Cisco Self-Defending Network（SDN）

自己防衛型ネットワーク ソリューション

多様化する脅威に対し、ネットワーク全体が自ら適応することで、
ビジネスの継続性を実現するシスコの自己防衛型ネットワーク

2007年6月版

自己防衛型ネットワーク　Self-Defending Network:SDN

ネットワークに自己防衛する力を

今日、ネットワークは、あらゆる企業や組織にとって、ビジネスを成功に導くための重要な要素になっています。常に信頼できる IT サービスを提供するためのセキュリティもまた、生産性向上のために必要不可欠なシステムです。
しかし現在、ネットワークは新たなタイプの脅威に直面しています。
犯罪集団が、特定の企業、組織を狙い撃ちにするスピア形攻撃。自社の PC が乗っ取られ第三者への攻撃に利用されるボットネット。
ファイアウォール、アンチウイルス ソフトなどの従来型のセキュリティシステムだけでは、もはやこれらの新たな脅威に対応ができなくなっています。
一方で、VPN リモートアクセス,無線 LAN などの便利なネットワーク技術が、機密情報の漏えいなどの発生要因として問題になっています。
このように多様化するネットワークにおいて、新たな脅威による被害を回避するには、ネットワーク全体にセキュリティが組み込まれ、その構成要素同士が一体となって防御するシステムが最も効果的です。
個人情報保護法、日本版 SOX 法などの内部統制強化の動きに対応し、現在、セキュリティリスクを管理、低減するシステムの導入は最優先すべき課題となっています。このことからも、持続的に運用可能な、予防的で広範囲なセキュリティ対策が、今、ネットワークシステム全体に求められているのです。

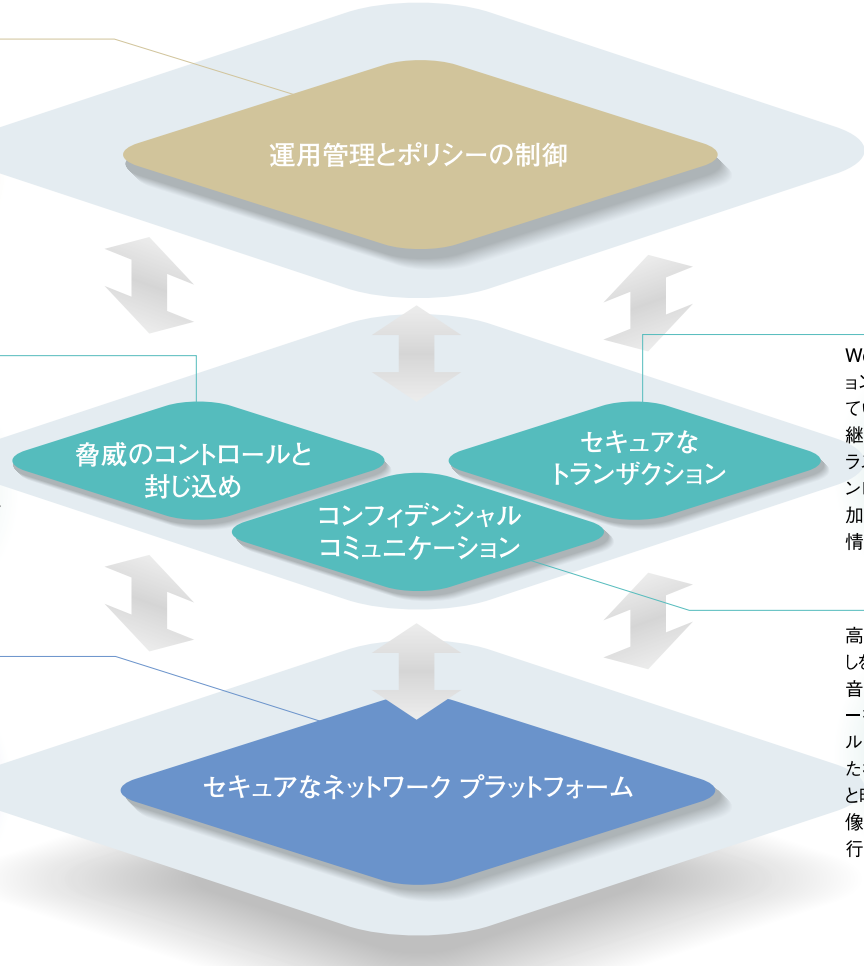
進化する自己防衛型ネットワーク

シスコの自己防衛型ネットワーク（Self-Defending Network ： SDN）は、セキュリティに対する脅威を、被害が発生してから対処するのではなく、事前に発見、防御し、実害を封じ込める、すなわち自己防衛を可能にします。インターネットとの境界はもちろん、組織内のユーザの PC からアプリケーションサーバまでのネットワーク上のすべての要素が、発生する攻撃や脅威に対し、より早い段階で自動的に対応することで、変異するウイルスやボットネットなどの活動を予防的に抑制し、被害を回避します。
自己防衛型ネットワークの "適応型防御システム（Adaptive Threat Defense ： ATD）" では、さまざまな種類の脅威に合わせた対策が、複数のポイントで展開されます。ネットワークに脅威が発生した場合、PC などのエンドポイントとネットワーク、および監視システムは、高度に連動して、ネットワーク全体の防御レベルを引き上げます。またこれと同時に、「どこでどのような問題がおこったのか」を、管理者に可視化して報告することで、発生したセキュリティ侵害の分析と対応のための迅速な意思決定（みえる化）を支援します。これにより、現在のシステムが持つリスクを正確に把握し、改善へと繋げるという、セキュリティシステムにおいて最も重要なライフサイクルが持続的に運用可能となり、新たな種類の脅威に対しても、常に最善の対策をとることができるようになるのです。

