CHAPTER 50

ディスカバリ イベントの使用

ディスカバリ(検出)イベントは、ユーザにネットワーク上のアクティビティを警戒するよう警告し、適切に対応する必要がある情報を提供します。これらのイベントは、管理対象デバイスが監視しているネットワーク セグメント内で、管理対象デバイスが検出する変更によってトリガーされます。*ネットワーク検出ポリシー*は、システムが収集するデータの種類、監視対象ネットワーク セグメント、およびシステムがトラフィックの監視で使用する特定のハードウェア インターフェイスについて明記しています。ネットワーク検出の詳細については、検出データ収集について(45-2 ページ)を参照してください。

ディスカバリ イベントの簡単な例として、会議室または予備の作業空間があり、そこへ来た従業員がネットワークにアクセスする場合があります。ユーザはこれらのセグメントで生成される New Host イベントを定期的に見ることが予想されますが、悪意のある行為だとは疑わないでしょう。ただし、ロック ダウンしたネットワーク セグメントで New Host イベントが見つかった場合は、それに応じて、応答のエスカレーションを行うことができます。

ユーザ ディスカバリ イベントは、ネットワーク上のホストにログインしているユーザに関する情報を提供します。ユーザは、ネットワーク上のユーザ アクティビティをカタログしているイベントを表示してドリル ダウンし、特定のユーザの情報を表示することができます。たとえば、新しいホストに関連付けられているユーザを表示する場合は、ホスト プロファイルを確認し、対象のホストとやりとりしているトラフィックで検出されたのがどのユーザかを特定することができます。

ディスカバリ イベントは、このような簡単な例に比べて、ネットワーク上のアクティビティを知るうえではるかに詳しく、精度の高い情報を提供します。監視されている各ホストについて、関連するアプリケーション プロトコル、ネットワーク プロトコル、クライアント、ユーザ、および潜在的な脆弱性を検出するようシステムを設定することができます。システムは、ユーザがホスト入力機能を使用して Defense Center にインポートしたサードパーティのスキャナで検出された脆弱性についても情報を提供することができます。侵入の痕跡(IOC)は侵入、マルウェア、および他のデータを使用して、セキュリティが侵害される可能性があるホストを特定します。またユーザは、ユーザ インターフェイスを介して入力するホストの重要度、ホスト属性、脆弱性の設定における何らかの変更を追跡できます。

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ディスカバリ イベントを分析することができます。また、特定のニーズにあ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データを収集および格納するには、Cisco の管理対象デバイスおよび NetFlow 対応デバイスがトラフィックを監視するネットワークおよびゾーンで適切なデータを検出するように、ネットワーク検出ポリシーを設定する必要があります。監視対象領域をディスカバリの範囲から除外するには、ネットワーク検出ポリシーで設定します。ネットワーク検出ポリシーを適用する前に、アクセス コントロール ポリシーを管理対象デバイスに適用する必要があります。詳細については、ネットワーク検出ポリシーの作成(45-25 ページ)を参照してください。

詳細については、以下を参照してください。

ディスカバリ イベントの統計情報の表示

ライセンス：FireSIGHT

[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、およびオペレーティング システムの概要が表示されます。

- 統計情報の概要は、イベントの合計、アプリケーション プロトコル、ホスト、ネットワーク デバイス、およびホストの使用制限に関する全般的な情報を提供します。統計情報のサマリ（50-3 ページ）を参照してください。
- イベントの明細には、システムで発生しているイベントのタイプに関する統計情報が示されます。イベント分類（Event Breakdown）（50-4 ページ）を参照してください。
- プロトコルの明細には、検出されたホストで使用しているプロトコルに関する統計情報が示されます。プロトコル分類（Protocol Breakdown）（50-5 ページ）を参照してください。
- アプリケーション プロトコルの明細には、ネットワーク上で稼働しているアプリケーション プロトコルの統計情報が示されます。アプリケーション プロトコル分類（Application Protocol Breakdown）（50-5 ページ）を参照してください。
- オペレーティング システムの明細には、ネットワーク上で稼働しているオペレーティング システムについて、およびそれぞれのオペレーティング システムを何台のホストが使用しているかが示されます。OS 分類（OS Breakdown）（50-5 ページ）を参照してください。

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選択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、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。

ディスカバリ統計情報サマリを表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

手順 1　[概要（Overview）] > [サマリ（Summary）] > [ディスカバリ統計情報（Discovery Statistics）] を選択します。

統計情報のサマリ ページが表示されます。

手順 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。Defense 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。

統計情報のサマリ

ライセンス：FireSIGHT

統計情報の概要は、イベントの合計、アプリケーション プロトコル、ホスト、ネットワーク デバイス、およびホストの使用制限に関する全般的な情報を提供します。

[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）

Defense 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 ホスト合計数（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

ホストの使用制限（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、FireSIGHT のライセンス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。モニタリングしているホストの使用についての詳細は、FireSIGHT ホスト使用量モニタリングの設定（68-18 ページ）を参照してください。

（注）　ホストの制限に達して、あるホストが削除された場合、ディスカバリを実行するよう設定されたすべての管理対象デバイスでネットワーク検出を再開するまで、ホストはネットワーク マップに表示されません。

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。

最後に受け取った接続（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）

ライセンス：FireSIGHT

[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。各イベント タイプの詳細な説明については、ディスカバリ イベントのタイプについて（50-10 ページ）およびホスト入力イベントのタイプについて（50-14 ページ）を参照してください。

[イベント分類（Event Breakdown）] セクションを使用して、ディスカバリ（検出）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。

ネットワーク検出イベントおよびホスト入力イベントをタイプごとに表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

手順 1　表示するイベントのタイプをクリックします。

デフォルトのディスカバリ イベント ワークフローの最初のページが、選択したイベント タイプによって制約されて表示されます。カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [ワークフロー切り替え（switch workflow）] をクリックします。別のデフォルト ワークフローの指定方法については、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。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。イベント時間の制約の設定（58-27 ページ）を参照してください。

ディスカバリ（検出）イベントの使用については、ディスカバリ イベントとホスト入力イベントの使用（50-9 ページ）を参照してください。

プロトコル分類（Protocol Breakdown）

ライセンス：FireSIGHT

[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。このセクションでは、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を表示します。

アプリケーション プロトコル分類（Application Protocol Breakdown）

ライセンス：FireSIGHT

[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。このセクションでは、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を表示します。

また [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、検出されたプロトコルを使用しているサーバの詳細を表示することもできます。

リストされたアプリケーション プロトコルを使用しているサーバを表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

手順 1　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。

デフォルトのサーバ ワークフローの最初のページが、選択したアプリケーション プロトコルによって制約されて表示されます。カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [ワークフロー切り替え（switch workflow）] をクリックします。別のデフォルト ワークフローの指定方法については、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。

サーバの使用については、サーバの使用（50-39 ページ）を参照してください。

OS 分類（OS Breakdown）

ライセンス：FireSIGHT

[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働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。

オペレーティング システムまたはベンダーによってホストを表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

手順 1　以下の 2 つの対処法があります。

- 特定のオペレーティング システムを実行しているすべてのホストを表示するには、[OS 名（OS Name）] の下でオペレーティング システムの名前をクリックします。
- 特定のベンダーからいずれかのオペレーティング システムを実行しているすべてのホストを表示するには、[OS ベンダー（OS Vendor）] の下でベンダーの名前をクリックします。

デフォルトのホスト ワークフローの最初のページが、選択したオペレーティング システムまたはベンダーによって制約されて表示されます。カスタム ワークフローなど、別のワークフローを使用するには、ワークフローのタイトルの横の [ワークフロー切り替え（switch workflow）] をクリックします。別のデフォルト ワークフローの指定方法については、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。

ホストの使用については、ホストの使用（50-21 ページ）を参照してください。

ディスカバリのパフォーマンス グラフの表示

ライセンス：FireSIGHT

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。

（注）　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、グラフをすぐにリロードしても、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。

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/秒（Processed Events/Sec）

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/秒（Processed Connections/Sec）

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/秒（Generated Events/Sec）

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（Mbits/Sec）

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（Avg Bytes/Packet）

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（K Packets/Sec）

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。

ディスカバリのパフォーマンス グラフを生成するには、以下を行います。

アクセス：Admin/Maint

手順 1　[概要（Overview）] > [サマリ（Summary）] > [ディスカバリのパフォーマンス（Discovery Performance）] を選択します。

[ディスカバリのパフォーマンス（Discovery Performance）] ページが表示されます。

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

[グラフの選択（Select Graph(s)）] リストでは、選択するアプライアンスによって、使用できるグラフの表示が変わります。

手順 3　[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。

ヒント　Ctrl キーまたは Shift キーを押しながらグラフのタイプをクリックすると、複数のグラフを選択できます。

手順 4　[時間帯の選択（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。過去 1 時間、前日、先週、または先月から選択できます。

手順 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。

選択したグラフが表示されます。

ディスカバリ イベントのワークフローについて

ライセンス：FireSIGHT

Defense Center は、ネットワークで生成されるディスカバリ イベントの分析で使用できるワークフロー 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。これらのワークフローには、システムによって生成された検出（ディスカバリ）データが挿入されたテーブルが含まれています。

[分析（Analysis）] > [ホスト（Hosts）] メニューから、ネットワークのディスカバリ ワークフローにアクセスします。Defense Center には、検出されたホストとそのホストの属性、サーバ、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 アクティビティ、およびユーザのワークフローだけでなく、ディスカバリ イベントの事前定義のワークフローが用意されています。ユーザはカスタム ワークフローを作成することもできます。ワークフローの詳細については、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。

ヒント　[分析（Analysis）] > [カスタム（Custom）] > [カスタム テーブル（Custom Tables）] を選択して、カスタム テーブルに基づいたワークフローにアクセスします。

ネットワークのディスカバリ ワークフローを使用している場合は、イベントのタイプに関係なく、多数の一般的なアクションを実行できます。これらの一般的な機能については、一般的なディスカバリ イベントのアクションの表で説明します。

表 50-1　一般的なディスカバリ イベントのアクション

目的	操作
IP アドレスのホスト プロファイルを表示する	プロファイル アイコン( )をクリックするか、または侵入の痕跡(IOC)タグがアクティブになっているホストで、IP アドレスの隣に示されている侵害されているホストのアイコン( )をクリックします。IOC については、侵入の痕跡の使用(50-35 ページ)を参照してください。
ユーザ プロファイル情報を表示する	ユーザ ID の隣に表示されているユーザ アイコン( )をクリックします。詳細については、ユーザの詳細とホストの履歴について(50-68 ページ)を参照してください。
データをソートする	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。
ワークフロー内の次のページにドリルダウンする	次のいずれかの方法を使用します。 • 特定の値に制限して、次のワークフロー ページにドリルダウンするには、行内の値をクリックします。この操作はドリルダウン ページでのみ可能です。テーブルの行内の値をクリックしても、テーブル ビューが制約されるだけで、次のページにはドリル ダウンしません。 • いくつかのイベントによって制約したまま次のワークフロー ページにドリルダウンするには、次のワークフロー ページに表示するイベントの横のチェックボックスを選択し、[表示(View)] をクリックします。 • 現在の制限を維持して次のワークフロー ページにドリルダウンするには、[すべて表示(View All)] をクリックします。 ヒント　テーブル ビューでは、必ずページ名に「Table View」が含まれます。 詳細については、イベントの制約(58-35 ページ)を参照してください。
表示されるカラムの制約	非表示にするカラムの見出しで、クローズ アイコン( )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、対象のチェック ボックスをオンまたはオフにします。無効にしたカラム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展開し、[無効になったカラム(Disabled Columns)] の下のカラム名をクリックします。
現在のワークフロー ページ内で移動する	ワークフロー内の他のページへのナビゲート(58-40 ページ)で詳細を参照してください。
現在の制限を維持して、現在のワークフロー内のページ間を移動する	ワークフロー ページの左上で、該当するページ リンクをクリックします。詳細については、ワークフローのページの使用(58-21 ページ)を参照してください。

表 50-1　一般的なディスカバリ イベントのアクション(続き)

