ネットワーク検出の概要

FireSIGHT システムは、*ネットワーク検出*と呼ばれる機能を使用して、ネットワーク上のトラフィックを監視し、ネットワーク アセットの包括的な地図を作成します。

管理対象デバイスは指定されたネットワーク セグメント上のトラフィックを受動的に監視するため、システムはネットワーク トラフィックからの特定のパケット 見出し値とその他の一意のデータ(*フィンガープリント*と呼ばれる)を設定された定義と比較し、ネットワーク上のホストの台数と種類(ネットワーク デバイスを含む)だけでなく、それらのホスト上のオペレーティング システム、アクティブ アプリケーション、およびオープン ポートも判断します。

また、ネットワーク上のユーザ活動を監視するように FireSIGHT システムの管理対象デバイスを設定することもできます。これにより、ポリシー違反、攻撃、またはネットワークの脆弱性の発生源を特定できます。

システムによって収集されたデータを補完するために、NetFlow 対応デバイス、Nmap アクティブ スキャン、ホスト入力機能、および Microsoft Active Directory サーバ上に存在し LDAP 認証を報告するユーザ エージェントによって生成されたレコードをインポートできます。FireSIGHT システムは、管理対象デバイスによる直接ネットワーク トラフィック監視を介して、これらのレコードと自ら収集した情報を統合します。

システムは、ネットワーク上のホストで発生した特定タイプの侵入、マルウェア、およびその他のイベントを関連付け、ホストが侵害された可能性がある時点を特定して、そのようなホストに*侵害の兆候*(IOC)タグを付けます。IOC データを使用すれば、監視対象ネットワークのホストに関連する脅威の現状を明確かつ直接的に把握できます。

システムは、この情報のすべてを使用して、科学捜査的分析、行動プロファイリング、アクセス コントロール、および組織が被りやすい脆弱性や悪用に対する対策と対応を支援します。

詳細については、以下を参照してください。

- 検出データ収集について(45-2 ページ)
- NetFlow について(45-18 ページ)
- 侵害の兆候(痕跡)について(45-22 ページ)
- ネットワーク検出ポリシーの作成(45-25 ページ)

検出データ収集について

ライセンス：FireSIGHT

検出データには、ネットワークのホスト、それらのホスト上のオペレーティング システム、アクティブ アプリケーション、およびユーザ活動に関する情報が含まれます。

検出データの収集を開始するには、まず、アクセス コントロール ポリシーを適用する必要があります。アクセス コントロール ポリシーは、許可するトラフィック、つまり、ネットワーク検出で監視可能なトラフィックを定義します。これは、アクセス コントロールを使用して特定のトラフィックをブロックすると、システムでホスト、ユーザ、またはアプリケーションの活動に関するトラフィックを検査できなくなることを意味することに注意してください。たとえば、ソーシャル ネットワーキング アプリケーションへのアクセスをブロックすると、システムからソーシャル ネットワーキング アプリケーションに関する検出データが提供されなくなります。

アクセス コントロール ポリシーの適用後は、管理対象デバイスで監視するネットワーク セグメントとポートと、収集するデータの種類を指定するようにネットワーク検出ポリシーを設定して適用する必要があります。ネットワーク検出ポリシーを適用すると、Defense Center Web インターフェイスを使用して表示または分析が可能な検出データの生成が開始されます。

ネットワーク検出データは Defense Center データベースに保存されます。保存制限の詳細については、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。データベース制限に加えて、Defense Center で保存可能な検出対象のホストとユーザの総数は FireSIGHT ライセンスによって異なります。

ライセンス ユーザ制限に達すると、ほとんどの場合、データベースへの新しいユーザの追加が停止されます。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。一方、ライセンス ホスト制限に達した場合は、データベースへの新しいホストの追加を停止するか、最も長い時間非アクティブのままだったホストを交換するようにシステムを設定できます。

システムによって収集されたデータを補完するために、NetFlow 対応デバイス、Nmap アクティブ スキャン、ホスト入力機能、および Microsoft Active Directory サーバ上に存在し LDAP 認証を報告するユーザ エージェントによって生成されたレコードをインポートできます。FireSIGHT システムは、管理対象デバイスによる直接ネットワーク トラフィック監視を介して、これらのレコードと自ら収集した情報を統合します。

詳細については、以下を参照してください。

- ホスト データ収集について（45-3 ページ）
- ユーザ データ収集について（45-3 ページ）
- アプリケーション検出について（45-11 ページ）
- 侵害の兆候（痕跡）について（45-22 ページ）
- サードパーティ検出データのインポート（45-17 ページ）
- 検出データの用途（45-17 ページ）

ホスト データ収集について

ライセンス：FireSIGHT

システムはネットワークを通過するトラフィックを受動的に監視するため、ネットワーク トラフィックからの特定のパケット ヘッダー値とその他の一意のデータを設定された定義と比較して（*フィンガープリント*と呼ばれる）、ネットワーク上のホストに関する次の情報を判断します。

- ホストの台数と種類（ブリッジ、ルータ、ロード バランサ、NAT デバイスなどのネットワーク デバイスを含む）
- ネットワーク上の検出ポイントからホストまでのホップ数を含む、基本的なネットワーク トポロジ データ
- ホスト上で動作しているオペレーティング システム
- これらのアプリケーションに関連付けられているホストとユーザのアプリケーション

システムでホストのオペレーティング システムを特定できない場合は、カスタム フィンガープリント機能を使用して、カスタム クライアント フィンガープリントまたはカスタム サーバ フィンガープリントを作成できます。システムはこれらのフィンガープリントを使用して新しいホストを特定します。フィンガープリントを脆弱性データベース（VDB）内のシステムにマップすることにより、カスタム フィンガープリントを使用してホストが特定されるたびに適切な脆弱性情報を表示できます。詳細については、カスタム フィンガープリントの使用（46-8 ページ）を参照してください。

また、ホスト入力機能を介してホスト データとオペレーティング システム データを追加または更新することもできます。加えて、ホスト検出が有効な NetFlow 対応検出ルールを作成すれば、NetFlow データからネットワーク マップにホストを追加できます。

システムで検出されたホストを Defense Center Web インターフェイスを使用して表示できます。

- イベント ビューアを使用したホストの表示および検索方法については、ホストの使用（50-21 ページ）を参照してください。
- ネットワーク アセットとトポロジが詳しく記載されたネットワーク マップの表示方法については、ネットワーク マップの使用（48-1 ページ）を参照してください。
- 検出されたホストで利用可能なすべての情報の完全なビューであるホスト プロファイルの表示方法については、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。

ユーザ データ収集について

ライセンス：FireSIGHT

FireSIGHT システムを使用してネットワーク上のユーザ活動を監視できます。これにより、脅威、エンドポイント、およびネットワーク インテリジェンスをユーザ ID 情報に関連付けることができます。ネットワーク動作、トラフィック、およびイベントを個別のユーザに直接リンクすることによって、ポリシー違反、攻撃、またはネットワークの脆弱性の発生源の特定に役立てることができます。つまり、システムが「現象」の背後に存在する「人物」を教えてくれます。たとえば、以下について決定できます。

- 脆弱（レベル 1：赤）影響レベルの侵入イベントの対象になっているホストの所有者
- 内部攻撃またはポートスキャンを開始した人物
- ホスト重要度の高いサーバの不正アクセスを試みている人物

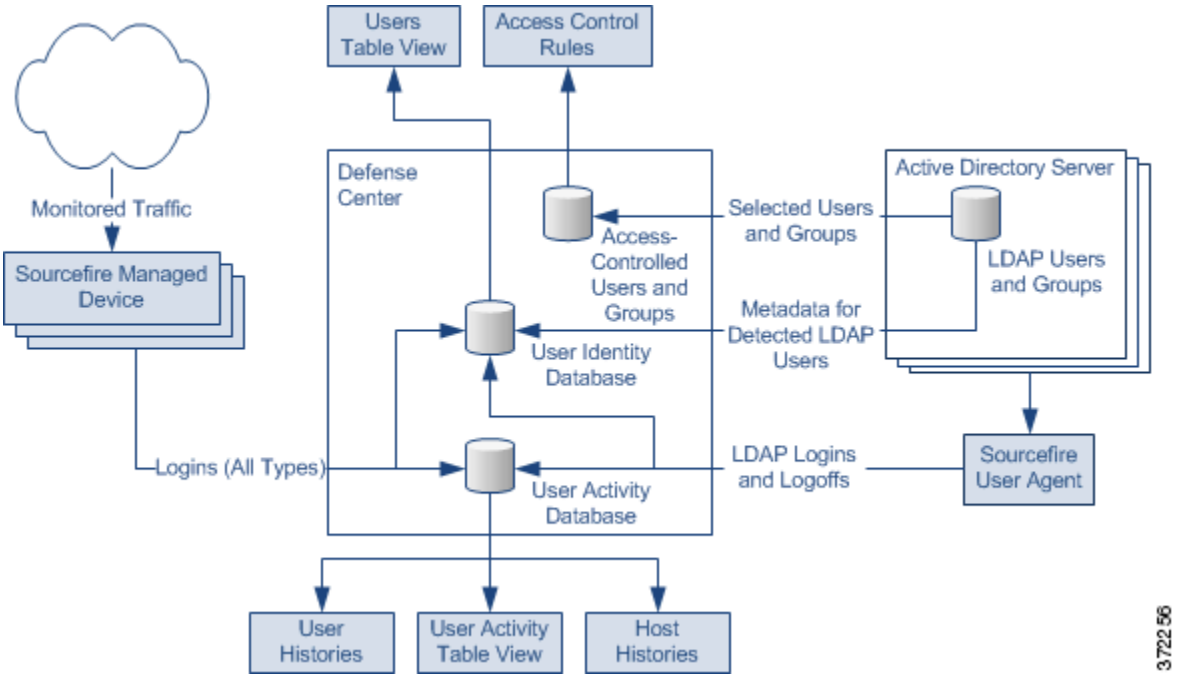
- 不合理な容量の帯域幅を使用している人物
- 重要なオペレーティング システム更新を適用しなかった人物
- 会社の IT ポリシーに違反してインスタント メッセージング ソフトウェアまたはピアツーピア ファイル共有アプリケーションを使用している人物

この情報を入手すれば、リスクを軽減したり、ユーザまたはユーザ活動をブロックしたり、その他の人を混乱させない措置を講じたりするための的を絞ったアプローチを使用できます。これらの機能により、監査制御が大幅に改善され、規制の順守が促進されます。

システムが LDAP 接続内のユーザ認識設定に基づいて Microsoft Active Directory LDAP サーバからアクセス コントロール ポリシー内で使用されているユーザをダウンロードします。その後で、ユーザ エージェントがこれらのユーザに関するログイン データを提供し、ユーザがユーザ データベースに追加されます。これらのユーザは *アクセス制御対象ユーザ*と呼ばれます。ユーザ条件を含むアクセス コントロール ポリシーを作成するときに、アクセス制御対象ユーザに対する条件を書き込みます。詳細については、アクセス コントロール ルールへのユーザ条件の追加 (17-3 ページ)を参照してください。

システムがユーザ ログイン、ユーザ エージェント、トラフィックで検出されたアプリケーション データ、あるいは POP3、SMTP、または IMAP 経由の電子メール ログインからユーザ データを検出すると、ユーザのリストに照らしてログインからのユーザがチェックされます。ログイン ユーザがエージェントから報告された既存のユーザと一致した場合は、ログインからのデータがそのユーザに割り当てられます。ログインが SMTP トラフィック内に存在しない場合は、既存のユーザと一致しないログインによって新しいユーザが作成されます。SMTP トラフィック内の一致しないログインは破棄されます。

次の図は、FireSIGHT システムがユーザ データをどのように収集して保存するかを示しています。



図に示すように、ユーザ データの 3 つの発生源と、そのデータが保存される 3 つの場所があります。ユーザ データ収集の詳細については、以下を参照してください。

管理対象デバイス

ライセンス：FireSIGHT

ネットワーク検出ポリシーを使用して、指定されたネットワーク上で LDAP、AIM、POP3、IMAP、Oracle、SIP（VoIP）、FTP、HTTP、MDNS および SMTP ログインを受動的に検出するように管理対象デバイスを設定します。ネットワーク検出ルールでユーザの検出を有効にすると、ホスト検出が自動的に有効になることに注意してください。

（注） 管理対象デバイスは、LDAP 接続に対する Kerberos ログインのみを LDAP 認証として解釈します。また、管理対象デバイスは、SSL や TLS などのプロトコルを使用して暗号化された LDAP 認証を検出できません。

デバイスがログインを検出すると、次の情報をユーザ活動として記録するために Defense Center に送信します。

- ログインで識別されたユーザ名
- ログインの時刻
- ログインに関係する IP アドレス。このアドレスは、ユーザのホスト（LDAP、POP3、IMAP、および AIM ログインの場合）、サーバ（HTTP、MDNS、FTP、SMTP および Oracle ログインの場合）、またはセッション発信元（SIP ログインの場合）の IP アドレスになります。
- ユーザの電子メール アドレス（POP3、IMAP、および SMTP ログインの場合）
- ログインを検出したデバイスの名前

ユーザがすでに検出されている場合、Defense Center はそのユーザのログイン履歴を更新します。Defense Center は POP3 および IMAP ログイン内の電子メール アドレスを使用して LDAP ユーザに関連付けることができることに注意してください。これは、Defense Center が新しい IMAP ログインを検出して、その IMAP ログイン内の電子メール アドレスが既存の LDAP ユーザのアドレスと一致した場合は、IMAP ログインで新しいユーザが作成されるのではなく、LDAP ユーザの履歴が更新されることを意味します。

そのユーザがこれまで検出されたことがなければ、Defense Center がそのユーザをデータベースに追加します。AIM、SIP、および Oracle ログインでは一意のにそれぞれ、新しいユーザ レコードが作成されます。これは、それらのログイン イベントには Defense Center が他のログイン タイプに関連付けることができるデータが含まれていないためです。

Defense Center は、次の場合に、ユーザ活動またはユーザ ID を記録**しません**。

- ユーザ ロギングの制限（45-33 ページ）の説明に従って、そのログイン タイプを無視するようにネットワーク検出ポリシーを設定した場合
- 管理対象デバイスが SMTP ログインを検出したものの、ユーザ データベースに電子メール アドレスが一致する、検出済みの LDAP、POP3、または IMAP ユーザが含まれていない場合

ユーザ エージェント

ライセンス：FireSIGHT

組織で Microsoft Active Directory LDAP サーバが使用されている場合、ユーザ エージェントをインストールし、Active Directory サーバを介してユーザ アクティビティをモニタすることを シスコ では推奨しています。ユーザ制御を実行する場合は、ユーザ エージェントをインストールして使用する**必要があります**。エージェントがユーザと IP アドレスを関連付けるため、ユーザ条件を含むアクセス コントロール ルールでトリガーできます。1 つのエージェントを使用して、最大 5 つの Active Directory サーバでユーザ アクティビティをモニタできます。

