

ネットワーク アドミッション コントロール

NAC の概要

Q. NAC ソリューションとは何ですか。

A. Network Admission Control (NAC; ネットワーク アドミッション コントロール) は、シスコシステムズが主導するマルチパートナー プログラムであり、ネットワークに接続する端末のセキュリティ レベルを既存のネットワーク機器で確保するという、シスコ主導の業界アライアンスをベースとしたセキュリティ ソリューションです。NAC では、OS レベルやパッチ状況、アンチウイルス ソフトをはじめとするクライアント セキュリティ ソフトの情報、資産管理的な要素など、NAC に対応したアプリケーションの状態を監視および精査することを可能にします。また、セキュリティ ポリシーに準拠した端末へのネットワーク アクセスの確保、基準値を満たさない端末の隔離と免疫作業をネットワークと融合することで、企業ネットワーク全体の健全度を向上させます。つまり NAC は、ネットワークのインフラストラクチャ レベルからセキュリティを確立していくためのアプローチとなります。

シスコでは、すべての組織における機能的なニーズに対応するために、包括的なアドミッション コントロール製品およびソリューションを提供しています。Cisco Clean Access (近日発売開始予定) は、NAC を実装するアプライアンス製品です。Cisco Clean Access は、独立型のエンドポイント評価、ポリシー管理、および修復サービスの迅速な導入を支援します。また、「Cisco ネットワーク アドミッション コントロール パートナー プログラム」を展開し、アンチウイルス ソフトウェアやその他のセキュリティ および管理ソフトウェア ソリューションの 60 を超える主要なメーカー (2005 年 10 月現在) のソリューションが、インテリジェントなネットワーク インフラストラクチャに組み込まれています。

NAC はシスコの自己防衛型ネットワークの一部であり、セキュリティ上の脅威を自動的に識別および防止し、それらに適応するためのネットワーク能力を大幅に強化します。

Q. NAC ソリューションはなぜ重要なのですか。

A. 「Day Zero (未知)」のウイルスおよびワームの侵入によるダウンタイムや継続的なパッチなど、ビジネスへの支障は続いています。NAC を使用すると、脆弱なホストに通常のネットワーク アクセスを与えないようにすることによって、このリスクを軽減できます。つまり、アンチウイルス ソフトウェア、セキュリティ ソフトウェア、および OS (オペレーティング システム) パッチに関する全社的な最新のポリシーに適合するホストだけが、通常のネットワーク アクセスを許可されます。脆弱なホストや非適合なホストは、パッチを適用して安全な状態になるまで隔離したり、アクセスを制限したりします。このようにして、これらのホストがワームやウイルスの感染源または感染対象にならないようにします。

NAC はネットワークを総合的に保護するために、ホストがネットワーク接続に使用するあらゆるアクセス方式に対応します。NAC の段階的なリリースにつれて、WAN リンク経由のゲートウェイ展開、IP Security (IPSec) リモート アクセス、ダイヤルアップ、さらに、スイッチングおよびワイヤレス インフラストラクチャを介したローカル ネットワーク展開も、NAC によって保護される予定です。

Q. NAC ソリューションにはどのような利点がありますか。

A. NAC には、次のような利点があります。

- **セキュリティの大幅な強化** — NAC を使用することで、エンドポイント (ノート型パソコン、PC、PDA、サーバなど) をセキュリティ ポリシーに準拠させて、ワーム、ウイルス、スパイウェア、およびマルウェアからネットワークをプロアクティブに保護します。また、被害を受けてから対処するのではなく、被害の防止に重点を置いています。
- **従来の投資の拡大** — NAC は、マルチベンダーのセキュリティ および管理ソフトウェアとの統合を拡充することで、ネットワーク インフラストラクチャやベンダー ソフトウェアに対する従来の投資を拡大します。
- **企業の復元力の強化** — NAC は、すべてのアクセス方式に対して総合的なアドミッション コントロールを提供し、非適合および不正なエンドポイントが、ネットワークの可用性に影響を与えないようにします。また、非適合、不正、および感染したシステムの識別と修復に関連する運用コストも削減します。

NAC はシスコの自己防衛型ネットワークの一部であり、脅威を識別および防止し、それらに適応するためのネットワークの可用性を大幅に強化します。

Q. なぜ、NAC は他にないソリューションなのですか。

A. NAC は脆弱なホストや非適当なホストによってネットワークの復元力が損なわれないようにするための独自のアプローチです。NAC を使用すれば、お客様はシスコ製品で構成されるネットワーク、アンチウイルス ソフトウェア、その他のセキュリティ ソフトウェアや管理ソフトウェアといった既存の投資を活用できます。NAC には次のような利点があります。

- **総合的な制御** — LAN、ワイヤレス、リモート アクセス、WAN など、すべてのアクセス方式に対応して、すべてのエンドポイントを検証します（一部は今後対応の予定）。
- **柔軟な展開オプション** — NAC アプライアンスおよび NAC フレームワークのアプローチは、すべての組織における技術上および運用上のニーズに対応するように設計されています。
- **エンドポイントの視覚化と制御** — 管理対象、管理対象外、ゲスト、および不正なデバイスが、企業のセキュリティ ポリシーを満たすようにします。
- **エンドポイント制御のライフサイクル サポート** — エンドポイントの検証、認証、許可、および修復を自動化します。
- **マルチベンダー ソリューション** — NAC は、シスコ主導による主要なセキュリティおよび管理ソフトウェア ベンダーとのコラボレーションです。

Q. NAC はどのような組織に役立ちますか。

A. NAC は、ウイルス、ワーム、スパイウェアなどの新型のセキュリティ上の脅威に対処することを望んでいるすべての組織に役立ちます。NAC は、環境へのアクセスを承認済みの適格な情報提供者のみに限定したいと考えている組織や、ネットワーク環境内のすべてのエンドポイントへのアクセスを監査し、監視する必要がある組織に役立ちます。特に、委託先や提携先のシステムを接続させるネットワークがあって、そのデスクトップやサーバの適合性の管理に頭を悩ませている企業に有益です。同じ理由から、NAC はより小さな組織にも有益です。金融、医療、官公庁、製造など、あらゆる業種で NAC を活用できます。

Q. NAC の実装には、シスコのどのような技術アプローチが使用されますか。

A. シスコでは、アプライアンス ベースのアプローチまたはアーキテクチャのフレームワークによるアプローチを使用して NAC を提供しています。

- Cisco Clean Access は、NAC の迅速な展開を可能にするアプライアンスです。Microsoft や主要なアンチウイルス ソフトウェア ベンダーからのパッチや更新を含めて、独立型のエンドポイント検証、クライアント、ポリシー管理、および修復サービスを導入します。現在、Cisco Clean Access はソフトウェアとして入手できます。また、専用のハードウェア アプライアンスとしても提供される予定です。Cisco Clean Access の価格は、中小・中堅企業も含めたすべてのお客様向けに設定されています。
- アーキテクチャのフレームワークによる NAC のアプローチでは、ネットワーク インフラストラクチャに対して、すべてのエンドポイントにセキュリティ ポリシーを適用するサードパーティ製ソリューションが組み込まれます。NAC は、アンチウイルス ソフトウェアやその他のセキュリティ および管理ソフトウェア ソリューションの主要ベンダー 60 社以上で、幅広く採用されている業界の先駆的ソリューションです。

