ネットワーク可視性モジュール

ネットワーク可視性モジュールについて

ユーザーが管理対象外デバイスを使用する状況が増加しているため、企業内管理者はネットワーク内外の状況を把握しにくくなっています。Network Visibility Module（NVM）は、オンプレミスまたはオフプレミスのエンドポイントから豊富なフローコンテキストを収集するもので、Cisco Secure Cloud Analytics などのシスコソリューション、Splunk、またはサードパーティソリューションと併用すると、ネットワークに接続されたデバイスおよびユーザーの動作に対する可視性を提供します。 これにより、企業内管理者は、キャパシティとサービスの計画、監査、コンプライアンス、およびセキュリティ分析を実行することができます。Network Visibility Module は、次のサービスを提供します。

- ネットワーク設計を情報に基づいてより適切に改善する（nvzFlow プロトコル仕様の IPFIX コレクタ要素の拡張：https://developer.cisco.com/site/network-visibility-module/）ために、アプリケーションの使用状況をモニタする。
- アプリケーション、ユーザー、またはエンドポイントを論理グループに分類する。
- 企業の資産を追跡し、移行アクティビティを計画するため、潜在的な異常を洗い出す。

この機能により、インフラストラクチャ導入環境全体ではなく、テレメトリを対象とするかどうかを選択できます。Network Visibility Module は、次の情報に対するより正確な可視性を得るため、エンドポイントテレメトリを収集します。

- デバイス：エンドポイント（場所に関係なく）
- ユーザー：エンドポイントにログインしているユーザー

- アプリケーション：トラフィックを生成するアプリケーション
- 場所：トラフィックが生成されるネットワークの場所
- 宛先：このトラフィックの宛先の実際の FQDN

信頼ネットワークでは、Cisco Secure Client Network Visibility Module はフローレコードをコレクタ（Cisco Secure Cloud Analytics、Splunk、またはサードパーティベンダー）にエクスポートし、このコレクタがファイル分析を実行し、UI インターフェイスおよびレポートを提供します。フロー レコードはユーザーの機能に関する情報を提供するもので、値は ID（たとえば、LoggedInUserAccountType は 12361、ProcessUserAccountType は 12362、ParentProcessUserAccountType は 12363）とともにエクスポートされます。Splunk に組み込まれた Cisco Endpoint Security Analytics（CESA）の詳細については、http://www.cisco.com/go/cesaを参照してください。ほとんどの企業内IT管理者は、データを使用して独自の可視化テンプレートを作成することを望むため、シスコは Splunk アプリケーション プラグインを介していくつかのサンプル ベース テンプレートを提供しています。

デスクトップ Cisco Secure Client 上の NVM

従来、フロー コレクタにはスイッチまたはルータのインターフェイスに入る時点またはインターフェイスから出る時点で IP ネットワーク トラフィックを収集できる機能がありました。ネットワーク内の輻輳の原因とフローパスを特定できましたが、それ以外は特定できませんでした。エンドポイントで Network Visibility Module を使用すると、デバイスのタイプ、ユーザー、アプリケーションなどの豊富なエンドポイントコンテキストによってフローが拡張されます。これにより、収集プラットフォームの機能に応じて、フローレコードがより実用的になります。IPFIX 経由で Network Visibility Module によって提供されるエクスポートデータは、Cisco NetFlow コレクタや Splunk だけでなく、他のサードパーティフロー収集プラットフォームとも互換性があります。追加情報については、各プラットフォームの統合ドキュメントを参照してください。たとえば、Splunk 統合については、https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/200600-Install-and-Configure-Cisco-Network-Visi.html で確認できます。

リリース 4.9 以降で Network Visibility Module コレクタを使用する場合、追加のパラメータを表示するには、Splunk アプリケーション 3.x を使用する必要があります。

この機能が有効になっている場合、Network Visibility Module の Cisco Secure Client プロファイルは、ISE または Secure Firewall ASA ヘッドエンドからプッシュされます。ISE ヘッドエンドでは、スタンドアロン プロファイル エディタを使用し、Network Visibility Module サービスプロファイル XML を生成して ISE にアップロードし、新しい Network Visibility Module モジュールに対してマップできます。これは、Network Access Manager での操作と同様です。Cisco Secure Firewall ASA ヘッドエンドでは、スタンドアロンプロファイルエディタまたは ASDM プロファイルエディタのいずれかを使用できます。

VPN の状態が接続済みに変更した時点と、エンドポイントが信頼ネットワーク内にある場合に、Network Visibility Module に通知が送信されます。

（注） Network Visibility Module を Linux で使用する場合は、必ず、Linux での Network Visibility Module の使用 に記載されている準備手順を事前に完了してください。

スタンドアロン NVM

展開していない、または別の VPN ソリューションを使用している場合は、Network Visibility Module のニーズに合わせてネットワーク可視性モジュールのスタンドアロンパッケージをインストールできます。Cisco Secure Clientこのパッケージは独立して動作しますが、既存の Cisco Secure Client Network Visibility Module ソリューションと同じレベルのフロー収集をエンドポイントから行います。スタンドアロンNetwork Visibility Module をインストールすると、アクティブなプロセス（macOS のアクティビティモニタなど）によってその使用が示されます。