エージェントを使用するには、エージェントに接続された各 Defense Center と監視対象 LDAP サーバ間の接続を設定する必要があります。この接続は、ログインとログオフがユーザ エージェントによって検出されたユーザのメタデータを取得可能にするだけでなく、アクセス コントロール ルール内で使用するユーザとグループを指定するためにも使用されます。ユーザ検出用の LDAP サーバの設定方法については、アクセス制御されたユーザおよび LDAP ユーザのメタデータの取得（17-4 ページ）を参照してください。

各エージェントは、定期的にスケジュールされたポーリングまたはリアルタイム モニタリングによって、暗号化トラフィックを使用するログインをモニタできます。ログインは、ユーザがワークステーションで、またはリモート デスクトップ ログインを介してコンピュータにログインしたときに、Active Directory サーバによって生成されます。

エージェントは、ユーザ ログオフをモニタして報告することもできます。ログオフは、ユーザがホスト IP アドレスからログアウトしたことをエージェントが検出したときに、エージェント自体によって生成されます。ログオフは、ホストにログインしているユーザが変更されたことを Active Directory サーバが報告する前に、エージェントが検出したときにも生成されます。ログイン データとログオフ データを組み合わせることで、ネットワークにログインしたユーザをより完全に把握できます。

Active Directory サーバのポーリングによって、エージェントは定義されたポーリング間隔でユーザ アクティビティ データをまとめて取得できます。リアルタイム モニタリングでは、Active Directory サーバがユーザ アクティビティ データを受信した直後に、エージェントにそのデータが送信されます。

特定のユーザ名または IP アドレスに関連付けられたログインまたはログオフの報告を除外するようにエージェントを設定できます。これは、ファイル共有やプリント サーバなどの共有サーバに対する反復ログインを除外したり、トラブルシューティングのためにマシンにログインしているユーザを除外したりする場合に役立ちます。

エージェントは除外するユーザ名または IP アドレスが含まれていない検出されたすべてのログインとログオフのレコードを Defense Center に送信し、レコードはそこでユーザ活動として記録および報告されます。エージェントは、Defense Center のバージョンを検出し、ログイン レコードを適切なデータ形式で送信します。これにより、管理対象デバイスで直接検出されたユーザ アクティビティが補完されます。ユーザ エージェントから報告されたログインによって、ユーザと IP アドレスが関連付けられるため、ユーザ条件を含むアクセス コントロール ルールをトリガーできます。

ユーザ エージェントは、ネットワークにログインしたとき、または、他の理由でアカウントが Active Directory 資格情報に照らして認証されたときにユーザを監視します。ユーザ エージェントのバージョン 2.1 は、ホストに対する対話型ユーザ ログイン、リモート デスクトップ ログイン、ファイル共有認証、およびコンピュータ アカウント ログインだけでなく、ユーザ ログオフとユーザがログオフしたリモート デスクトップ セッションも検出します。

検出されたログインのタイプによって、エージェントがログインをどのように報告するかと、ログインがホスト プロファイルでどのように表示されるかが決まります。ホストに対する *権限のあるユーザ ログイン* によって、ホスト IP アドレスにマップされた現在のユーザが新しいログインからのユーザに変更されます。他のログインでは、現在のユーザが変更されないか、ホスト上の既存のユーザにホストに対する権限のあるユーザ ログインが付与されていない場合にホストの現在のユーザだけが変更されるかのどちらかです。このようなケースでは、想定していたユーザがすでにログインしていなければ、エージェントがそのユーザのログオフを生成します。ネットワーク検出によって検出されたユーザ ログインでは、ホスト上の既存のユーザにホストに対する権限のあるユーザ ログインが付与されていない場合にホストの現在のユーザだけが変更されます。エージェント検出ログインはネットワーク マップに次のような影響を与えます。

- エージェントがユーザまたはリモート デスクトップ ログインによるホストに対する対話型ログインを検出した場合は、ホストに対する権限のあるユーザ ログインを報告して、ホストの現在のユーザを新しいユーザに変更します。
- ファイル共有認証のログインを検出した場合、エージェントはホストに対するユーザ ログインを報告しますが、ホストの現在のユーザは変更しません。
- ホストへのコンピュータ アカウントのログインを検出した場合、エージェントは NetBIOS 名変更のディスカバリ イベントを生成し、NetBIOS 名の変更をホスト プロファイルに反映します。
- 除外されたユーザ名のログインを検出した場合、エージェントは Defense Center にログインを報告しません。

ログインまたはその他の認証が実行されると、エージェントは次の情報を Defense Center に送信します。

- ユーザの LDAP ユーザ名
- ログインまたはその他の認証の時刻
- ユーザのホストの IP アドレス、およびエージェントがコンピュータ アカウント ログインの IPv6 アドレスを報告した場合のリンクローカル アドレス

Defense Center は、ログイン情報とログオフ情報をユーザ活動として記録します。ユーザ エージェントがユーザ ログインまたはログオフからのユーザ データを報告すると、報告されたユーザがユーザのリストに照らしてチェックされます。報告されたユーザがエージェントから報告された既存のユーザと一致した場合、報告されたデータがそのユーザに割り当てられます。報告されたユーザが既存のユーザと一致しなかった場合、新しいユーザが作成されます。

除外されたユーザ名に関連付けられたユーザ アクティビティは報告されませんが、関連するユーザ アクティビティは報告される場合があります。エージェントがマシンへのユーザ ログインを検出し、その後 2 人目のユーザ ログインを検出したときに、2 人目のユーザ ログインに関連付けられたユーザ名が報告対象から除外されていた場合、エージェントは元のユーザのログオフを報告します。ただし、2 人目のユーザのログインは報告されません。その結果、除外されたユーザがホストにログインしていた場合でも、IP アドレスにユーザはマップされません。

エージェントによって検出されるユーザ名の次の制限に注意してください。

- Defense Center に報告されるドル記号($)で終わるユーザ名は、ネットワーク マップを更新しますが、ユーザ ログインとして表示されません。
- Defense Center では、Unicode 文字を含むユーザ名の表示が制限される場合があります。

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 ユーザ制限に達した後、ほとんどの場合、データベースへの新しいユーザの追加が停止されます。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。

Defense Center と LDAP サーバ間の接続

ライセンス：FireSIGHT

Defense Center と LDAP サーバ間の接続を使用すれば、検出された特定のユーザのメタデータを取得できます。LDAP ユーザのメタデータとして、ログインが管理対象デバイスによって検出されたのか、ユーザ エージェントによって検出されたのかを取得できます。また、POP3 ユーザと IMAP ユーザのメタデータとして、それらのユーザが LDAP ユーザと同じ電子メール アドレスを持っているかどうかを取得できます。

組織で Microsoft Active Directory サーバを使用している場合は、接続を通して、アクセス コントロール ルールで使用する LDAP ユーザとグループを指定できます。ユーザ制御を実行する場合は、Defense Center と Active Directory サーバの接続を設定する**必要があります**。組織で Active Directory を使用していない場合でも、管理対象デバイスを使用してユーザ ログインを検出し、Oracle または OpenLDAP サーバから一部のユーザのメタデータを取得できます。ただし、これらのユーザまたはその活動に基づいてユーザ制御を実行することはできません。

Defense Center は LDAP サーバから、それぞれのユーザに関する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

ユーザ データベース

ライセンス：FireSIGHT

ユーザ データベースには、管理対象デバイスまたはユーザ エージェントで検出された各ユーザのレコードが格納されます。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、システムは権限のあるユーザ ログインを特別扱いします。制限に達してから、システムが未検出だったユーザの権限のあるユーザ ログインを検出した場合は、最も長い時間非アクティブのままだった権限のないユーザを削除して新しいユーザに置き換えます。

Defense Center Web インターフェイスを使用してユーザ データベースの内容を表示できます。検出されたユーザの表示、検索、および削除の方法については、ユーザの使用（50-65 ページ）を参照してください。

ユーザ アクティビティ データベース

ライセンス：FireSIGHT

ユーザ アクティビティ（活動）データベースには、ネットワーク上のユーザ アクティビティのレコードが格納されます。これらのアクティビティは、ユーザ エージェントが監視している Active Directory LDAP サーバとの接続から取得されるか、またはネットワーク ディスカバリによって取得されます。システムがイベントを記録するのは以下のような状況です。

- 個別のログインまたはログオフを検出したとき
- 新しいユーザを検出したとき
- 手動でユーザが削除されたとき
- データベース内に存在しないユーザをシステムが検出したものの、FireSIGHT のライセンス制限に達したためにそのユーザを追加できなかったとき

システムで検出されたアクティビティ（活動）を Defense Center Web インターフェイスを使用して表示できます。ユーザ アクティビティの表示、検索、および削除の方法については、ユーザ アクティビティ の使用（50-72 ページ）を参照してください。ユーザ エージェントのバージョン 2.1 を使用して LDAP ログイン データを Defense Center に送信する場合は、エージェントを接続する各 Defense Center 上でそれぞれのエージェント用の接続を設定する必要があります。エージェントはこの接続を使用して、ログイン データを送信可能なDefense Center とのセキュアな接続を確立することができます。エージェントが特定のユーザ名を除外するように設定されている場合は、そのようなユーザ名のログイン データは Defense Center に報告されません。

加えて、ユーザ アクセス コントロールを実装する場合は、データを収集する各 Microsoft Active Directory サーバへの接続を、ユーザ認識パラメータを設定してセットアップする必要があります。

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。

システムは、ユーザ活動を使用して、各ユーザがログインしていたホストを追跡する*ホスト履歴*と個別のホストにログインしていたユーザを追跡する*ユーザ履歴*も生成します。また、過去 24 時間の各ユーザの活動と過去 24 時間の各ホストへのログインがグラフで表示されます。詳細については、ユーザの詳細とホストの履歴について（50-69 ページ）およびホスト プロファイルでのユーザ履歴の使用（49-25 ページ）を参照してください。

アクセス制御対象ユーザ データベース

ライセンス：Control

アクセス制御対象ユーザ データベースには、FireSIGHT システムでユーザ制御を実行するためのアクセス コントロール ルールで使用できるユーザとグループが格納されます。これらのユーザは次の 2 つのタイプに分けられます。

- *アクセス制御対象ユーザ*は、アクセス コントロール ルールに追加してユーザ制御を実行可能なユーザです。Defense Center と LDAP サーバ間の接続を設定するときに、アクセス制御対象ユーザを追加する必要があるグループを指定します。
- *非アクセス制御対象ユーザ*は、検出されたその他のユーザです。

アクセス制御されたユーザおよび LDAP ユーザのメタデータの取得（17-4 ページ） の説明に従って、Defense Center と LDAP サーバ間の接続を設定するときに、アクセス制御対象ユーザを追加する必要があるグループを指定します。

ユーザ エージェントのバージョン 2.1 を使用して LDAP ログインおよびログオフ データをバージョン 5.x Defense Center に送信する場合は、エージェントを接続する各 Defense Center 上でそれぞれのエージェント用の接続を設定する必要があります。エージェントはこの接続を使用して、ユーザ アクティビティ データを送信可能な Defense Center とのセキュアな接続を確立することができます。

エージェントが特定のユーザ名を除外するように設定されている場合は、そのようなユーザ名のユーザ アクティビティ データは Defense Center に報告されません。これらの除外されたユーザ名はデータベースに残りますが、IP アドレスに関連付けられません。

加えて、ユーザ アクセス コントロールを実装する場合は、データを収集する各 Microsoft Active Directory サーバへの接続を、ユーザ認識パラメータを設定してセットアップする必要があります。

アクセス コントロールで使用可能なユーザの最大数は FireSIGHT ライセンスによって異なります。Defense Center と LDAP サーバ間の接続を設定するときに、含まれているユーザの総数が FireSIGHT ユーザ ライセンスの数より少ないことを確認してください。詳細については、FireSIGHT ホストおよびユーザ ライセンスの制限について（65-9 ページ）を参照してください。

ユーザ データ収集の制限

ライセンス：FireSIGHT

次の表に、ユーザ データ収集の制限事項を示します。

表 45-1　ユーザ認識の制限事項

制限事項	説明
ユーザ制御	ユーザ制御を実行するには、組織で Microsoft Active Directory LDAP サーバを使用している**必要があります**。システムは、Active Directory からアクセス コントロール ルールで使用可能なユーザとグループを取得し、Active Directory サーバにインストールされたユーザ エージェントから報告されたログインとログオフを使用してユーザを IP アドレスに関連付けます。
LDAP 接続用の非 Kerberos ログイン	管理対象デバイスは、LDAP 接続に対する Kerberos ログインのみを LDAP 認証として解釈します。管理対象デバイスは、SSL や TLS などの他のプロトコルが使用されている場合に、暗号化された LDAP 認証を検出できません。 一方、ユーザ エージェントは Active Directory サーバ上のセキュリティ ログを使用してユーザ ログイン データを収集するため、このような制限がありません。
ログイン検出	Active Directory サーバへのログインを検出する場合は、サーバの IP アドレスを使用して Active Directory サーバの接続を設定する必要があります。詳細については、『*User Agent Configuration Guide*』を参照してください。 複数のユーザがリモート セッションを使用してホストにログインしている場合は、エージェントがそのホストからのログインを正確に検出しない場合があります。これを回避する方法については、『*User Agent Configuration Guide*』を参照してください。
ログオフ検出	ログオフはすぐに検出されない場合があります。ログオフに関連付けられたタイムスタンプは、ユーザがホスト IP アドレスにマップされなくなったことをエージェントが検出した時点を反映しているため、ユーザがホストからログオフした実際の時間と対応しない可能性があります。 ログオフは、ユーザがホスト IP アドレスからログアウトしたことをエージェントが検出したときに、エージェント自体によって生成されます。ログオフは、ホストにログインしているユーザが変更されたことを Active Directory サーバが報告する前に、エージェントが検出したときにも生成されます。

