ホワイトペーパー

シスコの自己防衛型ネットワーク戦略のコア要素

シスコ Security Technology Group からの技術展望

2005 年 2 月

昨年は、シスコの自己防衛型ネットワーク（Self-Defending Network）の広告を見た方も多いことと思います。娘が知らずに父親のコンピュータにウィルスをダウンロードしようとする、看板が有刺鉄線でくるまれているといった愉快な TV コマーシャルや、セキュリティ デバイスをドーベルマンに見立てた印刷広告などです。シスコはネットワークおよびセキュリティ技術のプロバイダとして有名ですが、このような派手なマーケティング キャンペーンを行う会社であるとは思われていませんでした。しかし、こうした広告のおかげで、「自己防衛型ネットワーク（Self-Defending Network）とは、いったい何ですか？ ネットワークが自分自身をほんとうに守れるのですか？」という本質的なご質問をいただくようになりました。

短い答えで申し上げれば「はい、できます。」となります。セキュリティは、名前はよく知られているが煙突の中を通っているような実体の見えない産物から、システム全体のソリューションの領域へと移りつつあります。シスコは、この移行を可能にするために、技術開発とセキュリティ市場を推進しています。その理由は簡単です。特に規制措置の多い時代において、企業の IT 憲章のキーポイントは、企業の情報の完全性、機密性、永続性を守ることにほかなりません。私たちが情報駆動型のグローバル経済により深く移行するにつれ、情報と情報に対するアクセスを制御することの重要性は、これまでになく高まっています。そのため、IT インフラストラクチャを整備する目標は、正当なユーザにタイムリなアクセスを提供する一方で、不正アクセスを検出し、防御できるシステムを創造することになります。攻撃に直面して、単純にアクセスを拒否するだけの方法はもはや受け入れられません。今日のネットワークでは、ネットワークの可用性と信頼性を維持し、ビジネスの機能を継続できる方法で、攻撃に対応できなければなりません。ネットワークの「弾力性」を高めることで攻撃からの回復の速度を速めることが、多くの点でセキュリティの目標であるといえます。私たち人間はウィルスや細菌感染を被っても免疫システムによって機能を維持できます。同様に、ネットワークも攻撃によって倒れるのではなく、攻撃を吸収し機能を維持しなければなりません。

この文書では、自己防衛型ネットワークの基本要素とその機能を実現するためにシスコが採用した漸増的アプローチを論理的に説明します。

「セキュリティの全体像」の変化

好むと好まざるとにかかわらず、この 3 年間に起きたセキュリティの全体像の変化は、その前の 10 年間よりも大きいものでした。この変化の幅と割合が大きく、セキュリティ IT 部門にはこの変化に遅れずについていくことが難しくなっています。この変化を理解しないと、セキュリティに関するコントロールを回復することができません。

セキュア ネットワークの境界

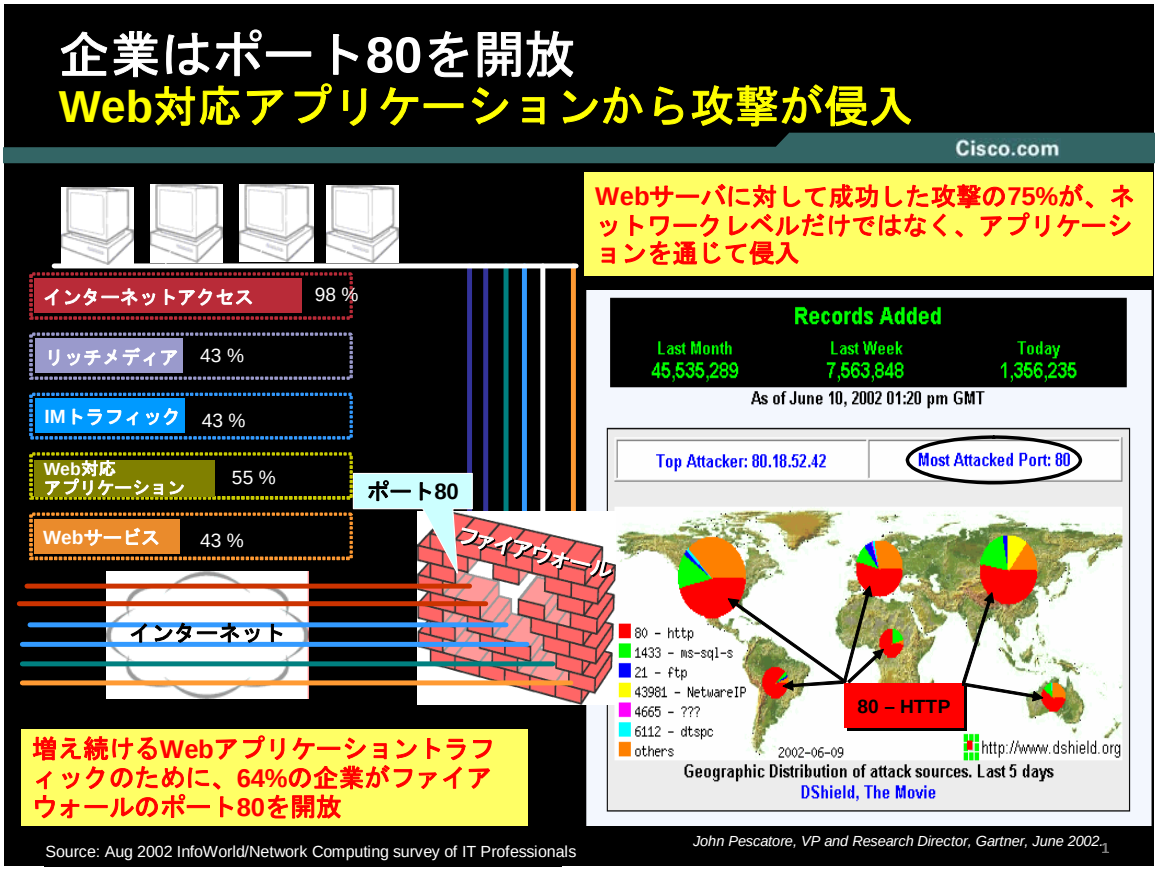
セキュア ネットワークの境界という概念は、企業がデータ センターを統合し、社内ネットワークを集約し、インターネットを取り込んだため、他のどんなトレンドよりも薄れてきてしまいました。かつては自社内で自己完結し、制御環境だったものが、今は B2B（Business-to-Business：企業間）エクストラ ネット経由のパートナーが接続し、ネットで小売が行われ、自宅で働く従業員にもネットワークが開放されることが普通です。企業ネットワークがこのように広がることで、信頼の境界は、信頼関係のない中間ネットワークを越え、制御されない環境にまで広がります。これらの経路を経由して企業ネットワークに接続するデバイスは、多くの場合、その企業のセキュリティ ポリシーに準拠していません。準拠しているデバイスであっても、企業ネットワークに接続する前に、他の制御されないネットワークへのアクセスにも頻繁に使用されているのです。結果として、これらの外部ネットワークのデバイスが、攻撃や付随する悪用の導入部になることがあります。

