにすばやく移動することができます。これらのイベントを分析すると、侵害される脅威に対処するのに必要なアクション、およびアクションが必要かどうかを判断するための情報が提供されます。

IOC タグのタイムスタンプの隣の[表示 (View) ] (◎) をクリックすると、関連するイベントタイプのイベントのテーブルビューに移動します。ここでは、IOC タグをトリガーしたイベントのみが表示されます。

ユーザー IOC の最初のインスタンスのみが Firewall Management Center に表示されます。後続のインスタンスは DNS サーバによって捕捉されます。

### 手順

- ステップ1 ホストまたはユーザープロファイルで、[侵害の兆候 (Indications of Compromise) ] セクションに移動します。
- ステップ2 調べたい IOC タグの [最初の痕跡 (First Seen) ] または [最後の痕跡 (Last Seen) ] 列にある[表示 (View) ] (◎) をクリックします。

## 侵害の兆候タグの解決

侵害の兆候 (IOC) タグで示された脅威が分析および対処された後、または IOC タグが誤検出を示していると判断した場合、イベントに解決済みのマークを付けることができます。イベントに解決済みのマークを付けると、そのイベントはホストプロファイルおよびユーザープロファイルから削除されます。プロファイル上のアクティブな IOC タグがすべて解決されると、侵害されたホスト またはユーザーが侵害の兆候に関連付けられていることを示す赤色のユーザー アイコン は表示されなくなります。解決した IOC についても、IOC のトリガー元であるイベントは引き続き表示できます。

IOC タグをトリガーしたイベントが繰り返された場合、ホストまたはユーザに対する IOC ルールが無効にされていない限り、このタグが再び設定されます。

## 手順

**ステップ1** ホストまたはユーザプロファイルで、[侵害の兆候 (Indications of Compromise) ] セクションに移動します。

**ステップ2** 次の 2 つの選択肢があります。

- 個別の IOC タグに解決済みとマークするには、解決するタグの右にある [削除 (Delete) ] (Delete) をクリックします。
- プロファイル上のすべての IOC タグに解決済みのマークを付けるには、[すべてに解決済みのマークを付ける (Mark All Resolved) ] をクリックします。

## サーバー データ

システムは、モニター対象ネットワークセグメント上のホストで稼動しているすべてのサーバーに関する情報を収集します。この情報には次のものが含まれます。

- サーバの名前
- サーバが使用するアプリケーションとネットワークプロトコル
- サーバのベンダーとバージョン
- サーバを実行しているホストに関連付けられている IP アドレス
- サーバが通信するポート

システムはサーバを検出すると、関連するホストがまだサーバの最大数に達していない場合は、ディスカバリイベントを生成します。Firewall Management Center の Web インターフェイスを使用して、サーバイベントを表示、検索、削除できます。

また、サーバイベントを相關ルールのベースにすることもできます。たとえばシステムが、いずれかのホスト上で稼働している ircd などのチャットサーバーを検出したときに相關ルールをトリガーできます。

システムは、エクスポートされた NetFlow レコードからネットワークマップにホストを追加できますが、これらのホストに使用できる情報は限られます ([NetFlow データと管理対象デバイスデータの違い](#)を参照)。

## サーバー データの表示

Firewall Management Center を使用して、検出されたサーバーのテーブルを表示できます。ここでユーザーは、検索する情報に応じてイベントビューを操作することができます。

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。

## ■ サーバー データ フィールド

ユーザーがサーバーにアクセスしたときに表示されるページは、使用するワークフローによって異なります。事前定義のすべてのワークフローはホストビューで終了しますが、このホストビューには、制約を満たすすべてのホストに対して1つずつホストプロファイルが含まれています。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。

### 手順

---

**ステップ1** 次のように、サーバー データにアクセスします。

- ・事前定義されたワークフローを使用する場合、[分析 (Analysis)] > [ホスト (Hosts)] 見出し > [サーバー (Servers)] を選択します。
- ・サーバーのテーブル ビューが含まれていないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow))] をクリックして [サーバー (Servers)] を選択します。

**ステップ2** 次の選択肢があります。

- ・[(ワークフローの切り替え) ((switch workflow))] をクリックしてカスタムワークフローを含む別のワークフローを使用します。
  - ・基本的なワークフロー操作を実行します ([ディスカバリおよびアイデンティティワークフローの使用 \(7ページ\)](#) を参照)。
  - ・テーブルのカラムの内容について詳しく調べます ([サーバー データ フィールド \(36ページ\)](#) を参照)。
  - ・編集するサーバーのイベントの横にあるチェック ボックスをオンにし、[サーバー アイデンティティの設定 (Set Server Identity)] をクリックすることによって、サーバーのアイデンティティを編集します。
  - ・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)。
- 

## サーバー データ フィールド

サーバー テーブルで表示および検索できるフィールドの説明は次のとおりです。

### 前回の使用 (Last Used)

ネットワーク上でサーバーが最後に使用された日付と時間、またはホスト入力機能を使用してサーバーが最初に更新された日付と時間。[前回の使用 (Last Used)] の値は、システムがサーバー情報の更新を検出したときだけでなく、少なくともユーザーがネットワーク検出ポリシーに設定した更新間隔の頻度で更新されます。

### [IPアドレス (IP Address)]

サーバーを実行しているホストに関連付けられている IP アドレス。

**Port**

サーバーが稼動しているポート。

**Protocol**

サーバーが使用するネットワークまたはトランスポートプロトコル。

**アプリケーションプロトコル (Application Protocol)**

次のいずれかです。

- サーバーのアプリケーションプロトコルの名前
- pending : システムで、いずれかの理由でサーバーをポジティブまたはネガティブに識別できない場合
- unknown : 既知のサーバーフィンガープリントに基づいてシステムでサーバーを識別できない場合、またはホストの入力を介してサーバーが追加され、アプリケーションプロトコルが含まれていなかった場合

**アプリケーションプロトコルのカテゴリ、タグ、リスク、またはビジネスとの関連性 (Category, Tags, Risk, or Business Relevance for Application Protocols)**

アプリケーションプロトコルに割り当てられているカテゴリ、タグ、リスクレベル、およびビジネス関連性。これらのフィルタを使用して、特定のデータセットを対象にすることができます。

**ベンダー (Vendor)**

次のいずれかです。

- サーバーのベンダー : システム、Nmap、その他のアクティブなソースで識別された、またはホスト入力機能を使用して指定されたサーバーのベンダー
- 空白 : システムが既知のサーバーフィンガープリントに基づいてベンダーを識別できなかった場合、またはNetFlowデータを使用してサーバーがネットワークマップに追加された場合

**バージョン**

次のいずれかです。

- サーバーのバージョン : システム、Nmap、その他のアクティブなソースで識別された、またはホスト入力機能を使用して指定されたサーバーのバージョン
- 空白 : システムが既知のサーバーフィンガープリントに基づいてバージョンを識別できなかった場合、またはNetFlowデータを使用してサーバーがネットワークマップに追加された場合

## ■ サーバー データ フィールド

### Web アプリケーション (Web Application)

HTTP トライフィックでシステムが検出したペイロードコンテンツに基づいた Web アプリケーション。システムが HTTP のアプリケーションプロトコルを検出したものの、特定の Web アプリケーションを検出できない場合は、一般的な Web ブラウジングの指定が提示されるので注意してください。

### Web アプリケーションのカテゴリ、タグ、リスク、またはビジネスとの関連性 (Category, Tags, Risk, or Business Relevance for Web Applications)

Web アプリケーションに割り当てられているカテゴリ、タグ、リスク レベル、およびビジネス関連性。これらのフィルタを使用して、特定のデータセットを対象にすることができます。

### ヒット数 (Hits)

サーバーがアクセスされた回数。ホスト入力機能を使用して追加されたサーバーの場合、この値は必ず 0 になります。

### ソース タイプ (Source Type)

次の値のいずれかを指定します。

- [ユーザー (User) ] : user\_name
- [アプリケーション (Application) ] : app\_name
- スキャナ : scanner\_type (ネットワーク検出の設定を介して追加された Nmap またはスキャナ)
- Firepower システムによって検出されたサーバーの Firepower、Firepower Port Match、または Firepower Pattern Match
- NetFlow データを使用して追加されたサーバーの NetFlow

### ドメイン (Domain)

サーバーを実行しているホストのドメイン。このフィールドは、マルチテナンシーのために Firewall Management Center を設定したことがある場合に表示されます。

### Device

トライフィックを検出した管理対象デバイスか、NetFlow またはホスト入力データを処理したデバイスのいずれか。

### 現在のユーザー (Current User)

ホストに現在ログインしているユーザーの ID (ユーザー名)。

権限のないユーザーがあるホストにログインすると、そのログインはユーザーとホストの履歴に記録されます。権限のあるユーザーがホストに関連付けられていない場合、権限のないユーザーがそのホストの現行ユーザーとなることが可能です。ただし、権限のあるユーザーがホス

トにログインした後は、権限のある別のユーザーがログインした場合のみ、現行ユーザーが変わります。また、権限のないユーザーがホストの現行ユーザーである場合、そのユーザーを使用してユーザー制御を行うことはできません。

#### メンバー数 (Count)

各行に表示される情報と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のみです。

#### 関連トピック

[イベントの検索](#)

## アプリケーションデータとアプリケーション詳細データ

監視対象ホストが別のホストに接続すると、システムは多くの場合、どのアプリケーションが使用されたかを判断することができます。Firepower システムは、電子メール、インスタントメッセージ、ピアツーピア、Web アプリケーション、およびその他のタイプのアプリケーションが多用されると検出します。

