ソリューション ガイド

シスコ統合化ネットワーク セキュリティ：自己防衛型ネットワークの構築に向けて

シスコ統合化ネットワーク セキュリティ：自己防衛型ネットワークの構築に向けて

「ネットワークは、閉鎖的なシステムから開かれた高度なシステムへと変化してきました。その結果、ネットワークの境界はもちろん、ネットワーク内部から発生するセキュリティに対する脅威は計り知れないほど大きくなっています。シスコはネットワーク インフラストラクチャにセキュリティ サービスを有機的に統合することによって、このような脅威に対抗する手段を提供しています。これは、現在のように拡大されてきたネットワークに柔軟かつ費用効率よくセキュリティを保つための包括的システム アプローチです。」

米Yankee Group
エンタープライズ コンピューティング＆ネットワーキング アプリケーション インフラストラクチャ＆ソフトウェア プラットフォーム担当副社長
ゼウス・ケラヴィーラ

先見的な企業では、次々とインターネットベースのネットワーク ソリューションを採用し、業務改革を進めています。その結果は、競争力の強化、新たな収益源の開拓、業務プロセスの最適化として現れています。

最近では、ミッションクリティカルなビジネス アプリケーションやサービスの多くがオープン ネットワーク上に配備され、インターネットと接続される例も増えています。このような状況では、適切なセキュリティ ポリシーや、プロセス、製品を導入しないと、インターネット接続によって向上するはずの生産性や、それによる利益の増大と顧客層の拡大に悪影響が生じかねません。

適切なセキュリティ ソリューションを導入すれば、企業は安心して顧客やパートナー、リモート オフィス、モバイル ワーカーにネットワークを拡大できます。そして、収益源の拡大、業務プロセスの効率化、従業員の生産性の向上などが実現されます。

業界によっては、データのプライバシ保護や訴訟の可能性が政府の要求事項として定められていることもあります。たとえば、米国の健康医療事業者は Health Insurance Portability and Accountability Act（HIPAA; 医療保険の携行性と説明責任に関する法律）を遵守しなければならず、米国の金融サービス事業者は Gramm-Leach-Bliley Act（GLBA; グラム リーチ ブライリー法）を守らなければなりません。また、英国企業は株式公開企業の社内統制に関するターンブル レポートや 1995 年のデータ保護法に従わなければなりません。日本においても、2005 年 4 月より「個人情報保護法」の全面施行が予定されており、個人情報を取り扱っている事業者に対して、その義務と対応が法律として定められます。

インターネットだけでなく、社内のネットワークを利用する場合にも、機密情報をやりとりする場合には、より高いレベルのプライバシ ポリシーや規制要求に従って、機密情報を確実に保護する必要があります。そのためには、セキュリティ制御やポリシーを使用して、リスクを軽減し、適切な注意を払うことが必要です。

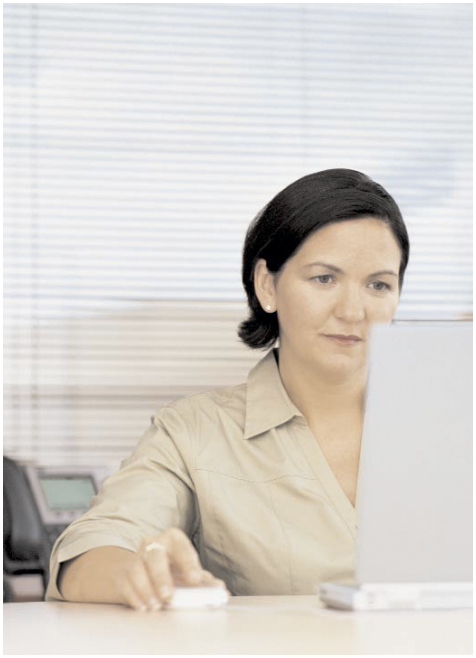
シスコの考え

シスコシステムズは、お客様の「信頼できるパートナー」として、お客様が重要な業務アプリケーションやプロセスを資産価値の高いインテリジェント ネットワーク上に安全に配備し、それによって生産性を高め、競争上優位に立つことができるよう支援します。これを実現するためには、回復力に富み、適応性のある統合化ネットワークを構築する必要があります。企業にとって、業務プロセスや情報資産のセキュリティが保証されるという安心感は、生産性向上やダイナミックな成長を促す重要な要因です。

