

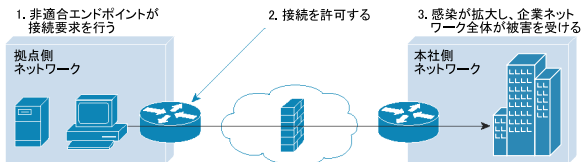
アドミッション コントロールの必要性

ウィルスやワームによる被害のために、企業ではシステムのダウン、復旧コスト、パッチの継続適用、社会的責任、収益の損失などの負担が生じています。

最近では攻撃の拡大速度も速くなり、システムの脆弱箇所セキュリティアップデートを適用する前、多くの場合はセキュリティベンダーがアップデートを開発して配布する前に、ネットワークが被害を受けています。

解決すべき問題とは？

エンドポイントがネットワークへログオンするたびに、ネットワークのセキュリティが損なわれる危険があります。古いウィルス対策ソフトのイメージファイルを使っていたり、OS へのパッチが適用されていないなど、ネットワークセキュリティポリシーに適合しないサーバやデスクトップが数多く存在し、それを検出することは困難で、事実上これらを封じ込めることはできません。そのため、こうしたサーバやデスクトップがネットワークに接続するたびに、ネットワーク環境の脆弱性が高まります。



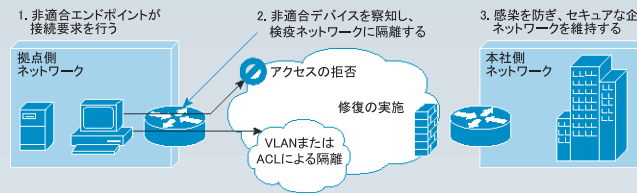
こうしたエンドポイントの1つがウィルスやワームに感染すると、それを突き止めて隔離し、ネットワークから切り離すことは、多くの時間とリソースを消費します。しかも、攻撃を受けているときは、そのような時間もありません。

そして、従来のエンドポイントのセキュリティテクノロジーは、攻撃を受けているホストを保護しようとしますが、ネットワークアベイラビリティの確保や企業の復旧には役に立ちません。

NAC

ネットワークアドミッションコントロール (NAC) とは、Cisco Systems® が主導する業界アライアンスで、ネットワークセキュリティポリシーに確実に適合していることを確認してから、エンドポイントのアクセスを許可するというソリューションです。

NAC では、定められたセキュリティポリシーに適合するエンドポイントデバイスにはネットワークアクセスを許可し、適合しないデバイスについてはアクセスを拒否して修復のために隔離するか、制限付きアクセスを許可します。



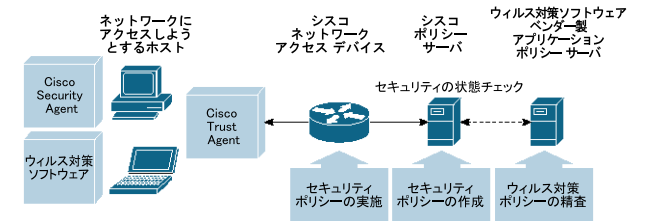
NAC は、次の重要なコンポーネントから構成されています。

- 1. 通信エージェント** — Cisco® Trust Agent は、ウィルス対策ソフトウェアや OS、Cisco Security Agent などのエンドポイント上のセキュリティソフトウェアソリューションからセキュリティステータスの情報を収集し、ネットワークアクセスデバイスに伝達するソフトウェアツールです。
- 2. ネットワークアクセスデバイス** — ネットワークにアクセスしようとするデバイスは、最初にネットワークアクセスデバイス (ルータ、スイッチ、VPN コンセントレータ、ファイアウォールなど) との通信を行います。ネットワークアクセスデバイスは、Cisco Trust Agent を通じてエンドポイントにセキュリティ「証明書」を要求し、この情報をポリシーサーバに送ってアドミッションの判定を受けます。
- 3. ポリシーサーバ** — Cisco Secure Access Control Server (ACS) およびサードパーティベンダー製ポリシーサーバでは、ネットワークアクセスデバイスから送られたエンドポイントの証明書を検査し、適用するアクセスポリシー (許可、拒否、隔離、制限) を判断します。
- 4. 管理システム** — CiscoWorks VPN/Security Management Solution (VMS) や NAC 協業パートナー製の管理ソリューションは、NAC コンポーネントのプロビジョニングを行い、モニタツールやレポートツールを提供し、エンドポイントのセキュリティアプリケーションを管理します。
- 5. アドバンスド サービス (Advanced Services)** — 計画、設計、実装を統合したコンサルティングサービスを提供して、ホストコンプライアンスを実施するための効果的な NAC ソリューション導入を支援します。(予定)

NAC のメリット

ネットワークリソースへのアクセス前に非適合エンドポイントデバイスに対してネットワークセキュリティポリシーを実施することにより、コストをかけずに、ネットワーク復旧性を強化し、生産性を向上させます。

NAC では既存のインフラストラクチャ資産を活用しながら、シスコのネットワークデバイス、Cisco Security Agent ソフトウェア、および協業パートナーのセキュリティソフトウェア (ウィルス対策ソフトやサードパーティ製のエンドポイントセキュリティテクノロジーなど) の価値を向上させます。



Why Cisco?

セキュリティポリシーへの適合性を総合的にすべてのシステムに対して評価するには、ネットワークで実施するのが最良の方法です。

NAC は、セキュリティのインテリジェンスとサービスをネットワーク環境に統合するシスコの構想である自己防衛型ネットワーク (Self-Defending Network) の一部です。