ワイヤレスとモビリティ

セキュア境界の概念と関係しますが、企業内の無線およびモバイル ネットワークは、現在、複数のネットワーク接続を保持するノートパソコン、PDA（Personal Digital Assistant）、携帯電話をサポートします。これらのマルチホーム ホストは、アプリケーション レベルでパケットを効率的にデバイス間で転送できるように、ピアツーピア通信を可能にするアドホックな（その場かぎりの）無線ネットワークを確立できます。この結果、ネットワークの境界がどこで始まって終わるのかが、さらに不明瞭になっています。セキュアシステムを管理し、ネットワークの可用性を維持するためには、企業は制御ポイントをモバイル デバイスまで拡張しなければなりません。

E コマース、エクストラネット、およびビジネスの Web 化

XML や SOAP などのメッセージング プロトコルに基づく共通アプリケーション インターフェイスが生まれたことは、E コマースや企業の生産性にとって恩恵でした。一方で、ほとんどの新規技術と同じく、これらの新規メッセージ プロトコルは、企業に、新たに取り組まなければならないネットワークの脆弱性と攻撃の道筋をもたらしてしまったのです。かつて複数のネットワーク プロトコルに広がったデータは、簡単にファイアウォール ポリシーでフィルタリングできていましたが、現在、1 つまたはいくつかの転送プロトコル（HTTP on TCP ポート 80 など）に混じり込んでいます。結果として、かつてはパケット ヘッダーにあった多くのデータが、今はパケット ペイロードに存在しています。これによって、明らかに処理の難易度が上がり、攻撃者が旧式のネットワーク保護機能を易々と回避してしまうようになりました。また、企業のデータ機密性と完全性の要件を満たすために、このアプリケーション レベルのトラフィックの多くが SSL/TLS や HTTPS プロトコルで暗号化されています。この傾向の副作用として、暗号化されたフローのパケット ペイロードを検査できないため、IT 部門がネットワークの境界部分で企業のアクセス ポリシーを実施することが難しくなってしまったのです。



ウィルス、ワーム、および伝搬の速度

この 3 年間に出現したウィルスとワームの数および種類の多さは、まぎれもない脅威です。しかし、ビジネスとその運用効率に与えた影響が最も大きかったのは以下の二つの要因です。

1）脆弱性が発見されてから虚弱点が攻撃に利用されるまでの時間が短くなったこと

2）これらの攻撃の多くが企業全体に広がるスピードの速さ

これによって、ビジネスの中断は受け入れがたいレベルに達し、要員、時間、そしてもともとこのタスクのために予算化されていなかった資金を消費する高価な復旧プロジェクトが発生します。

規制準拠 （コンプライアンス）

機密違反や企業内部の不正行為が広く報道されたことにより、多くの業界で規制団体が介入し、企業の情報リスクを管理するルールを作成することが強制されました。米国でのこのような規制として最も知られているものは、**Sarbanes-Oxley**（サーベンス・オクスリー法）、**Gramm-Leach-Bliley**（GLB; 金融機関向け顧客情報守秘に関する法律）、**Health Insurance Portability and Accountability Act**（HIPAA; 医療保険の携行性と責任に関する法律）です。これらは、企業ネットワーク、サーバ、データベース、およびホストを組織化する方法について、根本的な変革を強制しました。多くの組織は、規制に従っていれば、インフラストラクチャは安全になるという間違った仮定に立っています。しかし、これは多くの場合、正しくありません。意図しない法律に従うことによって規制を設ける行為自体が、新しい脆弱性の原因になることがあります。たとえば、中間ノードにおいて通過するトラフィックが不可視の場合、ワームやウィルスはエンドツーエンドVPNをサポートするネットワークでより効率的に広がりま