表 45-1　ユーザ認識の制限事項（続き）

制限事項	説明
リアルタイム データの取得	Active Directory サーバで Windows Server 2008 または Windows Server 2012 が実行されている必要があります。
複数のユーザによる同じホストへの複数のログイン	システムは、特定のホストにログインするユーザは一度に 1 人だけであり、ホストの現在のユーザが最後の権限のあるユーザ ログインであると見なします。ホストにログインしているのが権限のないログインだけの場合は、最後の権限のないログインが現在のユーザと見なされます。複数のユーザがリモート セッション経由でログインしている場合は、Active Directory サーバによって報告された最後のユーザが Defense Center に報告されるユーザです。
同じユーザによる同じホストへの複数のログイン	システムは、ユーザが初めて特定のホストにログインした時点を記録し、それ以降のログインを無視します。あるユーザが特定のホストにログインしている唯一の人物の場合は、システムが記録する唯一のログインがオリジナルのログインです。 ただし、そのホストに別のユーザがログインした時点で、システムは新しいログインを記録します。その後で、オリジナルのユーザが再度ログインすると、その人物の新しいログインが記録されます。
Unicode 文字	Unicode 文字を含むユーザ名は、ユーザ インターフェイスに正しく表示されない場合があります。
ユーザデータベース内の LDAP ユーザ アカウント	LDAP サーバで LDAP ユーザを削除または無効化するか、あるいは Defense Center に報告する対象からユーザ名を除外した場合、Defense Center はユーザ データベースからそのユーザを削除せず、そのユーザは引き続きデータベースに登録されるユーザのライセンス制限に照らしてカウントされます。データベースからユーザを手動で消去する必要があります。 ユーザ ライセンス制限がアクセス制御対象ユーザにも同時に適用されることに注意してください。アクセス制御対象ユーザのユーザ カウントは LDAP 設定で取得されたユーザ数によって異なります。
AOL Instant Messenger（AIM）ログイン検出	管理対象デバイスは OSCAR プロトコルを使用した AIM ログインだけを検出できます。ほとんどの AIM クライアントが OSCAR を使用するのに対して、一部のクライアントは TOC2 を使用します。

アプリケーション検出について

ライセンス：FireSIGHT

FireSIGHT システムは IP トラフィックを分析するときに、ネットワーク上でよく使用されているアプリケーションを特定しようとします。アプリケーション認識は、アプリケーション ベースのアクセス コントロールを行うために不可欠です。

システムによって検出されるアプリケーションには以下の 3 種類があります。

- HTTP や SSH などのホスト間の通信を表す*アプリケーション プロトコル*
- Web ブラウザや電子メール クライアントなどのホスト上で動作しているソフトウェアを表す*クライアント*
- HTTP トラフィックの内容または要求された URL を表す MPEG ビデオや Facebook などの *Web アプリケーション*

システムは、パケット 見出し内の ASCII または 16 進パターン、あるいは、トラフィックで使用されたポートを使用して、ネットワーク トラフィック内のアプリケーションを特定します。一部のアプリケーション ディテクタはポートおよびパターンの検出の両方を使用して、特定のアプリケーションのトラフィックを正しく識別する可能性を高めています。加えて、Secure Socket Layer（SSL）プロトコル ディテクタは、セキュアなセッションからの情報を使用して、セッションからアプリケーションを識別します。FireSIGHT システム内のアプリケーション ディテクタの供給元には次の 2 つがあります。

- *シスコ提供ディテクタ*。Web アプリケーション、クライアント、およびアプリケーション プロトコルを検出します

  アプリケーション（およびオペレーティング システム、ホスト データ収集について（45-3 ページ）を参照）に対する シスコ提供ディテクタの可用性は、インストールされている FireSIGHT システムのバージョンと VDB のバージョンによって異なります。リリース ノートとアドバイザリに、新しいディテクタと更新されたディテクタに関する情報が記載されています。また、プロフェッショナル サービスが作成した個別のディテクタをインポートすることもできます。検出されるアプリケーションの完全なリストについては、サポート サイトを参照してください。

- *ユーザ定義アプリケーション プロトコル ディテクタ*。システムのアプリケーション プロトコル検出機能を強化するために作成できます

また、*暗黙的アプリケーション プロトコル検出*を通してアプリケーション プロトコルを検出することもできます。これは、クライアントの検出に基づいてアプリケーション プロトコルの存在を暗示するものです。

システムは、次の表に示す基準を使用して、検出したアプリケーションのそれぞれを特徴付けます。また、これらの特徴を利用して、アプリケーション フィルタまたはアプリケーション グループを作成します。これらのフィルタと独自に作成したフィルタを使用して、アクセス コントロールを実行したり、検索、レポート、およびダッシュボード ウィジェットを制限したりできます。詳細については、アプリケーション フィルタの操作（3-16 ページ）を参照してください。

:

表 45-2　アプリケーションの特徴

特性	説明	例
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**は、ホスト上で動作しているソフトウェアを意味します。 • **Web アプリケーション**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。	HTTP と SSH はアプリケーション プロトコルです。 Web ブラウザと電子メール クライアントはクライアントです。 MPEG ビデオと Facebook は Web アプリケーションです。
リスク	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。	ピアツーピア アプリケーションはリスクが極めて高いと見なされます。
ビジネスとの関連性	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。	ゲーム アプリケーションはビジネス関連性が非常に低いと見なされます。

表 45-2　アプリケーションの特徴（続き）

特性	説明	例
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。	Facebook は**ソーシャル ネットワーキング**のカテゴリに入ります。
タグ	アプリケーションに関する追加情報。アプリケーションには任意の数（0 個を含む）のタグを付けることができます。	ビデオ ストリーミング Web アプリケーションには、大抵、**high bandwidth** と **displays ads** というタグが付けられます。

システムによって収集されたアプリケーション データを補完するために、NetFlow 対応デバイス、Nmap アクティブ スキャン、およびホスト入力機能によって生成されたレコードを使用できます。

詳細については、以下を参照してください。

- アプリケーション プロトコル検出プロセスについて（45-13 ページ）
- クライアント検出からの暗黙的アプリケーション プロトコル検出（45-15 ページ）
- アプリケーション プロトコル検出に関する特記事項：Squid（45-15 ページ）
- 特記事項：SSL アプリケーション検出（45-16 ページ）
- 特記事項：照会先 Web アプリケーション（45-16 ページ）
- アプリケーション ディテクタの操作（46-19 ページ）
- サードパーティ検出データのインポート（45-17 ページ）
- NetFlow について（45-18 ページ）

アプリケーション プロトコル検出プロセスについて

ライセンス：FireSIGHT

システムがアプリケーション トラフィックを検出すると、まず、その特定のポートを唯一の検出基準として使用するディテクタによって特定されたポート上でアプリケーション プロトコルが動作しているかどうかを判断します。アプリケーション プロトコルがそのようなポートの 1 つで動作している場合、システムは既知のポート ディテクタを使用してアプリケーション プロトコルを肯定的に識別します。

（注） シスコ提供のディテクタによって使用されるポート上でユーザ定義のポート ベース アプリケーション プロトコル ディテクタを作成してアクティブ化することができるため、シスコの検知機能がオーバーライドされる可能性があります。たとえば、ユーザ定義のディテクタがポート 22 上のすべてのアプリケーション プロトコル トラフィックを `myapplication` アプリケーション プロトコルとして識別する場合は、ポート 22 上の SSH トラフィックが `myapplication` トラフィックとして誤って識別されます。

アプリケーション プロトコルがそのようなポートの 1 つで動作していない場合は、システムがポート照合とパターン照合に基づいて識別するより確実な方法を採用します。2 つのディテクタが両方ともトラフィックを肯定的に識別する場合は、より長いパターン照合を採用しているディテクタが優先されます。同様に、複数のパターン照合を使用したディテクタは単一のパターン照合より優先されます。

ネットワーク検出ポリシーで定義されているように、システムは監視対象ネットワーク内のホスト上で動作しているアプリケーション プロトコルだけを識別することに注意してください。たとえば、監視されていないリモート サイト上の FTP サーバに内部ホストがアクセスする場合、システムはアプリケーション プロトコルを FTP として識別しません。一方、監視されているホスト上の FTP サーバにリモートまたは内部ホストがアクセスする場合、システムはアプリケーション プロトコルを肯定的に識別できます。

例外は、監視対象ホストがアクセスしている非監視対象サーバとの間の接続に使用しているクライアントをシステムが識別できる場合です。この場合、システムは、接続内のクライアントに対応する適切なアプリケーション プロトコルを肯定的に識別しますが、そのアプリケーション プロトコルをネットワーク マップに追加しません。詳細については、クライアント検出からの暗黙的アプリケーション プロトコル検出（45-15 ページ）を参照してください。アプリケーション検出が発生するためには、クライアント セッションにサーバからの応答が含まれている必要があることに注意してください。

次の表に、FireSIGHT システムが Defense Center Web インターフェイスで検出されたアプリケーション プロトコルを識別する方法（ネットワーク マップ、ホスト プロファイル、イベント ビューなど）の概要を示します。

表 45-3　FireSIGHT システムのアプリケーション プロトコルの識別

アプリケーション	説明
アプリケーション プロトコル名	Defense Center は、次のアプリケーション プロトコルの場合に、名前でアプリケーション プロトコルを識別します。 • システムによって肯定的に識別された • NetFlow データを使用して識別され、`/etc/sf/services` にポートとアプリケーション プロトコルの関連付けが存在する • ホスト入力機能を使用して手動で識別された • Nmap または別のアクティブな発生源によって識別された
`pending`	Defense Center は、システムが肯定的と否定的のどちらでもアプリケーションを識別できない場合に、アプリケーション プロトコルを `pending` として識別します。 大抵の場合、システムはより多くの接続データ（アプリケーションが識別される）を収集して分析しないと、pending アプリケーションを識別できません。 [アプリケーションの詳細（Application Details）] テーブル、[サーバ（Servers）] テーブル、およびホスト プロファイルで `pending` ステータスが表示されるのは、特定のアプリケーション プロトコル トラフィック（クライアントまたは Web アプリケーション トラフィック以外の）が検出されたアプリケーション プロトコルだけです。
`unknown`	Defense Center は、アプリケーションが以下の場合にアプリケーション プロトコルを `unknown` として識別します。 • システムのディテクタのどれとも一致しない • アプリケーション プロトコルが NetFlow データを使用して識別されたものの、`/etc/sf/services` にポートとアプリケーション プロトコルの関連付けが存在しない
blank	使用可能なすべての検出データが検証されましたが、アプリケーション プロトコルが識別されませんでした。[アプリケーションの詳細（Application Details）] テーブル、[サーバ（Servers）] テーブル、およびホスト プロファイルでは、アプリケーション プロトコルが検出されなかった非 HTTP 汎用クライアント トラフィックに対して、アプリケーション プロトコルが空白として表示されます。

クライアント検出からの暗黙的アプリケーション プロトコル検出

ライセンス：FireSIGHT

監視対象ホストがアクセスしている非監視対象サーバとの間の接続に使用しているクライアントをシステムが識別できる場合、Defense Center はその接続でクライアントに対応するアプリケーション プロトコルが使用されていると推測します。（システムは監視対象ネットワーク上のアプリケーションだけを追跡するため、通常、接続ログには監視対象ホストが非監視対象サーバにアクセスしている接続に関するアプリケーション プロトコル情報が含まれていません。）

クライアントの検出からのアプリケーション プロトコルの暗黙的検出の結果は複数存在します。

- システムはこれらのサーバの New TCP Port イベントまたは New UDP Port イベントを生成しないため、サーバが [サーバ（Servers）] テーブルに表示されません。加えて、これらのアプリケーション プロトコルの検出を基準にして、検出（ディスカバリ）イベント アラートまたは相関ルールをトリガーすることはできません。
- アプリケーション プロトコルはホストに関連付けられないため、ホスト プロファイルの詳細を表示したり、サーバ ID を設定したり、トラフィック プロファイルまたは相関ルールに関するホスト プロファイル資格内の情報を使用したりできません。加えて、システムはこの種の検出に基づいて脆弱性とホストを関連付けません。

ただし、接続内のアプリケーション プロトコル情報に対する相関イベントをトリガーできます。また、接続ログ内のアプリケーション プロトコル情報を使用して、接続トラッカーとトラフィック プロファイルを作成できます。

ホスト制限と検出イベント ロギング

ライセンス：FireSIGHT

システムがクライアント、サーバ、または Web アプリケーションを検出すると、関連するホストがすでにクライアント、サーバ、または Web アプリケーションの最大数に達していなければ、検出イベントが生成されます。

ホスト プロファイルには、ホストごとに最大 16 のクライアント、100 のサーバ、および 100 の Web アプリケーションが表示されます。詳細については、ホスト プロファイルでのサーバの使用（49-17 ページ）と ホスト プロファイルでのアプリケーションの表示（49-23 ページ）を参照してください。

クライアント、サーバ、または Web アプリケーションの検出によって異なるアクションはこの制限の影響を受けないことに注意してください。たとえば、サーバ上でトリガーするように設定されたアクセス コントロール ルールでは、引き続き、接続イベントが記録されます。

アプリケーション プロトコル検出に関する特記事項：Squid

ライセンス：FireSIGHT

システムは、次のいずれかの場合に Squid サーバ トラフィックを肯定的に識別します。

- 監視対象ネットワーク上のホストからプロキシ認証が有効になっている Squid サーバへの接続をシステムが検出した場合
- 監視対象ネットワーク上の Squid プロキシ サーバからターゲット システム（つまり、クライアントが情報または別のリソースを要求する宛先サーバ）への接続をシステムが検出した場合

ただし、システムは次の場合に Squid サービス トラフィックを識別できません。

- 監視対象ネットワーク上のホストが、プロキシ認証が無効になっている Squid サーバに接続している場合
- Squid プロキシ サーバが HTTP 応答から Via: 見出し フィールドを除去するように設定されている場合

特記事項:SSL アプリケーション検出

ライセンス: FireSIGHT

FireSIGHT システムは、Secure Socket Layer(SSL)セッションからのセッション情報を使用してセッション内のアプリケーション プロトコル、クライアント アプリケーション、または Web アプリケーションを識別するディテクタを備えています。

システムは暗号化された接続を検出すると、その接続を汎用 HTTPS 接続として、または、該当する場合に、SMTPS などのより特殊なセキュア プロトコルとしてマークします。システムは SSL セッションを検出すると、そのセッションに対する接続イベント内の **Client** フィールドに `SSL client` を追加します。セッションの Web アプリケーションが識別されると、システムでトラフィックの検出イベントが生成されます。

SSL アプリケーション トラフィックの場合は、管理対象デバイスも、サーバ証明書から一般名を検出して SSL ホスト パターンからのクライアントまたは Web アプリケーションと照合できます。システムが特定のクライアントを識別すると、`SSL client` をそのクライアントの名前に置き換えます。

SSL アプリケーション トラフィックは暗号化されるため、システムは暗号化されたストリーム内のアプリケーション データではなく、証明書内の情報しか識別に使用できません。そのため、SSL ホスト パターンではアプリケーションを制作した会社しか識別できない場合があり、同じ会社が作成した SSL アプリケーションは識別情報が同じ可能性があります。

HTTPS セッションが HTTP セッション内から起動される場合などは、管理対象デバイスがクライアント側のパケット内のクライアント証明書からサーバ名を検出します。