スタンドアロンNetwork Visibility Module の設定には Network Visibility Module のプロファイルエディタ を使用し、信頼ネットワーク検出（TND）の設定が必須となります。TND の設定を使用して、Network Visibility Module はエンドポイントが社内ネットワーク上にあるかどうかを判断し、適切なポリシーを適用します。

トラブルシューティングとロギングは引き続き Cisco Secure Client DART で実行されます。AnyConnect DART は Cisco Secure Client パッケージからインストールできます。

展開モード

Network Visibility Moduleは、1) Cisco Secure Client パッケージを使用して、または 2) スタンドアロンの Network Visibility Module パッケージ（Cisco Secure Client デスクトップのみ）を使用して展開できます。Cisco Secure Client パッケージの一部として展開する手順については、「*Cisco Secure Client* の展開」の章を参照してください。そうでない場合は、次のパッケージをダウンロードすることで、完全な Cisco Secure Client パッケージがなくても最初からスタンドアロン Network Visibility Module をインストールできます。

- cisco-secure-client-win-[バージョン]-nvm-standalone-k9.msi（Windows の場合）
- cisco-secure-client-macos-[バージョン]-nvm-standalone.dmg（macOS の場合）
- cisco-secure-client-linux64-[バージョン]-nvm-standalone.tar.gz（Linux の場合）

また、Network Visibility Module は Cisco XDR のコア部分です。エンドポイントに XDR デフォルト展開をインストールすることで、オンプレミスコレクタを必要とせずにCisco XDR にテレメトリを直接送信できます。Cisco XDR はこのデータを使用して新しい検出を作成し、複数のイベントを 1 つのインシデントに関連付け、ネットワーク内の不可視のギャップを埋めます。XDR 内では、[クライアント管理（Client Management）] > [展開（Deployments）] に移動して Cisco XDR 組織内のすべての Secure Client 展開のリストを確認でき、ユーザーは、組織内の特定の展開ですべてのコンピュータにインストールする必要があるすべてのパッケージと関連プロファイルのリストを定義できます。詳細については、XDR のマニュアルを参照してください。

スタンドアロン Network Visibility Module の機能は VPN には依存していません。したがって、VPN をインストールしなくてもエンドポイントに展開できます。

すでにスタンドアロン Network Visibility Module がインストールされている場合は、同じかそれ以上のバージョンの完全な Cisco Secure Client をインストールしてシームレスに移行でき、すべての Network Visibility Module データファイルとプロファイルが保持されます。

Network Visibility Module のスタンドアロン設定にアップグレードする場合は、Network Visibility Module プロファイルでアウトオブバンドの方法（SMS など）を使用する必要があります。エンドポイントに VPN と Network Visibility Module の両方の機能が必要な場合は、VPN と Network Visibility Module の両方をインストールするために Cisco Secure Client パッケージを展開することをお勧めします。個別のインストールは推奨されません。次のシナリオではインストールが失敗します。

- スタンドアロンの Network Visibility Module のダウングレード
- 新しいバージョンのスタンドアロンの Cisco Secure Client Network Visibility Module がすでに存在する場合に、古いバージョンの Network Visibility Module をインストールする。このシナリオでは、結果としてスタンドアロン Network Visibility Module がアンインストールされる。
- Cisco Secure Client Network Visibility Module がすでに存在する場合に、スタンドアロンの Network Visibility Module の任意のバージョンをインストールする

モバイル Cisco Secure Client での NVM

Network Visibility Module（NVM）は、Google Play Store で入手可能な Android 用の Cisco Secure Client の最新バージョンに含まれています。Network Visibility Module は、Samsung Knox バージョン 2.8 以降を実行している Samsung のデバイスでサポートされています。その他のモバイル デバイスは、現在サポートされていません。

Android の Network Visibility Module は、サービスプロファイル設定の一部です。Android 上で Network Visibility Module を設定するためには、Cisco Secure Client Network Visibility Module プロファイルエディタによって Cisco Secure Client Network Visibility Module プロファイルが生成され、モバイルデバイスマネジメント（MDM）を使用して Samsung のモバイルデバイスにプッシュされます。

ガイドライン

- Network Visibility Module は、Samsung Knox バージョン 3.0 以降を実行している Samsung のデバイスでサポートされています。その他のモバイルデバイスは、現在サポートされていません。
- モバイルデバイスでは、Network Visibility Module コレクタへの接続は、IPv4 または IPv6 でサポートされています。
- Java ベースのアプリケーションでのデータ収集トラフィックはサポートされています。

Network Visibility Module の使用方法

次のシナリオでは、Network Visibility Module を使用できます。

- セキュリティ インシデントの発生後、漏洩がなかったか確認するため、ユーザのネットワーク履歴を監査する。
- システムまたは管理者権限が、ユーザのマシンで実行されているネットワーク接続プロセスにどのように影響しているか確認する。
- レガシー OS を実行しているすべてのデバイスの一覧を取得する。
- ネットワーク内のどのアプリケーションが最も多くのネットワーク帯域幅を使用しているか確認する。
- ネットワーク内で何種類のバージョンの Firefox が使用されているか確認する。
- ネットワーク内で Chrome.exe 接続の何パーセントを IPv6 が占めているか確認する。

