Cisco Network Admission Control（NAC）

情報セキュリティガバナンスをネットワーク基盤で確立する、シスコ自己防衛型ネットワーク

2005年10月版

健全なネットワークインフラを目指して

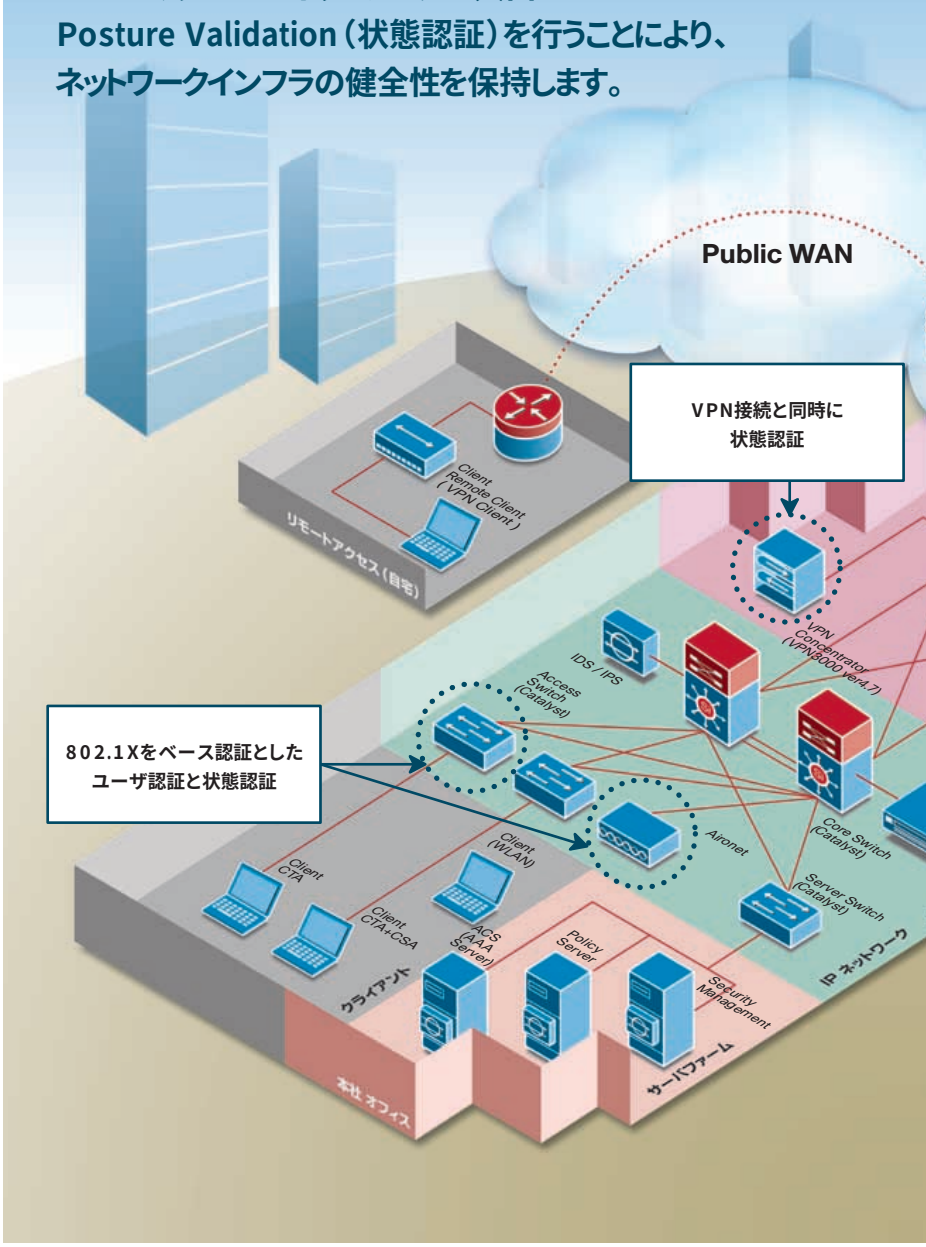
感染経路の多様化、被害の甚大化が進むセキュリティの脅威

今日の企業は自社の情報システムを守るため、ファイアウォールやウイルス対策ソフトなどを導入し、積極的にセキュリティ対策に取り組んでいます。しかし、その努力も空しく、ウイルスやワームなどによる被害は一向に減少しないどころか、むしろ感染速度の加速や被害の甚大化といった状況の悪化を招いています。その原因は、企業の情報ネットワークが社内だけで閉じず、自宅からのリモートVPNやモバイル端末、ワイヤレスLANなどにネットワークが拡張されていることが大きな要因であり、いわば利便性に伴ったセキュリティ対応への難しさが、この要因を生んでいるのだと考えられます。どれだけ堅牢なセキュリティ環境を構築しても、自宅PCを含むすべての端末にセキュリティポリシーを徹底することは不可能です。つまり、これはエンドポイントやエッジでのセキュリティ対策、従前の検疫ネットワークの限界を示唆するものであり、セキュリティ対策はネットワーク全体で考えなければ効力を発揮できないという現実を提示するものといえます。

情報セキュリティガバナンス基盤を確立するNAC（Network Admission Control）

シスコでは、複雑化と多様化が進むセキュリティの脅威に対する抜本的な対策として、NACという包括的なセキュリティ基盤の仕組みを提供しています。NACは、ネットワークに接続されるすべての端末に対し、リアルタイムでセキュリティポリシーとの精査を行い、基準を満たさない端末を隔離、あるいは免疫作業を実行することで、全社のネットワークおよび情報システムを健全な状態に保ちます。NACを導入することで、企業は全社規模の情報セキュリティガバナンスをインフラストラクチャレベルで構築可能となり、感染リスクや被害の拡大を未然に防止・縮小することができます。

