Self-Defending Networks
――ネットワークに、自己防衛する力を――

Cisco Network Admission Control（NAC）

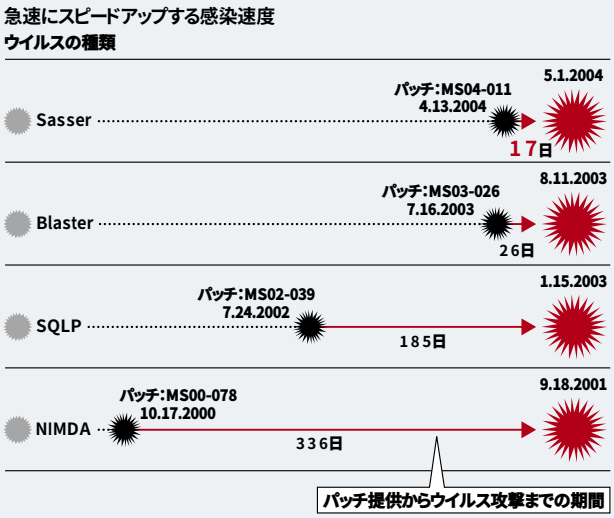
アンチウイルスソリューションと連携し インテリジェントなネットワークアクセス制御を実現

ネットワークに、自己防衛する力を

ネットワーク アドミッション コントロール（NAC）ソリューションは、ネットワークの多段的な防衛手段を提供するセキュリティソリューションです。NACソリューションによって、さまざまなセキュリティの脅威に対する予防・対応能力を持ち、免疫システムを備えたネットワークを実現します。

ネットワークにおける利便性と脆弱性のジレンマ

今日のネットワークは、ブロードバンドによる常時接続があたりまえになり、アクセス手段の多様化やモビリティの普及も急速に進んでいます。これにより、いつでも、どこでも、企業ネットワークを活用できるようになった反面、セキュリティに対する脅威も急速に拡大しているのが現状です。下図に示すとおり、2001年に大きな被害をもたらしたNIMDAの場合は、Windowsの脆弱性の公開とパッチの提供からウイルス攻撃までの経過日数が336日であったのが、2002年のSQLPでは185日、2003年のBlasterでは26日、そして、2004年のSasserでは17日と、その感染スピードはますます高速化しています。その感染経路は情報処理振興事業協会（IPA）の調べでは、実に25%が社外から、あるいはいったん社外に持ち出したPC経由であると報告されています。

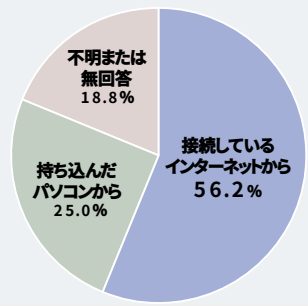


脅威のダメージを最小化するNACソリューション

このように、年々複雑化・悪質化が進むネットワークの脅威から企業情報システムを保護するには、従来のようにPC端末などのエンドポイントやファイアウォールなどインターネットの境界線であるエッジといった局所的なセキュリティ対策だけでは不十分です。あらゆるアクセス方法、さまざまな端末、利用環境に応じて、適切な対策を統合的に施さなくては企業情報システムを守ることはできません。さらに重要なことは未然の対策を講じるだけではなく、万一ウイルス感染してしまったときに、二次感染を確実に防ぎ、最小限の作業で一刻も早くシステムを復旧してビジネスを再開させる体制を整備しておくことです。

こうした課題を解決するため、シスコは、マカフィー、シマンテック、トレンドマイクロの大手アンチウイルスベンダー各社と協業し、NAC（Network Admission Control）ソリューションの提供を開始しました。NACソリューションは、ネットワークにアクセスするあらゆる端末に対して、その状態に最も適切なネットワーク上のリソースへのアクセスポリシーを適用し、セキュリティポリシーの基準を満たさない端末でも、そのポリシーに応じて、許可・隔離・検疫・拒否などのアクセス制御を行う統合的なソリューションです。これにより、端末情報をもとにネットワーク全体にセキュリティポリシーが適用できるため、ネットワークのセキュリティ強度は大幅に向上します。また、OS、アンチウイルスソフトのバージョン、パッチ管理情報などのコスト面や運用面でも大幅な効果があります。

