

ファイアウォール ～安全性の意味と代償～

二木 真明(エスシー・コムテクス)
Internet Week 2002
チュートリアル T11

このセッションの目的

- ファイアウォールという概念、考え方の理解
- ファイアウォールのしくみの理解
- ファイアウォールに出来ることできないことの理解
- セキュリティの枠組みからみた位置づけの理解
- ファイアウォールを導入することのメリット、デメリットの理解
- 統合管理・監視の考え方へのアプローチ

ファイアウォールの概念

- Firewall = 防火壁というよりは防火ドア
 - 何かを通す必要がなければ「壁」でいい
 - あけることが必要だから「ドア」
 - ドアを開ける = 延焼のリスク
- Firewall = 検問所
 - セキュリティポリシーの異なるネットワークを相互接続するためのセキュリティゲートウェイ
 - それぞれのポリシーを維持しながら通信する

ファイアウォールの「内側」「外側」という言葉のまやかしに注意が必要。

必ずしも「内側」=「安全」ということにはならないし、場合によっては「外側」より危険なケースもある。

ファイアウォールの仕事

- 基本的な仕事(かならず備えるべき機能)
 - ルータもしくは中継装置としての仕事
 - 通過させていい通信かどうかの判断と通過させてはならない通信の排除
 - 危険な兆候の検出と警告
 - 通信の許可、不許可状況などの記録の保存

必ずしも、「ルータ」である必要はない。アプリケーションを「中継」できれば可。(アプリケーションゲートウェイ:後述・・・もあり)

「記録」も重要な仕事であることに注意(意外と忘れがち)

ファイアウォールの仕事

- あると嬉しい機能(きちんと動かならば・・・)
 - ユーザ認証機能
 - IP アドレスではなく、ユーザ名、パスワードまたは電子的な証明書による認証とアクセス許可の機能
 - コンテンツの内容検査
 - ウイルスチェックや通信内容の検査
 - VPNゲートウェイ機能
 - IPSec 対応機器などとの相互通信
 - 侵入検知機能または侵入検知との連携
 - 検出した不正な通信をブロックする機能

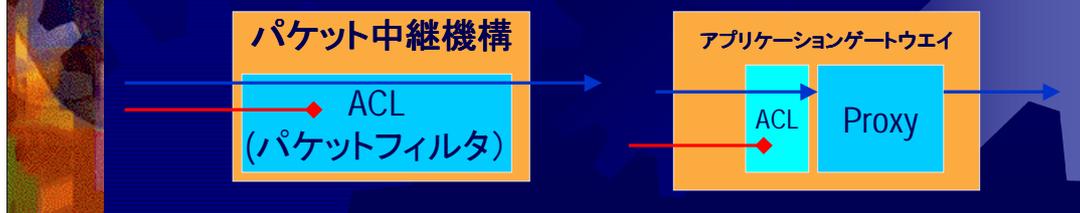
通信の中継機能

- 大別して2種類の方式がある
 - パケットフィルタ方式
 - ルータとしてIPパケットを中継することで、通信を行いたい機器同士が直接通信できる方式
 - アプリケーションゲートウェイ方式
 - Proxy (代理)サーバに一旦接続して、接続相手を指示して代理通信させる必要があるため、Proxy方式とも呼ばれる。
 - 直接的なパケット中継は行わず、要求を受けたProxyが相手方と通信して必要な情報を取得してから受け渡す方式。

たとえば図書館で、いわゆる「開架方式」と「閉架方式」の閲覧方法の違い。自分が直接本を取って来ることができるか、係りに頼んで出してもらおうかの違いと言える。

通信の許可、不許可

- 通信の発信元、相手先のIPアドレスやポート番号で許可、不許可を判断
 - ACL (Access Control List) の適用
 - パケットフィルタ方式では、フィルタ定義としてACLを適用する。
 - アプリケーションゲートウェイ方式では、Proxyサーバごとにアクセス許可情報としてACLを適用。



これがファイアウォールのもっとも基本的な仕事。いずれの方式も特定のサービスに対するアクセスの可否を決定し、強制できるが、パケットフィルタ方式では、一括した(すべて許可・禁止)的な記述が可能であるのに対し、アプリケーションゲートウェイでは、Proxy すなわちサービス単位での許可、不許可となる。

従って、パケットフィルタでは、とりあえず全部通しておこう・・・といった暫定措置が可能なのに対して、アプリケーションゲートウェイでは、Proxy が用意されているサービス以外は基本的に通せないため、あらかじめポリシーをきちんと決めないと導入が困難。(これが「安全さ」の所以かもしれないが)

危険な兆候の検出と警告

- 通信拒否の頻発
 - なんらかの攻撃的意図を持った通信の疑い
- 不正な形式のパケットの検出
 - 発信元詐称パケット(内部アドレスを詐称)
 - ソースルーティング指定パケット
 - 一部のTCP/IP層レベルの攻撃パケット
- 不正な通信内容(アプリケーションレベル)
 - セキュリティホールへの攻撃など
(IDS 的機能)

監視機能は「欲張ればきりが無い」＝「性能とのトレードオフ」であることに注意。

どちらかといえば、IDSとは違って、アプリケーションレベルの攻撃・異常よりも、TCP/IP
プロトコル(L3/L4)レベルの検出が中心。(特にパケットフィルタ系)

アプリケーションレベルでの検知は特に性能面を考慮する必要がある。

通信の記録

- 「記録」もファイアウォールの重要な仕事
 - 通過させなかった通信のみが重要ではない
 - 通過した通信のログは事象の追跡には不可欠
 - セキュリティ面のみならず、利用状況の集計にも利用可能

この機能は忘れられがち。

特に、通過させた通信のログが、後のインシデント対応に重要な役割をはたすこともあることに注意。

最近のファイアウォール製品

- オール・イン・ワン化の流れ
 - アンチウイルス、コンテンツフィルタ、IDS、VPNなど多彩な機能の一元化
 - 利便性とパフォーマンスのトレードオフ
- 高速化の流れ
 - ブロードバンド化への対応
 - 基本機能を中心にH/W化して高速化
 - VPN暗号処理のH/W化による性能向上
 - 付加的な機能はやはり低速？

オールイン・ワン型は、便利だが性能的に難があるケースも多い。H/W ベースのファイアウォールは性能は高いが融通がきかないことが難点でもある。(たとえば、ソフトウェア製品ならば、別のアプリケーションを同一H/W上に導入したりできる)

一般的に言えば、オールイン・ワン型は小規模なサイト向けと考えられ、大規模なサイトでは、ファイアウォールではなく、別のシステムを、それらの用途に導入した方が、最終的に問題がすくないと考えられる。

付加機能を使用する際の注意点

- 性能をとるか利便性をとるか
 - 付加機能はファイアウォールの負担を高める
 - たとえばウイルスチェックなどの重い処理は全体のスループット低下につながる可能性もある。
 - ファイアウォールに多くの仕事をさせるばあいは、その性能とトラフィックを天秤に掛ける必要性。
 - 残念ながら、メーカ、ベンダの性能評価資料はあまりあてにならない。(理想的な条件での試験)
 - 性能に余裕があれば、管理が楽な分、オールインワンタイプは有利

ファイアウォール関連用語・概念

- ダイナミックパケットフィルタ
 - (類) ステートフルインスペクション
- NAT (Network Address Translation)
 - (類) IP Masquerade, NAPT, PAT etc.
- DMZ (De-Militarized Zone)
- VPN (Virtual Private Network)
 - IPSec, L2TP etc.