目的	操作
以下のアイテムをシステムから削除する • ディスカバリ イベント ワークフローからディスカバリ イベントおよびホスト入力イベントを削除する • ホスト ワークフローからホスト デバイスおよびネットワーク デバイスを削除する • ホスト属性のワークフローからホスト属性を削除する • サーバ ワークフローからサーバを削除する • アプリケーション ワークフローからアプリケーションを削除する • サードパーティ脆弱性ワークフローからサードパーティの脆弱性を削除する • ユーザ ワークフローからユーザを削除する	次のいずれかの方法を使用します。 • いくつかのアイテムを削除するには、削除するアイテムの隣にあるチェック ボックスをオンにして [削除(Delete)] をクリックします。 • 現行の制約されているビューのすべてのアイテムを削除するには、[すべて削除(Delete All)] をクリックして、すべてのアイテムを削除することを確認します。 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。 **ヒント**　データベースからすべてのディスカバリ イベントを削除する方法、およびディスカバリを再開する方法については、データベースからの検出データの消去(B-1 ページ)を参照してください。 サードパーティの場合とは異なり、Ciscoの脆弱性は削除**できない**ことに注意してください。ただし、確認済みとしてマークすることはできます。詳細については、脆弱性の処理(50-54 ページ)を参照してください。
他のイベント ビューに移動して関連イベントを表示する	ワークフロー間のナビゲート(58-41 ページ)で詳細を参照してください。

ディスカバリ イベントとホスト入力イベントの使用

ライセンス: FireSIGHT

システムはディスカバリ(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とりします。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資産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働が検出された 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、NetFlow 対応のデバイスでエクスポートされたデータ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働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。NetFlow 対応のデバイスが含まれるように設定したディスカバリ ルールを作成する場合は、アプリケーション プロトコルの検出を無効にすることができます。ただし、設定された NetFlow 対応のデバイスを使用しないディスカバリ ルールでは、アプリケーションの検出を無効にすることはできません。NetFlow 以外のディスカバリ 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、以前に検出された資産の設定が変更されるたびに生成されます。

ディスカバリ イベントが生成されると、データベースに記録されます。Defense Center の Web インターフェイスを使用して、ディスカバリ イベントを表示、検索、および削除することができます。また、相関ルールでディスカバリ 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、生成されるディスカバリ イベントのタイプに基づいて、相関ルールを作成することができます。相関ルールは相関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。

詳細については、次の各項を参照してください。

- ディスカバリ イベントのタイプについて（50-10 ページ）
- ホスト入力イベントのタイプについて（50-14 ページ）
- ディスカバリ イベントおよびホスト入力イベントの表示（50-16 ページ）
- ディスカバリ イベント テーブルについて（50-17 ページ）
- ディスカバリ イベントの検索（50-18 ページ）

ディスカバリ イベントのタイプについて

ライセンス：FireSIGHT

ディスカバリ イベントには多数のタイプがあります。たとえば、監視対象ネットワーク セグメントで新しいホストが検出された場合、システムは New Host イベントを生成し、記録します。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。詳細については、ディスカバリ イベントおよびホスト入力イベントの表示（50-16 ページ）を参照してください。

監視対象ネットワークでシステムが変更を検出した（以前に検出されなかったホストからトラフィックが検出されたなど）ときに生成されるディスカバリ イベントとは異なり、ホスト入力イベントは、ユーザが特別なアクションを実行した（手動でホストを追加するなど）ときに生成されます。ホスト入力イベントの詳細については、ホスト入力イベントのタイプについて（50-14 ページ）を参照してください。

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ディスカバリ イベントのタイプを設定できます。デフォルトでは、システムですべてのタイプのディスカバリ イベントが記録されます。詳細については、データベース イベント制限の設定（63-16 ページ）を参照してください。

さまざまなタイプのディスカバリ 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、ディスカバリ イベントのさまざまな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。

ホップ数の変更

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。

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に、このような状況が発生することがあります。また、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に、このような状況が発生することもあります。

ホスト削除：ホスト制限に到達

このイベントは、Defense Center 上でホストの制限を超えて、Defense Center 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。

ホストのドロップ：ホスト制限に到達

このイベントは、Defense 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）] > [詳細設定（Advanced）] を選択し、[ホスト制限に到達したとき（When Host Limit Reached）] を [ホストをドロップ（Drop hosts）] に設定します。詳細については、データ保存の設定（45-39 ページ）を参照してください。

ホスト IOC 設定

このイベントは、ホストに対して IOC（侵入の痕跡/兆候）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。ホストのタイムアウト値の設定については、データ保存の設定（45-39 ページ）を参照してください。

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 FireSIGHT のライセンスに不利に作用しないようにします。詳細については、ホストのネットワーク マップの操作（48-2 ページ）を参照してください。

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、アイデンティティ競合イベントを使用して Nmap の修復をトリガーできます。詳細については、Nmap 修復の設定（54-12 ページ）を参照してください。

詳細については、ID の競合について（46-7 ページ）および ID 競合解決の設定（45-36 ページ）を参照してください。手動による競合の解決については、オペレーティング システムのアイデンティティの競合を解決する（49-15 ページ）およびサーバ アイデンティティの競合の解決（49-22 ページ）を参照してください。

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を介してネットワーク マップに追加されたアイデンティティ データがタイムアウトになっ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には、アイデンティティ競合イベントを使用して Nmap の修復をトリガーできます。詳細については、Nmap 修復の設定（54-12 ページ）を参照してください。

詳細については、サーバ アイデンティティの競合の解決（49-22 ページ）を参照してください。

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 が変わる可能性があります。

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 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。詳細については、アプリケーション検出について（45-11 ページ）を参照してください。

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働している新しいホストを検出したときに生成されます。

NetFlow デバイスが選択されているネットワーク検出 ルールで [検出（Discover）] オプションを選択して [ホスト（Hosts）] を選択した場合、新しいホストに関係する NetFlow データをデバイスが処理したときにも、このイベントが生成されます。

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か、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。

新しい TCP ポート

このイベントは、新しい TCP サーバ 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の識別には使用されないことに注意してください。情報は、TCP Server Information Update イベントで伝送されます。

NetFlow データについて、ネットワーク検出 ルールで [検出（Discover）] オプションを選択して [アプリケーション（Applications）] を選択した場合、監視対象ネットワーク上のサーバに関連する NetFlow データで、ネットワーク マップにまだ存在しないデータをデバイスが処理したときにも、このイベントが生成されます。

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、ホスト上で稼働している新しい UDP サーバ ポートを検出したときに生成されます。

NetFlow データについて、ネットワーク検出 ルールで [検出（Discover）] オプションを選択して [アプリケーション（Applications）] を選択した場合、監視対象ネットワーク上のサーバに関連する NetFlow データで、ネットワーク マップにまだ存在しないデータをデバイスが処理したときにも、このイベントが生成されます。

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ったときに生成されます。サーバのタイムアウト値の設定については、データ保存の設定（45-39 ページ）を参照してください。

TCP サーバ情報の更新

このイベントは、ホスト上で稼働しており、すでに検出されている TCP サーバ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。サーバのタイムアウト値の設定については、データ保存の設定（45-39 ページ）を参照してください。

UDP サーバ情報の更新

このイベントは、ホスト上で稼働しており、すでに検出されている UDP サーバで、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。VLAN タグの詳細については、ホスト プロファイルでの VLAN タグの使用（49-24 ページ）を参照してください。

ホスト入力イベントのタイプについて

ライセンス：FireSIGHT

ホスト入力イベントには多数のタイプがあります。たとえば、ユーザがホスト インポート機能を使用してホストを追加すると、システムはホストの追加（Add Host）イベントを生成および記録します。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。詳細については、ディスカバリ イベントおよびホスト入力イベントの表示（50-16 ページ）を参照してください。

ユーザが（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。ホスト入力イベントの詳細については、ディスカバリ イベントのタイプについて（50-10 ページ）を参照してください。

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。デフォルトでは、システムですべてのタイプのホスト入力イベントが記録されます。詳細については、データベース イベント制限の設定（63-16 ページ）を参照してください。

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

このイベントは、ユーザ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

このイベントは、ユーザ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

このイベントは、ユーザがプロトコルを追加したときに生成されます。

スキャン結果の追加

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

このイベントは、ユーザがサーバ 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

このイベントは、ユーザ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

このイベントは、ユーザがシステムから 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

このイベントは、ユーザ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

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

ホスト属性の追加

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。

ホスト属性の削除

このイベントは、ユーザが、ユーザ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

このイベントは、ユーザが、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

このイベントは、ユーザ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。

ホスト属性の更新

このイベントは、ユーザが、ユーザ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

このイベントは、ユーザ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

このイベントは、ユーザ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。

サーバ定義の設定

このイベントは、ユーザがサーバ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。

脆弱性の影響の認定の設定

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

このイベントは、ユーザが 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

このイベントは、ユーザが、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。

ディスカバリ イベントおよびホスト入力イベントの表示

ライセンス：FireSIGHT

ディスカバリ イベントとホスト入力イベントは、[ディスカバリ イベント（Discovery Events）] ワークフローを使用して表示できます。ディスカバリ イベントは、アプライアンスに対して設定されているネットワーク検出ポリシーに基づいてネットワーク検出データの検出を記録します。ホスト入力イベントは、ホスト入力機能を介してホスト データの入力をネットワーク マップへ記録します。詳細については、ディスカバリ イベントのタイプについて（50-10 ページ）およびホスト入力イベントのタイプについて（50-14 ページ）を参照してください。

Defense Center を使用して、ディスカバリ イベントまたはホスト入力イベントのテーブルを表示することができます。ここでユーザは、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。

ユーザ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。カスタム ワークフローの作成方法については、カスタム ワークフローの作成（58-44 ページ）を参照してください。

ディスカバリ イベントのアクションの表で、ディスカバリ イベントのワークフロー ページで実行できる特定の操作について説明します。一般的なディスカバリ イベントのアクションの表に記載されているタスクも実行できます。

表 50-2　ディスカバリ イベントのアクション

目的	操作
表示されたイベントの時刻と日付の範囲を変更する	イベント時間の制約の設定（58-27 ページ）で詳細を参照してください。 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ることに注意してください。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。
テーブルのカラムの内容について詳しく調べる	ディスカバリ イベント テーブルについて（50-17 ページ）で詳細を参照してください。

ディスカバリ 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）] > [ホスト（Hosts）] > [ディスカバリ イベント（Discovery Events）] を選択します。

デフォルトのディスカバリ イベント ワークフローの最初のページが表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え（switch workflow）] をクリックします。別のデフォルト ワークフローの指定方法については、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。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。イベント時間の制約の設定（58-27 ページ）を参照してください。

ディスカバリ イベント テーブルについて

ライセンス：FireSIGHT

システムはディスカバリ（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とりします。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資産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、および各ホストで検出する 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。またシステムは、検出された各ホスト上で稼働しているネットワーク、トランスポート、またはアプリケーション 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。NetFlow 関連のトラフィックについては、ホストで稼働しているアプリケーション プロトコルをシステムが検出したときに、システムが新しいイベントを作成するかどうかを制御できます。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。以前に検出されたホスト、サーバ、またはクライアントの設定が変更されるたびに、変更イベントが生成されます。

次に、ディスカバリ イベント テーブルの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

イベントのタイプ。使用可能な各イベントの説明については、ディスカバリ イベントのタイプについて（50-10 ページ）およびホスト入力イベントのタイプについて（50-14 ページ）を参照してください。

[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（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。

Device

イベントを生成したデバイス名。NetFlow データに基づいた新しいホストおよび新しいサーバ イベントの場合、これは NetFlow データを処理したデバイスになります。

ディスカバリ イベントの検索

ライセンス：FireSIGHT

ユーザは特定のディスカバリ イベントを検索することができます。実際のネットワーク環境に合わせてカスタマイズされた検索を作成して保存すると、あとで再利用できます。

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。
- いくつかのフィールドでは、フィールドに `n/a` または `blank` を指定して、そのフィールドで情報を使用できないイベントを特定することができます。`!n/a` または `!blank` を使用して、フィールドに値が挿入されるイベントを特定することができます。
- ほとんどのフィールドでは大文字/小文字が区別されません。
- IP アドレスは CIDR 表記を使用して指定できます。
- 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。