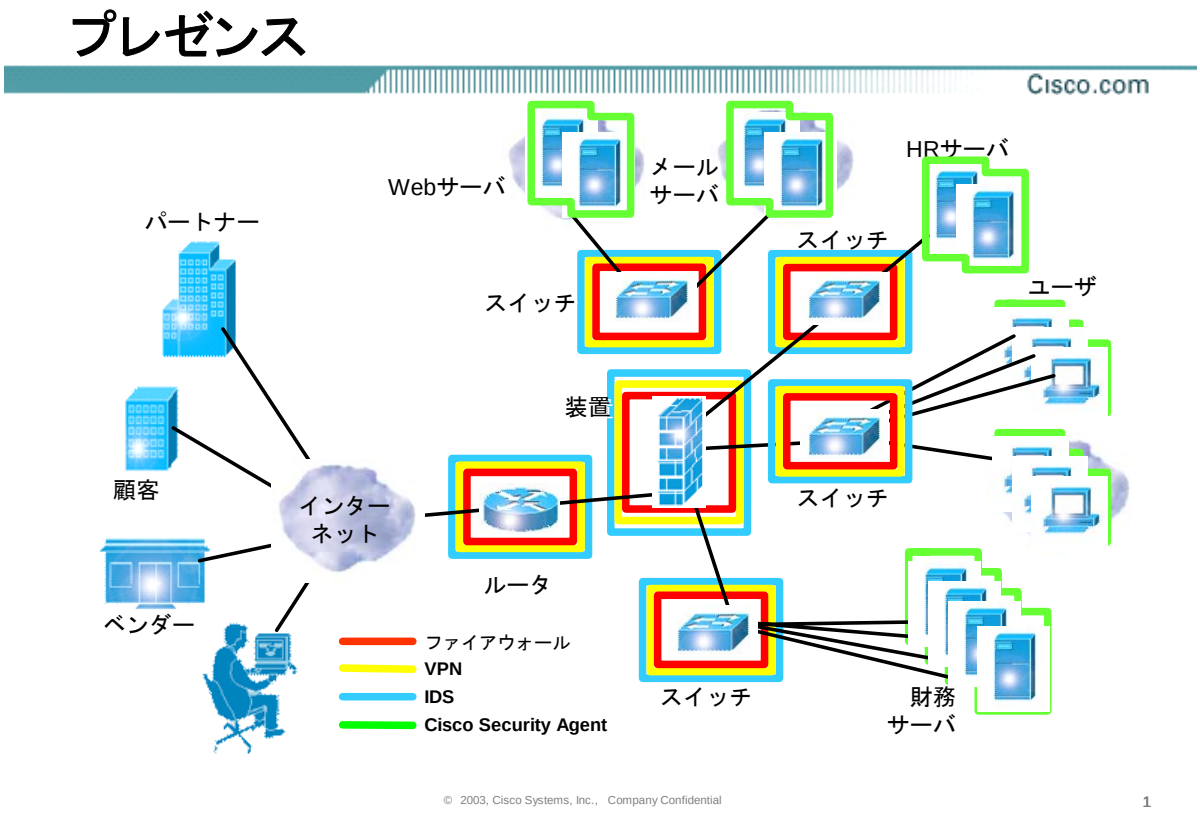
す。このようなトラフィックは、安全で暗号化されたパケットを通して、ワームを重要な企業のサーバに伝搬してしまうのです。こうした攻撃では診断に時間がかかるだけでなく、エンド ツー エンドVPNが問題の収拾を困難にします。

新しいセキュアネットワークの原則

セキュリティの全体像が変化しているため、企業は運用上許容できるかぎり多くの変化に対応する必要があります。理想的には、セキュリティの拡張が、現在使用しているルータやスイッチ設備などのインフラや、セグメント化やアクセス制御技術、これらのシステムをサポートする関連組織構造に与える影響を、最小にとどめるべきでしょう。このセクションでは、この目標をサポートする 自己防衛型ネットワーク の基本要素である**プレゼンス**、**コンテキスト**、**関連付け**、**信頼**について説明します。

プレゼンス

セキュア システムは、制御ポイントの主要概念から始まります。これを**プレゼンス**と定義します。私たち人間の免疫システムは、プレゼンス（存在）を達成するために、体中に分布する検出体と応答体に依存します。ネットワーク化された環境では、プレゼンスは、ネットワーク上の個々のノード内で、特定の機能が使用できるかどうかを意味します。これらの機能には、旧式の識別、アクセス制御、データ検査、および通信セキュリティ技術が含まれます。新しいアプリケーションでは、ピアツーピアのコンテンツ、Webサービス、音声サービス、およびダイナミックモバイルコンテンツの通信の増加に対応する機能が含まれます。



コンテキスト

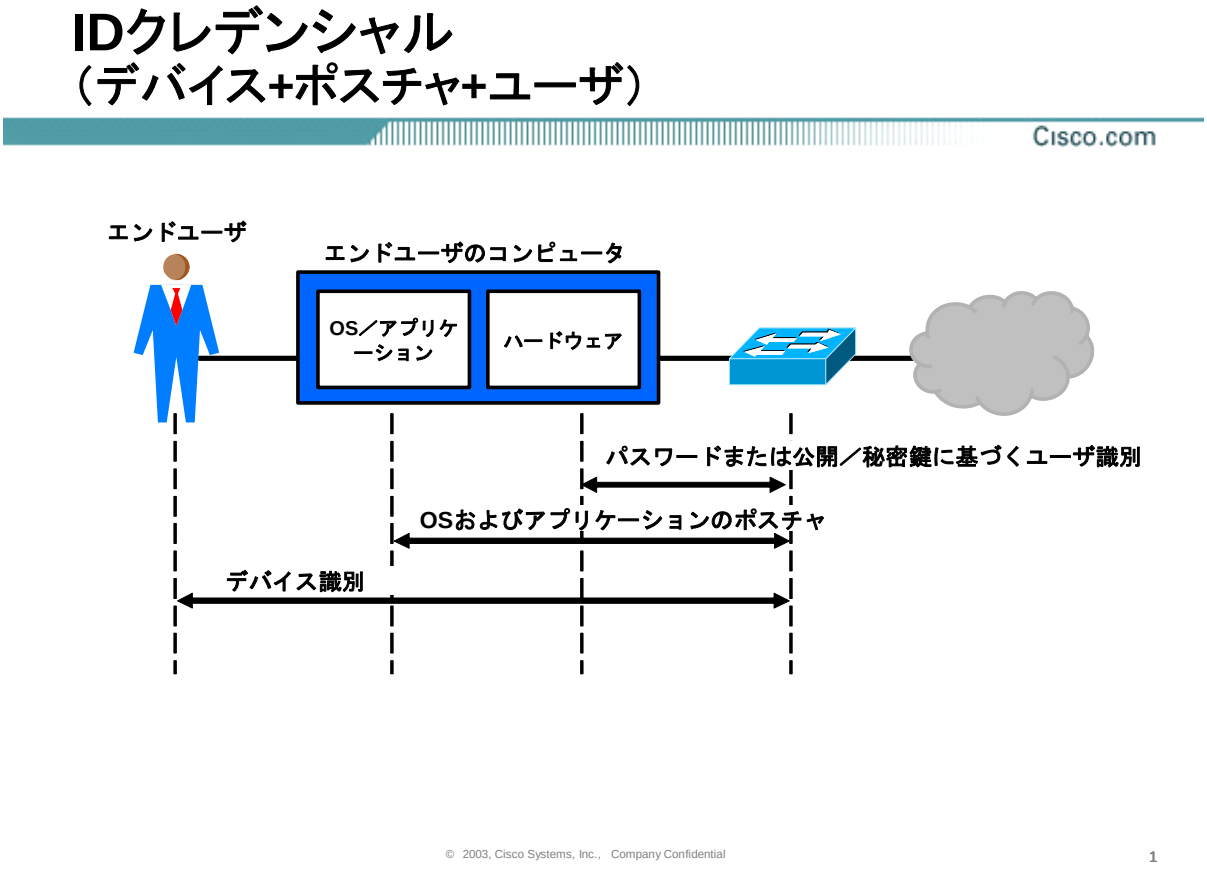
ユーザがネットワークにサインオンすると、ネットワークはエンドポイント**エンティティ（実在）**を構成するユーザとホスト双方のクレデンシャル セットへのアクセスを要求し、取得します。これらのクレデンシャルは、ネットワークに接続している間に、ホストのアクションに応じて変わる可能性があることに注意してください。接続中のクレデンシャルを全部まとめた情報を**コンテキスト**と呼びます。従来のネットワークでは、個々のユーザがネットワークに入った時点のアクセス権にのみ注目する傾向がありましたが、セキュア システムでは、エンティティとネットワークが関連付けられている間の動作の変化および関連付けられたコンテキストに基づいて、アクセス権を付与したり取り消したりします。たとえば、ホストがウィルスに感染したことをネットワークが検出した場合、このホストを治療ネットワーク セグメントに隔離することによって対処します。情報は改変される可能性があるため、セキュア システムでは、ある時点のホストの権限と特権を正しく評価するために、別のシステムからコンテキストを取得する必要があるでしょう。