システム管理者が想定する
Blaster感染経路



『W32/MSBlaster及びW32/Welchiウイルス被害に関する企業アンケート調査の結果について』
http://www.ipa.go.jp/about/press/20030918.html
平成15年9月18日　情報処理振興事業協会（IPA）

Blaster感染システム数

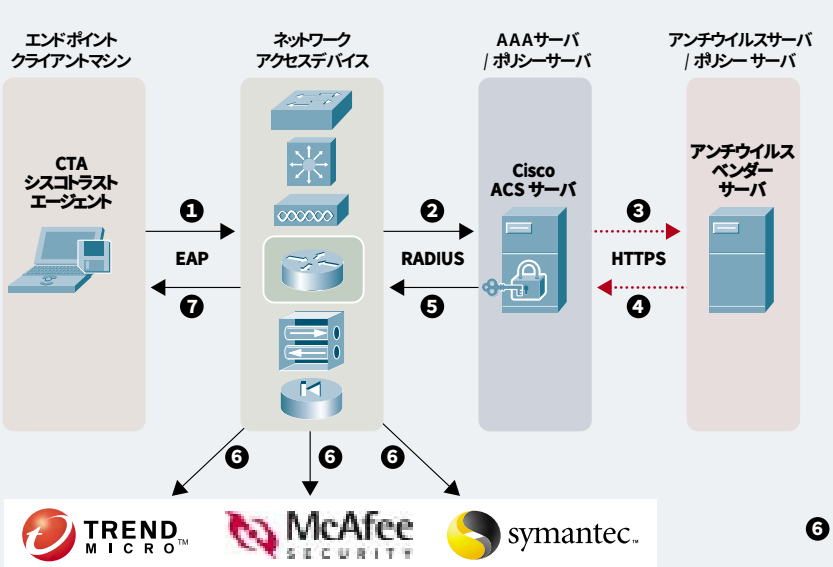
・最初の3時間で約12万8,000システムが感染
・残存するワームには、継続的な対策が必要
・被害は感染後、2週間に及ぶ

NACソリューションの概要

「不正」なアクセス対策から、「不適切」なアクセスへの未然防止へ

NACは、ネットワークにアクセスするあらゆる端末に対して、その状態に最も適切なポリシーを適用し、セキュリティポリシーの基準を満たさない端末に対しては、ポリシーに応じて許可・隔離・検疫・拒否などのアクセス制御を行います。

