CHAPTER 1

Cisco NAC Profiler の概要

この章は、次の内容で構成されています。

概要

Cisco NAC Profiler を利用すれば、ネットワーク管理者は、適切なネットワーク アクセスを確保し維持するために、デバイス タイプに関わりなく、接続されたすべてのネットワーク エンドポイントの機能を、特定、検索、および決定することによって、さまざまなスケールおよび複雑度のエンタープライズ ネットワーク内の Network Admission Control（NAC; ネットワーク アドミッション コントロール）を効率的に配置および管理できます。Cisco NAC Profiler は、ネットワークに接続されたすべてのエンドポイントを発見、カタログ化、およびプロファイリングする、エージェントレス システムです。

NAC Profiler は、NAC と 802.1X の導入をサポートすることに加え、NAC やポートベース認証の導入とは無関係に、エンドポイントのライフサイクル マネジメントでも重要な役割を果たします。多くの企業が、組織内のエンドポイントをそのライフサイクルにわたって管理することが、ネットワークの信頼性および可用性の継続的な向上の実現に向けての次の論理的ステップであることに気づいています。ここで言う「エンドポイント」とは、デスクトップやラップトップ コンピュータなどのユーザ デバイスを含む、ネットワークに接続するすべてのデバイスだけでなく、ますます多様化する、ネットワーク サービスを使用するその他の IP 対応デバイスも含みます。先ほど使用した「エンドポイント ライフサイクル」という用語は、タイプや機能を問わず、すべてのネットワーク接続デバイスのあらゆる面における耐用年数を意味します。新しいエンドポイントが初めてインフラストラクチャに接続された時点から開始され、そのエンドポイントが使用されなくなると終了です。

ネットワークが大規模化するにつれて、どのタイプのエンドポイントが各エッジ ポイントに接続されているのかを確実に把握することが次第に難しくなっていきます。これにより、NAC エッジ セキュリティ ソリューションの導入後における、エンタープライズ ネットワークの導入や現在行われている管理が困難になる可能性があります。個々の機能を問わず、許可されたエンドポイントすべてに対する、継続的で、信頼性が高く、セキュアなアクセスを実現するには、ネットワークのエッジにおける各エンドポイントが、導入済みの認証または NAC ソリューションと通信可能かどうかを把握することが非常に重要です。管理上の負担が最小限に抑えられ、また、本質的に動的であるような方法でそのような機能を提供することは、特に大規模なエンタープライズ ネットワークにおいて、エッジ セキュリティ ソリューションの導入および運用を成功させるための前提条件です。

一般的に言って、プリンタ、ファックス装置、IP 電話、無停電電源装置といったデバイスは、NAC クライアントを実行できません。つまり、NAC ソリューションの導入において、これらのような特殊な目的のデバイスには、利用可能なエージェントはなく、ユーザがブラウザを介して手動で介入できるような手段もありません。この場合、それらのエンドポイントを接続するポートを設定して、NAC システムを回避するか（たとえば特別な VLAN に置くとか）、あるいは、アドミッション コントロール プロトコルに直接参加せずにそれらのデバイスにアクセスさせるために、一意のハードウェア アドレスを介してそれらのデバイスを認識するように NAC システムを設定する必要があります。一般的に言えば、これには、MAC アドレスによって、NAC システムがそれらのエンドポイントを認識できるようにする必要があります。その結果、それらのエンドポイントを、クレデンシャルだけに基づいて許可することが可能になり、それ以上の NAC システムとの通信が不要になります。Cisco NAC アプライアンスの場合、これらのような非 NAC デバイスに対しては、Clean Access Manager の Device Filter リストによって対応します。

Cisco NAC Profiler には、エンドポイント プロファイリングおよび動作モニタリング機能が用意されており、管理者は、ネットワークに接続されたデバイスのタイプ、その位置、および、それらのデバイスが現在常駐しているポートの状態に応じた能力を十分に把握できます。エンドポイント プロファイリングおよび動作モニタリングは、ユーザ数が数百人から数万人規模までのエンタープライズ ネットワークに導入可能です。次の概要では、これらの Cisco NAC Profiler の中心機能のバックグラウンドについて解説します。