検出されたそれぞれのアプリケーションに対してシステムは、アプリケーションを使用したIP アドレス、製品、バージョン、および使用が検出された回数を記録します。Web インターフェイスを使用して、アプリケーションイベントを表示、検索、および削除できます。ホスト入力機能を使用して、1つ以上のホスト上のアプリケーションデータを更新することもできます。

どのアプリケーションがどのホストで稼動しているかがわかっている場合は、その情報をもとにホストプロファイルの認定を作成し、この認定によって、トラフィック プロファイルの作成中に収集するデータを制約することができます。また、相関ルールをトリガーする条件を制約することもできます。また、アプリケーションの検出を相関ルールのベースにすることもできます。たとえば、従業員に特定のメールクライアントを使用させたい場合は、システムが、いざれかの対象ホストで別のメールクライアントが稼動していることを検出したときに相関ルールをトリガーすることができます。

Firepower のアプリケーションディテクタに関する最新情報は、各 Firepower システム更新のリリース ノート、各 VDB 更新のアドバイザリをよくご確認ください。

分析用にアプリケーションデータを収集および保存するには、ネットワーク検出ポリシーでアプリケーションの検出が有効になっていることを確認します。

## アプリケーションデータの表示

Firewall Management Center を使用して、検出されたアプリケーションのテーブルを表示できます。ここでユーザーは、検索する情報に応じてイベント ビューを操作することができます。

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。

ユーザーがアプリケーションにアクセスするときに表示されるページは、使用的なワークフローによって異なります。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。

## ■ アプリケーションデータ フィールド

### 手順

---

**ステップ1** 次のようにして、アプリケーションデータにアクセスします。

- ・事前定義されたワークフローを使用する場合、[分析 (Analysis)] > [ホスト (Hosts)] 見出し > [アプリケーション詳細 (Application Details)] を選択します。
- ・アプリケーションの詳細のテーブルビューが含まれないカスタムワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow))] をクリックして [クライアント (Clients)] を選択します。

**ステップ2** 次の選択肢があります。

- ・[(ワークフローの切り替え) ((switch workflow))] をクリックしてカスタムワークフローを含む別のワークフローを使用します。
- ・基本的なワークフロー操作を実行します ([ディスカバリおよびアイデンティティワークフローの使用 \(7 ページ\)](#) を参照)。
- ・テーブルのカラムの内容について詳しく調べます ([アプリケーションデータ フィールド \(40 ページ\)](#) を参照)。
- ・クライアント、アプリケーションプロトコル、Web アプリケーションの横にある [アプリケーション詳細ビュー (Application Detail View)] をクリックすることによって、特定のアプリケーションの [アプリケーション詳細ビュー (Application Detail View)] を開きます。
- ・イベント値を右クリックして、システムの外部にあるソース内のデータを表示します。表示されるオプションはデータタイプによって異なり、パブリック ソースが含まれます。他のソースは設定したリソースによって異なります。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。
- ・テーブルでイベントの値を右クリックしてシスコまたはサードパーティのインテリジェンスソースを選択して、イベントに関するインテリジェンスを収集します。たとえば、不審な IP アドレスに関する詳細情報を Cisco Talos から入手できます。表示されるオプションは、データタイプやシステムに設定されている統合によって異なります。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。

---

## アプリケーションデータ フィールド

システムは、既知のクライアント、アプリケーションプロトコル、または Web アプリケーションについてトラフィックを検出すると、アプリケーションおよびそのアプリケーションを実行しているホストに関する情報をログに記録します。

次に、アプリケーションテーブルで表示および検索できるフィールドについて説明します。

### Application

検出されたアプリケーションの名前。

## IP アドレス

アプリケーションを使用しているホストに関連付けられている IP アドレス。

## タイプ

アプリケーションのタイプであり、次のものがあります。

### アプリケーション プロトコル (Application Protocols)

ホスト間の通信を意味します。

### クライアント アプリケーション

ホスト上で動作しているソフトウェアを意味します。

### Web アプリケーション (Web Applications)

HTTP トランザクションの内容や要求された URL を意味します。

## カテゴリ

アプリケーションの最も不可欠な機能を表す一般的な分類。各アプリケーションは、少なくとも 1 つのカテゴリに属します。

## タグ

アプリケーションに関する追加情報。アプリケーションには任意の数のタグを付けることができます（タグなしも可能）。

## リスク (Risk)

アプリケーションが組織のセキュリティポリシーに違反する目的で使用される可能性。アプリケーションのリスクの範囲は、[極めて低 (Very Low) ] から [極めて高 (Very High) ] までです。

侵入イベントをトリガーしたトランザクションで検出される Application Protocol Risk、Client Risk、Web Application Risk の 3 つ（存在する場合）の中で最も高いものとなります。

## ビジネスとの関連性 (Business Relevance)

アプリケーションが、娯楽目的ではなく、組織のビジネス活動の範囲内で使用される可能性。アプリケーションのビジネスとの関連性の範囲は、[極めて低 (Very Low) ] から [極めて高 (Very High) ] までです。

侵入イベントをトリガーしたトランザクションで検出される Application Protocol Business Relevance、Client Business Relevance、Web Application Business Relevance の 3 つ（存在する場合）の中で最も低いものとなります。

## 現在のユーザー (Current User)

ホストに現在ログインしているユーザーの ID（ユーザー名）。

## ■ アプリケーション詳細データの表示

権限のないユーザーがホストにログインすると、そのログインはユーザーおよびホストの履歴に記録されることに注意してください。権限のあるユーザーがホストに関連付けられていない場合、権限のないユーザーがそのホストの現行ユーザーとなることが可能ですが。ただし、権限のあるユーザーがホストにログインした後は、権限のある別のユーザーがログインした場合のみ、現行ユーザーが変わります。また、権限のないユーザーがホストの現行ユーザーである場合、そのユーザーを使用してユーザー制御を行うことはできません。

### ドメイン (Domain)

アプリケーションを使用しているホストのドメイン。このフィールドは、マルチテナントのために Firewall Management Center を設定したことがある場合に表示されます。

### メンバー数 (Count)

各行に表示される情報と一致するイベントの数。[カウント (Count) ] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

### 関連トピック

[イベントの検索](#)

## アプリケーション詳細データの表示

Firewall Management Center を使用して、検出されたアプリケーションの詳細テーブルを表示できます。ここでユーザーは、検索する情報に応じてイベント ビューを操作することができます。

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。

ユーザーがアプリケーションの詳細にアクセスするときに表示されるページは、使用するワークフローによって異なります。2つの事前定義されたワークフローがあります。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。

### 手順

---

**ステップ1** 次のようにして、アプリケーション詳細データにアクセスします。

- ・事前定義されたワークフローを使用する場合、[分析 (Analysis) ] > [ホスト (Hosts) ] 見出し > [アプリケーション詳細 (Application Details) ] を選択します。
- ・アプリケーションの詳細のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow)) ] をクリックして [クライアント (Clients) ] を選択します。

**ステップ2** 次の選択肢があります。

- ・[(ワークフローの切り替え) ((switch workflow)) ] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。

- 基本的なワークフロー操作を実行します（[ディスカバリおよびアイデンティティワークフローの使用（7ページ）](#) を参照）。
- テーブルのカラムの内容について詳しく調べます（[アプリケーションの詳細データフィールド（43ページ）](#) を参照）。
- クライアントの横にある [アプリケーション詳細ビュー（Application Detail View）] をクリックして、特定のアプリケーションの[アプリケーション詳細ビュー（Application Detail View）]を開きます。
- イベント値を右クリックして、システムの外部で利用可能なソース内のデータを表示します。表示されるオプションはデータタイプによって異なり、パブリック ソースが含まれます。他のソースは設定したリソースによって異なります。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。
- テーブルでイベントの値を右クリックしてシスコまたはサードパーティのインテリジェンス ソースを選択して、イベントに関するインテリジェンスを収集します。たとえば、不審な IP アドレスに関する詳細情報を Cisco Talos から入手できます。表示されるオプションは、データタイプやシステムに設定されている統合によって異なります。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。

## アプリケーションの詳細データ フィールド

システムは、既知のクライアント、アプリケーションプロトコル、または Web アプリケーションについてトラフィックを検出すると、アプリケーションおよびそのアプリケーションを実行しているホストに関する情報をログに記録します。

次に、アプリケーションの詳細テーブルで表示および検索できるフィールドについて説明します。

### 前回の使用（Last Used）

アプリケーションが前回使用された時間、またはホスト入力機能を使用してアプリケーションデータが更新された時間。[前回の使用（Last Used）]の値は、システムがアプリケーション情報の更新を検出したときだけでなく、少なくともユーザがネットワーク検出ポリシーに設定した更新間隔の頻度で更新されます。

### IP アドレス

アプリケーションを使用しているホストに関連付けられている IP アドレス。

### クライアント（Client）

アプリケーションの名前。ただし、システムがアプリケーションプロトコルを検出したにも関わらず特定のクライアントを検出できなかった場合は、アプリケーションプロトコル名に client が付加されて一般名が表示されます。

### バージョン（Version）

アプリケーションのバージョン。

## ■ アプリケーションの詳細データ フィールド

**クライアント、アプリケーション プロトコル、および Web アプリケーションのカテゴリ、タグ、リスク、またはビジネスとの関係性 (Category, Tags, Risk, or Business Relevance for Clients, Application Protocols, and Web Applications)**

アプリケーションに割り当てられているカテゴリ、タグ、リスク レベル、およびビジネスとの関連性。これらのフィルタを使用して、特定のデータ セットを対象にすることができます。

### アプリケーション プロトコル (Application Protocol)

アプリケーションで使用されるアプリケーションプロトコル。ただし、システムがアプリケーションプロトコルを検出したにも関わらず特定のクライアントを検出できなかった場合は、アプリケーションプロトコル名に `client` が付加されて一般名が表示されます。