ディスカバリ イベントの特別な検索構文

次の表に、特定のディスカバリ イベント フィールドに固有の検索情報について示します。ディスカバリ イベントのフィールドの詳細は、ホスト テーブルについて（50-22 ページ）を参照してください。

表 50-3　ディスカバリ イベントの検索条件のメモ

フィールド	検索条件のメモ
イベント	イベント名の対象は、ディスカバリ イベントのタイプについて（50-10 ページ）およびホスト入力イベントのタイプについて（50-14 ページ）に記載されています。
[MAC ベンダー（MAC Vendor）]	仮想 MAC ベンダー（つまり、仮想マシンが含まれているイベント）を検索するには、`virtual_mac_vendor` と入力します。 名前にカンマが含まれているベンダーを検索するには、検索語全体を引用符で囲みます。このようにしないと、Defense Center は検索語を 2 つの検索として扱い、それぞれの検索語に一致するイベントを返します。
[ポート（Port）]	注意すべき点として、次の処理は行うことはできません。 • 他の種類のイベントを検索するときと同じように、ポート/プロトコルの組み合わせを入力する • ポート番号または範囲を指定するときにスペースを使用する

ディスカバリ 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　テーブルのドロップダウン リストから [ディスカバリ イベント（Discovery 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　一般的な検索構文（50-18 ページ）およびディスカバリ イベントの特別な検索構文（50-19 ページ）に記載されているように、該当するフィールドに検索条件を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。オブジェクトを検索条件として使用するには、検索フィールドの隣にある追加アイコン（ ＋ ）をクリックします。

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、現行の時間範囲によって制約され、デフォルトのディスカバリ イベント ワークフローに表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え（switch workflow）] をクリックします。別のデフォルト ワークフローの指定方法については、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。

ホストの使用

ライセンス：FireSIGHT

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。Defense 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フィックのプロファイル、およびコンプライアンスのホワイト 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。そのあとで、相関ルールおよびポリシーの中でこれらの重要度の値、ホワイト 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。

NetFlow 対応デバイスによってエクスポートされたデータに基づきネットワーク マップにホストを追加するようネットワーク検出ポリシーを設定することはできますが、これらのホストに関して使用可能な情報は限られています。たとえば、これらのホストのオペレーティング システム データは得られません（ただしホスト入力機能を使って指定する場合を除く）。詳細については、NetFlow と FireSIGHT データの違い（45-19 ページ）を参照してください。

詳細については、次の項を参照してください。

- ホストの表示（50-21 ページ）
- ホスト テーブルについて（50-22 ページ）
- 選択したホストのトラフィック プロファイルの作成（50-26 ページ）
- 選択したホストに基づいたコンプライアンスのホワイト リストの作成（50-26 ページ）
- ホストの検索（50-27 ページ）
- 選択したホストのホスト属性の設定（50-32 ページ）

ホストの表示

ライセンス：FireSIGHT

Defense 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。その後、探している情報に応じて表示方法を操作できます。

ユーザ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、このホスト ビューには、ユーザ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。詳細については、カスタム ワークフローの作成（58-44 ページ）を参照してください。

ホスト アクションの表で、ホストのワークフロー ページで実行できる特定の操作について説明します。一般的なディスカバリ イベントのアクションの表に記載されているタスクも実行できます。

表 50-4　ホスト アクション

目的	操作
テーブルのカラムの内容について詳しく調べる	ホスト テーブルについて（50-22 ページ）で詳細を参照してください。
選択したホストにホスト属性を割り当てる	選択したホストのホスト属性の設定（50-32 ページ）で詳細を参照してください。
選択したホストのトラフィック プロファイルを作成する	選択したホストのトラフィック プロファイルの作成（50-26 ページ）で詳細を参照してください。
選択したホストに基づいて、コンプライアンスのホワイト リストを作成する	選択したホストに基づいたコンプライアンスのホワイト リストの作成（50-26 ページ）で詳細を参照してください。

ホストを表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [ホスト（Hosts）] > [ホスト（Hosts）] を選択します。

デフォルトのホスト ワークフローの最初のページが表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え（switch workflow）] をクリックします。別のデフォルト ワークフローの指定方法については、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。

ヒント　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、[ワークフロー切り替え（switch workflow）] をクリックして [ホスト（Hosts）] を選択します。

ホスト テーブルについて

ライセンス：FireSIGHT

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 システムなどを含めることが可能です。ユーザは、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。システムが、検出したホストに関して収集するデータの詳細は、ホスト プロファイルの使用（49-1 ページ）を参照してください。

次に、ホスト テーブルのフィールドについて説明します。

NetFlow 対応デバイスによってエクスポートされたデータに基づきネットワーク マップにホストを追加するようネットワーク検出ポリシーを設定することはできますが、これらのホストに関して使用可能な情報は限られています。たとえば、これらのホストのオペレーティング システム データは得られません（ただしホスト入力機能を使って指定する場合を除く）。詳細については、NetFlow と FireSIGHT データの違い（45-19 ページ）を参照してください。

最終表示（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。[最終表示（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、[最終表示（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 アドレス（IP Address）

ホストに関連付けられている IP アドレス。

MAC アドレス（MAC Address）

ホストが検出した NIC の MAC アドレス。

[MAC アドレス（MAC Address）] フィールドは、[ホスト（Hosts）] ワークフローの [ホストのテーブル ビュー（Table View of Hosts）] に表示されます。以下のものに対して [MAC アドレス（MAC Address）] フィールドを追加できます。

- [ホスト（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 ベンダー（MAC Vendor）

ホストが検出した NIC の MAC ハードウェア ベンダー。

[MAC ベンダー（MAC Vendor）] フィールドは、[ホスト（Hosts）] ワークフローの [ホストのテーブル ビュー（Table View of Hosts）] に表示されます。以下のものに対して [MAC ベンダー（MAC Vendor）] フィールドを追加できます。

- [ホスト（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

現在のユーザ（Current User）

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザ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、権限のないユーザがそのホストの現行ユーザとなることが可能です。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

ホストの重要度（Host Criticality）

ホストに割り当てられている、ユーザ指定の重要度の値。このフィールドの詳細については、ホスト属性のテーブルについて（50-31 ページ）の [ホストの重要度（Host Criticality）] カラムの説明を参照してください。

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。VLAN ID の詳細については、ホスト プロファイルでの VLAN タグの使用（49-24 ページ）を参照してください。

ホップ数（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、またはロード バランサ）。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。

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

ホスト上で稼働中の、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。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。

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で列挙されて表示されます。

このフィールドでは、`unknown` の値は、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のいずれにも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 ベンダー（OS Vendor）

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。

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で列挙されて表示されます。

このフィールドでは、`unknown` の値は、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のいずれにも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 名（OS Name）

ホスト上で稼働中の、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。

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で列挙されて表示されます。

このフィールドでは、unknown の値は、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のいずれにも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 のバージョン（OS Version）

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。

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で列挙されて表示されます。

このフィールドでは、unknown の値は、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のいずれにも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。

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 ソースに対する次のいずれかの値

- ユーザ：*user_name*
- アプリケーション：*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）
- FireSIGHT（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）

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。現在の ID について（46-5 ページ）を参照してください。

信頼性（Confidence）

次のいずれかになります。

- システムで検出されたホストについて、ホスト上で稼働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）。

注記（Notes）

Notes ホスト属性の、ユーザ定義のコンテンツ。

Device

トラフィックを検出した管理対象デバイス、またはネットワーク マップへホストを追加した NetFlow またはホスト入力データを処理したデバイス。

このフィールドが空白の場合、ホストが存在しているネットワークをネットワーク検出ポリシーの定義どおりに、明示的にモニタリングしていないデバイスによってホストがネットワーク マップに追加されたか、ホスト入力機能を使用してホストが追加され、システムでまだ検出されていません。

メンバー数(Count)

各行に表示された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。

選択したホストのトラフィック プロファイルの作成

ライセンス: FireSIGHT

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。

[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。

選択したホストのトラフィック プロファイルを作成するには、以下を行います。

アクセス:管理

手順 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。

手順 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。

[プロファイルの作成(Create Profile)] ページが表示され、監視対象のホストとして指定されたホストの IP アドレスが示されます。

手順 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。

トラフィック プロファイルの作成の詳細については、トラフィック プロファイルの作成 (53-1 ページ)を参照してください。

選択したホストに基づいたコンプライアンスのホワイト リストの作成

ライセンス: FireSIGHT

コンプライアンスのホワイト 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、トランスポート、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ホワイト 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、ホワイト 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。

選択したホストに基づいてコンプライアンスのホワイト リストを作成するには、以下を行います。

アクセス: 管理

手順 1　ホスト ワークフローのテーブル ビューで、ホワイト 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。

手順 2　ページの下部で [ホワイト リストの作成(Create White List)] をクリックします。

[ホワイト リストの作成(Create White List)] ページが表示され、指定したホストのホスト プロファイルの情報が示されます。

手順 3　特別なニーズに応じて、ホワイト リストを変更し、保存します。

コンプライアンスのホワイト リストの作成の詳細は、コンプライアンス ホワイト リストの作成(52-8 ページ)を参照してください。

ホストの検索

ライセンス: FireSIGHT

事前定義のいずれかの検索、または独自の検索条件を使用して、特定のホストについて検索することができます。

ホストを検索する場合には、NetFlow 対応のデバイスによってエクスポートされたデータに基づいてネットワーク マップにホストを追加するように、ネットワーク検出ポリシーを設定できますが、これらのホストについて利用できる情報は制限されることに注意してください。たとえば、これらのホストのオペレーティング システム データは得られません(ただしホスト入力機能を使って指定する場合を除く)。詳細については、NetFlow と FireSIGHT データの違い(45-19 ページ)を参照してください。

ユーザは特定のディスカバリ イベントを検索することができます。実際のネットワーク環境に合わせてカスタマイズされた検索を作成して保存すると、あとで再利用できます。

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。
- いくつかのフィールドでは、フィールドに n/a または blank を指定して、そのフィールドで情報を使用できないイベントを特定することができます。!n/a または !blank を使用して、フィールドに値が挿入されるイベントを特定することができます。
- ほとんどのフィールドでは大文字/小文字が区別されません。
- IP アドレスは CIDR 表記を使用して指定できます。FireSIGHT システムへの IP アドレスの入力については、IP アドレスの表記規則（1-24 ページ）を参照してください。

（注）　IP アドレスを使用してホストを検索した場合、結果には、少なくとも 1 つの IP アドレスが検索条件と一致するホストがすべて含まれます（つまり、IPv6 のアドレスの検索では、プライマリ アドレスが IPv4 であるホストが返されることがあります）。

- 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。

ホストの特別な検索構文

次の表に、特定のホスト フィールドに固有の検索情報について示します。ホストのフィールドに関する詳細は、ホスト テーブルについて（50-22 ページ）を参照してください。

表 50-5　　ホストの検索条件

フィールド	検索条件のメモ
ホスト タイプ（Host Type）	すべてのネットワーク デバイスを検索するには、!host と入力します。
MAC ベンダー（MAC Vendor）	仮想 MAC ベンダー（つまり、仮想マシンが含まれているイベント）を検索するには、virtual_mac_vendor と入力します。 名前にカンマが含まれているベンダーを検索するには、検索語全体を引用符で囲みます。このようにしないと、Defense Center は検索語を 2 つの検索として扱い、それぞれの検索語に一致するイベントを返します。
OS ベンダー/名前/バージョン（OS Vendor/Name/Version）	オペレーティング システムが不明であるホストを検索するには、unknown と入力します。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検索するには、n/a と入力します。

表 50-5　ホストの検索条件（続き）

フィールド	検索条件のメモ
信頼性（Confidence）	信頼度の前に、より大きい（>）、以上（>=）、より小さい（<）、以下（<=）、等しい（=）の演算子を付けることができます。 n/a の検索で一致するものには、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も含まれます。
OS 競合（OS Conflict）	検索結果には、[OS 競合（OS Conflict）] カラムは表示されないことに注意してください。表示しているホストにオペレーティング システムの競合が発生しているかどうかを判断するには、ワークフロー ページで検索の制約を展開します。オペレーティング システムにおける競合の解決の詳細については、オペレーティング システムのアイデンティティの競合を解決する（49-15 ページ）を参照してください。