SSL アプリケーション識別を有効にするには、応答側のトラフィックを監視するアクセス コントロール ルールを作成する必要があります。このようなルールには、SSL アプリケーションに関するアプリケーション条件または SSL 証明書からの URL を使用した URL 条件を含める必要があります。ネットワーク検出では、応答側の IP アドレスがネットワーク上に存在しなくても、ネットワーク検出ポリシーで監視できます。アクセス コントロール ポリシーの設定によって、トラフィックが識別されるかどうかが決まります。アプリケーション ディテクタ リストで、または、アプリケーション条件をアクセス コントロール ルールに追加するときに、`SSL protocol` タグでフィルタ処理して SSL アプリケーションのディテクタを識別できます。

特記事項:照会先 Web アプリケーション

Web サーバがトラフィックを他の Web サイト(アドバタイズメント サーバであることが多い)に照会する場合があります。ネットワーク上で発生するトラフィック照会のコンテキストをわかりやすくするために、システムは、照会セッションに対するイベント内の Web Application フィールドにトラフィックを照会した Web アプリケーションを列挙します。VDB に既知の照会先サイトのリストが含まれています。システムがこのようなサイトのいずれかからのトラフィックを検出すると、照会元サイトがそのトラフィックに対するイベントと一緒に保存されます。たとえば、Facebook 経由でアクセスされるアドバタイズメントが実際は Advertising.com 上でホストされている場合は、検出された Advertising.com トラフィックが Facebook Web アプリケーションに関連付けられます。また、システムは、Web サイトで他のサイトへの単リンクが提供されている場合などは、HTTP トラフィック内の参照元 URL を検出することもできます。この場合、参照元 URL は [HTTP 参照元(HTTP Referrer)] イベント フィールドに表示されます。

イベントでは、照会元アプリケーションが存在する場合に、それがトラフィックの Web アプリケーションとして列挙されますが、URL は照会先サイトの URL です。上の例では、トラフィックに対する接続イベントの Web アプリケーションは Facebook ですが、URL は Advertising.com です。照会元 Web アプリケーションが検出されない、ホストがそれ自体に照会する、または、照会のチェーンが存在する場合は、照会先アプリケーションがイベント内の Web アプリケーションとして表示されます。ダッシュボードでは、Web アプリケーションの接続カウントとバイト カウントに、Web アプリケーションが照会先のトラフィックに関連付けられたセッションが含まれます。

照会先トラフィックに対して明示的に機能するルールを作成する場合は、照会元アプリケーションではなく、照会先アプリケーションに関する条件を追加する必要があることに注意してください。Facebook から照会される Advertising.com トラフィックをブロックするには、Advertising.com アプリケーションのアクセス コントロール ルールにアプリケーション条件を追加します。

サードパーティ検出データのインポート

ライセンス：FireSIGHT

Nmap アクティブ スキャンを使用してオペレーティング システム、アプリケーション、および脆弱性に関する情報を追加することにより、システムによって収集されたデータを補完できます。Nmap スキャンとスキャン結果の詳細については、Nmap スキャンの概要（47-1 ページ）を参照してください。

ホスト入力機能を使用して API 経由で FireSIGHT システムと対話するようにサードパーティ アプリケーションを設定するか、手動でデータを追加することにより、システムがモニタリング ネットワーク トラフィックから収集した情報を補完することもできます。製品、脆弱性、および修正のマッピングを作成して、サードパーティ データをシスコ定義にマップすることにより、オペレーティング システムとサーバの影響相関を明確にすることができます。ホスト入力機能とサードパーティ データのマップ方法の詳細については、『*FireSIGHT システム Host Input API Guide*』と ホスト入力データのインポート（46-32 ページ）を参照してください。

システムは、オペレーティング システム ID とサーバ ID に関して収集されたデータを照合し、フィンガープリント ソース プライオリティ値、ID 競合解決設定、および収集の時刻に基づいて各 ID を決定します。

NetFlow 対応デバイスからのデータを使用してネットワーク マップ テーブルとイベント テーブルを拡張するようにネットワーク マップを設定することもできます。詳細については、NetFlow について（45-18 ページ）を参照してください。

検出データの用途

ライセンス：FireSIGHT

検出データを記録することにより、次のような FireSIGHT システム内のさまざまな機能を活用できます。

- ホストとネットワーク デバイス、ホスト属性、アプリケーション プロトコル、または脆弱性をグループ化して表示することが可能なネットワーク アセットとトポロジの詳細表現であるネットワーク マップの表示（ネットワーク マップの使用（48-1 ページ）を参照）
- 検出されたホストで利用可能なすべての情報の完全なビューであるホスト プロファイルの表示（ホスト プロファイルの使用（49-1 ページ）を参照）
- （他の機能のいずれかで）ネットワーク アセットとユーザ活動の概要を提供可能なダッシュボードの表示（ダッシュボードの使用（55-1 ページ）を参照）

- システムによって記録された検出イベントとユーザ活動に関する詳細情報の表示（ディスカバリ イベントの使用（50-1 ページ）を参照）
- 検出データに基づくレポートの作成（レポートの操作（57-1 ページ）を参照）
- アプリケーションおよびユーザ制御の実行、つまり、アプリケーション条件とユーザ条件を使用したアクセス コントロール ルールの作成（アプリケーション トラフィックの制御（16-2 ページ）と アクセス コントロール ルールへのユーザ条件の追加（17-3 ページ）を参照）
- ホストおよびそれが実行しているサーバまたはクライアントとそれらが影響を受ける悪用との関連付け。これにより、脆弱性を特定して軽減したり、ネットワークに対する侵入イベントの影響を評価したり、ネットワーク アセットの最大限の保護が提供できるように侵入ルール状態を調整したりできます（ホスト プロファイルでの脆弱性の使用（49-29 ページ）、影響レベルを使用してイベントを評価する（41-41 ページ）、侵害の兆候（痕跡）について（45-22 ページ）、およびネットワーク資産に応じた侵入防御の調整（33-1 ページ）を参照）
- システムが特定の影響フラグ付きの侵入イベントまたは特定のタイプの検出イベントを生成した場合の電子メール、SNMP トラップ、または Syslog 経由の警告（外部アラートの設定（43-1 ページ）を参照）
- 許可されたオペレーティング システム、クライアント、アプリケーション プロトコル、およびプロトコルのホワイト リストを使用した組織の準拠の監視（FireSIGHT システムのコンプライアンス ツールとしての使用（52-1 ページ）を参照）
- システムが検出イベントを生成するかユーザ活動を検出したときにトリガーして相関イベントを生成するルールを使用した相関ポリシーの作成（相関ポリシーおよび相関ルールの設定（51-1 ページ）を参照）
- NetFlow 接続を記録している場合のその接続データの使用（Defense Center または外部サーバへの接続のロギング（38-6 ページ）を参照）

NetFlow について

ライセンス：FireSIGHT

NetFlow は、ネットワーク運用を特徴づける シスコ IOS ソフトウェアに組み込まれた機能です。RFC プロセスを通して標準化された NetFlow は、シスコのネットワーキング デバイス上で使用できるだけでなく、Juniper、FreeBSD、および OpenBSD デバイスにも組み込むことができます。

NetFlow 対応デバイスは、デバイスを通過するトラフィックに関するデータを収集してエクスポートするために広く使用されています。NetFlow 対応デバイスには、デバイスを通過するフローのレコードを保存する NetFlow キャッシュと呼ばれるデータベースが付属しています。FireSIGHT システムで*接続*と呼ばれるフローは、特定のポート、プロトコル、およびアプリケーション プロトコルを使用する送信元ホストと宛先ホスト間のセッションを表すパケットのシーケンスです。

指定されたネットワークで、FireSIGHT システムの管理対象デバイスが NetFlow 対応デバイスからエクスポートされたレコードを検出して、それらのレコード内のデータに基づいて接続イベントを生成し、最後にそれらのイベントを Defense Center に送信して、データベースに記録します。NetFlow 接続内の情報に基づいて、ホストとアプリケーション プロトコルに関する情報をデータベースに追加するようにシステムを設定することもできます。

この検出データと接続データを使用して、管理対象デバイスによって直接収集されたデータを補完できます。これは、管理対象デバイスでモニタできないネットワーク上に NetFlow 対応デバイスを配置した場合に特に有効です。

接続ロギングを含む NetFlow データ収集は、ネットワーク検出ポリシー内のルールを使用して設定します。これを、アクセス コントロールの処理に基づく接続のロギング（38-18 ページ）の説明に従ってアクセス コントロール ルールごとに設定した FireSIGHT システム管理対象デバイスによって検出された接続の接続ロギングと比較してください。NetFlow データ収集は、アクセス コントロール ルールではなく、ネットワークにリンクされるため、記録する接続を細かく制御することはできません。また、システムは自動的にすべての NetFlow ベースの接続イベントを Defense Center 接続イベント データベースに保存するため、それらをシステム ログまたは SNMP トラップ サーバに送信できません。

詳細については、以下を参照してください。

- NetFlow と FireSIGHT データの違い（45-19 ページ）
- NetFlow データの分析準備（45-21 ページ）
- 検出データの用途（45-17 ページ）
- Defense Center または外部サーバへの接続のロギング（38-6 ページ）

NetFlow と FireSIGHT データの違い

ライセンス：FireSIGHT

1 つの例外（TCP フラグ）を除いて、NetFlow レコードで入手可能な情報は、管理対象デバイスを使用したネットワーク トラフィックのモニタによって生成される情報より限られています。システムは NetFlow データによって表されるトラフィックを直接分析できないため、NetFlow レコードを処理するときに、さまざまな手段を使用して、そのデータを接続ログだけでなく、ホスト レコードやアプリケーション プロトコル レコードに変換します。

変換された NetFlow データと、管理対象デバイスによって直接収集された検出および接続データにはいくつかの違いがあります。以下のことを必要とする分析を実行する場合に、この違いを意識しなければなりません。

- 検出された接続数に基づく統計情報
- オペレーティング システムとその他のホスト関連情報（脆弱性を含む）
- クライアント情報、Web アプリケーション情報、ベンダーおよびバージョン サーバ情報を含むアプリケーション データ
- 接続内の発信側のホストと応答側のホストの認識

ヒント　接続イベント内の各フィールドに関して、表 39-1（ 39-13 ページ）に、接続が FireSIGHT システムの管理対象デバイスによって直接検出されたかどうかによって、または、接続イベントが NetFlow データに基づいている場合に、使用可能なデータを示します。

モニタ対象セッションごとに生成される接続イベントの数

管理対象デバイスによって直接検出された接続の場合は、アクセス コントロール ルール アクションに応じて、接続の最初か最後またはその両方で双方向接続イベントを記録できます。

ただし、NetFlow 対応デバイスは一方向接続データをエクスポートするため、システムは、常に、デバイスの設定状態に応じて、NetFlow 対応デバイスによって検出された接続ごとに 2 つ以上の接続イベントを生成します。これは、概要の接続数が NetFlow データに基づいた接続ごとに 2 ずつ増加することも意味しており、ネットワーク上で実際に発生している接続数が急増することになります。

接続が終了したときにのみレコードを出力するように NetFlow 対応デバイスを設定した場合は、システムがそのセッションに対して 2 つの接続イベントを生成することに注意してください。一方、接続が継続中でも一定間隔でレコードを出力するように NetFlow 対応デバイスを設定した場合、システムはデバイスによってエクスポートされたレコードごとに 1 つずつの接続イベントを生成します。たとえば、長期間接続に関するレコードを 5 分ごとに出力するように NetFlow 対応デバイスを設定し、特定の接続が 12 分間続いた場合、そのセッションに対してシステムは次の 6 つの接続イベントを生成します。

- 最初の 5 分間の 1 つのイベント ペア
- 次の 5 分間の 1 つのペア
- 接続が終了した時点の最後のペア

そのため、シスコ 監視対象セッションが閉じるときにのみレコードを出力するように NetFlow 対応デバイスを設定することを**強く**お勧めします。

ホスト データとオペレーティング システム データ

NetFlow レコード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、ホスト プロファイルには接続に関係するホストのオペレーティング システムや NetBIOS のデータが含まれていないため、システムはホストがネットワーク デバイス（ブリッジ、ルータ、NAT デバイス、またはロード バランサ）なのかどうかを識別できません。ただし、ホスト入力機能を使用してホストのオペレーティング システム ID を手動で設定できます。

アプリケーション データ

管理対象デバイスによって直接検出された接続の場合は、接続内のパケットを検査することによって、システムはアプリケーション プロトコル、クライアント、および Web アプリケーションを識別できます。

システムは NetFlow レコードを処理するときに、`/etc/sf/services` 内のポート関連付けを使用して、アプリケーション プロトコル ID を推測します。ただし、これらのアプリケーション プロトコルに関するベンダーまたはバージョン情報が存在しないため、接続ログにはセッションで使用されるクライアントまたは Web アプリケーションに関する情報が含まれません。しかし、ホスト入力機能を使用してこの情報を手動で提供できます。

単純なポート関連付けでは、非標準ポート上で動作しているアプリケーション プロトコルが特定されないまたは誤認される可能性があることに注意してください。加えて、関連付けが存在しない場合は、システムがそのアプリケーション プロトコルを接続ログで `unknown` としてマークします。

脆弱性マッピング

ホスト入力機能を使用してホストのオペレーティング システム ID またはアプリケーション プロトコル ID が手動で設定されていなければ、FireSIGHT システムはネットワーク マップに追加されたホストに影響する脆弱性を NetFlow レコードに基づいて識別することはできません。NetFlow 接続内にクライアント情報が存在しないため、クライアントの脆弱性と NetFlow ホストを関連付けることができないことに注意してください。

接続内の発信側情報と応答側情報

管理対象デバイスによって直接検出された接続の場合、システムは発信側または送信元のホストと応答側または宛先のホストを識別できます。ただし、NetFlow データには発信側または応答側の情報が含まれていません。

システムは、NetFlow レコードを処理するときに、それぞれのホストが使用しているポートとそれらのポートが既知かどうかに基づいて、この情報を判断するアルゴリズムを使用します。

- 使用されているポートの両方が既知のポートの場合、または、どちらも既知のポートでない場合、システムは番号の小さい方のポートを使用しているホストを応答側と見なします。
- どちらかのホストだけが既知のポートを使用している場合は、システムがそのホストを応答側と見なします。

したがって、既知のポートは、1 ～ 1023 の番号が割り当てられたポートまたは管理対象デバイス上の `/etc/sf/services` にアプリケーション プロトコル情報が保存されているポートです。

NetFlow データの分析準備

ライセンス：FireSIGHT

NetFlow データを分析するように FireSIGHT システムを設定する前に、使用するルータまたはその他の NetFlow 対応デバイス上の NetFlow 機能を有効にして、管理対象デバイスのセンシング インターフェイスが接続されている宛先ネットワークに NetFlow バージョン 5 のデータをエクスポートするようにデバイスを設定する必要があります。