関連付け

別々のエンティティを関連付けることで、コンテキストを共有でき、「システム」を構成することができます。従来のネットワークは、Border Gateway Protocol（BGP）などのルーチング プロトコルによってデバイス間の関連付けを構築していました。最新型の脅威や悪用に対処するために、これらのネットワークの関連付けを、ネットワーク トラフィックの発信元から着信先までの端から端までに拡張する必要があります。また、マルチホーム モバイル デバイスの存在が増え続けているために、これらの関連付けは、従来のネットワークでは対象外とされていた範囲に広がっています。エンティティがネットワークに入ったときに受け取る特権と、その特権が接続中にどのように変化するかは、そのエンティティのコンテキストとネットワークへの関連付けに結び付いています。

信頼

セキュア システムは、そこで扱う情報の信頼性に依存します。セキュアシステムは、包括的な**信頼**関係と組み合わせると、さらに優れた機能を発揮します。以前のセキュリティ システムの信頼は、主にデバイスまたはユーザのIDに重点が置かれていました。最近の進化によって、セキュア システムでは、デバイスの状態（「**ポスチャ**」）と場所の認識も含めることが必要になりました。多くの点で、ネットワーク上のユーザおよびデバイスの活動は、道路での自動車の運転にたとえることができます。あるクラスの乗り物を運転するには運転免許証を取得するように、ユーザはネットワークにログインするために、一定の種類のIDを取得する必要があります。そして、自動車には車両登録番号（VIN）が付けられ自治体に登録されるように、すべてのネットワークとエンドポイント デバイスには、製造時にデジタル証明書がインストールされ、企業内に配備されるときには一定の種類の登録が必要となります。しかし、適切なクレデンシャルが常に指定された場所または時点で存在するとは限りません。自己防衛型ネットワークでは、**推定された信頼**と**ベストエフォート**という革新的な形式を使用して、エンティティを認証し権限を付与します。自己防衛型ネットワークは、デバイスおよびユーザの識別、デバイスのポスチャ、および環境内でデバイスが占める場所の情報に結び付くクレデンシャルを、少なくとも取得する必要があります。このために必要な技術が最終的にはユビキタスになり、802.1Xや Extensible Authentication Protocol（EAP; 拡張認証プロトコル）方式などの明確に定義された標準ベースのメッセージ形式およびプロトコルによって有効になります。



これらの概念は、どれも、それだけで特別に注目に値するものではありません。しかし、自己防衛型ネットワークと組み合わせることで、非常に強力なものになります。これ以降、これらの概念が 自己防衛型ネットワーク フレームワーク内でどのように機能するかについて説明します。

必然性：自己防衛型ネットワーク

企業ネットワークと、それをターゲットにした攻撃は、もはや、単独のメカニズムに依存して安全性を維持することは不可能なほど複雑になりました。その結果、「多層防御」というコンセプトが導き出されました。今までのところ、このコンセプトは**予防的**防御の概念の上で構築されてきました。しかし、変化し続けるネットワークには、脆弱性とそれに伴う攻撃がついて回ります。シスコは、より優れた**アダプティブ**（適応型の）ソリューションの構築を開始する必要があると確信しました。その結果、自己防衛型ネットワーク のモデルとして、私たち人間の免疫システムのような現実世界での例に目を向けました。他にも、有益と認められる実世界のシステムには、疫学の分野や、さまざまなコミュニティでのお互いの監視方法などがありました。これらのシステムに共通する趣旨は、**予防的**であると同時に**アダプティブ**な防衛を採用していることです。

さらに詳しく調査してみると、このような性質のシステムを保護している防御は、機能ブロックごとに組み込まれる傾向があることがわかりました。**アダプティブ**な防衛の主要な能力としては、次のものが挙げられます；

- 常にアクティブである
- 目立たないように実行される
- 攻撃の伝搬を最小限にする
- 未知の攻撃にもすばやく対応する

自己防衛型ネットワークに当てはめて考えると、こういったシステムは、リソースが有限であり、リソースの枯渇を避けるために注意深く配備される必要があるという前提で構築されているといえます。また、お客様の IT オペレーションに対する混乱を最小限にとどめるため、既存のインフラストラクチャになるべく影響を与えないように、デザインされています。

