



ネットワーク検出の概要

次のトピックでは、ネットワーク検出について説明します。

- ホスト、アプリケーション、およびユーザーのデータの検出について（1ページ）
- ホストおよびアプリケーション検出の基礎（2ページ）

ホスト、アプリケーション、およびユーザーのデータの検出について

システムは、ネットワーク検出およびアイデンティティポリシーを使用して、ネットワークトラフィックのホスト、アプリケーション、およびユーザーのデータを収集します。特定のタイプの検出およびアイデンティティデータを使用すると、ネットワークアセットの包括的なマップを作成し、フォレンジック分析、動作プロファイリング、アクセス制御を行い、組織が影響を受ける脆弱性およびエクスプロイトに対応して軽減することができます。

ホストおよびアプリケーションデータ

ホストやアプリケーションデータは、ネットワーク検出ポリシーの設定に従ってホストのアイデンティティソースとアプリケーションディテクタによって収集されます。管理対象デバイスは、指定したネットワークセグメントのトラフィックを確認します。

詳細については、[ホストおよびアプリケーション検出の基礎（2ページ）](#)を参照してください。

ユーザデータ（User Data）

ユーザデータはネットワーク検出およびアイデンティティポリシーの設定に従ってユーザーのアイデンティティソースによって収集されます。データはユーザ認識とユーザ制御のために使用できます。

詳細については、[ユーザー イデンティティについて](#)を参照してください。

検出データとアイデンティティデータをロギングすることにより、次のようなシステムのさまざまな機能を活用できます。

■ ホストおよびアプリケーション検出の基礎

- ・ネットワーク アセットとトポロジの詳細を示すネットワーク マップを表示します。その際、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できます。
 - ・アプリケーション、ルーム、ユーザ、ユーザ グループ、およびISE 属性の各条件を使ってアクセス コントロール ルールを作成することにより、アプリケーション制御およびユーザ制御を実行します。
 - ・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を表示します。
 - ・（さまざまな機能の 1 つとして）ネットワーク アセットとユーザ アクティビティの概要を示すダッシュボードを表示します。
 - ・システムによって記録された検出イベントとユーザアクティビティに関する詳細情報を表示します。
 - ・ホストおよびそこで実行されているサーバ/クライアントと、被害を及ぼす可能性のあるエクスプロイトとを関連付けます。
- 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を最大限に保護できるように侵入ルール状態を調整したりできます。
- ・システムで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が生成された場合に、電子メール、SNMP トラップ、またはsyslog によるアラートを発行します。
 - ・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allowリストを使用して組織のコンプライアンスをモニターします。
 - ・システムが検出イベントを生成するかユーザーアクティビティを検出したときにトリガーして相關イベントを生成するルールを使って、相關ポリシーを作成します。
 - ・該当する場合、NetFlow 接続をロギングして使用します。

ホストおよびアプリケーション検出の基礎

ネットワーク検出ポリシーを設定すると、ホストおよびアプリケーション検出を実行できます。

詳細については、「[概要：ホストのデータ収集](#)」および「[概要：アプリケーション検出](#)」を参照してください。

オペレーティング システムおよびホスト データのパッシブ検出

パッシブ検出は、システムがネットワーク トラフィック（およびエクスポートされたNetFlow データ）を分析してネットワークマップにデータを取り込む際のデフォルト方式です。パッシ

本検出では、ネットワークアセットに関するコンテキスト情報（オペレーティングシステムや実行中のアプリケーションなど）が提供されます。

モニタ対象のホストからのトライフィックが、ホストで実行されているオペレーティングシステムを示す決定的証拠とならない場合、使用されている可能性が最も高いオペレーティングがネットワークマップに表示されます。たとえば、複数のホストがNATデバイスの「背後」にあることから、NATデバイスが複数のオペレーティングシステムを実行しているように表示される場合があります。この最も可能性の高いオペレーティングを決定するためにシステムが使用するのは、検出された各オペレーティングシステムに割り当てられた信頼度の値と、検出されたオペレーティングシステムの中でその特定のオペレーティングシステムが使用されていることを裏付けるデータの量です。



(注) この決定を行う際、システムは「unknown」として報告されたアプリケーションとオペレーティングシステムを考慮しません。

パッシブ検出でネットワークアセットが正確に識別されない場合は、管理対象デバイスの配置について検討してください。また、システムのパッシブ検出機能をオペレーティングシステムのカスタムフィンガープリントとカスタムアプリケーションディクタで増補することができます。あるいは、アクティブ検出を使用するという方法もあります。アクティブ検出では、トライフィック分析をベースとするのではなく、スキャン結果やその他の情報ソースを使用して直接ネットワークマップを更新できます。