端末のセキュリティコンプライアンス情報をもとにインテリジェントなアクセス制御をネットワークで実行



❶ デバイスへアクセスするために端末がEAP認証（UDP or 802.1X）※1でクレデンシャル（状態情報）を送信

※1 EAP認証802.1Xは将来予定

❷ アクセスデバイスがクレデンシャルを RADIUS認証でポリシーサーバ（ACSサーバ）へ転送

❸ ACSサーバがアンチウイルス情報を アンチウイルスベンダーサーバへ照会

❹ アンチウイルスベンダーサーバが 照会結果を応答

❺ 照会結果にもとづきポリシーサーバがNAD（ネットワーク アクセス デバイス）へ適切なアクセス情報を応答

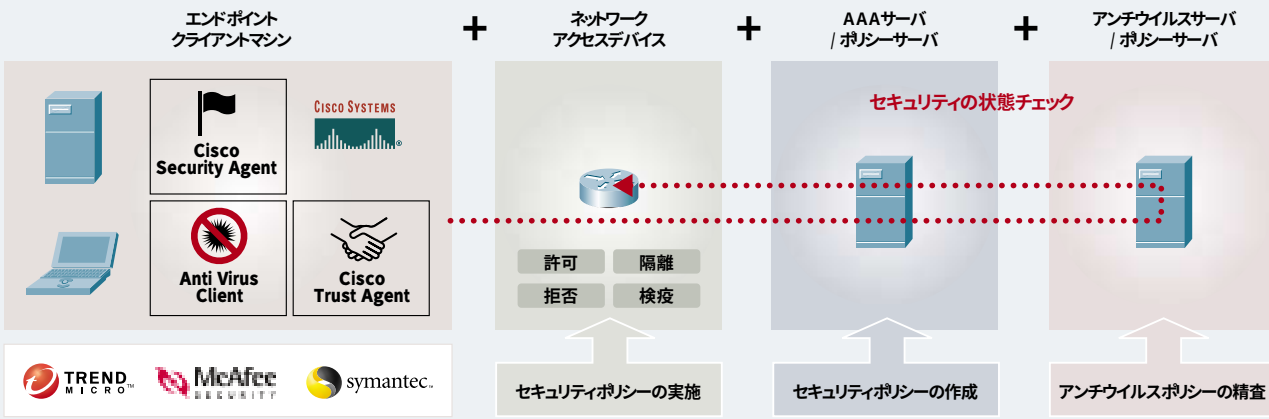
❻ ❼ NADがアクセスを制御、 ポリシーの適用&クライアントへ通知（許可・隔離・検疫・拒否）

NACソリューション対応 ルータ&認証ポリシーサーバ

NACのシステムアーキテクチャ

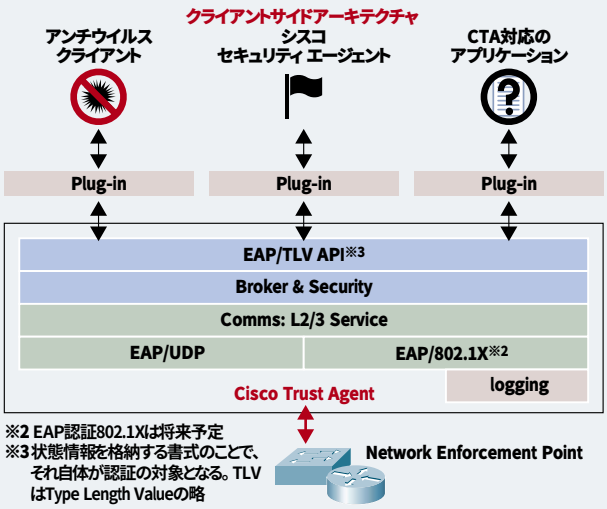
エンドポイントとネットワークのインテリジェントな協調

NACジョイントソリューション



●CTA（Cisco Trust Agent）

NACの核となるのは、CTA（シスコ トラスト エージェント）というエージェントソフトです。CTAは、各社が提供するセキュリティソフトウェア製品と、CSA（シスコ セキュリティ エージェント）製品に搭載され、各種ネットワーク機器とセキュリティソフトウェア間の情報交換を可能にします。



※2 EAP認証802.1Xは将来予定
※3 状態情報を格納する書式のことで、それ自体が認証の対象となる。TLVはType Length Valueの略

●ネットワーク機器（Network Access Device）

シスコのルータ、スイッチ、ワイヤレスアクセスポイント、ファイアウォール、IDS、VPNなど、シスコデバイスに対してサポートを予定しています（現段階では、シスコのルータ製品にて対応）。これらのシスコデバイスで製品であれば、シスコIOSや各種OSなどのファームウェアのアップデートによって迅速にNACソリューション対応が可能となります。

●アンチウイルスサーバ／ポリシーサーバ

最新パターンファイルの配信など企業全体のアンチウイルスソフトを管理・制御するサーバです。通常アンチウイルスベンダー製品群にインテグレートされます。ポリシーサーバはAAAサーバと連携することで、よりきめ細かいセキュリティポリシーの判定を実現します。

●CSA（Cisco Security Agent）

CSAは、悪意のある行為・ふるまいを検知し、潜在的なあらゆる種類の既知および未知（Day-Zero）の攻撃から企業ネットワークアプリケーションを守ります。

	CSA	AV	FW/IPS
既知のウイルス / ワームの感染防止	●	●	
未知のウイルス / ワームの感染防止	●		
ウイルス感染済みファイルのスキャン / 検出 / クリーンアップ		●	
ウイルス / ワームの認識		●	
Day-Zeroアタック / 未知のBuffer Over-flowアタック	●		
ネットワーク攻撃の防御（DoS、DDoS、ポートスキャンほか）	●		●
ネットワークリクエスト受信 / 送信のコントロール	●		●
大容量スマートメディアの書き込み/読み込み/実行コントロール	●		
任意P2Pアプリケーションのインストール / 実行	●		
任意レジストリ / 重要ファイルの改ざん検出	●		

