

## エクストラネットのセキュリティとビジネスの活用について

2008年1月



今日のビジネス活動において、ネットワークの利用は必要不可欠な要素です。取引先企業とデータやアプリケーションを共有し、コラボレーションを加速するためには、自社と取引先企業間を結ぶネットワーク(エクストラネット)が高い可用性や機密性を維持し、ビジネス環境へ柔軟に対応する必要があります。また、このようなネットワークを活用させ運用するためには、ITガバナンスやセキュリティポリシーを徹底させて、アーキテクチャアプローチにのっとりエクストラネットを構築しなければなりません。

### 1. ビジネスにおけるネットワークの変化

インターネットは1991年に米国で商用目的に開放されて以来、ビジネスにおいて必要不可欠な存在になりました。今日、企業のネットワーク利用の内訳は、一般消費者とのコミュニケーションに使用するインターネットに加えて、自社内のみで利用するイントラネット(企業内通信)、取引先企業とのコミュニケーションのために使われるエクストラネットに大別されています。

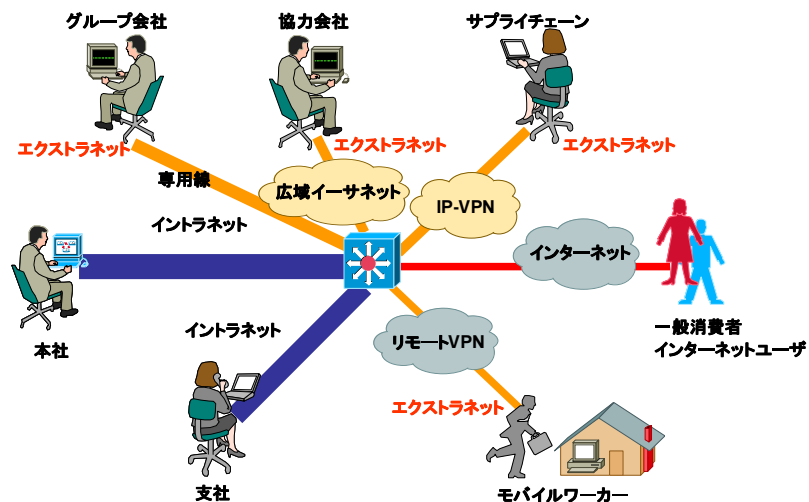


図1-1 ビジネスにおけるネットワーク概念図

## 2. エクストラネットの重要性

多くの企業は安全な拠点間通信を実現するために、コストの面からWAN上にVPN(仮想プライベートネットワーク)という論理的な専用線のネットワークを構築し、それを利用します。しかし最近ではユニファイドコミュニケーションやテレプレゼンスのような、通信の遅延へ敏感に対応するソリューションを導入する企業が増えており、WAN選択の際にはサービスレベルを検討する必要があります。

また、保険会社のような営業をアウトソーシングしている業種では、最新の高機能な携帯電話や無線LAN機能付のPDAを利用して外出先からエクストラネットにアクセスする需要が高まっています。さらに、目まぐるしく変化するビジネス環境において、エクストラネットは長期間の接続に限らずプロジェクト単位で期間、接続先、そしてアプリケーションを柔軟に変更しながらネットワーク内部の情報を共有したりアクセスに制限をかけたりする必要があります。

## 3. ITガバナンスとセキュリティポリシー

上記のようなビジネスの変化や世の中のセキュリティ脅威に対応できるエクストラネットの実現のためには、まずITガバナンスを徹底させセキュリティポリシーの構築が大切です。しかし、エクストラネットの普及に伴いITガバナンスが徹底されていない、またセキュリティポリシーの構築やネットワークの設計、運用プロセスが不十分であるために、ビジネスの変化や日々変化する現在のセキュリティ脅威に対応できないといったケースをよく耳にします。

エクストラネットに限らず、ネットワークに新しい機能要件を追加や修正をする際は、その管理、運用の負荷を最小限にとどめながら図3-1のようなプロセスで新しい機能要件の適用を行う必要があります。