NACは、すべてのネットワークの入口で Posture Validation（状態認証）を行うことにより、ネットワークインフラの健全性を保持します。



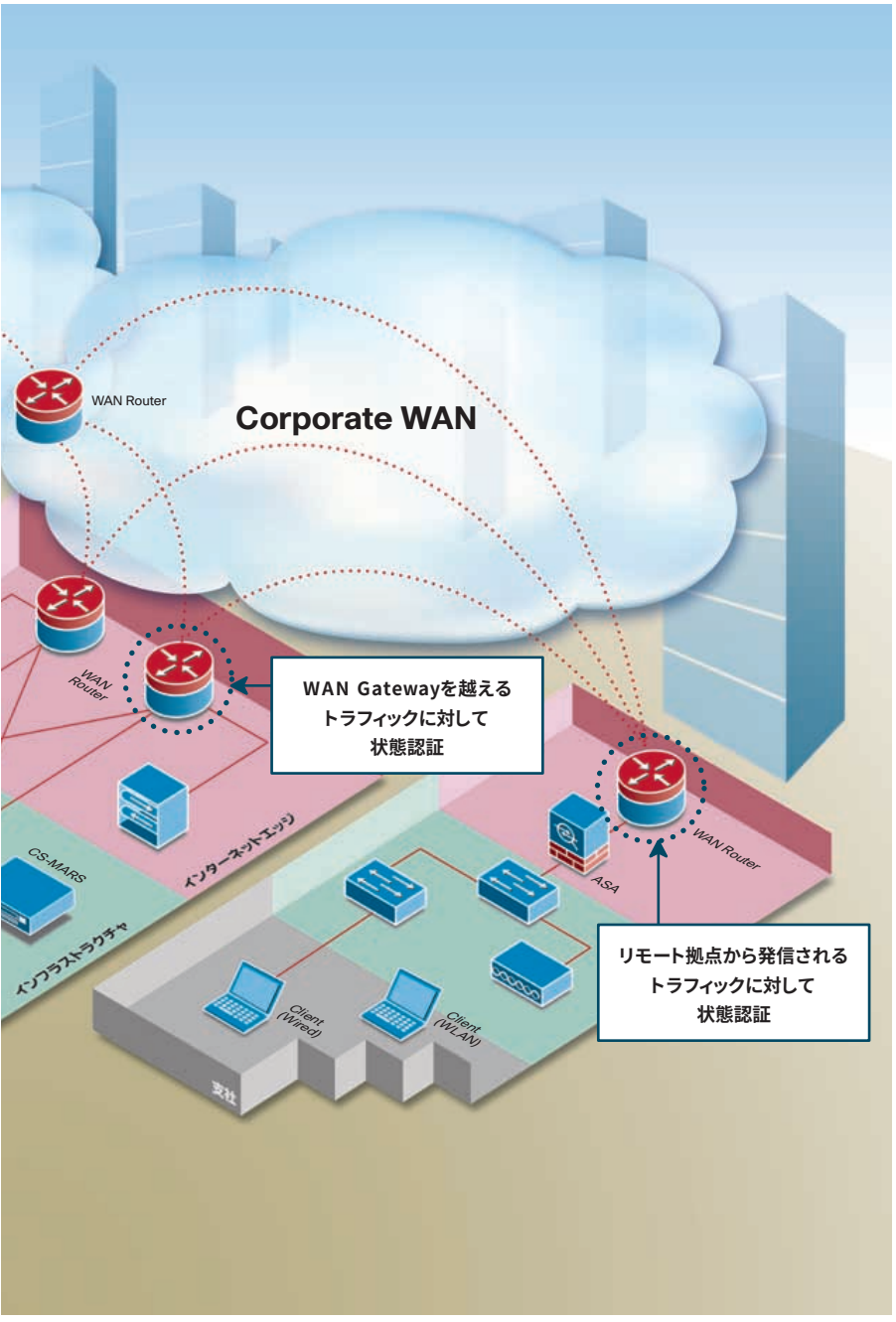
Cisco ISR
サービス統合型ルータ
シリーズ

Cisco Catalyst
LANスイッチ
シリーズ

Cisco Aironet
1100 / 1200 と
シリーズ

Ciscoと
Secure ACS
シリーズ

Cisco
VPN 3000
シリーズ



リモートVPN接続時の状態認証

通常、自宅などからリモートVPN接続を行う際に、ユーザ認証によるチェックが行われますが、ユーザの特定だけでは感染リスクを避けることはできません。NACでは、ネットワークに接続された端末のOSレベルやパッチ状況までを精査することで、本社システムへの感染を防ぎ、安全な接続環境を提供します。

IEEE802.1Xベース認証時の状態認証

ユーザ認証および端末認証によって不正アクセスを防止する802.1Xを利用する企業が増えていますが、これだけでは不正状態（ウイルス感染、スパイウェア常駐など）の端末からのアクセスを防御することはできません。NACを利用すれば、エンドポイントにまで踏み込んだセキュリティ対策を実現することが可能です。

WAN Gatewayを越えるトラフィックへの状態認証

企業活動における重要なリソースが集中するセンター拠点の汚染は、絶対に防止しなければいけないセキュリティの最重要事項です。ファイアウォールなどエッジでの対策だけでは不正アクセスやDOS攻撃は防げても、も、新種ウイルスやアプリケーションに埋め込まれたワームなどの検知は不可能です。NACでは、WAN Gatewayによるトラフィック監視を行うことで、外部からの脅威を水際で防止することができます。

