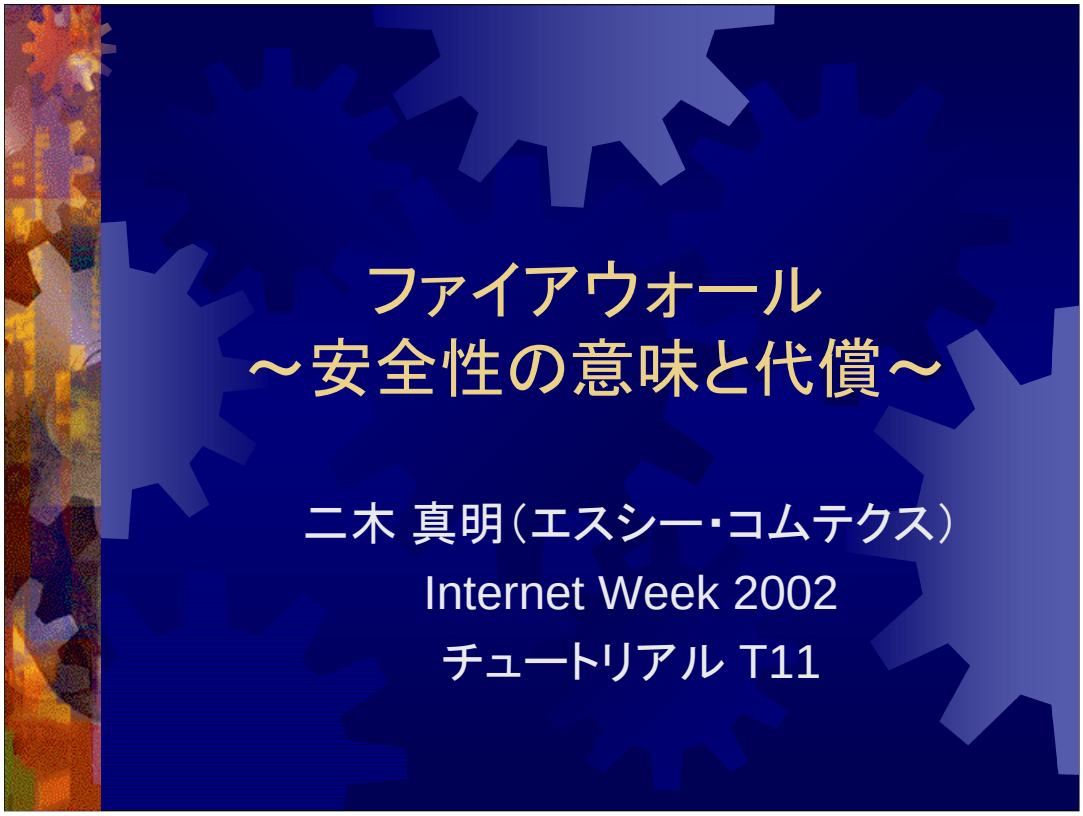
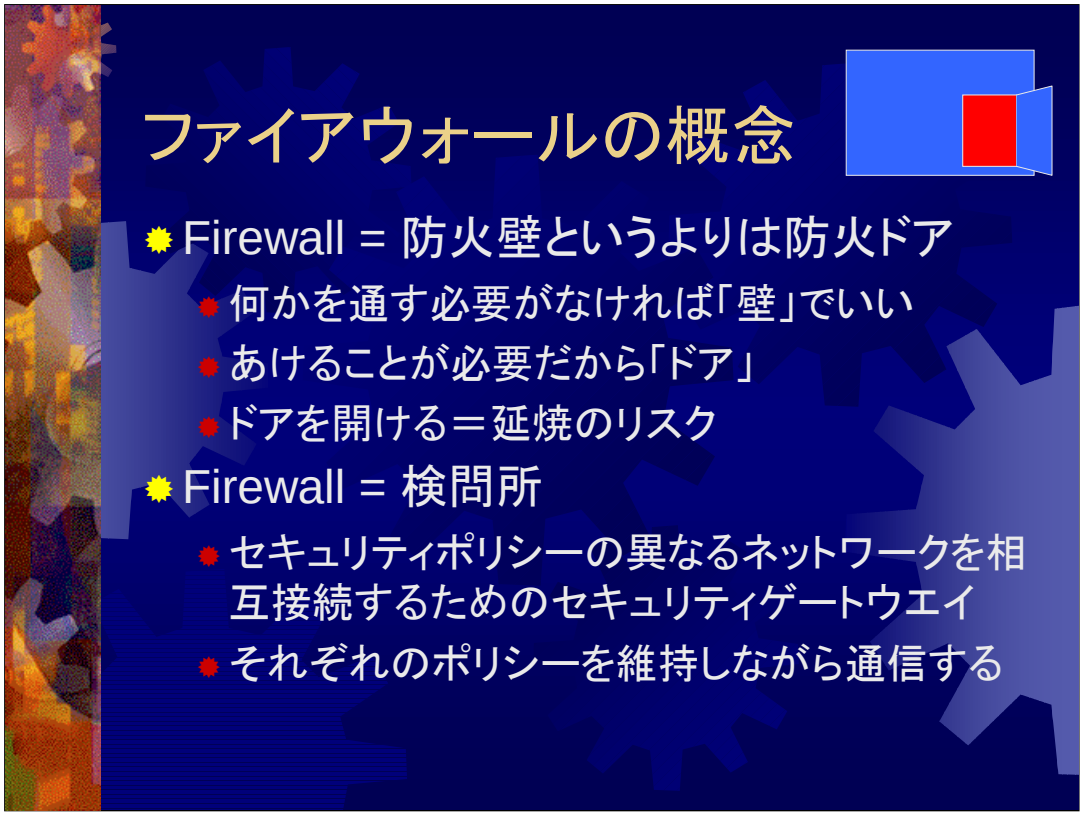

