

ネットワーク アドミSSION コントロール

ウイルス、ワーム、スパイウェアといった新型のネットワーク セキュリティへの脅威は絶えずユーザを悩まし、資金、生産性、およびビジネス チャンスを低減させる原因となっています。一方で、モバイル コンピューティングの普及によって、こうした脅威はさらに増大しています。モバイル ユーザは、自宅やホットスポットからインターネットやオフィスに接続できます。その結果、容易に、かつ多くの場合は気付かないうちにマシンにウイルスを取り込み、そのウイルスを企業環境に持ち込んで、ネットワークに感染させる可能性があります。

Network Admission Control (NAC; ネットワーク アドミSSION コントロール) は、ネットワーク リソースにアクセスするすべてのエンドポイント デバイス (PC、ノート型パソコン、サーバ、スマートフォン、PDA など) を、ネットワーク セキュリティへの脅威から適切に保護するために設計されています。NAC が実現する先進的ソリューションは、アンチウイルス、セキュリティ、および管理ソフトウェアの主要メーカーで受け入れられ、マスコミやアナリスト、あらゆる規模の企業から注目されています。

このホワイト ペーパーでは、ポリシーベースのセキュリティ戦略の一部として NAC が果たす、きわめて重要な役割を紹介し、さらに、利用可能な NAC のアプローチについて詳しく説明します。

NAC の利点

CSI/FBI の 2005 年版セキュリティレポートによると、多年にわたりセキュリティ技術の開発が行われ、実装に何百万ドルもの資金が投じられているにもかかわらず、ウイルス、ワーム、スパイウェア、およびその他のマルウェアは、依然として企業が今日直面している主要課題となっています。企業が直面する多数のセキュリティ問題は、ダウンタイム、収益の減少、データの損傷や破損、生産性の低下などを引き起こし、年間を通じて財務面に深刻な影響を与えます。

理由は明白です。従来のセキュリティ ソリューションだけでは、こうした問題に対処することはできません。このような現状の解決策として、シスコシステムズでは、包括的なセキュリティ ソリューションを開発しました。このソリューションは、アンチウイルス、セキュリティ、および管理についての先進的ソリューションとして機能し、ネットワーク環境に配置されたすべてのデバイスをセキュリティ ポリシーに適合させます。NAC によって、ネットワークにアクセスするすべてのデバイスの分析と制御が可能になります。あらゆるエンドポイント デバイスを企業のセキュリティ ポリシーに適合させることで、最新かつ最適のセキュリティ保護を適用し、感染ルートとして一般的なエンドポイントからの感染やネットワークの脆弱化を、企業ネットワークから大幅に削減することができます。

ネットワーク セキュリティの大幅な強化

ほとんどの企業では、ID 管理と Authentication, Authorization, Accounting (AAA; 認証、許可、アカウントリング) を使用してユーザ認証を行い、ネットワーク権限を許可しています。ところが、ユーザのエンドポイント デバイスのセキュリティ プロファイルを認証する手段は事実上ありませんでした。デバイスの「健全性」を正確に評価する手段がなければ、最も信頼性の高いユーザでさえ、感染したデバイスや十分な感染対策を施していないデバイスを使っていれば、無意識のうちにネットワーク上のほかのユーザを重大な危険にさらす可能性があります。

NAC は、シスコシステムズが主導する業界アライアンス構想に基づいて構築された、一連のテクノロジーとソリューションです。NAC は、ネットワークのコンピューティング リソースにアクセスしようとするすべてのデバイスを、ネットワーク インフラストラクチャを利用して強制的にセキュリティ ポリシーに適合させます。これによって、ウイルス、ワーム、スパイウェアといった新型のセキュリティの脅威による損害が軽減されます。NAC を使用すると、セキュリティ ポリシーに適合した信頼できるエンドポイント デバイス (PC、サーバ、PDA など) だけにネットワーク アクセスを許可し、非適合または管理対象外のデバイスについてはアクセスを制限することができます。

NAC の独自性は、ネットワーク インフラストラクチャへの統合が可能な点にあります。では、なぜネットワーク上で、ポリシーの適合性および確認方法が必要なのでしょうか。