オペレーティングシステムおよびホストデータのアクティブ検出

アクティブ検出では、アクティブソースによって収集されたホスト情報をネットワークマップに追加します。たとえば、Nmapスキャナを使用して、ネットワーク上の対象ホストをアクティブにスキャンできます。Nmapは、ホストでオペレーティングシステムおよびアプリケーションを検出します。

さらに、ホスト入力機能によって、ネットワークマップにホスト入力データをアクティブに追加することができます。ホスト入力データには2種類のカテゴリがあります。

- ユーザ入力データ：FirePOWERシステムユーザインターフェイスで追加されたデータ。このユーザインターフェイスを使用して、ホストのオペレーティングシステムやアプリケーションのIDを変更できます。
- ホストインポート入力データ：コマンドラインユーティリティを使用してインポートされたデータ。

システムは、それぞれのアクティブソースに対して1個のIDを保持します。たとえば、Nmapスキャンインスタンスを実行すると、以前のスキャンの結果は新しいスキャン結果に置き換えられます。ただし、Nmapスキャンを実行し、それらの結果をクライアントからのデータ（コマンドラインを使用してインポートした結果）と交換する場合、システムはNmapの結果のIDとインポートクライアントのIDの両方を保持します。システムは、ネットワーク検出ポリ

■ アプリケーションおよびオペレーティングシステムの現在の ID

シードで設定された優先順位を使用して、現在の ID として使用するアクティブ ID を判別します。

複数のユーザーが入力したとしても、ユーザー入力は 1 ソースと見なされることに注意してください。たとえば、UserA がホストプロファイルを使用してオペレーティングシステムを設定し、UserB がホストプロファイルを使用してその定義を変更した場合、UserB によって設定された定義が保持され、UserA によって設定された定義は破棄されます。また、ユーザー入力によって、他のアクティブソースすべてが上書きされ、存在する場合、現在の ID として使用されることに注意してください。

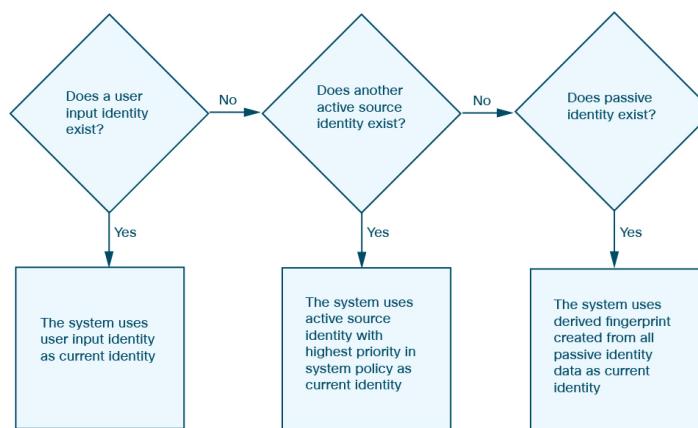
アプリケーションおよびオペレーティングシステムの現在の ID

ホストのアプリケーションまたはオペレーティングシステムの現在の ID は、ホストが最も正しい可能性が高いと認識する ID です。

システムは、以下の目的で、オペレーティングシステムまたはアプリケーションの現在の ID を使用します。

- 脆弱性のホストへの割り当て
- 影響評価
- オペレーティングシステムの識別、ホストプロファイルの認定、およびコンプライアンスの allow リストに対して記述された相関ルールの評価
- ワークフローのホストおよびサーバーのテーブルビューでの表示
- ホストプロファイルでの表示
- [検出統計情報 (Discovery Statistics)] ページでのオペレーティングシステムとアプリケーションの統計の計算

システムは、ソースの優先順位を使用して、アプリケーションまたはオペレーティングシステムの現在の ID として使用するアクティブ ID を判別します。



たとえば、ユーザーがホストでオペレーティングシステムを Windows 2003 Server に設定した場合、Windows 2003 Server が現在の ID になります。そのホストの Windows 2003 Server の脆弱

性を狙った攻撃により大きな影響力があると見なされ、ホストプロファイルのそのホストについてリストされた脆弱性に、Windows 2003 Server の脆弱性が含まれられます。

データベースは、ホストのオペレーティングシステムや特定のアプリケーションに関する複数のソースからの情報を保持する場合があります。

データのソースに最も高いソースの優先順位が付けられている場合に、システムはオペレーティングシステムまたはアプリケーションの ID を現在の ID として扱います。使用される可能性のあるソースには、次の優先順位があります。

1. ユーザー

2. スキヤナとアプリケーション（ネットワーク検出ポリシーで設定）

3. 管理対象デバイス

4. : NetFlow レコード

新しい優先順位の高いアプリケーション ID は、現在のアプリケーション ID ほど詳細でない場合、現在の ID を上書きしません。

また、ID の競合が発生した場合、競合の解決はネットワーク検出ポリシーの設定または手動解決によります。

現在のユーザー ID

システムは、同じホストに対して異なるユーザーによる複数のログインを検出すると、特定のホストにログインするユーザーは一度に1人だけであり、ホストの現在のユーザーが最後の権限のあるユーザー ログインであると見なします。権限のないユーザー ログインだけがホストにログインしている場合は、最後にログインしたもの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、サーバによって報告された最後のユーザが Firewall Management Center に報告されるユーザです。