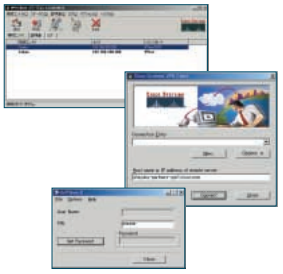
支店・営業所等リモート拠点からのアクセス時の状態認証

本社のセキュリティ環境は万全でも、支店や営業所、出張所の対策は不完全という企業は少なくありません。NACを導入すれば、距離を超えたネットワーク機器間で自動的にセキュリティポリシーを連動させられるため、セキュリティ担当者の手を煩わせることなく、全社レベルでセキュリティポリシーの徹底を図ることができます。

Cisco セキュリティ
アプライアンス
Cisco ASA 5500

Ciscoł
IDS / IPS 4200
シリーズ

CSA
（Cisco
Security Agent）



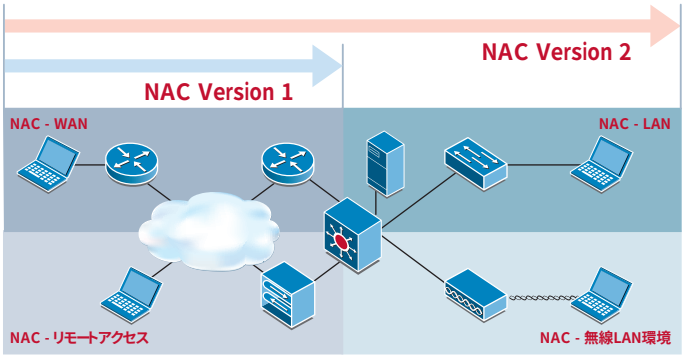
VPN クライアント
ソフトウェア

Cisco
Secure MARS
シリーズ

Network Admission Control（NAC）

NAC（Version 2）とは

NACとはネットワークに接続され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を導入したネットワークでは、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、資産管理的な要素をはじめ、NACに対応したアプリケーションの状態の監視、精査を可能とします。
ポリシーに準拠した端末へのネットワークアクセス確保、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の向上を図ります。
2004年6月にVersion 1がスタートしたNACは、現在、適用範囲をLAN環境のポートアクセスおよび無線LANにまで拡張し、あらゆる接続方法への包括的なアクセスコントロールを可能にしたVersion 2の提供がはじまっています。