ステートフルインスペクションはチェックポイント社の考案した用語であり、正確には同社の製品のみに適用される概念。しかし、「ステートフル」を名乗る製品は多いものの、その仕様は千差万別。多くが、単純なダイナミックフィルタ機能を「ステートフル」と称している。(本格的なステートフルインスペクションがはたして必要かどうかという議論はあるので、それで充分という話もあるのだが、議論をややこしくしているところだ)

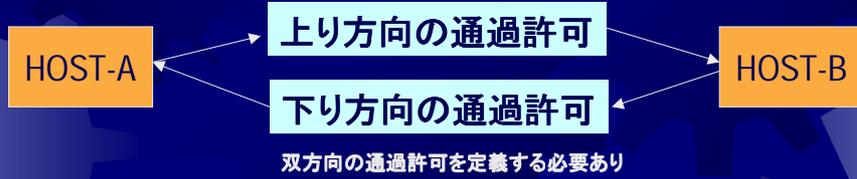
DMZという言葉も誤解が多く要注意:後述

ダイナミックパケットフィルタ

- ファイアウォール製品とルータのフィルタ機能の最大の相違点
 - 通過を許可した通信パケットへの応答や付随する他のセッションなどを総合的に管理、自動処理を行う。
 - ポリシー設定を単純化できる。(許可するセッションの方向のみ定義)

単純パケットフィルタとの比較

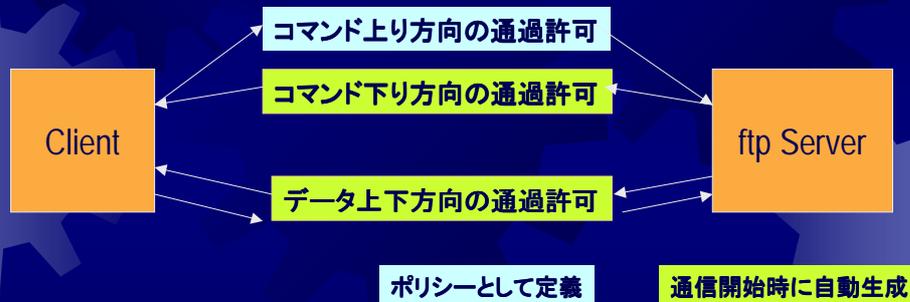
単純パケットフィルタ



動的パケットフィルタ



FTPの場合のダイナミックフィルタ



FTPの通信は2つのコネクションから構成される。データコネクションの開設や使用するポート番号は、コマンドコネクション内でネゴされる。また、データコネクションはデータ転送のたびに新しいコネクションが生成される。

ダイナミックフィルタの特徴

- 1コネクションのみで構成される通信は確実に対応可能
- 複数コネクション／セッションから構成される通信は対応できないものあり。(ストリーミング系の通信など)

ステートフルインスペクション

☀ Checkpoint社オリジナルの用語

- 本来は、単なるパケットヘッダのみのチェックではなく、アプリケーションレイヤまで、プロトコルをデコードして細部の検査ができる方式のこと。
- 一般にはダイナミックフィルタと同義に使用されることが多い。C社以外のファイアウォールの場合、厳密にはこの言葉に該当しないものが多いが、ステートフルと称することが多い。

NAT, IP Masquerade, Etc.

- 内部アドレスにプライベートアドレスを使用したネットワークとインターネットの境界にファイアウォールを置く場合に必須。(除く、アプリケーションゲートウェイ型FW)
- プライベートアドレスネットワークを起点とする通信がファイアウォールを通過する時点で、発信元をグローバルアドレスに変換する。

NATも混乱の多い言葉。NATと呼ばれている機能にも様々なものがあり、その方式に応じて、使えるプロトコルに制限があったりすることに注意。

NAT(RFC1631)

- グローバルアドレスプールからアドレスを割り当て。
- 内部側ホストが外部と通信する際にプールからアドレスを一次的に割り当てて、アドレスを変換
- 同時通信数はグローバルアドレスの数に制約される
- 多数の内部ホストがある際に現実的ではない

本来のNATをサポートしているファイアウォール製品は少ない。(あまり利用されないから?)

IP Masquerade, NAPT, PAT

- 1個もしくは少数のグローバルアドレスを多数の内部ホストで共有
- アドレス変換後のセッションが重複しないように発信元のポート番号も含めて変換
- 利用可能なポート番号数×アドレス数分の同時セッションをサポート
- 一部のプロトコルに対応が困難

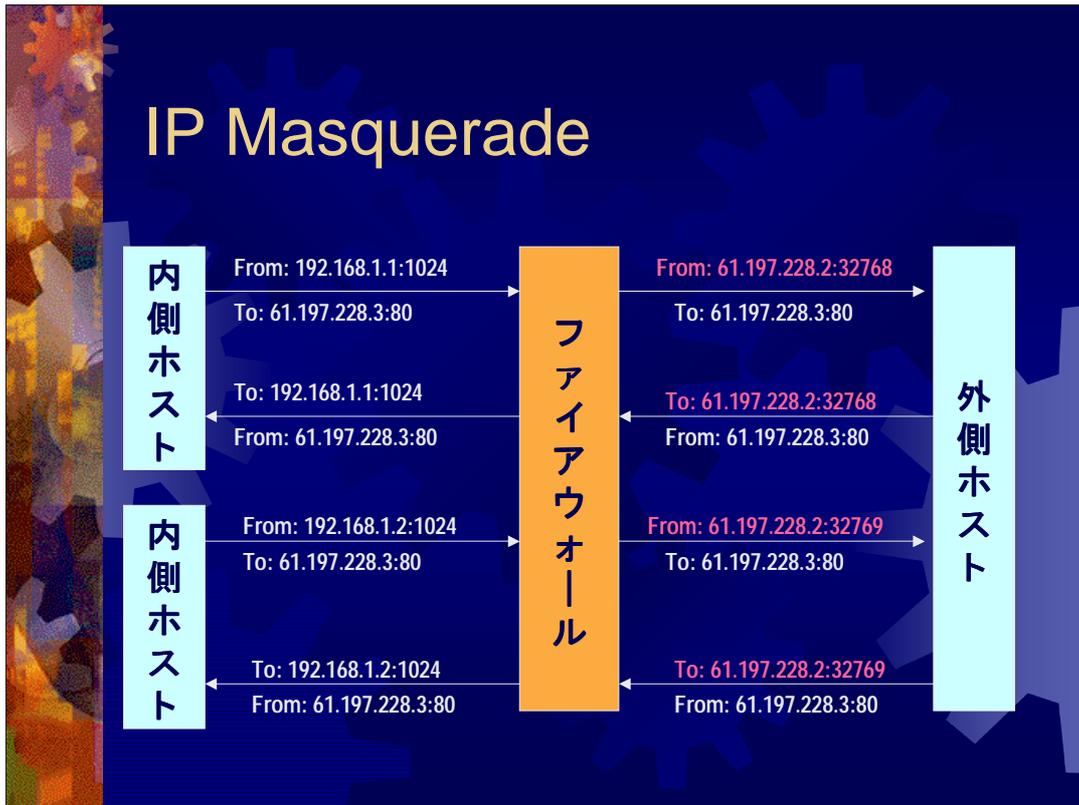
これらの表現は、すべてほぼ同等の機能を表す。

NAT 全般に言えることだが、アプリケーションプロトコル内で、IPアドレスやポート番号を受け渡すような仕様の場合、NAT越えの通信がうまくできない場合があることに注意。
(メーカーが個別対応していないとダメ)