Q. OS およびアプリケーションパッチの管理に NAC を使用できますか。

A. はい。NAC は OS やアプリケーションのパッチ管理テクノロジーではありませんが、パッチが適用されていない非適当なシステムを検疫エリアに隔離し、それらのシステムに修復を施すことができます。使用するテクノロジーによっては、シスコや NAC のベンダー パートナーが修復サイクルを推進して、プロセスの効率化を図ることができます。

Q. シスコはなぜ、アンチウイルス ソフトウェア、セキュリティ ソフトウェア、およびパッチ管理ベンダーと協業しているのですか。

A. お客様から従来より、エンドポイントの適合性の管理における問題を解決し、ウイルス、ワーム、およびスパイウェアによる損害を最小化するための総合ソリューションを、主要なアンチウイルス ソフトウェア、セキュリティ、およびパッチ管理ソフトウェア プロバイダーと共同で開発してほしいという要望がありました。この共同開発を通じて、ネットワークとエンドポイントのセキュリティおよび管理テクノロジーに対する既存の投資を活用できる、効果的なソリューションが実現しました。

Q. シスコと主要なアンチウイルス ソフトウェア、セキュリティ ソフトウェア、およびパッチ管理ベンダーは、NAC についてどのような関係にありますか。

A. シスコは主要セキュリティ ソフトウェア ベンダーである McAfee、Symantec、Trend Micro の協力を得て、NAC のアーキテクチャ、仕様、および共同マーケティング ガイドラインを定義しました。シスコはこれらの NAC ベンダー パートナーにエンドポイント ソフトウェア テクノロジーをライセンス供与し、複数のセキュリティ ソフトウェア クライアントからエンドポイントのセキュリティ ステータス情報をシスコのネットワークに伝達できるようにしています。このソフトウェアは Cisco Trust Agent と呼ばれ、シスコおよび NAC ベンダー パートナーの各ソリューションに組み込まれます。シスコおよび NAC サポート ベンダーの何社かは、お客様に Cisco Trust Agent を無料で配布する予定です。

NAC とシスコのセキュリティ戦略

Q. なぜシスコは NAC を推進しているのですか。

A. シスコは現在、お客様が直面している最も重要なセキュリティ上の課題の 1 つに取り組んでいます。セキュリティ ポリシーに適合したエンドポイントに基づいて NAC を実行するようになれば、ウイルス、ワーム、およびスパイウェアによる業務の中断を最小化することができます。ウイルスやワームによって引き起こされている損害を考えると、運用上および技術上の既存の対策では不十分であることが明らかです。NAC はホストに関するパッチ ポリシーの普遍的な実施を可能にし、非適合なシステムや潜在的に脆弱性のあるシステムを検疫エリアに移してネットワーク アクセスを禁止または制限する、新しい総合的なソリューションです。エンドポイントのセキュリティ ステータスに関する情報を入手し、その情報をネットワーク アドミッションに結び付けることによって、コンピューティング インフラストラクチャのセキュリティは大きく改善されます。

Q. シスコが提唱する自己防衛型ネットワークとは何ですか。

A. シスコの自己防衛型ネットワークは、革新的かつ多面的なセキュリティ構想であり、セキュリティ上のさまざまな脅威を識別および防止し、それらに適応するためのネットワーク能力を大幅に強化します。シスコの自己防衛型ネットワークは、システムレベルでの新しい防御機能を提供することによって、IP ネットワーク全体にセキュリティ サービスを統合するという考えに基づいています。

Q. NAC と自己防衛型ネットワークは、どのような関係にありますか。

A. NAC は、シスコの自己防衛型ネットワークの基本コンポーネントの 1 つです。

Q. NAC と SAFE ブループリントはどのような関係にありますか。

A. シスコの SAFE ブループリントは、ネットワーク設計者がネットワークのセキュリティ要件について考慮する際のガイドラインとなります。Cisco SAFE ではネットワーク セキュリティ設計に多層防御のアプローチを採用し、予測される脅威とその軽減方法に重点を置き、いずれか 1 つのセキュリティ システムに障害が発生してもネットワーク リソースが危険にさらされることのない、階層型のセキュリティ アプローチを実現します。

SAFE ブループリントは、設計および実装に関する他の付随事項と同様に、この新しいセキュリティ ソリューションを反映して更新される予定です。

NAC アプライアンス/Cisco Clean Access の概要

Q. NAC アプライアンス製品である CCA の特徴は何ですか。

A. Cisco Clean Access は、複雑な設定が不要であるため、簡単かつスピーディーに導入することができます。Cisco Clean Access により、認証と許可、ステータス検査、検疫、修復といった NAC の主機能が 1 つのシスコ製品に統合されます。

Q. Cisco Clean Access の導入実績はありますか。

A. はい。Cisco Clean Access は、幅広く導入されている実証済みの NAC ソリューションです。350 以上の組織と 250 万人のユーザが Clean Access で保護されたネットワークを利用しています。Cisco Clean Access には、企業での展開に対応したサーバベースの製品と、ユーザの数が 100、250、および 500 の環境に対応した小規模組織向けの製品があります。

Q. Cisco Clean Access は、Cisco Security Agent にどのように対応しているのですか。

A. Cisco Security Agent は、悪意のある脅威や攻撃からエンドポイントそのものを保護します。エンドポイントのセキュリティ状態に基づいたネットワーク アクセスの許可や拒否は実行しません。Cisco Clean Access はセキュリティ ポリシーの実行に重点を置いています。アクセスを許可する前に、各エンドポイントをネットワークの基準に適合させます。この 2 つのソリューションは連携が可能です。Cisco Clean Access を使用すれば、Cisco Security Agent をエンドポイント デバイスで実行できます。

Q. 通常、Cisco Clean Access はどのように使用されていますか。

A. Cisco Clean Access は、さまざまなシナリオで使用されています。LAN 経由のネットワークを保護する以外に、VPN コンセントレータやワイヤレス アクセス ポイントを介して接続するユーザとデバイスの検証にも使用されます。また、ネットワークを保護しながらも、ゲストや仮ユーザのアクセスは可能にしたい場合にも使用されます。

Q. Cisco Clean Access では、どのようなスキャンが行われますか。

A. Cisco Clean Access は、ネットワークベースおよびエージェントベースのスキャンを行います。ネットワークベースのスキャンでは、Remote Procedure Call (RPC; リモート プロシージャ コール) のバッファのオーバーフローやメッセージャーのバッファのオーバーフローなど、ネットワークの脆弱性がスキャンされ、エージェントベースのスキャンでは、ユーザのシステム レジストリ、ファイル システム、および特定のサービスとアプリケーションのシステム メモリがチェックされます。