### Web アプリケーション (Web Application)

HTTP トラフィックでシステムが検出したペイロード コンテンツまたは URL に基づく Web アプリケーション。ただし、HTTP のアプリケーションプロトコルが検出されたにも関わらず特定の Web アプリケーションを検出できない場合、ここには、標準の Web 閲覧先が表示されます。

### ヒット数 (Hits)

システムが使用中のアプリケーションを検出した回数。ホスト入力機能を使用して追加されたアプリケーションの場合、この値は常に 0 になります。

### ドメイン (Domain)

アプリケーションを使用しているホストのドメイン。このフィールドは、マルチテナントのために Firewall Management Center を設定したことがある場合に表示されます。

### デバイス

アプリケーションの詳細が含まれている検出イベントを生成したデバイス。

### 現在のユーザー (Current User)

ホストに現在ログインしているユーザーの ID (ユーザー名)。

権限のないユーザーがホストにログインすると、そのログインはユーザーおよびホストの履歴に記録されることに注意してください。権限のあるユーザーがホストに関連付けられていない場合、権限のないユーザーがそのホストの現行ユーザーとなることが可能ですが。ただし、権限のあるユーザーがホストにログインした後は、権限のある別のユーザーがログインした場合のみ、現行ユーザーが変わります。また、権限のないユーザーがホストの現行ユーザーである場合、そのユーザーを使用してユーザー制御を行うことはできません。

### メンバー数 (Count)

各行に表示される情報と一致するイベントの数。[カウント (Count) ] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

## 関連トピック

[イベントの検索](#)

# 脆弱性データ

システムには、独自の脆弱性追跡データベースが含まれています。これはシステムのフィンガープリント機能と組み合わせて使用して、ネットワーク上のホストに関連付けられている脆弱性を特定します。ホストで稼動しているオペレーティングシステム、サーバ、およびクライアントには、関連付けられている異なる脆弱性一式があります。

Firewall Management Center を使用して次のことを行えます。

- ホストごとの脆弱性を追跡および確認できます。
- ホストにパッチを適用した後、またはホストが脆弱性に影響されないと判断した場合は、そのホストの脆弱性を非アクティブにすることができます。

サーバで使用されるアプリケーションプロトコルが Firewall Management Center 構成内でマップされない限り、ベンダーレスおよびバージョンレスのサーバの脆弱性はマップされません。ベンダーレスおよびバージョンレスのクライアントの脆弱性はマップできません。

## 関連トピック

[サーバの脆弱性のマッピング](#)

# 脆弱性データのフィールド

注記がある場合を除き、これらのフィールドは、[分析 (Analysis)] > [ホスト (Hosts)] > [脆弱性 (Vulnerabilities)] の下のすべてのページに表示されます。

## メンバー数 (Count)

各行に表示される情報と一致するイベントの数。[カウント (Count)] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

## CVE ID

MITRE の Common Vulnerabilities and Exposures (CVE) データベース (<https://cve.mitre.org/>) の脆弱性に関連付けられた識別番号。

National Vulnerability Database (NVD) でこの脆弱性の詳細を表示するには、CVE ID を右クリックし、[NVDで説明を表示する (View description in NVD)] を選択します。

## 発行日 (Date Published)

脆弱性が公開された日付。

## 説明 (Description)

National Vulnerability Database (NVD) からの脆弱性の簡単な説明。

## 脆弱性データのフィールド

完全な説明については、CVE ID を右クリックし、[NVDで説明を表示する（View description in NVD）]を選択して、National Vulnerability Database (NVD) の詳細を表示します。

### 影響

「脆弱性の影響（Vulnerability Impact）」（下記）を参照してください。

#### 影響修飾子（Impact Qualification）

このフィールドは、[脆弱性の詳細（Vulnerability Details）] ページでのみ使用できます。

ドロップダウンリストを使用して、脆弱性を有効または無効にします。Firewall Management Centerは、影響の相関関係において、無効な脆弱性を無視します。

ユーザーがここで指定する設定によって、システム全体で脆弱性がどのように処理されるか、およびユーザーが値を選択するホストプロファイルに脆弱性が限定されないかが決まります。

#### リモート（Remote）

脆弱性がリモートで不正利用されるかどうかを示します（TRUE/FALSE）。

### 重大度

National Vulnerability Database (NVD) の基本スコアと Common Vulnerability Scoring System スコア (CVSS)。

### Snort ID

[Snort ID] (SID) データベースにおいて脆弱性に関連付けられている識別番号。つまり、侵入ルールで特定の脆弱性を悪用するネットワーク トライフィックを検出できる場合、その脆弱性は、侵入ルールの SID に関連付けられます。

脆弱性は複数の SID に関連付けることが可能（または SID に関連付けないことも可能）であることに注意してください。脆弱性が複数の SID に関連付けられている場合、脆弱性テーブルには、各 SID に対して 1 つのローが含まれています。

### SVID

脆弱性を追跡するためにシステムで使用する脆弱性の識別番号。

この脆弱性の詳細を表示するには、[表示（View）] (👁) をクリックします。

### 脆弱性の影響/影響

脆弱性のシビラティ（重大度）。0~10 の値で、10 は最も重大であることを示します。

### 関連トピック

[イベントの検索](#)

## 脆弱性の非アクティブ化

脆弱性を非アクティブ化すると、システムでこの脆弱性を使用して侵入の影響の関連付けを評価することができなくなります。ネットワーク上のホストにパッチを適用した後、またはホストが脆弱性の影響を受けないと判断した後に、脆弱性を非アクティブ化できます。システムが、この脆弱性から影響を受けている新しいホストを検出すると、この脆弱性はこのホストに対して有効であると見なされます（自動的には非アクティブ化されません）。

IP アドレスによって制約されていない脆弱性ワークフロー内である 1 つの脆弱性を非アクティブ化すると、ネットワーク上の検出されたすべてのホストに対してその脆弱性が非アクティブ化されます。脆弱性ワークフロー内の脆弱性を非アクティブ化できるのは、次の各ページだけです。

- デフォルトの脆弱性ワークフローの 2 ページ目の [ネットワーク上の脆弱性 (Vulnerabilities on the Network)]。これには、ネットワーク上のホストに適用される脆弱性のみが表示されます。
- 脆弱性ワークフロー（カスタムまたは事前定義）のページ。このワークフローは、検索を使用して IP アドレスに基づいて制約されます。

1 台のホストに対して 1 つの脆弱性を非アクティブ化できます。この非アクティブ化は、ネットワークマップの使用、ホストのホストプロファイルの使用、または脆弱性を非アクティブ化する対象の 1 つ以上のホストの IP アドレスに基づいて脆弱性ワークフローを制約することによって行えます。関連付けられた複数の IP アドレスを持つホストの場合、この機能はそのホストの選択された 1 つの IP アドレスのみに適用されます。

マルチドメイン展開では、先祖ドメインで脆弱性を非アクティブ化すると、すべての子孫ドメインでその脆弱性が非アクティブ化されます。リーフドメインでは、脆弱性が先祖ドメインでアクティブ化された場合、リーフドメインのデバイスの脆弱性をアクティブ化または非アクティブ化できます。

### 関連トピック

[個々のホストに関する脆弱性の非アクティブ化](#)

[個々の脆弱性の非アクティブ化](#)

[複数の脆弱性の非アクティブ化 \(49 ページ\)](#)

## 脆弱性データの表示

Firewall Management Center を使用して、脆弱性のテーブルを表示できます。ここでユーザーは、検索する情報に応じてイベント ビューを操作することができます。

脆弱性にアクセスするときに表示されるページは、使用するワークフローによって異なります。ユーザーは事前定義のワークフローを使用できますが、これには脆弱性のテーブルビューが含まれています。検出されたいずれかのホストが脆弱性を示しているかどうかに関係なく、テーブルビューにはデータベース内の各脆弱性に対して 1 つのローが含まれています。事前定義のワークフローの 2 ページ目には、ネットワーク上で検出されたホストに適用されるそれぞれの脆弱性（まだユーザーが非アクティブにしていないもの）に対して 1 つのローが含まれています。事前定義のワークフローは脆弱性の詳細ビューで終了しますが、このビューには、制約を満たすすべての脆弱性について詳細な説明が含まれています。

## 脆弱性の詳細の表示



**ヒント** 単一のホストまたはホストのセットに適用される脆弱性を表示する場合は、ホストの IP アドレスまたは IP アドレスの範囲を指定して、脆弱性の検索を実行します。

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。

脆弱性のテーブルは、マルチドメイン展開のドメインによって制限されません。

## 手順

**ステップ1** 次のように、脆弱性のテーブルにアクセスします。

- ・事前定義された脆弱性ワークフローを使用する場合、[分析 (Analysis)]>[ホスト (Hosts)]見出し>[脆弱性 (Vulnerabilities)]を選択します。
- ・脆弱性テーブルビューが含まれないカスタムワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow))]をクリックして[脆弱性 (Vulnerabilities)]を選択します。

**ステップ2** 次の選択肢があります。

- ・基本的なワークフロー操作を実行します（[ディスカバリおよびアイデンティティワークフローの使用 \(7 ページ\)](#) を参照）。
- ・脆弱性を非アクティブにして、現在脆弱な状態にあるホストについて、侵入の影響の相関に使用しないようにします（[複数の脆弱性の非アクティビ化 \(49 ページ\)](#) を参照）。
- ・SVID カラムの[表示 (View)] (◎) をクリックして、脆弱性に関する詳細を表示します。または、脆弱性 ID を制約して脆弱性の詳細ページへドリルダウンします。[脆弱性の詳細の表示 \(48 ページ\)](#) でその他の詳細を表示するオプションを確認してください。
- ・タイトルを右クリックして[フルテキストの表示 (Show Full Text)]を選択することによって、脆弱性タイトルのフルテキストを表示します。