自己防衛型ネットワークのフレームワーク

自己防衛型ネットワーク（SDN）では、基本的なセキュリティ システムは、ネットワーク全体に、あらかじめ組み込まれます。
その上に、必要に応じて、さらに高度なテクノロジーを用いたセキュリティサービスを追加することで、脅威発生時の影響を極小化します。
さらに、それらの管理を統合化することで、真に効果が実感できるセキュリティシステムを運用することが可能となります。

企業ポリシーへの準拠を管理、監査するため、セキュリティシステムの統合管理が必要です。複数デバイスからの情報を自動的に相互分析することで、脅威を迅速に識別し、管理者の意思決定を支援します。さらに、対策内容を速やかにネットワーク全体に反映し、最適化することが可能となります。



ネットワーク上の構成要素が、綿密に連携することで、単に脅威からの「防御」を行うだけではなく、脅威をネットワーク自身が予防的に抑制し、多段階で封じ込めます。また、シスコの運用管理およびポリシー制御は、脅威の監視、分析、相互関連、および予防的な対応を行うための、強力な一連のツール群を提供します。

Web、E メールなどのトランザクションは、社内外を問わずに発生しています。それらの通信を安全に継続するために、セキュアなインフラストラクチャ上にアプリケーションレイヤセキュリティの要素を追加し、可用性維持、脅威の防御、情報漏えい防止を実現します。

IP ネットワークには、あらかじめセキュリティ機能が統合され、組み込まれます。従来はアドオン要素であった、ファイアウォール、アクセス制御、侵入防御（IPS）などの機能もルータ、スイッチなどのネットワーク機器の中に組み込まれ、必要に応じて使用が可能となります。

高度な暗号化技術や、成り済ましを防止する技術を用いて、データ、音声、映像などの通信プライバシーを保護します。音声などのリアルタイム通信の特性が考慮された技術を用いることにより、場所と時間を問わず、データ、音声、映像のコミュニケーションを安全に行うことが可能となります。

自己防衛型ネットワーク（SDN）の柱となる3つのセキュリティ戦略

シスコは自己防衛型ネットワーク（SDN）の基本方針に基づき、
（1）統合化セキュリティ、（2）コラボレーションセキュリティ、（3）適応型防御セキュリティ
の3つの具体的な柱となる戦略に基づいたソリューションを提案しています。