保存されている検索をロードおよび削除する方法など、検索の詳細については、イベントの検索（60-1 ページ）を参照してください。

ホストを検索するには、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　テーブルのドロップダウン メニューから [ホスト（Hosts）] 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。

ヒント　データベース内で別の種類のイベントを検索するには、テーブルのドロップダウン リストから選択します。

手順 3　表ホストの検索条件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。

複数のフィールドに条件を入力すると、Defense Center はすべてのフィールドに対して指定された検索条件に一致するレコードのみを返します。オブジェクトを検索条件として使用するには、検索フィールドの隣にある追加アイコン（ ＋ ）をクリックします。

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　制約された権限を持つカスタム ユーザ ロールの制約として検索を保存する場合は、検索を非公開として保存する**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、デフォルトのホスト ワークフローに表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、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。

ホスト属性の使用

ライセンス: FireSIGHT

FireSIGHT 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関する追加情報をアナリストに提供する必要が生じることがあるたもしれません。ホスト プロファイルにメモを追加したり、ホストのビジネス重要度を設定したり、選択した他の情報を提供したりできます。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、相関ルールをトリガーする条件を制限することができます。相関ルールに応じて属性値を設定することもできます。

詳細については、以下を参照してください。

- ホスト属性の表示(50-30 ページ)
- ホスト属性のテーブルについて(50-31 ページ)
- 選択したホストのホスト属性の設定(50-32 ページ)
- ホスト属性の検索(50-33 ページ)
- セット属性修復の構成(54-17 ページ)

ホスト属性の表示

ライセンス: FireSIGHT

Defense 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。その後、探している情報に応じて表示方法を操作できます。

ユーザ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。カスタム ワークフローの作成方法については、カスタム ワークフローの作成（58-44 ページ）を参照してください。

ホスト属性のアクションの表で、ホスト属性のワークフロー ページで実行できる特定の操作について説明します。一般的なディスカバリ イベントのアクションの表に記載されているタスクも実行できます。

表 50-6　　ホスト属性のアクション

目的	操作
テーブルのカラムの内容について詳しく調べる	ホスト属性のテーブルについて（50-31 ページ）で詳細を参照してください。
選択したホストにホスト属性を割り当てる	選択したホストのホスト属性の設定（50-32 ページ）で詳細を参照してください。

ホストの属性を表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [ホスト（Hosts）] > [ホスト属性（Host Attributes）] を選択します。

デフォルトのホスト属性ワークフローの最初のページが表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え（switch workflow）] をクリックします。別のデフォルト ワークフローの指定方法については、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。

ヒント　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。

ホスト属性のテーブルについて

ライセンス：FireSIGHT

FireSIGHT 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関する追加情報をアナリストに提供する必要が生じることがあるたもしれません。ホスト プロファイルにメモを追加したり、ビジネスの重要度を設定したり、選択した他の情報を提供したりできます。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、相関ルールをトリガーする条件を制限することができます。

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。

ホスト属性の詳細については、事前定義のホスト属性の使用（49-34 ページ）およびユーザ定義のホスト属性の使用（49-35 ページ）を参照してください。

次に、ホスト属性テーブルのフィールドについて説明します。

[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（Current User）

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザ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、権限のないユーザがそのホストの現行ユーザとなることが可能です。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

ホストの重要度（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。

ホストの重要度の設定については、事前定義のホスト属性の使用（49-34 ページ）および選択したホストのホスト属性の設定（50-32 ページ）を参照してください。

注記（Notes）

他のアナリストに提示する、ホストに関する情報。メモを追加する方法については、事前定義のホスト属性の使用（49-34 ページ）を参照してください。

コンプライアンスのホワイト リストを含む、ユーザ定義の任意のホスト属性（Any user-defined host attribute, including those for compliance white lists）

ユーザ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。詳細については、ユーザ定義のホスト属性の使用（49-35 ページ）を参照してください。

メンバー数（Count）

各行に表示された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。

選択したホストのホスト属性の設定

ライセンス：FireSIGHT

各ホストに割り当てることができる事前定義のホスト属性として、ホストの重要度とホスト特有のメモの 2 つの属性があります。

ホストの重要度を使用して、特定のホストのビジネス重要度を特定します。ホストの重要度に基づいて、相関ポリシーとアラートを作成することができます。たとえば、ユーザの業務にとって、組織のメール サーバは一般のユーザ ワークステーションよりも重要です。メール サーバや、他のビジネスに不可欠なサーバに対しては高いホスト重要度を割り当てて、その他のホストには中程度、または低い重要度を割り当てることができます。次に相関ポリシーを作成できます。これは、影響を受けるホストの重要度に基づいてさまざまなアラートを起動します。

メモを使用して、他のアナリストに提示するホストの情報を記録します。たとえば、ネットワーク上のコンピュータに、パッチが適用されていない古いバージョンの、テスト用オペレーティング システムが搭載されている場合、メモ機能を使用して、システムは意図的にパッチが適用されていないと示すことができます。

ユーザ定義のホスト属性を作成することもできます。たとえば、ファシリティ コード、市、または部屋番号など、ホストに対して物理的な場所の識別子を割り当てるホスト属性を作成することもできます。作成したユーザ定義のホスト属性の詳細については、ユーザ定義のホスト属性の作成（49-36 ページ）を参照してください。

選択したホストのホスト重要度は、ホスト ワークフローで設定することも、ホスト プロファイル、または修復によって設定することもできます。詳細については、事前定義のホスト属性の使用（49-34 ページ）またはセット属性修復の構成（54-17 ページ）を参照してください。

選択したホストのホスト属性を設定するには、以下を行います。

アクセス：Admin/Any Security Analyst

手順 1　ホスト属性に追加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。

ヒント　ソートおよび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。

手順 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。

[ホスト属性（Host Attributes）] ポップアップ ウィンドウが表示されます。

手順 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。

手順 4　必要に応じて、選択したホストのホスト プロファイルにメモを追加することができます。メモは、最大 255 文字の英数字、特殊文字、およびスペースを使用してテキスト ボックスに入力します。

手順 5　必要に応じて、自身で設定したユーザ定義のホスト属性を設定します。

手順 6　[保存（Save）] をクリックします。

指定したホスト属性は、選択されたホストに割り当てられます。

ホスト属性の検索

ライセンス：FireSIGHT

特定のホストの属性を持つホストを検索できます。たとえば企業に複数の支社がある場合、いずれかのホストが存在する都市を示すホスト属性を設定することができます。これで、特定の地域のホストを検索できるようになります。ホスト属性の詳細については、ユーザ定義のホスト属性の使用（49-35 ページ）を参照してください。

実際のネットワーク環境に合わせてカスタマイズされた検索を作成して保存すると、あとで再利用できます。ホスト属性のフィールドの詳細については、ホスト属性のテーブルについて（50-31 ページ）を参照してください。

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。
- いくつかのフィールドでは、フィールドに `n/a` または `blank` を指定して、そのフィールドで情報を使用できないイベントを特定することができます。`!n/a` または `!blank` を使用して、フィールドに値が挿入されるイベントを特定することができます。
- ほとんどのフィールドでは大文字/小文字が区別されません。
- IP アドレスは CIDR 表記を使用して指定できます。FireSIGHT システムへの IPv4 および IPv6 のアドレスの入力については、IP アドレスの表記規則（1-24 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。

ホスト属性を検索するには、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　テーブルのドロップダウン リストから [ホスト属性（Host Attributes）] 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。

ヒント　データベース内で別の種類のイベントを検索するには、テーブルのドロップダウン リストから選択します。

手順 3　ホスト属性のテーブルについてに記載されているように、該当するフィールドに検索条件を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。オブジェクトを検索条件として使用するには、検索フィールドの隣にある追加アイコン（ ＋ ）をクリックします。

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　制約された権限を持つカスタム ユーザ ロールの制約として検索を保存する場合は、検索を非公開として保存する**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、デフォルトのホスト属性ワークフローに表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え（switch workflow）] をクリックします。別のデフォルト ワークフローの指定方法については、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。

侵入の痕跡の使用

ライセンス：FireSIGHT

FireSIGHT システムは、監視対象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そう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入の痕跡/兆候（IOC）タグをトリガーとして使用します。IOC のタグが付けられたホスト IP アドレスは、侵害されたホストの特別なアイコン（  ）付きでイベント ビューに表示されます。ユーザはコンプライアンス ルールを記述して、IOC のタグが付けられているホストについて説明することができます。

この機能を使用するには、ネットワーク検出ポリシーで IOC ルールを有効にしておく必要があります。侵害されたホストの IOC タグをトリガーするために、事前定義のいずれか、またはすべてのルールを有効にすることができます。詳細については、侵害の兆候ルールの設定（45-38 ページ）を参照してください。

侵入の痕跡に関する詳細は、以降の項を参照してください。

- 侵入の痕跡の表示（50-36 ページ）
- 侵害の痕跡テーブルについて（50-37 ページ）
- 侵害の痕跡の検索（50-37 ページ）

侵入の痕跡の表示

ライセンス：FireSIGHT

Defense Center を使用して、トリガーされた侵入の痕跡（IOC）のテーブルを表示することができます。ここでユーザは、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。

ユーザが IOC 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 IOC 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。詳細については、カスタム ワークフローの作成（58-44 ページ）を参照してください。

次の表では、IOC のワークフロー ページでユーザが実行できる特定のアクションについて説明します。一般的なディスカバリ イベントのアクションの表に記載されているタスクも実行できます。

表 50-7　侵入の痕跡のアクション

目的	操作
テーブルのカラムの内容について詳しく調べる	侵害の痕跡テーブルについて（50-37 ページ）で詳細を参照してください。
侵害されたホストのホスト プロファイルを表示する	[IP アドレス（IP Address）] カラムで侵害されたホストのアイコン（  ）をクリックします。
選択した 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する	編集する IOC イベントの隣にあるチェック ボックスをオンにして、[解決マーク（Mark Resolved）] をクリックします。詳細については、侵害の兆候を解決済みにする（49-11 ページ）を参照してください。
IOC をトリガーとして使用したイベントの詳細を表示する	[初回表示（First Seen）] または [最終表示（Last Seen）] カラムで表示アイコン（  ）をクリックします。

侵入の痕跡を表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [ホスト（Hosts）] > [侵入の痕跡（Indications of Compromise）] を選択します。

デフォルトの侵害の痕跡（IOC）ワークフローの最初のページが表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え（switch workflow）] をクリックします。別のデフォルト ワークフローの指定方法については、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。

ヒント　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、[ワークフロー切り替え（switch workflow）] をクリックして [侵害の痕跡（Indications of Compromise）] を選択します。

侵害の痕跡テーブルについて

ライセンス：FireSIGHT

FireSIGHT システムは、監視対象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そう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イベント データとの関連性を示します。これらの相関は、ホストに関連付けられている侵害の痕跡（IOC）として表示されます。ホストの IOC を解決済みにマークして、ホストから IOC タグを削除することができます。1 つのホストで複数の IOC タグをトリガーできます。ユーザは、ホスト プロファイルの [侵害の痕跡（Indications of Compromise）] セクションで、ホストに関連付けられているすべての IOC タグを表示できます。ホスト プロファイルにおける IOC データの詳細については、ホスト プロファイルでの侵害の兆候の使用（49-9 ページ）を参照してください。

次に、IOC テーブルのフィールドについて説明します。

[IP アドレス（IP Address）]
IOC をトリガーしたホストに関連付けられている IP アドレス。

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）
特定の侵害の兆候（IOC）に関連付けられている識別子であり、その IOC をトリガー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について、IOC が表している内容の説明（`This host may be under remote control` や `Malware has been executed on this host` など）。

初回確認日時/最新確認日時（First/Last Seen）
ホストの IOC をトリガーしたイベントが発生した最初（または最新）の日付と時刻。

侵害の痕跡の検索

ライセンス：FireSIGHT

事前定義のいずれかの検索を使用するか、または独自の検索条件を使用して、監視対象のホスト上でトリガーされた特定の侵害の痕跡（IOC）タグを検索することができます。定義済み検索は例として使用でき、これによりネットワークに関する重要な情報に素早くアクセスできます。

