CHAPTER 3

導入の準備

この章は、次の内容で構成されています。

概要

Cisco NAC Profiler を配備し、設定する前に、Cisco NAC Profiler が既存のインフラストラクチャとどのように相互作用するかに応じていくつかの計画タスクを実行する必要があります。

第 2 章「Cisco NAC Profiler アーキテクチャの概要」で概説するように、Cisco NAC Profiler システムは、スタンドアロン アプライアンスである Cisco NAC Profiler Server と、Cisco NAC アプライアンス システムの一部として配置された Clean Access Server アプライアンス（NAC-3310 または NAC-3350）上で実行される、1 つ以上の Cisco NAC Profiler Collector によって構成されます。

エンドポイント プロファイリングと動作モニタリングについては、第 2 章「Cisco NAC Profiler アーキテクチャの概要」で説明しました。ここでは特に、Cisco NAC Profiler の柔軟性と、Cisco NAC アプライアンスの導入におけるニーズに対応したエンドポイント プロファイリングと動作モニタリング システムを策定するうえで取り入れられる戦略を中心に取り上げます。ここで説明したさまざまなデータ収集技術を選択して組み合せると、各環境においてシステムに提供されるエンドポイント データのソースを活用するシステムを構築できます。

準備のステップ

次のステップで、データの収集と、Cisco NAC Profiler をエンタープライズ ネットワークに実装する前に考慮するべき事項を示します。このリストは、すべてを網羅しているわけではありません。NetFlow などの外部データ ソースを使用したり、エンドポイントのアクティブ プロファイリングに NetInquiry モジュールを使用したりするオプションもあります。これらのトピックについては後述します。次のステップは、Cisco NAC Profiler システムの初期設定を支援するために行われます。Cisco NAC Profiler は、システムを調整し、オプション機能を活用することによって構築されます。

ステップ 5　「モニタリング インターフェイスの要件」（P.3-4）

ステップ 6　「SNMP トラップの設定」（P.3-4）

ステップ 7　「必須プロファイルの決定」（P.3-5）

Profiler Server の IP 設定の決定

Cisco NAC Profiler は、安全な HTTP 経由で管理されます。Cisco NAC Profiler Server は Profiler システム管理を管理し、システム コンポーネント（Server や Collector）は TCP/IP 経由で互いに、およびネットワーク デバイスやその他のコンポーネントと通信します。

Cisco NAC Profiler Collector は、Clean Access Server で使用されるアプライアンスと同じネットワーク インターフェイスを使用します。環境内で IP 接続をイネーブルにするには、Profiler Server のアプライアンスの管理インターフェイス（eth0）に対し、必須の TCP/IP アドレス、およびその他のパラメータを設定する必要があります。

Profiler Server アプライアンスの管理インターフェイスに対し、次の可動環境固有パラメータを決定します。

- IP ホスト アドレスとネットマスク
- システムによって使用される、デフォルト ゲートウェイの IP アドレス
- ネーム サーバの IP アドレス

Collector の初期設定を実行するには、Profiler Server の IP アドレスが必要です。これは、第 4 章「設置および初期設定」で説明するように、Collector の初回起動前に決定する必要があります。

加えて、Collector を実行する各 CAS アプライアンスの IP アドレスも決定したうえで、メモする必要があります。そうすると、第 6 章「Cisco NAC Profiler Server の設定」で説明するように、Profiler Server の設定が簡便化されます。

Collector とネットワーク デバイス（スイッチ、ルータなど）、および HTTPS 経由で Cisco NAC Profiler を管理するために使用されるコンピュータとの間のネットワーク通信に伴う、ACL やその他の潜在的な問題を考慮に入れる必要があります。ネットワーク上で Cisco NAC Profiler にコマンドライン アクセスを行うには SSH が使用されるので、管理コンピュータから Profiler Server および Collector への SSH アクセスをイネーブルにすることも考慮する必要があります。