▲

自己防衛型ネットワークは、お客様が既存のインフラストラクチャを新しい方法で活用できるシステムベースのソリューションを提供します。これによって、脆弱性の穴を減らし、攻撃の影響を最小化し、インフラストラクチャの全体的な可用性と信頼性を高めることができます。また、人的介入をほとんど必要とせずにアウトブレーク（大規模感染など）に迅速に対応できる自律システムも構築中です。このような迅速な対応は、以前にも増して伝染力が強い最新の攻撃を阻止するために必要です。

シスコの自己防衛型ネットワークは、新しい脅威に対応して機能の向上を続けています。第 1 段階の**統合化セキュリティ**では、スイッチやルータなどのネットワーク要素にセキュリティ要素を組み込みました。第 2 段階の**コラボレーション セキュリティ**では、ネットワーク セキュリティ要素間の関連付けを設定し、ネットワークの存在をネットワークに接続するエンドポイントまで拡張します。自己防衛型ネットワークの最終段階では、**Adaptive Threat Defense（ATD）**機能を導入し、新たな一連の**Anti-X**テクノロジに基づいて脅威に対応できるように、ネットワークの機能を拡張します。

自己防衛型ネットワーク のブロック構築

ほとんどのお客様は、自己防衛型ネットワークのすべてのコンポーネントを一度に採用することはないでしょう。第一の理由として、IT サービスの完全性を失わずに、必要なサブシステムのすべてを一度にオーバーホールすることは困難であることが挙げられます。また、もう 1 つの理由は、システムが信頼できる方法で運用されることを確認するまで、自動化システムにセキュリティ制御を引き継ぐことがたいへん難しいことです。自己防衛型ネットワーク構想は、相互に独立して便利に配備できる製品を最初に提供し、各製品やサブシステムに対する信頼が構築されたところで、これらの製品を互いに接続できるソリューションを提供し、こうした懸念に対応します。これらは、製品開発、製品取得、システム開発、提携の組み合わせに依存します。このことを念頭に置いて、自己防衛型ネットワーク構想の現在までの主要なマイルストーンを確認する必要があります。

エンドポイント保護

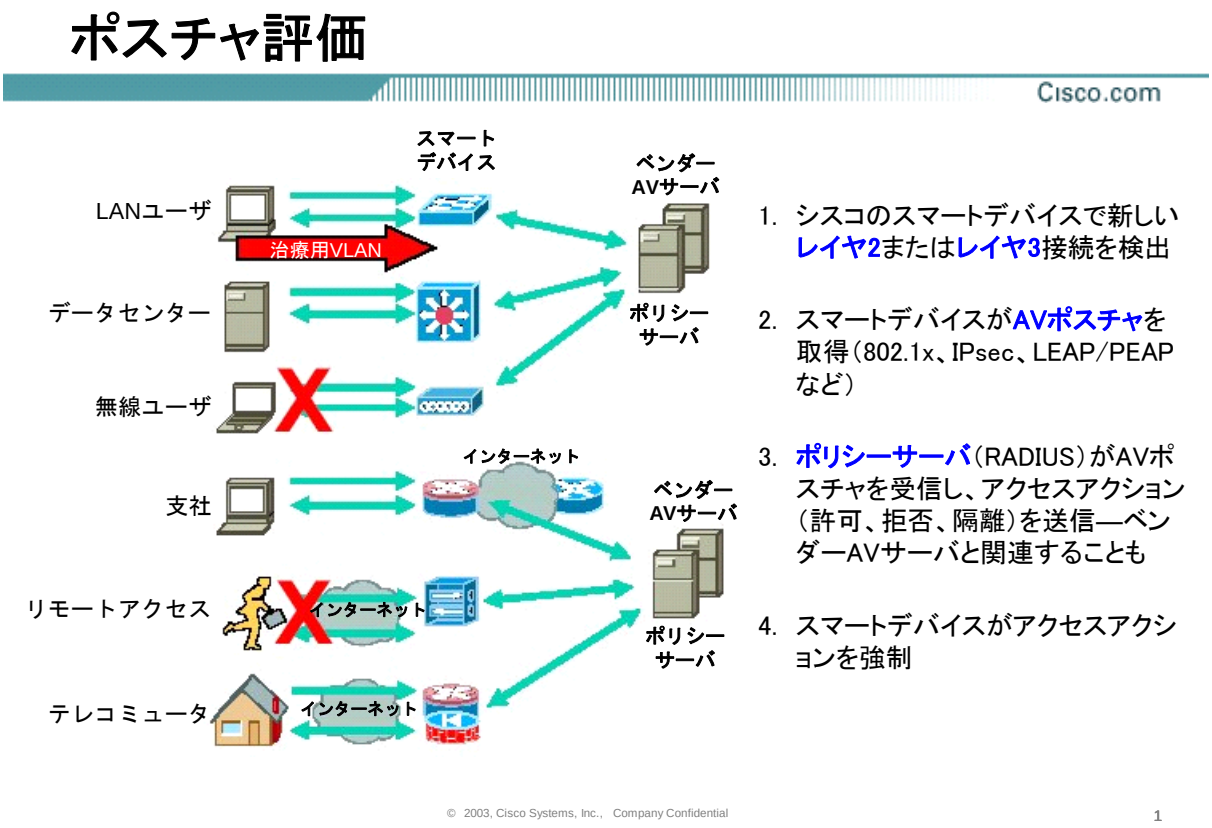
ウィルスやワームの実態として挙げられるのは、急速な伝搬とエンドポイントへの感染の副作用として、しばしばネットワークの輻輳を発生させることです。シスコは、お客様にOkena（現在の CSA； Cisco Security Agent）のエンドポイント侵入防止製品を提供することで、感染と輻輳の両方の問題に対処できると考えました。CSA は、新しい方式の動作セキュリティを使用して、エンドポイント システムに足場を築こうとするウィルスおよびワームを検出し、防ぎます。同時にCSA はウィルスおよびワームがネットワークで伝搬されることも防ぎます。事実上、CSA はウィルスおよびワームの伝搬効果に対する**第 1 の抑制機能**になります。CSAを取得する 2 番目の理由は、1 番目と同様に切実ですが、CSAによってエンドポイントの認識が可能になったことです。ネットワークのエッジで入手できないステート情報を得ることができるようになり、これによって、エンドポイントとネットワークの間のフィードバック ループが確立されるので、発生したばかりの脅威にすばやく適応できるネットワークとなります。