1. 企業の利害に関係するデータや重要なデータは、多くの場合、すべてネットワークからアクセス可能です。
2. 企業の利害に関係するデバイスや重要なデバイスは、多くの場合、すべてその同じネットワークに接続されています。
3. アドミッション コントロールをネットワーク上に実装することで、企業は最大数のネットワーク接続デバイスをカバーする、最も広範なセキュリティ ソリューションを導入できます。
4. この方法では、企業が持つ既存のインフラストラクチャ、セキュリティ、および管理設備を利用するため、新たな IT 機器の購入と設置面積の確保が最小限で済みます。

NAC を実装すると、エンドポイント デバイスがネットワーク接続の確立を試みた場合、常にネットワーク アクセス デバイス (LAN、WAN、無線、またはリモート アクセス) によって、自動的にそのエンドポイント デバイスのセキュリティ プロファイルが要求されます。このプロファイルは、インストール済みのクライアント ツールまたは評価ツールによって提供されます。次に、このプロファイル情報はネットワークのセキュリティ ポリシーと比較され、ポリシーに対するデバイスの適合レベルによって、ネットワークがそのアドミッション要求をどのように処理するかが決まります。ネットワークはアクセスの許可または拒否だけを行うこともできますが、別のネットワーク セグメントへとデバイスをリダイレクトして脆弱性を持つ恐れのある部分から切り離し、アクセスを制限することもできます。また、非適合デバイスを修復サーバへとリダイレクトして隔離することも可能です。修復サーバのコンポーネントによってデバイスを更新し、ポリシーの適合性を矯正できることもあります。

NAC では、以下のようなセキュリティ ポリシーの適合チェックを実行できます。

- デバイスが許可されたバージョンの OS (オペレーティング システム) を実行しているかどうかを確認する
- OS に正しいパッチ、または最新のホットフィックスが適用されているかどうかを確認する
- デバイスにアンチウイルス ソフトウェアがインストールされているかどうかと、デバイスが最新のシグニチャ ファイル セットを備えているかどうかを確認する
- アンチウイルス テクノロジーが有効化され、最近実行されたことを確認する
- パーソナルファイアウォール、侵入防御、またはその他のデスクトップ セキュリティ ソフトウェアがインストールされているかどうかと、それらが正しく設定されているかどうかを確認する
- 企業のデバイス イメージが変更または改ざんされていないかどうかを確認する

こうしたセキュリティ プロファイルに関する確認結果に基づき、ネットワーク アドミッションについて、ポリシーベースのインテリジェントな決定が下されます。

NAC ソリューションの導入には、次のような利点があります。

1. すべてのユーザが使用するネットワーク デバイスをセキュリティ ポリシーに適合させることによって、規模や複雑度にかかわらず、あらゆるネットワークのセキュリティ レベルが大幅に向上します。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することによって、企業では事後対応ではなく予防に重点を置いた運用ができます。
2. 主要メーカーによって広く採用および統合されているため、シスコ製品のネットワークや、アンチウイルス、セキュリティ、および管理ソフトウェアへの既存の投資の価値が高まります。
3. アクセス方式 (ルータ、スイッチ、無線、VPN、ダイヤルアップなど) にかかわらず、ネットワークに接続するすべてのデバイスに対して検査および制御手段を提供することによって、企業ネットワークの復元力とスケーラビリティが増大します。
4. 非適合および管理対象外のエンドポイント デバイスが、ネットワークの可用性やユーザの生産性に影響を与えるのを防止します。
5. 非適合、管理対象外、および感染したシステムの特定制と修復に関連する運用コストを削減できます。

NACの実装オプション

NACでは、アプライアンスベースとアーキテクチャベースのフレームワークアプローチが提供されます。シンプルなセキュリティポリシーを必要としているか、または多数のセキュリティベンダー製品を使った複雑なセキュリティ構成のサポートを必要としているかにかかわらず、NACは企業のデスクトップ管理ソリューションと連携し、あらゆる企業の機能面および運用面のニーズを満たします。