統合化セキュリティ

ネットワーク構成要素としての防御システム

- セキュアコネクティビティ（高度な VPN 技術など）
- 攻撃防御システム
- ユーザ認証システム
- 不正なルーティングの防止機能

など

コラボレーション セキュリティ

高度に相互連携するセキュリティシステム

- ネットワークアドミッションコントロール（NAC）
- 有線・無線 LAN 環境のアクセス認証（IBNS）
- 不正検知情報の集約とポリシーへの反映

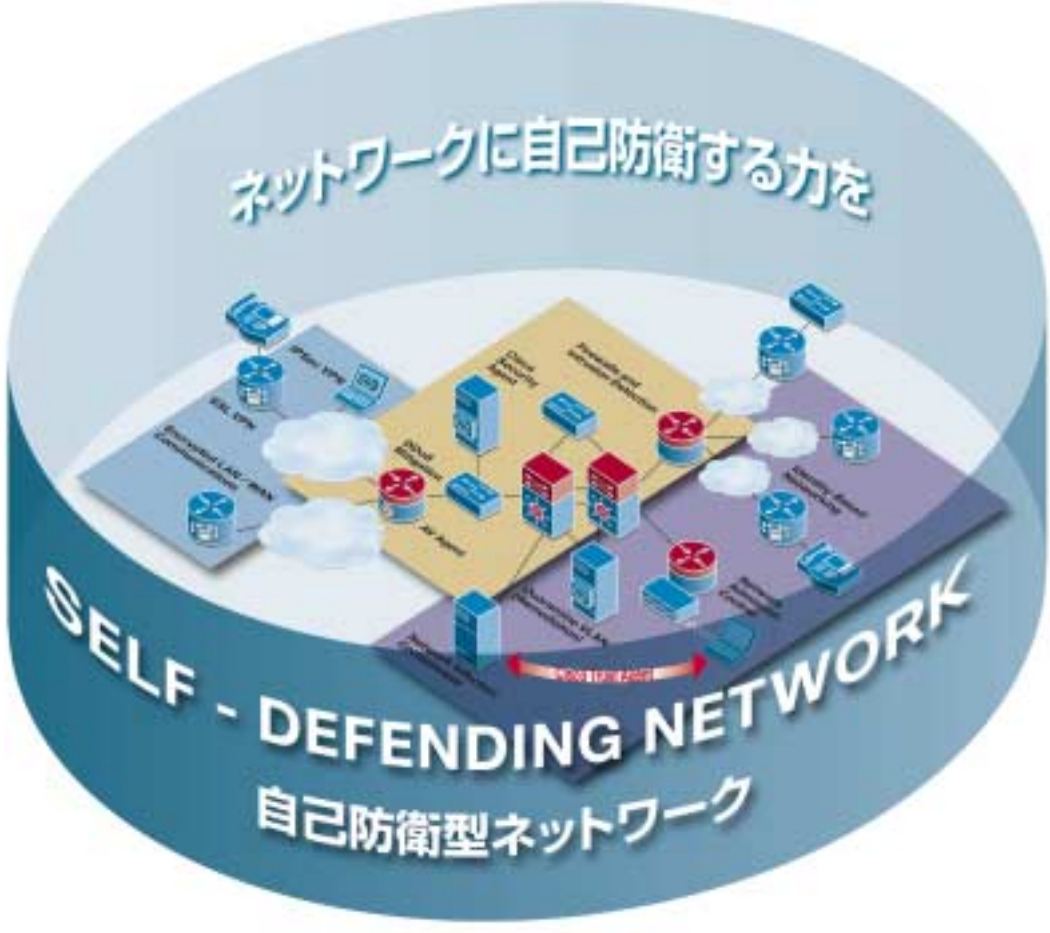
など

適応型防御セキュリティ

適材適所による、予防的な防御

- Web、E メールのアプリケーションを利用した攻撃からの防御
- マルウェア（悪質なソフトウェア）のブロック
- ネットワーク異常の検出と対処
- 不正トラフィックの封じ込め

など



セキュリティ専用製品が個別に機能する従来のポイントソリューションと異なり、ネットワークに統合されたセキュリティでは、ネットワークを構成するルータやスイッチなどの各デバイスにもセキュリティ機能を搭載し、ネットワークそのものが自らを保護します。
自己防衛型ネットワーク（SDN）では、アプリケーション間の安全な接続性を実現するセキュア コネクティビティ、多様な攻撃を無効化するマルチレイヤの防御システム、許可されないアクセスをネットワークで制御するユーザ認証システムなどのソリューションを提供しています。

攻撃手法や、脅威の侵入経路の多様化に対応するためには、さまざまなセキュリティ技術が相互に連携して動作することが重要です。
たとえば NAC は、PC の「健康状態」に応じてネットワーク上のデバイスが連動することで、組織のセキュリティ ポリシーを満たさないノードを隔離します。
IBNS による LAN アクセスのユーザ認証は、リモート VPN アクセスなどのユーザ認証と一元管理することが可能です。
また、検知した攻撃情報をネットワーク全体の防御デバイスに迅速に反映させることで、被害の拡大を食い止めたり、検知の精度を向上することも、綿密な相互連携によって実現できます。

適応型防御システム（Adaptive Threat Defense：ATD）は、さまざまな脅威に対して、「適材適所」の防御を実現します。たとえば、従来のファイアウォールで防御できない、Web、E メールなどのアプリケーション アクセスを利用した攻撃には、より高度な通信内容の検査や、「Anti-X 防御」技術で対処することが可能になります。
「適材適所」のシステムでは、エンドポイントや、ネットワークを流れる通信のより厳密な検査と管理が行われることで、未知の脅威に対しても柔軟に適応できるため、予防的な対策をとることが可能となります。

シスコの自己防衛型ネットワーク（SDN）ソリューションは、お客様が直面 する4つの

今日のネットワーク システムでは、インターネットやブロードバンド、IP 電話や無線 LAN など、あらゆる形態からのアクセスが想定されます。
利用者の利便性が高まる一方で、それは同時にさまざまな点でセキュリティ ホールとなりうるぜい弱性をはらんでしまいます。
こうした中、ネットワーク環境が直面するセキュリティ脅威に対する課題は、以下の 4 つにフォーカスすることができます。

Outbreak Prevention

課題 1

ウイルスやワームの大規模感染の危険

近年のウイルスやワームは、変異のスピードが数時間単位へと早まり、通常のウイルス対策ソフトでは検知、駆除できなくなっています。大規模感染に伴う大量の通信が、商取引などの重要システムの通信を麻痺させることも大きな問題です。
SDN では、ルータ、スイッチなどの通信機器にあらかじめ組み込まれたセキュリティ機能と、ふるまい検知、検疫などの高度なセキュリティ機能が連携します。これにより、PC の制御、ネットワークからの隔離、異常通信の抑制などの処理が自動実行されることで、甚大な被害を与えないよう封じ込め、大規模感染を未然に防止します。

● Cisco Catalyst 6500用 ファイアウォール サービス モジュール（FWSM） ● Cisco IOS アプリケーション ファイアウォール 機能 ● Cisco ASA 5500 シリーズ	● ぜい弱性攻撃の予防、監視 ● 不正な通信の防止 ● 拡散の遮断
● Cisco Catalyst 6500用 IDS サービス モジュール（IDSM-2） ● Cisco IPS 4200 シリーズ ● Cisco Secure MARS シリーズ	● ネットワーク単位でのぜい弱性攻撃の予防、感染活動の監視
● セキュアインフラストラクチャ （Cisco ISR サービス統合型ルータ、 Cisco Catalyst スイッチ シリーズ、Cisco Aironet シリーズ）	● トラフィック変動、挙動の監視 ● 不正なルーティングの防止 ● 優先制御による重要トラフィックの保護
● Cisco Security Agent（CSA） ● ネットワーク アドミッション コントロール（NAC）	● PC 端末からの大規模感染活動の抑止/攻撃の防御、拡散の遮断
● Catalyst 6500用 DDoS 軽減対策、 トラフィック異常検出サービス モジュール（ADM、AGM）	● 異常トラフィック、ワームによる DoS 攻撃の軽減、抑止 ● ネットワーク機能の低下、停止の防止
● Cisco ASA 5500 シリーズ ● ネットワーク アドミッション コントロール（NAC）	● VPN リモートクライアントPCの接続制御、状態認証の実施
● Cisco Secure MARS シリーズ	● 異常な PC 、トラフィックの可視化