エンドポイント プロファイリングの概要

エンドポイント プロファイリングは、観察可能な動作を記録し、その特定可能な特性を、特定のグループ（プロファイル）に分類するために分析し、指定された認証や NAC ソリューションなどの特定の領域に参加する能力を評価します。エンドポイント プロファイリングとは、本質的に、機能、能力、またはその他の固有の特性において同一のエンドポイントを特定し、グループ化することを目的とした、エンドポイントに対する動作ベースの特性解析です。

NAC Profiler は、ネットワーク上で検出および位置を特定した各エンドポイントを、エンドポイント プロファイリング エンジンのパッシブおよびアクティブなプロファイリング メカニズムに従って、1 つのプロファイルに分類またはプロファイリングします。各プロファイルは、動作ベースの特性が同じであり（プリンタ、IP 電話、ゲーム機など）、ネットワーク内の各エンドポイントに与えられた認証、NAC、またはその他要件に準拠するための機能が同じである 1 つ以上のエンドポイントを格納する論理的なコンテナまたはグループです。

エンタープライズ ネットワークに接続された各エンドポイントは、そのネットワークにアクセスするために認証またはアドミッション コントロール システムと通信できるものもあればできないものもあります。Windows コンピュータや Linux コンピュータのようなエンドポイントは、一般的に、認証および NAC システムのすべての要件を満たすことができますが、プリンタ、セキュリティ バッジ リーダー、管理可能な無停電電源装置（UPS）といったデバイスは、満たすことができません。

認証またはアドミッション コントロールへのエンドポイントの参加には、一般的に言って、ネットワークに対する接続について問題なく認証または許可を受けるために、自動的に（たとえば、エンドポイント上で実行され、また、正しいクレデンシャルで適切に設定されたサプリカントまたはエージェント経由で）、または手動によるユーザの介入によって（たとえば、ブラウザを介してユーザ クレデンシャルを手動で入力するなどして）クレデンシャルを送信する必要があります。この機能を持たないエンドポイントについては、それらが認証またはアドミッション コントロールの直接的な対象にならないように識別する必要があります。

さらに、エンタープライズ ネットワークには、Windows を実行しているが、政府によって規制されているのでソフトウェア イメージが変更できない（生物医学装置など）、あるいは、ユーザ中心の装置ではない（ロボット用、研究開発用など）という理由で、認証または NAC プロセスに参加できないシステムもあります。それらのエンドポイントは、自動、あるいはユーザによる介入のいずれによっても認証要求に対して応答できないので、代替のネットワーク プロビジョニングを実行し、これらのエンド

ポイントが、認証または NAC に基づいてポートを実装した後のネットワークに対して、セキュアで信頼性の高いアクセスを実行できるようにする必要があります。これらのエンドポイントは実際には許可を受けたエンドポイントですが、その固有の制限によって、認証または NAC システムとの通信によって認証されたり許可されたりできなくなっています。このような企業の環境には、NAC が可能なデバイスと NAC が不可能なデバイスとが同じくらいの数だけ存在している可能性があります。Cisco NAC Profiler は、このようなネットワークに対処できるように設計されています。

Cisco NAC Profiler は、動的なエンドポイント プロファイリングを実行します。エンドポイント プロファイリングは、ネットワーク上の各エンドポイントを特定および検索し、それらのエンドポイントを、その機能や制限に基づいてグループ化してから、手動による再プロビジョニングを可能にするためにネットワーク インフラストラクチャと直接通信するか、あるいは、非認証または非 NAC 対応エンドポイントのディレクトリとして動作するかのどちらかのメカニズムを選択することによって、非認証または非 NAC エンドポイントに対する対応を可能にします。

NAC Profiler ディレクトリによって、認証や NAC システムは、特定のエンドポイントに関して正しい決定を下すことができます。認証サーバまたは NAC システムは、API または LDAP のようなプロトコルを介して NAC Profiler ディレクトリにアクセスし、ネットワークにアクセスしようとしているエンドポイントに関するリアルタイムのプロファイリング情報を取得します。

Cisco NAC Profiler のエンドポイント プロファイリングは本質的に動的であり、ネットワークの追加、移動、および変更の結果生じたネットワーク エッジにおける変更を検知できます。新しく導入された MAC またはプロファイル変更イベント（第 10 章「Cisco NAC Profiler Events の設定」を参照）を使用して、ネットワークやセキュリティの運用に警告を発したり、認証またはアドミッション コントロールの対象となるネットワークにおける移動、追加、変更に対して有効に対応するために必要な再プロビジョニングをイネーブルにしたりできます。