シスコは、IP ネットワークに基本的なレベルのセキュリティしか提供できない他のセキュリティ ベンダーとは異なり、企業のミッションクリティカルなネットワークに必要とされる高度な統合型ネットワーク セキュリティ システムやサービスを提供します。

シスコは今後もネットワーク インフラストラクチャにセキュリティ インテリジェンスを付加していきます。セキュリティは単なる補足ではなく、業務プロセスの基礎であり、最終的にはビジネスの成功を左右する重要な要因であると私たちは考えているからです。

自己防衛型ネットワークの構築



シスコの自己防衛型ネットワーク戦略は、セキュリティ システムに対するシスコの考えを形にしたものです。企業に対する脅威は常に変化します。したがって、変化に対応できるような防御態勢が必要です。これまでは、内部からの脅威も外部からの脅威もそれほど急激に変化することはなく、防御も比較的容易で一点集中的でした。しかし、インターネット ワームが数分で世界中に広がる現在の環境では、セキュリティ システムに（そしてネットワーク自体にも）即座に反応できる能力が必要とされます。

自己防衛型ネットワークの基盤は統合型セキュリティです。シスコの統合型セキュリティでは、あらゆるレベルにセキュリティ機能が組み込まれています。つまり、デスクトップから LAN へ、そしてさらに WAN へと広がるネットワーク内のすべてのデバイスが、ネットワーク環境のセキュリティにそれぞれの役割を果たし、グローバルな分散防御機能を実現します。このようなシステムが構築されれば、社内リソースへのアクセスを制御する能力を管理者に与えつつ、伝送情報のプライバシを守り、内外からの脅威に対抗できます。シスコは、対処的な製品を提供するだけのセキュリティから、このような統合型セキュリティへとアプローチを進化させてきました。この構想をさらに発展させ、シスコでは他のセキュリティ ベンダーが提供している機能も取り込む方向へと進みつつあります。たとえば、Cisco NAC（Network Access Control）プログラムでは、ウィルス対策ソフトウェア ベンダーと共同で、感染デバイスがネットワークに接続するのを防ぐためのソリューション活動を進めています。このような自己防衛型ネットワークでは、脅威を識別し、重大度に応じて適切に反応し、感染サーバやデスクトップを隔離して、ネットワーク リソースを再構成するという方法で攻撃に対抗できます。

シスコの自己防衛型ネットワーク構想は、脅威に対する防御（Threat Defense）、安全な接続性（Secure Connectivity）、信頼性および認証管理（Trust & Identity）に、感染修復機能および危険デバイス隔離機能を統合したソリューションになります。