デフォルトの検索内の特定のフィールドを変更して、使用するネットワーク環境に合わせてカスタマイズし、後で再利用できるようにそれらを保存することもできます。データを取得するために使用できるフィールドは、侵害の痕跡テーブルについて（50-37 ページ）に記載されています。

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。
- いくつかのフィールドでは、フィールドに `n/a` または `blank` を指定して、そのフィールドで情報を使用できないイベントを特定することができます。`!n/a` または `!blank` を使用して、フィールドに値が挿入されるイベントを特定することができます。
- ほとんどのフィールドでは大文字/小文字が区別されません。
- IP アドレスは CIDR 表記を使用して指定できます。FireSIGHT システムへの IPv4 および IPv6 のアドレスの入力については、IP アドレスの表記規則（1-24 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。

侵害の痕跡を検索するには、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　テーブルのドロップダウン リストから、[侵害の痕跡（Indications of Compromise）] 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。

ヒント　データベース内で別の種類のイベントを検索するには、テーブルのドロップダウン リストから選択します。

手順 3　侵害の痕跡テーブルについて（50-37 ページ）に記載されているように、該当するフィールドに検索条件を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。オブジェクトを検索条件として使用するには、検索フィールドの隣にある追加アイコン（ ＋ ）をクリックします。

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　制約された権限を持つカスタム ユーザ ロールの制約として検索を保存する場合は、検索を非公開として保存する**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、デフォルトの IOC ワークフローに表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え（switch workflow）] をクリックします。別のデフォルト ワークフローの指定方法については、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。

サーバの使用

ライセンス：FireSIGHT

FireSIGHT システムは、監視対象ネットワーク セグメント上のホストで稼働しているすべてのサーバに関する情報を収集します。システムが収集する情報には、サーバ名、サーバが使用するアプリケーションおよびネットワークのプロトコル、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、およびサーバが通信しているポートが含まれています。

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。詳細については、ホスト制限と検出イベント ロギング（45-15 ページ）を参照してください。Defense 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、および削除できます。

また、サーバ イベントを相関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 サーバを検出したときに相関ルールをトリガーできます。

NetFlow 対応のデバイスによってエクスポートされたアプリケーション データに基づいてサーバをネットワーク マップに追加するよう、ネットワーク検出ポリシーを設定できますが、これらのサーバについて使用できる情報は制限されます。詳細については、NetFlow と FireSIGHT データの違い（45-19 ページ）を参照してください。

詳細については、次の各項を参照してください。

- サーバの表示（50-40 ページ）
- サーバのテーブルについて（50-41 ページ）
- サーバの検索（50-43 ページ）
- サーバのアイデンティティの編集（49-20 ページ）

サーバの表示

ライセンス：FireSIGHT

Defense Center を使用して、検出されたサーバのテーブルを表示できます。ここでユーザは、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。

ユーザがサーバ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。詳細については、カスタム ワークフローの作成（58-44 ページ）を参照してください。

サーバの操作の表で、サーバ ワークフロー ページで実行できる特定の操作について説明します。一般的なディスカバリ イベントのアクションの表に記載されているタスクも実行できます。

表 50-8　　サーバの操作

目的	操作
テーブルのカラムの内容について詳しく調べる	サーバのテーブルについて（50-41 ページ）で詳細を参照してください。
サーバ アイデンティティを編集する	編集するサーバのイベントの隣にあるチェック ボックスをオンにして、[サーバ アイデンティティの設定（Set Server Identity）] をクリックします。詳細については、サーバのアイデンティティの編集（49-20 ページ）を参照してください。

サーバを表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [ホスト（Hosts）] > [サーバ（Servers）] を選択します。

デフォルトのサーバ ワークフローの最初のページが表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え（switch workflow）] をクリックします。別のデフォルト ワークフローの指定方法については、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。

ヒント　サーバのテーブル 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、[ワークフロー切り替え(switch workflow)] をクリックして [サーバ(Server)] を選択します。

サーバのテーブルについて

ライセンス:FireSIGHT

FireSIGHT システムは、監視対象ネットワーク セグメント上のホストで稼働しているサーバに関する情報を収集します。

次に、サーバのテーブルのフィールドについて説明します。

NetFlow 対応のデバイスによってエクスポートされたデータに基づいてサーバをネットワーク マップに追加するよう、ネットワーク検出ポリシーを設定できますが、これらのサーバについて使用できる情報は制限されます。詳細については、NetFlow と FireSIGHT データの違い (45-19 ページ)を参照してください。

前回の使用(Last Used)
ネットワーク上でサーバ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。更新間隔の設定については、データ保存の設定 (45-39 ページ)を参照してください。

[IP アドレス(IP Address)]
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。

[ポート(Port)]
サーバが稼働しているポート。

プロトコル
サーバ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)
以下のいずれかによって示されるアプリケーション プロトコル

- サーバのアプリケーション プロトコルの名前
- `pending`:システムで、いずれかの理由のでサーバ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 フィンガープリントに基づいてシステムでサーバ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。詳細については、表 45-2(45-12 ページ)を参照してください。

ベンダー（Vendor）

次のいずれかになります。

- サーバのベンダー：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のベンダー
- 空白：システムが既知のサーバ 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がネットワーク マップに追加された場合

バージョン（Version）

次のいずれかになります。

- サーバのバージョン：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のバージョン
- 空白：システムが既知のサーバ 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い場合、または NetFlow データを使用してサーバがネットワーク マップに追加された場合

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。詳細については、表 45-2（45-12 ページ）を参照してください。

ヒット件数（Hits）

サーバ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：*user_name*
- アプリケーション：*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）
- FireSIGHT、FireSIGHT Port Match、または FireSIGHT Pattern Match（FireSIGHT システムで検出されたサーバの場合）
- NetFlow（NetFlow データに基づいてネットワーク マップに追加されたサーバの場合）

システムでは、サーバ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。現在の ID について（46-5 ページ）を参照してください。

Device

サーバを検出したデバイスの名前、またはネットワーク マップにサーバを追加した NetFlow あるいはホスト入力データを処理したデバイスの名前。

現在のユーザ（Current User）

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザ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、権限のないユーザがそのホストの現行ユーザとなることが可能です。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

メンバー数（Count）

各行に表示された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。

サーバの検索

ライセンス：FireSIGHT

事前定義のいずれかの検索、または独自の検索条件を使用して、監視対象のホストで稼働中の特定のサーバを検索することができます。定義済み検索は例として使用でき、これによりネットワークに関する重要な情報に素早くアクセスできます。

デフォルトの検索内の特定のフィールドを変更して、使用するネットワーク環境に合わせてカスタマイズし、後で再利用できるようにそれらを保存することもできます。データを取得するために使用できるフィールドは、サーバのテーブルについて（50-41 ページ）に記載されています。

サーバを検索する場合には、NetFlow 対応のデバイスによってエクスポートされたデータに基づいてアプリケーションやサーバをネットワーク マップに追加するよう、ネットワーク検出ポリシーを設定できますが、これらのサーバについて使用できる情報は制限されることに注意してください。詳細については、NetFlow と FireSIGHT データの違い（45-19 ページ）を参照してください。

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。
- いくつかのフィールドでは、フィールドに n/a または blank を指定して、そのフィールドで情報を使用できないイベントを特定することができます。!n/a または !blank を使用して、フィールドに値が挿入されるイベントを特定することができます。
- ほとんどのフィールドでは大文字/小文字が区別されません。
- IP アドレスは CIDR 表記を使用して指定できます。FireSIGHT システムへの IPv4 および IPv6 のアドレスの入力については、IP アドレスの表記規則（1-24 ページ）を参照してください。
- 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。

サーバを検索するには、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　テーブルのドロップダウン リストから [サーバ（Servers）] 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。

ヒント　データベース内で別の種類のイベントを検索するには、テーブルのドロップダウン リストから選択します。

手順 3　該当するフィールドに検索基準を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。オブジェクトを検索条件として使用するには、検索フィールドの隣にある追加アイコン（ ＋ ）をクリックします。

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　制約された権限を持つカスタム ユーザ ロールの制約として検索を保存する場合は、検索を非公開として保存する**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、デフォルトのサーバ ワークフローに表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、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。

アプリケーションの使用

ライセンス: FireSIGHT

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。FireSIGHT システムは多くの電子メールの使用、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の使用を検出します。

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働しているかがわかっている場合は、そのことを使用してホスト 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、いずれかの対象ホストで別のメール クライアントが稼働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。

各 FireSIGHT システムの更新プログラムのリリース ノートや更新されたディテクタの情報に関する各 VDB アップデートのアドバイザリを注意深く読んでください。

分析用にアプリケーション データを収集および格納するには、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。詳細については、検出データ収集について(45-2 ページ)を参照してください。

詳細については、次の各項を参照してください。

- アプリケーションの詳細の表示(50-50 ページ)
- アプリケーションの詳細テーブルについて(50-51 ページ)
- アプリケーションの詳細の検索(50-52 ページ)

アプリケーションの表示

ライセンス：FireSIGHT

Defense 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。

ユーザ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、使用する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。詳細については、カスタム ワークフローの作成（58-44 ページ）を参照してください。

アプリケーションの操作の表で、アプリケーション ワークフロー ページで実行できる特定の操作について説明します。一般的なディスカバリ イベントのアクションの表に記載されているタスクも実行できます。

表 50-9　アプリケーションの操作

目的	操作
テーブルのカラムの内容について詳しく調べる	アプリケーション テーブルについて（50-46 ページ）で詳細を参照してください。
特定のアプリケーションに対する [アプリケーションの詳細表示（Application Detail View）] を開く	クライアント、アプリケーション プロトコル、または Web アプリケーションの隣にあるアプリケーション詳細ビューのアイコン（ ）をクリックします。

アプリケーションを表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [ホスト（Hosts）] > [アプリケーションの詳細（Applications Details）] を選択します。

デフォルトのアプリケーション詳細ワークフローの最初のページが表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え（switch workflow）] をクリックします。別のデフォルト ワークフローの指定方法については、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。

ヒント　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。

アプリケーション テーブルについて

ライセンス：FireSIGHT

監視対象ホストが別のホストに接続すると、FireSIGHT 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。システムはさまざまな Web ブラウザまたはサーバ、電子メール クライアントまたはサーバ、インスタント メッセンジャー、ピアツーピア アプリケーションなどを検出します。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対し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記録します。

FireSIGHT システムはアプリケーション データを 3 つのタイプ(クライアント、Web アプリケーション、アプリケーション プロトコル)に分類します。アプリケーション テーブルは、アプライアンスで検出された 3 つのすべてのタイプのアプリケーションの組み合わせのリストを提供します。

次に、アプリケーション テーブルの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(IP Address)]

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。

カテゴリ(Category)

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(Tag)

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(0 個を含む)のタグを付けることができます。

リスク(Risk)

この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かもしれない目的で使用される可能性がどの程度であるか。アプリケーションのリスクは、`Very Low` から `Very High` までの範囲です。

侵入イベントをトリガーとして使用したトラフィックで検出された 3 つの Application Protocol Risk、Client Risk、および Web Application Risk の中で最も高いものとなります(有効な場合)。

ビジネスとの関連性(Business Relevance)

アプリケーションが、娯楽としてではなく、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は、`Very Low` から `Very High` までの範囲です。

侵入イベントをトリガーとして使用したトラフィックで検出された 3 つの Application Protocol Business Relevance、Client Business Relevance、および Web Application Business Relevance の中で、最も低いものとなります(有効な場合)。

現在のユーザ(Current User)

ホストに現在ログインしているユーザの ID(ユーザ名)。

権限のないユーザがホストにログインすると、そのログインはユーザ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、権限のないユーザがそのホストの現行ユーザとなることが可能です。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

タイプ(Type)

アプリケーションのタイプ:

- **アプリケーション プロトコル**は、ホスト間の通信手段を意味します。
- **クライアント アプリケーション**は、ホスト上で稼働しているソフトウェアを表します。
- **Web アプリケーション**は、HTTP トラフィックの内容または要求された URL を意味します。