Cisco NAC Profiler のエンドポイント プロファイリングによって、ネットワーク管理者は、ネットワークの状態を、エンドポイントおよびネットワーク ポート レベルに至るまで見ることができます。Cisco NAC Profiler のレポート機能を利用すれば、ネットワーク内の各スイッチ ポート、それらスイッチ ポートに接続された各エンドポイント、現在割り当てられているプロファイルに関するリアルタイムの運用状態を知ることができます。Cisco NAC Profiler は、各エンドポイントに関する履歴を保持するので、位置、論理的なアドレッシング、およびプロファイルに関する情報を、セキュリティ イベント管理フォレンジックなどの目的のために、簡単に取得できます。

エンドポイント動作モニタリング

非認証または非 NAC エンドポイントに対しては、長期間に渡って監視を行い、それらの動作が、既知のデバイス タイプの動作と矛盾していないかどうかを確認する必要があります。各プロファイルはデバイス タイプの分類であり、これにより、認証クレデンシャルを必要とすることなく、適切なレベルのネットワークが可能となります。一般的に言って、認証、または、ネットワーク アドミッション コントロールへの参加ができないエンドポイントは、ネットワーク上で専用のサービスを提供する特別な目的のデバイス（プリンタ、IP 電話、ワイヤレス アクセス ポイント、UPS、HVAC デバイスなど）です。特別な目的のエンドポイントが、汎用目的のコンピューティング デバイス（デスクトップ コンピュータやラップトップ コンピュータなど）の動作を示すと、動作モニタリング機能がこれを検出します。たとえば、動作モニタリングは MAC スプーフィングを検出できます。MAC スプーフィングとは、認証されていないネットワーク アクセスを行うために使用される基本的な手法の 1 つです。

Cisco NAC Profiler の動作モニタリングは、ネットワークを利用しているすべてのエンドポイントに関する動作情報を、継続的に収集および分析します。あるエンドポイントの動作特性が変更されると、NAC Profiler エンジンは、その動作の変更に伴って、当該エンドポイントのプロファイルも変更するべきかどうかを評価します。プロファイルを変更するべきだと判断した場合、NAC Profiler は、そのエンドポイント プロファイルを変更し、ネットワークおよびセキュリティ管理に警告を発します。さ

らに、NAC Profiler は、疑いのあるデバイスへのアクセスを拒否するために、認証または NAC システムによって許可されたネットワーク アクセスを自動的に変更できます。このようにして、Cisco NAC Profiler は、エッジ セキュリティ システムを妨害する試みを自動的に無効にします。

エンドポイント プロファイリングが非認証および非 NAC ノードに対応するために、例外リストまたはホワイト リストの自動登録を行うのに対し、動作モニタリングは、追加のセキュリティ メカニズムに加え、ネットワーク認証システムおよびアドミッション コントロール システムのこれらの重要な要素に対する自動化された継続的な管理を提供します。NAC Profiler の動作モニタリング機能は、既知の、そして許可された非認証または非 NAC エンドポイントに対して、2 番目のクレデンシャルを追加します。これは動作シグニチャのクレデンシャルであり、それらのデバイスの MAC アドレスが、ネットワーク認証やアドミッション コントロールを迂回する手段として悪用できないようにするためのものです。

エンドポイント プロファイリングと動作モニタリングのストラテジ

Cisco NAC Profiler は、タイプおよび位置（スイッチとポート）を含む、ネットワークに接続されたすべてのデバイスの状況をすべて反映したインベントリを作成および維持するために、数多くのメカニズムを使用しています。

Cisco NAC Profiler は、「インライン」モードでは動作しません。そのため、ネットワーク上のすべてのブロードキャストまたはレイヤ 2 ドメインにおけるネットワーク トラフィックの可視性を必要としません。Cisco NAC Profiler は、VLAN を介したレイヤ 2、およびレイヤ 3 の両方で分割されたネットワーク内でも効率的に動作させることができます。