Q. Cisco Clean Access の詳細は、どこで参照できますか。

A. <http://www.cisco.com/jp/go/cca> にアクセスしてください。

Cisco Clean Access の技術詳細

Q. Cisco Clean Access にはどのようなコンポーネントがありますか。

A. Cisco Clean Access は、Cisco Clean Access Server、Cisco Clean Access Manager、およびオプションの Cisco Clean Access Agent の 3 つのコンポーネントで構成されています。少なくとも 1 つの Cisco Clean Access Server と 1 つの Cisco Clean Access Manager が必要です。通常は、追加のフェールオーバー ペアを使用することを推奨します。Cisco Clean Access Agent とルール セットの更新は、価格に含まれています。

Q. Cisco Clean Access にはどのような展開オプションがありますか。

A. Cisco Clean Access は、インライン (すべてのトラフィックが Clean Access Server を通過) またはアウトオブバンドに展開できます。アウトオブバンドの構成例では、トラフィックは認証、評価、および修復プロセス時のみインラインになり、その後認証されたデバイスは、コアのルーティング ネットワークに切り替えられます。実際の IP ゲートウェイまたは仮想ゲートウェイとして、中央またはエッジで展開できます。

Q. 非適格なマシンはどのようにブロックされるのですか。

A. Cisco Clean Access Server をインラインで展開した場合、非適格なマシンは特定のサブネットに制限することで直接ブロックされます。Cisco Clean Access をアウトオブバンドに展開した場合は、VLAN 割り当てを使用してスイッチ ポート レベルで非適格ユーザをブロックします。

Q. Cisco Clean Access は、以前に確認および検証されたシステムも含めて、アクセスを試行するすべてのシステムをチェックするのですか。

A. いいえ。Cisco Clean Access では、認証済みデバイス リスト方式が使用されます。Cisco Clean Access Server は、認証済みデバイス リストに未記載のホストのみをチェックします。管理者は、新たな脆弱性に基づいたネットワーク スキャンを実行するために、セッション タイマーを使用してリストの更新頻度を設定することができます。

Q. Cisco Clean Access は、他社製のネットワーク機器と連携しますか。

A. Cisco Clean Access をインライン モードで展開した場合は、すべてのネットワーク機器と連携できます。アウトオブバンド モードで展開した場合は、シスコのスイッチのみと連携します。サポートされているスイッチのリストについては、下記を参照してください。 http://www.cisco.com/en/US/products/ps6128/products_device_support_table09186a008043a8d9.html

Q. 既存の Active Directory を使用して許可と認証を調整できますか。

A. Cisco Clean Access を使用すると、Active Directory グループに基づいて、ネットワーク アクセス権、帯域幅制限、およびセッション時間を調整できます。Cisco Clean Access は認証プロキシとして機能するため、認証データベースとの同期や、データベースの複製を行う必要はありません。RADIUS、Lightweight Directory Access Protocol (LDAP)、Kerberos、および Windows NT など、主要な認証形式のほとんどがサポートされています。

Q. Cisco Clean Access は、Cisco Secure Access Control Server (ACS) と連携しますか。

A. はい。Cisco Clean Access は、RADIUS を使用して Cisco Secure ACS と連携します。Cisco Clean Access は、詳細な RADIUS アカウンティングとフェールオーバーのサポートも提供します。

Q. Cisco Clean Access は認証に 802.1X を使用しますか。

A. いいえ。Cisco Clean Access は認証に 802.1X を必要としません。このため、Cisco Clean Access は 802.1X 以外の環境にも展開可能です。

Q. Cisco Clean Access にはどのようなチェック機能がプリインストールされていますか。

A. Cisco Clean Access には、最も一般的なアンチウイルス ソフトウェア ベンダー 16 社、Microsoft の更新プログラム、およびスパイウェア対策ソフトウェアに対応した、150 以上のチェック機能がプリインストールされています。これらのルールセットを更新するための追加コストは不要です。

NAC フレームワークの概要

Q. NAC フレームワークとは何ですか。

A. NAC フレームワークは、シスコシステムズが主導する業界イニシアチブ構想に基づいたアーキテクチャベースの技術的アプローチで、ネットワーク インフラストラクチャとサードパーティ製ソフトウェアを活用して、すべてのエンドポイントにセキュリティ ポリシーを適合します。NAC を使用すると、シスコ製品で構成されるネットワークやアンチウイルス テクノロジー、その他のセキュリティおよび管理ソフトウェアへの投資を統合して効果的に活用できます。現在、NAC フレームワーク ソリューションには、60 を超えるベンダーのソフトウェアを組み込み可能です。

NAC フレームワークを使用すると、管理対象ネットワークにアクセスしようとするエンドポイント デバイスに対して、ルータやスイッチを含むシスコのネットワーク デバイスがアクセス権を設定することができます。どの程度のアクセス権を与えるかは、アンチウイルス ソフトウェアや OS のパッチ レベルを含めた、現在のソフトウェア状態などのエンドポイント デバイスに関する情報に基づいて決定されます。非適切なデバイスについては、アクセスを拒否するか、そのデバイスを検疫エリアに入れるか、またはコンピューティング リソースへのアクセスを制限することができます。

Q. NAC を導入するためには、インフラストラクチャをアップグレードする必要がありますか。

A. NAC の導入に際しては、シスコと主要なセキュリティおよび管理ベンダーがさまざまな方法を試行しますが、特定のネットワークやセキュリティ要素については、更新やアップグレードが必要となる場合もあります。

NAC ネットワーキング ソリューションの大部分は、標準アップグレードまたは SmartNet 契約によって使用できるソフトウェア機能です。ネットワーク アクセス デバイスでは、NAC に対応したソフトウェア バージョンが実行されている必要があります。サードパーティのソリューションでは通常、NAC をサポートするように設計された製品のバージョンが実行されていることも必要です。

ルータ、スイッチ、VPN コンセントレータ、ワイヤレス アクセス ポイント、ワイヤレス LAN コントローラなどのシスコのネットワーク デバイスでは、現在 NAC がサポートされています（一部は近いうちにサポート予定）。

Q. NAC フレームワークはいつから使用できますか。

A. 現在、NAC は Cisco Catalyst[®] スイッチ、シスコのワイヤレス アクセス ポイント、シスコのアクセス ルータおよびミッドレンジルータ、Cisco VPN 3000 シリーズ コンセントレータで使用できます。今後のリリースでは、シスコの他のセキュリティ アプライアンスも含まれる予定です。Cisco Trust Agent は、シスコ製品、および NAC ベンダー プログラム メンバーのクライアントと管理ソフトウェア製品に組み込まれています。NAC の組み込み対応製品を出荷しているベンダー、または NAC の組み込みを予定しているベンダーのリストについては、<http://www.cisco.com/jp/go/nac> を参照してください。

Q. NAC フレームワークは輸出規制の対象となりますか。

A. NAC フレームワークは単独の製品ではなく、さまざまなコンポーネントを介して提供されるテクノロジーです。NAC フレームワークに関する輸出規制については、Web に掲載されている個別のコンポーネントのデータシートを参照してください。ソリューション自体は、輸出規制の対象外です。