あらゆる接続方法への包括的なアクセスコントロール環境

WAN	- キャンパス間、エクストラネット、ノンプロダクションセグメント、学部間ネット
リモートアクセス	- クライアント端末からの一時的なアクセス、永続的なアクセス環境
LAN	- スイッチング環境下におけるポートアクセス接続
無線LAN環境	- キャンパス内におけるモバイルアクセス

全体的な運用、部分的な運用、管理配下にない端末へのセキュリティポリシーの適用

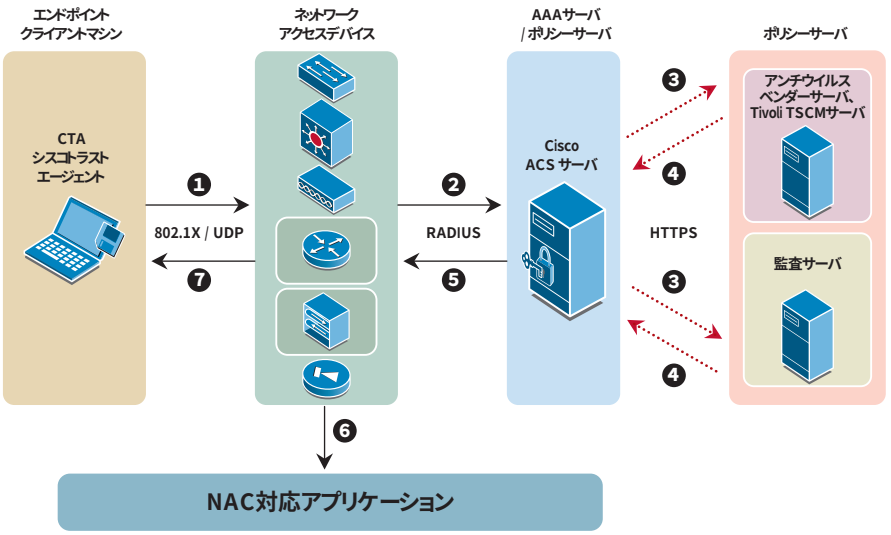
- 策定されたセキュリティポリシーに基づき、CTAのインバウンドアセスメントを適用
- “ 非エージェント ”クライアント端末のためのアウトバウンド監査

非コンプライアント端末の隔離、ポリシーに基づいた修復、回復プロセスの提供

- L2 VLANs、L3 ACLs やユーザポリシー等をベースにした隔離方法
- ベンダーサーバによるサービス統合に基づいた修復、回復方法の適用

NACの仕組み

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

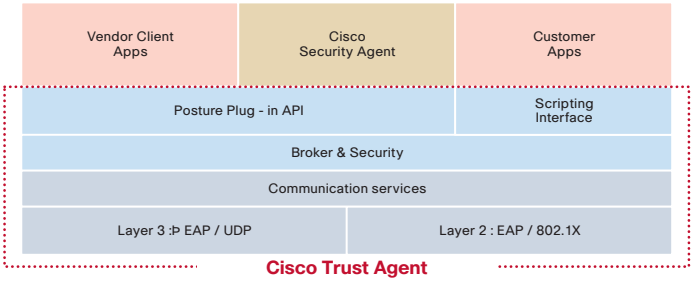


1. ネットワークへ接続しようとする端末は暗号化された状態情報（EAP認証）を送信（UDPや802.1X技術を採用）
2. NAD（ネットワークアクセスデバイス）が状態情報をRADIUS認証でポリシーサーバ（ACSサーバ）へ転送
3. ACSサーバが各種ポリシー情報をベンダーポリシーサーバへ照会
4. ベンダーポリシーサーバが照会結果を応答
5. 照会結果に基づきACSサーバがNADへ適切なアクセス情報を応答
6. 7. NADがアクセスを制御、ポリシーの適用&クライアントへ通知（許可・隔離・検疫・拒否）