ファイアウォール
～安全性の意味と代償～
二木 真明（エスシー・コムテクス）
Internet Week 2002
チュートリアル T11

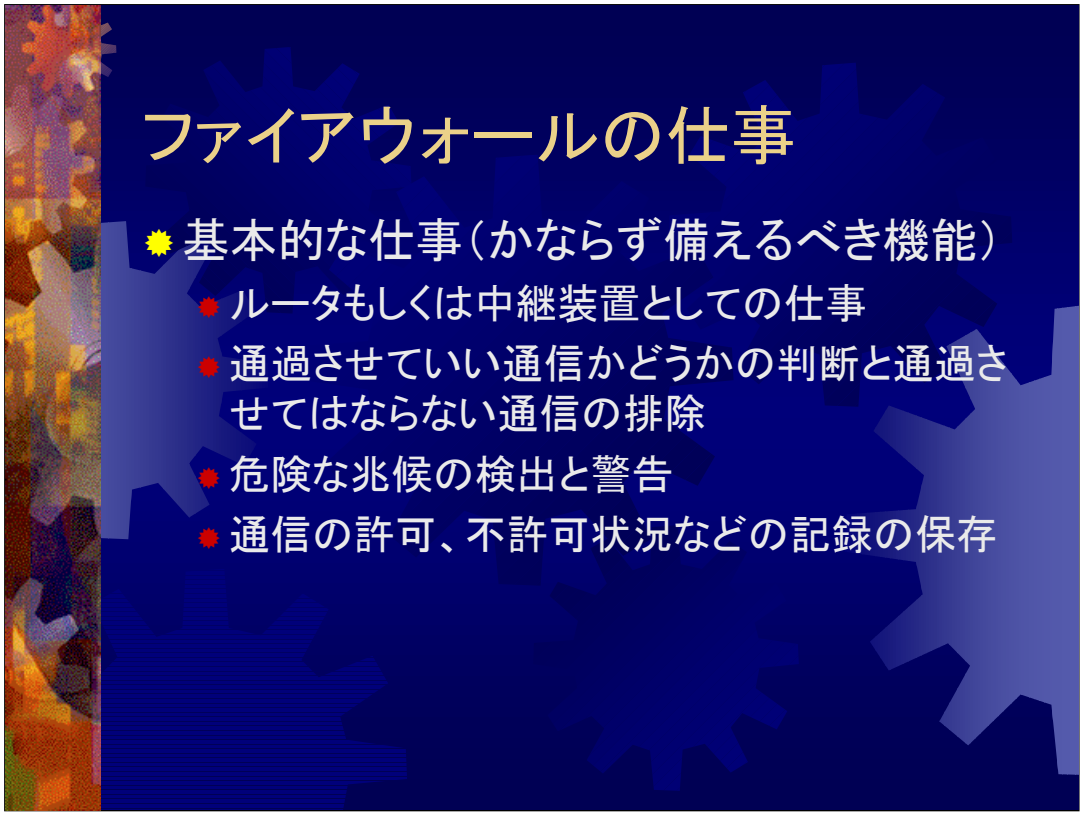
このセッションの目的

- 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「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。