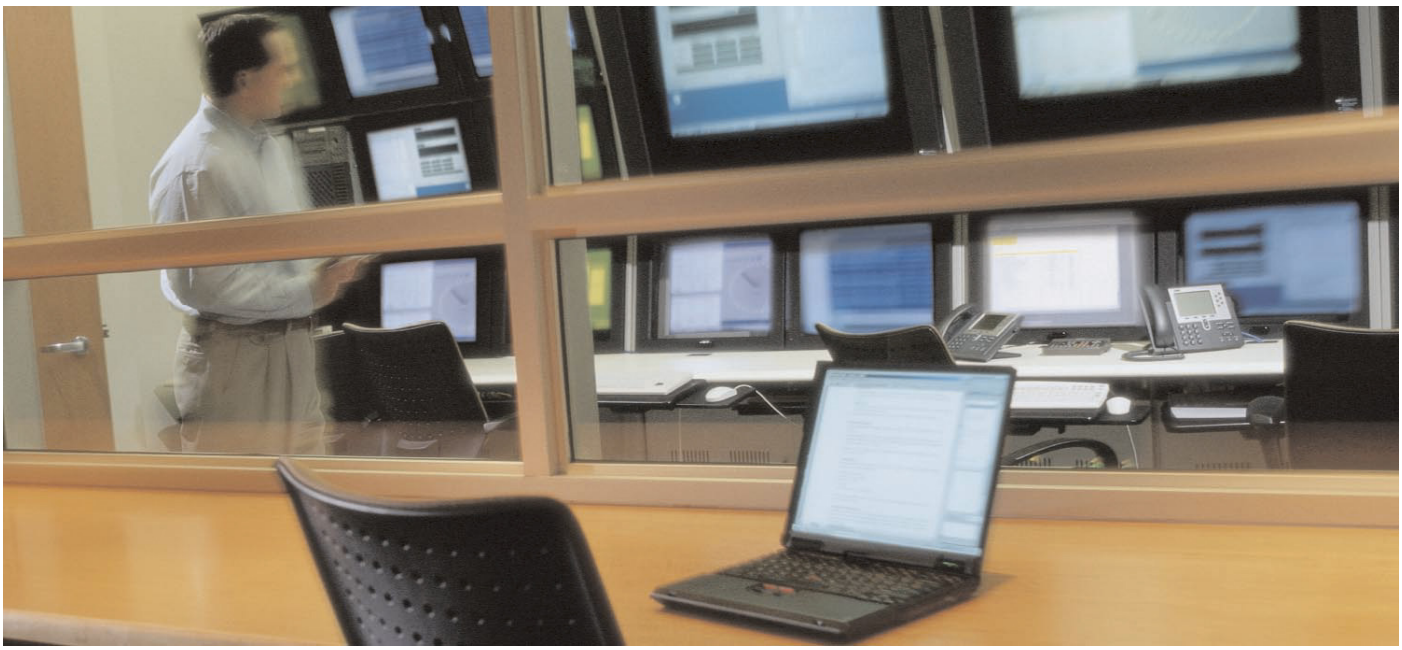
ネットワーク セキュリティの主要な要素

シスコの統合型ネットワーク セキュリティ ソリューションは、効果的なネットワーク セキュリティに不可欠であるとシスコが考える 3 つの要素で構成されています。

脅威から防御するシステム（Threat Defense）

今日の脅威は、既知、未知を問わず破壊力を増し、発生頻度も高くなっています。ワーム、DoS 攻撃、man-in-the-middle 攻撃、トロイの木馬など、企業組織内外からの脅威は、事業利益に大きな影響を及ぼす力を持っています。シスコの脅威防御システムは、このような既知および未知の攻撃からネットワークを守ることのできる強力な防御機能を備えています。

攻撃を効果的に防ぐには、高度なネットワーキング インテリジェンスとともに適切なセキュリティ技術が必要です。対処的な製品や技術だけを導入しても、ネットワーク全体にセキュリティが実装されていなければ、最大限の効果を得ることはできません。なぜなら、ネットワーク上のあらゆるポイントが攻撃の起点になる可能性があり、その影響は即座にネットワーク リソース全体に広がるからです。シスコの脅威防御システム（Threat Defense）は、既存のネットワーク インフラストラクチャのセキュリティ強化、エンドポイント（サーバとデスクトップの両方）への包括的なセキュリティの追加、そしてネットワーキング デバイスやアプライアンスへのセキュリティ専用技術を追加することによって、業務、アプリケーション、ユーザ、ネットワークへの脅威を未然に排除し、業務妨害、収益低下、企業イメージの失墜から企業を守ります。



脅威から防御するシステム（Threat Defense）は、ルータ、スイッチ、セキュリティ専用装置（ファイアウォール、ネットワークベースの侵入防止センサ、検知機器、トラフィック隔離技術）などにセキュリティ機能を統合する技術や製品で構成されています。また、エンドポイント（ノートパソコン、デスクトップ、サーバ機器）での防御には、Cisco Security Agent（CSA）が使われます。

安全な接続性を実現するシステム（Secure Connectivity）

ネットワークへの接続数が多くなるほど、ネットワークが危険にさらされる可能性も高くなります。イントラネット、エクストラネット、在宅勤務者などに、ブロードバンドなどのいわゆる常時接続によるインターネット接続が使用されるようになった今、これらの接続全体におけるセキュリティ、データの整合性、プライバシの維持が重要な問題になっています。

かつて信頼できるネットワークとみなされていた社内 LAN 接続においても、今では高いレベルのセキュリティ対策が必要となっています。実際、内部からの脅威は、外部からの脅威の 10 倍もの経済的損失を企業にもたらします。無線 LAN や有線 LAN で伝送されるデータやアプリケーションの機密性と整合性をどのように守るかは、企業が決定しなければならない重要事項として認識しなければなりません。

安全な接続を実現するシステム（Secure Connectivity）は、暗号化と認証の機能を利用して、信頼性の低いネットワーク上でセキュアな伝送を実現します。シスコは、無線および有線メディアを通じて伝送されるデータ、音声、ビデオのアプリケーション保護に、IP Security（IPSec）、Secure Sockets Layer（SSL）、Secure Shell（SSH）、マルチプロトコル ラベル スイッチング（MPLS）といった VPN 技術を提供しています。また、あらゆる IP コミュニケーションにおいてプライバシを保証するために、無線 LAN や IP テレフォニーのソリューションに広範なセキュリティ機能を組み込んでいます。