システムは NetFlow バージョン 5 と NetFlow バージョン 9 のレコードを解釈できることに注意してください。NetFlow 対応デバイスは、FireSIGHT システム導入と一緒に使用する場合に、これらのバージョンのどちらかを使用する**必要があります**。加えて、システムは、NetFlow 対応デバイスが送信するテンプレートとレコード内に特定のフィールドが存在することを必要とします。NetFlow 対応デバイスがカスタマイズ可能なバージョン 9 を使用している場合は、デバイスが送信するテンプレートとレコードに次のフィールドが任意の順序で含まれていることを確認する**必要があります**。

- IN_BYTES (1)
- IN_PKTS (2)
- PROTOCOL (4)
- TCP_FLAGS (6)
- L4_SRC_PORT (7)
- IPV4_SRC_ADDR (8)
- L4_DST_PORT (11)
- IPV4_DST_ADDR (12)
- LAST_SWITCHED (21)
- FIRST_SWITCHED (22)
- IPV6_SRC_ADDR (27)
- IPV6_DST_ADDR (28)

FireSIGHT システムは管理対象デバイスを使用して NetFlow データを分析するため、NetFlow 対応デバイスを監視可能な 1 つ以上の管理対象デバイスを導入に含める必要があります。この管理対象デバイス上の 1 つ以上のセンシング インターフェイスを、NetFlow 対応デバイスがエクスポートするデータを収集可能なネットワークに接続する必要があります。通常、管理対象デバイス上のセンシング インターフェイスには IP アドレスが割り当てられないため、システムは NetFlow レコードの直接収集をサポートしません。

加えて、シスコでは、監視対象セッションが閉じるときにのみレコードを出力するように NetFlow 対応デバイスを設定することを**強く**推奨しています。一定間隔でレコードを出力するように NetFlow 対応デバイスを設定した場合は、NetFlow レコードから抽出された接続データの分析がより複雑になる可能性があります。モニタ対象セッションごとに生成される接続イベントの数(45-19 ページ) を参照してください。

最後に、一部の NetFlow 対応デバイス上で使用可能なサンプル NetFlow 機能は、デバイスを通過するパケットのサブセットだけに基づく NetFlow 統計情報を収集することに注意してください。この機能を有効にすると、NetFlow 対応デバイス上の CPU 使用率が改善される可能性がありますが、システムで分析するために収集されているデータに影響する場合があります。

侵害の兆候(痕跡)について

ライセンス: FireSIGHT

ネットワーク検出の一部として、FireSIGHT システムの Data Correlator は、ホストに関連す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、およびマルウェア イベント)を関連付けることにより、監視対象ネットワーク上のホストが悪意のある手段で侵害される可能性があるかどうかを特定できます。この関連付けは侵害の兆候/痕跡(IOC)と呼ばれています。この機能をアクティブにするには、検出ポリシー エディタでこの機能とシスコによるさまざまな事前定義の *IOC ルール*のうちのいずれかを有効にします。この機能が有効になっている場合は、そのホストのホスト プロファイルからの個別のホストのルール状態を編集することもできます。IOC ルールのそれぞれがホストに関連付けられた 1 つの特定の *IOC タグ*に対応します。

Data Correlator に加えて、シスコのエンドポイント ベースの Collective Security Intelligence クラウド データも IOC ルールから IOC タグを生成できます。このデータがホスト自体の活動(個別のプログラムによってまたはプログラム上で実行されるアクションなど)を検査するため、ネットワーク専用データでは理解するのが難しい可能性がある脅威に対する理解が促されます。エンドポイントからの FireAMP IOC データはシスコ クラウド接続経由で送信されます。

アクティブ IOC タグ付きのホストは、通常のホスト アイコン( )ではなく、侵害されたホスト アイコン( )を伴ってイベント ビューの [IP アドレス(IP Address)] 列に表示されます。IOC タグをトリガー可能なイベントのイベント ビューで、イベントが IOC をトリガーしたかどうかが示されます。

侵害の兆候タイプについて

ライセンス: FireSIGHT

多くの侵害の兆候(IOC)ルールとタグ タイプがあります。すべてがシスコにより事前定義済みで、1 つの IOC ルールが 1 つの IOC タグに対応します。IOC ルールは FireSIGHT システムのその他の機能(および一部のイベントはシスコ クラウド)から提供されるデータに基づいてトリガーされるため、これらの機能を使用可能にして、IOC タグをセットする IOC ルールに対してアクティブにする必要があります。シスコが新しいエンドポイント ベースのマルウェア イベントの IOC タイプを作成すると、システムはクラウド経由で自動的にそれらをダウンロードし、使用します。下のリストに、IOC ルール タイプ、それらが関連付けられた機能、および追加のライセンス要件(ネットワーク検出に必要な FireSIGHT ライセンス以外)の詳細を示します。

- エンドポイント ベースのマルウェア イベント IOC タイプ(45-23 ページ)
- 侵入イベント IOC タイプ(45-23 ページ)
- セキュリティ インテリジェンス イベント IOC タイプ(45-24 ページ)

エンドポイント ベースのマルウェア イベント IOC タイプ

ライセンス：FireSIGHT

次のリストには、シスコ クラウドへのサブスクリプションが必要な、エンドポイント ベースのマルウェア イベントに関連付けられている IOC タイプの例が含まれています。次に示す IOC タイプに加えて、シスコでは定期的に新しいタイプを作成しており、システムはクラウドへの接続を介してそれらを自動的にダウンロードして実装しています。

エンドポイント ベースのマルウェア防御の設定方法については、FireAMP 用のクラウド接続の操作（37-30 ページ）と ネットワークベースの AMP とエンドポイント ベースの FireAMP の比較（37-9 ページ）を参照してください。

- Adobe Reader 侵害：Adobe Reader がシェルを起動
- Adobe Reader 侵害：FireAMP によって検出された PDF 侵害
- CnC の接続：FireAMP によって検出された疑わしいボットネット
- ドロッパ感染：FireAMP によって検出されたドロッパ感染
- Excel 侵害：FireAMP によって検出された Excel 侵害
- Excel 侵害：Excel がシェルを起動
- FireAMP によって検出された汎用 IOC
- Java 侵害：FireAMP によって検出された Java 侵害
- Java 侵害：Java がシェルを起動
- マルウェアの検出：FireAMP によって検出された脅威：未実行
- マルウェアの検出：ファイル転送中に検出された脅威
- マルウェアの実行：FireAMP によって検出された脅威：実行
- Microsoft Calculator 侵害：FireAMP によって検出された Microsoft Calculator 侵害
- Microsoft Notepad 侵害：FireAMP によって検出された Microsoft Calculator 侵害
- PowerPoint 侵害：FireAMP によって検出された PowerPoint 侵害
- PowerPoint 侵害：PowerPoint がシェルを起動
- QuickTime 侵害：FireAMP によって検出された QuickTime 侵害
- QuickTime 侵害：QuickTime がシェルを起動
- Word 侵害：FireAMP によって検出された Word 侵害
- Word 侵害：Word がシェルを起動

侵入イベント IOC タイプ

ライセンス：FireSIGHT + Protection

次の IOC タイプは、Protection ライセンスが必要な侵入イベントに関連付けられます。侵入イベントの表示方法と侵入検知および防御の設定方法については、侵入ポリシーおよびファイル ポリシーを使用したトラフィックの制御（18-1 ページ）と侵入イベントの表示（41-10 ページ）を参照してください。

- CnC の接続：侵入イベント - malware-backdoor
- CnC の接続：侵入イベント - malware-cnc
- エクスプロイト キット：侵入イベント - exploit-kit

- 影響 1 攻撃:影響 1 侵入イベント - attempted-admin
- 影響 1 攻撃:影響 1 侵入イベント - attempted-user
- 影響 1 攻撃:影響 1 侵入イベント - successful-admin
- 影響 1 攻撃:影響 1 侵入イベント - successful-user
- 影響 1 攻撃:影響 1 侵入イベント - web-application-attack
- 影響 2 攻撃:影響 2 侵入イベント - attempted-admin
- 影響 2 攻撃:影響 2 侵入イベント - attempted-user
- 影響 2 攻撃:影響 2 侵入イベント - successful-admin
- 影響 2 攻撃:影響 2 侵入イベント - successful-user
- 影響 2 攻撃:影響 2 侵入イベント - web-application-attack

セキュリティ インテリジェンス イベント IOC タイプ

ライセンス: FireSIGHT + Protection

サポートされるデバイス:すべて(シリーズ 2 を除く)

サポートされる防御センター:任意(DC500 を除く)

CnC の接続:セキュリティ インテリジェンス イベント - CnC タイプは接続イベントの一種であるセキュリティ インテリジェンス イベントに関連付けられています。セキュリティ インテリジェンス機能には、Protection ライセンスが必要です。セキュリティ インテリジェンスの設定方法とセキュリティ インテリジェンス イベントの表示方法については、セキュリティ インテリジェンスの IP アドレス レピュテーションを使用したブラックリスト登録(13-1 ページ)と接続データとセキュリティ インテリジェンスのデータの表示(39-16 ページ)を参照してください。

侵害の兆候(痕跡)データの表示と編集

ライセンス: FireSIGHT

ネットワーク検出ポリシーそのものを除いて、FireSIGHT システム Web インターフェイスの他の部分で侵害の兆候/痕跡(IOC)データを表示して編集できます。

- ダッシュボードでは、デフォルトで、サマリー ダッシュボードの [脅威(Threats)] タブに、ホスト別の IOC タグと一定期間にトリガーされた新しい IOC ルールが表示されます。カスタム分析ウィジェットは IOC データに基づくプリセットを提供します。詳細については、ダッシュボードの使用(55-1 ページ)およびCustom Analysis ウィジェットの設定(55-17 ページ)を参照してください。
- Context Explorer の [侵害の兆候(ndications of Compromise)] セクションに、IOC カテゴリ別のホストとホスト別の IOC カテゴリのグラフが表示されます。詳細については、[侵入の痕跡(Indications of Compromise)] セクションについて(56-4 ページ)を参照してください。
- 検出(IOC)イベント、接続イベント、セキュリティ インテリジェンス イベント、侵入イベント、およびマルウェア イベントのイベント ビューには、イベントが IOC ルールをトリガーしたかどうかが表示されます(IOC 列)。IOC ルールをトリガーするエンドポイント ベースのマルウェア イベントは、イベント タイプが FireAMP IOC であり、侵害を指定するイベント サブタイプと一緒に表示されます。イベント ビューアに表示されるすべての IOC データに対して準拠ルールを作成できます。詳細については、次の項を参照してください。

- 接続データとセキュリティ インテリジェンスのデータの表示（39-16 ページ）
- 侵入イベントの表示（41-10 ページ）
- マルウェア イベントの操作（40-18 ページ）
- 侵入の痕跡の使用（50-35 ページ）
- 相関ポリシーおよび相関ルールの設定（51-1 ページ）
- ネットワーク マップの [侵害の兆候（Indications of Compromise）] タブに、監視対象ネットワーク上のホストが、IOC タグでグループ化されて一覧表示されます。詳細については、侵入の痕跡のネットワーク マップの操作（48-5 ページ）を参照してください。
- 侵害された可能性のあるホストのホスト プロファイル ビューでは、そのホストに関連付けられたすべての IOC タグを表示したり、IOC タグの一部または全部を解決したり、IOC ルール状態を設定したりできます。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。

ネットワーク検出ポリシーの作成

ライセンス：FireSIGHT

Defense Center 上のネットワーク検出ポリシーは、システムが組織のネットワーク アセットに関するデータを収集する方法と、どのネットワーク セグメントとポートを監視対象とするかを制御します。

ポリシー内の検出（ディスカバリ）ルールは、FireSIGHT システムが監視してトラフィック内のネットワーク データに基づいて検出データを生成するネットワークおよびポートと、ポリシーを適用するゾーンを指定します。ルール内では、ホスト、アプリケーション、およびユーザを検出するかどうかを設定できます。検出からネットワークとゾーンを除外するルールを作成できます。NetFlow デバイスから検出するためのルールを作成するときに、接続を記録するだけにすることもできます。

ネットワーク検出ポリシーには、0.0.0.0/0 ネットワーク上の IPv4 トラフィックでアプリケーションを検出するように設定された、単一のデフォルト ルールが組み込まれています。アクセス コントロール ポリシーを対象のデバイスに適用しておかなければ、ネットワーク検出ポリシーを適用できないことに注意してください。このルールでは、どのネットワーク、ゾーン、またはポートも除外されず、ホストとユーザの検出が設定されず、NetFlow デバイスが設定されません。管理対象デバイスが Defense Center に登録されるときに、デフォルトでは、すべての管理対象デバイスにポリシーが適用されることに注意してください。ホストまたはデータの収集を開始するには、検出ルールを追加または変更して、ポリシーをデバイスに再適用する必要があります。

アクセス コントロール ポリシーは許可されたトラフィック、つまり、ネットワーク検出を使用して監視可能なトラフィックを定義することに注意してください。これは、アクセス コントロールを使用して特定のトラフィックをブロックすると、システムでホスト、ユーザ、またはアプリケーションの活動に関するトラフィックを検査できなくなることを意味することに注意してください。たとえば、アクセス コントロール ポリシーでソーシャル ネットワーキング アプリケーションへのアクセスをブロックすると、システムはそのようなアプリケーションに関する検出データを提供しなくなります。

ネットワーク検出の範囲を調整する場合は、追加の検出ルールを作成して、デフォルト ルールを変更または削除できます。NetFlow デバイスからのデータの検出を設定して、ネットワーク上でユーザ データが検出されるトラフィックのプロトコルを制限できます。

FireSIGHT システムを使用して侵入検知および防御を実行するものの検出データを利用する必要がない場合は、新しい検出を無効にしてパフォーマンスを最適化できます。まず、適用されるアクセス コントロール ポリシーに、ユーザ、アプリケーション、または URL の条件を扱うルール

が含まれないことを確認してください。その後、ネットワーク検出ポリシーからすべてのルールを削除し、それを管理対象デバイスに適用します。アクセス コントロール ルールの設定方法については、アクセス コントロール ルールを使用したトラフィック フローの調整（14-1 ページ）を参照してください。

検出ルールでユーザ検出を有効にすると、一連のアプリケーション プロトコル全体のトラフィック内のユーザ ログイン活動を通してユーザを検出できます。必要に応じて、すべてのルールにわたって特定のプロトコル内の検出を無効にできます。一部のプロトコルを無効にすると、FireSIGHT ライセンスに関連付けられたユーザ制限に達するのを防ぐのに役立ち、他のプロトコルからのユーザに使用可能なユーザ カウントを確保できます。

詳細ネットワーク検出設定を使用すれば、記録するデータの種類、検出データの保存方法、アクティブにする侵害の兆候（IOC）ルール、影響評価に使用する脆弱性マッピング、送信元からの検出データが競合していた場合の対処を管理できます。また、ホスト入力として NetFlow デバイスと送信元を追加できます。