ウイルスなどによる大規模感染の課題

- 広まったウイルス駆除に必要なリソースとコスト
- 感染した端末から社内ネットワークへの攻撃、汚染
- ネットワーク、端末のダウンタイムから発生する損失

自己防衛型ネットワークによる解決

- ネットワークが連携し、自動的に対策
- 従来型のアンチウイルス製品の課題を補完
- 定義ファイルの更新前でもウイルスの活動を抑止
- 異常トラフィックの検出とネットワークの保護
- 発生源、被害状況の可視化（みえる化）と履歴の記録

情報やデ
ビジネ
継続性
ため
ネットワー

DDoS Attack Prevention

課題 3

ますます重要視されるネットワークの機能停止

ネットワークシステムがビジネスの根幹をなすものである以上、その機能が停止した場合は、即、企業活動に損害をもたらすものになります。
悪意のある攻撃や、ウイルス感染によるトラフィック異常などの脅威から、ビジネスを守るには、ネットワーク自体が抵抗力を持つ必要があります。
シスコでは、脅威に耐える強固なネットワーク構築はもちろん、SDN ソリューションを通して、通常対策が難しい DDoS 攻撃など、ネットワークのサービス停止につながる新たな脅威にも対抗できるシステムの構築を支援します。

● Cisco ASA 5500 シリーズ ● Cisco Catalyst 6500用 ネットワークトラフィック分析モジュール（NAM） ● Cisco Secure MARS シリーズ	● アタック トラフィックのイベントログなどの詳細な分析
● Cisco IOS IPS 機能 ● Cisco IPS 4200 シリーズ ● Cisco ASA 5500 シリーズ ● Cisco Secure MARS シリーズ	● アタック トラフィックの検知、詳細分析とその対処
● セキュア インフラストラクチャ （Cisco ISR サービス統合型ルータ、 Cisco Catalyst スイッチ シリーズ、Cisco Aironet シリーズ）	● アタック トラフィックの検知と緩和 ● デバイス自身のコントロール プレーン保護
● Cisco Catalyst 6500用 DDoS軽減対策、 トラフィック異常検出サービス モジュール（ADM、AGM）	● アタック トラフィックのブロック ● 高負荷によるサーバ アプリケーションの機能停止を回避
● Cisco Security Agent（CSA）	● 不正なプログラムやトラフィック挙動の監視、阻止

機能停止の課題

- 組織化、悪質化が進む DDoS 攻撃
- 社内へのボット感染により、加害者となる可能性
- ウイルス感染などの損失によるネットワークの停止
- ワームの影響によるサーバへのアクセス不能

自己防衛型ネットワークによる解決

- 不正なトラフィック挙動の監視
- アタックトラフィックの検知、詳細分析、ブロック
- 攻撃被害の最小化、軽減対策
- 正常なトラフィックに影響を与えない DDoS 攻撃対策

の課題を解決します。

シスコは、ネットワーク技術のプロフェッショナルとしての視点から、進化するネットワークが抱える新たなリスクを常に分析しています。
自己防衛型ネットワーク（SDN）では、それらのセキュリティの脅威に対する予防・対応能力を、ネットワーク自体が備えることで、
企業や組織が直面する 4 つの課題を解決します。

Theft of Information Prevention

深刻さを増す個人情報保護と情報漏えい、データ盗難

課題 2

情報漏えい、データ盗難の課題

- 個人情報・顧客情報・社外秘書類・社員名簿等の流出
- 問われる会社の社会的責任
- 機密情報流出に関するビジネス上の損害
- スパイウェアやキーロガーなどの盗聴プログラム

自己防衛型ネットワークによる解決

- 標準化された PC 上での不正なふるまいの検知
- 不正 PC の接続拒否、コンプライアンス準拠の徹底
- ユーザ認証により不正ユーザのネットワーク利用を防止
- ネットワーク上での不正アクセス対策
- 管理者への迅速なアラートと状況分析、記録

個人情報保護法では、企業から個人情報が漏えいした場合、その企業は行政処分の対象になります。その結果、社会的経済的な損失に加えて、法的な責任を追わなければなりません。
情報漏えい対策では、ネットワークシステム全体で対策をとることが欠かせません。
SDN では、ネットワーク アクセスのユーザ認証や、不正な通信からの防御、許可していない PC の操作抑制など、あらゆるポイントでネットワークからの情報漏えいを防止します。また、ルータやスイッチ、ファイアウォール、無線アクセスポイントなどを統合的に管理することで、不正な挙動の検知が即座に可能となり、ネットワーク全体で防御策をとることも可能となります。

Cisco Catalyst 6500用 ファイアウォール サービスモジュール（FWSM） Cisco IOS アプリケーション ファイアウォール機能 Cisco ASA 5500 シリーズ	脆弱性攻撃の予防、監視 ネットワーク侵入の監視、抑止 ユーザ認証によるネットワーク接続制御
Cisco Catalyst 6500用 IDS サービス モジュール（IDSM-2） Cisco IOS IPS 機能 Cisco IPS 4200 シリーズ	侵入、不正挙動の検知 ネットワークへの不正侵入検知
セキュアインフラストラクチュア（Cisco ISR サービス統合型ルータ、Cisco Catalyst スイッチ シリーズ、Cisco Aironet シリーズ）	データや IP 電話音声の盗聴防止 ユーザ認証によるネットワーク接続制御 ネットワークデバイスへの侵入防止
Cisco Security Agent（CSA） ネットワーク アドミッション コントロール（NAC）	スパイウェア活動の抑止 リムーバブルメディアへの書き出し防止 クライアント端末の状態認証、監視、運用
Cisco ASA 5500 シリーズ	通信の暗号化（盗聴の防止）
Cisco Security Manager	ネットワーク構成情報の統合管理
Cisco Secure MARS シリーズ	ネットワーク上の不正挙動の統合監視、可視化