シスコは、安全な接続を実現するための動的ルーティング機能やマルチプロトコル サポート機能に加えて、業界のさまざまな接続オプションを統合することによって、信頼性が高く柔軟な接続ソリューションを提供しています。

信頼性および認証管理システム（Trust & Identity）

信頼性および認証管理システム（Trust & Identity）は、セキュアなネットワークやシステムを構築するための基盤となる、E ビジネスには不可欠な技術です。このシステムには、ユーザ権限に基づいて、業務アプリケーションやネットワーク経由でのリソースへのアクセスを許可または拒否する機能が含まれています。

信頼性および認証管理システム（Trust & Identity）は、ネットワークベースのアドミッション コントロールに重点を置いています。ユーザやデバイスの身元と企業のセキュリティ ポリシーへの遵守状況を検証してからでないと、所定のリソースやネットワークへのアクセスが許可されないようにします。そのための識別、許可、強制は、ネットワークで判断します。シスコの信頼性および認証管理によるソリューションでは、シスコ製スイッチやルータに組み込まれている Cisco Secure Access Control Server（ACS）、認証プロトコル（802.1X など）、Authentication, Authorization and Accounting（AAA; 認証、許可、アカウンティング）の機能によって、細かいアクセス権や非適合エンドポイント用の隔離ゾーンを柔軟に設定できます。また、未認証アクセスを完全に遮断することもできます。

自己防衛型ネットワークを実現するシスコ統合化セキュリティ ソリューション—ネットワーク セキュリティ製品ファミリー

シスコは、プロダクト、デリバリ、サポート、コンサルティング サービスを通じて、企業が必要とするセキュリティ ソリューションを提供します。

ファイアウォール、VPN、侵入防止システム（IDS/IPS）の統合

Cisco PIX 500シリーズ セキュリティ アプライアンス

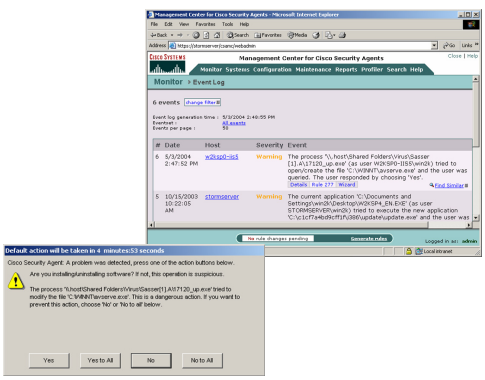
Cisco PIX® 500 シリーズ セキュリティ アプライアンスは、優れた信頼性、拡張性、機能を備えた世界最高水準のファイアウォールです。Cisco PIX セキュリティ アプライアンスは、ステートフル インスペクションと IPSec VPN 統合機能を含む画期的なハイブリッド セキュリティ アーキテクチャを実現し、専用アプライアンスとして提供されるほか、Cisco Catalyst® スイッチの統合モジュール（FWSM; ファイアウォール サービス モジュール）としても提供されています。Cisco PIX セキュリティ アプライアンスは、他のどのようなファイアウォールよりも高速かつ多数の同時接続に対応し、最高レベルのセキュリティとパフォーマンスをもたらします。

シスコのセキュリティ統合型ルータとCisco Catalystスイッチ

シスコは、シスコ ルータや Cisco Catalyst スイッチのセキュリティ機能を強化することによって、ネットワーク インフラストラクチャにセキュリティを統合し、非常に柔軟なセキュリティ配備と費用の節約を可能にしました。これらのネットワーク デバイスを活用することにより、企業はこれまでのインフラストラクチャへの投資を活用しながら、エンドツーエンドでセキュリティ ポリシーを実施できます。シスコ ルータや Cisco Catalyst スイッチに搭載されている Cisco IOS® ソフトウェアは、標準ベースの多機能 MPLS VPN や IPSec VPN をサポートし、あらゆるリモート アクセスやブランチ オフィスの接続に対応できます。またシスコ ルータや Cisco Catalyst スイッチには、強固なステートフル ファイアウォールや Intrusion Detection System（IDS; 侵入検知システム）の機能を内蔵でき、プラグイン アクセラレーション モジュールを利用してパフォーマンスを拡張することもできます。これによりシスコ ルータや Cisco Catalyst スイッチは、ネットワーク接続されたリソースへのエンドポイントからの接続を許可または拒否する主要なアクセス制御メカニズムを提供します。