内部ネットワーク アドレス ブロック

NAC Profiler の設定では、システムによってプロファイリングされる必要があるデバイスのホスト アドレス範囲を指定します。これらのアドレス ブロックは、通常、NAC Profiler がエンドポイント プロファイリングと動作モニタリングを提供する物理ネットワーク上のエンドポイントに IP アドレスを割り当てるために使用される、1 つ以上の IP サブネットまたはネットワークで構成されます。そうすると、システムは、組織によって管理されるアドレス空間外のソース アドレスを持つエンドポイントのプロファイル情報を保持せずに済みます。

NAC Profiler を導入するネットワークでプロファイリングされるすべてのエンドポイントのホスト アドレスを指定するアドレス ブロック（CIDR フォーマット：x.x.x/ マスク ビット）を収集します。

ネットワーク デバイス リスト

NAC Profiler はネットワーク インフラストラクチャをモデル化し、SNMP 経由でネットワーク インフラストラクチャ デバイス（スイッチおよびルータ）と通信し、ネットワーク トポロジに関する情報（ある場合）を収集します。この機能を利用するには、Cisco NAC Profiler にネットワーク デバイスの IP アドレスのリストを提供する必要があります。また、この通信をイネーブルにするには、SNMP read-only コミュニティ ストリングを提供する必要があります。エッジ デバイスで SNMP がイネーブルになっていなければ、SNMP をイネーブルにすることを推奨します。SNMP をイネーブルにすると、システムがネットワーク トポロジのモデルを維持するために、Cisco NAC Profiler によるポーリングを行えるようになります。

プロファイリングされるエンドポイントへの接続を提供するネットワーク デバイス（スイッチとルータ）のリストを作成する必要があります。このリストには、IP アドレス、デバイス名、および read-only コミュニティ ストリングが含まれている必要があり、可能であれば、データ入力タスクを簡便化するために CSV フォーマットのスプレッドシートを使用します。

第 8 章「Cisco NAC Profiler 設定へのネットワーク デバイスの追加」に、Cisco NAC Profiler 設定にネットワーク デバイスを追加する方法について説明します。

多くのネットワーク管理ソフトウェア ソリューションは、Cisco NAC Profiler で必要となる情報を含むデバイス リストを、CSV フォーマットでエクスポートする機能を提供しています。NAC Profiler は、CSV フォーマットのネットワーク デバイス情報をインポートする機能を備えています。

基本的には、読み取り専用デバイスとの読み取り専用接続により、次のようなフォーマットの CSV ファイルのネットワーク デバイス リストが作成されます。

```
DeviceName1,IP1,ReadOnlyCommString
DeviceName2,IP1,ReadOnlyCommString
...
```

NAC Profiler を使用し、第 2 章「Cisco NAC Profiler アーキテクチャの概要」で説明する NAC の導入および管理に伴うネットワーク管理タスクを簡便化するインフラストラクチャ デバイスをプロビジョニングする場合は、NAC Profiler がネットワーク デバイスへの SNMP セットを実行できるよう、read-write コミュニティ ストリングも提供する必要があります。

NAC Profiler をポート プロビジョニング モードで使用するには、次のようにフォーマットされた CSV ファイルのネットワーク デバイス リストを作成します。

```
DeviceName1,IP1,ReadOnlyCommString,ReadWriteCommString
DeviceName2,IP1,ReadOnlyCommString,ReadWriteCommString
...
```

DHCP トラフィック分析

Cisco NAC Profiler はエンドポイントからの DHCP 要求を、エンドポイント プロファイリング のデータのソースとして使用できます。プロファイリングされる一部のホスト、またはすべてのホストが、DHCP を使用してアドレス指定を行う場合は、エンドポイントからの DHCP 要求を、Cisco NAC Profiler で見えるようにするかどうかを考慮する必要があります。Cisco NAC Profiler が DHCP 要求を直接収集できない場合は（DHCP を使用するホストと同じ LAN 上にない場合など）、LAN とネットワークの残りの部分を接続するために使用されるルータ インターフェイスからのブロードキャスト DHCP 要求パケットをリダイレクトするための IP ヘルパー アドレスを使用するか、単純に SPAN または RSPAN を使用し、DHCP サーバが接続されているイーサネット ポートからトラフィックを送信します。