Network Visibility Module の収集パラメータ

3 つの syslog データソース（フロー、エンドポイント ID、インターフェイス情報） の固有識別子（UDID）フィールドが、これらのソース間でレコードを関連付ける方法として使用されます。特定のインターフェイスの詳細を収集するために、InterfaceInfoUDID フィールドを使用して、フローごとのレコードをインターフェイス情報レコードと関連付けることができます。エンドポイントで収集され、コレクタにエクスポートされるパラメータを次に示します。

表 *1:* エンドポイントアイデンティティ

パラメータ	説明/注意事項
[仮想ステーション名（Virtual Station Name）]	エンドポイントで設定されたデバイス名（Boris-Macbook など） ドメイン参加マシンはの形式は <machinename>.<domainname>.<com>（CESA-WIN10-1.mydomain.com など）になります。 Android の場合、Samsung による提供がないため、空。
[UDID]	汎用一意識別子。各フローに対応するエンドポイントを一意に識別します。この UDID 値は、デスクトップの Secure Firewall ポスチャ およびモバイルの ACIDex でも報告されます。
[OS 名（OS Name）]	エンドポイントのオペレーティングシステムの名前（WinNTなど）

パラメータ	説明/注意事項
[OS のバージョン（OS Version）]	エンドポイントのオペレーティングシステムのバージョン（6.1.7601など）
[OS のエディション（OS Edition）]	OS のエディション（Windows 8.1 Enterprise Edition など）
[SystemManufacturer]	エンドポイントの製造元（Lenovo、Apple など）
[システム タイプ（System Type）]	Android の場合、`arm` に設定。 それ以外のプラットフォームの場合、`x86` または`x64`。
[Agent バージョン（Agent Version）]	エンドポイント上で実行されている Network Visibility Module クライアントソフトウェアのバージョン。通常は major_v.minor_v.build_no の形式
Timestamp	エンドポイント データの絶対タイムスタンプ（ミリ秒単位）。
AMP GUID	Cisco Secure Endpoint（AMP）の一意のエンドポイント ID

表 *2:* インターフェイス情報

パラメータ	説明/注意事項
[エンドポイント UDID（Endpoint UDID）]	UDID と同じ。
[InterfaceInfoUID]	インターフェイスメタデータの一意の ID。InterfaceInfo レコードからインターフェイスメタデータを検索するために使用されます。
[インターフェイス インデックス（Interface Index）]	OSによって報告されたネットワーク インターフェイスのインデックス。
[インターフェイス タイプ（Interface Type）]	インターフェイスのタイプ（有線、ワイヤレス、セルラー、VPN など）。
[インターフェイス名（Interface Name）]	OSによって報告されたネットワーク インターフェイス/アダプタの名前。
[インターフェイス詳細リスト（Interface Details List）]	状態およびSSID、InterfaceDetailsListの属性。インターフェイスのネットワークの状態（信頼または非信頼）と、当該の接続の SSID を示す。

パラメータ	説明/注意事項
[インターフェイス MAC アドレス（Interface MAC address）]	インターフェイスの MAC アドレス。 デスクトップのみ。Android の場合は空（サポートされていないため）
Timestamp	インターフェイスレコードの絶対値（ミリ秒単位）。

表 *3:* フロー情報

パラメータ	説明/注意事項
[送信元 IPv4 アドレス（Source IPv4 Address）]	フローがエンドポイントで生成されたインターフェイスの IPv4 アドレス。
[宛先 IPv4 アドレス（Destination IPv4 Address）]	フローがエンドポイントから生成された宛先の IPv4 アドレス。
[送信元転送ポート（Source Transport Port）]	フローがエンドポイントで生成された送信元ポート番号。
[宛先転送ポート（Source Transport Port）]	フローがエンドポイントから生成された宛先ポート番号。
フローの方向	エンドポイントで観測されるフローの方向。これは、エンドポイントから収集される必須パラメーターです。2 つの値は、0 が入力フロー、1 が出力フローです。
[送信元 IPv6 アドレス（Source IPv6 Address）]	フローがエンドポイントで生成されたインターフェイスの IPv6 アドレス。 Android の場合は空（サポートされていないため）
[宛先 IPv6 アドレス（Destination IPv6 Address）]	フローがエンドポイントから生成された宛先の IPv6 アドレス。 Android の場合は空（サポートされていないため）
[開始時刻（秒）（Start Sec）] [終了時刻（秒）（End Sec）]	フローの開始または終了を示す絶対タイムスタンプ（ミリ秒単位）。
[開始ミリ秒（Start Msec）] [終了ミリ秒（End Msec）]	フローの開始または終了を示す絶対タイムスタンプ（秒単位）。
[フロー UDID（Flow UDID）]	UDID と同じ。