侵入防止システム（IDS/IPS）

Cisco IDS/IPS は、ネットワーク境界、エクストラネット、および脆弱性が問題になっている内部ネットワークにリアルタイムの侵入防止機能を提供します。このシステムは、センサを内蔵した高速のネットワーク アプライアンスになっており、個々のパケットを解析し、疑わしい活動を検知します。未許可の活動やネットワーク攻撃の兆候を示すデータ ストリームがネットワーク内に出現した場合、センサがリアルタイムで不正利用を検知し、管理者に警告して、攻撃元デバイスをネットワークから排除します。



エンドポイントのセキュリティ ソリューション

Cisco Security Agent（CSA）

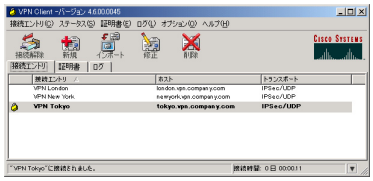
CSA は、PC 端末やサーバにインストールされるエンドポイント セキュリティ ソフトウェアです。CSA は、悪意ある動作を未然に識別して食い止め、既知、未知を問わず（Day Zero 攻撃も含め）、インターネット ワームなどの潜在的なセキュリティ リスクを排除し、万が一 端末が被害にあってしまった場合でも二次被害を防止するという点で、従来型のソリューションより優れています。

シスコ リモート アクセスVPNソリューション

Cisco VPN 3000シリーズ コンセントレータ

Cisco VPN 3000 シリーズ コンセントレータは、現在利用できる最高レベルの暗号化および認証技術に、高い可用性、高パフォーマンス、拡張性に優れた技術を組み込んだリモート アクセス VPN プラットフォームです。最新の VPN 技術が使用されており、通信にかかる費用を大幅に軽減できます。Cisco VPN 3000 シリーズ コンセントレータは、非常に拡張性に富み、購入後にコンポーネントの交換やアップグレードが可能な将来性の高いプラットフォームです。このような Scalable Encryption Processing（SEP）モジュールと呼ばれるコンポーネントは、ユーザが容量やスループットを簡単に追加できるように設計されています。また Cisco VPN 3000 シリーズ コンセントレータは、IPSec-VPN と SSL-VPN のいずれの VPN トンネリングにも対応できるので、すでにお使いの IPSec による VPN サービスに加えて SSL-VPN も利用可能になり、柔軟性の向上と所有コストの軽減にも役立ちます。

シスコのVPNクライアント ソリューション



Cisco VPN Client

Cisco VPN Client は、E コマース、モバイル ユーザ、在宅勤務などの用途に対応できるリモート アクセス VPN 用のセキュアな接続を実現します。Cisco VPN Client は、Windows、Linux、Solaris、Macintosh のオペレーティング システムに対応しています。また、Data Encryption Standard（DES）、Triple DES（3DES）、AES の暗号化に加え、デジタル証明書、ワンタイム パスワード トークン、事前共有鍵、RADIUS、NT Domain、Active Directory/Kerberos および LDAP の許可機能による認証など、IPSec 標準が完全に実装されています。Cisco VPN Client は、Cisco VPN 3000 コンセントレータ、Cisco PIX ファイアウォール、VPN 対応のシスコ ルータなど、シスコの多くのヘッドエンド プラットフォームでサポートされています。現在のバージョンでは日本語ユーザ インターフェイスに対応しているため、直感的な利用が可能です。

シスコ コンテント マネジメント ソリューション

Cisco SSL アクセラレータ

シスコのソリューションは、SSL ベースのイントラネット、エクストラネット、インターネットのアプリケーションをサポート可能な業界最高レベルの多彩な機能とパフォーマンスを提供します。また、SSL トランザクションを最適化することにより、サーバ容量の解放、サイト パフォーマンスの拡大、セキュア トランザクションの信頼性の向上、ユーザの証明書管理の簡素化、設備投資と運営費の軽減をもたらします。

コンテント アクセス マネジメントとコンテント フィルタリング

シスコは、ネットワーク エッジでのコンテント アクセス マネジメントのためのソリューションを提供し、企業や学校での好ましくない Web サイトのブロックと URL フィルタリングを可能にします。これを導入することにより、Web アクセスの管理が改善され、生産性が向上されるだけでなく、思いがけない被害を防止できます。