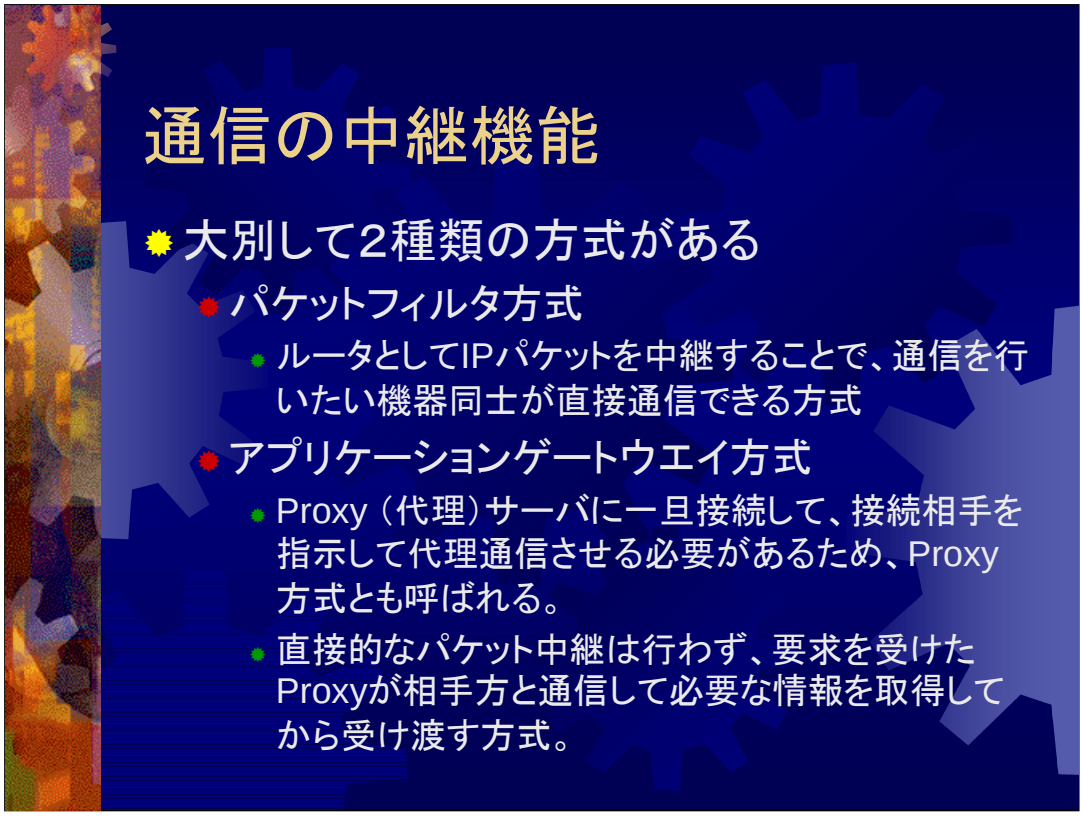


必ずしも、「ルータ」である必要はない。アプリケーションを「中継」できれば可。（アプリケーションゲートウエイ：後述・・もあり）

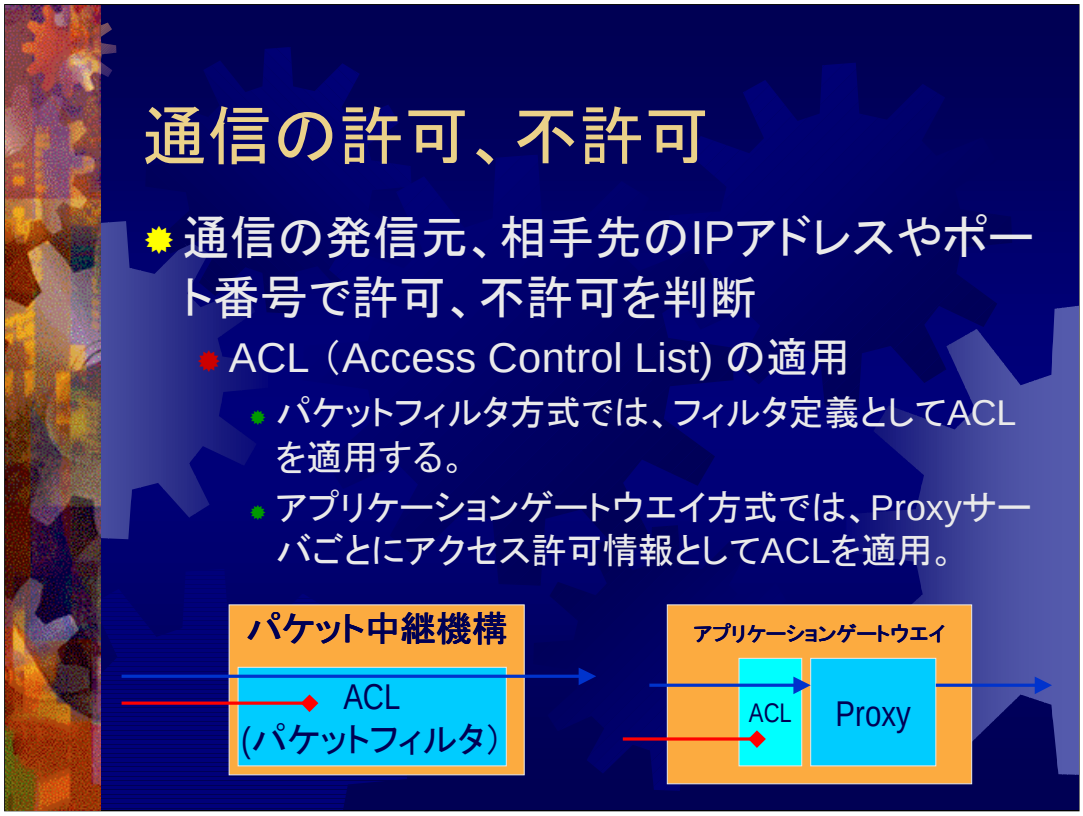
「記録」も重要な仕事であることに注意（意外と忘れがち）

ファイアウォールの仕事

- あると嬉しい機能（きちんと動くならば・・）
  - 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ゲートウエイ機能
    - 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