## 脆弱性の詳細の表示

## 手順

脆弱性の詳細は、次の方法のいずれかで表示できます。

- ・[分析 (Analysis)]>[ホスト (Hosts)]見出し>[脆弱性 (Vulnerabilities)]を選択し、SVID の横にある[表示 (View)] (◎) をクリックします。
- ・[分析 (Analysis)]>[ホスト (Hosts)]見出し>[サードパーティの脆弱性 (Third-Party Vulnerabilities)]を選択し、SVID の横にある[表示 (View)] (◎) をクリックします。

- [分析 (Analysis)] > [ホスト (Hosts)] 見出し > [ネットワークマップ (Network Map)] を選択し、[脆弱性 (Vulnerabilities)] をクリックします。
- 脆弱性の影響を受けるホストのプロファイルを表示し ([分析 (Analysis)] > [ホスト (Hosts)] 見出し > [ネットワークマップ (Network Map)] ([Analysis]>[Hosts]>[Network Map]) 、 [ホスト (Hosts)] をクリックし、調査しているホストをドリルダウンしてクリックします) 、そのプロファイルの [脆弱性 (Vulnerabilities)] セクションを展開します。
- [分析 (Analysis)] > [ホスト (Hosts)] > [脆弱性 (Vulnerabilities)] の下にある任意のテーブルで、[CVE ID] 列の値を右クリックし、[NVDで説明を表示する (View description in NVD)] を選択して、NVD (National Vulnerabilities Database) Web サイトでその CVE を表示します。

## 複数の脆弱性の非アクティブ化

IP アドレスで制約されていない脆弱性ワークフロー内で脆弱性を非アクティブにすると、ネットワーク上で検出されたすべてのホストに対する脆弱性が非アクティブ化されます。

マルチドメイン導入では、先祖ドメインで脆弱性を非アクティブ化すると、すべての子孫ドメインでも脆弱性が非アクティブ化されます。リーフドメインは、先祖ドメインで脆弱性がアクティブ化されていれば、自分のデバイスの脆弱性をアクティブ化または非アクティブ化できます。

### 手順

**ステップ1** 次のように、脆弱性のテーブルにアクセスします。

- 事前定義された脆弱性ワークフローを使用する場合、[分析 (Analysis)] > [ホスト (Hosts)] 見出し > [脆弱性 (Vulnerabilities)] を選択します。
- 脆弱性テーブルビューが含まれないカスタムワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow))] をクリックして [脆弱性 (Vulnerabilities)] を選択します。

**ステップ2** [ネットワークの脆弱性 (Vulnerabilities on the Network)] をクリックします。

**ステップ3** 非アクティブにする脆弱性の横にあるチェックボックスをオンにします。

**ステップ4** ページ下部の [レビュー (Review)] をクリックします。

### 関連トピック

[個々のホストに関する脆弱性の非アクティブ化](#)

[個々の脆弱性の非アクティブ化](#)

## サードパーティの脆弱性データ

Firepower システムには、それ独自の脆弱性追跡データベースが含まれています。そのデータベースは、このシステムのフィンガープリンティング機能と組み合わせて使用されて、ネットワーク上のホストに関連付けられている脆弱性が特定されます。

システムの脆弱性データは、サードパーティ製のアプリケーションからインポートしたネットワーク マップデータで補完できます。これを行うには、組織で、このデータをインポートするためのスクリプトを記述できるか、コマンドラインでファイルのインポートを作成できなければなりません。詳細については、*Firepower* システムホスト入力 API ガイドを参照してください。

インポートしたデータを影響の相間に含めるには、サードパーティの脆弱性情報を、データベース内のオペレーティングシステムおよびアプリケーションの定義にマップする必要があります。サードパーティの脆弱性情報は、クライアントの定義にマップすることはできません。

## サードパーティの脆弱性データの表示

ホスト入力機能を使用してサードパーティの脆弱性データをインポートした後で、Firewall Management Center を使用してサードパーティの脆弱性のテーブルを表示することができます。ここでユーザーは、検索する情報に応じてイベント ビューを操作することができます。

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。

サードパーティの脆弱性にアクセスするときに表示されるページは、使用するワークフローによって異なります。2つの事前定義されたワークフローがあります。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。

### 手順

**ステップ1** 次のようにして、サードパーティの脆弱性データにアクセスします。

- 事前定義されたワークフローを使用する場合、[分析 (Analysis)] > [ホスト (Hosts)] 見出し > [サードパーティの脆弱性 (Third-Party Vulnerabilities)] を選択します。
- サードパーティの脆弱性のテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow))] をクリックして [送信元別の脆弱性 (Vulnerabilities by Source)] または [IP アドレス別の脆弱性 (Vulnerabilities by IP Address)] を選択します。

**ステップ2** 次の選択肢があります。

- [(ワークフローの切り替え) ((switch workflow))] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します ([ディスカバリおよびアイデンティティワークフローの使用 \(7 ページ\)](#) を参照)。

- テーブルのカラムの内容について詳しく調べます（[サードパーティの脆弱性データのフィールド（51 ページ）](#) を参照）。
- SVID カラムの [表示（View）] (◎) をクリックして、サードパーティの脆弱性に関する詳細を表示します。または、脆弱性 ID を制約して脆弱性の詳細ページへドリルダウンします。

## サードパーティの脆弱性データのフィールド

サードパーティの脆弱性テーブルで表示および検索できるフィールドの詳細は以下のとおりです。

### 脆弱性ソース（Vulnerability Source）

サードパーティの脆弱性のソース（QualysGuard、NeXpose など）。

### 脆弱性 ID（Vulnerability ID）

ソースの脆弱性に関連付けられている ID 番号。

### IPアドレス（IP Address）

脆弱性の影響を受けるホストに関連付けられている IP アドレス。

### ポート

ポート番号（脆弱性が、特定のポート上で実行されているサーバに関連付けられている場合）。

### Bugtraq ID

Bugtraq データベースにおいて脆弱性に関連付けられている識別番号。

### CVE ID

MITRE の Common Vulnerabilities and Exposures (CVE) データベース (<https://cve.mitre.org/>) の脆弱性に関連付けられた識別番号。

### SVID

脆弱性を追跡するためにシステムで使用する従来の脆弱性識別番号。

SVID について脆弱性の詳細にアクセスするには、[表示（View）] (◎) をクリックします。

### Snort ID

[Snort ID] (SID) データベースにおいて脆弱性に関連付けられている識別番号。つまり、侵入ルールで特定の脆弱性を悪用するネットワーク トラフィックを検出できる場合、その脆弱性は、侵入ルールの SID に関連付けられます。

## アクティブセッション、ユーザー、およびユーザー アクティビティ データ

脆弱性は複数の SID に関連付けることが可能（または SID に関連付けないことも可能）であることに注意してください。脆弱性が複数の SID に関連付けられている場合、脆弱性テーブルには、各 SID に対して 1 つのローが含まれています。

### タイトル (Title)

脆弱性のタイトル。

### 説明 (Description)

脆弱性についての簡単な説明。

### ドメイン (Domain)

この脆弱性を持つホストのドメイン。このフィールドは、マルチテナントのために Firewall Management Center を設定したことがある場合に表示されます。

### メンバー数 (Count)

各行に表示される情報と一致するイベントの数。[カウント (Count) ] フィールドは、複数の同一行が生成される制限を適用した後でのみ表示されることに注意してください。

### 関連トピック

[イベントの検索](#)

## アクティブセッション、ユーザー、およびユーザー アクティビティ データ

アイデンティティ ソースは、アクティブなセッションデータ、ユーザデータ、およびユーザアクティビティデータを収集します。データは、次の個々のユーザ関連のワークフローに表示されます。

- [アクティブなセッション (Active Sessions) ] : このワークフローには、ネットワーク上の現在のすべてのユーザセッションが表示されます。複数の同時アクティブセッションを実行する単一ユーザは、この表で複数の行を占めます。このワークフローに表示されるユーザデータの種類について、詳しくは[アクティブセッションデータ \(63 ページ\)](#) を参照してください。
- ユーザ : このワークフローは、ネットワークで認識されるすべてのユーザを表示します。この表では 1 ユーザが 1 つの行を占めます。このワークフローに表示されるユーザデータの種類について、詳しくは[ユーザー データ \(User Data\) \(65 ページ\)](#) を参照してください。
- ユーザアクティビティ : このワークフローは、ネットワークで認識されるすべてのユーザアクティビティを表示します。この表では、複数のユーザアクティビティインスタンスを持つ 1 ユーザが複数の行を占めます。このワークフローに表示されるユーザアクティビティの種類の詳細については、[ユーザー アクティビティ データ \(68 ページ\)](#) を参照してください。

これらのワークフローの入力元であるユーザー イデンティティ ソースの詳細については、『Cisco Secure Firewall Management Center デバイス構成ガイド』の「」を参照してください。

## ユーザー関連フィールド

ユーザー関連データは、アクティブ セッション、ユーザー、およびユーザー アクティビティ のテーブルに表示されます。



(注) Azure AD レルムユーザーおよびパッシブ ID エージェントによって検出されたユーザーのアクティブ セッションは、新しいUI レイアウトの[アクティブ セッション (Active Sessions) ]にのみ表示され、レガシー UI には表示されません。