また、発信元のポートが変わってしまうとうまく動作しないようなケースでは、IP Masqueradeなどの方式には対応できないケースが多い。

たとえば、一部のリモートアクセスプロトコルなどで、発信元が特権ポートであると扱いがかわるものなどがある。このような場合、特権を使えなかったりする。

IP Masquerade



発信元ポート番号を書き換えていることに注意

NAT使用上の注意点

- 複数のコネクションを使うプロトコルで対応できない可能性がある。(ダイナミックフィルタと同様の理由)
- データとしてIPアドレスを受け渡すようなアプリケーションの動作を保証できない。(FTPなどは一般に対応されているが、新しいアプリケーションでは未対応のものも多い)
- パケットヘッダの改ざんチェックを行うようなプロトコルに対応できない。(IPSecなど)

サーバ保護とDMZ

☀ DMZの意味合い

- もともとは軍事用語
- De-Militarized Zone = 非武装地帯(直訳)
- 直接侵入を防ぐための「緩衝地帯」的意味合いが強い(決して「非武装=無防備」ではない)
- ファイアウォールの限界ゆえに……

DMZ: 誤解のほうが多い言葉

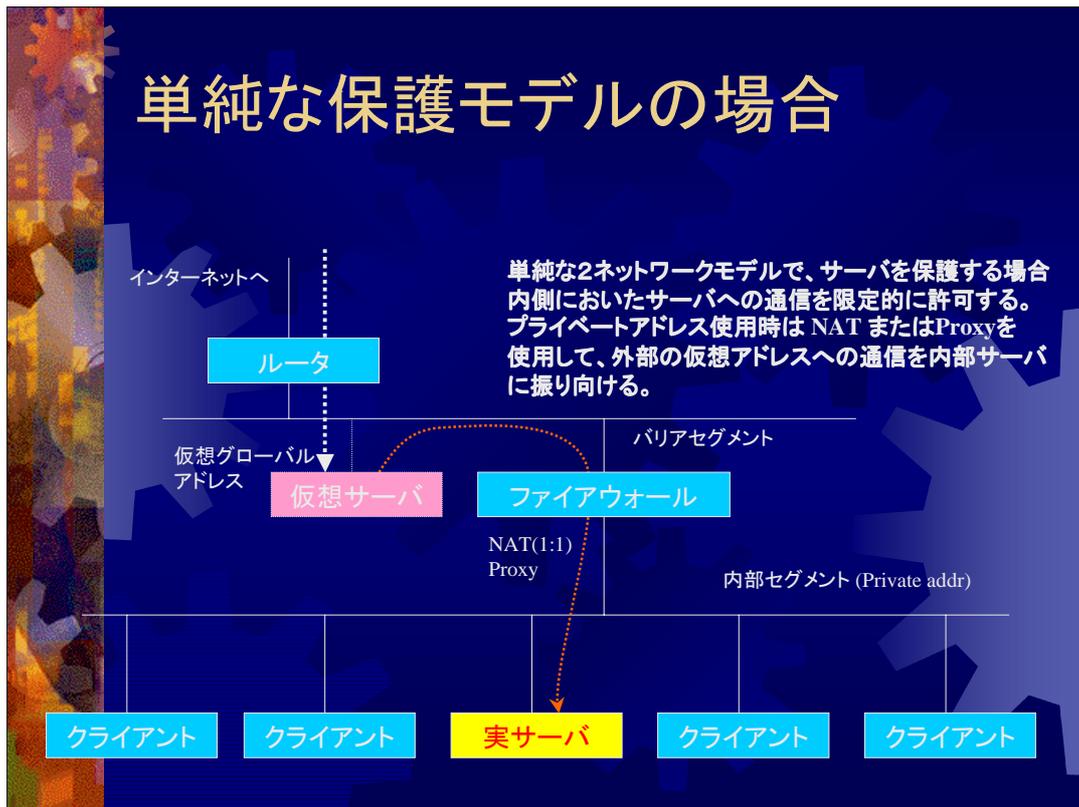
「非武装」=「無防備」という誤解が一番多く、次に、単純に内部とは違うセグメントを作ることがDMZをつくることという単純な誤解がある。

基本的な考え方は、「ファイアウォール」で防げなかった場合の「予防策」

公開サーバの保護

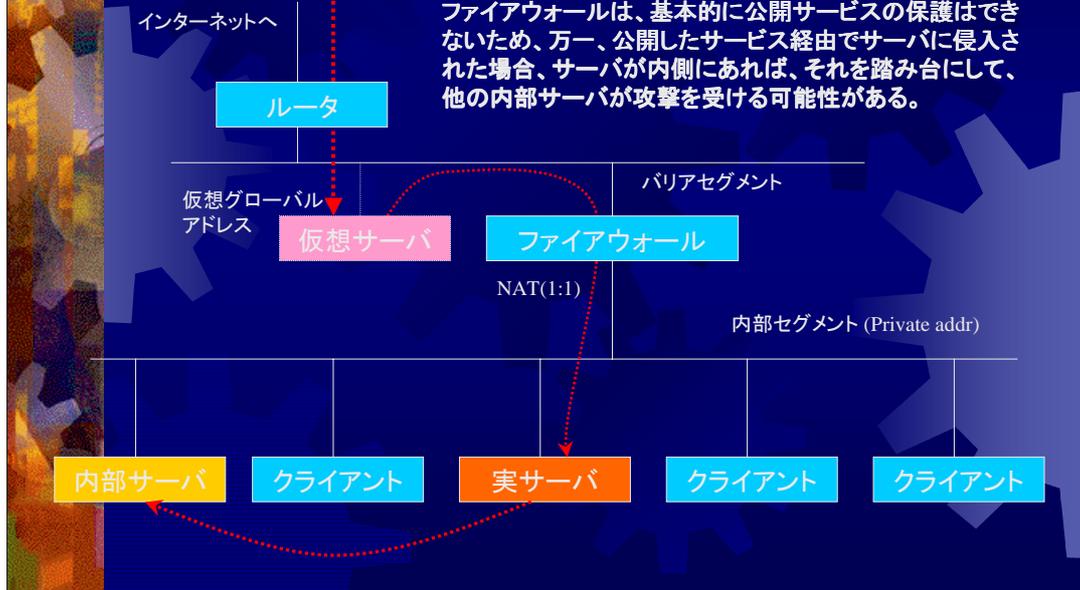
- サーバをファイアウォール下に配置
- 外部からサーバに対して、公開するサービス以外へのアクセスを禁止
- しかし、公開サービスは通さねばならない
 - サーバの公開サービスに脆弱性があると、攻撃、侵入の可能性がある。
 - これをファイアウォールで防ぐことは難しい