Cisco NAC Profiler Collector モジュールは、エンドポイントと中央サービス（アプリケーション サーバとプリント サーバ、インターネット リンクなど）間のトラフィックがアクセス可能であり、Cisco NAC アプライアンスの Clean Access Server（CAS）上のモニタリング インターフェイスにリダイレクト可能なネットワーク内の集約ポイントに配置されます。そのため、Collector モジュールは CAS 上に配置されます。第 2 章「Cisco NAC Profiler アーキテクチャの概要」で解説したとおり、配布された各 Collector は、エンドポイント情報を中央の Cisco NAC Profiler Server に集約します。

Cisco NAC Profiler は、エンドポイント上にロードされたいかなるソフトウェア エージェントにも依存しません。また、エンドポイント プロファイリングまたは動作モニタリングを実行するうえで、エンドポイントに対する管理者レベルのアクセスも必要としません。ただし、Cisco NAC Profiler は、ネットワーク上におけるエンドポイント動作の直接観察可能な属性には、場合によっては、その機能を実行するためにネットワーク インフラストラクチャ デバイス（エッジ スイッチ、ルータ、NetFlow 収集装置など）から収集された情報と組み合せた形で依存します。多くの環境では、Cisco NAC Profiler は、主にパッシブ モードで動作していますが、同時に各種アクティブ コンポーネントも用意されており、パッシブにプロファイリングすることが困難なある種のエンドポイントをプロファイリングするために、非侵襲的な方法でネットワーク サービス（DNS など）からの標準的な情報を活用できます。

他の IT アセット インベントリ ディスカバリ システムとは異なり、Cisco NAC Profiler は、その機能を継続的に実行し、環境内のエンドポイントに関する情報のリアルタイム データベースおよび履歴データベースを維持します。ネットワークを定期的にスキャンして、接続されているものを判断し、ポート スキャンなどの手法に基づいてエンドポイント タイプを明らかにするような、「スナップショット」ベースでは動作しません。Cisco NAC Profiler は、各エンドポイントの動作を継続的に監視し、どのプロファイルがそのエンドポイントに最も適合するのかを評価するために Collector モジュールが提供するデータに基づいて、そのデータベースを更新します。履歴はエンドポイントごとに保持され、あるエンドポイントの情報が記録されているプロファイル（複数可）、そのエンドポイントが使用しているアドレス、およびそのエンドポイントがネットワークに接続されている場所についてのサマリー ビューを提供します。

多くの場合、Cisco NAC Profiler システム、特にそのパッシブ トラフィック分析コンポーネントは、集約されたネットワーク トラフィックを処理するために、高く持続的なスループットを実現できなければならないと見なされています。Cisco NAC Profiler は決してインライン モードでは導入されず、ボトルネックになることはありえません。ネットワークに対する攻撃の可能性を検出するため、基本的に、送信されてきたすべてのパケットを検査しなければならない IDS や IPS とは異なり、Cisco NAC Profiler 検査しなければならないのは、エンドポイント プロファイリングと動作モニタリングにとって有用なパケットだけです。そのため、Cisco NAC Profiler には、それほど高いスループット能力は必要ではありません。また、フォレンジック動作をサポートするのにすべてのパケット情報を保存する必要がないので、データ ストレージの要件は比較的低いものとなっています。

Cisco NAC Profiler は、ほとんどどんな環境でもエンドポイント プロファイリングと動作モニタリングを提供できるほど柔軟性が高く、たとえそれらの機能が有用でないような環境でさえ提供可能です。複数のエンドポイント データ元を利用する場合は、考慮事項と代償が伴います。ネットワーク環境によって異なりますが、エンドポイント プロファイリングの細やかさと、動作モニタリングを提供する機能のレベルは、そのシステムに与えられた可視性とアクセスに比例します。

Collector は、レイヤ 2 からの、OSI スタックのさまざまなレベルで動作します。Cisco NAC Profiler は、ネットワーク上で発見された個々のエンドポイントを、その物理的なネットワーク インターフェイス アドレス（MAC アドレスなど）、およびそのインターフェイスの登録済み製造元を基に、追跡記録します。

Cisco NAC Profiler は、基本的に、ネットワーク インフラストラクチャ デバイスとの SNMP 通信を利用して、ネットワーク上のすべてのエンドポイントを発見します。NAC Profiler は、ネットワーク内のスイッチとルータに対して SNMP 経由でポーリングを実行し、どのエンドポイントがどのポートに接続され、どの論理（IP）アドレスを各デバイスが使用中なのかを判断します。NAC Profiler エンジンは、ネットワーク トポロジをエンド ノード レベルまで解析し、ネットワークのモデルやマップを作成します。