表 1:アクティブ セッション、ユーザー、およびユーザー アクティビティ のフィールドの説明

フィールド	説明	[アクティブなセッション (Active Sessions) ] テーブル	[ユーザー テーブル (Users Table) ]	[ユーザー アクティビティ (User Activity) ] テーブル
アクティブ セッション数 (Active Session Count)	ユーザーに関連付けられているアクティブ セッションの数。	非対応	はい	非対応
認証タイプ (Authentication Type)	認証のタイプ : [認証なし (No Authentication) ]、[パッシブ認証 (Passive Authentication) ]、[アクティブ認証 (Active Authentication) ]、[ゲスト認証 (Guest Authentication) ]、[失敗した認証 (Failed Authentication) ]、または [VPN 認証 (VPN Authentication) ]。  各認証タイプでサポートされるアイデンティティ ソースの詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。	はい	非対応	はい

## ■ ユーザー関連フィールド

フィールド	説明	[アクティブなセッション (Active Sessions) ] テーブル	[ユーザー テーブル (Users Table) ]	[ユーザー アクティビティ (User Activity) ] テーブル
ポリシーに使用可能	<p>値 [はい (Yes)] は、ユーザーがユーザーストア (Active Directory など) から取得されたことを意味します。 (パッシブ ID エージェントは一時的なユーザーをダウンロードしません。)</p> <p>値 [いいえ (No)] は、Firewall Management Center がそのユーザーのログインのレポートを取得したものの、そのユーザーがユーザーストアに存在しないことを意味します。これは、除外されたグループのユーザーがユーザーストアにログインした場合に発生することがあります。ルームを設定するときにグループをダウンロード対象から除外することができます。</p> <p>ポリシーに使用できないユーザー (一時的なユーザーなど) は、Firewall Management Center には記録されますが、管理対象デバイスには送信されません。</p>	非対応	はい	非対応
メンバー数 (Count)	<p>(注) [カウント (Count) ] フィールドは、制約を適用した結果、同じ行が複数作成された場合にのみ表示されます。</p> <p>テーブルに応じて、特定の行に表示される情報と一致するセッション、ユーザー、またはアクティビティイベントの数。</p>	はい	はい	はい
現在の IP (Current IP)	<p>(「現在の IP/ドメイン (Current IP/Domain) 」および「IP アドレス (IP address) 」も参照してください)</p> <p>ユーザーがログインしたホストに関連付けられている IP アドレス。</p> <p>ユーザーにアクティブセッションがない場合、[ユーザー (Users) ] テーブルでこのフィールドが空白になります。</p>	はい	非対応	非対応

フィールド	説明	[アクティブなセッション (Active Sessions) ] テーブル	[ユーザーテーブル (Users Table) ]	[ユーザーアクティビティ (User Activity) ] テーブル
<b>部署名 (Department)</b>	<p>ユーザーの部署（レルムが取得）。サーバー上のユーザーに明示的に関連付けられている部門がない場合、この部門は、サーバーが割り当てるいずれかのデフォルトグループとして示されます。たとえば、Active Directory では、これは Users (ad) となります。以下の場合、このフィールドは空白になります。</p> <ul style="list-style-type: none"> <li>• レルムを設定していない。</li> <li>• Firewall Management Center が、Firewall Management Center データベースのユーザーと LDAP レコードを相關させていない（AIM、Oracle、または SIP ログインによってユーザーがデータベースに追加された場合など）。</li> </ul>	はい	はい	非対応
<b>Description</b>	セッション、ユーザー、またはユーザーアクティビティについての詳細情報（利用可能な場合）。	いいえ	非対応	はい
<b>[デバイス (Device) ]</b>	<p>トラフィックベースの検出またはアクティブ認証アイデンティティソースによって検出されたユーザーアクティビティの場合は、ユーザーを識別したデバイスの名前。</p> <p>他のタイプのユーザーアクティビティの場合は、管理している側の Firewall Management Center になります。</p> <p><b>(注)</b> 高可用性展開で VPN を構成した場合、アクティブな VPN セッションに対して表示されるデバイス名は、ユーザーセッションを識別したプライマリデバイスまたはセカンダリデバイスである可能性があります。</p>	はい	非対応	はい

## ■ ユーザー関連フィールド

フィールド	説明	[アクティブなセッション (Active Sessions) ] テーブル	[ユーザー テーブル (Users Table) ]	[ユーザー アクティビティ (User Activity) ] テーブル
ディスカバリ アプリケーション (Discovery Application)	<p>ユーザーの検出に使用されるアプリケーションまたはプロトコル。</p> <ul style="list-style-type: none"> <li>トライフィックベースの検出によって検出されたユーザー アクティビティの場合は、ldap、pop3、imap、oracle、sip、http、ftp、mdns、またはaim のいずれか。</li> </ul> <p>(注) ユーザーはSMTPログインに基づいてデータベースに追加されません。</p> <ul style="list-style-type: none"> <li>他のすべてのユーザー アクティビティの場合：ldap。</li> </ul>	はい	はい	はい
[現在の IP ドメイン (Current IP Domain) ]/[ドメイン (Domain) ]	<p>[アクティブセッション (Active Sessions) ] テーブルでは、ユーザー アクティビティが検出されたマルチテナンシー ドメイン。</p> <p>[ユーザー (Users) ] テーブルでは、ユーザーのルームに関連付けられたマルチテナンシー ドメイン。</p> <p>[ユーザー アクティビティ (User Activity) ] テーブルでは、ユーザー アクティビティが検出されたマルチテナンシー ドメイン。</p> <p>このフィールドは、マルチテナンシーのために Firewall Management Center を設定したことがある場合に表示されます。</p>	はい	はい	はい
Eメール (Email)	<p>ユーザーの電子メールアドレス。以下の場合、このフィールドは空白になります。</p> <ul style="list-style-type: none"> <li>AIM ログインによってユーザーがデータベースに追加された。</li> <li>LDAP ログインによってユーザーがデータベースに追加されており、LDAP サーバー上にユーザーと関連付けられている電子メールアドレスが存在しない。</li> </ul>	○	対応（電子メールとして）	いいえ

フィールド	説明	[アクティブなセッション (Active Sessions) ] テーブル	[ユーザーテーブル (Users Table) ]	[ユーザーアクティビティ (User Activity) ] テーブル
終了ポート (End Port)	TS エージェントによってユーザーが報告され、そのユーザーのセッションが現在アクティブである場合、このフィールドは、ユーザーに割り当てられたポート範囲の終了値を示します。ユーザーの TS エージェントセッションが非アクティブである場合、またはユーザーが別のアイデンティティソースによって報告された場合、このフィールドは空白になります。	はい	非対応	はい
エンドポイントロケーション (Endpoint Location)	ISE で指定された、ユーザーの認証に ISE を使用したネットワークデバイスの IP アドレス。ISE を設定していない場合、このフィールドは空白です。	いいえ	非対応	はい
エンドポイントプロファイル (Endpoint Profile)	Cisco ISE によって識別されるユーザーのエンドポイントデバイスタイプ。ISE を設定していない場合、このフィールドは空白です。	いいえ	非対応	はい
イベント	ユーザー アクティビティのタイプ。	いいえ	非対応	はい
First Name	ユーザーの名（レルムが取得）。以下の場合、このフィールドは空白になります。 <ul style="list-style-type: none"><li>• レルムを設定していない。</li><li>• Firewall Management Center が、Firewall Management Center データベースのユーザーと LDAP レコードを相關させていない（AIM、Oracle、または SIP ログインによってユーザーがデータベースに追加された場合など）。</li><li>• サーバーに、対象のユーザーと関連付けられている名がない。</li></ul>	はい	はい	非対応

## ■ ユーザー関連フィールド

フィールド	説明	[アクティブなセッション (Active Sessions) ] テーブル	[ユーザーテーブル (Users Table) ]	[ユーザーアクティビティ (User Activity) ] テーブル
[IPアドレス (IP Address) ]	<p>[ユーザー ログイン (User Login) ] ユーザー アクティビティの場合は、次のログインに関連する IP アドレスまたは内部 IP アドレス。</p> <ul style="list-style-type: none"> <li>• LDAP、POP3、IMAP、FTP、HTTP、MDNS、および AIM ログイン：ユーザーのホストのアドレス</li> <li>• SMTP および Oracle のログイン：サーバーのアドレス</li> <li>• SIP ログイン：セッション発信者のアドレス</li> </ul> <p>(「現在の IP (Current IP)」および「現在の IP/ドメイン (Current IP/Domain)」も参照してください)</p> <p>関連付けられている IP アドレスは、そのユーザーが IP アドレスの現行のユーザーであることを意味するわけではありません。権限を持たないユーザーがホストにログインすると、そのログインはユーザーおよびホストの履歴に記録されます。権限のあるユーザーがホストに関連付けられていない場合、権限のないユーザーがそのホストの現行ユーザーとなることが可能です。ただし、権限のあるユーザーがホストにログインした後は、権限のある別のユーザーがログインした場合のみ、現行ユーザーが変わります。</p> <p>他のタイプのユーザー アクティビティの場合、このフィールドは空白です。</p>	いいえ	非対応	はい