Q. 現在、NAC フレームワークでサポートされているプラットフォームとソフトウェアは何ですか。

A. シスコ製および NAC ベンダー製の複数のコンポーネントが NAC フレームワークに対応しています。シスコ製のコンポーネントは次のとおりです。

- サポートされるスイッチ プラットフォーム（随時追加予定）
 - Catalyst 6500 — Supervisor Engine 2, 32, 720 — Catalyst OS、Hybrid、および Cisco IOS (Cisco IOS のサポートは Supervisor Engine 32 および 720)
 - Catalyst 4000 — Supervisor Engine II+, II+TS、IV、V、V-10GE — IOS
 - Catalyst 4948、4948-10GE
 - Catalyst 3550、3560、3750 — IP ベースおよび IP サービス
 - Catalyst 2940、2950、2955、2960、2970 — すべて

- サポートされるワイヤレスプラットフォーム (随時追加予定)
 - Aironet 1100、1130AG、1200、1230AG、1300 Cisco IOS ソフトウェア ベースのアクセス ポイント
 - Cisco 2000、4100、または 4400 Wireless LAN Controller に接続された LWAPP を実行している Aironet 1000、1130AG、1200、1230AG、1240AG Lightweight アクセス ポイント
 - Catalyst 6500 シリーズ Wireless LAN Services Module (WLSM)
 - サポートされるルータプラットフォーム (随時追加予定)
 - セキュリティに対応した Cisco IOS® ソフトウェア リリース 12.3(8)T イメージ (およびそれ以上)
 - Cisco 75xx
 - Cisco 72xx
 - Cisco ISR 3800 シリーズ
 - Cisco 3700 シリーズ
 - Cisco 3640 および 3660-ENT
 - Cisco ISR 2800 シリーズ
 - Cisco 2600XM および 2691
 - Cisco 1812J、1812JW
 - Cisco ISR 1800
 - Cisco 1712、1721、1751、1751-V、1760
 - Cisco 871
 - Cisco VPN 3000 シリーズ コンセントレータ
 - Cisco Secure ACS
 - Cisco Trust Agent v1.0 のサポート対象プラットフォームは次のとおりです。
 - Windows XP Professional (Service Pack 1 以下)
 - Windows 2000 Professional および Windows 2000 Server (Service Pack 4 以下)
 - Windows NT 4.0
- また、v2.0 のサポート対象プラットフォームは次のとおりです。
- Windows 2003
 - Windows XP Professional (Service Pack 2 以下)
 - Red Hat Enterprise Linux 3.0
- Cisco Security Agent
 - Cisco Secure Monitoring, Analysis and Response System (MARS)

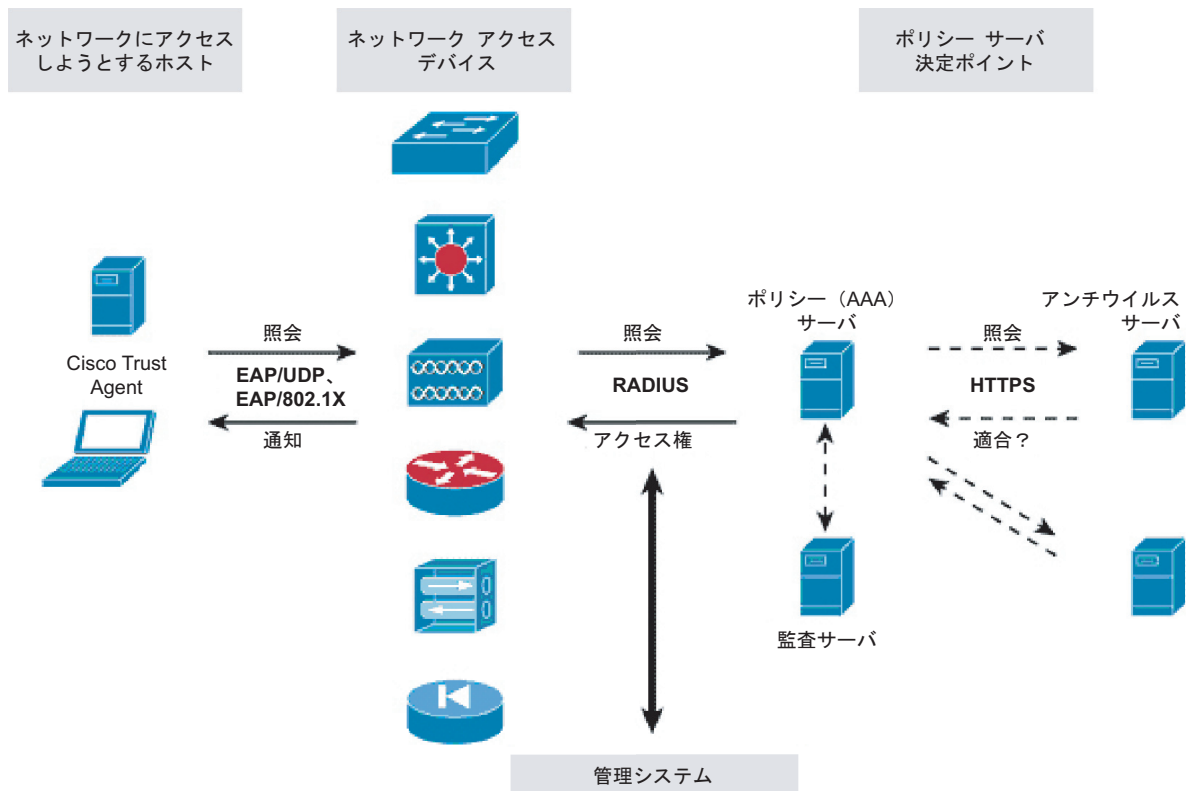
NAC フレームワークの組み込み対応製品を出荷しているベンダー、または組み込みを予定しているベンダーのリストについては、<http://www.cisco.com/jp/go/nac> を参照してください。