ータを守る
ネスの
実現の
めに
ークを守る

Insider Abuse / Application Misuse Prevention

社内外での対策が必要な不正侵入、不正利用

課題 4

不正侵入・不正利用の課題

- ぜい弱性の攻撃によるサーバ上の機密情報盗難
- 許可されていない無線、PLC 機器の LAN 接続
- スパイウェア、ボットなど「見えない脅威」の蔓延
- P2P ソフトなどを介した機密情報の流出

自己防衛型ネットワークによる解決

- ネットワーク侵入の監視、抑止
- IEEE802.1x を用いた LAN アクセスのユーザ認証
- 許可されない機器接続の検知と防止
- ポリシーに準じた PC およびネットワークの制御
- 不正なアプリケーションの通信抑止と封じ込め

情報漏えいの被害件数の80%以上は、外部からの侵入ではなく、内部からの不正アクセスによるものといわれます。一方で、特定の企業、公的機関に狙いを絞った、確信犯的な侵入や盗聴による大きな損害も出ています。
SDN では、不正アクセス、不正利用を阻止するための、ID 管理とネットワークへのアクセス制御はもちろん、ユーザの PC利用ポリシーの遵守状況の監視、メッセージやアプリケーションレベルでの安全な通信の確保など、複数ポイントでリスクをコントロールすることで、情報漏えいなどの不正侵入、不正利用による被害を回避できます。

Cisco Catalyst 6500用 ファイアウォール サービス モジュール（FWSM） Cisco IOS アプリケーション ファイアウォール機能 Cisco ASA 5500 シリーズ Cisco Secure MARS シリーズ	ぜい弱性攻撃の予防、監視 ネットワーク侵入の監視、抑止 不正なアプリケーションの通信抑止
Cisco Catalyst 6500用 IDS サービス モジュール（IDSM-2） Cisco IOS IPS 機能 Cisco IPS 4200 シリーズ Cisco ASA 5500 シリーズ	不正侵入、不正な通信アプリケーションの利用禁止 P2P アプリケーションの利用検知
セキュアインフラストラクチャ（Cisco ISRサービス統合型ルータ、Cisco Catalyst スイッチ シリーズ、Cisco Aironet シリーズ）	ユーザ認証による不正なアクセスの防止 不正なルーティングの防止 暗号化、LAN スイッチの機能による通信の盗聴防止
Cisco Security Agent（CSA） ネットワーク アドミッション コントロール（NAC）	利用禁止アプリケーションの作動検知、抑制 アプリケーションの不正動作の検知、抑制 クライアントPCからの不正な通信の抑止 リモートクライアントPCからのアタックの抑止
Cisco Security Manager Cisco Secure MARS シリーズ	ネットワーク構成情報の統合管理 不正な通信、異常なデバイス上の挙動監視

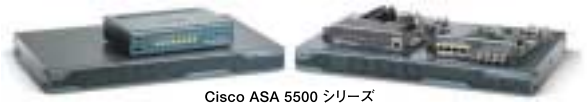
自己防衛型ネットワークを実現する製品群

自己防衛型ネットワーク（Self-Defending Network：SDN）では、ネットワーク全体を構成するパーツが協調して、適切なセキュリティ対策をとることができます。
シスコは、SDN を実現する製品、ソリューション、サービスをトータルに提供しています。
また、シスコはセキュリティ関連企業とのパートナーシップに基づき、戦略的な製品、およびサービスの拡充を進めてきました。
個々の機能および性能の向上はもちろん、製品間のコラボレーションの拡充を図ることで、お客様の抱える課題やリクエストにお応えしています。

適応型セキュリティ アプライアンス

Cisco ASA 5500 シリーズ

適応型セキュリティ アプライアンス（Adaptive Security Appliance）では、複数の機能を組み合わせることで、これまで対応が難しかった高度な攻撃および不正なアクセスを抑止することが可能となります。高機能なファイアウォール機能、IPSec/SSL-VPN 機能をベースに、サービスモジュールを増設することで、より高度な防御機能を利用しながら、実用的なパフォーマンスを維持できます。
統合された GUI による容易な設定と、サービスの仮想化機能により、セキュリティサービス開始に必要な時間の短縮、運用コストの削減を図ることも可能となります。
ネットワークセキュリティ上の最重要ポイントに配置することで、新たな脅威に対抗するシステムの効果的な運用を実現します。



Cisco ASA 5500 シリーズ

侵入検知・防御システム

Cisco IDS / IPS

ファイアウォールだけでは防御しきれない脅威の増加は、現在の IT ガバナンス上、最も考慮すべき対策課題です。IPS は、これらの攻撃が発する「特徴的な通信のふるまい」を詳細に監視し、リスクを含んだ通信を検知、遮断します。これにより、変異の激しいワームの感染活動の抑制、サーバのぜい弱性攻撃のブロックだけではなく、Winny などの P2P ソフトをはじめとする、許可されていないソフトウェアの通信を検知し、発生するリスクを予防的に回避することが可能となります。また、仮想化機能により、保護するシステムに応じて、異なるポリシーを適用することで、管理、運用コストの削減を図ることが可能です。