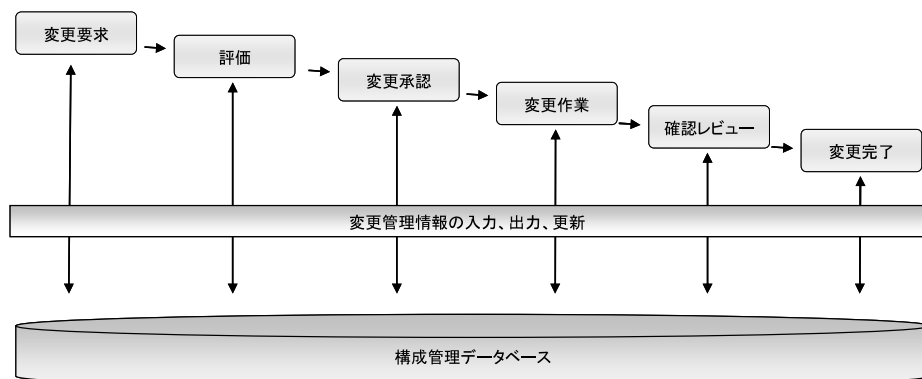


図3-1 ネットワークの変更管理

プロセスの不備がエクストラネットのセキュリティのボトルネックにならないために、ITガバナンスを徹底し、セキュリティポリシーを構築することが重要です。また変更管理や運用を意識し、アーキテクチャアプローチに基づいたネットワークポロジータを設計することが重要になります。

加えて、金融商品取引法(日本版SOX法)では、COBIT 4.1に沿ってIT全般統制が行われようとしています。その中のドメイン3である、「供給とサポート(DS: Deliver and Support)」の5に「システムセキュリティの保証」が記載されています。その記載の中には、ネットワークの不正アクセスへの防止措置やセキュリティ事象のモニタリングや報告が義務付けられており、このようなコンプライアンスを意識したネットワークの設計や運用も必要です。

#### 4. エクストラネットにおけるセキュリティ脅威

年々巧妙になっているアタック手法に応じてインターネットにおける脅威の傾向も変わってきています。表1はComputer Security Instituteが発表した、過去1年間のセキュリティ脅威の傾向を示したものです。従来から脅威とされていたウイルスによる被害以上に、内部もしくは関係者による不正アクセスによる影響が急増していることがわかります。

表 4-1 CSI Survey 2007 Figure 14 より

Types of Attacks or Misuse	割合
Insider abuse of Net access 内部の人間によるネットワークの不正使用	59%
Virus ウイルスによる被害	52%
Laptop / mobile device theft ノートPCや携帯端末の盗難	50%
Phishing where your organization was fraudulently represented as sender フィッシング	26%
Instant messaging misuse インスタントメッセージャーの悪用	25%
Denial of service サービス妨害	25%
Unauthorized access to Information 不正アクセス	25%
Bots within the organization ボットネット	21%
Theft of customer / employee data 顧客や社員データの盗難	17%
Abuse of wireless network 無線LANの不正使用	13%

エクストラネットは限られた取引企業間で扱われる比較的保護されたネットワークではありますが、上記のセキュリティ脅威がエクストラネットにまで影響を及ぼす可能性があるため、セキュリティ脅威としてはインターネットに近いレベルまで想定する必要があります。特に上記統計の上位を占める脅威を想定し、その対策案を適用することがエクストラネットを利用したビジネスの成功条件となります。

##### 4.1. エクストラネットで想定される脅威

###### • サービス妨害攻撃

攻撃者は高度に自動化されたツールを使用し、大量の不正パケットを特定のサーバやセグメントに送りつけることで、エクストラネットで提供されるサービスを低下させ、場合によってはそのサービスを使用不可能にすることがあります。

###### • 不正アクセス

正規のアクセス権をもたない人による、ソフトウェアの脆弱性や不具合を利用したアクセス。接続が認められていない端末による不正アクセスは情報漏えいなどの被害を引き起こす場合があります。

- **IP スプーフィング**

不正侵入の方法のひとつであり、信頼されている内部ネットワークの端末になりすまして、必要とされる認証をバイパスしたり、アクセスが制限された情報資産に不正アクセスしたりすることがあります。また、サービス妨害攻撃の際に、送信元の身元を詐称するために使われることもあります。

- **パスワードクラック**

他人やアドミニストレータに属するパスワード情報を解析して探り当てる行為のことであり、サーバやホストだけではなくネットワークデバイスに対しても行われます。特に暗号化されていないトラフィックをパケットスニファなどのキャプチャリング機能により盗聴し、トラフィック内の個人情報よりパスワードを特定する場合があります。