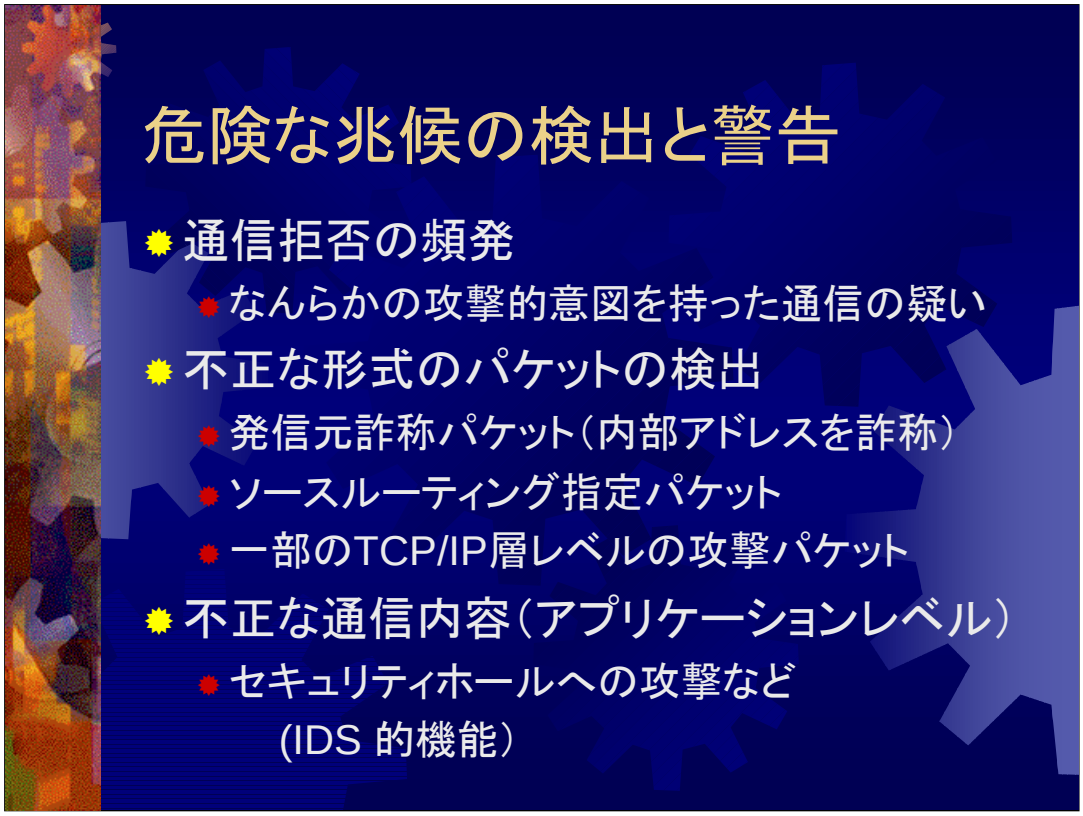


たとえれば図書館で、いわゆる「開架方式」と「閉架方式」の閲覧方法の違い。自分が直接本を取って来ることができるか、係りに頼んで出してきてもらうかの違いと言える。



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エイでは、Proxy すなわちサービス単位での許可、不許可となる。