Cisco NAC Profiler は、エンタープライズ ネットワーク管理用に採用されたものと同じプロトコルを使用して通信を行い、Read Only モードを使用して、設定可能な間隔でネットワーク デバイスからトポロジ情報を収集します。NAC Profiler は、これらのデバイス上に保持される管理情報ベースの小さなサブセットだけが必要なので、NAC Profiler による定期的なポーリングは帯域幅を集中的に使用することがなく、デバイスに対する悪影響はありません。SNMP ポーリングが利用可能な場合、NAC Profiler は、環境内に存在するすべてのエンドポイントを迅速に、そして正確に確認できます。SNMP が利用できない場合、NAC Profiler は、他の手段に依存して環境内のデバイス一覧を作成します。

Cisco NAC Profiler は、エッジ インフラストラクチャからの SNMP トラップを利用できる場合、それを活用して、ほぼリアルタイムでエンドポイント トポロジの変更を検出します。NAC Profiler は、影響を受けるデバイスに即座にポーリングを実行してネットワーク トポロジを再マッピングするために、Link State トラップを使用して、エンドポイントがいつネットワークに加入し、いつネットワークから去ったかを判断します。SNMP が利用できない場合、NAC Profiler は、一連のタイマーを使用して、ネットワークの変更情報を取得します。この結果、リアルタイムでネットワークの変更に対して応答するシステムの機能に遅延が生じる可能性がありますが、実際には、タイマーが、エンドポイントの移動を追跡必要な機能を提供します。

また、Cisco NAC Profiler は、プロファイリングの基準として、エンドポイントの論理（IP）アドレス指定を追跡および活用することもできます。NAC Profiler は、各エンドポイントの物理アドレスから論理アドレスへのアドレス バインディングを継続的に追跡するので、特定のアドレスを使用しているエンドポイントとデバイス タイプを対応付けるルールを作成できます。これにより、ネットワーク インフラストラクチャや、ホスト アドレスの予約されたプールからアドレス指定されたとわかっている他のデバイスのような、スタティックにアドレス指定されたデバイスをプロファイリングするための、直接的なアプローチが可能になります。

Collector モジュールに対してリダイレクトされたネットワーク トラフィックが入力されると、Cisco NAC Profiler は、ネットワーク層およびその上位層でのエンドポイントの動作の観察可能な属性に基づいて、プロファイリングを実行できます。リダイレクトされたネットワーク トラフィックは、通常、エンドポイントと、共有サービスとして機能しているセグメント（データ サーバとアプリケーション

サーバ、インターネット リンクなど）との間で収集されたトラフィックです。Cisco NAC Profiler には、NetWatch モジュールを実行している Clean Access Server 上のモニタリング インターフェイスに対してネットワーク トラフィックを配信するために、トラフィック リダイレクション（ミラー ポート、SPAN、RSPAN など）を介して、これらのセグメントからのネットワーク トラフィックに対するアクセスが提供されます。

Collector に存在するこれらのディスカバリ メカニズムに加え、Profiler Server は、ネットワークにすでに配置された NetFlow 収集装置からの NetFlow エクスポート データを処理できます。ネットワーク トラフィックを直接、またはトラフィック フロー データを検査することによって、Cisco NAC Profiler は、すでに解説した IP アドレス ルール、およびレイヤ 4 以上で動作するその他のルール タイプのような、Profiling 上の決定を行うために使用可能な、エンドポイント トラフィック パターンおよびその他の特性を決定できます。エンドポイント プロファイリングに対して、エンドポイント トラフィックやフロー データを使用する例を次に示します。

- NAC Profiler は、特定のリソースを使用するサービス（TCP や UDP ポートなど）と通信するエンドポイントを特定できます。たとえば、TCP ポート 9100 上にあるプリント サーバと通信するネットワーク プリンタを監視できます。
- NAC Profiler は、特定可能なソフトウェア エージェントを実行しているエンドポイントの監視に基づいて、特定のデバイスを明確に特定できます。たとえば、Windows デバイスを、その端末が、ある Web サイトにアクセスする際にブラウザを開く時のブラウザ エージェントの存在によって、特定できます。
- NAC Profiler は、サーバ バナーを監視することによって、さまざまなサーバ タイプを特定できます。