NAC フレームワークの技術詳細

Q. NAC フレームワークはどのようなコンポーネントから構成されますか。

A. NAC システムには 4 つのコンポーネントがあります (図 1)。

図 1 NAC フレームワークの 4 つのコンポーネント



- エンドポイント セキュリティ ソフトウェア (アンチウイルス ソフト、Cisco Security Agent など) および Cisco Trust Agent** — Cisco Trust Agent は、アンチウイルス ソフトウェアや Cisco Security Agent などの OS およびセキュリティ ソフトウェア クライアントからセキュリティ ステータス情報を収集し、アクセス制御を行うネットワーク デバイスにその情報を伝達します。ネットワーク アドミッションを適切に決定するための情報としては、アプリケーションおよび OS のステータス (アンチウイルス ソフトウェア、OS のパッチ レベル、証明書など) が使用されます。シスコおよび NAC ベンダー パートナーが提供するセキュリティ ソフトウェア クライアントには、Cisco Trust Agent が組み込まれています。
- ネットワーク アクセス デバイス** — アドミッション コントロール ポリシーを実行するネットワーク デバイスには、ルータ、スイッチ、ワイヤレス アクセス ポイント、ワイヤレス LAN コントローラ、およびセキュリティ アプライアンスがあります。これらのデバイスはホスト証明書を要求し、この情報をポリシー サーバに伝達し、そのサーバでネットワーク アドミッション コントロールの決定が行われます。このようにネットワークは、各サイトで定義したポリシーに基づいて、許可、拒否、隔離、制限など、適切なアドミッション コントロールを実行します。
- ポリシー サーバ** — ポリシー サーバはネットワーク デバイスから伝達されたエンドポイントのセキュリティ情報を評価し、適用すべきアクセス ポリシーを決定します。ポリシー サーバシステムの基盤となっているのは、Authentication, Authorization, and Accounting (AAA; 認証、許可、アカウンティング) RADIUS サーバである Cisco Secure ACS です。このサーバは、アンチウイルス ポリシー サーバなど、証明書に関する詳しい検証を提供する NAC ベンダー パートナーのアプリケーション サーバと連動して機能します。また、NAC 証明書の照会に応答しないシステムの検証を支援する監査サーバとも連携します。
- 管理システム** — NAC 要素のプロビジョニングはシスコの管理ソリューションによって行われます。このソリューションは、運用ツールの監視機能と報告機能も提供します。この機能は、CiscoWorks VPN/Security Management Solution (VMS) および Cisco Secure MARS に基づいています。また、NAC のベンダー パートナーからも、それぞれのエンドポイント セキュリティ ソフトウェア用管理ソリューションが提供されています。

Q. Cisco Trust Agent とは何ですか。

A. Cisco Trust Agent は、OS、およびアンチウイルス ソフトウェアや Cisco Security Agent などのセキュリティ ソフトウェア クライアントからセキュリティ ステータス情報を収集し、アクセス制御を行うネットワーク デバイスにその情報を伝達します。Cisco Trust Agent の主な役割は、次の 3 つです。

- **ネットワーク通信** — アプリケーションおよび OS の情報（アンチウイルス ソフト、OS パッチの詳細など）に関するネットワークからの要求に応答します。現在は、レイヤ 3 の通信プロトコルのサポートが含まれます。リリース 2 では、レイヤ 2 も含まれる予定です。
- **セキュリティ モデル** — ホスト証明書を要求するアプリケーションまたはデバイスを認証し、この情報を暗号化して伝送します。
- **アプリケーションブローカ** — API を介して、さまざまなアプリケーションがステータス情報および証明書の要求に応答できるようにします。

シスコは NAC ベンダー パートナー各社に Cisco Trust Agent をライセンス供与し、各社がそれぞれのセキュリティ ソフトウェア クライアント製品に Cisco Trust Agent を組み込めるようにしています。製品配布の一部に、Cisco Trust Agent を組み込んでいたベンダーもあります。Cisco Security Agent v4.5 には、Cisco Trust Agent がインストール オプションとして組み込まれています。シスコおよび一部の NAC サポート パートナーからは、Cisco Trust Agent が無料で配布される予定です。

Cisco Trust Agent 2.0 には、NAC をシスコのスイッチに有線で展開する 802.1X サプリカントがオプションに含まれています。このサプリカントは無料で提供されますが、ワイヤレスのサポート、および集中管理インターフェイスの提供は行っていません。

Q. NAC をサポートする 802.1X サプリカントを教えてください。

A. 有線またはワイヤレスのトポロジーに対応した 802.1X 構成で NAC を使用する場合、NAC および NAC に関連する EAP タイプをサポートする 802.1X サプリカントが必要です。現在、NAC 対応サプリカントを入手するには、次の方法があります。

- Cisco Trust Agent 2.0 には、NAC をシスコのスイッチに有線で展開する 802.1X サプリカントがオプションに含まれています。このサプリカントは無料で提供されますが、ワイヤレスのサポート、および集中管理インターフェイスの提供は行っていません。

Windows およびその他の OS の実稼働プラットフォームで使用できるネイティブ サプリカントでは、現在 NAC はサポートされていません。

Q. ネットワーク デバイスは、どのようにホストと通信するのですか。

A. ネットワーク デバイスは、要求および応答メッセージの仕組みを利用して、ホストからアプリケーションおよび OS の証明書入手します。ホスト証明書のパッケージ化と認証には、EAP が使われます。主に使用するトランスポート プロトコルは、ゲートウェイ通信のためのレイヤ 3 プロトコルである IP と、ファーストホップ通信のためのレイヤ 2 プロトコルである 802.1X の 2 つです。IP は、ネットワーク デバイスがホストから任意のホップ数だけ先にあり、最初にネットワーク デバイスがホストを認識するのが IP パケットである場合に使われます。これにはルータ、ファイアウォール、およびリモート アクセス通信が含まれます。802.1X は、スイッチを使用した LAN 内、およびアクセス ポイントとワイヤレス LAN コントローラを使用したワイヤレス接続で使用されます。特定のスイッチでは、スイッチポート レベルでのレイヤ 3 による IP 通信がサポートされているため、802.1X を使用する必要はありません。

Q. ホストが適合性のあるアンチウイルス ソフトウェアを実行していることを確認できますか。

A. はい。NAC は、主要なアンチウイルス ソフトウェア ベンダー製のソフトウェアとリンクします。これによって、ホストでアンチウイルス ソフトウェアが稼働し、ソフトウェア、エンジン、およびパターン ファイルのバージョンがセキュリティ ポリシーに準拠していることが確認されます。この情報は Cisco Trust Agent によって収集され、ネットワークに伝達されます。アンチウイルス ソフトウェアを実行していないホスト、または適正なバージョンが機能していないホストについては、あらかじめ定義されたポリシーにしたがって、ネットワークへのアクセスが制限されたり、アクセスが拒否されたりします。この機能は、Windows NT、XP、2000、2003 プラットフォーム、および特定のバージョンの Red Hat Linux でサポートされています。

Q. ホストが適正な OS パッチを適用していることを確認できますか。

A. はい。Cisco Trust Agent は、OS バージョン、パッチ、およびホットフィックス情報を検証し、この情報をアクセス制御を行うシスコのネットワーク デバイスに伝達します。適正なパッチを実行していないホストについては、ネットワークへのアクセスを制限するか、アクセスを拒否することができます。現在この機能は、Windows NT、XP、2000、2003 プラットフォーム、および特定のバージョンの Red Hat Linux でサポートされています。Cisco Security Agent および多くの NAC ベンダー製品でも、OS パッチ情報が提供されています。また、エンドポイントが適合するように修復および更新される場合もあります。

Q. ゲスト、委託先、および提携先のシステムがポリシーに適合していることを確認できますか。

A. はい。NAC を使用すれば、IT 部門の管理下にあるシステムだけでなく、ネットワークにアクセスしようとするすべてのシステムについて、適合性をチェックできます。委託先や提携先のシステムを含めて、ホストがどこで管理されているものであっても、アンチウイルスソフトウェアと OS に関するポリシーに適合しているかどうかを検証されます。ネットワークにアクセスしようとしているホストで Cisco Trust Agent が稼働していない場合、NAC の第一段階では、デフォルトのアクセスポリシーが適用されます。適正なパッチを実行していないホストについては、ネットワークへのアクセスを制限するか、アクセスを拒否することができます。NAC の第二段階では、サードパーティ製ホストのスキャン ツールおよび監査ツールが組み込まれ、エージェントレス（応答しない）エンドポイントについては、検証結果に応じたアクセスレベルを設定できるようになります。