- **ウイルス、トロイの木馬およびスパイウェアによる攻撃**

メールに添付されているファイルの開封やアプリケーションのインストール、Webサイトへのアクセスなどをきっかけに、ユーザが気づかぬうちにコンピュータに侵入し、自身の複製やコンピュータの利用調査、そして外部からの不正アクセスを許可するバックドアの設置などを行い、場合によってはボットネットの一部として活動することで自らが加害者になる場合があります。ウイルスによる感染はコンピュータをクラッシュさせ、使用不可能な状態にする場合があります。これらは俗にマルウェアと呼ばれ、新機能をダウンロードすることで成長するダウンロード型マルウェアは、駆除しない限り悪意ある活動を継続します。

- **P2P ネットワークへの情報漏えい**

ユーザが自身のPCにインストールしたアプリケーションが脅威の原因となるケースがあります。エクストラネット内で取り扱われている機密情報が、Winny などのP2P 型ファイル共有ソフトやIM(インスタントメッセージ)の誤った使用方法によって流出してしまったり、またこのようなアプリケーションを経由して、マルウェアがPC内に侵入し、新たな被害を引き起こしたりする場合があります。

- **第3者による改ざん、中間者による偽装攻撃**

通信を行う二者の間に割り込んで両者の情報を自身の情報と効果的にすり替えることで、両者に気づかれずに情報の盗聴やその情報の改ざんをする場合があります。

## 4.2. エクストラネットのデザインにおいて考慮すべき点

ネットワークの一般的な位置づけとして、エクストラネットはイントラネットとインターネットの中間に位置するものです。提供されるサービスの柔軟性と適用すべきセキュリティは常にトレードオフの関係にあります。現在のビジネス環境においては両立を求められます。昨今のビジネス形態からエクストラネットはビジネス上必要不可欠であり、今まで以上に柔軟に対応可能で、運用しやすい形態を求められます。つまり、エクストラネットを設計する上では、必ず次の要件をバランスよく検討することが重要です。

- セキュリティ
- 拡張性
- 冗長性、可用性
- 管理、運用性

第1に、プロアクティブなセキュリティアプローチを施して、ビジネスに多大な影響を与える脅威を防ぐ必要があります。要件に応じたフィルタルールを適用するだけでなく、適用箇所や適用内容の最適化、既存ルールとの整合性を常に確認する必要があります。

第2に、接続規模の大小や多数の接続を収容する拡張性が不可欠です。あらかじめ想定するエクストラネットの規模とそのキャパシティプランニングを実施し、随時収容構成を検討するために消費される時間やコストを軽減します。

第3に、これらのビジネスを支えるインフラとして、要件に応じたサービスレベルとネットワークの可用性が求められます。

そして第4に、管理の容易さと運用のプロセスです。接続するビジネスパートナーの増加やその接続に対して適用するルール管理、そしてACLの申請から適用にいたる運用プロセスの整備、特に過去に適用したACLの有効性の確認や削除のプロセスが不明瞭であることから、メンテナンスが困難になり、結果的にコストが増大する可能性があります。

これらをすべて網羅するためには、エクストラネットを単なるコアネットワークへの接続部分としてのポイントで見るのではなく、アーキテクチャとしてネットワーク全体でとらえることが成功への鍵となります。

## 5. エクストラネットの接続形態

エクストラネットを含めた企業間のネットワーク接続形態は、相手のビジネス要件やIT要件によって、大きく次の4つに使い分けられています。

### (1) DMZ接続

一般的なインターネットへのサービス提供形態がエクストラネットに応用される場合があります。DMZ上にエクストラネット サービスを提供するサーバを構築し、サーバ自身のVPN機能を使用することで拠点間VPN接続と同等のセキュリティを確保したサービス提供が可能です。各サーバ単位での実装となるため拡張性に欠けますが、容易に実装できることから提供するサービスが比較的限られている場合に使用されることがあります。

### (2) VPN接続

専用線での接続に対し、インターネット上をVPN接続することにより論理的な専用線を構成します。本方式は費用対効果が高く、安価にセキュリティを確保した接続を構成できることから多くの企業で採用されています。一般的には拠点間VPN接続が使用されていますが、PC上のVPNクライアントソフトウェアを使用したリモートアクセスVPNを併用することで、ユーザ数の少ない取引先企業の効果的な収容を実現します。