シスコの信頼性および識別管理ソリューション

Cisco Secure ACS

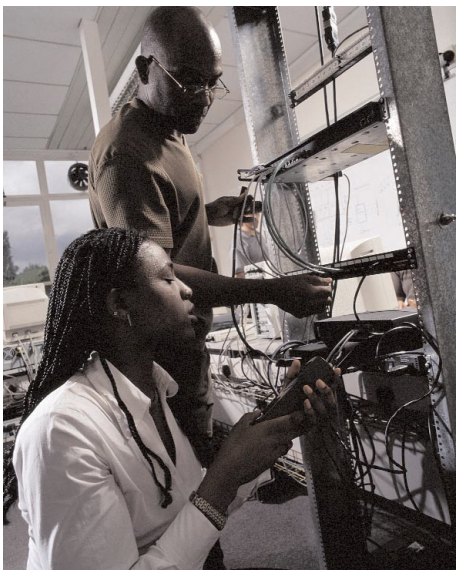
Cisco Secure ACS（Access Control Server）は、拡張性に優れた高パフォーマンスのアクセス制御サーバであり、集中管理が可能な RADIUS または TACACS+ サーバ システムとして機能します。このサーバは、ネットワーク経由で企業のリソースにアクセスするユーザの接続認証を制御します。またネットワーク管理者は、Cisco Secure ACS を使用することで、ネットワークへのユーザ アクセスの制御や、ユーザおよびユーザ グループに対する各種ネットワーク サービスの許可、およびネットワーク内の全ユーザ アクションに関するアカウントの記録が可能になります。さらに、TACACS+ によるロールとグループの管理、および内部でのネットワークの変更 / アクセス / 設定方法の制御に同じ AAA（Authentication, Authorization, Accounting）フレームワークを使用できます。

Cisco Secure ACS は、Cisco NAC ソリューションのポリシー策定エンジンとして、企業のセキュリティ ポリシーを支えるインテリジェンスと制御機能を提供します。

シスコのセキュリティ管理ソリューション

CiscoWorks VPN/Security Management Solution（VMS）による統合管理

CiscoWorks VMS は、全社的なインフラストラクチャ管理に画期的なアプローチを提供します。この拡張ソリューションは、リモート ファイアウォール管理の簡素化と改善を可能にする自動化によってネットワーク セキュリティを強化します。また、シンプルで使いやすい Web インターフェイスを使用した高速配信とソフトウェア アップグレードも可能です。このソリューションは、インテリジェントな機能を通じて不必要な業務の混乱を防ぎながら、業務プロセスやポリシーを強化することにより、生産性の向上と総所有コストの削減をもたらします。CiscoWorks VMS は現在、最大 5 台のデバイスをサポートするエントリ レベルの基本バージョンから、1000 台以上の Cisco IOS セキュリティ ルータをサポートするハイエンド バージョンまで提供されています。CiscoWorks VMS は、ネットワーク インフラストラクチャを管理する他の CiscoWorks ツールとの統合によって、生産性を向上し、投資回収を増大します。



シスコが提供している
ネットワーク セキュリティ サービス

- CSA 導入サービス
- IP テレフォニーのセキュリティ コンサルテーション
- ネットワーク セキュリティの設計開発
- ネットワーク セキュリティの設計コンサルテーション
- ネットワーク セキュリティの導入エンジニアリング
- ネットワーク セキュリティ導入計画レビュー
- ネットワーク セキュリティの最適化
- セキュリティ状態の評価

単一デバイスおよび複数デバイスの管理

各プラットフォームには、それぞれにデバイス管理用のインテリジェント GUI が提供されています。生産性と総所有コストは、使いやすい Web ベースの GUI によって向上します。CiscoWorks VMS は複数のデバイスの管理にも使用できます。

シスコのサービスとサポート

インターネットの力を活用すれば、ネットワーキングに関する問題を迅速に解決できるだけでなく、お客様が重要な情報に迅速にアクセスできるようになり、お客様が自らの知識や能力を高めることによって、ネットワーク全体のパフォーマンスを事前に向上させることができるとシスコは考えています。シスコのサービスとサポートは、このような考え方に基づいてモデル化されています。