Cisco IDS / IPS 4200 シリーズ

セキュア スイッチ

Cisco Catalyst 6500 サービスモジュール

Cisco Catalyst 6500 LAN スイッチにサービスモジュールを追加することで、物理的なケーブルの接続作業を行うことなく、必要に応じて、任意のネットワークにハイパフォーマンスなセキュリティ機能を追加することが可能となります。

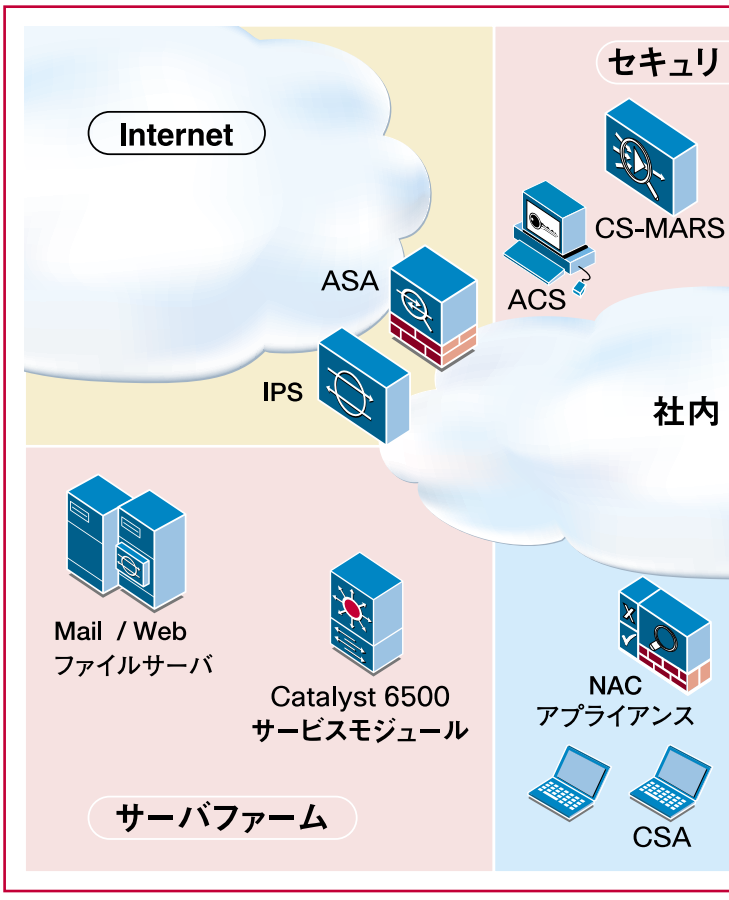
- ●FWSM（ファイアウォールサービスモジュール）
  高速ファイアウォール、ファイアウォール機能の仮想化に対応
- ●IDSM2（IDS サービスモジュール）
  IDS（侵入検知）/ IPS（侵入防御）モジュール IDS 機能の仮想化に対応
- ●VPN SPA（IPSec VPN 共有ポートアダプタ）
  高速 IPsec-VPN 用ポートアダプタ 大規模なサイト間 VPN のセンター集約に対応
- ●NAM-2（Network Analysis モジュール）
  ネットワークトラフィック分析 異常トラフィックのリモート解析にも対応
- ●ADM/AGM（DDoS トラフィック検出モジュール）
  ボットネットなどからの、DDoS（分散型サービス不可能）攻撃の検知、抑制

アクセス セキュリティ制御

Cisco Secure ACS シリーズ

組織の管理ポリシーに基づき、ユーザ認証、状態認証を用いて、ネットワーク上のリソースへのアクセスや、検疫、隔離を制御する、認証サーバ機能を提供します。
外部のユーザデータベース、認証システム、ポリシーサーバと連動することで、ポリシーの集中管理と、柔軟な導入および展開を実現します。

Cisco Secure ACS シリーズ



サービス統合型ルータ

Cisco ISR サービス統合型ルータ

実績に基づくシスコ IOS のルーティング機能に加え、セキュリティ、音声サービスを 1台のルータ上に統合することで、「あらかじめセキュリティ対策の考慮されたインフラ」を、ネットワーク全域に渡り展開することが可能となります。VPN 機能に加え、ファイアウォール機能、IPS 機能を有効にすることで、緊急事態が発生した場合、ネットワーク全体のセキュリティレベルを上げ、被害の拡大を抑制します。これらの予防措置により、PCの再インストールなど莫大な事後対策コストを削減します。