フィールド	説明	[アクティブなセッション (Active Sessions) ] テーブル	[ユーザーテーブル (Users Table) ]	[ユーザーアクティビティ (User Activity) ] テーブル
<b>Last Name</b>	<p>ユーザーの姓（レルムが取得）。以下の場合、このフィールドは空白になります。</p> <ul style="list-style-type: none"> <li>レルムを設定していない。</li> <li>Firewall Management Center が、Firewall Management Center データベースのユーザーと LDAP レコードを相關させていない（AIM、Oracle、または SIP ログインによってユーザーがデータベースに追加された場合など）。</li> <li>サーバーに、対象のユーザーと関連付けられている姓がない。</li> </ul>	はい	はい	非対応
<b>前回の検出 (Last Seen)</b>	ユーザーのセッションが最後に開始された（またはユーザー データが更新された）日時。	はい	はい	非対応
<b>ログイン時刻 (Login Time)</b>	ユーザーのセッションが開始した日時。	はい	非対応	非対応
<b>PAT 範囲の開始 (PAT Range Start)</b>	TS エージェントユーザーのポートアドレス変換範囲の開始。	はい	非対応	非対応
<b>Phone Number</b>	<p>ユーザーの電話番号（レルムが取得）。以下の場合、このフィールドは空白になります。</p> <ul style="list-style-type: none"> <li>レルムを設定していない。</li> <li>Firewall Management Center が、Firewall Management Center データベースのユーザーと LDAP レコードを相關させていない（AIM、Oracle、または SIP ログインによってユーザーがデータベースに追加された場合など）。</li> <li>サーバーに、対象のユーザーと関連付けられている電話番号が存在しない。</li> </ul>	対応（電話として）	はい	非対応
<b>レルム</b>	ユーザーに関連付けられているアイデンティティ レルム。	はい	はい	はい

## ■ ユーザー関連フィールド

フィールド	説明	[アクティブなセッション (Active Sessions) ] テーブル	[ユーザーテーブル (Users Table) ]	[ユーザーアクティビティ (User Activity) ] テーブル
セキュリティグループタグ (Security Group Tag)	パケットが信頼できる TrustSec ネットワークへ送信されたときに、Cisco TrustSec によって適用される [セキュリティグループタグ (Security Group Tag) ] (SGT) 属性。ISE を設定していない場合、このフィールドは空白です。	いいえ	非対応	はい
セッション時間 (Session Duration)	[ログイン時刻 (Login Time) ] と現在の時刻から計算されたユーザー セッションの期間。	はい	非対応	非対応
開始ポート (Start Port)	TS エージェントによってユーザーが報告され、そのユーザーのセッションが現在アクティブである場合、このフィールドは、ユーザーに割り当てられたポート範囲の開始値を示します。ユーザーの TS エージェントセッションが非アクティブである場合、またはユーザーが別のアイデンティティソースによって報告された場合、このフィールドは空白になります。	はい	非対応	はい
時刻 (Time)	システムがユーザー アクティビティを検出した時間。	いいえ	非対応	はい
[ユーザー (User) ]	このフィールドには少なくとも、ユーザーのレルムとユーザー名が表示されます。たとえば、Lobby\jsmith と表示された場合は、Lobby がレルム、jsmith がユーザー名です。  レルムが LDAP サーバーから追加のユーザーデータをダウンロードし、システムがそれをユーザーに関連付けた場合は、このフィールドにユーザーの名、姓、タイプも表示されます。たとえば、John Smith (Lobby\jsmith, LDAP) と表示された場合は、John Smith がユーザーの名前、LDAP がそのタイプです。  (注) トライフィックベースの検出では失敗した AIM ログインが記録される可能性があるため（たとえば、ユーザーが正しくないユーザー名を入力した場合など）、Firewall Management Center は無効な AIM ユーザーを保存する可能性があります。	はい	はい	非対応

フィールド	説明	[アクティブなセッション (Active Sessions) ] テーブル	[ユーザーテーブル (Users Table) ]	[ユーザー活動 (User Activity) ] テーブル
<b>Username</b>	ユーザーに関連付けられているユーザー名。	はい	はい	はい
<b>VPN 受信バイト数 (VPN Bytes In)</b>	<p>リモートアクセス VPN の報告によるユーザーアクティビティの場合は、Firewall Threat Defense がリモートピアまたはクライアントから受信した合計バイト数。</p> <p>(注) ユーザーの VPN セッションが終了した後、受信した合計バイト数を表示できます。継続中の VPN セッションでは、これは動的カウンタではありません。</p> <p>他のタイプのユーザー活動の場合、このフィールドは空白です。</p>	はい	非対応	はい
<b>VPN 送信バイト数 (VPN Bytes Out)</b>	<p>リモートアクセス VPN の報告によるユーザーアクティビティの場合は、Firewall Threat Defense がリモートピアまたはクライアントに伝送された合計バイト数。</p> <p>(注) ユーザーの VPN セッションが終了した後、送信した合計バイト数を表示できます。継続中の VPN セッションでは、これは動的カウンタではありません。</p> <p>他のタイプのユーザー活動の場合、このフィールドは空白です。</p>	いいえ	非対応	はい
<b>VPN クライアントのアプリケーション (VPN Client Application)</b>	<p>リモートアクセス VPN の報告によるユーザーアクティビティの場合は、リモートユーザーの Cisco Secure Client の AnyConnect VPN モジュール アプリケーション。</p> <p>他のタイプのユーザー活動の場合、このフィールドは空白です。</p>	はい	非対応	はい

## ■ ユーザー関連フィールド

フィールド	説明	[アクティブなセッション (Active Sessions) ] テーブル	[ユーザーテーブル (Users Table) ]	[ユーザーアクティビティ (User Activity) ] テーブル
<b>VPN クライアントの国 (VPN Client Country)</b>	リモートアクセス VPN の報告によるユーザーアクティビティの場合は、セキュアクライアント VPN クライアントによって報告された国名。 他のタイプのユーザーアクティビティの場合、このフィールドは空白です。	いいえ	非対応	はい
<b>VPN クライアントの OS (VPN Client OS)</b>	リモートアクセス VPN の報告によるユーザーアクティビティの場合は、セキュアクライアント VPN によって報告されたリモートユーザーのエンドポイントオペレーティングシステム。 他のタイプのユーザーアクティビティの場合、このフィールドは空白です。	はい	非対応	はい
<b>VPN クライアントのパブリック IP (VPN Client Public IP)</b>	リモートアクセス VPN の報告によるユーザーアクティビティの場合は、セキュアクライアント VPN デバイスのパブリックルーティング可能な IP アドレス。 他のタイプのユーザーアクティビティの場合、このフィールドは空白です。	はい	非対応	はい
<b>VPN 接続期間 (VPN Connection Duration)</b>	リモートアクセス VPN の報告によるユーザーアクティビティの場合は、セッションがアクティブだった合計時間 (HH:MM:SS)。 他のタイプのユーザーアクティビティの場合、このフィールドは空白です。	いいえ	非対応	はい
<b>VPN 接続プロファイル (VPN Connection Profile)</b>	リモートアクセス VPN の報告によるユーザーアクティビティの場合は、VPN セッションで使用される接続プロファイル (トンネルグループ) の名前。接続プロファイルは、リモートアクセス VPN ポリシーに含まれます。 他のタイプのユーザーアクティビティの場合、このフィールドは空白です。	はい	非対応	はい

フィールド	説明	[アクティブなセッション (Active Sessions) ] テーブル	[ユーザー テーブル (Users Table) ]	[ユーザー アクティビティ (User Activity) ] テーブル
VPN グループ ポリシー (VPN Group Policy)	<p>リモートアクセス VPN の報告によるユーザー アクティビティの場合は、VPN セッションが確立されたときにクライアントに割り当てられたグループ ポリシーの名前。これは VPN 接続プロファイルに関連付けられた静的に割り当てられたグループ ポリシー、または RADIUS が認証に使用されている場合は動的に割り当てられたグループ ポリシーです。RADIUS サーバーによって割り当てられている場合、このグループ ポリシーは VPN 接続プロファイル用に設定された静的ポリシーよりも優先されます。グループ ポリシーは、リモートアクセス VPN ポリシーのユーザー グループに共通の属性を設定します。</p> <p>他のタイプのユーザー アクティビティの場合、このフィールドは空白です。</p>	はい	非対応	はい
VPN セッション タイプ (VPN Session Type)	<p>リモートアクセス VPN の報告によるユーザー アクティビティの場合は、セッションのタイプ ([LAN 間 (LAN-to-LAN)] または [リモート (Remote)])。</p> <p>他のタイプのユーザー アクティビティの場合、このフィールドは空白です。</p>	はい	非対応	はい

## アクティブ セッション データ

[分析 (Analysis)] > [ユーザ (Users)] > [アクティブなセッション (Active Sessions)] ワークフローには、現在のユーザ セッションに関する選択情報が表示されます。ネットワーク上のユーザーが複数のセッションを同時に実行するとき、Firepower システムは次の場合にセッションを一意に識別できます。

- 一意の IP アドレス値を持っている。
- Cisco Terminal Services (TS) エージェントによって提供される、一意の開始ポート値と終了ポート値を持っている。
- 一意の現在の IP ドメイン値を持っている。
- 異なるアイデンティティ ソースによって認証された。
- 異なるアイデンティティ レルムと関連付けられた。

## ■ アクティブセッションデータの表示

システムによって保存されるユーザおよびユーザアクティビティデータの詳細については、[ユーザー データ \(User Data\) \(65 ページ\)](#) および [ユーザー アクティビティ データ \(68 ページ\)](#) を参照してください。

一般的なユーザー関連イベントのトラブルシューティングとリモートアクセス VPN のトラブルシューティングの詳細については、[Cisco Secure Firewall Management Center デバイス構成ガイド](#) の「*the Troubleshoot Realms and User Downloads*」および「*VPN Troubleshooting*」を参照してください。

### アクティブセッションデータの表示

アクティブセッションのテーブルを表示して、検索する情報に応じてイベントビューを操作することができます。

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。

ユーザーにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローを使用することができますが、これには、検出されたすべてのユーザーが記載されているユーザーのテーブルビューが含まれています。このワークフローは、ユーザーの詳細ページで終了します。ユーザーの詳細ページは、制約を満たす各ユーザーについての情報を提供します。