### (3) 専用WAN接続

専用のWANを構成する場合、そのエクストラネット サービスに要求されるパフォーマンスや信頼性、そしてコストを検討し、回線の選択や冗長化構成の選択を行います。またその回線上でのサービスレベルをその取引先企業ごとに柔軟に設定し、クリティカルなサービスへのプライオリティを上げるなど、サービスを種別することにより適切なサポートリソースの投入計画につながります。

### (4) 社内LAN接続

オンサイトでの作業形態の普及や企業間の業務委託契約の増加から、社員以外の作業者を通常の社内LANエリアに直接接続させるケースが増加しています。その際、いかにセキュリティを確保できるかが大きな課題となります。同様の形態は一時的な協力関係である場合や、ゲストアクセス用のネットワークを提供する場合にも用いられます。

## 6. エクストラネットのネットワークポロジ

セキュリティポリシーの適用や明確な運用ポリシー実現のためにはエクストラネットのネットワークポロジを同等のセキュリティレベルの単位で分割し、ネットワークにモジュール化して組み込むことが必要です。モジュール化することで、統一したセキュリティルールや可用性要件を適用することが容易になり、運用時の変更や管理が容易になります。大きく分けて、Outside ExtranetモジュールとInside Extranetモジュールの2つのトポロジについて紹介します。

### (1) Outside Extranetモジュール

図3のような、社内LANから明確に分離できる旧来のエクストラネットつまり専用線を経由したWAN接続やVPN接続をするケースです。

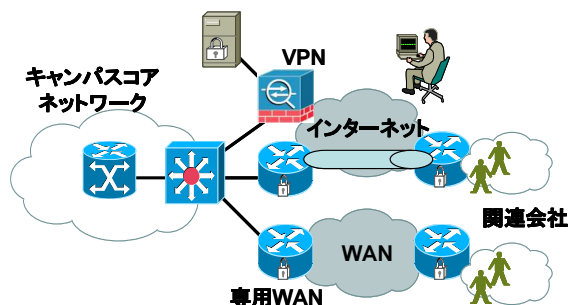


図6-1 旧来からのエクストラネット

WANのエッジとなるセグメントから専用線またはインターネットを経由したVPN接続により実現します。拠点間はIP SecやSSL VPNによる暗号化、リモートアクセスVPNにおいては証明書やユーザベースの認証を実装し、接続ポイントにおいてはFirewallまたはACLによるアクセスコントロールを行います。エクストラネットに配置される関連会社間の通信を制御するために、Virtual Firewall機能を使用されるケースもあります。一般にこれらの終端装置はコアから分離されたセグメントモジュールとして收容され、モジュール単位またはVirtual Firewallのコンテキスト単位でポリシーを適用・管理します。

### (2) Inside Extranetモジュール

図4のような取引先企業の社員が、外部ではなく社内のキャンパスLAN内に直接接続して、業務上必要なリソースにアクセスするケースです。Partner Intranetと呼ばれる場合もあります。

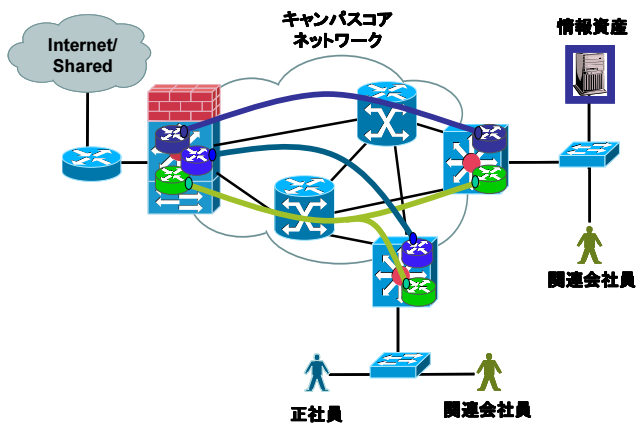


図6-2 Inside Extranet ネットワーク

接続形態としては、有線接続と無線接続があります。どちらのケースでもセキュリティを確保するために、VLANによる收容個所の分離と、社内LAN接続のための認証が使用されます。認証には802.1xを使う場合やNAC(Network Admission Control)による方法が挙げられます。認証時にそのユーザや接続デバイスに適切なVLANのアサインをして、アクセスコントロールを動的に行います。デバイス認証においては、そのデバイス上のセキュリティパッチやウイルス情報定義ファイルの適用状況に応じたアクセスコントロールを実施します。ネットワークインフラ上にスタティックにVRF(Virtual Route Forwarding)を構成し、それをVLAN単位に適用することでTrafficだけでなくルーティング情報も完全に分離する方法をとる場合もあります。VRFをVirtual Firewallのコンテキストとマッピングすることで、論理的に完全に独立したセグメントを構成することが可能になります。