NAC は、異なるベンダー製のアンチウイルス ソフトウェアが混在する環境にも対応します。たとえば、社員は McAfee 社のアンチウイルス ソリューションを使用していて、委託先が Symantec 社のアンチウイルス ソリューションを使用している場合、どちらにも Cisco Trust Agent が稼働していれば、同じネットワーク上でそれぞれの証明書の適合性をチェックし、ユーザの ID とエンドポイントのセキュリティ ステータスに基づいて差別化されたポリシーを適用することができます。

Q. サポート対象のホスト プラットフォームを教えてください。

A. NAC の動作は、あらゆるホスト プラットフォームに対応できます。ただし、ホストのタイプによって、そのホストに関してどれくらい詳細な検証が実行できるかが異なります。

- **応答 (responsive) ホスト** — Cisco Trust Agent が稼働しているホスト。セキュリティ ソフトウェア、アプリケーション、および OS の情報をネットワークに伝達して検証させることができます。
- **非応答 (non-responsive) ホスト** — Cisco Trust Agent がアクティブでない（インストールされていない、または稼働していない）エージェントレス ホスト。アプリケーションや OS の情報をネットワークに伝達できません。

応答デバイスに関するネットワーク アドミッション ポリシーは、ホストから取得したアプリケーションおよび OS の検証結果（たとえば、アンチウイルス ソフトや OS のパッチ レベル）に基づいて設定できます。非応答デバイスはこれらの情報を転送しないので、そのデバイスに関するネットワーク アドミッション ポリシーは、システムの IP アドレスや経由している回線を監査するなど、その他の考慮事項に基づいて設定する必要があります。

NAC の段階ごとに、応答デバイスおよび非応答デバイスの両方について、検証できる情報の種類を増やしていく予定です。応答デバイスの場合、NAC フレームワークに組み込むアプリケーションを増やすことで、より詳細なチェックが実行できるようになります。非応答のデバイスの場合、デバイスを検証してデバイス タイプや状態を判別する監査システムの導入によって対応します。

Cisco Trust Agent は、Windows NT、XP、2000、および 2003 と、特定のバージョンの Red Hat Linux でサポートされています。第二段階以降では、OS サポートを拡充し、広範囲のプラットフォームを容易にサポートできるオープン フレームワークに進化します。

Q. ホストが Cisco Trust Agent を実行していない場合でも、NAC フレームワークは役に立ちますか。

A. Cisco Trust Agent を実行していないホストは、アプリケーションおよび OS 情報に対するネットワーク要求に応答しないので、これらのデバイスは非応答またはエージェントレス デバイスと呼ばれます。ネットワーク アドミッション ポリシーは、応答デバイスだけでなく、非応答デバイスについても設定できます。非応答デバイスには、MAC アドレスや IP アドレスなどのネットワーク情報に基づいてポリシーを適用できます。特定の使用例では、サードパーティ製のホスト スキャンおよび監査ツールとリンクし、監査プロセスを通じてポリシー選択基準をさらに細かく設定できます。

Q. 非適合なホストについては、どのような取り扱いができますか。ポリシーに適合していないホストを適合させることはできますか。

A. NAC の主な目的は、管理者が各ホストの適合レベルを監視して、非適合なホストによる通常のネットワーク アクセスを制限または拒否できるようにすることです。多くの場合、アクセスの制限とは、ホストを隔離してネットワークの限られたエリアとしか通信できないようにすること、またはパブリック セグメントにしか接続できないようにすることを意味します。システムを隔離するさらなる目的は、非適合なシステムを修復するためのセキュアな環境を用意し、アンチウイルス ソフトウェアのパターン ファイルを更新したり、OS ホットフィックスを適用したりすることで、これらのシステムを適合した状態にすることです。

現在、シスコのルータおよび Cisco VPN 3000 シリーズ コンセントレータでは、ルータに Access Control List (ACL; アクセス制御リスト) を適用することによって、非適合なシステムのアクセスを制限するネットワーク アドミッション コントロールが提供されています。ポリシーに合わせた ACL を詳細に設定することで、非適合ホストとネットワーク上の他のシステムとの通信を制限できます。たとえば、アンチウイルス サーバとだけ通信できるようにして新しいパターン ファイルをダウンロードさせたり、パッチ管理サーバと通信してホストのソフトウェア バージョンを更新したりといった設定ができます。

Cisco Catalyst スイッチとワイヤレス アクセス ポイント、またはワイヤレス LAN コントローラでは、レイヤ 2 ポートに適用される VLAN 割り当てを使用することで、非適合システムのアクセスを制限するネットワーク アドミッション コントロールが提供されます。ユーザは、適合ホストと非適合ホスト間の通信を制限するレイヤ 2 環境を設定できます。また、特定の Catalyst スイッチでは、ポートベースの ACL 割り当てをサポートしているため、ルータベースのアプローチ方式に似た代替セグメンテーションアプローチとして通信を制限することもできます。

Q. 非適合ホストは常にアクセスを拒否されるのですか。

A. いいえ。管理ポリシーによって異なります。非適合ホストの取り扱いは、組織が定義するポリシーによって異なります。非適合ホストであることが判明しても、通常のネットワーク アクセスを許可することができます。また、パブリック セグメントに限ってアクセスを許可することも、更新のため修復セグメントへのアクセスを許可することも、または完全にアクセスを拒否することも可能です。多くの場合、非適合デバイスの取り扱いは、そのデバイスの場所によって左右されます。たとえば、ラボに属する非適合なマシンについては実稼働ネットワークとの通信を完全に禁止し、非適合なユーザのデスクトップについては、隔離して修復サーバとしか通信できないようにします。

Q. NAC フレームワークはユーザおよびデバイス AAA とどのように連携しますか。

A. NAC を使用することで、組織はネットワークに接続するエンドポイントのステータスに基づいてアドミッション ポリシーを監査できます。これは、同じ目的で行われるユーザおよびデバイス ID のチェックを補完するものです。シスコ ルータおよび VPN 3000 シリーズ コンセントレータでは、ネットワークの境界ポイントにおいて IP ベースでこの処理を行います。ただし、NAC の処理はユーザおよびデバイス AAA とは独立しています。NAC では、Cisco Catalyst スイッチおよびシスコのワイヤレス アクセス ポイントまたはワイヤレス LAN コントローラを使用したレイヤ 2 もサポートされているため、オプションで 802.1X と連携することもできます。現在これらのアクセス方式では、ユーザとデバイスの AAA を実行するメカニズムを利用できるようになっており、NAC がこれらと連携することで、管理者はユーザとデバイスの ID だけでなく、デバイス ステータスも組み合わせた情報に基づいてポリシーを定義できるようになります。