### 手順

---

#### ステップ1 次のように、ユーザー データにアクセスします。

- 事前定義されたワークフローを使用している場合は、[分析 (Analysis)] > [ユーザー (Users)] 見出し > [アクティブセッション (Active Sessions)] をクリックします。
- アクティブセッションのテーブルビューが含まれないカスタムワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow))] をクリックして [アクティブなセッション (Active Sessions)] を選択します。

#### ステップ2 次の選択肢があります。

- [(ワークフローの切り替え) ((switch workflow))] をクリックしてカスタムワークフローを含む別のワークフローを使用します。
- 基本的なワークフロー操作を実行します ([ディスカバリおよびアイデンティティワークフローの使用 \(7 ページ\)](#) を参照)。
- テーブルのカラムの内容について詳しく調べるには、[アクティブセッションデータ \(63 ページ\)](#) および [ユーザー関連フィールド \(53 ページ\)](#) を参照してください。

## ユーザー データ (User Data)

アイデンティティ ソースが、データベースに存在しないユーザーのユーザー ログインを報告した場合、そのログインタイプが特に制限されていない限り、そのユーザーはデータベースに追加されます。

次のいずれかが発生すると、システムはユーザー データベースを更新します。

- Firewall Management Center のユーザーが、[ユーザー (Users) ] テーブルから権限のないユーザーを手動で削除する。
- アイデンティティ ソースが、そのユーザーによるログオフを報告する。
- レルムがレルムの[ユーザー セッションのタイムアウト : 認証されたユーザー (User Session Timeout: Authenticated Users) ] 設定、[ユーザー セッションのタイムアウト : 認証に失敗したユーザー (User Session Timeout: Failed Authentication Users) ] 設定、または [ユーザー セッションのタイムアウト : ゲストユーザー (User Session Timeout: Guest Users) ] 設定で指定されているユーザー セッションを終了した。



(注) ISE/ISE-PIC が設定されている場合は、ユーザー テーブルにホストデータが表示されることがあります。ISE/ISE-PIC によるホスト検出は完全にはサポートされていないため、ISE が報告したホスト データを使用してユーザー 制御を実行することはできません。

システムによって検出されたユーザー ログインのタイプに応じて、新しいユーザーのどの情報が保存されるかが決まります。

ID ソース	ログイン タイプ	格納されるユーザー データ
ISE/ISE-PIC	Active Directory LDAP RADIUS RSA	<ul style="list-style-type: none"> <li>ユーザー名</li> <li>現行の IP アドレス</li> <li>セキュリティ グループ タグ (SGT) (ISE-PIC ではサポートされていない)</li> <li>エンドポイントのプロファイル/デバイス タイプ (ISE-PIC ではサポートされていない)</li> <li>エンドポイントの場所/場所 IP (ISE-PIC ではサポートされていない)</li> <li>タイプ (LDAP)</li> </ul>

■ ユーザー データ (User Data)

ID ソース	ログインタイプ	格納されるユーザー データ
TS エージェント	Active Directory	<ul style="list-style-type: none"> <li>• ユーザー名</li> <li>• 現行の IP アドレス</li> <li>• 開始ポート</li> <li>• 終了ポート</li> <li>• タイプ (LDAP)</li> </ul>
キャプティブ ポータル	Active Directory LDAP	<ul style="list-style-type: none"> <li>• ユーザー名</li> <li>• 現行の IP アドレス</li> <li>• タイプ (LDAP)</li> </ul>
トラフィックベースの 検出	LDAP AIM Oracle SIP HTTP FTP MDNS	<ul style="list-style-type: none"> <li>• ユーザー名</li> <li>• 現行の IP アドレス</li> <li>• タイプ (AD)</li> </ul>
	POP3 IMAP	<ul style="list-style-type: none"> <li>• ユーザー名</li> <li>• 現行の IP アドレス</li> <li>• 電子メール アドレス</li> <li>• タイプ (pop3 または imap)</li> </ul>



(注) このテーブルには、Microsoft Azure Active Directory ユーザーに関するデータは表示されません。

ユーザーを自動的にダウンロードするようにレルムを設定すると、Firewall Management Center は指定した間隔に基づいてサーバーに対するクエリを実行します。システムが新しいユーザーのログインを検出してから、Firewall Management Center データベースがユーザーのメタデータを更新するまでに、5~10 分かかることがあります。Firewall Management Center は、ユーザーごとに次の情報とメタデータを取得します。

- ユーザー名
- 姓と名

- 電子メール アドレス
- 部門
- 電話番号
- 現行の IP アドレス
- セキュリティ グループ タグ (SGT) (使用可能な場合)
- エンドポイントのプロファイル (使用可能な場合)
- エンドポイントの場所 (使用可能な場合)
- 開始ポート (使用可能な場合)
- 終了ポート (使用可能な場合)

Firewall Management Center がデータベースに格納できるユーザーの数は、Firewall Management Center のモデルによって異なります。ホストに対して権限を持たないユーザーがログインしていることが検出された場合、そのログインはユーザーおよびホストの履歴に記録されます。権限のあるユーザーがホストに関連付けられていない場合、権限のないユーザーがそのホストの現行ユーザーとなることができます。ただし、ホストに対して権限を持つユーザーのログインが検出された後は、権限を持つ別のユーザーがログインした場合にのみ、現行ユーザーが変わります。

AIM、Oracle、および SIP のログインがトラフィックベースで検出された場合は、システムが LDAP サーバーから取得したどのユーザー メタデータにも関連付けられないため、これらのログインにより重複したユーザー レコードが作成されることに注意してください。これらのプロトコルから重複したユーザー レコードを取得することに起因するユーザー カウントの過度な使用を回避するには、これらのプロトコルを無視するようにトラフィックベースの検出を設定します。

データベースからユーザーを検索、表示、削除することができます。また、データベースからすべてのユーザーを消去することもできます。

一般的なユーザー関連のイベントトラブルシューティングについては、[Cisco Secure Firewall Management Center デバイス構成ガイド](#) を参照してください。

## ユーザー データの表示

ユーザーのテーブルを表示して、検索する情報に応じてイベント ビューを操作することができます。

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。

ユーザーにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローを使用することができますが、これには、検出されたすべてのユーザーが記載されているユーザーのテーブル ビューが含まれています。このワークフローは、ユーザーの詳細ページで終了します。ユーザーの詳細ページは、制約を満たす各ユーザーについての情報を提供します。

## 手順

---

**ステップ1** 次のように、ユーザー データにアクセスします。

- ・事前定義されたワークフローを使用する場合は、[分析 (Analysis)]>[ユーザー (Users)]>[ユーザー (Users)]を選択します。
- ・ユーザーのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow))]をクリックして[ユーザー (Users)]を選択します。

**ステップ2** 次の選択肢があります。

- ・[(ワークフローの切り替え) ((switch workflow))]をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
  - ・基本的なワークフロー操作を実行します ([ディスカバリおよびアイデンティティワークフローの使用 \(7 ページ\)](#) を参照)。
  - ・テーブルのカラムの内容について詳しく調べます ([ユーザー関連フィールド \(53 ページ\)](#) を参照)。
- 

## ユーザー アクティビティ データ

システムは、ネットワーク上のユーザーアクティビティの詳細を伝達するイベントを生成します。システムがユーザーアクティビティを検出すると、そのユーザーアクティビティデータはデータベースに記録されます。ユーザーアクティビティは、表示、検索、および削除することも、すべてのユーザーアクティビティをデータベースから消去することもできます。

あるユーザがネットワーク上で初めて確認されると、システムはそのユーザーアクティビティイベントをログに記録します。そのユーザがその後に確認された場合、新しいユーザーアクティビティイベントはログに記録されません。ただし、そのユーザのIPアドレスが変わった場合、システムは新しいユーザーアクティビティイベントをログに記録します。

システムは、ユーザーアクティビティと他のタイプのイベントとの関連付けも行います。たとえば、侵入イベントは、そのイベントの発生時に送信元ホストと宛先ホストにログインしていたユーザを通知することができます。この関連付けにより、攻撃の対象になったホストにログインしていたユーザ、または内部攻撃やポートスキャンを開始したユーザがわかります。

ユーザーアクティビティは、相関ルールで使用することもできます。相関ルールは、ユーザーアクティビティのタイプだけでなく、指定した他の条件に基づいて作成することができます。相関ルールが相関ポリシーで使用される場合、ネットワーク トラフィックが条件を満たしたときは、相関ルールが修復およびアラートの応答を起動します。



(注) ISE/ISE-PIC が設定されている場合は、ユーザー テーブルにホストデータが表示されることがあります。ISE/ISE-PIC によるホスト検出は完全にはサポートされていないため、ISE が報告したホストデータを使用してユーザー制御を実行することはできません。

次に、4 つのタイプのユーザ アクティビティ データについて説明します。

#### 新しいユーザのアイデンティティ (New User Identity)

このタイプのイベントは、システムがデータベースに存在しない不明なユーザによるログインを検出したときに生成されます。

あるユーザがネットワーク上で初めて確認されると、システムはそのユーザ アクティビティ イベントをログに記録します。そのユーザがその後に確認された場合、新しいユーザ アクティビティ イベントはログに記録されません。ただし、そのユーザの IP アドレスが変わった場合、システムは新しいユーザ アクティビティ イベントをログに記録します。

#### ユーザ ログイン (User Login)

このタイプのイベントは、次のことが発生した後に生成されます。

- キャプティブ ポータルのユーザー認証の実行が成功または失敗した。
- トライフィック ベースの検出がユーザ ログインの成功または失敗を検出した。



(注) トライフィック ベースの検出で検出された SMTP ログインは、一致する電子メール アドレスを持つユーザがデータベースにすでに存在する場合を除いて記録されません。