パラメータ	説明/注意事項
[ログイン ユーザ（Logged In User）]	物理デバイス上のログインユーザ名（Authority\Principal 形式） Android の場合は空（サポートされていないため）
[ログイン ユーザのアカウント タイプ（Logged In User Account Type）]	ログインユーザのアカウントタイプ。 Android の場合は空（サポートされていないため）
[プロセス ID（Process ID）]	ネットワークフローを開始したプロセスのプロセス ID。
[プロセス名（Process Name）]	エンドポイントでネットワークフローを生成する実行可能ファイルの名前。
[プロセス ハッシュ（Process Hash）]	エンドポイントでネットワークフローを生成する実行可能ファイルの一意の SHA256 ハッシュ。
[プロセス アカウント（Process Account）]	エンドポイントでネットワークフローを生成するアプリケーションが実行されたコンテキストでの Authority\Principle 形式の完全修飾アカウント。 Android の場合は空（サポートされていないため）
[プロセスアカウントタイプ（Process Account Type）]	プロセスアカウントのアカウントタイプ。 Android の場合は空（サポートされていないため）
[プロセスパス（Process Path）]	ネットワークフローを開始したプロセスのファイルシステムパス Android の場合は空（サポートされていないため）
[プロセス引数（Process args）]	ネットワークフローを開始したプロセスのコマンドライン引数（プロセスパスを除く）。 Android の場合は空（サポートされていないため）
[親プロセス ID（Parent Process ID）]	ネットワークフローを開始したプロセスの親プロセスの ID。
[親プロセス名（Parent Process Name）]	エンドポイントでネットワークフローを生成するアプリケーションの親プロセスの名前。
[親プロセス ハッシュ（Parent Process Hash）]	エンドポイントでネットワークフローを生成するアプリケーションの親プロセスの実行可能ファイルの一意の SHA256 ハッシュ。Android の場合、0 に設定。

パラメータ	説明/注意事項
[親プロセスのアカウント（Parent Process Account）]	エンドポイントでネットワークフローを生成するアプリケーションの親プロセスが実行されたコンテキストでの Authority \ Principle 形式の完全修飾アカウント。 Android の場合は空（サポートされていないため）
[親プロセスのアカウント タイプ（Parent Process Account Type）]	親プロセスアカウントのアカウントタイプ。 Android の場合は空（サポートされていないため）
[親プロセスパス（Parent Process Path）]	ネットワークフローを開始したプロセスの親のファイルシステムパス。 Android の場合は空（サポートされていないため）
[親プロセス引数（Parent Process Args）]	ネットワークフローを開始したプロセスの親のコマンドライン引数（親プロセスパスを除く）。 Android の場合は空（サポートされていないため）
[DNS サフィックス（DNS suffix）]	エンドポイント上のフローに関連付けられたインターフェイス上で設定。
[L4ByteCountIn]	レイヤ 4 のエンドポイントでの特定のフロー中にダウンロードされた合計バイト数（L4 ヘッダーを除く）。
[L4ByteCountOut]	レイヤ 4 のエンドポイントでの特定のフロー中にアップロードされた合計バイト数（L4 ヘッダーを除く）。
[宛先ホスト名（Destination Hostname）]	エンドポイントの宛先 IP に解決される実際の FQDN
[インターフェイス UID（Interface UID）]	インターフェイス情報テーブルのインターフェイス UID と同じ。UDID とともに送信されるインターフェイスレコードからこのフローのインターフェイス情報を識別するために使用されます。
[モジュール名リスト（Module Name List）]	フローを生成したプロセスによってホストされているモジュールの 0 個以上の名前のリスト。dllhost、svchost、rundll32 などの一般的なコンテナ内にメインの DLL を含めることができます。また、JVM の jar ファイルの名前など、他のホストされているコンポーネントを含めることもできます。 Android の場合は空（サポートされていないため）

パラメータ	説明/注意事項
[モジュールのハッシュ リスト（Module Hash List）]	モジュール名リストに関連付けられているモジュールの 0 個以上の SHA256 ハッシュのリスト。 Android の場合は空（サポートされていないため）
追加のログインユーザーリスト	（Windows のみ） nzFlowLoggedInUser 以外のデバイスにログインしているユーザーのリスト（各ユーザーは SessionType:AccountType:Authority\Principal の形式で表される）。たとえば、rdp:8001:ACME\JSmith console:0002:<machine>\Administrator アップグレード中、デフォルトでは、このパラメータは、1）古いバージョンの NVM のプロファイルにデータ収集ポリシーがないか、データ収集ポリシーが含まれている場合、または 2）古いバージョンの NVM のプロファイルに除外データ収集ポリシーがあり、4.10 プロファイルエディタでプロファイルが開かれて保存された場合に、レポートから除外されます。 （注） 非システムプロセスの場合、このフィールドは空です。
プロセス完全性レベル	完全性レベルは、プロセスと別のオブジェクト（ファイル、プロセス、またはスレッド）間の信頼を定義します。
親プロセスの完全性レベル	完全性レベルは、親プロセスと別のオブジェクト（ファイル、プロセス、またはスレッド）間の信頼を定義します。
フローレポートステージ	フローレコードのステージ。0：終了フローレコード、1：開始フローレコード、2：定期/中間フローレコード。

Network Visibility Module のプロファイルエディタ

プロファイル エディタで、コレクション サーバの IP アドレスまたは FQDN を設定します。送信するデータのタイプや、データ匿名化の有効/無効を選択することで、データ収集ポリシーをカスタマイズすることもできます。

ネットワーク可視性モジュールは、OS で優先される IP アドレスに対して、IPv4 アドレスのシングル スタック IPv4、IPv6 アドレスのシングル スタック IPv6、またはデュアル スタック IPv4/IPv6 で接続を確立できます。