●アンチウイルス（AV）ソフト

クライアントマシンにインストールされた、マカフィー、シマンテック、トレンドマイクロが提供するNAC対応のアンチウイルスソフトが、CTAとの連携によりウイルスを検知・駆除します。

これらのソフトウェアをエンドポイントのクライアントマシンに組み込むことにより、あらゆるネットワークアクセスに対してシームレスなオペレーションを実施し、すべてのエンドポイントに対してポリシー適用が可能となります。

●AAAサーバ／ポリシーサーバ

アクセスしてきた端末が基準に合っているか、ユーザのIDは間違っていないか、ネットワーク アクセス デバイス経由で送られる「クレデンシャル」（状態情報）の評価にもとづき設定されたセキュリティポリシーとの整合性を判断。その判断結果にもとづき各ネットワーク アクセス デバイスに適当なアクセスポリシー（許可、不許可、制限付き許可、隔離）を適用します。

アンチウイルスソリューション

世界をリードするアンチウイルスベンダーとのコラボレーション

symantec.

●シマンテック

Symantec™ Client Security 2.0

アンチウイルス、クライアントファイアウォール、侵入検知を統合した、クライアントのための統合的なセキュリティ

Symantec Client Securityは、アンチウイルスにクライアントファイアウォールと侵入検知システムを統合し、クライアントPCを1台1台個別に保護します。ウイルススキャンに加え、各PCごとに通信の監視と制御を行うため、ネットワーク経由で感染するウイルスやワーム、企業内部からのハッキング、DDoS攻撃などへの対策やモバイルPCのセキュリティ、情報漏えい、アクセス管理など、さまざまなセキュリティ課題に対処することができます。また、個々のPC上で動作しているアンチウイルス、クライアントファイアウォール、侵入検知システムのコントロールとログの監視、ウイルス定義ファイル、ファイアウォールのルール、侵入検知のためのシグネチャーのアップデートなどを、ひとつのコンソールから一元的に行うことが可能です。

TREND MICRO™

●トレンドマイクロ

TREND MICRO
ウイルスバスター
コーポレートエディション

企業向けウイルス対策製品として、数多くの実績を誇るウイルスバスター コーポレートエディションが、NACに完全対応

NACに完全対応した新しいウイルスバスター コーポレートエディションは、従来のウイルス対策機能に加え、シスコのネットワーク製品と連携、パターンファイルや検索エンジンの状態をチェックし、自社のセキュリティポリシーに準拠しないクライアントのアクセスを規制します。規制されたクライアントは、自動的に検疫サイトに誘導され、ポリシーに準拠した状態に更新後、再度アクセスを試みるため、管理者、利用者双方にとって容易な運用が可能です。ウイルスバスター コーポレートエディションには、Cisco Trust Agentと、トレンドマイクロのポリシーサーバが同梱されており、高いコストパフォーマンスをご提供いたします。