NACの構成要素

● CTA（Cisco Trust Agent）2.0Ł

NACの核となるエージェントソフトであるCTAは、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実現します。バージョン2.0では、Windows 2000、XP、2003、Red Hat Linuxへの対応と、OSのセキュリティパッチ、Hotfix情報の自動収集機能が追加されました。



・サポートOS：
Windows 2000、XP、2003、Red Hat Linux

・2 transport layers のサポート
EAPoUDP - layer 3
EAPo802.1X - layer 2（Windows only）

・802.1X supplicant 機能のサポート
有線認証のみサポート

・OSのセキュリティパッチ、Hotfix情報（incl. Service Pack）を収集可能
（CTA1.xではCSAにてサポート）

・Customer Scripting Interfaceをサポート

・NACパートナーがCTA1.0用に提供している Plug-¼互換性を持つ

・Diagnosticやデバッグ情報機能を強化

● 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を守ります。
※最新バージョン4.5ではCTA v1.0をバンドル

● ネットワーク機器（Network Access Device）

ルータ、スイッチ、ワイヤレスアクセスポイント、VPNなどのシスコ製品がNACに対応しています。シスコIOSのアップデートでNACソリューションに対応可能なため、既存の投資を保護したままでセキュリティレベルを向上できます。（ファイアウォール、IDSは将来対応予定）

● ACSサーバ / ポリシーサーバ

アクセスしてきた端末が基準を満たしているか、ユーザ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）に基づき、設定されたセキュリティポリシーとの整合性を判断します。例えば「Healthy（健全）」であれば制限なしのアクセスを適用、「Quarantine（隔離）」であれば隔離ネットワークを適用、「Infected（未保護）」であれば、厳しく制限されたネットワークのみを適用可能とします。

● NACパートナーポリシーサーバ

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。

● 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。

NACの導入効果

新たな付加価値の創造

- 「だれ?」が「何を持っている?」かのプロアクティブアプローチ
- 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
- ポリシー適用のフレキシビリティ（拒否、許可、制限、隔離、検疫）
- バラエティに富んだアプリケーションサポート
- ユーザ透過型サービスの提供

ROIの向上とTCO削減を両立

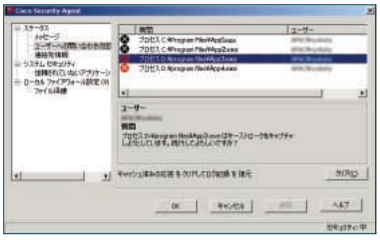
- すべてのクライアントに最新のセキュリティポリシーを適用することで、全社規模のセキュリティレベルを低コストで大幅に向上
- ネットワークの耐障害性を向上させ、生産性を拡大
- 既存のシスコネットワーク製品への投資を保護し、ROIを向上
- 既存のアンチウイルス製品への投資を保護し、ROIを向上

NACとともにネットワークを守る製品群

NACソリューションの最大のメリットは、ネットワークインフラストラクチャとホストのセキュリティ技術を連携させることで、これまでの投資を無駄にすることなく活用できるという点にあります。ネットワークを構成するシスコのルータ、スイッチ、ワイヤレス機器、セキュリティ機器などが、確実にウイルス対策ソフトウェアを使用するようユーザに強制することが可能になります。

Cisco Security Agent（CSA）シリーズ

企業ネットワークをセキュリティの脅威から防御する、エンドポイントセキュリティソフトウェア。シグネチャに依存するセキュリティソフトウェアが既知の攻撃にしか対応できないのに対して、コンピュータの振る舞いを解析するCSAは、未知の攻撃についてもリスクを軽減することができます。バージョン4.5によるサービス強化により、アンチスパイウェア / マルウェアの防御が向上、ロケーションベースのポリシー強制、NACへの準拠ならびに日本語環境対応を図りました。



Cisco Security Agent 4.5 の新機能

- スパイウェア / マルウェア対策
- 情報漏えい対策
- Cisco NACの統合
- 日本語を含む多言語対応

Cisco侵入検知・侵入防御システム（IDS / IPS）

アプリケーション監視および制御機能、ポート80タイプの制御や誤用認知、ならびにVoIP環境への対応などのアプリケーションセキュリティの強化を図りました。従来からのリアルタイムの侵入防止機能に加えて、ワームやウイルス、スパイウェア / マルウェア、ならびにP2Pやインスタントメッセージング（IM）の利用に伴う脅威などに対して、既存のトラフィックに影響を与えることなく発見および抑止するインラインでの正確性が向上されました。