単純な保護モデルの場合

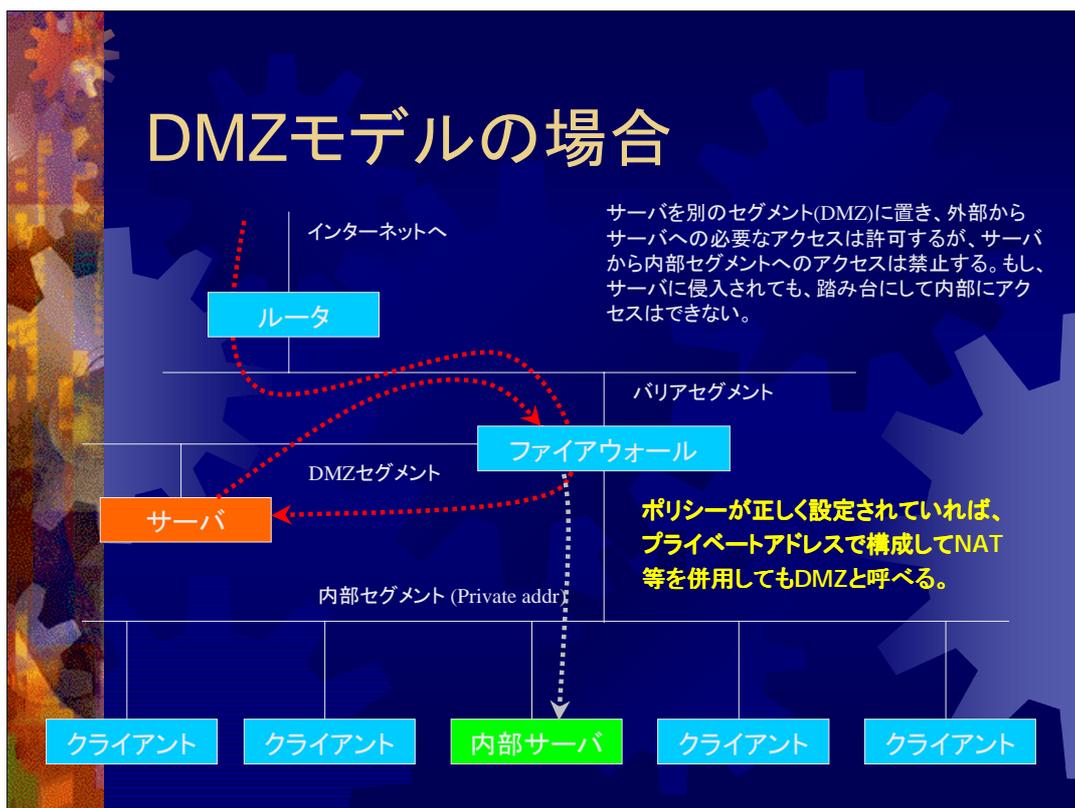


一部のSOHO向けブロードバンドルータなどで、この機能をDMZと称しているものが見られるが、「重大な誤解」である。

単純モデルで攻撃を受けたら



なぜ、「重大な誤解」なのかは、これを見れば一目瞭然。こうならないように考えられたのがDMZの概念だから。



これが、一般的なファイアウォール製品のDMZ構成モデル

ただし、セグメントをわけるだけでは無意味。DMZ上のサーバが侵入された場合に、それを踏み台にして他が攻撃されることを防ぐにはどうすればいいか。これは自明。

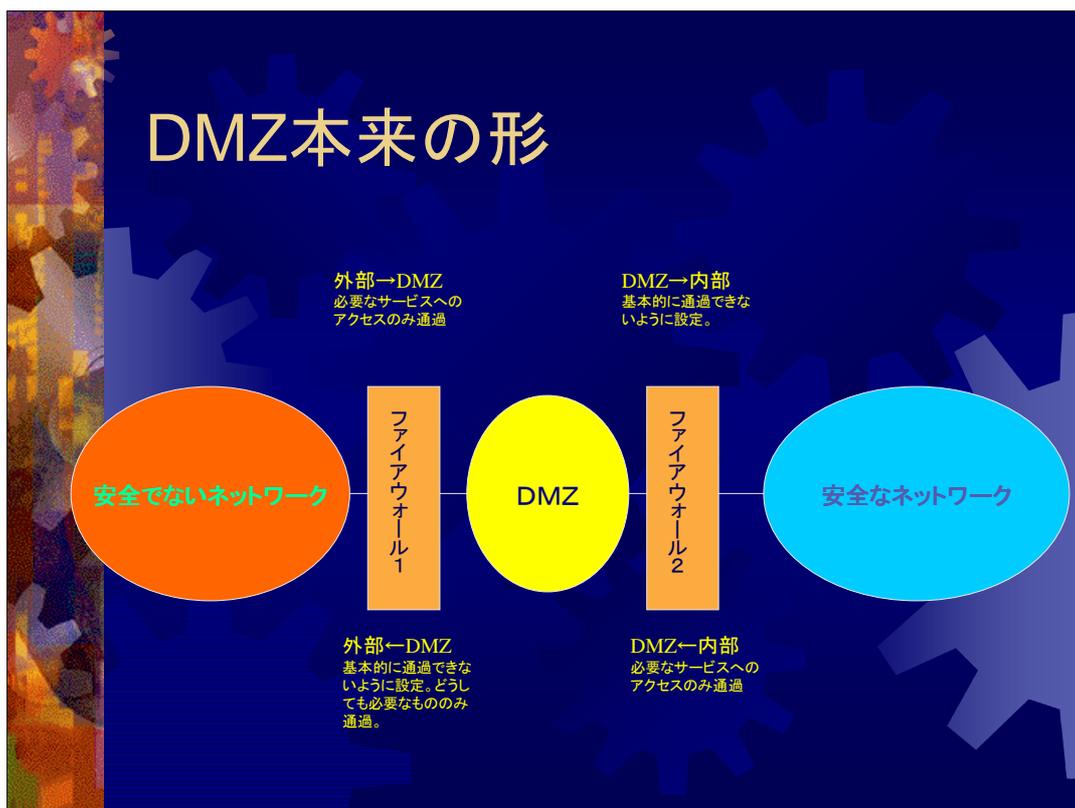
DMZを構成する意味

★ DMZは中間的な保護層

- 公開サーバ群をファイアウォールで保護し、必要以外のアクセスを排除する。
- 万一、公開サーバが不正アクセスにより侵入されるなどの事態が生じて、そこから内部に直接入れないようにすることで、安全性の向上をはかる。(不正アクセスに対応する時間をかせぐ)
- さらに、外部へのアクセスも制限することで、侵入されたサーバを踏み台にして外部を攻撃することも困難にする。(かごの鳥作戦)
- 不正アクセスによって深刻な事態に陥るような重要なホストは置かない。

原則論はこのとおり。

例外を作る場合は、そのリスクを考えて。



ファイアウォールの古典的な教科書に登場するDMZの形。これが一番わかりやすいし、たとえば、2個のファイアウォールやルータを使っても構成ができる。

DMZを正しく理解するために

- DMZは「非武装」ではない
- 正しくポリシー設定しなければDMZではない
 - 外部からDMZへのアクセスは必要なものに限定
 - DMZから内部へのアクセスは原則不許可
 - DMZから外部へのアクセスも必要最小限に限定

VPNとファイアウォール

● VPNゲートウェイ機能

- インターネットなどの安全でない(セキュリティポリシーの異なる)ネットワークを介して、安全にネットワーク間接続を行う。
- VPNゲートウェイは相手側のネットワークに対するルータの役割をする。
- ゲートウェイ間は暗号通信によって、通信の内容が保護される。