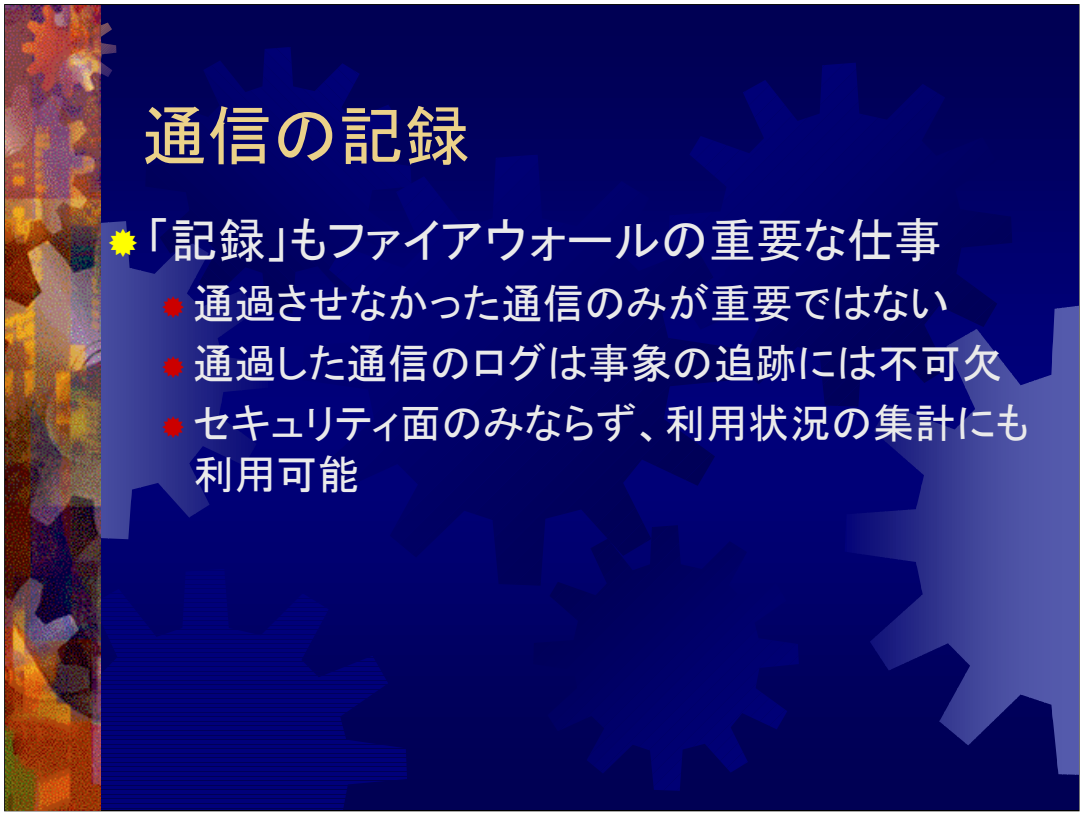
従って、パケットフィルタでは、とりあえず全部通しておこう・・・といった暫定措置が可能なのに対して、アプリケーションゲートウエイでは、Proxy が用意されているサービス以外は基本的に通せないため、あらかじめポリシーをきちんと決めないと導入が困難。（これが「安全さ」の所以かもしれないが）