## 7. ネットワーク セキュリティ アーキテクチャ

エクストラネットを構成するセキュリティ、拡張性、冗長性/可用性、管理/運用性を実現するためには、ネットワークをセキュリティレベルでモジュール化し、そのモジュールごとに必要な要素を含める必要があります。以下に各モジュールで実装すべき機能について紹介します。

### (1) エクストラネットWANモジュール

取引先企業との適切なサービスレベルを維持するためには、適切な回線業者の選択が不可欠です。回線を提供するサービスプロバイダ側のサービスレベルに応じて可用性設計が明確になります。またサービス妨害攻撃対策やウイルス対策を提供するサービスプロバイダを選定することで、ユーザ側で実施すべき対策項目を軽減できます。専用線で接続されているものの、その先から接続してくるユーザは明確に指定することが難しいため、FirewallやACLによる適切なフィルタリングやアンチウイルス ゲートウェイによるウイルスチェックを実装します。そしてIPSによって不正トラフィックを常時監視することでセキュリティ インシデント発生時における早期対応を可能にします。

### (2) エクストラネットVPNモジュール

インターネットを経由し接続するVPNにおいては、上記エクストラネットWANモジュールに加え、IP SecやSSL Tunnelによる通信の保護が必要になります。IP Secにおいては、通信の暗号化による秘匿性の確保だけでなく、接続先サイトの認証とデータが、改ざんされていないという完全性を保証します。暗号化はより強度な暗号方式としてAES(Advanced Encryption Standard)の採用が一般的ですが、その暗号キーをやり取りするインターネット鍵交換プロトコル(IKE: Internet Key Exchange)についても、より強固なIKE Version 2がRFC4306で規定されています。認証においては事前共有鍵(Pre-Shared Key)の採用が一般的ですが、より強固なセキュリティを実現するためには証明書による認証が不可欠であり、拡張性の点からも推奨されます。

### (3) パートナーイントラネットモジュール

イントラネット外からのアクセスは境界部分でセキュリティ ゲートウェイによるポリシーの適用が容易ですが、社内イントラネットに直接接続する場合、通常はそのフロアスイッチまたはアクセススイッチで收容されます。そのため、仮に問題が発生した場合のモジュール外への影響をおさえ、被害を極小化するために、そのアクセススイッチまたはそのモジュール境界でセキュリティポリシーを適用する必要があります。そのひとつとして挙げられるNACは、接続するデバイスのセキュリティパッチの適用状態によって適用するルールを決定するアドバンスドセキュリティ機能を提供します。また802.1xなどによるユーザ認証やMACアドレスによる端末認証を併用し、接続する端末、ユーザ固有の情報を識別します。接続するビジネスパートナーごとに接続するVLANを割り当て、そのVLANと必要なリソースへのフィルタリングルールの適用やVirtual Firewallコンテキストへのマッピングをそのモジュールとコアとの境界で実施します。

#### (4) エッジモジュール

それぞれのエクストラネット モジュールを一括して收容するのがエッジモジュールです。ここでは個々のビジネスパートナーごとのフィルタリングルールだけではなく、コアから社内イントラネット内のリソースへのアクセスをFirewallやACLにてコントロールします。ビジネスパートナー単位にVirtual Firewallをアサインし、そのコンテキストに一般的な接続ルールとビジネスパートナー特有のルールを階層的に適用する管理製品を併用することで、ルール管理に費やされるコストが軽減されます。またこのモジュールには、IPSを設置し、アクセスを許可されたデバイスからの不正な活動を監視することが望まれます。

#### (5) コアモジュール

ビジネスを支える屋台骨として、コアモジュールはセキュリティ侵害の影響を受けない強固なインフラとして高い可用性が要求されます。単なる機器の冗長化だけではなく、CoPP (Control Plane Policing)やInfrastructure ACLなどの自衛機能によるデバイス自体の堅牢化と、スイッチネットワーク特有の脅威に対して、ARP InspectionやIP Source Guard、Port Securityといった機能が有効となります。またインフラ自体のセキュリティを高めるために、ルーティングプロトコル セキュリティの実装やNetFlowでトラフィックの使用状況を視覚化し、トラフィックの適正利用を確認します。