モバイル ネットワーク可視性モジュールは、IPv4 を使用してのみ接続を確立できます。IPv6 接続はサポートされていません。

（注） ネットワーク可視性モジュールがフロー情報を送信するのは、信頼できるネットワーク上に限られます。デフォルトでは、データは収集されません。データが収集されるのは、プロファイルでそのように設定されている場合のみです。エンドポイントが接続されている間は、データが継続して収集されます。非信頼ネットワーク上で収集が行われた場合、データはキャッシュされ、エンドポイントが信頼ネットワーク上に接続された際に送信されます。収集データを Cisco Secure Cloud Analytics 7.3.1 以前のリリース（または Splunk や同様の SIEM ツール以外のもの）に送信する場合、キャッシュデータは信頼ネットワークに送信はされますが、処理されません。Cisco Secure Cloud Analytics アプリケーションについては、『Cisco Secure Cloud Analytics Enterprise Endpoint License and NVM Configuration Guide』[英語] を参照してください。

TND が Network Visibility Module プロファイルに設定されている場合、信頼ネットワーク検出は Network Visibility Module によって実行され、エンドポイントが信頼ネットワーク内にあるかどうかの判断は VPN に依存しません。また、VPN 接続状態にある場合、エンドポイントは信頼ネットワークにあると見なされ、フロー情報が送信されます。NVM に固有のシステムログに信頼ネットワーク検出の使用状況が表示されます。

Network Visibility Module プロファイルで TND を直接設定する場合、管理者が定義した信頼できるサーバーと証明書ハッシュによって、ユーザーが信頼できるネットワーク上にいるか、信頼できないネットワーク上にいるかが判別されます。コア VPN プロファイルの信頼ネットワーク検出を設定する管理者は、代わりに、コア VPN プロファイルで信頼された DNS ドメインと信頼された DNS サーバーを設定します。Cisco Secure Client プロファイルエディタ、プリファレンス（Part 2）

- [デスクトップ（Desktop）] または [モバイル（Mobile）] ：Network Visibility Module をデスクトップとモバイルデバイスのどちらにセットアップするかを決定します。[デスクトップ（Desktop）] がデフォルトです。
- **コレクタの設定**
  - [IP アドレス/FQDN（IP Address/FQDN）] ：コレクタの IPv4 または IPv6 の IP アドレス/FQDN を指定します。
  - [ポート（Port）] ：コレクタがリッスンするポート番号を指定します。
  - [セキュア（Secure）] ：Network Visibility Module が DTLS 経由でコレクタにデータを安全に送信するかどうかを決定します。このチェックボックスをオンにすると、Network Visibility Module はトランスポートに DTLS を使用します。DTLS 接続では、DTLS サーバ（コレクタ）証明書がエンドポイントによって信頼されている必要があります。信頼できない証明書はサイレントに拒否されます。

    DTLS サポートには CESA Splunk App v3.1.0 の一部としてのコレクタが必要であり、DTLS 1.2 が最小サポートバージョンです。
- **キャッシュの設定**
  - [最大サイズ（Max Size）] ：データベースが到達できる最大サイズを指定します。以前はキャッシュ サイズに事前設定の制限がありましたが、プロファイル内で設定でき

るようになりました。キャッシュのデータは暗号化された形式で保存され、ルート権限のプロセスのみがデータを復号化できます。

サイズ制限に到達すると、最新データの代わりに最も古いデータがスペースからドロップされます。

- [最高期間（Max Duration）]：データを保存する日数を入力します。最大サイズも設定している場合は、最初に到達した制限が優先されます。

  日数制限に到達すると、最新の日付のデータの代わりに最も古い日付のデータがスペースからドロップされます。[最高期間（Max Duration）] のみを設定している場合は、サイズ制限がありません。どちらも無効にしている場合は、サイズが 50 MB に制限されます。

- **[定期テンプレート（Periodic Template）]**：テンプレートがエンドポイントから送信される間隔を指定します。デフォルト値は 1440 分です。

- [定期的なフローレポート（Periodic Flow Reporting）]（任意、デスクトップのみに該当）：クリックすると、フローレポートが定期送信されます。デフォルトで、Network Visibility Module は接続終了時にフローに関する情報を送信します（このオプションが無効のとき）。フローを閉じる前にフローに関する情報が定期的に必要な場合は、間隔を秒単位で設定します。値 0 は各フローの開始時と終了時にフロー情報が送信されることを意味します。値が *n* の場合、フロー情報は各フローの開始時、*n* 秒ごと、および終了時に送信されます。長時間の接続を、フローが閉じられるまで待つことなく追跡するためには、この設定を使用します。

- **[集約間隔（Aggregation interval）]**：データフローをエンドポイントからエクスポートする間隔を指定します。デフォルト値の 5 秒を使用すると、単一のパケットで複数のデータフローがキャプチャされます。間隔の値が 0 秒の場合は、パケットごとに単一のデータフローが含まれます。有効な範囲は 0 ~ 600 秒です。

- [スロットル レート（Throttle Rate）]：スロットリングは、エンド ユーザーへの影響が最小限になるように、キャッシュからコレクタにデータが送信されるレートを制御します。キャッシュされたデータがある限り、リアルタイムデータとキャッシュされたデータの両方にスロットリングを適用できます。スロットル レートを Kbps 単位で入力します。デフォルト値は 500 Kbps です。