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

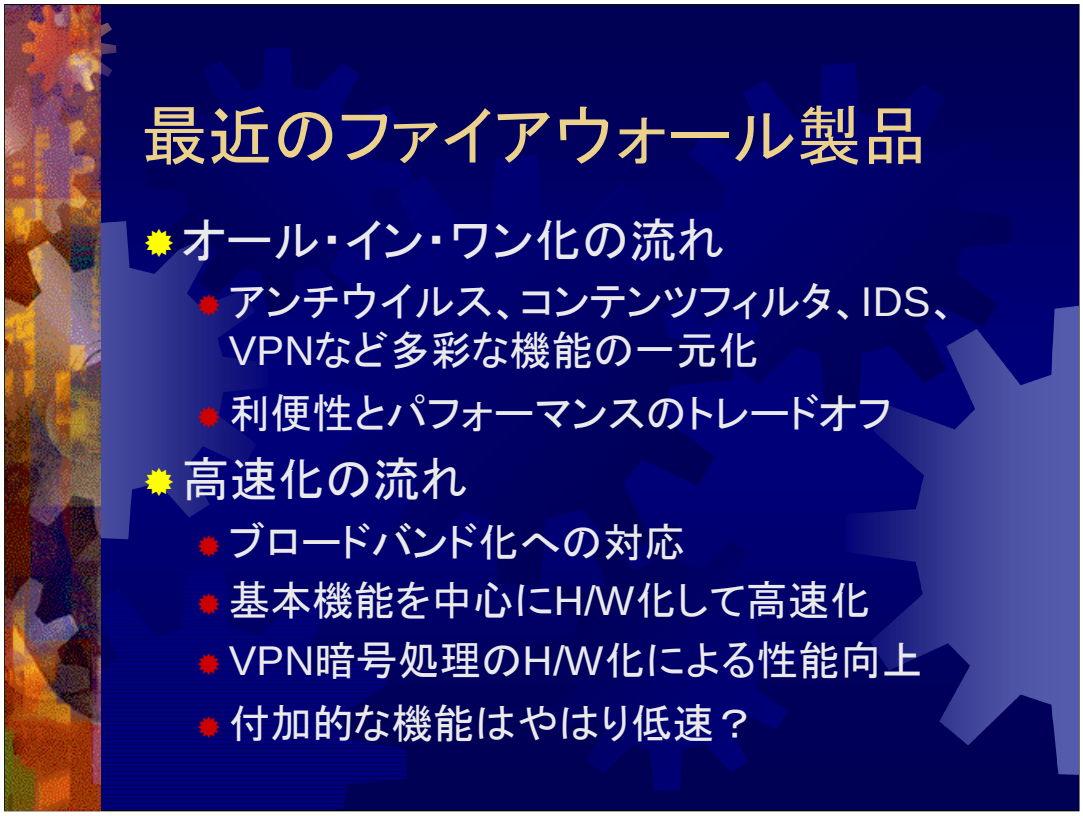
どちらかといえば、IDSとは違って、アプリケーションレベルの攻撃・異常よりも、TCP/IPプロトコル（L3/L4）レベルの検出が中心。（特にパケットフィルタ系）