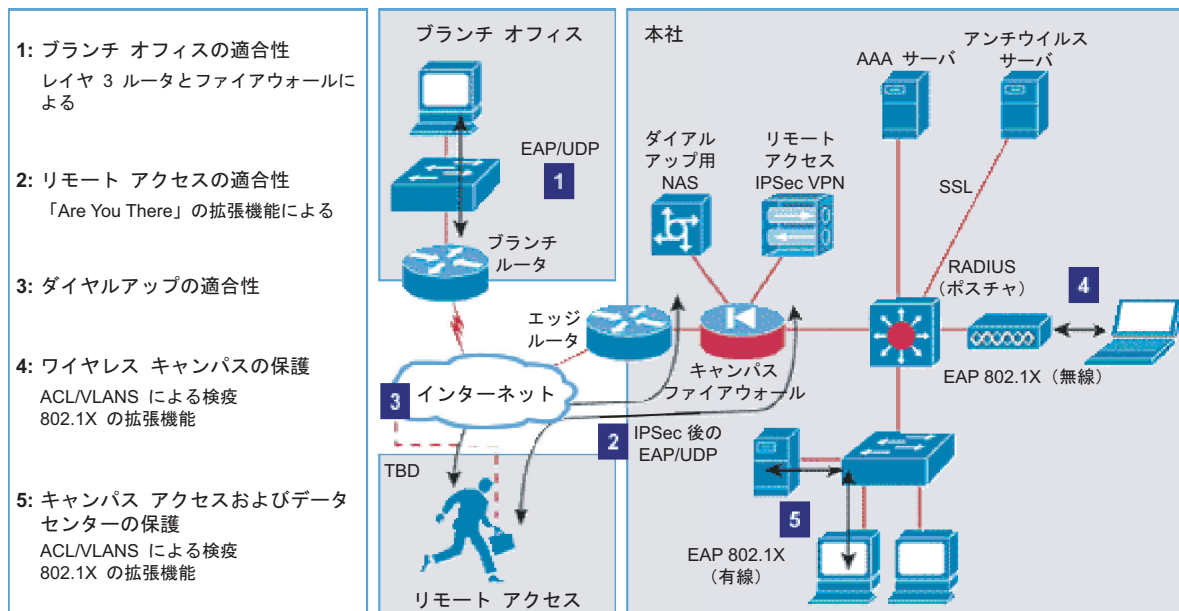
NAC フレームワークの展開

Q. NAC フレームワークにはどのような展開シナリオがありますか。

A. NAC は、キャンパス スイッチング、ワイヤレス、ルータ WAN および LAN リンク、IPSec リモート アクセス、ダイヤルアップなど、ホストがネットワーク接続に使用するあらゆるアクセス方式に対応し、総合的な制御を提供します。図 2 に、いくつかの展開シナリオを示します。

- **ブランチ オフィス (および SOHO) の適合性** — プライベート WAN またはインターネット上のセキュア チャネル経由で、中央の企業リソースに接続しようとするリモート オフィスまたは SOHO のホストの適合性を確認します。この適合性チェックは、ブランチ オフィスの出力側ルータまたはメイン オフィスのアグリゲーション ルータなどで実行されます。
- **リモート アクセスの適合性** — リモートおよびモバイル ワーカーのデスクトップに最新のアンチウイルス ソフトウェアおよび OS パッチが使用されていることを確認してから、IPSec などの VPN 接続による企業リソースへのアクセスを許可します。
- **ダイヤルアップ アクセスの適合性** — IPSec リモート アクセスの適合性と同じように、従来型のダイヤルアップ接続を使用するホストが、企業ポリシーに適合していることを確認します。
- **ワイヤレス キャンパスの保護** — ネットワークにワイヤレス接続するホストをチェックし、適正なパッチが適用されていることを確認します。802.1X 通信を使用し、デバイス認証およびユーザ認証と組み合わせて検証を行います。
- **キャンパス アクセスおよびデータ センターの保護** — オフィス内のデスクトップおよびサーバを監視して、企業のアンチウイルス ポリシーおよび OS パッチ ポリシーに適合していることを確認してから、通常の LAN アクセスを許可します。ホストにとってネットワークの入り口であるレイヤ 2 スイッチのポート単位でアドミッション コントロールを行うことにより、組織内のウイルス感染およびワーム感染のリスクを軽減します。

図 2 総合的な適合性の検証



Q. NAC フレームワークの各コンポーネントは、どこから提供されますか。

A. NAC ソリューションの各コンポーネントは、シスコおよび NAC ベンダー パートナーから提供されます。シスコが提供する NAC の基本コンポーネントには、次のようなものがあります。

- アドミッション コントロールを実行するネットワーク デバイス — ルータ、スイッチ、ワイヤレス アクセス ポイント、ワイヤレス LAN コントローラ、およびセキュリティアプライアンス。ソフトウェアの機能拡張により、既存および新規のプラットフォームに NAC の機能が組み込まれます。
- Cisco Secure ACS — アドミッション権限を判別するポリシー決定ポイントである AAA RADIUS サーバ。Cisco Secure ACS の機能は NAC をサポートするように拡張されています。
- Cisco Trust Agent — シスコが開発したホスト エージェント。シスコまたは NAC ベンダー パートナーからスタンドアロン エージェントとして直接提供されるほか、Cisco Security Agent に組み込まれるなど、さまざまな方法で配布されます。
- Cisco Security Agent — ホスト上で使用し、Day Zero 攻撃となるワームおよびウイルスからの保護を提供するとともに、NAC が適合性を検証するために使用する OS パッチおよびホットフィックスの情報を提供します。
- Cisco Secure MARS — システムの監視およびレポートを行うツール。
- CiscoWorks VMS — 複数のルータに対して一度に NAC を設定できます。

NAC ベンダー パートナーは、エンドポイント検証用のセキュリティ製品の統合、検証および修復用のポリシー管理コンポーネント、システム内のイベントを認識する監視機能とレポート機能など、さまざまな拡張機能を NAC 環境に提供しています。

Q. Cisco Trust Agent の入手方法を教えてください。

A. NAC ベンダー パートナーのなかには、Cisco Trust Agent をソフトウェアに組み込んで提供するところがあります。また、Cisco Security Agent に組み込まれているほか、Cisco.com から入手することもできます。

Q. NAC フレームワークを展開するには、どうすればよいですか。

A. NAC の展開方法については、ソリューション ガイドに詳しく記載されています。NAC の展開に関する主要テクノロジー コンポーネントは次のとおりです。

- 適切なネットワーク デバイス ハードウェアによる NAC のサポート
- 適切なネットワーク デバイス上のイメージのアップグレード
- ホストのアンチウイルス ソフトウェアおよびエンドポイント ソフトウェアのアップグレード
- ホスト上の Cisco Trust Agent
- Cisco Secure ACS サーバ (適合性のチェックおよびポリシーの実施に対応)
- Cisco Secure MARS
- NAC システムのコンポーネント (ルータなど) を設定する CiscoWorks VMS などの管理ツール