詳細については、以下を参照してください。

- 検出ルールの操作（45-26 ページ）
- ユーザ ロギングの制限（45-33 ページ）
- 高度なネットワーク検出オプションの設定（45-34 ページ）
- ネットワーク検出ポリシーの適用（45-43 ページ）

検出ルールの操作

ライセンス：FireSIGHT

検出（ディスカバリ）ルールを使用すれば、ネットワーク マップに対して検出される情報を調整し、必要な特定のデータだけを含めるようにすることができます。ネットワーク検出ポリシー内のルールは順番に評価されます。モニタリング基準が重複したルールを作成できますが、その場合はシステム パフォーマンスに影響する可能性があることに注意してください。

モニタリングからホストまたはネットワークを除外すると、そのホストまたはネットワークがネットワーク マップに表示されず、それに対するイベントが報告されません。シスコでは、モニタリングからロード バランサ（またはロード バランサ上の特定のポート）と NAT デバイスを除外することを推奨しています。これらのデバイスは紛らわしいイベントを過剰に生成するため、データベースがいっぱいになったり、Defense Center が過負荷になったりする可能性があります。たとえば、監視対象 NAT デバイスが短期間にオペレーティング システムの複数の更新を表示する場合があります。ロード バランサと NAT デバイスの IP アドレスがわかっている場合は、モニタリングからそれらを除外できます。

ヒント　システムは、ネットワーク トラフィックを検査することにより、複数のロード バランサと NAT デバイスを識別できます。ネットワーク上のどのホストがロード バランサでどのホストが NAT デバイスかを特定するには、ネットワーク検出ポリシーを適用して、システムがネットワーク マップを生成するまで待機してから、ホスト タイプで絞り込んだホストの検索を実行します。

加えて、カスタム サーバ フィンガープリントを作成する必要がある場合は、フィンガープリントを行っているホストとの通信に使用されている IP アドレスをモニタリングから一時的に除外する必要があります。そうしないと、ネットワーク マップおよびディスカバリ イベント ビューに、その IP アドレスによって表されるホストに関する不正確な情報が混在することになります。フィンガープリントを作成したら、その IP アドレスを監視するようにポリシーを設定し直すことができます。詳細については、サーバ フィンガープリントの作成（46-12 ページ）を参照してください。

シスコでは、NetFlow 対応デバイスと FireSIGHT システム管理対象デバイスを使用して、同じネットワーク セグメントを監視**しない**ことも推奨しています。重複しないルールを使用してネットワーク検出ポリシーを設定するのが理想ですが、管理対象デバイスによって生成された重複接続ログはシステムによって破棄されます。管理対象デバイスと NetFlow 対応デバイスの両方で検出された接続に関する重複接続ログは破棄**できない**ことに注意してください。

詳細については、次の項を参照してください。

- デバイス選択について（45-27 ページ）
- アクションと検出されるアセットについて（45-27 ページ）
- 監視対象ネットワークについて（45-28 ページ）
- ネットワーク検出ポリシー内のゾーンについて（45-29 ページ）
- ポート除外について（45-29 ページ）
- 検出ルールの追加（45-29 ページ）
- ネットワーク オブジェクトの作成（45-32 ページ）
- ポート オブジェクトの作成（45-32 ページ）

デバイス選択について

ライセンス：FireSIGHT

検出ルール内で NetFlow デバイスを選択する場合、ルールは指定されたネットワークの NetFlow データの検出に制限されます。NetFlow デバイスを選択すると使用可能なルール アクションが変更されるため、NetFlow デバイスを選択してからルール動作の他の側面を設定します。加えて、NetFlow トラフィックのポート除外は設定できません。

ネットワーク検出ルール内で NetFlow デバイスを選択する場合は、ネットワーク検出の詳細設定で NetFlow デバイスへの接続を設定しておく必要があります。詳細については、NetFlow 対応デバイスの追加（45-39 ページ）を参照してください。

アクションと検出されるアセットについて

ライセンス：FireSIGHT

検出ルールを設定するときに、ルールのアクションを選択する必要があります。このアクションによって、システムがルールを処理するときに、どのアセットが検出され、どのアセットが除外されるかが決まります。ただし、ルール アクションの影響は、管理対象デバイスからのデータを検出するルールを使用しているかまたは NetFlow 対応デバイスからのデータを検出するルールを使用しているかによって異なることに注意してください。

ホストまたはユーザを検出するルールを使用せずにネットワーク検出ポリシーを作成して適用すると、アプライアンスの新しい検出が無効になることに注意してください。管理対象デバイスを侵入防御のためだけに使用する場合にパフォーマンスを最適化するには、ポリシーからすべての検出ルールを削除し、アクティブ デバイスに適用します。

次の表に、これら 2 つのシナリオで指定されたアクション設定を使用したルールで検出されるアセットの説明を示します。

表 45-4　検出ルールのアクション

アクション(Action)	管理対象デバイス(Managed Device)	NetFlow
除外	モニタリングから指定されたネットワークを除外します。接続の発信元ホストまたは宛先ホストを検出から除外すると、接続は記録されますが、除外したホストの検出イベントは作成されません。	
検出:ホスト	検出イベントに基づいてネットワーク マップにホストを追加します(任意、ユーザ検出が有効になっていない場合は必須)。	NetFlow レコードに基づいてネットワーク マップにホストを追加します。(必須)
検出:アプリケーション	アプリケーション ディテクタに基づいてネットワーク マップにアプリケーションを追加します。アプリケーションも検出しないルールでは、ホストまたはユーザを検出できないことに注意してください。(必須)	NetFlow レコードと /etc/sf/services 内のポートとアプリケーション プロトコルの関連付けに基づいてネットワーク マップにアプリケーション プロトコルを追加します。`/etc/sf/services`。(オプション)
検出:ユーザ	ネットワーク検出ポリシーで設定されたユーザ プロトコルと一致するトラフィックで検出された活動に基づいてユーザをユーザ テーブルに追加し、ユーザ活動を記録します。(オプション)	適用対象外
NetFlow 接続の記録	適用対象外	NetFlow 接続のみを記録します。ホストまたはアプリケーションを検出しません。

監視対象ネットワークについて

ライセンス:FireSIGHT

検出ルールは、監視対象アセットの検出を、指定されたネットワーク上のホストとの間のトラフィックだけを対象にして行います。検出ルールでは、指定されたネットワーク内の 1 つ以上の IP アドレスが割り当てられた接続に対して検出が行われ、監視対象ネットワーク内の IP アドレスに対してのみイベントが生成されます。デフォルトの検出ルールは、`0.0.0.0/0` ネットワークと `::/0` ネットワーク上でのみアプリケーションを検出します。

ルールで NetFlow デバイスが指定され、[ネットワーク接続の記録(Log Network Connections)] オプションが有効になっている場合は、指定されたネットワーク内の IP アドレスとの間の接続も記録されます。ネットワーク検出ルールが NetFlow ネットワーク接続を記録する唯一の方法を提供することに注意してください。

また、ネットワーク オブジェクトまたはオブジェクト グループを使用して監視対象ネットワークを指定することもできます。ネットワーク検出ポリシーで使用されているネットワーク オブジェクトを変更した場合は、その変更を検出に反映させるためにポリシーを再適用する必要があります。

ネットワーク検出ポリシー内のゾーンについて

ライセンス：FireSIGHT

パフォーマンス上の理由で、ルール内の監視対象ネットワークに物理的に接続されている管理対象デバイス上のセンシング インターフェイスがルール内のゾーンに含まれるように各検出ルールを設定する必要があります。

残念ながら、ネットワーク設定の変更が常に通知されるわけではありません。ネットワーク管理者が通知せずにルーティングやホストの変更によりネットワーク設定を変更した場合、正しいネットワーク検出ポリシー設定を完全に把握するのが難しくなります。管理対象デバイス上のセンシング インターフェイスが物理的にネットワークに接続されている方法がわからない場合は、導入内のすべてのゾーンに検出ルールが適用されるデフォルトのゾーン設定のまま変更しないでください（ゾーンが除外されていなければ、検出ポリシーがすべてのゾーンに適用されます）。

ポート除外について

ライセンス：FireSIGHT

モニタリングからホストを除外できる（アクションと検出されるアセットについて（45-27 ページ）を参照）のと同様に、モニタリングから特定のポートを除外できます。

たとえば、ロード バランサは短期間に同じポート上の複数のアプリケーションを報告する可能性があります。モニタリングからそのポートを除外する（Web ファームを処理するロード バランサ上のポート 80 を除外するなど）ようにネットワーク検出ポリシーを設定できます。

別のシナリオとして、組織で特定の範囲のポートを使用するカスタム クライアントを使用しているとします。このクライアントからのトラフィックが紛らわしいイベントを過剰に生成する場合は、モニタリングからそれらのポートを除外できます。同様に、DNS トラフィックを監視しないように設定することもできます。この場合は、ポート 53 を監視しないように、ポリシーを設定します。

除外するポートを追加するときには、[利用可能なポート（Available Ports）] リストから再利用可能なポート オブジェクトを選択するのか、送信元または宛先除外リストにポートを直接追加するのか、新しい再利用可能なポートを作成してからそれを除外リストに移動するのかを決定できます。

NetFlow 対応デバイスは、モニタリングからポートを除外するように設定できないことに注意してください。

検出ルールの追加

ライセンス：FireSIGHT

検出ルールを設定し、ニーズに合わせてホスト データとアプリケーション データの検出を調整できます。ルールで参照されているオブジェクトを変更した場合は、その変更を反映させるためにネットワーク検出ポリシーを再適用する必要があることに注意してください。

検出ルールを追加する方法：

アクセス：Admin/Discovery Admin

手順 1　アクセス コントロール ポリシーをチェックして、ネットワーク データを検出するトラフィックの必要な接続が記録されていることを確認します。

詳細については、アクセス コントロールの処理に基づく接続のロギング（38-18 ページ）を参照してください。ほとんどのデータを検出するには、検出するトラフィックの接続の最後で記録します。

手順 2　[ポリシー(Policies)] > [ネットワーク検出(Network Discovery)] の順に選択します。

[ネットワーク検出ポリシー(Network Discovery Policy)] ページが表示されます。

手順 3　[ルールの追加(Add Rule)] をクリックします。

[ルールの追加(Add Rule)] ポップアップ ウィンドウが表示されます。

手順 4　次の 2 つの対処法があります。

- NetFlow トラフィックを監視するルールを使用する場合は、[ルールの追加(Add Rule)] ポップアップ ウィンドウで、[NetFlow デバイス(NetFlow Device)] をクリックします。

  [NetFlow デバイス(NetFlow Device)] ページが表示されます。

  NetFlow ページは、NetFlow デバイスを検出ポリシーに追加した場合にのみ使用できることに注意してください。詳細については、NetFlow 対応デバイスの追加(45-39 ページ)を参照してください。
- 管理対象デバイスを監視するルールを使用する場合は、手順 6 を省略します。

詳細については、NetFlow と FireSIGHT データの違い(45-19 ページ)およびデバイス選択について(45-27 ページ)を参照してください。

手順 5　ドロップダウンリストから、使用する NetFlow デバイスの IP アドレスを選択します。

手順 6　ルールのアクションの設定:

- ネットワーク検出からルールと一致するすべてのトラフィックを除外するには、[除外(Exclude)] を選択します。このルール アクションを選択すると、[ポート除外(Port Exclusions)] タブが無効になることに注意してください。
- ルールと一致するトラフィックの選択したデータのタイプを検出するには、[開始段階(Discovery)] を選択して、該当するデータ タイプのチェック ボックスをオンまたはオフにします。

  管理対象デバイス上のトラフィックを監視している場合は、アプリケーション ロギングが必須です。ユーザを監視している場合は、ホスト ロギングが必須です。NetFlow トラフィックを監視している場合は、ユーザを記録できないことと、アプリケーションのロギングが任意であることに注意してください。
- NetFlow トラフィックを監視している場合は、NetFlow トラフィック内の接続を記録するルールを使用するために、[NetFlow 接続の記録(Log NetFlow Connections)] を選択します。このオプションは、ルール内で NetFlow デバイスを選択した後でしか表示されないことに注意してください。

(注)　システムは、ネットワーク検出ポリシー設定に基づいて NetFlow トラフィック内の接続を検出します。管理対象デバイス トラフィックでの接続ロギングはアクセス コントロール ポリシーで設定します。詳細については、ネットワーク トラフィックの接続のロギング(38-1 ページ)を参照してください。

ルール アクションとアセットの検出の詳細については、アクションと検出されるアセットについて(45-27 ページ)を参照してください。

手順 7　すべての検出ルールに 1 つ以上のネットワークを含める必要があります。オプションで、ルール アクションを特定のネットワークに制限するには、[ネットワーク(Networks)] タブをクリックして、[利用可能なネットワーク(Available Networks)] リストからネットワークを選択し、[追加(Add)] をクリックするか、[ネットワーク(Networks)] リストの下でネットワークを入力して [追加(Add)] をクリックします。

ネットワーク モニタリングの詳細については、監視対象ネットワークについて（45-28 ページ）を参照してください。[利用可能なネットワーク（Available Networks）] リストにネットワーク オブジェクトを追加する方法については、ネットワーク オブジェクトの作成（45-32 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使用されているネットワーク オブジェクトを変更した場合は、その変更を検出に反映させるためにポリシーを再適用する必要があることに注意してください。

手順 8　オプションで、ルール アクションを特定のゾーン内のトラフィックに制限するには、[ゾーン（Zones）] をクリックして、[利用可能なゾーン（Available Zones）] リストから 1 つまたは複数のゾーンを選択し、[追加（Add）] をクリックします。

モニタリング用のゾーンの選択方法については、ネットワーク検出ポリシー内のゾーンについて（45-29 ページ）を参照してください。

手順 9　モニタリングからポートを除外するには、[ポート除外（Port Exclusions）] をクリックします。

[ポート除外（Port Exclusions）] ページが表示されます。

手順 10　モニタリングから特定の送信元ポートを除外するには、次の 2 つの選択肢があります。

- [利用可能なポート（Available Ports）] リストから 1 つまたは複数のポートを選択して、[送信元に追加（Add to Source）] をクリックします。
- ポート オブジェクトを追加せずに特定の送信元ポートからのトラフィックを除外するには、[選択済みの送信元ポート（Selected Source Ports）] リストの下にある [プロトコル（Protocol）] ドロップダウンリストから該当するプロトコルを選択して、[ポート（Port）] フィールドに 1 ～ 65535 のポート番号を入力し、[追加（Add）] をクリックします。

  モニタリングからポートを除外する方法については、ポート除外について（45-29 ページ）を参照してください。[利用可能なネットワーク（Available Networks）] リストにポート オブジェクトを追加する方法については、ポート オブジェクトの作成（45-32 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使用されているポート オブジェクトを変更した場合は、その変更を検出に反映させるためにポリシーを再適用する必要があることに注意してください。