Cisco Clean Access (近日発売開始予定)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するNACアプライアンスです。さらに、NACフレームワークにより、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と、50社を超えるメーカーから提供される主要な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とが統合されます。

NACアプライアンス

NACアプライアンス製品はCisco Clean Accessとして提供され、完全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。迅速な導入が可能な「ワンボックスソリューション」テクノロジーによって、ネットワークへのアクセスを求める有線または無線エンドポイントの感染あるいは脆弱性を、自動的に検出、隔離、および駆除できます。

Cisco Clean Accessでは、3つの重要な保護機能を提供します。

- 認証および許可の時点で、ユーザとそのデバイス、およびネットワークにおけるルールを識別します。
- スキャンおよび分析テクノロジー、またはより詳細なステータス評価を行う Lightweight エージェントを利用してエンドポイントのセキュリティステータスを評価し、脆弱性の確認を行います。
- 非適合エンドポイントをブロック、隔離、および修復することにより、ネットワークでセキュリティポリシーを確保します。

Cisco Clean Accessの実装には、次のような利点もあります。

- スケーラビリティ — Cisco Clean Access コンポーネントは、より広範なNACフレームワークアーキテクチャへと統合できるため、Cisco Clean Accessを導入してネットワークアドミッションのニーズに対応できるのと同時に、NACフレームワークを設計および評価できます。
- 迅速な導入 — Cisco Clean Accessはオールインワンのパッケージソリューションで、アンチウイルス、スパイウェア対策、およびMicrosoftアップデートへのサポートが組み込まれています。
- 柔軟性 — Cisco Clean Accessは、複数のデスクトップOSが稼働する異種ネットワークインフラストラクチャをサポートしています。

Cisco Clean Accessは、以下のような特性を持つネットワークに最適です。

- 802.1Xに準拠していないLAN環境
- 無線、ブランチ、リモートのLAN環境、またはシンプルなLAN環境
- 中央集中型のIT環境と管理
- 管理対象外のコンピュータ(ゲスト、委託先、学生など)によるネットワークアクセス
- 異種(マルチベンダー)ネットワークインフラストラクチャ

NACフレームワークソリューション

NACはアーキテクチャベースのフレームワークソリューションとしても利用でき、シスコの既存のネットワークテクノロジーと、他社の実装済みセキュリティおよび管理ソリューションの両方を活用できるように設計されています。

NACフレームワークソリューションには、次のような利点があります。

- すべてのエンドポイントをあらゆるアクセス方式(LAN、無線、リモートアクセス、WANなど)にわたって評価することにより、包括的な制御を実現します。
- エンドポイントの視覚化および制御機能により、管理対象デバイス、管理対象外デバイス、ゲスト、および不正デバイスを、企業のセキュリティポリシーに適合させます。

- エンドポイント制御のライフサイクル サポートで、エンドポイントの評価、認証、許可、および修復を自動化します。
- ポリシーの集中管理、インテリジェント ネットワーク デバイス、およびネットワーク サービスを、多数の主要ベンダーから提供されるアンチウイルス、セキュリティ、および管理ソリューションと組み合わせることにより、精細なアドミッション コントロール管理を実現します。
- 柔軟性を持つ標準規格の API を通じ、豊富なパートナー体制とテクノロジーをサポートしているため、ソリューション全体でさまざまなサードパーティ製品を活用できます。

NAC フレームワークの導入は、以下のような特性を持つネットワークに最適です。

- 中～大規模クラスのネットワーク環境での導入
- 広範囲にわたる LAN、WAN、または無線環境
- すべてまたは大部分がシスコのテクノロジーに基づいた LAN、WAN、または無線インフラストラクチャ
- NAC パートナーのセキュリティおよび管理ソリューションと相互運用
- IP テレフォニーを実装済み、または実装を予定
- 802.1X を実装済み、または実装を予定

投資の保護

シスコは、あらゆる企業の機能要件を満たす、最も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のセットを提供します。多くの企業ではニーズが変化するため、導入済みの Cisco Clean Access 製品コンポーネントは、将来的に NAC フレームワークの実装をサポートするために利用できます。