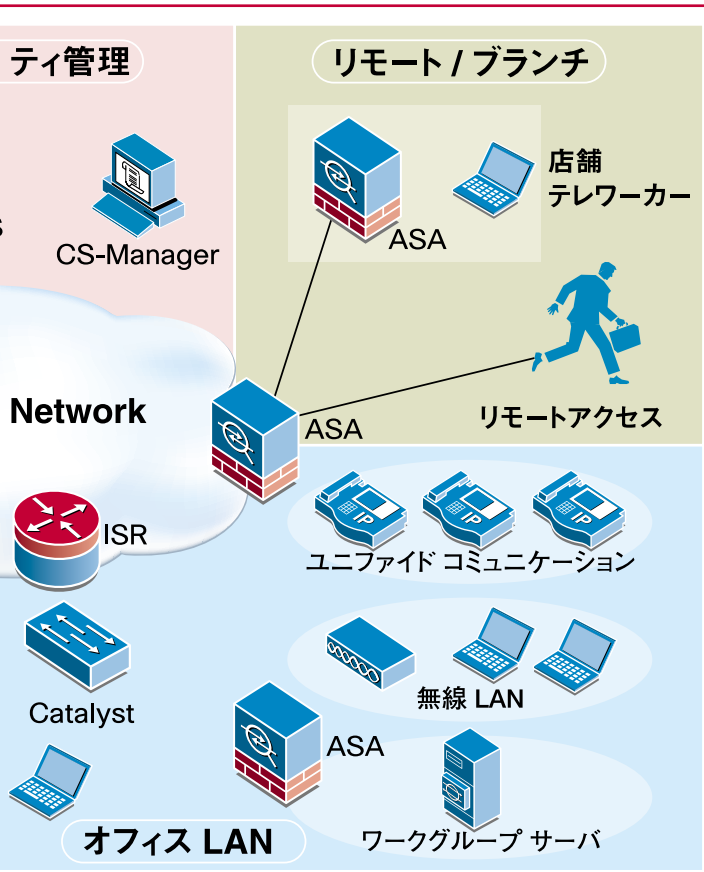
Cisco ISR 1800 シリーズ　Cisco ISR 2800 シリーズ　Cisco ISR 3800 シリーズ

セキュリティ統合監視・可視化

Cisco Secure MARS（CS-MARS）シリーズ

多数のセキュリティデバイスが配置されると膨大なログを記録として生成します。それらの情報から現在起こっている危機の状況を速やかに把握するには、ログを集約、相関分析し、整理する作業が必要となります。これらの作業には通常、非常に高度なセキュリティの専門スキルが必要ですが、CS-MARSではこの作業を自動化し、「ドコでナニが起きているか」を、管理者がリアルタイムかつ視覚的に把握することができ、短時間で有効な対策をとることが可能となります。

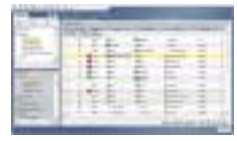
Cisco Secure MARS シリーズ



セキュリティ統合管理

Cisco Security Manager（CS-Manager）

多数のセキュリティデバイスを管理者の意図に合わせて最適化し、ポリシーを反映させるには、多くの時間と手間がかかります。この統合管理ソフトウェアは、管理者の生産性の向上と運用コストの削減を達成するだけでなく、統合監視システムとの連携により、緊急時の迅速なポリシー展開を実現します。



無線 LAN & ユニファイド コミュニケーション

Cisco Aironet & Unified Communication

豊富な実績に基づくユーザ認証と暗号化に加え、IPS との連携による不正な PC からの通信の抑止など多くのセキュリティ機能により、不正利用者の手軽な侵入経路になりやすい無線 LAN を、安心して利用できる IT インフラとして活用できます。
また、Cisco Unified IP Phone をはじめとする製品群は、IP ベースのコミュニケーションに潜む、盗聴などのリスクを考慮した、セキュアなユニファイド コミュニケーションをサポートしています。

Cisco WLC 2106

Cisco Aironet 1131

7970G　7921G

Cisco Unified IP Phone

セキュア スイッチ

Cisco Catalyst LAN スイッチ

NAC によるエンドポイントの隔離、IEEE 802.1X によるユーザ アクセス認証などの高度な付加機能だけではなく、意図的なトラフィックの操作による不正な盗聴や不正アクセス、ネットワーク停止を引き起こす攻撃に対抗できるセキュリティ機能を実装しています。まさにネットワーク全体でセキュリティが考慮されたネットワークの構築が可能となります。

Cisco Catalyst シリーズ

隔離・検疫

Cisco NAC ソリューション

持ち込み PC からのワーム感染や攻撃、情報漏えいなど、コンプライアンス条件を満たさない状態にあるユーザの PC からネットワークへの攻撃による被害は後を絶ちません。シスコが提唱したNAC（Network Admission Control）は、危険な状態にある PC を見分け、隔離、検疫を行うことで、ネットワークに弱点ができることを予防するシステムです。NAC の特徴は、LAN スイッチ、ルータ、VPN など、さまざまな接続形態に、隔離のための制御ポイントを設けることができる点です。これらの複雑な制御をシンプルに構築できることも、シスコ NAC の強みです。