  キャッシュ データはこの一定期間後にエクスポートされます。この機能を無効にするには 0 を入力します。

- [収集モード（Collection Mode）]：エンドポイントのデータを収集する時点を指定するには、[収集モードがオフ（collection mode is off）]、[信頼ネットワークのみ（trusted network only）]、[信頼できないネットワークのみ（untrusted network only）]、または [すべてのネットワーク（all networks）] を選択します。

- [収集基準（Collection Criteria）]：データ収集期間に不要なブロードキャストを減らすことによって、関連データだけを分析できるようになります。次のオプションを使用して、データ収集を制御します。

  - [ブロードキャスト パケット（Broadcast packets）] および [マルチキャスト パケット（Multicast packets）]：デフォルトでは、効率性のため、バックエンド リソースにか

かる時間が削減されるよう、ブロードキャストパケットおよびマルチキャストパケットの収集はオフになっています。ブロードキャストパケットとマルチキャストパケットの収集を有効にし、データをフィルタリングするには、チェックボックスをオンにします。

- [KNOX のみ（KNOX only）]（任意、モバイルのみ）：オンにすると、KNOX ワークプレイスからのみデータが収集されます。デフォルトではこのフィールドはオフで、ワークプレイス外からもデータが収集されます。

- [データ収集ポリシー（Data Collection Policy）]：データ収集ポリシーを追加して、ネットワーク タイプまたは接続シナリオに関連付けできます。複数のインターフェイスを同時にアクティブにすることができるため、あるプロファイルを VPN トラフィックに適用し、別のプロファイルを非 VPN トラフィックに適用できます。

  [追加（Add）] をクリックすると、[データ収集ポリシー（Data Collection Policy）] ウィンドウが表示されます。ポリシーを作成するときに、次の点に留意してください。

  - ポリシーを作成していない場合、またはポリシーをネットワーク タイプに関連付けていない場合は、デフォルトでは、すべてのフィールドがレポートおよび収集されます。
  - それぞれのデータ コレクション ポリシーを少なくとも 1 つのネットワーク タイプに関連付ける必要がありますが、2 つのポリシーを同じネットワーク タイプに関連付けることはできません。
  - より具体的なネットワーク タイプを含むポリシーが優先されます。たとえば、VPN は信頼ネットワークに属しているため、VPN をネットワーク タイプとして含むポリシーはネットワーク タイプとして信頼が指定されたポリシーより優先されます。
  - 選択したコレクションモードに基づいて適用されるネットワークに対してのみデータ コレクション ポリシーを作成できます。たとえば、[収集モード（Collection Mode）] が[信頼ネットワークのみ（Trusted Network Only）] に設定されている場合、[非信頼（Untrusted）] の[ネットワーク タイプ（Network Type）] には、[データ収集ポリシー（Data Collection Policy）] を作成できません。
  - 以前の Cisco Secure Client リリースのプロファイルがそれより後の Cisco Secure Client リリースのプロファイルエディタで開かれた場合、プロファイルは、新しい方のリリースに自動的に変換されます。変換により、以前匿名化されていたフィールドを除外するデータ収集ポリシーが追加されます。
  - [名前（Name）]：作成するポリシーの名前を指定します。
  - [ネットワーク タイプ（Network Type）]：収集モードを指定するか、[VPN]、[信頼（trusted）]、または [非信頼（untrusted）] を選択してデータ収集ポリシーを適用するネットワークを指定します。信頼を選択した場合は、ポリシーが VPN ケースにも適用されます。
  - [フロー フィルタ ルール（Flow Filter Rule）]：一連の条件と、すべての条件が満たされたときに実行するアクションを、フローの収集または無視として定義します。最大

25 のルールを設定でき、各ルールに最大 25 の条件を定義できます。[フロー フィルタ ルール（Flow Filter Rule）] リストの右側にある上下ボタンを使用してルールの優先順位を調整し、後続のルールよりも優先的に考慮されるように設定します。[追加（Add）] をクリックし、フロー フィルタ ルールのコンポーネントを設定します。

- [名前（Name）]：フロー フィルタ ルールの一意の名前。
- [タイプ（Type）]：各フィルタ ルールには[収集（Collect）]または[無視（Ignore）]が指定されます。フィルタ ルールが満たされた場合に適用するアクション（[収集（Collect）] または [無視（Ignore）]）を決定します。[収集（Collect）] する場合、条件が満たされるとフローが許可されます。[無視（Ignore）] する場合、フローはドロップされます。
- [条件（Conditions）]：照合する各フィールドのエントリと、合致と見なすのはそのフィールド値が等しいときか等しくないときか、判断する操作を追加します。各操作にはフィールド識別子とそのフィールドに対応する値が含まれます。フィールドの一致では、フィルタ エンジン ルールの設定でルール セットに大文字と小文字を区別しない操作（EqualsIgnoreCase）を適用しない限り、大文字と小文字が区別されます。有効にした後、ルール下で設定された値フィールドへの入力は、大文字と小文字が区別されません。

- **[包含（Include）]/[除外（Exclude）]**
  - [タイプ（Type）]：データ収集ポリシーで [包含（Include）] または [除外（Exclude）] するフィールドを決定します。デフォルトは [除外（Exclude）] です。オンになっていないフィールドはすべて収集されます。どのフィールドもオンになっていない場合は、フィールドはすべて収集されます。
  - [フィールド（Fields）]：エンドポイントから受信する情報と、ポリシー要件を満たすためにデータ収集に含めるフィールドを決定します。ネットワークタイプ、およびどのフィールドを含めるか、または除外するかに基づいて、Network Visibility Module はエンドポイント上で適切なデータを収集します。