手順 11　モニタリングから特定の宛先ポートを除外するには、次の 2 つの選択肢があります。

- [利用可能なポート（Available Ports）] リストから 1 つまたは複数のポートを選択して、[送信先に追加（Add to Destination）] をクリックします。
- ポート オブジェクトを追加せずに特定の宛先ポートからのトラフィックを除外するには、[選択済みの送信先ポート（Selected Destination Ports）] リストの下にある [プロトコル（Protocol）] ドロップダウンリストから該当するプロトコルを選択して、[ポート（Port）] フィールドに 1 ～ 65535 のポート番号を入力し、[追加（Add）] をクリックします。

手順 12　ルールの編集が終了したら、[保存（Save）] をクリックして、検出ポリシー ルールのリストに戻ります。

変更を反映させるためにネットワーク検出ポリシーを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適用（45-43 ページ）を参照してください。

ネットワーク オブジェクトの作成

ライセンス: FireSIGHT

検出ルールに表示される利用可能なネットワークのリストには、FireSIGHT システムのあらゆる場所で使用できる再利用可能なネットワーク オブジェクトとグループが含まれています。このリストに新しいネットワーク オブジェクトを追加することができます。ルールで参照されているオブジェクトを変更した場合は、その変更を反映させるためにネットワーク検出ポリシーを再適用する必要があることに注意してください。

新しいネットワーク オブジェクトを作成する方法:

Admin/Discovery Admin

手順 1　[ポリシー(Policies)] > [ネットワーク検出(Network Discovery)] の順に選択します。

[ネットワーク検出ポリシー(Network Discovery Policy)] ページが表示されます。

手順 2　[ルールの追加(Add Rule)] をクリックします。

[ルールの追加(Add Rule)] ポップアップ ウィンドウが表示されます。

手順 3　[ネットワーク(Networks)] ページで、追加アイコン( )をクリックします。

[ネットワーク オブジェクト(Network Objects)] ポップアップ ウィンドウが表示されます。

手順 4　[名前(Name)] にネットワーク オブジェクトの名前を入力します。縦線(|)と中カッコ({})を除き、印字可能な任意の標準 ASCII 文字を使用できます。

手順 5　ネットワーク オブジェクトに追加する IP アドレス、CIDR ブロック、およびプレフィックス長ごとに、その値を入力して [追加(Add)] をクリックします。

手順 6　[保存(Save)] をクリックして、[利用可能なネットワーク(Available Networks)] リストにネットワーク オブジェクトを追加します。

ヒント　ネットワークがすぐにリストに表示されない場合は、更新アイコン( )をクリックします。

ポート オブジェクトの作成

ライセンス: FireSIGHT

検出ルールに表示される利用可能なポートのリストには、FireSIGHT システムのあらゆる場所で使用できる再利用可能なポート オブジェクトとグループが含まれています。このリストに新しいポート オブジェクトを追加することができます。ルールで参照されているオブジェクトを変更した場合は、その変更を反映させるためにネットワーク検出ポリシーを再適用する必要があることに注意してください。

新しいポート オブジェクトを作成する方法:

Admin/Discovery Admin

手順 1　[ポート除外(Port Exclusions)] をクリックします。

[ポート除外(Port Exclusions)] ページが表示されます。

手順 2　[利用可能なポート(Available Ports)] リストにポートを追加するには、追加アイコン( )をクリックします。

[ポート オブジェクト(Port Objects)] ポップアップ ウィンドウが表示されます。

手順 3　ポート オブジェクトの [名前(Name)] を入力します。縦線(|)と中カッコ({})を除き、印字可能な任意の標準 ASCII 文字を使用できます。

手順 4　[プロトコル(Protocol)] フィールドで、除外するトラフィックのプロトコルを指定します。

[TCP]、[UDP]、または [その他(Other)] を選択して、ドロップダウンリストからオプションを選択し、プロトコルまたは [すべて(All)] を選択します。

手順 5　[ポート(Port(s))] フィールドに、モニタリングから除外するポートを入力します。

単一のポート、ダッシュ(-)を使用したポートの範囲、またはポートとポート範囲のカンマ区切りのリストを指定できます。許容されるポート値は 1 ～ 65535 です。

手順 6　[保存(Save)] をクリックして、[利用可能なポート(Available Ports)] リストにポートを追加します。

ヒント　ポートがすぐにリストに表示されない場合は、更新アイコン( )をクリックします。

ユーザ ロギングの制限

ライセンス: FireSIGHT

ユーザを検出するルールを使用したネットワーク検出ポリシーを適用すると、AIM、IMAP、LDAP、Oracle、POP3、SMTP、FTP、HTTP、MDNS および SIP プロトコルを使用するトラフィック内でユーザが検出されます。これらのユーザは、[分析(Analysis)] メニューからアクセス可能な [ユーザ(users)] テーブルに追加されます。ユーザ アクティビティを検出するプロトコルを制限して、検出するユーザの総数を削減することにより、ほぼ完全なユーザ情報を提供していると思われるユーザに焦点を絞ることができます。

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。プロトコル検出を制限すれば、ユーザ名の氾濫を最小限に抑え、FireSIGHT ユーザ ライセンスを節約できます。

たとえば、AIM、POP3、IMAP などのプロトコル経由でユーザ名を取得すると、契約業者、訪問者、およびその他のゲストからのネットワーク アクセスによって組織に無関係なユーザ名が収集される可能性があります。

別の例として、AIM、Oracle、および SIP ログインは、無関係なユーザ レコードを作成する可能性があります。この現象は、このようなログイン タイプが、システムが LDAP サーバから取得するユーザ メタデータのいずれにも関連付けられていないうえ、管理対象デバイスが検出するその他のログイン タイプに含まれている情報のいずれにも関連付けられていないために発生します。そのため、Defense Center は、これらのユーザとその他のユーザ タイプを関連付けることができません。

管理対象デバイスだけは非 LDAP ユーザ ログインを検出できることに注意してください。Microsoft Active Directory サーバにインストールされたユーザ エージェントのみを使用してユーザ活動を検出している場合は、非 LDAP ログインを制限しても効果はありません。また、SMTP ロギングを制限することはできません。これは、ユーザが SMTP ログインに基づいてデータベースに追加されていないためです。モジュールが SMTP ログインを検出しても、一致する電子メール アドレスのユーザがデータベース内に存在しなければ、そのログインは記録されません。

LDAP、POP3、FTP または IMAP トラフィック内でユーザ ログインの失敗が検出された場合にそのログイン試行の失敗を記録するように選択できます。失敗ログイン試行で新しいユーザがデータベース内のユーザのリストに追加されることはありません。ユーザ エージェントは失敗ログイン活動を報告しないことに注意してください。検出された失敗ログイン活動のユーザ活動タイプは Failed User Login です。

システムは失敗した HTTP ログインと成功した HTTP ログインを区別できないことに注意してください。HTTP ユーザ情報を表示するには、[失敗ログイン試行の検出（Capture Failed Login Attempts）] を有効にする必要があります。

ユーザ ログインを検出するプロトコルを制限する方法:

Admin/Discovery Admin

手順 1　[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）] の順に選択します。

[ネットワーク検出ポリシー（Network Discovery Policy）] ページが表示されます。

手順 2　[ユーザ（User）] をクリックします。

[ユーザ（User）] ページが表示されます。

手順 3　ログインを検出するプロトコルのチェック ボックスをオンにするか、ログインを検出しないプロトコルのチェック ボックスをオフにします。

手順 4　オプションで、LDAP、POP3、FTP、または IMAP トラフィックで検出されたログイン試行の失敗を記録したり、HTTP ログインのユーザ情報を取得するには、[失敗ログイン試行の検出（Capture Failed Login Attempts）] を有効にします。

手順 5　[保存（Save）] をクリックして、ネットワーク ポリシーを保存します。

変更を反映させるためにネットワーク検出ポリシーを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適用（45-43 ページ）を参照してください。

高度なネットワーク検出オプションの設定

ライセンス: FireSIGHT

ネットワーク検出ポリシーの [詳細設定（Advanced）] タブを使用すれば、検出するイベント、検出データの保存期間と更新頻度、影響相関に使用する脆弱性マッピング、およびオペレーティング システム ID とサーバ ID の競合の解決方法に関するポリシー全体の設定を構成できます。加えて、ホスト入力ソースと NetFlow 対応デバイスを追加して、他のソースからのデータのインポートを許可できます。

検出イベントとユーザ活動イベントのデータベース イベント制限はシステム ポリシーで設定されることに注意してください。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。

高度な設定を設定するには、次の手順を実行します。

Admin/Discovery Admin

手順 1　[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）] の順に選択します。

[ネットワーク検出ポリシー（Network Discovery Policy）] ページが表示されます。

手順 2　[詳細設定（Advanced）] をクリックします。

[詳細設定（Advanced）] ページが表示されます。

手順 3　必要に応じて詳細設定を編集します。

- 一般設定の構成（45-35 ページ）
- ID 競合解決の設定（45-36 ページ）
- 脆弱性影響評価マッピングの有効化（45-37 ページ）
- 侵害の兆候ルールの設定（45-38 ページ）
- NetFlow 対応デバイスの追加（45-39 ページ）
- データ保存の設定（45-40 ページ）
- 検出（ディスカバリ）イベント ロギングの設定（45-41 ページ）
- ID ソースの追加（45-41 ページ）

手順 4　設定の編集が終了したら、[保存（Save）] をクリックしてポリシーを保存します。

手順 5　ポリシーを編集して保存したら、それを適用して更新した設定を反映させます。詳細については、ネットワーク検出ポリシーの適用（45-43 ページ）を参照してください。

一般設定の構成

ライセンス：FireSIGHT

一般設定は、システムがネットワーク マップ内の情報を更新する頻度と、検出中にサーバ バナーをキャプチャするかどうかを制御します。

バナーのキャプチャ（Capture Banners）

サーバ ベンダーとバージョン（「バナー」）をアドバタイズするネットワーク トラフィックからの見出し情報をシステムで保存させる場合、このチェック ボックスをオンにします。この情報は、収集された情報に追加のコンテキストを提供できます。サーバ詳細にアクセスすることによって、ホストに関して収集されたサーバ バナーにアクセスできます。

アップデート間隔（Update Interval）

システムが情報を更新する時間間隔（ホストの IP アドレスのいずれかが最後に検出された時点、アプリケーションが使用された時点、アプリケーションのヒット数など）。デフォルト設定は 3600 秒（1 時間）です。

更新タイムアウトの時間間隔を短く設定すると、より正確な情報がホスト画面に表示されますが、より多くのネットワーク イベントが生成されることに注意してください。

一般設定を更新する方法:

Admin/Discovery Admin

手順 1　[全般設定(General Settings)] の横にある編集アイコン( )をクリックします。

[全般設定(General Settings)] ポップアップ ウィンドウが表示されます。

手順 2　必要に応じて設定を更新します。

手順 3　[保存(Save)] をクリックして一般設定を保存し、ネットワーク検出ポリシーの [詳細設定(Advanced)] タブに戻ります。

変更を反映させるためにネットワーク検出ポリシーを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適用(45-43 ページ)を参照してください。

ID 競合解決の設定

ライセンス: FireSIGHT

システムは、オペレーティング システムとサーバのフィンガープリントとトラフィック内のパターンを照合することによって、特定のホスト上で実行しているオペレーティング システムとアプリケーションを判断します。最も信頼できるオペレーティング システムとサーバの ID 情報を提供するために、システムは複数のソースからのフィンガープリント情報を照合します。

システムは、すべてのパッシブ データを使用して、オペレーティング システム ID を抽出し、信頼値を割り当てます。最新の ID とシステムが最新の ID を選択する方法の詳細については、ネットワーク マップの拡張(46-4 ページ)を参照してください。

デフォルトでは、ID 競合が存在しなければ、スキャナまたはサード パーティ アプリケーションによって追加された ID データで、FireSIGHT システムによって検出された ID データが上書きされます。[ID ソース(Identity Sources)] 設定を使用して、スキャナとサードパーティ アプリケーションのフィンガープリント ソースをプライオリティでランク付けできます。システムはソースごとに 1 つずつの ID を保持しますが、プライオリティが最も高いサードパーティ アプリケーションまたはスキャナ ソースからのデータのみが最新の ID として使用されます。ただし、プライオリティに関係なく、ユーザ入力データによって、スキャナとサードパーティ アプリケーションのデータが上書きされることに注意してください。

ID 競合は、[ID ソース(Identity Sources)] 設定に列挙されたアクティブなスキャナ ソースまたはサードパーティ アプリケーション ソースと FireSIGHT システム ユーザのどちらかから取得された既存の ID と競合する ID をシステムが検出した場合に発生します。デフォルトでは、ID 競合は自動的に解決されないため、ホスト プロファイルを通して、または、ホストをスキャンし直すか新しい ID データを追加し直してパッシブ ID を上書きすることにより、解決する必要があります。ただし、パッシブ ID を維持しつつ常に自動的に競合を解決するようにシステムを設定することも、アクティブ ID を維持しつつ常に競合を解決するようにシステムを設定することもできます。

ID 衝突イベントを生成する(Generate Identity Conflict Event)

ネットワーク マップ内のホストで ID 競合が発生したときにイベントを生成する場合に、このオプションを有効にします。

自動的に衝突を解決する（Automatically Resolve Conflicts）

次の選択肢があります。

- ID 競合の手動競合解決を強制するには、[自動的に衝突を解決する（Automatically Resolve Conflicts）] ドロップダウンリストから [無効（Disabled）] を選択します。
- ID 競合が発生したときにパッシブ フィンガープリントを使用するには、[自動的に衝突を解決する（Automatically Resolve Conflicts）] ドロップダウンリストから [ID（Identity）] を選択します。
- ID 競合が発生したときにプライオリティが最も高いアクティブ ソースからの最新の ID を使用するには、[自動的に衝突を解決する（Automatically Resolve Conflicts）] ドロップダウンリストから [アクティブを維持（Keep Active）] を選択します。

ID 競合解決設定を更新する方法:

Admin/Discovery Admin

手順 1　[ID 競合設定（Identity Conflict Settings）] の横にある編集アイコン（ ）をクリックします。

[ID 競合設定の編集（Edit Identity Conflict Settings）] ポップアップ ウィンドウが表示されます。

手順 2　必要に応じて設定を更新します。

手順 3　[保存（Save）] をクリックして ID 競合設定を保存し、ネットワーク検出ポリシーの [詳細設定（Advanced）] タブに戻ります。

変更を反映させるためにネットワーク検出ポリシーを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適用（45-43 ページ）を参照してください。