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。



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。



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、ソフトウエア製品ならば、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

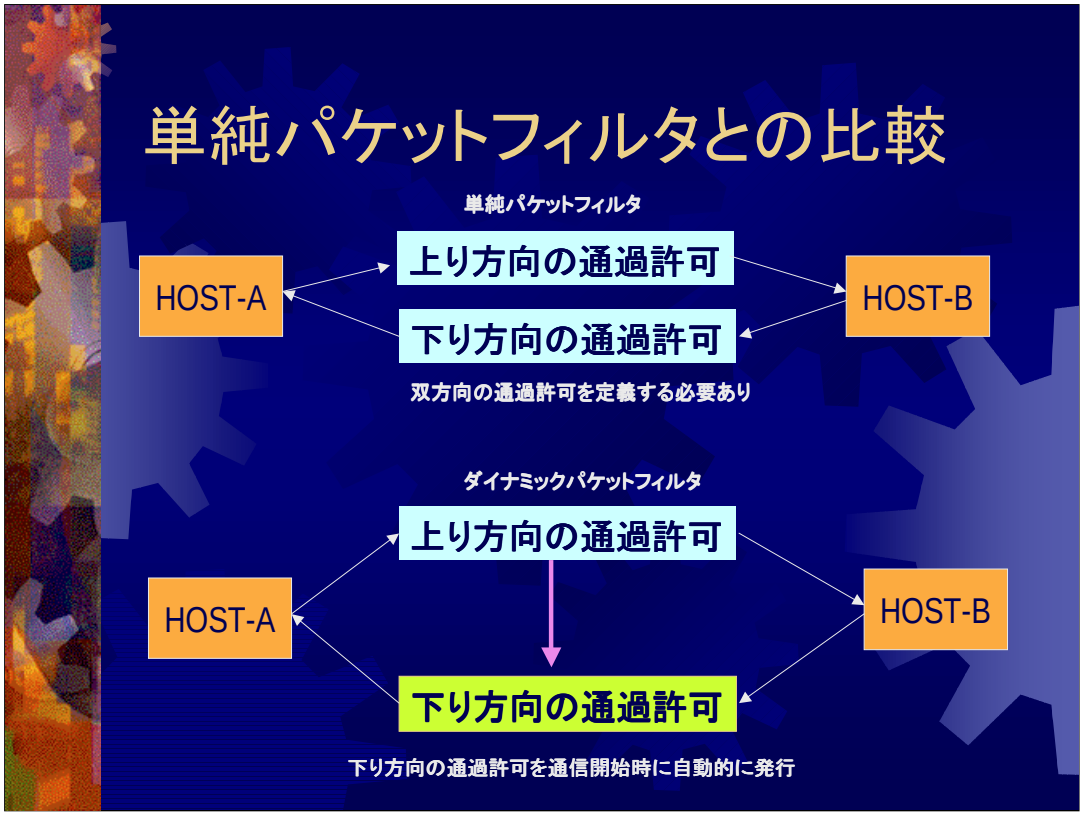
- 性能をとるか利便性をとるか
  - 付加機能はファイアウォールの負担を高める
    - たとえばウイルスチェックなどの重い処理は全体のスループット低下につながる可能性もある。
    - ファイアウォールに多くの仕事をさせるばあいは、その性能とトラフィックを天秤に掛ける必要性。
    - 残念ながら、メーカ、ベンダの性能評価資料はあまりあてにならない。(理想的な条件での試験)
    - 性能に余裕があれば、管理が楽な分、オールイン・ワンタイプは有利

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)