（注） 次のシナリオのいずれかが存在する場合、アップグレード中に、ProcessPath、ParentProcessPath、ProcessArgs、および ParentProcessArgs はデフォルトで、フロー情報でレポートされないように除外されます。

- 古いバージョンの Network Visibility Module のプロファイルにデータ収集ポリシーがない場合、またはデータ収集ポリシーが含まれていない場合。
- 古いバージョンの Network Visibility Module のプロファイルに除外データ収集ポリシーがあり、新しいバージョンのプロファイルエディタでプロファイルが開かれて保存された場合。古いバージョンの Network Visibility Module のプロファイルに除外データ収集ポリシーがあったが、新しい 4.9 以降のバージョンのプロファイルエディタでプロファイルが開かれて保存されていない場合は、次の 4 つのフィールドが含まれます。

Network Visibility Module が親プロセス ID を計算できない場合、値はデフォルトで 4294967295 になります。

FlowStartMsec と FlowStopMsec は、フローのエポックタイムスタンプをミリ秒単位で決定します。

インターフェイスの状態と SSID を選択して、インターフェイスのネットワーク状態が信頼できるかどうかを指定できます。

- [任意の匿名化フィールド（Optional Anonymization Fields）]：同一のエンドポイントからのレコードを、プライバシーを維持しつつ関連付ける場合は、該当するフィールドを匿名化対象に選択します。次に、実際の値ではなく、値のハッシュとして送信されます。匿名化ではフィールドのサブセットが利用できます。

  包含/除外指定のフィールドは匿名化できません。同様に、匿名化と指定したフィールドは包含/除外できません。

- [Knoxのデータ収集ポリシー（モバイルのみ）（Data Collection Policy for Knox (Mobile Specific)]：モバイルプロファイルを選択した場合にデータ収集ポリシーを指定するオプションです。Knox コンテナのデータ収集ポリシーを作成するには、[範囲（Scope）] の下の [Knox のみ（Knox-Only）] チェックボックスをオンにします。[デバイスの範囲（Device Scope）] で適用されるデータ収集ポリシーは、別の Knox コンテナデータ収集ポリシーが指定されていない限り、Knox コンテナトラフィックの場合も適用されます。データ収集ポリシーを追加または削除するには、前述の [データ収集ポリシー（Data Collection Policy）] の説明を参照してください。モバイルプロファイルでは最大 6 つの異なるデータ収集ポリシー（デバイス用に 3 つ、Knox 用に 3 つ）を設定できます。

- [利用規定（Acceptable Use Policy）]（任意、モバイルのみ）：[編集（Edit）] をクリックして、ダイアログ ボックス上でモバイル デバイス用の利用規定を定義します。終了したら、[OK] をクリックします。最大 4000 文字を使用できます。

  このメッセージは、Network Visibility Module が設定されると、ユーザーに対して表示されるようになります。リモートユーザーは、Network Visibility Module アクティビティの拒否を選択できません。ネットワーク管理者は、MDM 機能を使用して Network Visibility Module を制御します。

- [モバイルネットワークでのエクスポート（Export on Mobile Network）]（オプションおよびモバイルのみ）：デバイスがモバイルネットワークを使用している場合に Network Visibility Module フローのエクスポートを許可するかどうかを指定します。有効な場合（デフォルト値）、エンドユーザーは、[利用許可ポリシー（Acceptable User Policy）] ウィンドウが表示されているとき、または後で Cisco Secure Client Android アプリケーションで **[設定（Settings）]** > **[NVM 設定（NVM-Settings）]** > > **[NVM にモバイルデータを使用する（Use mobile data for NVM）]** チェックボックスをオンにして、管理者を上書きできます。[モバイルネットワークでのエクスポート（Export on Mobile Network）] チェックボックスをオフにすると、デバイスがモバイルネットワークを使用している場合に Network Visibility Module フローがエクスポートされず、エンドユーザーはそれを変更できません。

- [信頼ネットワーク検出（Trusted Network Detection）]：この機能は、エンドポイントが物理的に社内ネットワーク上にあるかどうかを検出します。ネットワークの状態は、いつデータをエクスポートし、いつ適切なデータ収集ポリシーに適用するかを決定するために Network Visibility Module によって使用されます。[設定（Configure）] をクリックして、信頼ネットワーク検出の設定を行います。SSL プローブが設定済みの信頼できるヘッドエンドに送信され、到達可能であれば、証明書で応答します。次に、サムプリント（SHA-256 ハッシュ）が抽出され、プロファイル エディタのハッシュ セットと照合されます。一致が見つかった場合はエンドポイントが信頼ネットワーク内にあることを意味します。ただし、ヘッドエンドが到達不能である場合、または証明書ハッシュが一致しない場合、エンドポイントは信頼されていないネットワーク内にあると見なされます。