Cisco NAC アプライアンス

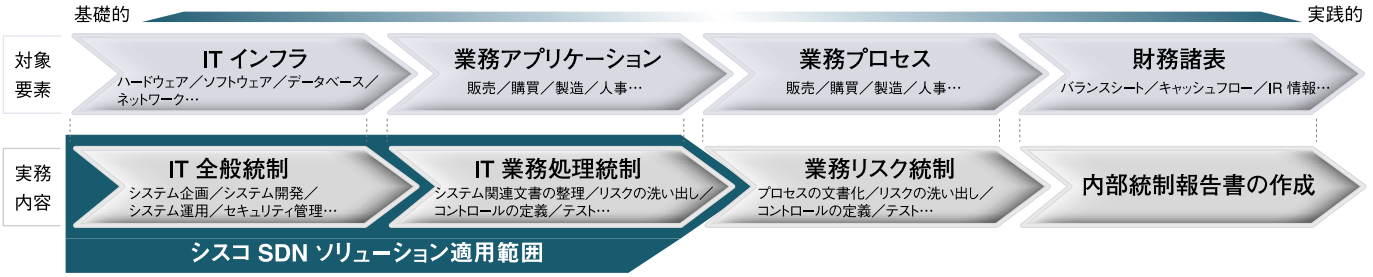
エンドポイント セキュリティ

Cisco Security Agent（CSA）

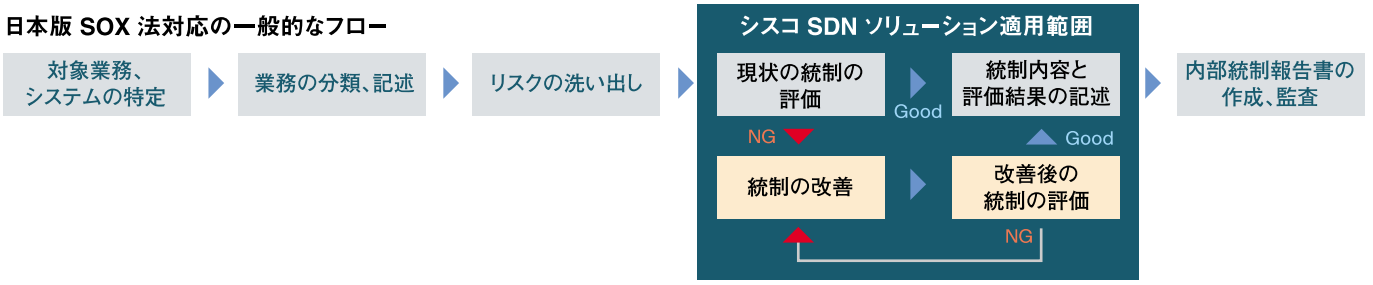
ウイルス、ワーム、スパイウェア、ボットなど日を追って増加する不正なプログラムは、従来型のアンチウイルス ソフトだけで対処することが困難です。
CSA は、PC 内で「ふるまい検知」を行うことにより、定義ファイルの更新なしに、これらの未知の脅威の活動をゼロタイムから抑制し、被害を最小化するソフトウェアです。
また、許可されていない PC 内の動作をカスタム定義することで、USB メモリによるデータの盗難、Winny や P2P ソフト利用など、ユーザの故意による PC の不正利用を防止することも可能です。IPS などと連動することで、PC 内部、ネットワークに渡り、複数のレイヤの防御システムを構築できます。

日本版 SOX 法に向けた対応

2008年4月1日以降に開始する年度から適用される「日本版 SOX 法」。
これは、金融商品取引法の一部の規定を指したもので、企業の会計監査や内部統制を徹底させることを旨としています。
現代のビジネスは IT システム抜きには成立しない現実を踏まえて、「 IT の利用（ IT の統制）」も必要な項目に含まれています。
これを受け、企業の IT 部門には、迅速かつ確実な対応が求められています。
法令遵守のみならず、実務面での効果を確かなものとするためには、その基盤となる IT インフラ、ネットワークにおける統制が必要であり、
シスコではこれらに対し具体的なソリューションを用意しています。



日本版 SOX 法対応の一般的なフロー



IT 統制ガイドライン「COBIT」とシスコの対応

COBIT（Control Objectives for Information and related Technology）とは、ISACA（情報システムコントロール協会）と IT ガバナンス協会が提唱する IT ガバナンスのフレームワークであり、米国 SOX 法対応で求められる IT 統制を構築するためのガイドラインとして多くの企業で採用されています。
2007年6月時点で日本語化されている最新バージョンの COBIT4.0 には全部で 513 の統制項目があります。
シスコでは、そのうち特に関連の深い項目を取り上げて、具体的な SDN 製品、ソリューションとの対応表を用意しています。

たとえば、COBIT の統制項目「DS5.9」が求める要件は…

- 脆弱性からの防御、脆弱性の検知、セキュリティ パッチの適用を実現する仕組みを導入しなくてはならない
- ウイルスからの防御、ウイルス定義ファイルの更新状況チェック、定義ファイルの適用を実現する仕組みを導入しなくてはならない
- ウイルスだけでなく、ワームやスパイウェアなど、さまざまなマルウェアからの防御を実現しなくてはならない

この項目に対するシスコのソリューションは…

IPS	システムの脆弱性に対する攻撃から防御
CSC - SSM	Web や E メール の通信を利用して拡散するウイルスや アドウェア、マルウェアを検知して削除するなどの防御を行う
IPS + ICS	危険度の高い新たなウイルスが発見された場合に、 ベンダーから正規のシグニチャが配信される前にウイルスの拡散を自律的に防止する
CSA	脆弱性に対する攻撃や、未知のものを含むウイルスの発症を防ぐ また、さまざまなマルウェアの引き起こす悪影響を防止
NAC / CCA	ネットワークアクセスする端末に対して、OS のパッチやウイルス定義ファイルのバージョンなど状態を把握。 任意に定められるポリシーに準拠しているか否かに基づき、接続制限などを行う

この他の項目に関しても、幅広いラインアップが、網羅的に対応しています。

詳しくは > **http://www.cisco.com/jp/go/jsox**

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先（シスコ コンタクトセンター）
http://www.cisco.com/jp/go/contactcenter
0120-933-122（通話料無料）、03-6670-2992（携帯電話、PHS）
電話受付時間:平日 10:00 ～12:00、13:00 ～17:00

0484-0706-20A-F