Admission Control （アドミッション コントロール）

自己防衛型ネットワーク構想のなかで、現在のところ最も注目を浴びているものの 1 つが、Network Admission Control（NAC）プログラムです。NACにより、エンドポイントに対して付与するネットワークアクセスのレベルをセキュリティポスチャに基づいて決定することができます。セキュリティ **ポスチャ**に基づくことは、アクセスを要求したユーザのセキュリティ状態だけではなく、オペレーティング システムや使用中のアプリケーションのセキュリティ状態に基づくことになります。NAC はアクセスを制御するほかに、IT管理者にとって、自動的に非準拠エンドポイントの隔離と治療を行う手段となります。エンドポイントがOSのパッチやアンチ ウィルス ソフトウェアのアップデートに準拠していることを確認できるので、ウィルスおよびワームの伝搬効果に対する**第 2 の抑制機能**として効果を発揮します。 (1)

NAC の際立った機能として、お客様が望むエンドポイント セキュリティ製品やポリシーベンダーの製品をクライアントとバックエンド AAA インターフェイスの双方に組み込み、Network Admission Control プレーンを駆動できることがあげられます。
NAC プログラムには現在、30 を超える業界トップクラスのベンダーが参加し、自社技術をネットワークに積極的に組み込んでいます。▼

(1) NAC は、オンデマンドの脆弱性評価およびパッチ管理ツールとして見ることもできます。



NAC 機能を中小規模のビジネスに拡張する必要があります。シスコは Perfigo 社を買収し、Cisco Clean Access という一括販売型コンプライアンスを中小規模のビジネス向けの市場で販売します。（日本では未発表）

Infection Containment（感染の封じ込め）

強力なネットワーク許可ポリシーによってすべてが解決するわけではありません。デバイスがネットワークに追加された後は、監視し続ける必要があります。ハッカーがその気になれば、ほとんどすべてのチェックを回避できます。準拠デバイスであっても、ネットワークのメンバになった後は、ウィルスに感染したコンテンツを保存したUSBキーなど、さまざまな「経路」から感染する可能性があります。結果として、自己防衛型ネットワーク は、アクセス許可時に実行するセキュリティチェックを、ネットワークに接続している間中、継続するように設計されています。問題は、感染した要素が自ら感染を報告してくることにネットワークが常に依存する（信頼する）ことができない点です。自己防衛型ネットワーク は、他のエンドポイントなど、他のネットワーク要素に依存して、別のエンドポイントが「悪い状態になった」ときに検出できるようにしました。これは、911（緊急）コールセンター経由でコミュニティの犯罪を警察が監視しているのと似ています。シスコは感染の封じ込めを、ウィルスおよびワームの伝搬効果に対する**第 3 の抑制機能**と見なしています。

ただし、既存の認証プロトコルは、最初の交換以降に機能するようには設計されていません。そのため、自己防衛型ネットワーク では、デバイスの状態（コンテキスト）を伝達する新しい方法と、推定される信頼および直接の信頼形式に基づいてその情報の信ぴょう性を測定する新しい方法を提供する必要があります。たとえば、管理者は、CSA を実行しているエンドポイントから受信した通知の方が、保護されていないエンドポイントからの通知よりも、信頼できるというルールを作ることができます。こうして、シスコは推定された属性に基づく新しい種類の関連付けとフィードバックの開発を開始しました。

インテリジェントな関連付けおよびインシデント対応

感染の封じ込めなどの恒常的に状態をフィードバックするメカニズムが効果的に機能するように、自己防衛型ネットワークでは、リアルタイムなイベント関連付け、イベントがセキュリティに与える影響の迅速な評価といったサービスを提供し，必要なアクションを決定し、対応を実施する最も近い制御ポイントの識別をするなどの必要があります。そのためにシスコは最近、Protego Networks 社の買収を発表しました。同社の MARS 製品ファミリは、ネットワーク内に存在するさまざまなポイント（ファイアウォール、 ネットワーク型 IDS、ルータ、 スイッチ、 ホスト）からのフィードバックを、レイヤ 2 およびレイヤ 3 ネットワークトポロジを記憶することから取得したコンテキストと、重ね合わせる手段を提供します。この機能によって、Security Incident Response（セキュリティインシデント対応）チームは、ネットワーク上で攻撃が発生している場所を迅速に識別できます。
加えて、シスコは netForensics 社などのパートナー企業と協力して、関連付け機能を拡張し、自己防衛型ネットワークをよりよく監査できるようにします。

インライン IDS と異常（Anomaly）検出

シスコで進行中のセキュリティ開発の重要な分野が Network Intrusion Detection System （NIDS）です。この分野でシスコが最初に行った革新の 1 つが、ルータおよびスイッチプラットフォームへの NIDS の統合です。しかし、NIDS が完全に機能を発揮するためには、インラインフィルタリング機能を具えた Intrusion Prevention System（IPS）に変える必要があります。IPS は、きめ細かくプログラム可能な分類エンジンで、望ましくないトラフィックを除去するメカニズムを提供します。