メンバー数(Count)

各行に表示された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。

アプリケーションの検索

ライセンス: FireSIGHT

特定のクライアント、アプリケーション プロトコル、または Web アプリケーションを実行しているホストを検索することができます。実際のネットワーク環境に合わせてカスタマイズされた検索を作成して保存すると、あとで再利用できます。

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。
- いくつかのフィールドでは、フィールドに `n/a` または `blank` を指定して、そのフィールドで情報を使用できないイベントを特定することができます。`!n/a` または `!blank` を使用して、フィールドに値が挿入されるイベントを特定することができます。
- ほとんどのフィールドでは大文字/小文字が区別されません。
- IP アドレスは CIDR 表記を使用して指定できます。FireSIGHT システムへの IPv4 および IPv6 のアドレスの入力については、IP アドレスの表記規則(1-24 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。

アプリケーションを検索するには、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　テーブルのドロップダウン リストから [アプリケーション（Applications）] 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。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。オブジェクトを検索条件として使用するには、検索フィールドの隣にある追加アイコン（ ＋ ）をクリックします。

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　制約された権限を持つカスタム ユーザ ロールの制約として検索を保存する場合は、検索を非公開として保存する**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、デフォルトのクライアント ワークフローに表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え（switch workflow）] をクリックします。別のデフォルト ワークフローの指定方法については、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。

アプリケーションの詳細の使用

ライセンス：FireSIGHT

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。FireSIGHT システムは多くの電子メールの使用、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の使用を検出します。

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働しているかがわかっている場合は、そのことを使用してホスト 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、いずれかの対象ホストで別のメール クライアントが稼働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。

各 FireSIGHT システムの更新プログラムのリリース ノートや更新されたディテクタの情報に関する各 VDB アップデートのアドバイザリを注意深く読んでください。

分析用にアプリケーション データを収集および格納するには、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。詳細については、アプリケーション検出について（45-11 ページ）を参照してください。

詳細については、次の各項を参照してください。

- アプリケーションの詳細の表示（50-50 ページ）
- アプリケーションの詳細テーブルについて（50-51 ページ）
- アプリケーションの詳細の検索（50-52 ページ）

アプリケーションの詳細の表示

ライセンス：FireSIGHT

Defense 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。

ユーザ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。詳細については、カスタム ワークフローの作成（58-44 ページ）を参照してください。

アプリケーションの詳細の操作の表で、アプリケーション詳細ワークフロー ページで実行できる特定の操作について説明します。一般的なディスカバリ イベントのアクションの表に記載されているタスクも実行できます。

表 50-10　アプリケーションの詳細の操作

目的	操作
テーブルのカラムの内容について詳しく調べる	アプリケーションの詳細テーブルについて（50-51 ページ）で詳細を参照してください。
特定のアプリケーションに対する [アプリケーションの詳細表示（Application Detail View）] を開く	クライアントの隣にあるアプリケーション詳細ビューのアイコン（  ）をクリックします。

アプリケーションの詳細を表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [ホスト（Hosts）] > [アプリケーションの詳細（Applications Details）] を選択します。

デフォルトのアプリケーション詳細ワークフローの最初のページが表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え（switch workflow）] をクリックします。別のデフォルト ワークフローの指定方法については、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。

ヒント　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。

アプリケーションの詳細テーブルについて

ライセンス：FireSIGHT

監視対象ホストが別のホストに接続すると、FireSIGHT 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。システムはさまざまな Web ブラウザ、電子メール クライアント、インスタント メッセンジャー、ピアツーピア アプリケーションなどを検出します。

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対し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記録します。次に、アプリケーションの詳細テーブルの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最後に使用された時間、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。更新間隔の設定については、データ保存の設定（45-39 ページ）を参照してください。

[IP アドレス（IP Address）]
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。システムがアプリケーション プロトコルを検出したものの、特定のクライアントを検出できなかった場合は、一般的な名前を提示するために、アプリケーション プロトコル名に `client` が付加されます。

バージョン（Version）
アプリケーションのバージョン。

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、またはビジネス関連性（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。詳細については、表 45-2（45-12 ページ）を参照してください。

アプリケーション プロトコル（Application Protocol）

アプリケーションによって使用されるアプリケーション プロトコル。システムがアプリケーション プロトコルを検出したものの、特定のクライアントを検出できなかった場合は、一般的な名前を提示するために、アプリケーション プロトコル名に `client` が付加されます。

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ここで提示されるので注意してください。

ヒット件数（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、この値は必ず `0` になります。

Device

アプリケーションの詳細が含まれているディスカバリ イベントを生成したデバイス。

現在のユーザ（Current User）

ホストに現在ログインしているユーザの ID（ユーザ名）。

権限のないユーザがホストにログインすると、そのログインはユーザ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、権限のないユーザがそのホストの現行ユーザとなることが可能です。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

メンバー数（Count）

各行に表示された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。

アプリケーションの詳細の検索

ライセンス：FireSIGHT

特定のクライアント、アプリケーション プロトコル、または Web アプリケーションを実行しているホストを検索することができます。実際のネットワーク環境に合わせてカスタマイズされた検索を作成して保存すると、あとで再利用できます。

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。
- いくつかのフィールドでは、フィールドに `n/a` または `blank` を指定して、そのフィールドで情報を使用できないイベントを特定することができます。`!n/a` または `!blank` を使用して、フィールドに値が挿入されるイベントを特定することができます。
- ほとんどのフィールドでは大文字/小文字が区別されません。
- IP アドレスは CIDR 表記を使用して指定できます。FireSIGHT システムへの IPv4 および IPv6 のアドレスの入力については、IP アドレスの表記規則（1-24 ページ）を参照してください。
- 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。

アプリケーションの詳細を検索するには、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　テーブルのドロップダウン リストから [アプリケーションの詳細（Application Details）] 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。

ヒント　データベース内で別の種類のイベントを検索するには、テーブルのドロップダウン リストから選択します。

手順 3　該当するフィールドに検索基準を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。オブジェクトを検索条件として使用するには、検索フィールドの隣にある追加アイコン(+)をクリックします。

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　制約された権限を持つカスタム ユーザ ロールの制約として検索を保存する場合は、検索を非公開として保存する**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、デフォルトのアプリケーション詳細ワークフローに表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、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。

脆弱性の処理

ライセンス: FireSIGHT

FireSIGHT 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ティング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。

ホストで稼働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一連の脆弱性があります。ホストにパッチを適用した後、またはホストが脆弱性に関して問題ないと判断された場合は、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。Defense Center を使用して、各ホストに対する脆弱性を追跡および確認できます。

サーバで使用されるアプリケーション プロトコルがシステム ポリシー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に対する脆弱性はマップされないことに注意してください。ベンダーレスおよびバージョンレスのクライアントに対する脆弱性はマップできません。詳細については、サーバの脆弱性のマッピング（63-33 ページ）を参照してください。

詳細については、以下を参照してください。

- 脆弱性の表示（50-55 ページ）
- 脆弱性テーブルについて（50-56 ページ）
- 脆弱性の非アクティブ化（50-58 ページ）
- 脆弱性の検索（50-58 ページ）

脆弱性の表示

ライセンス：FireSIGHT

Defense 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。

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。脆弱性の検索の詳細については、脆弱性の検索（50-58 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 ワークフローの作成方法については、カスタム ワークフローの作成（58-44 ページ）を参照してください。

次の表では、脆弱性のワークフロー ページでユーザが実行できる特定の操作について説明します。一般的なディスカバリ イベントのアクションの表に記載されているタスクも実行できます。

表 50-11　脆弱性の操作

目的	操作
テーブルのカラムの内容について詳しく調べる	脆弱性テーブルについて（50-56 ページ）で詳細を参照してください。
脆弱性の詳細を表示する	[SVID] カラムの表示アイコン（🔍）をクリックします。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。詳細については、脆弱性の詳細の表示（49-31 ページ）を参照してください。

表 50-11　脆弱性の操作（続き）

目的	操作
選択した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する	脆弱性の非アクティブ化（50-58 ページ）で詳細を参照してください。
脆弱性のタイトルの全テキストを表示する	タイトルを右クリックして [全テキストを表示（Show Full Text）] を選択します。

脆弱性を表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [脆弱性（Vulnerabilities）] > [脆弱性（Vulnerabilities）] を選択します。

デフォルトの脆弱性ワークフローの最初のページが表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え（switch workflow）] をクリックします。別のデフォルト ワークフローの指定方法については、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。

ヒント　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、[ワークフロー切り替え（switch workflow）] をクリックして [脆弱性（Vulnerabilities）] を選択します。

脆弱性テーブルについて

ライセンス：FireSIGHT

FireSIGHT 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ティング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。

ホストで稼働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一連の脆弱性があります。ホストにパッチを適用した後、またはホストが脆弱性に関して問題ないと判断された場合は、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。Defense Center を使用して、各ホストに対する脆弱性を追跡および確認できます。

脆弱性の詳細については、脆弱性のネットワーク マップの操作（48-8 ページ）およびホスト プロファイルでの脆弱性の使用（49-29 ページ）を参照してください。

次に、脆弱性テーブルのフィールドについて説明します。

SVID

脆弱性を追跡するためにシステムで使用するCiscoの脆弱性の識別番号。

SVID について脆弱性の詳細にアクセスするには、表示アイコン（🔍）をクリックします。詳細については、脆弱性の詳細の表示（49-31 ページ）を参照してください。

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。（http://www.securityfocus.com/bid/）

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と、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。

役職（Title）

脆弱性のタイトル。

[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。

公開日（Date Published）

脆弱性が公開された日付。

脆弱性の影響（Vulnerability Impact）

Bugtraq データベースにおいて脆弱性に割り当てられている重大度を示します。0～10 の値で、10 は最も重大であることを示します。脆弱性の影響は、Bugtraq エントリの作成者によって決定されます。この作成者は、自身の判断および SANS Critical Vulnerability Analysis（CVA）の基準に従って脆弱性の影響を決定します。

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。

利用可能なエクスプロイト（Available Exploits）

脆弱性に対して既知のエクスプロイトがあるかどうかを示します。

説明

脆弱性についての簡単な説明。

技術的説明（Technical Description）

脆弱性に関する詳細な技術的説明。

ソリューション

脆弱性の修復に関する情報。

メンバー数（Count）

各行に表示された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。

脆弱性の非アクティブ化

ライセンス：FireSIGHT

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に関して問題ないと判断された後に、脆弱性を非アクティブにします。非アクティブにした脆弱性は、侵入の影響の相関には使用されなくなります。システムが、この脆弱性によって影響を受けている新しいホストを検出すると、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になりません）。

ユーザは、ネットワーク上の特定のホストに対して脆弱性を示すワークフローのページ（以下を参照）で**のみ**、脆弱性ワークフロー内で脆弱性を非アクティブにすることができます。

- 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）]。これは、ネットワーク上のホストに適用される脆弱性のみを示します。
- 脆弱性の（カスタムまたは事前定義の）ワークフローの任意のページ。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。

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。1 つのホストに対して脆弱性を非アクティブにするには、次の 3 つの方法があります。

- ネットワーク マップを使用する。

  詳細については、脆弱性のネットワーク マップの操作（48-8 ページ）を参照してください。
- ホストのホスト プロファイルを使用する。

  詳細については、個々のホストに対する脆弱性の設定（49-34 ページ）を参照してください。
- 脆弱性を非アクティブにする 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。関連する複数の IP アドレスを持つホストの場合、この機能は 1 つのアドレス（そのホストで選択された IP アドレス）のみに適用されます。

IP アドレスに基づいてビューを制約するには、脆弱性を非アクティブにするホストに対して 1 つの 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。脆弱性の検索の詳細については、脆弱性の検索（50-58 ページ）を参照してください。

脆弱性を非アクティブにするには、以下を行います。

アクセス：Admin/Any Security Analyst

手順 1　[ネットワーク上の脆弱性（Vulnerabilities on the Network）] ページで、非アクティブにする脆弱性の隣にあるチェック ボックスをオンにして [確認（Review）] をクリックします。