● セキュリティの観点から見ればファイアウォールに別のネットワークを追加接続したのと同じ意味合い。

- 接続先ネットワークのセキュリティが破られれば、当然、リスクにさらされることに注意

VPN接続は特別な接続ではない。セキュリティ的に考えれば、専用線やダイヤルアップ接続となんら変わらないことに注意。

たとえば、取引先とのネットワーク接続にはどのようなリスクが伴うか……これを考える必要あり。

ファイアウォール製品とVPN

- ファイアウォール製品の多くがVPN接続に対応
- IPSecへの対応による相互接続性
- ファイアウォール、ルータなどとの相互接続による仮想ネットワーキング
- モバイルクライアントへの安全・安価なアクセス手段の提供

VPNに対応出来る製品はファイアウォール以外にも各種のルータ、専用のVPNサーバなど様々。必ずしもファイアウォールで対応させることが得策でない場合もある。(負荷の問題その他)

VPNの方式と互換性

● 独自方式のVPN

- 初期のファイアウォールなどに搭載されたメーカー独自の方式
- 基本的に他社製機器との接続性は保証されない
- 高いシェアのメーカーによる顧客の囲い込みに有利
- 互換性がないことが利点である場合もないではないが...

● 標準方式のVPN(最近はほとんどが標準方式)

- IPSec の標準化の進行(RFC24xx)
- 標準に準拠した異なるメーカーの機器を相互接続
- 暗号鍵を自動的に交換、定期的な再発行(IKE)
- 複数の認証方法 (X.509認証/PKI、暗証による認証)
- エクストラネットの構成などに利用しやすい

最近は標準方式がほとんど。しかし、標準方式といえども必ずつながるわけではない。

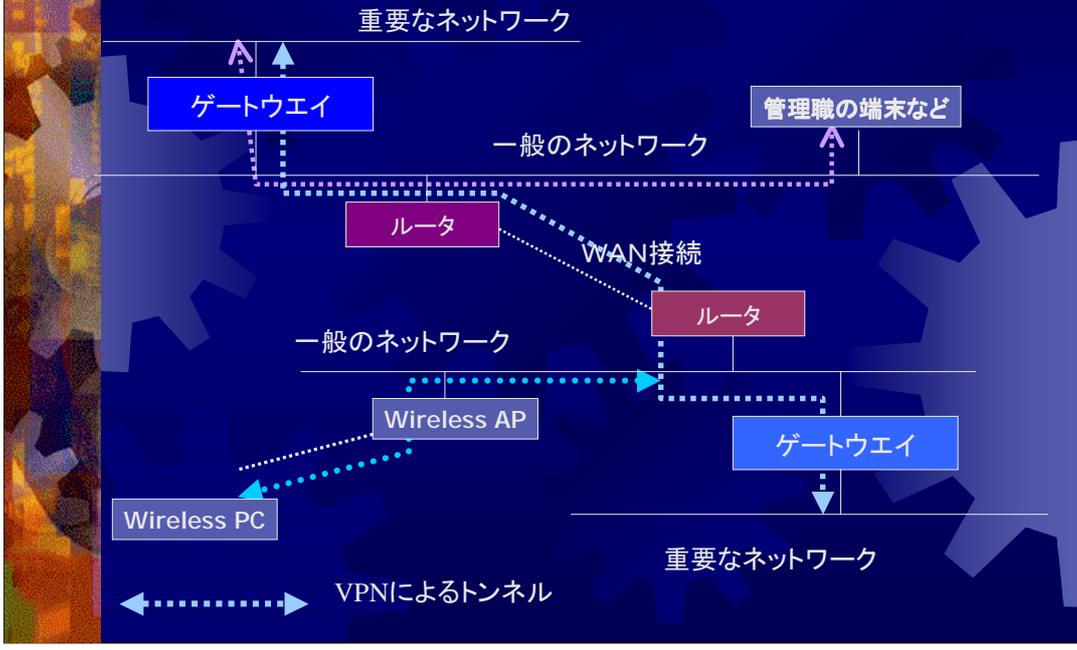
現在の標準は実装に依存している部分を若干残している。実装依存部分が異なれば接続できないので、異機種間接続は必ず検証が必要。

VPNの利用目的

- 同一組織のブランチ間のインターネット経由接続
 - 専用回線の代替えまたはバックアップ、回線費用の節約
- モバイルアクセスのコスト削減と安全性の確保
- 複数組織の協同ネットワーク(エクストラネット)構築
 - 回線費用の節約
 - インターネットの利用による柔軟性の確保
- 組織内のネットワークセキュリティの階層的強化
 - 組織内 LAN のセキュリティ階層化
 - セキュリティの低いネットワークを使って重要なネットワークを接続
 - ワイヤレスLANのセキュリティ強化策

VPNの利用は、なにもインターネットに限ったことではない。たとえば、物理的に異なる複数のネットワークを作る代わりに1個のネットワーク内に作られた複数のVPNを利用することもできる。(帯域が許せば・・・だが)これらは、別個のネットワークよりも安全に分離される上、配線などのインフラを共有できるため、コストダウンもはかれる。

組織内でのVPN利用例



VPN利用時の注意点

- VPNは安全か？
 - 通信方式は安全でも、接続先によっては問題が生じることに注意(ポリシー設定や認証はきちんと行う必要あり)
- パケットサイズ(MTUまたはMSS)に注意
 - カプセルリングを行うことで最大パケットサイズ(MTU)が減少するため、フラグメントが発生する可能性あり。
- NAT越えの場合、通信できない場合あり
 - IPSec の場合、特殊な方法(NAT Traversal)を使用する必要がある。

VPNは安全か？ 答え:NO!

パフォーマンスの問題では、まず、MTU問題(不要なパケット分割の発生)を疑う。

ここでは、IPSecのみを紹介したが、他にもL2TP, PPTPなどがあるので、たとえば、個人(ユーザ)ベースでの認証や、クライアントへの内部アドレスの割り当てなどが必要な場合、これらを使うことも考えられる。

そのほかの付加機能

- コンテンツスキヤニング
 - URLフィルタ、コンテンツフィルタ機能
 - ウイルス検出、排除機能
 - なんでもかんでもファイアウォールで・・・は問題あり？
- 障害対策
 - ファイアウォールの二重化(Hot Stand-by/fail over)
 - 負荷(トラフィック)分散(Load balancing)
 - トラフィックの分散が必要な局面では、設定内容も複雑になりがちに留意する必要がある。すべてのポリシーを入り口のファイアウォールで管理することは本当に妥当だろうか。

二重化、負荷分散には様々な方法がある。

ファイアウォール製品自体がサポートしているケースも多いが、ロードバランサを使うケースもある。違いはあまりないが、ファイアウォール製品自体がサポートしている場合、たとえば、あるセッションを担当しているファイアウォールが通信中にダウンした場合、そのセッションを別のファイアウォールが引き継ぐようなことができるものもある。(VPNセッションについても可能なものあり)



ファイアウォールがもたらす安全とは

- 基本的にはIPアドレスやサービスをベースにした通信の到達性の制御
- つながるか、つないでいいかの制御
- つないだことの記録、つなげなかったことの記録
- アクセスされる必要のないホスト、サービスに到達できなくなること。