シスコは、Cisco.com/jp を基盤とする双方向のネットワーク アプリケーション スイートによって、シスコの情報、リソース、システムへの迅速かつオープンなアクセスを提供しています。お客様やパートナーは、Cisco.com/jp を利用して、オンラインで包括的な技術サポートを提供する Cisco Internet Technical Support（ITS）など、さまざまなアプリケーションにアクセスできます。ネットワークのアップタイムを最大限にするために、TAC（Technical Assistance Center）のネットワーキング エンジニアからは 24 時間いつでも技術支援を受けることができます。詳細は、http://www.cisco.com/jp/go/tac をご覧ください。

ネットワーク セキュリティに関するCisco Advanced Service

Cisco Advanced Service のコンサルタントは、CCIE® および CCSP の認定を獲得し、大企業や政府組織における大規模ネットワーク セキュリティ インフラストラクチャの計画、設計、導入、最適化に豊富な経験をもつ専門家です。

計画と評価

計画と評価 シスコは企業のネットワーク セキュリティの状況の包括的な評価を提供できます。シスコは「セキュリティ状態評価」（Cisco Security Posture Assessment）サービスを通じて、実地経験豊富なセキュリティ専門家を派遣し、ネットワーク デバイス、サーバ、デスクトップ、データベースの全体的な評価を実施し、ネットワーク セキュリティ状態に対する寸評を行います。シスコの専門家は、業界のベスト プラクティスを参考にしてネットワーク セキュリティを分析し、業務の脅威となり得る脆弱性を明らかにします。また、詳細な分析によって、ネットワーク全体のセキュリティ改善方法を推奨するとともに、修復のために優先すべき措置を提示します。

設計

シスコはお客様とともに、強力な自己防衛型ネットワークを設計します。シスコの専門家は詳細なアーキテクチャ アプローチを使用して、ハッカー、ウィルス、ワームからの攻撃に対抗する多階層の防御策を開発できるようにお客様を支援します。シスコは、ネットワーク トポロジー、デバイスの配置、接続など、既存のセキュリティ設計に対する改善点を指摘し、スケーラビリティ、パフォーマンス、管理性能を含めたすべてのネットワーク セキュリティ面を考慮したうえで、セキュリティ強化に効果的なプロトコル、ポリシー、機能を設定することを推奨します。

実装

自己防衛型ネットワークをうまく機能させるためには、戦略的な設計だけでなく、入念な配備、設定、ネットワーク インフラストラクチャとの統合が必要です。セキュリティ ソリューションの設計が完了したのち、シスコのエンジニアはお客様の社内チームと一緒に、新しいソリューションを実働環境に統合するための導入作業に取り組みます。シスコのエンジニアは、インフラストラクチャに及ぼす影響を最小限に抑えながらスケジュールどおりに作業を進行できるように社内チームの能力を高めつつ、セキュリティ ソリューションの配備、統合、管理に必要な専門知識を提供します。

最適化

セキュリティ ソリューションの設計と配備が完了したあとで、業務ダイナミクスの変化やネットワーク要件の増大が生じることがありますが、このような需要増にネットワーク インフラストラクチャが適応できるようになっていることも重要です。ネットワークの状況が変化した場合、シスコのエンジニアはお客様とともに、最適化検査を行い、お客様のネットワーク セキュリティ インフラストラクチャが目標とするパフォーマンスを維持できるようにします。

シスコのアウトソーシング サービス

シスコのマネージド セキュリティ サービス ソリューション

セキュアなマネージド サービスや VPN サービスに対する需要は増大しつつあります。サービス プロバイダーがこの需要増を活かして、迅速かつ費用効率よくサービスを導入できるように、シスコではさまざまなサービスを提供しています。IPSec、MPLS、またはこれらの両方に基づくマネージド VPN サービスを利用すれば、サービス プロバイダーは、既存の接続サービスにリモート アクセスやサイト間オプションを追加したり、IP テレフォニー、E コマース、サプライ チェーン マネジメント、コンテンツ配信などの付加価値サービスを提供できるようになります。マネージド ファイアウォールやマネージド IDS などのマネージド セキュリティ サービスは、ほかのサービスに付帯して提供される付加価値サービスです。

マネージド VPN サービス、マネージド セキュリティ サービスのいずれか、またはその両方を提供する場合でも、お客様は現在接続に使用しているシスコ製ルータや Cisco Catalyst スイッチの能力を活用できます。したがって、現在の投資を活かして配備にかかる費用を最小限に抑えながら、新たな収益をもたらすサービスを提供する機会が最大限に拡大されます。