システムは、同じホストに対して異なるユーザーによる複数のログインを検出すると、ユーザー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ー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。

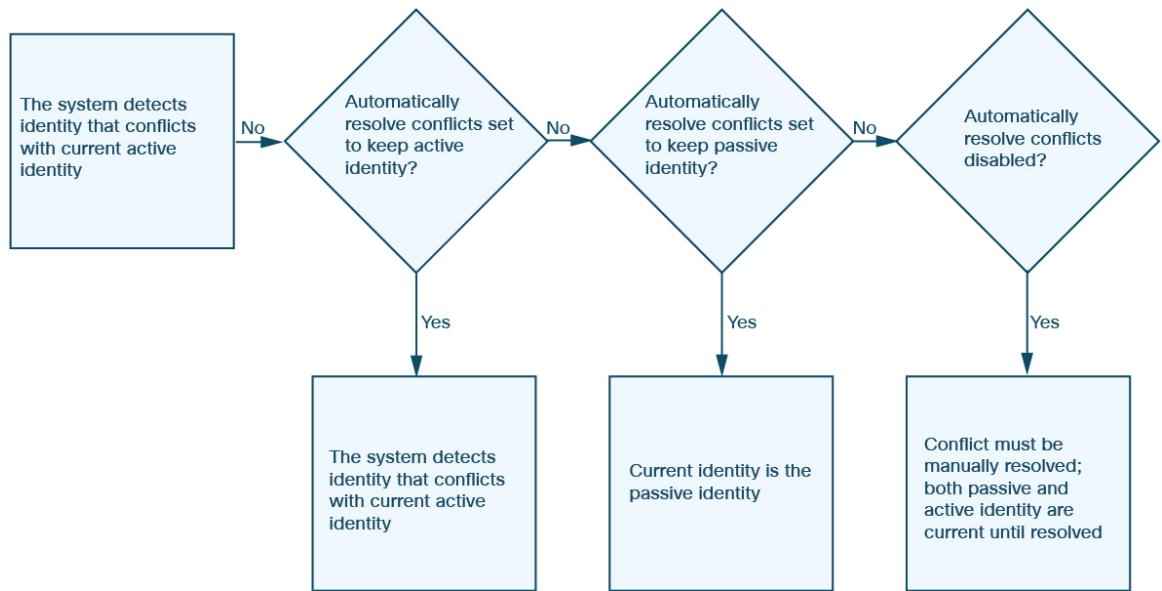
アプリケーションおよびオペレーティング システムの ID の競合

現在のアクティブ ID および以前に報告されたパッシブ ID と競合する新しいパッシブ ID が報告されると、ID の競合が発生します。たとえば、オペレーティング システムの以前のパッシブ ID は Windows 2000 と報告され、Windows XP のアクティブ ID が現在の ID になります。次に、システムが Ubuntu Linux 8.04.1 の新しいパッシブ ID を検出します。Windows XP と Ubuntu Linux の ID が競合状態になります。

NetFlow データ

ホストのオペレーティングシステムまたはホスト上のいずれかのアプリケーションの ID に対して ID の競合が存在する場合、システムは現在の ID として競合する両方の ID をリストし、競合が解決されるまで影響評価に両方の ID を使用します。

管理者特権を持つユーザは、パッシブ ID を常に使用するか、またはアクティブ ID を常に使用するかを選択することによって、自動的に ID の競合を解決できます。ID の競合の自動解決を無効にしない限り、ID の競合は常に自動的に解決されます。



管理者特権を持つユーザーは、ID の競合が発生した場合に、イベントを生成するようにシステムを設定することもできます。そのユーザは、相関応答として Nmap スキャンを使用する相関ルールで相関ポリシーを設定できます。イベントが発生すると、Nmap はホストをスキャンして、更新されたホストのオペレーティングシステムとアプリケーションデータを取得します。

NetFlow データ

NetFlowは、ルータを通過するパケットの統計情報を提供する、Cisco IOS アプリケーションの1つです。NetFlowはCiscoネットワーキングデバイスで使用できます。また、Juniper、FreeBSD、OpenBSDデバイスに組み込むことも可能です。

NetFlowがネットワークデバイスで有効にされている場合、そのデバイス上のデータベース(NetFlowキャッシュ)に、ルータを通過するフローのレコードが格納されます。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。このNetFlowデータをエクスポートするようにネットワークデバイスを設定できます。本書では、そのように設定されたネットワークデバイスをNetFlowエクスポートと呼びます。