リダイレクトを行う場合は、IP ヘルパー アドレスをルータの設定ファイルに追加し、DHCP 情報を処理する Collector（具体的には、Collector 上の NetWatch モジュール）のアプライアンス インターフェイスの IP アドレスを指定します。この設定では、ルータは、エンドポイント プロファイリングと動作モニタリングの分析を行えるように、DHCP サーバだけではなく、Cisco NAC Profiler にも DHCP ブロードキャストを転送します。

NAC Profiler は、DHCP 要求をどのように受信するかにかかわらず、DHCP プロセスには**関与しません**。要求パケットをパッシブに収集し、エンドポイント プロファイリングや動作モニタリング用としてデータを使用するだけなので、ネットワークの DHCP サービスには影響はありません。

モニタリング インターフェイスの要件

Collector は、NAC-3310 および NAC-3350 Clean Access Server（CAS）アプライアンス上の 3 倍速ネットワーク インターフェイスの一部を使用し、エンドポイント プロファイリングと動作モニタリングにおいて有益なパケットを収集し、分析できます。これらのパッシブ アナライザ インターフェイスは、Collector を実行する NetWatch モジュールによって分析されるネットワーク トラフィックを収集するために使用されます。いずれの CAS モデルでも、eth3 インターフェイスを使用し、SPAN または RSPAN 経由でリダイレクトされたトラフィックを受信できます。

Cisco NAC Profiler のエンドポイント プロファイリング情報の最も有益な情報源の 1 つとして、DHCP が挙げられます。環境で DHCP が使用されている場合は、DHCP サーバ（複数可）に対してサービスを提供するリンク上にモニタリング インターフェイスを配置すると、Cisco NAC Profiler に非常に有益なデータが提供されます。あるいは、「DHCP トラフィック分析」（P.3-3）で説明するように、LAN セグメントにサービスを提供するルータに対し、IP ヘルパー アドレスを設定する方法もあります。

ネットワーク エッジからサーバ ファームを通過するエンドポイント トラフィックの、リダイレクト トラフィックを（SPAN、RSPAN を使用して）eth3 インターフェイスで受信することと、インターネット リンクを使用することを検討する必要があります。エンドポイント プロファイリングと動作モニタリングに有益なトラフィックの生成が可能になります。

追加情報については、第 7 章「Collector モジュールの設定」を参照してください。

SNMP トラップの設定

Cisco NAC Profiler は、エッジ デバイスからのトラップを使用し、エンドポイント プロファイリングと動作モニタリング機能を実行できます。エンドポイント接続を提供するネットワーク デバイスを、リンク ステート変更の SNMP トラップと MAC-address-change 通知トラップ（後者は、一部ベンダーのスイッチでだけ使用可能）を Collector に送信するよう設定することを推奨します。あるデバイスのトラップ レシーバとして指定されている Collector は、そのデバイスの定期ポーリングを行う NetMap モジュールを実行する Collector と同じである必要があります。

エンドポイント接続を提供するインフラストラクチャ デバイスは、デバイスのポーリング設定において指定されている NetMap モジュールを実行する Collector の管理インターフェイスの IP アドレスに、リンク ステート トラップと新規 MAC トラップを送信するよう設定されていなければなりません。SNMP トラップの設定の詳細手順については、デバイス製造元の資料を参照してください。

次に、Cisco IOS ベースのスイッチの SNMP トラップ設定を示します。

目的のトラップを Cisco NAC Profiler に送信するために、アクセス スイッチを設定する方法を説明します。ここに示す設定コマンドは、最新リリースのファームウェアを実装した、大半の Cisco IOS ベースのスイッチで使用できます。中には、すべてのトラップ タイプをサポートしていないスイッチもあります（具体的に言うと、本ガイドの執筆時点では、Cisco Catalyst 6500 シリーズのスイッチでは、MAC-address-change 通知トラップがサポートされていません）。Cisco 以外のスイッチについては、各デバイスの資料を確認してください。