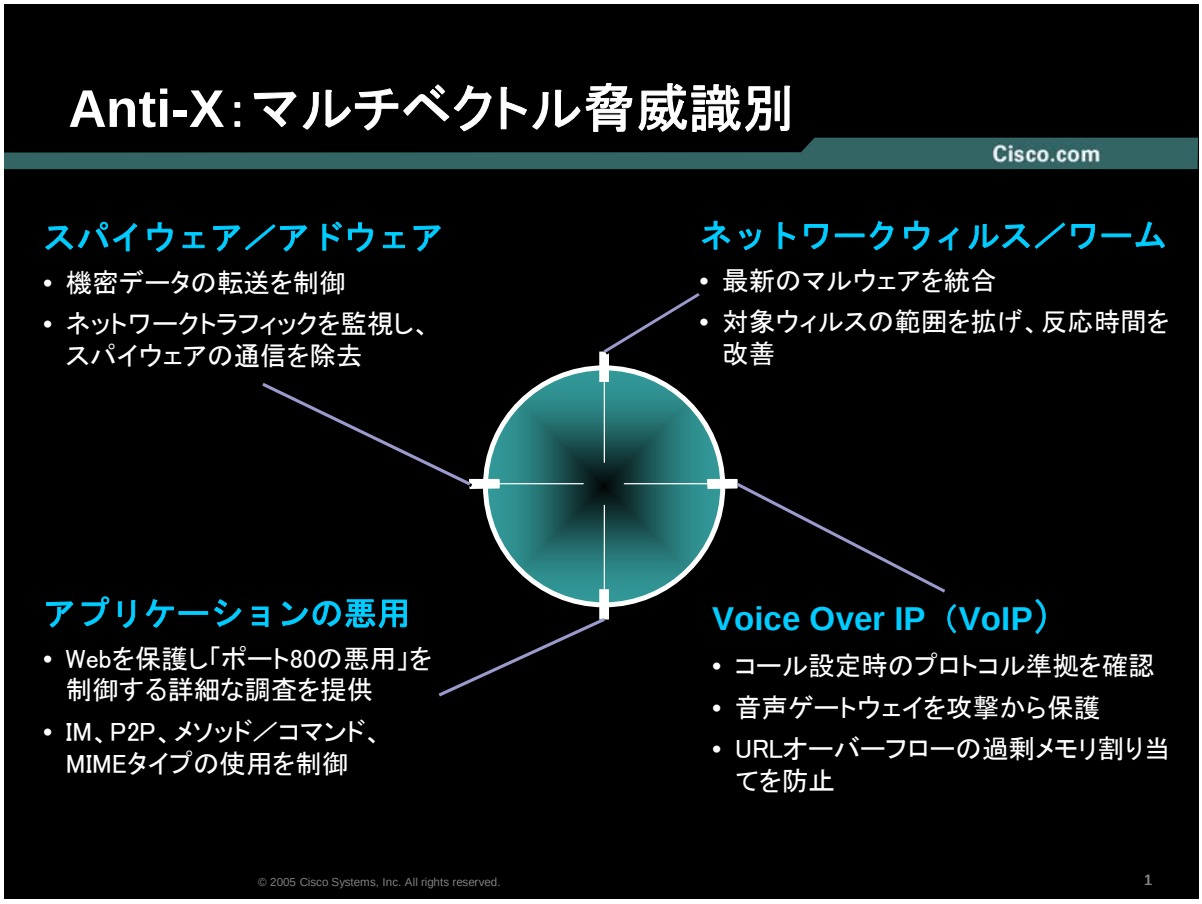
残念ながら、ほとんどの NIDS システムは、インラインセキュリティ サービスとして信頼度の高い運用ができないほどの大量の擬陽性（ログの誤検知）を生成してしまいます。問題の一端は、短い時間で大量の情報（コンテキスト）を組み合わせ、処理する必要があることにあります。特に、アプリケーションベースのプロトコル用に収集する必要がある大量のコンテキストが問題になります。この問題は、特にパケットの転送遅延に非常に敏感な IP テレフォニーなどのアプリケーションに該当します。そのためシスコは、これらのインライン分類エンジンに忠実度の高いシグナリングを送るいくつかの方式を開発しています。

多くの正当なアクティビティが異常と誤認識されることがあります。特に変数の数が多いネットワークに当てはまります。そのため、シスコは異常検出に、慎重な漸増型のアプローチを意図的に採用しました。オペレーティング システムはネットワーク環境よりも簡単にモデル化できるため、まず CSA から着手しました。次に、DoS（denial of service）攻撃のアクティビティは他のネットワーク アクティビティよりもはっきりと目立つため、擬陽性の割合が低いといえます。この DoS 攻撃に効果的なインライン防止システムを製造する Riverhead 社を買収しました。

CSA と Riverhead ファミリの DoS 防御製品で得た DoS 攻撃のパターンから学習した成果に基づき、シスコはインライン IPS（Intrusion Prevent System）を導入します。IPS では、革新的な異常検出技術およびエンドポイントとネットワーク要素の間の状態（コンテキスト）の共有（関連付け）機能を適用することによって、擬陽性の割合を減らしています。また、脆弱性および悪用をタイムリに査定するため、マルチベクトル脅威識別およびメタイベント関連付けを提供します。これらの技術を漸増的に市場に投入し、自己防衛型ネットワークを拡張することによって、これらの機能に対するお客様からのより多くの信頼を得ています。