#### (6) サーバモジュール

ビジネスの最も重要なリソースが配置されるサーバモジュールには、他のモジュール以上に高いセキュリティレベルが要求されます。また提供するサービスという点からもアプリケーションレベルでのセキュリティを実装する必要があります。ウイルスなどの悪意ある振る舞いを検知するホスト型IPSは、サーバ自体を不正なアクセスやデイズロアタックから保護するだけでなく、新たなセキュリティパッチをサーバへの適用準備期間を与えることができるため、計画的なメンテナンスを実現し、提供するサービスの利用時間を最大化します。Webアプリケーションに潜む脆弱性を多層的に防御することが最も重要です。

#### (7) ネットワーク管理モジュール

上述したネットワークデバイス上のセキュリティ機能を管理/運用していく仕組みが不可欠であり、これらの機能は一般にネットワーク管理モジュールに配置されます。各FirewallやACLのルールやポリシーの一元管理や認証/承認/アカウント管理が要求されます。こういった作業は運用プロセスのワークフローに沿ったツールの利用が効果的です。そしてFirewall、IPS、VPNデバイス、ルータ、スイッチ、ホストIPSからのセキュリティ イベント情報を一元的に収集/分析し、発生しているセキュリティインシデントを早期に発見する仕組みづくりが不可欠となります。

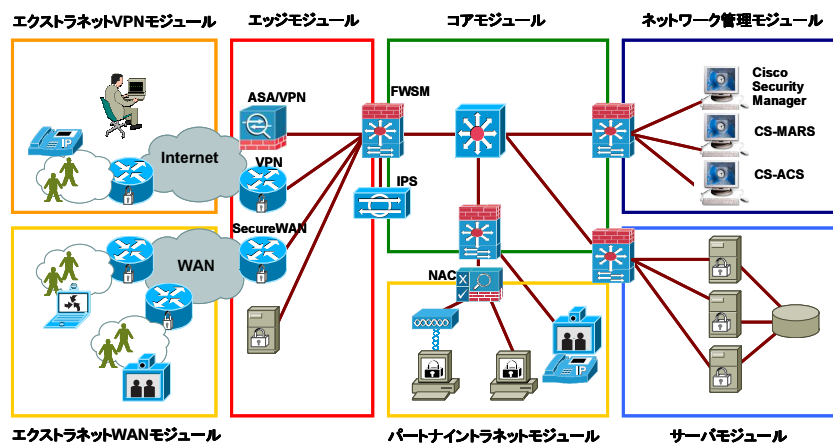


図7-1 Extranet/Campusネットワーク セキュリティアーキテクチャ

## 8. 現状分析とそのチェックポイント

これまでに述べてきたアーキテクチャ アプローチを実施するにあたり、まず必要なのは既存のエクストラネットがセキュリティ、拡張性、冗長性、管理性といった観点からどのような問題点を抱えているかを調査、整理することです。調査はネットワーク構成やデバイスのコンフィギュレーション、そしてセキュリティポリシーや運用体制に対しても行う必要があり、現状と目指すべき方向のギャップを正確に分析することが重要です。

次に整理された問題点に対して、ITガバナンスの強化、セキュリティポリシーの見直し、ネットワークのデザイン、セキュリティ技術の採用を別途検討していく必要があります。さらに、ユニファイドコミュニケーションなどのビジネスコラボレーションを加速する、最新の技術動向やセキュリティ動向を加味していくことで、ビジネスを牽引するエクストラネットの実現につながります。

### Extranetセキュリティのチェックポイント(例)

- Extranet として独立した専用モジュールになっていますか？
- Extranet に関するセキュリティポリシーが存在しますか？
- Firewall やACL等によるトラフィックフィルタリングが実装されていますか？
- Firewall やACLは特定のビジネスパートナーからの特定のトラフィックだけを許可していますか？
- Firewall やACLはExtranetシステムと内部ネットワークの間に存在していますか？
- Extranet のサーバから外部への接続は制限されていますか？
- Firewall やACLはきちんとメンテナンスされていますか？
- Firewall ルールは監査されていますか？
- Extranet へのトラフィックはIDS/IPSにて監視されていますか？
- Extranet はHost IPSにて保護されていますか？