次の IOS コマンドを実行すると、目的の SNMP トラップを Cisco NAC Profiler に送信できます。

```
(config)# snmp-server enable traps mac-notification
(config)# snmp-server enable traps snmp linkup linkdown
(config)# snmp-server host <NAC Profiler-IP-address> traps version 1 <community-string>
mac-notification snmp
```

そうすると、すべてのインターフェイスの link-status トラップが有効になり、*場合によっては* MAC-address-change 通知トラップを送信できるよう、スイッチが設定されます。
MAC-address-change 通知が実際に行われるようにするには、対象となる各インターフェイスで次のコマンドを使用する必要があります。

```
(config)# interface GigabitEthernet 2/29
(config-iface)#  snmp trap mac-notification change added
```

MAC-address-change 通知は、エンドポイントが接続されるアクセス スイッチ ポートでイネーブルにする必要があります。　特に興味深いのは、ワイヤレス コントローラ（Cisco WLC など）に接続されるポートです。MAC-address-change 通知は、スイッチ間リンク（トランクなど）では絶対にイネーブルに***してはなりません***。

ネットワーク デバイスは、Cisco NAC Profiler が リンク ステート および MAC-address-change 通知トラップだけを受信するよう設定する必要があります。すべてのネットワーク デバイス トラップを NAC Profiler に転送すると、システムに追加情報が提供されず、システムの性能に悪影響を与える可能性があるので、望ましくありません。

必須プロファイルの決定

プロファイルとは、デバイスを検出して特定し、デバイスタイプやクラスに分類するために使用される論理コンテナであり、類似した動作特性、機能、および制限を持ちます。

NAC が配置されるネットワークでは、すべてのエンドポイントの検出、特定、および分類が主な働きであり、中でも Cisco NAC アプライアンスと相互作用することができないエンドポイントに特に注意を払います。この大半は、NAC エージェントを使用できない、または Web ブラウザ経由で NAC システムとユーザの相互作用が許可されていない Windows 以外の PC やその他のデバイスです。プリンタ、管理可能な無停電電源装置、ゲーム コンソール、およびその他の専用デバイスには、代替的なネットワーク プロビジョニングによるネットワーク アクセスを提供する必要があります。これらのデバイスを識別して特定し、動的なプロビジョニングをイネーブルにするには、環境内の各デバイス タイプに対してプロファイルを作成する必要があります。そうすると、それらのデバイスを識別、特定、および追跡し、NAC 実装の完全性を拡張し、維持しながらネットワーク アクセスを提供できます。

NAC Profiler には、現時点までの導入実績に基づき、いくつかのエンドポイント プロファイルがあらかじめ設定されて提供されます。システムにあらかじめ設定されている既存プロファイルのいくつかを、環境に適用できます。事前設定済みプロファイルには、次のようなものがあります。

- APC UPS
- Cisco WLAN Access Point
- HP Jet Direct Printer
- IP Phone
- Windows User
- Linux OS

製品の導入準備の一環として、ネットワークに接続されているエンドポイント デバイスの種類、コンテクスチュアル インベントリの必要性、および認証の計画や NAC の導入計画について話し合い、必須プロファイルの暫定リストを作成したうえでまとめる必要があります。

Cisco NAC Profiler システムの設定ワークフロー

Cisco NAC Profiler のシステム設定は、複数の手順を踏むことで行われます。システムへの実装を開始する前に、システムレベルの計画を作成することを推奨します。最も重要なのは、Cisco NAC Profiler コンポーネントを理解することです。どのようにアドレス指定を行うか、ネットワークのどの位置に配置するか、ネットワーク デバイスのポーリングを、CAS および Collector を実行するシステムの NetMap モジュールにどのように分散するかを把握する必要があります。

システムを構成する Profiler Server と Collector を起動する前に、この点を十分に定めておく必要があります。起動手順では、システムのセットアップ時にこれらのパラメータを入力し、第 4 章「設置および初期設定」で説明するように、初期化を実行する担当者がすぐに使える状態にする必要があります。