アプリケーションセキュリティと Anti-X 防御

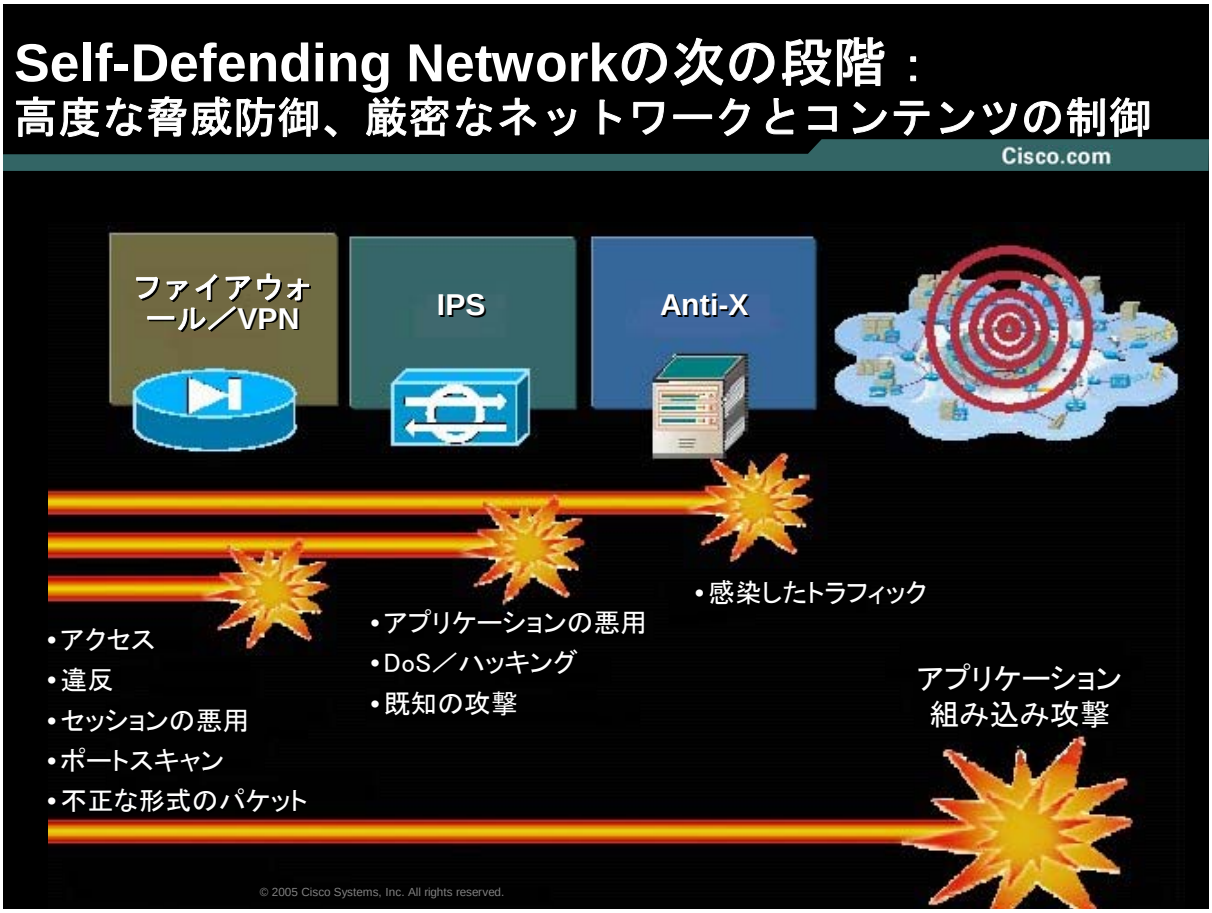
過去数年にわたり、旧式のファイアウォールおよび NIDS製品では適切に処理されない新しいクラスの脅威（**ウィルス、ワーム、E メール ベースのSPAM、フィッシング、スパイウェア、Webサービスの悪用、IPテレフォニーの悪用、不正なピアツーピアアクティビティなど**）に対応するために、多くの新しいアプリケーションレイヤネットワーク製品が現われました。シスコは、このような種類の脅威および悪用に対処するために、次世代のパケットおよびコンテンツ検査セキュリティサービスを開発しました。この統合は、主要なネットワーク セキュリティ実施ポイントにきめ細かいトラフィック検査サービスを導入することで、ネットワーク全体に伝搬される前に悪意のあるトラフィックを封じ込めます。



これらのサービスをマルチサービス プラットフォームに統合することは、ベンダーの刷新と同時にお客様のライセンス所有コストの削減をもたらす好機です。アプリケーションがエンドツーエンドの暗号化を採用している場合、自己防衛型ネットワークでは、ネットワークのエッジで失われる可視性を補完するために、エンドポイントから情報を収集できます。

次のステップ

シスコは、エンドポイントシステムまでとエンドポイントシステム自体を含み、ネットワークをまたがるプレゼンスのポイント間を関連付ける自己防衛型ネットワークの構築に重点的に投資を続けます。これによってシスコは、組織のインフラストラクチャで通信するデバイス、ユーザ、およびアプリケーションの可視性および制御性を高めることができます。これは、通信ファブリックによるパケット転送にインテリジェント ルーチングプロトコルが期待されたのと同様に、以前からネットワークに期待されていた必要で重要な進歩です。



この文書では、自己防衛型ネットワークについて簡単に説明しました。現在可能なことについて理解するためにも、また将来のセキュリティおよびネットワーク デザイン プロジェクトの基礎を築くためにも、継続的なより深い探求が必要です。何を選択するかは、各組織が日々直面している固有のセキュリティ、リスク、コンプライアンスの問題によって異なります。

- ネットワークの境界領域のセキュリティ担当の方は、最近発表された PIX7.0 と Integrated Service Router（ISR）プラットフォームをご参照下さい。詳細なデータの検査と、さまざまなプロトコルとそれに伴う攻撃経路の制御ができます。その他にも多くのセキュリティ機能とネットワーキング機能についての情報があります。
- セキュリティサービスを運用されるグループの方は、インシデントに対応するため、非合理的で過剰な労力を費やしておられることと思います。Protego 社から新しく取得した技術を調査、参照いただき、インフラストラクチャとセキュリティ装置の新しいインライン侵入防止機能についてご検討ください。
- 頻繁に DoS や DDoS 攻撃に対処されているデータセンター等のサーバ管理、システム管理の責任者の方は、Riverhead 社から取得した Anomaly Guard（異常検知、防御）技術をご参照ください。
- ワームやウィルスの影響を受け続けている組織、またはエンドポイント コンプライアンス ソリューションを必要とされる組織は Cisco Security Agent、 Network Admission Control および Perfigo から取得した Cisco Clean Access をご参照ください。
- 法的準拠の評価をご担当の監査者は、通信インフラストラクチャ全体の使用に関する詳細情報を提供するツールである Cisco Works SIMS のほかに、NAC もご検討ください。

最後に、セキュリティシステムおよびネットワークインフラストラクチャの設計および配備を担当される皆様には、各地域のシスコパートナー各社及びシスコの担当営業に、自己防衛型ネットワークの詳細と、IT 環境に与える有意義な効果について問い合わせていただきたいと思います。

■この文書の原文：

Core Elements of the Cisco Self-Defending Network Strategy

http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns413/networking_solutions_white_paper0900aecd80247914.shtml

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

05.02