ユーザが自身の環境に合わせて採用するアプローチの種類にかかわらず、Cisco NAC テクノロジーは、対応するネットワーク テクノロジーへの投資を保護するように設計されています。同時に、相互運用性と機能互換性を備えているため、Cisco Clean Access から、より多くの利点と機能を持つ NAC フレームワーク テクノロジーへと円滑に移行できます。

NAC テクノロジー

NAC アプライアンス コンポーネント

Cisco Clean Access は、次の要素から構成されています。

- **Cisco Clean Access Server** は、デバイス評価機能を提供し、エンドポイントの適合性に基づいてアクセス権限を付与します。
- **Cisco Clean Access Manager** は、ポリシーの適用や修復サービスなど、Cisco Clean Access ソリューションの集中管理機能を提供します。
- **Cisco Clean Access Agent** はオプションの無償クライアントで、管理対象環境と管理対象外環境の両方で、より厳格なエンドポイントのポリシー適合性評価と効率的な修復機能を提供します。

Cisco Clean Access は、以下のテクノロジーを利用した無線アクセスでサポートされています。

- すべての 802.11 Wi-Fi アクセス ポイント (Cisco Aironet アクセス ポイントなど)
- NAC 対応の IEEE 802.1X サブリカントを備えた任意の Wi-Fi クライアント デバイス

NAC フレームワーク コンポーネント

NAC フレームワークは、以下のテクノロジーをサポートします。

- キャンパス内の LAN、WAN、VPN、および無線アクセス ポイントに対応した、幅広いネットワーク デバイスをサポート
- 無人デバイス、「エージェントレス」のデバイス、その他の非応答型デバイス向けに、サードパーティ製のホスト評価ツールとの互換性を提供し、各デバイスに異なるポリシーを適用することが可能
- Cisco Trust Agent に対応した幅広いプラットフォームをサポート
- アンチウイルス ソフトウェアや基本的な OS パッチをはるかに超えるアプリケーションと OS のステータスチェックによって、マルチベンダー構成の統合を強化

NAC フレームワークは、以下のテクノロジーでサポートされています。

- **Cisco ルータ** : Cisco 871、Cisco 1812J、Cisco ISR (Integrated Services Router) 18xx、28xx、38xx シリーズ。Cisco 1712、1721、1751、1751-V、1760 モジュラ アクセス ルータ。Cisco 2600XM、2691、3640、3660-ENT マルチサービス アクセス ルータ。Cisco 72xx シリーズ ルータ
- **Cisco Catalyst スイッチ** :
 - Cisco Catalyst OS、Cisco IOS® ソフトウェア、またはハイブリッド アプリケーションを搭載した Cisco Catalyst 6500 シリーズ Supervisor Engine 2、32、および 720 (Cisco IOS ソフトウェアは Supervisor Engine 32 および 720 でサポート)
 - Cisco IOS ソフトウェア搭載の Cisco Catalyst 4000 シリーズ Supervisor Engine II+、IV、および V-10GE
 - Cisco Catalyst 4948 および 4948-10GE
 - Cisco IOS の IP ベースおよび IP サービス搭載の Cisco Catalyst 3550、3560、3750
 - Cisco Catalyst 2940、2950、2955、2960、および 2970
- **シスコ無線アクセス** : Cisco Aironet アクセス ポイント、Cisco Wireless LAN Controller に接続された Cisco Aironet Lightweight アクセス ポイント、Cisco Catalyst 6500 シリーズ Wireless LAN Services Module (WLSM)、NAC 対応の IEEE 802.1X サブリカントを備えたすべての Cisco Aironet、シスコ互換アクセスポイント、および Wi-Fi クライアント デバイス
- **Cisco VPN 3000 シリーズ コンセントレータ**
- **Cisco Trust Agent**
- **Cisco Secure Access Control Server (ACS)**
- サードパーティ ベンダー製のソフトウェア
- **推奨されるコンポーネント** :
 - Cisco Security Agent
 - Cisco Security Monitoring, Analysis and Response System (MARS)

©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