脆弱性の検索

ライセンス：FireSIGHT

ネットワーク上のホストに影響を及ぼす脆弱性を検索できます。実際のネットワーク環境に合わせてカスタマイズされた検索を作成して保存すると、あとで再利用できます。

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。
- いくつかのフィールドでは、フィールドに `n/a` または `blank` を指定して、そのフィールドで情報を使用できないイベントを特定することができます。`!n/a` または `!blank` を使用して、フィールドに値が挿入されるイベントを特定することができます。
- ほとんどのフィールドでは大文字/小文字が区別されません。
- IP アドレスは CIDR 表記を使用して指定できます。FireSIGHT システムへの IPv4 および IPv6 のアドレスの入力については、IP アドレスの表記規則（1-24 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。

脆弱性に対する特定の検索条件

以下の、脆弱性の検索に特有な情報に注意してください。

- Bugtraq ID 番号の検索は http://www.securityfocus.com/bid で行います。
- エクスプロイトされる脆弱性を検索する場合は `TRUE` を入力し、そのような脆弱性を除外する場合は `FALSE` を入力します。

脆弱性を検索するには、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　テーブルのドロップダウン リストから [脆弱性（Vulnerabilities）] 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。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。オブジェクトを検索条件として使用するには、検索フィールドの隣にある追加アイコン(+)をクリックします。

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、デフォルトの脆弱性ワークフローに表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、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。

サードパーティの脆弱性の処理

ライセンス: FireSIGHT

FireSIGHT 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ティング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。

組織でスクリプトを記述するか、またはコマンドライン インポート ファイルを作成して、サードパーティ アプリケーションからネットワーク マップ データをインポートできる場合には、サードパーティの脆弱性データをインポートして、システムの脆弱性データを増やすことができます。詳細については、『*FireSIGHT システム Host Input API Guide*』を参照してください。

インポートしたデータを影響の相関に含めるには、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定義にマップできません。

詳細については、以下を参照してください。

- サードパーティの脆弱性の表示（50-61 ページ）
- サードパーティの脆弱性テーブルについて（50-62 ページ）
- サードパーティの脆弱性の検索（50-63 ページ）

サードパーティの脆弱性の表示

ライセンス：FireSIGHT

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、Defense 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。

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。詳細については、カスタム ワークフローの作成（58-44 ページ）を参照してください。

次の表では、サードパーティ脆弱性のワークフロー ページでユーザが実行できる特定の操作について説明します。一般的なディスカバリ イベントのアクションの表に記載されているタスクも実行できます。

表 50-12　サードパーティの脆弱性の操作

目的	操作
テーブルのカラムの内容について詳しく調べる	サードパーティの脆弱性テーブルについて（50-62 ページ）で詳細を参照してください。
サードパーティの脆弱性の詳細を表示する	[SVID] カラムの表示アイコン（🔍）をクリックします。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。詳細については、脆弱性の詳細の表示（49-31 ページ）を参照してください。

サードパーティの脆弱性を表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [脆弱性（Vulnerabilities）] > [サードパーティの脆弱性（Third-Party Vulnerabilities）] を選択します。

デフォルトのサードパーティの脆弱性ワークフローの最初のページが表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え（switch workflow）] をクリックします。別のデフォルト ワークフローの指定方法については、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。

ヒント　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、[ワークフロー切り替え（switch workflow）] をクリックして [ソースごとの脆弱性（Vulnerabilities by Source）] または [IP アドレスごとの脆弱性（Vulnerabilities by IP Address）] を選択します。

サードパーティの脆弱性テーブルについて

ライセンス：FireSIGHT

ホスト入力機能を使用して、サードパーティの脆弱性情報をインポートすると、システムはその情報をデータベースに格納します。サードパーティの脆弱性テーブルのフィールドについては、次の表で説明します。

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）

ソースで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（Port）]

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。（http://www.securityfocus.com/bid/）

CVE ID

MITRE の Common Vulnerabilities and Exposures（CVE）データベースで、脆弱性に関連付けられている識別番号（http://www.cve.mitre.org/）。

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、表示アイコン（  ）をクリックします。詳細については、脆弱性の詳細の表示（49-31 ページ）を参照してください。

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と、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。

役職（Title）

脆弱性のタイトル。

説明

脆弱性についての簡単な説明。

メンバー数(Count)

各行に表示された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。

サードパーティの脆弱性の検索

ライセンス: FireSIGHT

ネットワーク上のホストに影響を及ぼすサードパーティの脆弱性を検索できます。実際のネットワーク環境に合わせてカスタマイズされた検索を作成して保存すると、あとで再利用できます。

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。
- いくつかのフィールドでは、フィールドに `n/a` または `blank` を指定して、そのフィールドで情報を使用できないイベントを特定することができます。`!n/a` または `!blank` を使用して、フィールドに値が挿入されるイベントを特定することができます。
- ほとんどのフィールドでは大文字/小文字が区別されません。
- IP アドレスは CIDR 表記を使用して指定できます。FireSIGHT システムへの IPv4 および IPv6 のアドレスの入力については、IP アドレスの表記規則(1-24 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。

脆弱性に対する特定の検索条件

以下の、脆弱性の検索に特有な情報に注意してください。

- Bugtraq ID 番号の検索は http://www.securityfocus.com/bid で行います。
- エクスプロイトされる脆弱性を検索する場合は TRUE を入力し、そのような脆弱性を除外する場合は FALSE を入力します。

サードパーティの脆弱性を検索するには、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　テーブルのドロップダウン リストから [サードパーティの脆弱性（Third-Party Vulnerabilities）] 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。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。オブジェクトを検索条件として使用するには、検索フィールドの隣にある追加アイコン（ ＋ ）をクリックします。

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、デフォルトのサードパーティ脆弱性ワークフローに表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え（switch workflow）] をクリックします。別のデフォルト ワークフローの指定方法については、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。

ユーザの使用

ライセンス：FireSIGHT

Active Directory Agent または管理対象デバイスがデータベースにないユーザのユーザ ログインを検出した場合、そのログイン タイプが特に制限されていない限り、そのユーザはデータベースに追加されます（ユーザ ロギングの制限（45-33 ページ）を参照してください）。

（注）　システムは SMTP ログインを検出しますが、電子メール アドレスが一致するユーザがデータベースにない場合、それらのログインは記録されず、ユーザは、SMTP ログインに基づいたデータベースに追加**されません**。

新しいユーザについてどの情報を格納するかは、次の表に記載されている、システムが検出したログインのタイプによって判断されます。

表 50-13　ログインのタイプと格納されるユーザ データ

ログイン タイプ	格納されるユーザ データ
LDAP AIM Oracle SIP HTTP FTP MDNS	• ユーザ名 • 現行の IP アドレス • ログイン タイプ（`aim`、`ldap`、`oracle`、`sip`、`http`、`ftp`、または `mdns`）
POP3 IMAP	• ユーザ名 • 現行の IP アドレス • 電子メール アドレス • ログイン タイプ（`pop3` または `imap`）

Defense Center と LDAP サーバとの接続を設定すると、Defense Center は LDAP サーバに 5 分ごとに問い合わせして、ユーザ データベースの新しいユーザに関するメタデータを取得します。それと同時に Defense Center は、レコードが Defense Center データベースに格納されており、12 時間以上経過しているユーザの更新情報を LDAP サーバに問い合わせします。システムが新しいユーザのログインを検出してから、Defense Center データベースがユーザ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。Defense Center は LDAP サーバから、各ユーザについて次の情報とメタデータを取得します。

- LDAP ユーザ名
- 姓と名
- 電子メール アドレス
- 部署
- 電話番号

Defense Center がデータベースに格納できるユーザの数は、FireSIGHT のライセンスによって異なります。AIM、Oracle、および SIP のログインは、システムが LDAP サーバから取得したどのユーザ 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 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でのユーザ レコードの重複により、ユーザ カウントが過剰に使用されないようにするために、ネットワーク検出ポリシーではプロトコルのロギングを無効にします。詳細については、ユーザ ロギングの制限（45-33 ページ）を参照してください。

データベースからユーザを検索、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を消去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。

- ユーザの表示（50-66 ページ）
- ユーザ テーブルについて（50-67 ページ）
- ユーザの詳細とホストの履歴について（50-68 ページ）
- ユーザの検索（50-69 ページ）

ユーザの表示

ライセンス：FireSIGHT

ユーザ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が記載されているユーザのテーブル ビューが含まれています。このワークフローは、ユーザの詳細ページで終了します。ユーザの詳細ページは、制約を満たす各ユーザについての情報を提供します。

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 ワークフローの作成方法については、カスタム ワークフローの作成（58-44 ページ）を参照してください。

テーブルのカラムの内容については、ユーザ テーブルについて（50-67 ページ）に詳しく記載されています。次の表は、ユーザ ワークフロー ページで実行できる特定の操作について説明します。一般的なディスカバリ イベントのアクションの表に記載されている操作も実行できます。

ユーザを表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [ユーザ（Users）] > [ユーザ（Users）] を選択します。

デフォルトのユーザ ワークフローの最初のページが表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え（switch workflow）] をクリックします。別のデフォルト ワークフローの指定方法については、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。

ヒント　ユーザのテーブル 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、[ワークフロー切り替え（switch workflow）] をクリックして [ユーザ（Users）] を選択します。

ユーザ テーブルについて

ライセンス：FireSIGHT

システムはユーザを検出したときに、そのユーザに関するデータを収集してデータベースに格納します。次に、ユーザ テーブルのフィールドについて説明します。

ユーザ（User）

次のいずれかになります。

- ユーザの姓、名、およびユーザ名（Defense Center と LDAP サーバの接続を設定した場合に収集されます）
- ユーザ名のみ（Defense Center と LDAP サーバの接続を設定していない場合、または Defense Center が LDAP レコードと相関できなかったユーザの場合）

Defense Center は、ユーザの検出に使用したプロトコルも表示します。

成功しなかった AIM ログインの試行も記録されるため、Defense Center には、（ユーザが入力するユーザ名のスペルを間違っていた場合など）無効な AIM ユーザが格納されている可能性があることに注意してください。

現在の IP（Current IP）

ユーザ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。（あるユーザが権限を持っており、新しいユーザが権限を持っていない場合を除いて）、ユーザがログインした後で、権限を持っている他のユーザが同じ IP アドレスでホストにログインすると、このフィールドは空白になります（システムは、IP アドレスと、最後にホストにログインした権限のあるユーザを関連付けます）。権限のあるユーザと権限のないユーザの詳細については、ユーザ データベース（45-8 ページ）を参照してください。

名

ユーザの名（オプションの Defense Center と LDAP サーバとの接続で取得されたもの）。以下の場合、このフィールドは空白になります。

- Defense Center と LDAP サーバの接続を設定していない
- Defense Center が、Defense Center データベースのユーザと LDAP レコードを相関させていない（AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など）
- LDAP サーバに、対象のユーザと関連付けられている名前がない

姓

ユーザの姓（Defense Center と LDAP サーバの接続を設定した場合に収集されます）。以下の場合、このフィールドは空白になります。

- Defense Center と LDAP サーバの接続を設定していない
- Defense Center が、Defense Center データベースのユーザと LDAP レコードを相関させていない（AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など）
- LDAP サーバに、対象のユーザと関連付けられている姓がない

電子メール(E-Mail)

ユーザのメール アドレス。以下の場合、このフィールドは空白になります。

- AIM ログインによってユーザがデータベースに追加された
- LDAP ログインによってユーザがデータベースに追加されており、LDAP サーバ上にユーザと関連付けられている電子メール アドレスがない

部署名(Department)

ユーザの部門(Defense Center と LDAP サーバの接続を設定した場合に収集されます)。LDAP サーバ上のユーザ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。

- Defense Center と LDAP サーバの接続を設定していない
- Defense Center が、Defense Center データベースのユーザと LDAP レコードを相関させていない(AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など)

電話

ユーザの電話番号(Defense Center と LDAP サーバの接続を設定した場合に収集されます)。以下の場合、このフィールドは空白になります。

- Defense Center と LDAP サーバの接続を設定していない
- Defense Center が、Defense Center データベースのユーザと LDAP レコードを相関させていない(AIM、Oracle、または SIP ログインによってユーザがデータベースに追加された場合など)
- LDAP サーバに、対象のユーザと関連付けられている電話番号がない