McAfee SECURITY

●マカフィー

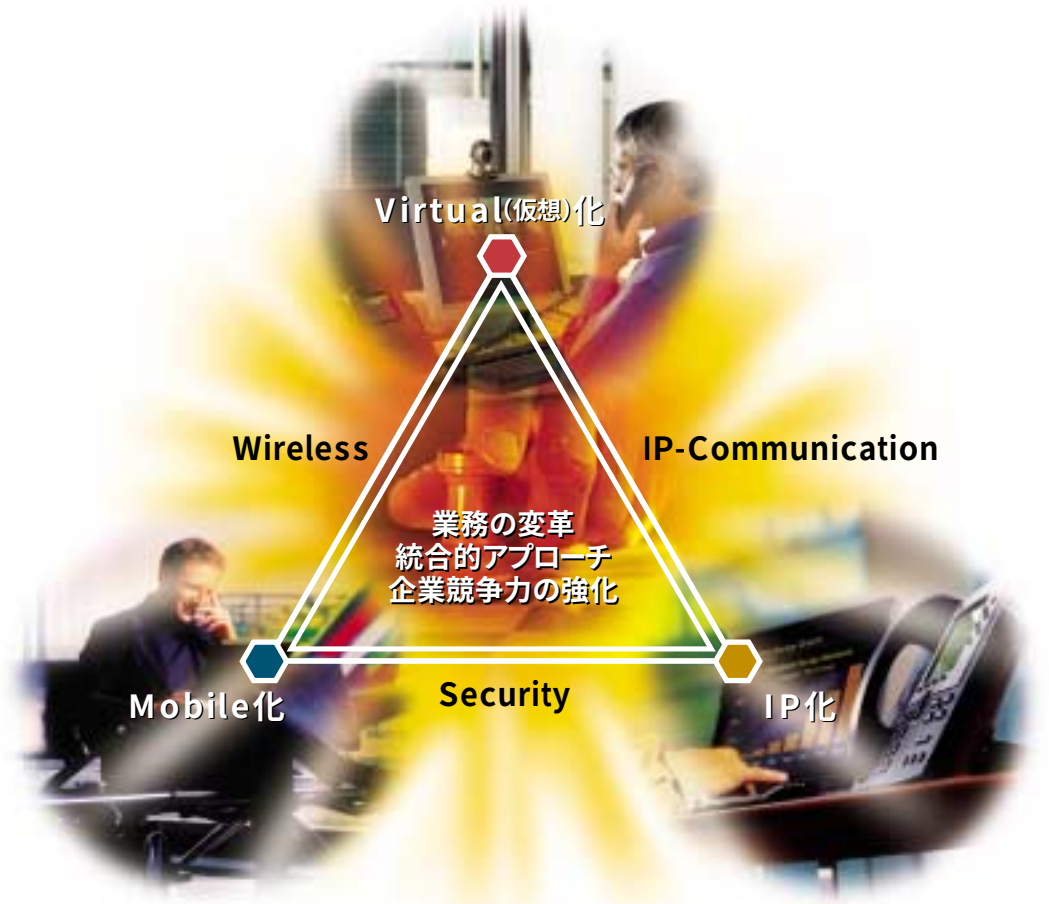
VirusScan Enterprise 8.0i

企業内コンプライアンスを確実に確保、AV/IPS/FW統合クライアントソリューション

Cisco NACを標準サポートしたVirusScan Enterpriseにより、企業内PCのコンプライアンスを容易に確保することができます。CTAがVirusScan Enterpriseのステータス情報を自動収集し、ノンコンプライアンスなマシンを隔離、最新の状態に再設定します。またVirusScan Enterpriseでは、ウイルス対策のほかに、IPS機能、FW機能、アンチスパイウェア機能が標準でサポートされているので、幅広いセキュリティ脅威にさらされる企業PCのセキュリティをより確実に確保することが可能です。

NACソリューションがもたらす価値

システムレベルの包括的なアプローチでセキュリティの全体最適を実現



自己防衛型ネットワークソリューションの効果

質の高いサービスレベルを実現

- リアクティブ対策からプロアクティブ対策への移行
- 接続方式に左右されない一貫したアクセスポリシーの適用
- フレキシブルなポリシー適用（許可・隔離・検疫・拒否）
- 多種多様なアプリケーションサービスのサポート

投資の保護とTCOの削減

- 管理コストと工数を削減しつつ、耐障害性を大幅に向上
- 既存ネットワークインフラ、アンチウイルスインフラをそのまま活用可能
- ソフトウェアのアップデートのみでハードウェア機器の増設が不要
- 業界アライアンスによる相互運用性を実現

©2004 Cisco Systems,Inc. All rights reserved.
Cisco、Cisco Systems、Cisco Powered Networkロゴ、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。
その他、記載されている会社名、製品名は各社の商標、登録商標または登録サービスマークです。
この資料の記載内容は2004年6月現在のものです。
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。

CISCO SYSTEMS

シスコシステムズ株式会社
URL：http://www.cisco.com/jp/
問い合せURL：http://www.cisco.com/jp/service/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
電話でのお問い合せは、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

0492-0406-20A-F