（注） 内部ネットワーク外から操作している場合、信頼ネットワーク検出は DNS 要求を行い、設定されたサーバーへの SSL 接続を確立しようとします。シスコでは、内部ネットワーク外で使用されているマシンからのこのような要求によって組織内の名前や内部構造が明らかになることを防ぐために、エイリアスの使用をお勧めします。

1. **https://**：信頼されている各サーバの URL（IP アドレス、FQDN、またはポートアドレス）を入力し、[追加（Add）] をクリックします。

（注） プロキシの背後にある信頼サーバはサポートされません。

2. [証明書ハッシュ（SHA-256）（Certificate Hash (SHA-256)）]：信頼されているサーバへのSSL接続が成功した場合、このフィールドは自動的に入力されます。それ以外の場合は、サーバ証明書のSHA-256ハッシュを入力して[設定（Set）]をクリックすることにより手動で設定できます。
3. [信頼されているサーバのリスト（List of Trusted Servers）]：このプロセスで複数の信頼されているサーバを定義できます（最大値は10です）。サーバは、設定されている順序で信頼ネットワーク検出に対して試行されるため、[上に移動（Move Up）]ボタンと[下に移動（Move|Down）]ボタンを使用して順序を調整できます。エンドポイントが最初のサーバに接続できなかった場合は、2番目のサーバという順序で試行されます。リスト内のすべてのサーバをした後、エンドポイントは10秒待機してからもう一度途最終試行を行います。サーバが認証されると、エンドポイントは信頼ネットワーク内で考慮されます。

プロファイルを`NVM_ServiceProfile.xml`として保存します。この名前でプロファイルを保存する必要があります。そうしないと、Network Visibility Moduleはデータの収集と送信に失敗します。

フロー フィルタについて

フローフィルタの追加により、各フローで指定したフィールドに対してアクションが設定されている、単にフィールド中心であるものから現在のデータ収集ポリシーが拡張されます。フローフィルタを使用して、フロー全体（特定のフィールドのみでなく）を収集または無視するルールを作成して適用できるため、関心対象のトラフィックだけを監視し、ストレージ要件を軽減できる可能性があります。

ルール条件

- ルールとは、ルールに指定したすべての条件がフローデータに対して満たされた場合のみの一致です。
- 最初に満たされたルールがフローに適用されます。
- フィルタポリシーで許可されている場合は、残りのデータ収集ポリシー（[包含（include）]フィールド、[除外（exclude）]フィールド、[匿名化（anonymized）]フィールド）もフローに適用されます。
- 複数のルールのインスタンスを使用する場合、
  - フローデータに一致するルールがない場合、フローに対して行われるアクションはありません。デフォルトの動作（フローの収集）が行われます。
  - ルールがフローデータと一致すると、そのフローのルールで指定されたアクションが適用されます。それより後のルールはチェックされません。Network Visibility Moduleのプロファイルエディタの[フロー フィルタ ルール（Flow Filter Rule）]パラメータで指定したルールの順序は、一致が複数発生した場合の優先順位を表します。

ワイルドカード、CIDR、およびエスケープ シーケンスのサポートの使用

ルールの条件を入力する際、IP アドレスの場合は、ワイルドカード文字または CIDR 表記法を使用して、より広い範囲のフィールド値を定義できます。また、フィールド値に特定のエスケープ シーケンスを使用できます。IP フィールドの場合、CIDR スラッシュ（/）表記法で、ルールに一致する必要がある IP アドレスを指定できます。たとえば、「192.30.250.00/16」は、「255.255.0.0」のサブネット マスクを適用することで派生したルーティング プレフィックス「192.30.0.0」を持つすべてのアドレスと一致します。テキスト フィールドの場合、ワイルドカード（* および ?）とエスケープ シーケンス（*、\?、および \\）を使用してより広い入力範囲を取得できます。たとえば、「Jane*」というログイン ユーザーは、「Jane」で開始するすべてのユーザー名と一致します。

フロー フィルタリング シナリオを実現するサンプル設定

特定のポート（ポート 53 など）ですべての UDP トラフィックをドロップするには、フロー フィルタ ルール タイプ [無視（Ignore）] と、次の 2 つの条件を設定します。

- 条件 1：フロー プロトコルは UDP と [等しい（Equals）] ことを指定します。
- 条件 2：ポート番号が 53 と [等しい（Equals）] ことを指定します。

1 つの特定のプロセス（Tor ブラウザなど）から発信されたトラフィックのみを収集するには、次の 1 つの条件を追加して、その他すべてのフローをドロップする [無視（Ignore）] のタイプを使用したフィルタ ルールを設定します。

- 条件 1：プロセス名が Tor ブラウザと [等しくない（Not Equals）] ことを指定します。

サブネット内の 1 つの特定の IP から発信されたトラフィックのみを収集するには、次の 2 つのルールを設定します。

- ルール 1：IPv4 発信元アドレスが 192.168.30.14 と [等しい（Equals）] 条件で [収集（Collect）] するタイプのルールを設定します。
- ルール 2：IPv4 発信元が 192.168.30.0/24 と [等しい（Equals）] 条件で [無視（Ignore）] するタイプの 2 つ目のルールを設定します。

カスタマー フィードバック モジュールによる NVM ステータスの提供

カスタマー フィードバック モジュールのコレクションの一部は、Network Visibility Module がインストールされているかどうか、1 日のフロー数、および DB サイズについてのデータを提供します。

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。