ユーザ タイプ(User Type)

ユーザの検出に使用されるプロトコル。たとえば、POP3 ログインを検出したときにデータベースに追加されるユーザの場合、ユーザ タイプは `pop3` になります。

メンバー数(Count)

各ローに示される情報と一致するユーザの数。[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。

ユーザの詳細とホストの履歴について

ライセンス: FireSIGHT

特定のユーザについて詳細を示すために、ユーザのテーブル ビューだけでなく、ユーザ ID データを他の種類のイベントに関連付けているイベント ビューを利用して [ユーザ ID(User Identity)] ポップアップ ウィンドウを表示することができます。ユーザ ワークフローの最終ページには、ユーザの情報も表示されます。

このユーザ データは、ユーザのテーブル ビューで表示されるものと同じです。詳細については、ユーザ テーブルについて(50-67 ページ)を参照してください。

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 アドレスのリストは、ログインとログアウトの回数の概数を棒グラフで示します。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い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、長いセッションとして示されます。

ホストに対して権限のないユーザ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、権限のないユーザがそのホストの現行ユーザとなることが可能です。ただし、ホストに対して権限のあるユーザのログインが検出された後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。ネットワーク検出ポリシーで、失敗したログインのキャプチャを設定した場合、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示されます。

ホストの履歴を生成するの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ています。このデータベースは、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。ホストの履歴で特定のユーザに関するデータが表示されない場合、そのユーザ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さなければならないことが考えられます。詳細については、データベース イベント制限の設定(63-16 ページ)を参照してください。

ユーザの詳細およびホストの履歴を表示するには、以下を行います。

アクセス: Admin/Any Security Analyst

手順 1　以下の 2 つの対処法があります。

- ユーザが示されているいずれかのイベント ビューで、ユーザ ID の隣に示されているユーザ アイコン( )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。

ユーザの詳細が表示されます。

ユーザの検索

ライセンス: FireSIGHT

特定のユーザを検索することができます。実際のネットワーク環境に合わせてカスタマイズされた検索を作成して保存すると、あとで再利用できます。

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。
- いくつかのフィールドでは、フィールドに `n/a` または `blank` を指定して、そのフィールドで情報を使用できないイベントを特定することができます。`!n/a` または `!blank` を使用して、フィールドに値が挿入されるイベントを特定することができます。
- ほとんどのフィールドでは大文字/小文字が区別されません。
- IP アドレスは CIDR 表記を使用して指定できます。FireSIGHT システムへの IPv4 および IPv6 のアドレスの入力については、IP アドレスの表記規則 (1-24 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。

特定のユーザの検索条件

[ユーザ タイプ (User Type)] の有効な検索条件は `ldap`、`pop3`、`imap`、`oracle`、`sip`、`http`、`ftp`、`mdns`、および `aim` です。ユーザは SMTP ログインに基づいてデータベースに追加されることがないため、`smtp` と入力しても結果は返されません。

ユーザを検索するには、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　テーブルのドロップダウン リストから [ユーザ (Users)] を選択します。

[ユーザ検索 (Users search)] ページが表示されます。

ヒント　データベース内で別の種類のイベントを検索するには、テーブルのドロップダウン リストから選択します。

手順 3　該当するフィールドに検索基準を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。

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　制約された権限を持つカスタム ユーザ ロールの制約として検索を保存する場合は、検索を非公開として保存する**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、デフォルトのユーザ ワークフローに表示されます。別のワークフローを使用するには、[ワークフロー切り替え(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、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。

ユーザ アクティビティ の使用

ライセンス: FireSIGHT

FireSIGHT システムは、ネットワーク上のユーザ アクティビティの詳細についてやりとりするイベントを生成します。次に、ユーザ アクティビティの 4 つのタイプについて説明します。

新規ユーザ ID(New User Identity)

このイベントは、システムが、データベースに存在しないユーザのユーザ ログインを検出したときに生成されます。

ユーザ ログイン(User Login)

このイベントは、以下の後に生成されます。

- Active Directory サーバにインストールした Active Directory Agent が LDAP ログインを検出した
- 管理対象デバイスが LDAP、POP3、IMAP、SMTP、AIM、Oracle、FTP、HTTP、MDNS、または SIP のログインを検出した
- ユーザ ログイン イベントについては、以下の点について留意しておく必要があります。
- 一致する電子メール アドレスを持つユーザがすでにデータベースに存在する場合を除いて、SMTP ログインは記録されません。

– 失敗したログインは、トラフィック内で検出された LDAP、IMAP、FTP、および POP3 に限定されます。ログインに失敗すると、検出されたユーザ データベースにユーザは追加されません。ただし、ネットワーク検出ポリシーのユーザ ログインの設定に基づいて、ユーザ アクティビティ データベースにオプションとしてアクティビティが記録されます。

– 特別にログイン タイプを制限している場合は、ユーザ ログインは記録されません。ユーザ ロギングの制限（45-33 ページ）を参照してください。

権限のないユーザがホストにログインすると、そのログインはユーザ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、権限のないユーザがそのホストの現行ユーザとなることが可能です。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。また、権限のないユーザがホストの現行ユーザである場合、そのユーザを使用してユーザ制御を行うことはできません。

ユーザ ID の削除（Delete User Identity）

このイベントは、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。

ユーザ ID のドロップ:ユーザ制限に到達（User Identity Dropped: User Limit Reached）

このイベントは、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、FireSIGHT ライセンスで設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。

Defense Center で保存できる検出済みユーザの総数は、FireSIGHT ライセンスによって異なります。ライセンス制限に達すると、ほとんどの場合、システムはデータベースへの新しいユーザの追加を停止します。新しいユーザを追加するには、古いユーザまたは非アクティブなユーザ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。

システムがユーザ アクティビティを検出すると、そのアクティビティはデータベースに記録されます。ユーザ アクティビティを表示、検索、および削除することも、データベースからすべてのユーザ アクティビティを消去することもできます。

可能な場合はいつでも、FireSIGHT システムがユーザ活動とその他のタイプのイベントを関連付けます。たとえば、侵入イベントは、イベント発生時に送信元ホストおよび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。これにより、攻撃の対象になっていたホストの所有者、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。

また、相関ルールでユーザ アクティビティを使用することもできます。ユーザ アクティビティのタイプだけでなく、自分で指定する他の条件に基づいて、相関ルールを作成することができます。相関ルールは相関ポリシーで使用され、ネットワーク トラフィックが条件を満たしたときに、修復およびアラートの応答を起動します。ユーザ アクティビティの詳細については、ユーザ データ収集について（45-3 ページ）を参照してください。

詳細については、次の項を参照してください。

- ユーザ アクティビティ イベントの表示（50-73 ページ）
- ユーザ アクティビティ テーブルについて（50-73 ページ）
- ユーザ アクティビティの検索（50-74 ページ）

ユーザ アクティビティ イベントの表示

ライセンス：FireSIGHT

ユーザ 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 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 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の詳細が含まれている、ユーザ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 ワークフローの作成方法については、カスタム ワークフローの作成（58-44 ページ）を参照してください。

テーブルのカラムの内容については、ユーザ アクティビティ テーブルについて（50-73 ページ）に詳しく記載されています。次の表は、ユーザ アクティビティのワークフロー ページで実行できる特定の操作について説明しています。一般的なディスカバリ イベントのアクションの表に記載されている操作も実行できます。

ユーザ アクティビティを表示するには、以下を行います。

アクセス：Admin/Any Security Analyst

手順 1　[分析（Analysis）] > [ユーザ（Users）] > [ユーザ アクティビティ（User Activity）] を選択します。

デフォルトのユーザ アクティビティ ワークフローの最初のページが表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え（switch workflow）] をクリックします。別のデフォルト ワークフローの指定方法については、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。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。イベント時間の制約の設定（58-27 ページ）を参照してください。

ヒント　ユーザ 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、[ワークフロー切り替え（switch workflow）] をクリックして [ユーザ アクティビティ（User Activity）] を選択します。

ユーザ アクティビティ テーブルについて

ライセンス：FireSIGHT

システムがユーザ アクティビティを検出すると、そのアクティビティはデータベースに記録されます。次に、ユーザ テーブルのフィールドについて説明します。

時刻（Time）

システムがユーザ アクティビティを検出した時間。

イベント

ユーザ アクティビティのタイプ。詳細については、ユーザ アクティビティ の使用（50-71 ページ）を参照してください。

ユーザ(User)

アクティビティに関連付けられているユーザ。このフィールドには少なくとも、ユーザの検出に使用されたユーザ名とプロトコルが含まれています。ユーザの LDAP メタデータがある場合は、このフィールドには、ユーザの名前と姓も含まれることがあります。

ユーザ タイプ(User Type)

ユーザの検出に使用されるプロトコル。たとえば、システムが POP3 ログインを検出したときにデータベースに追加されるユーザの場合、ユーザ タイプは `pop3` になります。

[IP アドレス(IP Address)]

User Login アクティビティの場合はログインに関連する IP アドレスです。ユーザのホストの IP アドレス(LDAP、POP3、IMAP、FTP、HTTP、MDNS、および AIM ログインの場合)、サーバの IP アドレス(SMTP および Oracle ログインの場合)、またはセッションの開始者の IP アドレス(SIP ログインの場合)のいずれかになります。

関連付けられている IP アドレスは、そのユーザが IP アドレスの現行のユーザであることを意味するわけではないので注意してください。権限を持たないユーザがホストにログインすると、そのログインはユーザおよびホストの履歴に記録されます。権限のあるユーザがホストに関連付けられていない場合、権限のないユーザがそのホストの現行ユーザとなることが可能です。ただし、権限のあるユーザがホストにログインした後は、権限のある別のユーザがログインした場合のみ、現行ユーザが変わります。

他のタイプのユーザ アクティビティの場合、このフィールドは空白です。

説明

ユーザ ID の消去(Delete User Identity)およびユーザ ID のドロップ(User Identity Dropped)アクティビティの場合、データベースから削除されたユーザの名前、またはデータベースへの追加に失敗したユーザの名前になります。ネットワーク リソースへのログインの場合、`network login` が表示されます。他のタイプのユーザ アクティビティの場合、このフィールドは空白です。

Device

管理対象デバイスで検出したユーザ アクティビティの場合は、そのデバイスの名前。他のタイプのユーザ アクティビティの場合は、管理している Defense Center になります。

メンバー数(Count)

各行に表示された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。

ユーザ アクティビティの検索

ライセンス: FireSIGHT

特定のユーザ アクティビティを検索することができます。実際のネットワーク環境に合わせてカスタマイズされた検索を作成して保存すると、あとで再利用できます。

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。
- いくつかのフィールドでは、フィールドに `n/a` または `blank` を指定して、そのフィールドで情報を使用できないイベントを特定することができます。`!n/a` または `!blank` を使用して、フィールドに値が挿入されるイベントを特定することができます。
- ほとんどのフィールドでは大文字/小文字が区別されません。
- IP アドレスは CIDR 表記を使用して指定できます。FireSIGHT システムへの IPv4 および IPv6 のアドレスの入力については、IP アドレスの表記規則(1-24 ページ)を参照してください。
- 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。

ユーザ アクティビティを検索するには、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　テーブルのドロップダウン メニューから [ユーザ アクティビティ(User Activity)] を選択します。

[ユーザ アクティビティの検索(User Activity search)] ページが表示されます。

ヒント　データベース内で別の種類のイベントを検索するには、テーブルのドロップダウン リストから選択します。

手順 3　該当するフィールドに検索基準を入力します。

複数のフィールドに条件を入力して検索すると、すべてのフィールドに対して指定された検索条件に一致するレコードのみが返されます。オブジェクトを検索条件として使用するには、検索フィールドの隣にある追加アイコン(+)をクリックします。

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　制約された権限を持つカスタム ユーザ ロールの制約として検索を保存する場合は、検索を非公開として保存する**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、現行の時間範囲によって制約され、デフォルトのユーザ アクティビティ ワークフローに表示されます。カスタム ワークフローを含む別のワークフローを使用するには、[ワークフロー切り替え(switch workflow)] をクリックします。別のデフォルト ワークフローの指定方法については、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。