ファイアウォールは、ポリシーがなければただの「箱」であることに注意。
「安全性」はポリシーしだい。

ファイアウォールが苦手なこと

★ 通信内容の厳密なチェックと内容による通信制限

- 特にパケットフィルタ系はこれが苦手（複雑な処理は負担が大きい）ため
- アプリケーションゲートウェイ系はこうしたことも可能だが、スピードはそれなり。
- オール・イン・ワン型もあるにはあるが・・・
- 基本的に通過させたサービスに関する保護はサーバ側で行うのが基本となる

機能と性能のトレードオフに注意

ファイアウォールの利点とリスク

- ポリシーの異なるネットワークとの接続において、お互いのポリシーについて原則を維持しながら通信が可能。(利点)
- しかし、なんらかの通信が発生することによって新たな問題が生じる可能性がある(リスク)
- 通信のボトルネックが生じる可能性(リスク)
- これまで可能だった通信ができなくなる(通過させることが仕様の的に困難なケースなど)可能性がある。(リスク)

「繋がらない」が一番安全。

繋ぐ必要があるとしたら……

ファイアウォールのポリシー

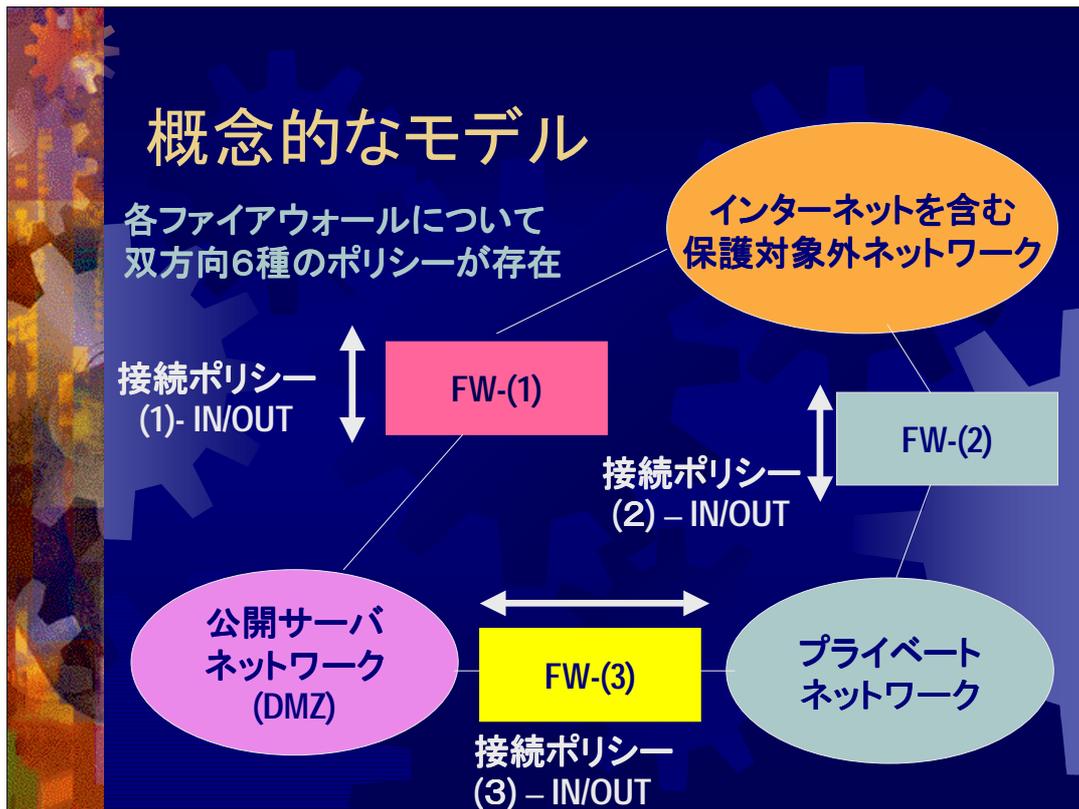
- 基本的に「ネットワーク上のサービスの相互接続」に関する取り決めである。
 - ファイアウォールに保護されるネットワークの位置づけの明確化が必要
 - 外部に提供されるサービスと、外部から提供されるべきサービスの明確化

ファイアウォールの「ポリシー」は、いわゆるセキュリティポリシーのサブセットである。サブセットの意味は、「ネットワーク間の相互接続性」に限定された・・・という意味。

インターネット接続を考える場合

- 最低限考えるべき3つのネットワーク
 - (内部ネットワーク) 保護すべきプライベートなネットワーク
 - (公開サーバネットワーク) 一部のサービスを外部に公開する必要があるネットワーク
 - (外部ネットワーク) インターネットなど、保護対象外のネットワーク

(内部) (外部)という言葉はあまり使いたくないが……。ここでは、「外部＝組織外」から保護される・・・という意味で。



このように複数のファイアウォールを使ったモデルにおきかえて考えると個々のポリシーが考えやすい。

モデル化の必要性

- ファイアウォールのモデルを単純化することで、個々のポリシーを単純化できる
- 接続ネットワーク数が増加するとポリシー数が激増する(複雑さが加速度的に増える)ことへの理解
- 実際は1台のファイアウォールに複数ネットワークを接続するが、ポリシー数(複雑さ)はモデルの場合とかわらないことへの理解。(変わらない必要がある)
- 多数のネットワークを1台のファイアウォールで管理することの困難さへの理解

たとえば、多ポートのファイアウォールのポリシー設定は非常に煩雑になる。きちんと整理しないと必ず間違いが起きる。

実際のモデル



- 1台のファイアウォール製品に3個のネットワークを接続
- 概念モデルと同等のポリシーを実現可能（但し、ポリシーの複雑さは軽減できない。むしろ、1台の製品の設定項目の増加はミスの入り込む余地を増加させる）
- ファイアウォールが陥落した際のリスクの増加

公開サーバ
ネットワーク

DMZポリシーを適用

ファイアウォールの設定ポリシー

● 原則と例外（インターネット接続の場合）

● 原則：

- 外部→内部：原則不許可が一般
- 外部→DMZ：原則不許可が一般
- 内部→外部：（ポリシーによる）
- 内部→DMZ：（ポリシーによる）
- DMZ→外部：原則不許可が一般
- DMZ→内部：原則不許可が一般

● 内部→外部 のポリシー

- 原則許可：インターネットアクセスに対しゆるやかな規制
- 原則禁止：インターネットアクセスに対し厳密な規制
- インターネットへのアクセシビリティの利便性を重視するか、リスクを重視するかの違い

原則を決め、必要に応じて例外を設ける。ただし、原則が骨抜きになってしまうよう、必ずリスクを考えて例外を設けること。

ファイアウォールの設定ポリシー

★ 原則と例外(インターネット接続の場合)

● 例外

- 外部→内部: 一般に例外はつukらないほうがよい
- 外部→DMZ: 公開サービスを例外として許可
- DMZ→外部: 運用上必要なもののみ例外として許可
- DMZ→内部: 運用上必要なもののみ例外として許可(*)
- 内部→外部/DMZ: 原則に対し、変更が必要なものを許可または禁止

(*)あまり推奨できないが……

ファイアウォール導入の注意点

- まず、モデリングをしてポリシーの確認を
 - VPNを含む多数のネットワーク接続がある場合は、要注意。
- 複数のファイアウォール製品の導入も視野に
 - ポリシー設計、設定、管理の煩雑さを緩和。
 - 通信上のボトルネックにならないように製品1台あたりの負荷を最適化。
 - 集中管理システムの導入(特に、VPN接続が多い場合、拠点のファイアウォールを含めて集中管理することは重要)