Cisco IDS / IPS 4200 シリーズ

- レイヤ2～7のトラフィックを詳細に検査することで、ポリシー違反、脆弱性の悪用、および異常な動作からネットワークを保護し、多種多様な脅威を防護

Cisco ASA 5500 シリーズ

適応型防御システムセキュリティ（Adaptive Threat Defense）と“ Clean VPN ”サービスを統合したASA 5500 シリーズは、新たなセキュリティ脅威に対応した最新のテクノロジーを搭載すると同時に、導入の容易さと低運用コストを可能にします。シスコ AIM(*)アーキテクチャに基づく優れた拡張性とポリシー制御を、アプリケーションセキュリティ、ワーム / ウイルス被害の軽減、悪意のあるソフトウェアからの防御、安全なVPN接続といったユニファイドセキュリティサービスとともに提供します。

Cisco ASA 5500 シリーズ

* AIM（Adaptive Identification and Mitigation）：環境に適合した認識および被害の軽減

Cisco Secure MARS シリーズ

多様化および巧妙化が進むネットワーク攻撃に対して、攻撃防御、監視、対応のための高速かつスケーラブルなアプリケーションを提供するCisco Security Monitoring, Analysis and Response System（CS-MARS）は、複数デバイスの関連するログを集約して表示し、その組み合わせから発生事象を推定することができます。

Cisco Secure MARS シリーズ

各デバイスの設定内容を認識してネットワーク構成を把握し、トポロジーマップ生成してトラフィックフロー表示したり、さまざまなイベントの相関分析、ベクター分析、異常検出、ホットスポット識別、被害の拡散防止の自動化機能を含む製品で、ネットワーク攻撃を正確に識別、管理、排除することを支援します。

Cisco ISRサービス統合型ルータ

包括的なセキュリティサービスと音声サービスをルーティングシステムに組み込んだサービス統合型ルータです。複数サービスを1台のシステムで提供するアプローチにより、システムの迅速な導入と運用コストの削減というメリットを生み出します。拡張性に優れ、業界最高クラスの性能と信頼性、柔軟性を実現しています。

Cisco VPN 3000 シリーズ

刷新されたVPN機能の提供により、統合化されたエンドポイントセキュリティの実現が行われました。接続前に接続する装置のセキュリティ「状態（Posture）評価」、機密データの保護、接続後のクリーンアップによるセッション情報の痕跡消去を提供するSSL-VPNサービスによる新しいアプリケーション最適化機能に加えて、IPSecトラフィックにもNAC機能が対応したことで、リモートアクセス環境下での、端末状態の妥当性の評価（Posture Validation）が強化されます。

Cisco ワイヤレス & IPコミュニケーション

信頼性の高いセキュアな無線LAN環境により、場所にしばられない効率的なワーキングスタイルを実現します。また、これまで別々に存在していた電話やFAX、Eメールなどのコミュニケーション手段がIPに統合されることで、先進的な「ビジネスコミュニケーション」を実現します。

Cisco Secure ACS シリーズ

シスコ自己防衛型ネットワークを実現するための中核となり、ユーザ認証、アクセス制御、ポリシー制御によってアクセスセキュリティを制御するサーバです。中央集中型のアイデンティティネットワークを実現してネットワーク全体に統一したポリシーを実行できます。

Cisco Catalyst 2900 シリーズ

Catalyst 2900 シリーズは、従来のLANスイッチングの簡素さを維持しつつ、高度なQoS、レート制限、セキュリティフィルタ、マルチキャスト管理などのインテリジェントサービスを、ネットワークエッジに低価格で提供する製品ラインです。NAC機能の対応により、強固なL2レベルでのセキュリティを実現します。


Cisco Catalyst 2940 シリーズ


Cisco Catalyst 2950 シリーズ


Cisco Catalyst 2970 シリーズ

Cisco ISR 2800 シリーズ　Cisco ISR 3800 シリーズ


Cisco ISR 1800 シリーズ

Cisco Catalyst 3000 シリーズ

Cisco Catalyst 3500 シリーズは、エンタープライズクラスのスタッカブルマルチレイヤスイッチであり、高いアベイラビリティ、スケーラビリティ、L2 / L3レベルによるセキュリティ、および制御を提供してネットワークの運用を向上させます。ネットワークのコアにも用いられるパフォーマンスを実現します。