NAC Profiler は、DNS や DHCP などのネットワーク サービスから情報を収集することもできます。DHCP の場合、NAC Profiler は、そのプロトコルを利用しているエンドポイントからの DHCP 要求を処理できます。DHCP 要求を、クライアント名、および、プロファイリングで使用するクラアント ベンダー情報に関して検査できます。エンドポイント接続を提供しているセグメントからの DHCP 要求を、次の 2 つの方法で Collector に配信できます。

- NAC Profiler アプライアンス上のモニタリング インターフェイスは、そのインターフェイスにリダイレクトされた DHCP サーバ（複数可）をサポートする LAN セグメントからのトラフィックを受信できます。このモードでは、エンドポイントからのすべての DHCP 要求が、モニタ インターフェイスによって受信され、クライアント名またはクライアント ベンダー情報に関して検査されます。
- また、LAN に接続されたルータのインターフェイス上における DHCP リダイレクション（IP ヘルパー アドレッシングと呼ばれることもあります）を利用して、そのルータ インターフェイスが接続された LAN（複数可）からのすべての DHCP 要求のカーボン コピーを、NAC Profiler インターフェイス上の管理インターフェイスに直接転送することもできます。NAC Profiler は、直接 DHCP プロトコルには関わりません。単に、DHCP 要求の、上記のようなリダイレクトされたユニキャスト コピーを利用して、プロファイリング データを収集するだけです。IP ヘルパー手法を使用する場合、Cisco NAC Profiler は、エンドポイントからの要求に対する可視性を持つことに注意してください。Cisco NAC Profiler システムは DHCP 要求に対しては無効なので、エンドポイントの現在の IP アドレスを判断するためには、他の手法に頼る必要があります。

パッシブな手法では、すべてのエンドポイントをプロファイリングするには不十分であるような環境の場合、Cisco NAC Profiler では、さまざまな、アクティブなプロファイリング手法を利用できます。アクティブなプロファイリング機能は、特定の環境、特に、中央サービスと定期的に通信を行わないスタティックにアドレス指定されたエンドポイントが存在している場合に、使用可能なオプションです。Cisco NAC Profiler のアクティブなプロファイリング機能は、エンドポイントのディスカバリ用に再利用される他のツールとはまったく異なります。たとえば、Cisco NAC Profiler は、指定されたエンドポイントがどのポートをオープンするのか判断するために集中的なトラフィックにエンドポイントをさらすアクティブ スキャナは利用しません。その代わり、Cisco NAC Profiler では、管理者が、プロファイリング データをアクティブに収集することを目的に、選択したエンドポイント自体や、DNS のようなネットワーク サービスの選択プローブを複数設定できます。たとえば、アクティブなプロファイリ

ング機能を使用して、NAC Profiler アプライアンスそれ自体に、ターゲット セグメント上のエンドポイントとの TCP ポートにおける通信を開始させることができます。NAC Profiler は、指定された一連の端末との、任意の TCP ポート上でのセッションを確立しようとします。その試行の成功または失敗は、本文書内ですでに解説したように、次に利用可能なトラフィックを発生させるため、NAC Profiler アプライアンス インターフェイス上でキャプチャされます。指定されたエンドポイントとの TCP セッションをアクティブに確立しようとすることに加えて、アクティブなプロファイリングは、選択されたエンドポイントのホスト名を取得するために DNS に問い合せを行ったり、Web および SMTP サーババナーを要求したりするために使用することも可能です。次に、これらのパラメータを使用するルールは、アクティブに生成されるトラフィックと、NAC Profiler エンジンが利用するパッシブに収集されるトラフィックに対して利用し、一致を検出して、エンドポイントを正しい Profile に割り当てることができます。

要約

NAC Profiler によって、現代のエンタープライズ ネットワークに対し、ネットワーク エンドポイントのディスカバリに関わるユニークな機能である、プロファイリングおよび動作モニタリングを導入できます。Cisco NAC Profiler は、独立して動作して、Endpoint Lifecycle Monitoring ソリューションを提供でき、本マニュアルで後に解説するとおり、収集されたエンドポイント データは、他のシステムでも活用できます。