いかに高性能の製品でも、それは処理性能の話。多くのネットワークを1台でさばく際のポリシーの複雑化は避けられない。敢えて機器をわけることも必要。

VPNは、集中管理ツールを使うとうまく管理できることがある。

ファイアウォールの運用と管理

★ ファイアウォールの日常管理

- ログ、アラートの管理
 - ログは情報の宝庫
 - アラートは時として「狼少年」
- ポリシーの変更、見直し
 - 状況の変化に応じた見直し
 - ネットワーク構成の変更に伴う再設計
- トラフィック状況の掌握
 - ファイアウォールはボトルネックになりやすい

ログ管理せずしてファイアウォール管理者を名乗るなかれ！！！！

ポリシー変更は慎重に。変更手続きについてはルール化も必要。

セキュリティのみではなく、トラフィックも重要な管理項目。

ログ・アラートの管理

- ログは定期的集計を
 - 拒否された通信の種類と発信元、宛先別頻度
 - 許可した通信の種類と発信元、宛先別頻度
 - 日次、週間、月次の変化パターンの掌握
 - 普段にない異常な現象をみきわめることは重要
- アラートは発生原因をつきとめよ
 - アラート発生には意味がある
 - 既知のもの以外は必ずログとつきあわせて確認を
 - 攻撃→成功したものかどうかの確認(他のシステムを併用)
 - 誤認→確認方法の確立と、必要であればアラートの停止
 - ファイアウォールのアラートからネットワークのミスコンフィグレーションが見える場合もある
 - IDSやサーバのログとの突き合わせも必要
 - アラートに対する判断、対処方法のマニュアル化
 - 個人の判断に委ねないことも必要

ログはできれば別サーバに転送して管理を。(Syslogサーバなど)

リアルタイムに転送できなければ定期的にバックアップを。

最低でも一週間程度、できれば一ヶ月くらいはログを保存しておく、何か問題が発生した際にトレースしやすい。(必要があればもっと長期間になる場合もある)

アラートの確認方法

- アラート発生理由(トリガ条件)の理解
 - どのような条件で発生するアラートであるかをあらかじめ理解しておくこと
- 誤認もしくは必然性のあるアラートかどうかの判断
 - ネットワークや機器の構成上、ありえない、または問題ないと判断できるものを排除する。
- 攻撃または不正アクセスの疑いある場合は、成功／不成功を確認して対処
 - IDS の情報、サーバのログの確認
 - 攻撃対象から発生している通信の確認(たとえば、DMZ上のサーバから、外部に対して不必要と考えられるような通信が発生していないか・・・など)

確認はさぼらずに行う。

誤認とわかっているアラートは、排除すべく設定変更や環境の変更を行うことも必要。

なによりも、「狼がきた・・・」にならないことが重要。

ポリシーの変更、見直し

- ポリシーは「作ったきり」ではダメ
 - 適切に運用出来ているか、無理はないかなど、定期的に見直しを。
 - ユーザに想定外の不便はないか
 - ネットワーク構成の変更や、基本となるセキュリティポリシーに変更はないか
- ポリシー変更は、全体を考えて
 - 一カ所のポリシー変更がネットワーク全体にリスクをもたらす場合があることに注意

ネットワーク構成を変更した場合は、ポリシーも見直しを。

たった一カ所のポリシー変更だからと言って、場当たり的に行ってはいけない。他の部分に思わぬ影響を与えることがあるばかりでなく、設定変更作業のミスなども考えられるので、作業後の確認も慎重に。

トラフィック状況の管理

- インターネットが遅い・・・という原因
 - 上位回線の帯域の不足
 - ファイアウォールの能力不足や障害
 - 内部ネットワークの帯域の不足や他のボトルネック、障害の存在
 - DNSなどの必要なサービスの不具合
- どこが悪いかの切り分けはまず、FWから
 - ファイアウォールの負荷状況（プロトコル別）の掌握
 - ログに現れるセッション数などから（こうした統計がとれる製品もある）
 - ソフト製品の場合は、OS ベースでの負荷状況
 - 接続された回線の使用帯域の統計
 - Sniffer™ などのツールを利用
 - ファイアウォールは「悪者」にされやすいのでデータで武装を。（笑）

だいたい、何かあるとファイアウォール管理者に話が飛んでくる。たとえば、ユーザサポートには、何かあれば必ず電話がかかってくるし、最終的にその障害がファイアウォールによるものでなかったケースも多い。

ファイアウォール製品のサポートには、当然として周辺の機器やネットワーク構成についての知識が必要。きちんと切り分けて、まず、ファイアウォールかどうかをユーザに示すことができないと、泥沼に引き込まれることになりかねないので注意が必要。

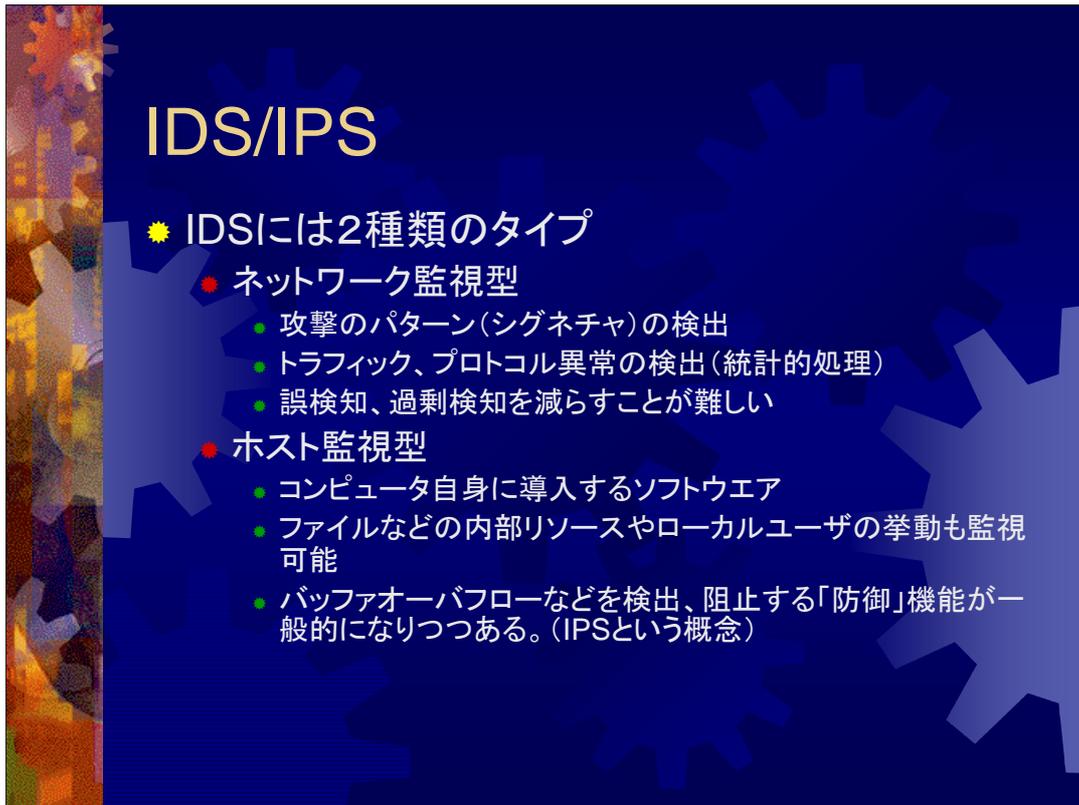
ファイアウォールを補完するもの

- IDS / IPS (侵入検知 / 防御システム)
- アンチウイルスシステム
- コンテンツフィルタ
- ログ解析 / 監視システム

IDS は、単独ではなかなか使いにくい。(誤認、見落とし、成功・不成功にかかわらず攻撃を検知するなど)しかし、たとえば、ファイアウォールを通過した通信が攻撃パターンを含むかどうかなど、組み合わせて使うと有効な場合も多い。