Cisco Powered Networkプログラム

Cisco Powered Network マークは、それを表示しているサービス プロバイダーのサービス品質を表しています。このマークを表示できるのは、ネットワークの質を維持し、インターネット トラフィックを担っている装置にシスコ製デバイスを使用してサービスを構築しているサービス プロバイダーです。 つまり、このマークは、そのプロバイダーの提供サービスがセキュアで信頼性が高いことを説明しています。

シスコ チャネル パートナー

シスコ Security/VPN スペシャリゼーション プログラムは、シスコのネットワーク セキュリティ ソリューションの販売、設計 導入、サポートに必要な技能を習得したシスコ チャネル パートナーを認定するものです。インターネット ビジネス ソリューションが急速に普及したために、必要なセキュリティの導入やサポート サービスに対する需要も増大しています。シスコ セキュリティ スペシャリゼーション パートナーは、このような需要に対応できます。

シスコのトレーニング サービス

シスコ セキュリティ認定

シスコ セキュリティ認定は、最高レベルのトレーニングと試験を使用し、セキュリティ専門家の技能と資格に関する判断材料を提供します。シスコは、IT セキュリティ市場の認定制度に対する要求を満たすため、CCIE や CCSP™ のほか、Cisco VPN スペシャリスト、Cisco Firewall スペシャリスト、Cisco IDS スペシャリストという 3 種類の認定を提供しています。CCSP 認定を取得することにより、お客様のスタッフが包括的なエンドツーエンドのセキュリティ ソリューションを確実に導入できるようになります。

セキュリティに関するシスコ認定ラーニング パートナー

世界中のさまざまなシスコ認定ラーニング パートナーが、シスコ認定のセキュリティトレーニング コース、リモートラボ、自己学習用教材など、最新のセキュリティ技術に関するリソースを提供しています。たとえば、Advanced Cisco PIX Firewalls、Cisco Secure Intrusion Detection System、Cisco SAFE Design Implementation、Managing Cisco Network Security などのトレーニング コースが提供されています。認定およびトレーニング情報、コース情報、試験日、およびセキュリティ専門パートナーの詳細なリストについては、以下のサイトをご覧ください。

http://www.cisco.com/jp/event/tra_ccc/ccc/

シスコ セキュリティ エコシステム

シスコのセキュリティ製品、技術、サービスは、ネットワーク セキュリティ ソリューションの構築を成功させるための基本的な要素です。しかし、ネットワーク セキュリティに包括的に取り組むためにはそれだけでは不十分です。シスコの製品ラインがもたらす利点を最大限に活用できるような「セキュリティ エコシステム」を構築する必要があります。セキュリティ エコシステムを構築するための重要な要素には、相互運用可能なサードパーティ製品、実装サービス、顧客サポート、整合性のあるサービス商品などがあります。

Cisco AVVID セキュリティ & VPN パートナー プログラムは、シスコ製品を補完するサードパーティ製セキュリティ ソリューションとの相互運用性検証を目的とした試験および共同マーケティング プログラムです。シスコはこのプログラムを通じて、個別の製品をより効果的なセキュリティ ソリューションに発展させ、検証済みの信頼できるセキュリティ ソリューションをお客様に提供します。

まとめ

シスコが目指す自己防衛型ネットワークの構築

お客様それぞれが生産性を安全に高める能力を持つことによって、真のセキュリティが実現されるとシスコは考えています。この考え方に基づいて、シスコはお客様のネットワーク セキュリティと、お客様の長期的な成功を支援しています。

シスコは現在、インフラストラクチャ製品への多彩なセキュリティ機能の組み込みや、さまざまなセキュリティ専用アプライアンス、ソフトウェア、コンサルティング サービスを提供することで、セキュアなインターネットワーキングを可能にする統合セキュリティ ソリューションをお客様に提供しています。

シスコのセキュリティ ソリューションによって、お客様はインターネット エコノミーを費用効率よく活用できるようになるとともに、次世代のチャンスを開拓する自信とそれがもたらす大きな成長を手に入れることができます。

シスコの統合セキュリティおよび自己防衛型ネットワークの構築に関する詳細は、以下のサイトをご覧ください。

http://www.cisco.com/jp/go/sdn

http://www.cisco.com/jp/go/securityhotnews

CISCO SYSTEMS

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

04.10