## 9. シスコのセキュリティ対策の考え方

単一のセキュリティ対策だけでシステムのアクセス制御をした場合、そのセキュリティ対策に不備があって攻撃者がセキュリティを突破したときには、セキュリティのリスクが一気に高まります。

そこで同様の機能を持つセキュリティ対策を異なる層で実装し、二重、三重の防御体制を推奨します。

たとえば「ワームによる脅威」の場合、セキュリティ対策の層の上層から次の対策をとることができます。

- セキュリティポリシー層の教育(情報)による、正しいワーム対策の周知
- ネットワーク境界部層に置いたセキュリティゲートウェイによるワームの遮断
- 内部ネットワーク層における Layer2, Layer3 デバイスでのワームの遮断
- ホスト層の PC におけるホスト型侵入防御ソフト、アンチウイルスソフトによるワームの遮断
- アプリケーション層のプログラムのセキュアコーディングによるワームの無力化

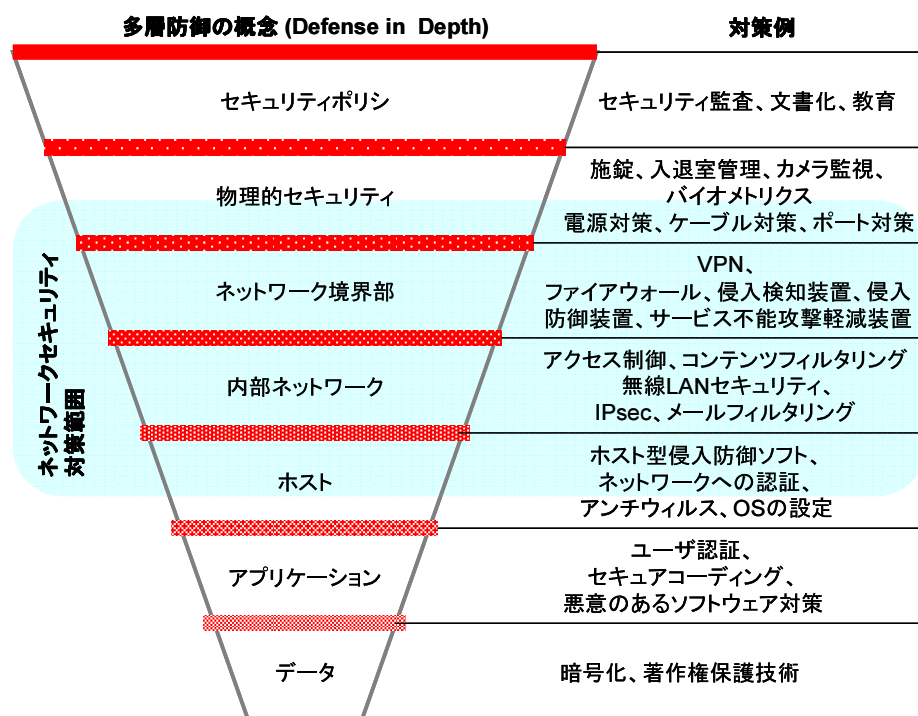


図9-1 多層防御(Defense in Depth)の概念

## 10. シスコが提供するセキュリティサービス

セキュリティ要件は、単にセキュリティソリューション製品を導入することで解決できるものではありません。お客様のビジネスにフォーカスしたプロセスにおいて体系的にアプローチすることが必要です。

シスコは、ネットワーク環境におけるセキュリティ面に不安をお持ちのお客様や、新たにシスコのセキュリティソリューション製品を導入するにあたり不安をお持ちのお客様に対して、セキュリティの観点からアセスメント、コンサルティング、デザイン、そしてセキュリティソリューション製品の導入支援を行うセキュリティサービスを提供します。このサービスは「準備」、「計画」、「設計」、「導入」、「運用」、「最適化」の6つの基本フェーズからなるネットワークライフサイクル<sup>※1</sup>を基盤とし、パートナー様をご担当されるシステム構築案件を各フェーズにおいて強力にバックアップいたします。また、ソリューション製品の導入だけでなく、お客様のネットワーク環境の安全の度合いを判定し、助言を行う「脆弱性検査」サービスや、セキュリティ強度を高めるための「ネットワーク設計」サービスも提供いたします。