Cisco Catalyst 3560 シリーズ


Cisco Catalyst 3750 シリーズ


VPN クライアント ソフトウェア


Cisco VPN 3000 シリーズ

● リモートアクセスユーザが100人以下の小規模な企業から、最大で10,000人が同時アクセスする大規模な組織まで、幅広くサポートするさまざまなモデルを用意

Cisco Catalyst 4000 シリーズ

統合型ネットワークの制御に対応できる復元力を備えたモジュール型のマルチレイヤスイッチ。高いアベイラビリティとレイヤ2～4スイッチング機能によって、音声 / ビデオ/ データ統合型ネットワークを実現します。GRIDコンピューティングのサーバ収容などにおいて、優れたパフォーマンスと信頼性を提供するCatalyst 4948 シリーズなど、並外れた信頼性とサービス性が実現されます。


Cisco Catalyst 4500 シリーズ


Cisco Catalyst 4948 シリーズ


Cisco Aironet
1130AG / 1200 シリーズ


7961G　7970G　7920
Cisco IP Phone

Cisco Catalyst 6500 シリーズ

数多くの稼動実績に裏づけされた高信頼性かつ高性能なモジュール型マルチレイヤスイッチの最上位機種。アクセスレイヤからコア、データセンター、およびWANエッジまで、セキュアな統合型サービスを可能にします。さまざまなセキュリティサービスモジュールの追加によって、レイヤ4以上の機能も1つの筐体に統合することができます。


Cisco Catalyst 6500 シリーズ


Cisco Secure ACS シリーズ

Catalyst 6500用 サービスモジュール

以下のサービスモジュールを用意しています。

- FWSM（ファイアウォール サービスモジュール）
- WLSM（ワイヤレスLAN サービスモジュール）
- IDSM-2（第2世代IDS サービスモジュール）
- IPSec VPNSM（IPSec VPN サービスモジュールポートアダプタ）
- NAM-2（第2世代Network Analysisモジュール）
- SSLSM（SSL サービスモジュール）
- ADM（DDoS、トラフィック異常検出 サービスモジュール）
- AGM（Guard DDoS軽減対策モジュール）

Cisco NAC パートナープログラム

シスコは、セキュリティの標準化を推進していきます

Cisco NACパートナープログラムは、ウイルス対策ソフトウェアベンダー（McAfee、Symantec、Trend Micro）、デスクトップ管理（IBM Tivoli）などの業界大手セキュリティベンダー間の協力による成果です。シスコは、50社を超えるセキュリティベンダーとのマルチベンダーソリューションによるパートナーシップを推進しています（2005年10月現在）。複雑で常に変化するセキュリティ脅威を一社で解決できる企業はありません。シスコがセキュリティ市場においてリーダーシップをとり、NACのオープンフレームワークを通じて、複雑化し悪質化するネットワークの脅威に対処する業界標準を形成していくこと、セキュアなネットワークインフラの構築を実現していくこと、シスコはこれによって、企業ネットワークが直面する課題に対して、強力なセキュリティソリューションを提供します。

NACパートナープログラム参画企業に関する情報は、以下のWebサイトでご覧いただけます。
http://www.cisco.com/en/US/partners/pr46/nac/partners.html

NACパートナープログラム参画企業 （2005年10月時点）

ANTI VIRUS

McAfee SECURITY
symantec.
TREND MICRO
AhnLab
Computer Associates
KINGSOFT 金山软件有限公司
F-SECURE
NORMAN
RISING 瑞星
SOPHOS
Panda

REMEDIATION

IBM
altiris
BIGFIX
iPass
LANDesk SOFTWARE
PATCHLINK

CLIENT SECURITY

authentium
CITADEL SECURITY SOFTWARE
Netcordia
secure elements
SkyRecon
BELARC
CREDANT TECHNOLOGIES Be mobile. Be secure.
Check Point We Secure the Internet.
INTERNET SECURITY SYSTEMS
NEW BOUNDARY TECHNOLOGIES
Safend
BIND VIEW Insight at Work
elemental security
infoexpress
OPSWAT
SENFORCE
StillSecure
BLUECAT NETWORKS secure networks. simplified.
ENDFORCE
eEye Digital Security
PREVENTSYS
TRUST DIGITAL
SYGATE
CA SYSTEMS
GUARDEDNET
lockdown
phoenix technologies
PREDATORWATCH
TriGeo Network Security
WHOLESECURITY

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

0492-0510-20A-F