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。ネットワークの可視性モジュール（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、Stealthwatch などのシスコ ソリューションまたは Splunk などのサードパーティ 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。NVM 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（VzFlow プロトコル仕様の IPFIX コレクタ要素の拡張）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、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。NVM 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：エンドポイントにログインしているユーザ
- 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、AnyConnect NVM はフロー レコードをコレクタ（Cisco Stealthwatch、または LiveAction などのサードパーティ 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 インターフェイスを提供します。フロー レコードはユーザ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 などのサードパーティ ベンダーも、レポートを表示するための UI インターフェイスを提供します。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 AnyConnect での 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 NVM を使用すると、デバイスのタイプ、ユーザ、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 NVM によって提供されるエクスポート データは、Cisco NetFlow コレクタだけでなく、Splunk、IBM Qradar、LiveAction などの他のサードパーティ フロー収集プラットフォームと互換性があります。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。

ネットワーク可視性モジュールのインストールを選択すると、AnyConnect Secure Mobility Client UI の [バージョン情報（About）] 画面に、このモジュールがインストール済みとしてリストされます。NVM の実行中、AnyConnect UI に他の表示はありません。

NVM の AnyConnect プロファイルは、ISE または ASA ヘッドエンドからプッシュされます（この機能が有効な場合）。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、NVM 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 NVM モジュールに対してマップできます。これは、Web セキュリティ、ネットワーク アクセス マネージャなどでの操作と同様です。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、NVM に通知が送信されます。

（注） NVM を Linux で使用する場合は、必ず、Linux 上での NVM 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。

モバイル AnyConnect での NVM

ネットワーク可視性モジュール（NVM）は、Google Play ストアで入手可能な Android 用の Cisco AnyConnect セキュア モビリティ クライアントの最新バージョン（リリース 4.0.09xxx）に含まれています。NVM 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 のネットワーク可視性は、サービス プロファイル設定の一部です。Android 上で NVM を設定するためには、AnyConnect NVM プロファイル エディタによって AnyConnect NVM 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。NVM をモバイル デバイス用に設定するには、AnyConnect リリース 4.4.3 以降の AnyConnect NVM プロファイル エディタが必要です。

ガイドライン

- NVM 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、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。

NVM の使用方法

NVM は、次のシナリオで使用できます。

- 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。

NVM 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。

（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。

TND が NVM 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 NVM 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。ただし、TND が NVM プロファイルに明示的に設定されていない場合、NVM は VPN の TND 機能を使用してエンドポイントが信頼ネットワーク内にあるかどうかを判断します。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 TND の使用状況が表示されます。TND パラメータの設定については、「AnyConnect プロファイル エディタ、プリファレンス（Part 2）」を参照してください。

- [デスクトップ（Desktop）] または [モバイル（Mobile）]：NVM 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。 モバイルは、将来的にサポートされます。
- **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。
- **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、NVM 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。

- [スロットルレート（Throttle Rate）]：スロットリングは、エンドユーザ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 AnyConnect リリースのプロファイルがそれより後の AnyConnect 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。追加情報については、フロー フィルタについて （9 ページ）を参照してください。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。このフィールドに入力する文字列はすべて、大文字と小文字が区別されます。

  [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がすべて収集され、すべてのフィールドがオフにされます。
  - [フィールド（Fields）]：データ収集ポリシーの一部とするフィールドを決定します。 ネットワーク タイプと包含または除外するフィールドに基づいて、NVM はエンドポイント上で該当するデータを収集します。

    AnyConnect リリース 4.4（およびそれ以降）では、インターフェイスの状態と SSID を選択できるようになりました。これによりインターフェイスのネットワーク状態を信頼する/信頼しないを指定します。
  - [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。これにより、フィールド情報は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。

- [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、NVM が設定されると、ユーザに対して表示されるようになります。リモート ユーザは、NVM 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 NVM を制御します。

- [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 NVM が使用して、いつ NVM 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します。[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、TND は DNS 要求を行い、設定されたサーバへの 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。

TND が NVM プロファイルに設定されておらず、VPN モジュールがインストールされている場合、NVM は VPN の TND 機能を使用して、エンドポイントが信頼ネットワーク内にあるかどうかを判断します。NVM プロファイル エディタの TND 設定には次が含まれます。

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、NVM 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。NVM 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 ユーザは、「Jane」で開始するすべてのユーザ名と一致します。

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。

NVM のコレクション パラメータ

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）]	
[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 HostScan でも報告されます。
[OS 名（OS Name）]	
[OS のバージョン（OS Version）]	
[SystemManufacturer]	
[システム タイプ（System Type）]	それ以外のプラットフォームの場合、`x86` または `x64`。
[OS のエディション（OS Edition）]	

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。

パラメータ	説明/注意事項
[インターフェイス UID（Interface UID）]	
[インターフェイス インデックス（Interface Index）]	
[インターフェイス タイプ（Interface Type）]	
[インターフェイス名（Interface Name）]	
[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。
[インターフェイス MAC アドレス（Interface MAC address）]	Windows および Mac OS のみ

表 *3:* フロー情報

プロトコル識別子	説明/注意事項
[送信元 IPv4 アドレス（Source IPv4 Add）]	
[宛先 IPv4 アドレス（Destination IPv4 Addr）]	
[送信元転送ポート（Source Transport Port）]	
[宛先転送ポート（Source Transport Port）]	
[送信元 IPv6 アドレス（Source IPv6 Addr）]	
[宛先 IPv6 アドレス（Destination IPv6 Addr）]	
[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的なタイムスタンプ。
[フロー UDID（Flow UDID）]	UDID と同じ。
[ログイン ユーザ（Logged In User）]	

プロトコル識別子	説明/注意事項
[ログイン ユーザのアカウント タイプ（Logged In User Account Type）]	Windows および Mac OS のみ。
[プロセス アカウント（Process Account）]	
[プロセス アカウントのタイプ（Process Account type）]	Windows および Mac OS のみ。
[プロセス名（Process Name）]	
[プロセスハッシュ（Process Hash）]	
[親プロセスのアカウント（Parent Process Account）]	
[親プロセスのアカウント タイプ（Parent Process Account Type）]	Windows および Mac OS のみ。
[親プロセス名（Parent Process Name）]	
[親プロセス ハッシュ（Parent Process Hash）]	
[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]	
[L4ByteCountOut]	
[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）]	
[モジュール名リスト（Module Name List）]	
[モジュールのハッシュ リスト（Module Hash List）]	

（注） また NVM は、エンドポイントのアイデンティティに関する情報を定期的に送信します。

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、NVM 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。