権限のないユーザーがあるホストにログインすると、そのログインはユーザーとホストの履歴に記録されます。権限のあるユーザーがホストに関連付けられていない場合、権限のないユーザーがそのホストの現行ユーザーとなることが可能です。ただし、権限のあるユーザーがホストにログインした後は、権限のある別のユーザーがログインした場合のみ、現行ユーザーが変わります。

キャプティブ ポータルまたはトライフィック ベースの検出を使用する場合、失敗したユーザ ログインと失敗したユーザ認証データについて、次の点に注意してください。

- トライフィック ベースの検出 (LDAP、IMAP、FTP、および POP3 トライフィック) から報告された失敗したログインは、ユーザ アクティビティ のテーブル ビューに表示されますが、ユーザのテーブル ビューには表示されません。既知のユーザがログインに失敗した場合、システムではそのユーザをそのユーザ名で識別します。不明なユーザがログインに失敗した場合、システムではそのユーザ名として [失敗した認証 (Failed Authentication)] を使用します。
- キャプティブ ポータルから報告された失敗した認証は、ユーザ アクティビティ のテーブル ビューとユーザのテーブル ビューの両方に表示されます。既知のユーザが認証に失敗

## ■ ユーザー アクティビティ データの表示

した場合、システムではそのユーザをそのユーザ名で識別します。不明なユーザが認証に失敗した場合、システムではそのユーザをそのユーザが入力したユーザ名で識別します。

### ユーザのアイデンティティの削除（Delete User Identity）

このタイプのイベントは、データベースからユーザを手動で削除したときに生成されます。

#### ドロップ（廃棄）されたユーザのアイデンティティ：ユーザ制限に到達（UserIdentity Dropped: User Limit Reached）

このタイプのイベントは、システムがデータベースに存在しないユーザを検出したものの、Firewall Management Center のモデルで決定されているデータベースの最大ユーザ数に達したためにユーザを追加できなかったときに生成されます。

ユーザー制限に達すると、ほとんどの場合、データベースへの新しいユーザーの追加が停止されます。新しいユーザーを追加するには、古いユーザーまたは非アクティブなユーザーをデータベースから手動で削除するか、データベースからすべてのユーザーを消去する必要があります。

ただし、システムでは権限のあるユーザが優先されます。すでに制限に達しており、これまでに検出されていない権限のあるユーザのログインが検出された場合、システムは長期間非アクティブな状態が続いている権限のないユーザを削除して、権限のある新しいユーザに置き換えます。

### ユーザの侵害の兆候イベント

次のユーザの IOC の変化がユーザ アクティビティ データベースに記録されます。

- 侵害の兆候が解決された場合。
- 侵害の兆候ルールがユーザーに対して有効または無効にされた場合。

一般的なユーザー関連のイベント トラブルシューティングについては、Cisco Secure Firewall Management Center デバイス構成ガイドを参照してください。

## ■ ユーザー アクティビティ データの表示

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。

ユーザー アクティビティのテーブルを表示して、検索する情報に応じてイベント ビューを操作することができます。ユーザー アクティビティにアクセスするときに表示されるページは、使用するワークフローによって異なります。事前定義のワークフローを使用することができます。このワークフローにはユーザー アクティビティのテーブル ビューが含まれており、制約を満たすすべてのユーザーの詳細が含まれている、ユーザーの詳細ページで終了します。また、特定のニーズを満たす情報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。

## 手順

---

**ステップ1** 次のように、ユーザー アクティビティ データにアクセスします。

- 事前定義されたワークフローを使用する場合、[分析 (Analysis)] > [ユーザー (Users)] 見出し > [ユーザー アクティビティ (User Activity)] を選択します。
- ユーザー アクティビティのテーブル ビューが含まれないカスタム ワークフローを使用している場合は、[(ワークフローの切り替え) ((switch workflow))] をクリックして [ユーザー アクティビティ (User Activity)] を選択します。

### ヒント

イベントが表示されない場合は、時間範囲の調整が必要な可能性があります ([時間枠の変更を参照](#))。

**ステップ2** 次の選択肢があります。

- [(ワークフローの切り替え) ((switch workflow))] をクリックしてカスタム ワークフローを含む別のワークフローを使用します。
  - 基本的なワークフロー操作を実行します ([ディスカバリおよびアイデンティティ ワークフローの使用 \(7 ページ\)](#) を参照)。
  - テーブルのカラムの内容について詳しく調べます ([ユーザー関連フィールド \(53 ページ\)](#) を参照)。
- 

## ユーザー プロファイルとホスト履歴

特定のユーザーの詳細については、[ユーザー (User)] ポップアップ ウィンドウを表示して確認することができます。表示されるページ（このマニュアルでは「ユーザプロファイル」と呼んでいます）には、Web インターフェイスで「ユーザのアイデンティティ (User Identity)」というタイトルが付いています。

このウィンドウは、次のビューから表示できます。

- ユーザー データを他の種類のイベントに関連付けるすべてのイベント ビュー
- アクティブなセッションのテーブル ビュー
- ユーザーのテーブル ビュー

ユーザ情報は、ユーザ ワークフローの最終ページにも表示されます。

表示されるユーザー データは、ユーザーのテーブル ビューで表示されるものと同じです。

### [侵害の兆候 (Indications of Compromise) ] セクション

このセクションについては、次のセクションを参照してください。

- [Cisco Secure Firewall Management Center デバイス構成ガイド](#) の「*Indications of Compromise*」

## ■ ユーザの詳細およびホスト履歴の表示

- [侵害の兆候データ フィールド \(33 ページ\)](#)
- [単一ホストまたはユーザにおける侵害の兆候のルール状態の編集 \(33 ページ\)](#)
- [侵害の兆候タグの解決 \(34 ページ\)](#)
- [侵害の兆候のタグのソース イベントの表示 \(34 ページ\)](#)

### [ホストの履歴 (Host History) ] セクション

ホストの履歴には、過去 24 時間のユーザ アクティビティがグラフィック表示されます。ユーザーがログインおよびログオフしたホストの IP アドレスのリストには、ログインとログアウトの概算時間が棒グラフで示されます。一般的なユーザは、1 日の間に複数のホストに対してログオンおよびログオフする可能性があります。たとえば、メールサーバに対する定期的な自動ログインは複数回の短時間のセッションとして示されますが、(勤務時間中などの) 長時間のログインは、長時間のセッションとして示されます。

トライフィック ベースの検出またはキャプティブ ポータルを使用して失敗したログインをキャプチャした場合、ホストの履歴にはユーザがログインに失敗したホストも含まれます。

ホストの履歴を生成するために使用されるデータは、ユーザの履歴データベースに格納されます。このデータベースには、デフォルトで 1000 万のユーザ ログインイベントが格納されます。ホストの履歴に特定のユーザーに関するデータが表示されない場合、そのユーザーが非アクティブであるか、またはデータベースの制限を増やすなければならないことがあります。

#### 関連トピック

- [ユーザー データのフィールド](#)

## ユーザの詳細およびホスト履歴の表示

### 手順

---

以下の 2 つの対処法があります。

- ユーザーをリストする任意のイベントビューで、ユーザー ID のユーザーアイコン、または、侵入の痕跡に関連付けられているユーザーの場合は赤色のユーザーアイコンの横に表示されるユーザーをクリックします。
  - いずれかのユーザ ワークフローで、[ユーザ (Users) ] の最終ページをクリックします。
-

# 検出イベントの操作の履歴

表 2:

機能	最小 Firewall Management Center	最小 Firewall Threat Defense	詳細
脆弱性ページの変更	6.7	いずれか	<p>Bugtraq とその脆弱性データは使用できなくなりました。次の変更が行われました。</p> <ul style="list-style-type: none"> <li>現在、ほとんどの脆弱性データは National Vulnerability Database (NVD) から取得されています。</li> <li>廃止された冗長なフィールドが削除されました。</li> <li>新しい [CVE ID] 列がテーブルビューに追加され、新しい [シビラティ (重大度) (Severity) ] フィールドがテーブルと詳細のページに追加されました。</li> <li>テーブルで CVE ID を右クリックすると、NVD のその脆弱性に関する詳細を表示できるようになりました。</li> <li>テーブルの [脆弱性の影響 (Vulnerability Impact) ] 列の名前が [影響 (Impact) ] に変更されました。（詳細ビューのフィールド名は変更されていません。）</li> <li>[分析 (Analysis) ] &gt; [ホスト (Hosts) ] &gt; [ネットワークマップ (Network Map) ] &gt; [ホスト (Hosts) ] でホストプロファイルの脆弱性を表示するときに、脆弱性の詳細（サードパーティの脆弱性を除く）により新しい一連のフィールドが使用されます。</li> <li>[分析 (Analysis) ] &gt; [ホスト (Hosts) ] &gt; [ネットワークマップ (Network Map) ] &gt; [脆弱性 (Vulnerabilities) ] ページの [脆弱性 (Vulnerabilities) ] オプションから、[Bugtraq] オプションが削除されました。</li> </ul> <p>変更された画面：</p> <ul style="list-style-type: none"> <li>[分析 (Analysis) ] &gt; [ホスト (Hosts) ] &gt; [脆弱性 (Vulnerabilities) ] の下のすべてのページ</li> <li>[分析 (Analysis) ] &gt; [ホスト (Hosts) ] &gt; [ネットワークマップ (Network Map) ] ページの [ホスト (Hosts) ] タブと [脆弱性 (Vulnerabilities) ] タブ</li> </ul> <p>サポート対象プラットフォーム：Firewall Management Center</p>

## ■ 検出イベントの操作の履歴

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。