管理対象デバイスは、NetFlowエクスポートからレコードを収集して、それらのレコードに含まれるデータに基づいて单方向の接続終了イベントを生成し、それらのイベントを接続イベントデータベースに記録するためにFirewall Management Centerに送信するように設定できます。

また、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ためのネットワーク検出ポリシー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ーできないネットワークをNetFlowエクスポートにモニターさせる場合には特に有効です。

NetFlow データを使用するための要件

NetFlow データを分析するために Firepower System を設定する前に、ルータまたは使用する他の NetFlow が有効なネットワークデバイス上で NetFlow 機能を有効にし、管理対象デバイスのセンシングインターフェイスを接続する宛先ネットワークへ NetFlow データをブロードキャストするようにデバイスを設定する必要があります。

Firepower System では、NetFlow バージョン 5 レコードと NetFlow バージョン 9 レコードをいずれも解析できます。Firepower System にデータをエクスポートするには、NetFlow エクスポートがいずれかのバージョンを使用する必要があります。さらに、このシステムでは、特定のフィールドがエクスポートされた NetFlow テンプレートとレコードに存在する必要があります。NetFlow エクスポート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、エクスポートされた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)

Firepower System 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 エクスポートの監視可能な 1 つ以上の管理対象デバイスを展開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、エクスポートされた NetFlow 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。

■ NetFlow データと管理対象デバイス データの違い

一部のネットワークデバイス上で使用可能な Sampled 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、ネットワークデバイス上の CPU 使用率が改善される可能性がありますが、Firepower System で分析するために収集されている NetFlow データに影響する場合があります。

NetFlow データと管理対象デバイス データの違い

NetFlow データで表示されるトライフィックは、直接的には分析されません。代わりに、エクスポートした NetFlow レコードを接続ログおよびホストとアプリケーションのプロトコルデータに変換します。

その結果、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、これら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

ネットワーク検出ポリシーとアクセス コントロール ポリシーの違い

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 コントロールルールごとに設定した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。

接続イベントのタイプ

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ているため、システムがログに記録する NetFlow 接続をきめ細かく制御することはできません。

NetFlow データは、セキュリティインテリジェンスイベントを生成することはできません。

NetFlow ベースの接続イベントは、接続イベントデータベースにのみ保存できます。システムログまたは SNMP トラップサーバに送信することはできません。

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を設定して、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ログに記録できます。

それに対し、エクスポートされた NetFlow レコードには単方向接続データが含まれているため、システムは処理する各 NetFlow レコードに対し少なくとも 2 つ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。

接続がまだ実行中であっても、NetFlow エクスポートは固定間隔でレコードを出力するため、長時間実行しているセッションの場合は複数のエクスポートされたレコードが生成される場合があり、その各レコードが接続イベントを生成します。たとえば、NetFlow エクスポートが 5 分ごとにエクスポートする場合に、特定の接続が 12 分間続いている場合、システムはそのセッションに対し 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

ホスト データとオペレーティング システム データ

NetFlow データからのネットワークマップに追加されたホストには、オペレーティングシステム、NetBIOS、またはホストタイプ（ホストまたはネットワークデバイス）の情報がありません。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

システムは、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 を手動で設定しない限り、NetFlow エクスポートによってモニタされるホストに脆弱性をマッピングできません。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を NetFlow データから作成されたホストに関連付けることは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。

■ NetFlow データと管理対象デバイス データの違い

システムが NetFlow レコードを処理するときには、各ホストが使用しているポート、およびそれらのポートがウェルノウンであるかどうかに基づき、アルゴリズムに従ってその情報が判別されます。

- 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、システムは番号の若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。

さらに、管理対象デバイスによって直接検出された接続の場合、システムは対応する接続イベントの 2 バイト数を記録します。

- [イニシエータ バイト数 (Initiator Bytes)] フィールドは送信バイト数を記録します。
- [レスポンダ バイト数 (Responder Bytes)] フィールドは受信バイト数を記録します。

単方向 NetFlow レコードに基づく接続イベントには、1 バイト数しか含まれておらず、ポートベースアルゴリズムに応じて、システムが [イニシエータ バイト数 (Initiator Bytes)] または [レスポンダ バイト数 (Responder Bytes)] に割り当てます。システムによって他のフィールドは 0 に設定されます。NetFlow レコードの接続の概要 (集約接続データ) を表示している場合に、両方のフィールドに値が読み込まれる場合があることに注意してください。

NetFlow のみの接続イベント フィールド

いくつかのフィールドは、NetFlow レコードから生成された接続イベントでのみ表示されます (『Cisco Secure Firewall Management Center アドミニストレーション ガイド』の「*Information Available in Connection Event Fields*」を参照してください)。

翻訳について

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