脆弱性影響評価マッピングの有効化

ライセンス：FireSIGHT

FireSIGHT システムで侵入イベントとの影響相関を実行する方法を設定できます。オプションは次のとおりです。

- システム ベースの脆弱性情報を使用して影響相関を実行する場合は、[ネットワーク検出脆弱性マッピングを使用する（Use Network Discovery Vulnerability Mappings）] をオンにします。
- サードパーティの脆弱性参照を使用して影響相関を実行する場合は、[サードパーティ脆弱性マッピングを使用する（Use Third-Party Vulnerability Mappings）] をオンにします。詳細については、サードパーティの脆弱性のマッピング（46-37 ページ）または『*FireSIGHT システム Host Input API Guide*』を参照してください。

チェック ボックスのどちらかまたは両方を選択できます。システムが侵入イベントを生成し、選択された脆弱性マッピング セット内の脆弱性のあるサーバまたはオペレーティング システムがそのイベントに関係するホストに含まれている場合、侵入イベントは脆弱（レベル 1：赤）影響アイコンでマークされます。ベンダーまたはバージョン情報のないサーバの場合は、システム ポリシーで脆弱性マッピングを設定する必要があることに注意してください。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。

両方のチェック ボックスをオフにした場合は、侵入イベントが脆弱（レベル 1：赤）影響アイコンでマーク**されません**。詳細については、影響レベルを使用してイベントを評価する（41-41 ページ）を参照してください。

脆弱性設定を更新する方法:

Admin/Discovery Admin

手順 1　[影響評価を使用するための脆弱性(Vulnerabilities to use for Impact Assessment)] の横にある編集アイコン( )をクリックします。

[脆弱瀬尾設定の編集(Edit Vulnerability Settings)] ポップアップ ウィンドウが表示されます。

手順 2　必要に応じて設定を更新します。

手順 3　[保存(Save)] をクリックして脆弱性設定を保存し、ネットワーク検出ポリシーの [詳細設定(Advanced)] タブに戻ります。

変更を反映させるためにネットワーク検出ポリシーを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適用(45-43 ページ)を参照してください。

侵害の兆候ルールの設定

ライセンス: FireSIGHT

システムで侵害の兆候(IOC)を検出してタグを付けるには、まず、検出ポリシーで 1 つ以上の IOC ルールをアクティブにする必要があります。IOC ルールのそれぞれが IOC タグの 1 つのタイプに対応します。すべての IOC ルールはシスコが事前定義しています。オリジナル ルールを作成することはできません。ネットワークや組織のニーズに合わせて、一部またはすべてのルールを有効にすることができます。たとえば、Microsoft Excel などのソフトウェアを使用しているホストがモニタ対象ネットワーク上に出現することがない場合は、Excel ベースの脅威に関係する IOC タグを有効にしないようにできます。IOC 機能の詳細については、侵害の兆候(痕跡)について(45-22 ページ)を参照してください。

また、有効にした侵入防御やマルウェア防御などの IOC ルールに関連付けられた FireSIGHT システム機能を有効にする必要もあります。ルールに関連した機能が有効になっていない場合は、関連データが収集されず、ルールをトリガーできません。IOC ルールのタイプと関連機能の詳細については、侵害の兆候タイプについて(45-22 ページ)を参照してください。

検出ポリシーで侵害の兆候ルールを設定する方法:

Admin/Discovery Admin

手順 1　[侵害の兆候設定(Indications of Compromise Settings)] の横にある編集アイコン( )をクリックします。

[侵害の兆候設定の編集(Edit Indications of Compromise Settings)] ポップアップ ウィンドウが表示されます。

手順 2　IOC 機能全体のオンとオフを切り替えるには、[IOC の有効化(Enable IOC)] の横にあるスライダをクリックします。

手順 3　個別の IOC ルールを有効または無効にするには、ルールの [有効(Enabled)] 列のスライダをクリックします。

手順 4　[保存(Save)] をクリックして、IOC ルール設定を保存し、検出ポリシーの [詳細設定(Advanced)] タブに戻ります。

変更が保存されます。

変更を反映させるためにネットワーク検出ポリシーを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適用(45-43 ページ)を参照してください。

NetFlow 対応デバイスの追加

ライセンス：FireSIGHT

NetFlow 対応デバイス上で NetFlow 機能を有効にした場合は、そのデバイスからエクスポートされた接続データを使用して、シスコ デバイスによって収集された接続データを補完することができます。

NetFlow 対応デバイスを検出ルールで使用するには、そのデバイスを設定（NetFlow データの分析準備（45-21 ページ）を参照）してから、ネットワーク検出ポリシーに追加する必要があります。

FireSIGHT システムで NetFlow データを使用する方法については、その他の前提条件に関する情報も含め、NetFlow について（45-18 ページ）を参照してください。

接続データ収集用の NetFlow 対応デバイスを追加するには、次の手順を実行します。

Admin/Discovery Admin

手順 1　[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）] の順に選択します。

[ネットワーク検出ポリシー（Network Discovery Policy）] ページが表示されます。

手順 2　[詳細設定（Advanced）] をクリックします。

[詳細設定（Advanced）] ページが表示されます。

手順 3　NetFlow デバイスの横にある追加アイコン（  ）をクリックします。

[NetFlow デバイスの追加（Add NetFlow Device）] ポップアップ ウィンドウが表示されます。

手順 4　[IP アドレス（IP Address）] フィールドに、接続データを収集するために使用する NetFlow 対応デバイスの IP アドレスを入力します。

手順 5　さらに NetFlow 対応デバイスを追加するには、手順 3 と 4 を繰り返します。

ヒント　NetFlow 対応デバイスを削除するには、削除するデバイスの横にある削除アイコン（）をクリックします。検出ルールで NetFlow 対応デバイスを使用する場合は、先にルールを削除しないと、[詳細設定（Advanced）] ページからデバイスを削除できないことに注意してください。詳細については、検出ルールの操作（45-26 ページ）を参照してください。

手順 6　[保存（Save）] をクリックします。

デバイスが NetFlow 対応デバイスのリストに表示されます。

変更を反映させるためにネットワーク検出ポリシーを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適用（45-43 ページ）を参照してください。

データ保存の設定

ライセンス：FireSIGHT

データ保存設定によってデータベースに保存されるデータの種類が制御されるため、FireSIGHT システムで使用可能なデータが決まります。この設定は、データがネットワーク マップに保存される期間も制御します。

次のオプションがネットワーク検出データ保存設定を構成しています。

ホスト制限到達時（When Host Limit Reached）

Defense Center がホスト制限（FireSIGHT ライセンスによって決定される）に達して、ネットワーク マップがいっぱいになったときのホストの処理方法を制御できます。このオプションは、特に、スプーフィングされたホストがネットワーク マップ内の有効なホストに取って代わるのを防ぐ場合に重要です。古いホストを除外するには、[ホスト制限到達時（When Host Limit Reached）] ドロップダウンリストから [ホストのドロップ（Drop hosts）] を選択します。新しいホストを除外するには、[ホスト制限到達時（When Host Limit Reached）] ドロップダウンリストから [新しいホストを挿入しない（Don't insert new hosts）] を選択します。詳細については、FireSIGHT ホストおよびユーザ ライセンスの制限について（65-9 ページ）を参照してください。

ホスト タイムアウト（Host Timeout）

システムが、非アクティブであるという理由でネットワーク マップからホストを除外するまでの分単位の時間。デフォルト設定は 10080 分（7 日）です。ホスト IP アドレスと MAC アドレスは個別にタイムアウトすることができますが、関連するアドレスのすべてがタイムアウトするまで、ホストはネットワーク マップから削除されません。

ホストの早期タイムアウトを避けるために、ホストのタイムアウト値がネットワーク検出ポリシー内の更新間隔より長いことを確認します。更新間隔の詳細については、一般設定の構成（45-35 ページ）を参照してください。

サーバ タイムアウト（Server timeout）

システムが、非アクティブであるという理由でネットワーク マップからサーバを除外するまでの分単位の時間。デフォルト設定は 10080 分（7 日）です。

サーバの早期タイムアウトを避けるために、サーバのタイムアウト値がネットワーク検出ポリシー内の更新間隔より長いことを確認します。詳細については、一般設定の構成（45-35 ページ）を参照してください。

クライアント アプリケーション タイムアウト（Client Application Timeout）

システムが、非アクティブであるという理由でネットワーク マップからクライアントを除外するまでの分単位の時間。デフォルト設定は 10080 分（7 日）です。

クライアントのタイムアウト値がネットワーク検出ポリシー内の更新間隔より長いことを確認する必要があります。詳細については、一般設定の構成（45-35 ページ）を参照してください。

データ保存設定を更新する方法:

Admin/Discovery Admin

手順 1　[データ保存設定(Data Storage Settings)] の横にある編集アイコン( )をクリックします。

[データ保存設定(Data Storage Settings)] ポップアップ ウィンドウが表示されます。

手順 2　必要に応じて設定を更新します。

手順 3　[保存(Save)] をクリックしてデータ保存設定を保存し、ネットワーク検出ポリシーの [詳細設定(Advanced)] タブに戻ります。

変更を反映させるためにネットワーク検出ポリシーを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適用(45-43 ページ)を参照してください。

検出(ディスカバリ)イベント ロギングの設定

ライセンス: FireSIGHT

イベント ロギング設定は、検出イベントとホスト入力イベントを記録するかどうかを制御します。イベントを記録しない場合は、イベント ビューで検索することも、相関ルールをトリガーするために使用することもできません。

イベント ロギング設定を構成する方法:

Admin/Discovery Admin

手順 1　[イベント ロギング設定(Event Logging Settings)] の横にある編集アイコン( )をクリックします。

[イベント ロギング設定(Event Logging Settings)] ポップアップ ウィンドウが表示されます。

手順 2　データベースに記録する検出イベント タイプとホスト入力イベント タイプの横にあるチェック ボックスをオンまたはオフにします。各イベント タイプに関する情報については、ディスカバリ イベントのタイプについて(50-10 ページ)と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。

手順 3　[保存(Save)] をクリックしてイベント ロギング設定を保存し、ネットワーク検出ポリシーの [詳細設定(Advanced)] タブに戻ります。

変更を反映させるためにネットワーク検出ポリシーを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適用(45-43 ページ)を参照してください。

ID ソースの追加

ライセンス: FireSIGHT

このページで新しいアクティブ ソースを追加することも、既存のソースのプライオリティまたはタイムアウト設定を変更することもできます。このページにスキャナを追加しても、Nmap スキャナ用の完全統合機能は追加されませんが、インポートされたサードパーティ アプリケーションまたはスキャン結果の統合が可能になることに注意してください。サードパーティ アプリケーションまたはスキャナからデータをインポートする場合は、ソースからの脆弱性とネットワーク マップ内の脆弱性がマップされているかどうかを確認するのを忘れないでください。詳細については、サードパーティの脆弱性のマッピング(46-37 ページ)を参照してください。

ID ソースを追加する方法:

Admin/Discovery Admin

手順 1　[OS とサーバ ID ソース(OS and Server Identity Sources)] の横にある編集アイコン( )をクリックします。

[OS とサーバ ID ソースの編集(Edit OS and Server Identity Sources)] ポップアップ ウィンドウが表示されます。

手順 2　新しいソースを追加するには、[ソースの追加(Add Sources)] をクリックします。

[ID ソースの追加(Add Identity Source)] ポップアップ ウィンドウが表示されます。

手順 3　ソースの [名前(Name)] を入力します。

手順 4　[タイプ(Type)] ドロップダウンリストから入力ソース タイプを選択します。

- AddScanResult 機能を使用してスキャン結果をインポートする場合は、[スキャナ(Scanner)] を選択します。
- スキャン結果をインポートしない場合は、[アプリケーション(Application)] を選択します。

手順 5　このソースによるネットワーク マップへの ID の追加からその ID の削除までの期間を指定するには、[タイムアウト(Timeout)] ドロップダウンリストから、[時間(Hours)]、[日(Days)]、または [週(Weeks)] を選択し、該当する期間を入力します。

ヒント　追加したソースを削除するには、そのソースの横にある削除アイコン( )をクリックします。

手順 6　オプションで、ソースを昇格させて、オペレーティング システム ID とアプリケーション ID よりもリストでは下にあるソースを優先的に使用するには、そのソースを選択して上矢印をクリックします。

手順 7　また、オプションで、ソースを降格させて、リストで上にあるソースから提供される ID が存在しない場合にのみオペレーティング システム ID とアプリケーション ID を使用するには、そのソースを選択して下矢印をクリックします。

手順 8　[保存(Save)] をクリックして ID ソース設定を保存し、ネットワーク検出ポリシーの [詳細設定(Advanced)] タブに戻ります。

変更を反映させるためにネットワーク検出ポリシーを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適用(45-43 ページ)を参照してください。

ネットワーク検出ポリシーの適用

ライセンス：FireSIGHT

デフォルトでは、ネットワーク検出ポリシーは、Defense Center に登録されている管理対象デバイス上のすべてのターゲット ゾーンに適用されます。ネットワーク検出ポリシーを適用すると、システムが指定内容に従ってネットワークの監視を開始します。ネットワーク検出ポリシーを変更した場合は、その変更を反映させるためにポリシーを再適用する必要があります。

ネットワーク検出ポリシーを再適用した場合：

- システムは、監視対象ネットワーク内のホストのネットワーク マップから MAC アドレス、TTL、およびホップ情報を削除してから、再検出を行います
- 影響を受ける管理対象デバイスは、まだ Defense Center に送信されていない検出データを破棄します。

ネットワーク検出ポリシーを適用するときは、Defense Center によって管理されるすべてのデバイスにアクセス コントロール ポリシーがすでに適用されていることを確認します。アクセス コントロール ポリシーが各デバイスに適用されていない場合は、ネットワーク検出ポリシーの適用が失敗します。FireSIGHT ライセンスがインストールされていない Defense Center にはネットワーク検出ポリシーを適用できないことに注意してください。

ネットワーク検出ポリシーで使用されているネットワークまたはポート オブジェクトを変更した場合は、その変更を検出に反映させるためにポリシーを再適用する必要があります。

FireSIGHT システムの別のバージョンを実行しているスタックされたデバイス（デバイスのいずれかのアップグレードが失敗した場合など）にはネットワーク検出ポリシーを適用できないことに注意してください。

ネットワーク検出ポリシーを適用する方法：

Admin/Security Approver

手順 1　[ポリシー（Policies）] > [ネットワーク検出（Network Discovery）] の順に選択します。

[ネットワーク検出ポリシー（Network Discovery Policy）] ページが表示されます。

手順 2　[適用（Apply）] をクリックします。

Defense Center 上のアクセス コントロール ポリシーの対象となるすべてのゾーンにポリシーを適用するかどうかを確認するメッセージが表示されます。

手順 3　[はい（Yes）] をクリックしてポリシーを適用します。