シスコ アドバンスドサービスでは、CCIEだけではなく、セキュリティの専門資格であるCISSP、ISMS審査員、BS7799、情報セキュリティアドミニストレータ、CompTIA Security+ などを持っています。セキュリティコンサルティングやセキュリティアセスメント、そしてセキュリティ監査経験を持ち、セキュアなネットワークを設計した経験を豊富に持つ、専門のネットワークコンサルティングエンジニアが、これらのサービスを推進し支援させていただきます。

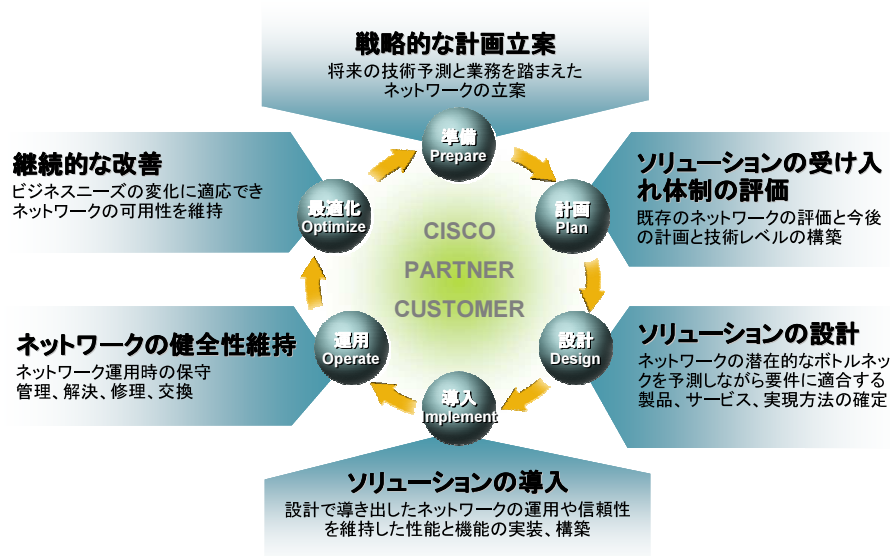


図10-1 シスコが提唱するネットワークライフサイクル<sup>※1</sup>

<sup>※1</sup> ネットワークライフサイクルとはネットワークに新しい機器や技術が追加され、ネットワークが成熟していくに伴い、さらに新たに登場する新しい機器や技術を導入していく反復的で継続的なネットワークの成長や拡大のフェーズもしくはステージを表しています。

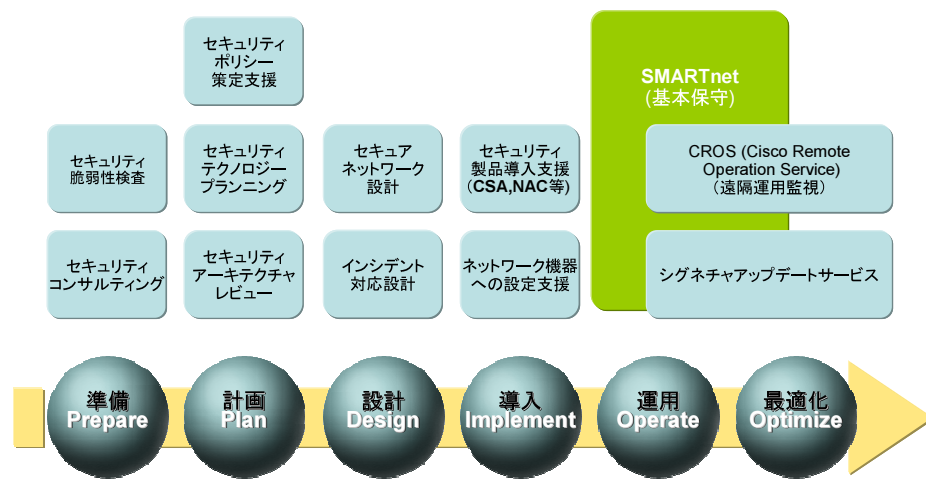


図10-2 シスコが提供するセキュリティサービス

シスコシステムズ合同会社  
アドバンスドサービス  
セキュリティ プラクティス

©2008 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0704R) 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。



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

お問い合わせ先