Cisco NAC Profiler システムの管理は、Profiler Server を通じて提供され、標準的な Web ブラウザおよび HTTPS 経由でアクセスされます。

表 3-1 に、Cisco NAC Profiler の設定ワークフローを示します。このガイドの残りの章では、表 3-1 で説明した設定タスクを完了するための手順について解説します。ワークフローは、システムに配置される Clean Access Server 上で実行される Profiler Server および Collector のアプライアンス起動が完了したところから始まります。アプライアンスの起動手順は、キーボードとモニタ、または端末セッションを使用して、各アプライアンスで行われます。Profiler Server アプライアンスと CAS および Collector の初期起動の詳細手順については、第 4 章「設置および初期設定」を参照してください。Server と Collector（複数可）の初期設定が完了したら、それ以降のシステム設定は Web インターフェイス経由で行われます。

表 3-1　　タスクのフローチャート

タスク	説明
1. アプライアンスの起動	第 4 章「設置および初期設定」の手順に従い、Profiler Server および Collector のアプライアンス起動手順を行います。これらのステップを実行するとすべてのコンポーネントが初期化され、アドレスが指定されるとともに、すべてのコンポーネントのネットワーク通信がイネーブルにされます。Profiler Server との Web セッションを確立し、システム設定を完了します。
2. ネットワーク設定	第 5 章「ターゲット環境用の Cisco NAC Profiler の設定」に、ターゲット環境への Cisco NAC Profiler の設定と、システム設定の変更を保存する方法を説明します。
3. Profiler Server の設定	第 6 章「Cisco NAC Profiler Server の設定」に、Profiler Server コンポーネントの設定手順を説明します。Collector を追加する前に、Profiler Server の設定を完了させます。
4. Collector の追加	第 7 章「Collector モジュールの設定」に、システムに各 Collector を追加する手順と、システムに必須の、各 Collector で実行されるソフトウェア モジュール（Forwarder、NetMap、NetWatch、NetInquiry、および NetTrap）の設定の手順について説明します。
5. ネットワーク デバイスの設定	第 8 章「Cisco NAC Profiler 設定へのネットワーク デバイスの追加」に、システム設定にネットワーク デバイスを追加する手順を説明します。ネットワーク デバイスのポーリングは、システムの Collector 上で実行される NetMap モジュール間で分散されます。ネットワーク デバイスと、SNMP の必須情報がシステム設定に追加、またはインポートされ、NetMap モジュールは各デバイスをポーリングするよう指定されます。

表 3-1　タスクのフローチャート

タスク	説明
6. エンドポイント プロファイルの設定	第 9 章「エンドポイント プロファイルの設定」に、NAC Profiler に含まれるエンドポイント プロファイルをイネーブルにするための手順と、エンドポイント プロファイルを新規作成する手順を説明します。パッシブおよびアクティブ エンドポイント プロファイリングにおけるプロファイルで使用されるルール タイプについて説明します。
7. エンドポイント イベントの設定	第 10 章「Cisco NAC Profiler Events の設定」に、Profiler Server と Cisco NAC アプライアンス CAM の統合をイネーブルにし、非 NAC エンドポイントの自動実装と管理を行う手順を説明します。
8. Cisco NAC アプライアンスの統合の設定	第 11 章「Cisco NAC アプライアンスとの統合」に、エンドポイント イベントのイネーブル化、Cisco NAC Profiler システムとエンタープライズ ネットワークやセキュリティ管理との通信の確立の手順を説明します。
9. ユーザ アカウントの設定	第 12 章「Cisco NAC Profiler ユーザ アカウントの管理」に、NAC プロファイル ユーザ アカウントを追加、編集、および削除する手順を説明します。

この段階で Profiler Server および Collector の初期化が済んでいなければ、この章で説明する必須情報を収集し、第 4 章「設置および初期設定」に従って Server と各 Collector の初期化を行います。

初期化手順と、Profiler Server の Web 管理の確立が終了したら、第 5 章「ターゲット環境用の Cisco NAC Profiler の設定」に戻り、Cisco NAC Profiler システム設定を行います。