また、運用面での考慮事項は次のとおりです。

- システムを管理し、管理コンポーネントを適切に調整するための、管理上の権限モデルの決定
- ネットワーク アドミッション コントロール ポリシーの定義および実装
- システムがピーク状況に対応できるようにするための、スケーラビリティおよびパフォーマンス要件の決定 (Cisco Secure ACS などのポリシー決定インフラストラクチャでは特に重要)
- 検疫および修復用の環境の決定および実装

NAC を初めて展開する際は、はじめからポリシーを実施するのではなく、まずポリシーの適合性をチェックすることを推奨します。そのためには、ホストのアドミッション証明書の検証を実行してレポートを作成し、検証結果にかかわらず、通常のネットワーク アクセスを許可します。いつから実際にポリシーを実施するかは、組織のポリシーや準備状態のほかに、危機状況の重大度によって異なります。

Q. NAC の展開を容易に行うためには、シスコのどのようなサービスを利用できますか。

A. シスコのサービスおよびサポートでは、専門性の高いコンサルティング サービスやテクニカル サポートなど、さまざまなサービスを提供しています。Cisco Advanced Services では、効果的な NAC ソリューションに不可欠な要件の分析、プランニング、設計、および実装に関して、専門家によるコンサルティングを提供しています。一貫性のある実証済みの方法で NAC を実装するために、Advanced Services コンサルタントでは次のサービスを提供しています。

- **NAC の適応性の検証** — NAC の展開要件を分析し、NAC ソリューションをサポートするためのネットワーク デバイス、運用、およびアーキテクチャの適応性を検証します。
- **NAC の限定的導入** — ソリューションを限定的にインストールおよび設定し、NAC ソリューションをテスト運用で経験できるようにします。
- **NAC の設計開発** — NAC をネットワーク インフラストラクチャに統合するための詳細な設計の開発を支援します。
- **NAC の実装エンジニアリング** — NAC の全面実装をサポートし、インストール、設定、統合、および管理を行うための詳細な展開計画を作成します。

NAC ソリューションの展開に際し、シスコのテクニカル サポート サービスでは、社内リソースを補完して、シスコ製品の動作の効率化、高可用性の維持、最新のシステム ソフトウェアの導入を図ります。

Q. NAC フレームワークを実装するには、新しい AAA サーバが必要ですか。

A. はい。NAC の展開には、Cisco Secure ACS が必須となります。Cisco Secure ACS は、NAC をサポートするように機能拡張されており、ユーザおよびデバイスの AAA などの従来の RADIUS および TACACS+ サービスを引き続き提供しながら、これらの新しい機能をサポートします。つまり、ユーザ、デバイス、OS、およびアプリケーションのステータスに関する AAA を実行します。また、シスコは RADIUS の主要ベンダーと協業して NAC をサポートしていく予定です。

NAC には、テクニカル ソリューション ガイドが付属しています。このガイドには、既存の Cisco Secure ACS 展開を拡張して、NAC によるポリシー管理の実現方法決定に役立つ設計、パフォーマンス、および拡張に関する考慮事項が示されています。

Q. アドミッション コントロールは、どのように実行されますか。

A. ネットワーク アクセス デバイスは、証明書を要求するメッセージをホストに送信します。AAA サーバである Cisco Secure ACS によって、ホスト上の Cisco Trust Agent との間でセキュアな EAP 通信が成立します。このとき、Cisco Trust Agent は Cisco Secure ACS を検証します。ホスト アプリケーションが証明書を Cisco Trust Agent に渡すと、証明書はネットワーク デバイスを經由して Cisco Secure ACS に送信され、そこで認証と許可が行われます。場合によっては、Cisco Secure ACS がベンダー パートナーのポリシー サーバのプロキシとして動作し、ソフトウェア アプリケーション証明書をサーバに直接転送して、検証を行うこともあります。

証明書が検証されると、Cisco Secure ACS はネットワーク デバイスに対応する適切なポリシーを選択します。たとえば、Cisco Secure ACS がルータに ACL を送信し、そのホストに対して特定のポリシーを実施することができます。

非応答 (エージェントレス) デバイス (Cisco Trust Agent がアクティブでないデバイス) については、ネットワークまたは Cisco Secure ACS がデフォルトのポリシーを適用します。特定の使用例以外に、脆弱性検証ツールなどの監査サーバによって、ホスト システムの動的な検証が行われ、エンドポイントに許可されるネットワーク アクセスの適切なレベルが決定されることもあります。

Q. ネットワーク デバイスは、どのように AAA インフラストラクチャと通信しますか。

A. ネットワーク デバイスと Cisco Secure ACS 間の通信には、RADIUS が使われます。

Q. AAA サーバと NAC ベンダー パートナーのサーバは、どのように NAC フレームワークに関与していますか。

A. Cisco Secure ACS AAA サーバは、証明書を検証してホストのアプリケーションおよび OS パッチの適合性を調べ、適用すべきネットワーク アドミッション ポリシーを判別し、モニタリング システム用に適切なアカウンティング レコードを生成する役割を果たします。場合によっては、Cisco Secure ACS がアプリケーション証明書の認証のためのプロキシとして動作し、その情報を別のアプリケーション ポリシー サーバに転送することも可能です。たとえば、アンチウイルス ソフトウェア証明書をアンチウイルスまたはパッチ管理ポリシー サーバに転送して検証を行うように、Cisco Secure ACS を設定することができます。この場合、アプリケーション ポリシー サーバは情報を検証すると、適合性のレベル (完全適合、部分適合、または非適合) を定義するトークンを Cisco Secure ACS に渡します。このプロキシ通信は、現在 AAA サーバが One Time Password (OTP; ワンタイム パスワード) ユーザを認証している方法とよく似ています。Cisco Secure ACS はこのトークンを適切なポリシーにマッピングし、ネットワーク デバイスを適切なアドミッション コントロール設定に更新します。

Q. NAC は標準規格に基づくアプローチですか。

A. NAC では、EAP、EAP over UDP、802.1X、RADIUS など、標準規格に基づくテクノロジーを使用しています。NAC ソリューションをサポートするために、場合によってはこれらのテクノロジーを特定の拡張機能に対応させる必要があります。シスコでは、該当する規格団体を通じてこれらの拡張機能の採用を推進していく予定です。

Q. さらに詳しい情報はどこにありますか。

A. NAC についての詳細は、シスコの販売代理店にお問い合わせいただくか、<http://www.cisco.com/jp/go/nac> を参照してください。

©2005 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco ロゴは米国およびその他の国における Cisco Systems, Inc. の商標または登録商標です。
この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービスマーク、登録商標、登録サービスマークです。
この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ株式会社

URL: <http://www.cisco.com/jp/>

問合せ URL: <http://www.cisco.com/jp/go/contactcenter/>

〒 107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館

TEL: 03-6670-2992

電話でのお問合せは、以下の時間帯で受付けております。

平日 10:00 ~ 12:00 および 13:00 ~ 17:00

お問合せ先