アンチウイルス・コンテンツフィルタについては、ファイアウォール複合製品よりも、単独の製品のほうが、ある程度規模のあるサイトでは障害が少ないかもしれない。

ログの管理が煩雑ならば、それを補完するシステム導入も一つの方法



ネットワーク型は、トラフィック量と検出率が逆の相関関係にあることに注意。

アノマリイ型IDSというものもある(ネットワーク型的一种でもある)。

基本は、トラフィック量を始め、アクセス数、データ転送量など、多くのパラメータについて統計的に傾向(ベースライン)をもとめ、その傾向から乖離したような状況が生じた場合に警告するようなタイプのシステム。

シグネチャ検出型では検知が難しいDoS(サービス妨害)攻撃のようなものを検出するのが得意。場合によっては未知のタイプの攻撃検出にも対応できる可能性がある。

ホスト監視型は、将来的にはアンチウイルスシステムなどと統合されていく可能性が高い。たとえば、リソース(ファイル)監視などにより、未知ウイルスの検出なども可能。

攻撃を検出するだけでなく、それを妨害、防御するプロテクション機能は、誤認の可能性が高いネットワーク型よりは、より確実なホスト型で実現するほうが容易。最近のホスト型はこの機能を入れる傾向にある。

一方、ネットワーク型での攻撃妨害は、誤認との戦い。精度をいかに上げるかがポイント。単独の機器では難しく、複数の機器の情報を相関(Correlate)して、正確な判断を行うようなシステムが必要。

アンチウイルス、コンテンツフィルタ

- 両方ともコンテンツ検査の機能
 - アンチウイルスは、コンテンツに含まれるウイルス固有のパターンを検査
 - コンテンツフィルタは、単語その他の一般的なパターンを検査(不正または不審な内容のブロック)
 - パターンマッチングゆえの負荷の重さがネックだが、必要な機能

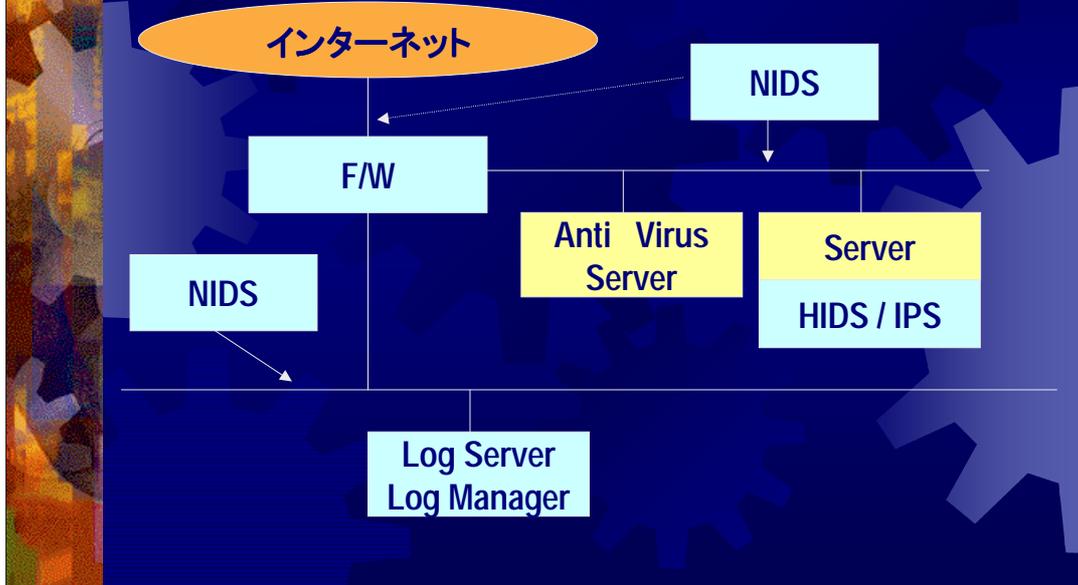
主なアンチウイルスソフトに登録されたパターンは数万種にのぼる。これらをすべてマッチングさせる処理の負荷は想像を絶する。そういう意味では、これをファイアウォールで行うよりも、メールサーバ、Webキャッシュなどの別の部分で行った方が、ファイアウォールが負荷によるボトルネックに陥る危険性が少ない。

ログ解析、監視システム

- ログの集計、解析、統計処理などを行うことで、傾向分析を行うもの
- 複数機器のログを集中管理できるもの
 - F/W IDS Server Router Anti-Virus etc.
- 複数機器からのログや時系列的に発生したログを関連つけて分析 (Correlate) し、より正確に事象を判断してアラートを出力できるもの。
 - 判断結果によるポリシーなどの自動変更、セッションの制御なども可能に・・・(正確さが要求される機能)
- 管理者のログ管理、監視の負担の軽減、判断の一部肩代わりなど

同一メーカーによる集中管理システムは一般的だが、マルチベンダのものはまだ少ない。しかし、ファイアウォールもIDSも、次々と新しいものが出てくる以上、ユーザがこうした新しい技術を取り入れやすくするには、マルチベンダ対応が不可欠である。また、各機器から上がってきた情報を個別に監視、管理するだけでなく、それらの中の関連性を調べ、原因となった事象を特定するようなCorrelation (邦訳は相関分析?)を行うようなツールも増加しつつある。こうしたシステムによって処理された後のアラートは格段に正確なものとなるため、これらをもとにした自動処理による攻撃への対応といったことの可能性も大きくなっていく。

ファイアウォールを中心に見た機器配置



集中か分散か

- 管理は集中することが望ましい
 - 各種の機器からの情報は総合的に判断する必要あり
- 個別機器の導入か複合型機器の導入か
 - オール・イン・ワン型FWは便利だが、性能とリスク集中の可能性を十分に考慮する必要がある。
 - 個々の機器導入は、個別管理になり、集中管理が困難→マルチベンダ対応管理ツールの検討

すべては、バランスの上に……

まとめ

- ファイアウォール導入の目的
 - 異なるネットワークを「**取り決めどおりに**」「**接続する**」ことが目的
- ファイアウォール導入で失うもの
 - なんでもできるという**利便性**(しかし、これは**リスク**でもある)
- ファイアウォールの限界
 - 通過させた通信へのチェックは限定的(**あくまで検問所の役割**。監視カメラや警報装置は別途必要)

お疲れさまでした

- ご静聴ありがとうございました。
- この資料は以下の URL からダウンロード可能です。
 - <http://www.kazamidori.jp/SECURITY/>
- E-mail: futagi@kazamidori.jp

Copyright © 2002 Masaaki Futagi