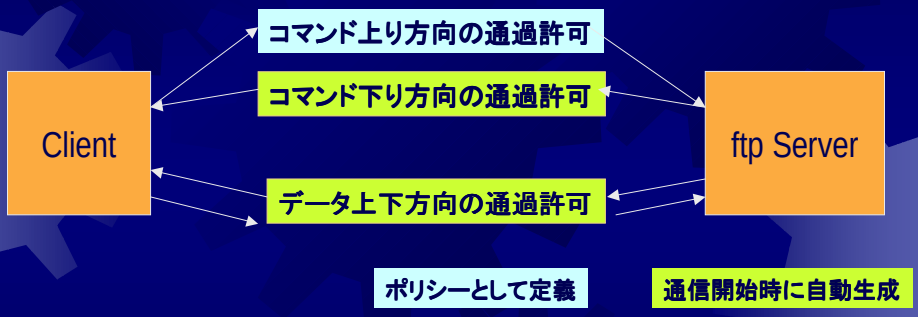
DMZという言葉も誤解が多く要注意:後述

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
HOST-A
上り方向の通過許可
下り方向の通過許可
HOST-B
双方向の通過許可を定義する必要あり
ダイナミックパケットフィルタ
HOST-A
上り方向の通過許可
下り方向の通過許可
HOST-B
下り方向の通過許可を通信開始時に自動的に発行

FTPの場合のダイナミックフィルタ



ポリシーとして定義　　通信開始時に自動生成

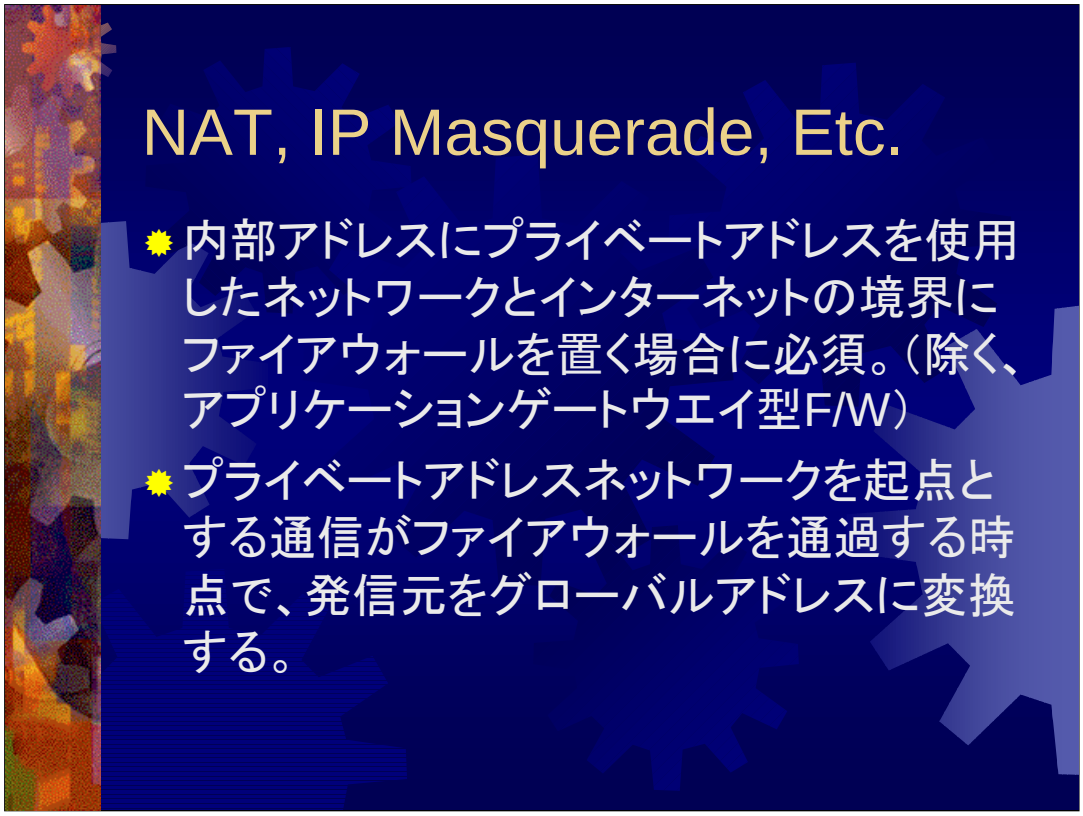
FTP の通信は2つのコネクションから構成される。データコネクションの開設や使用するポート番号は、コマンドコネクション内でネゴされる。また、データコネクションはデータ転送のたびに新しいコネクションが生成される。

ダイナミックフィルタの特徴

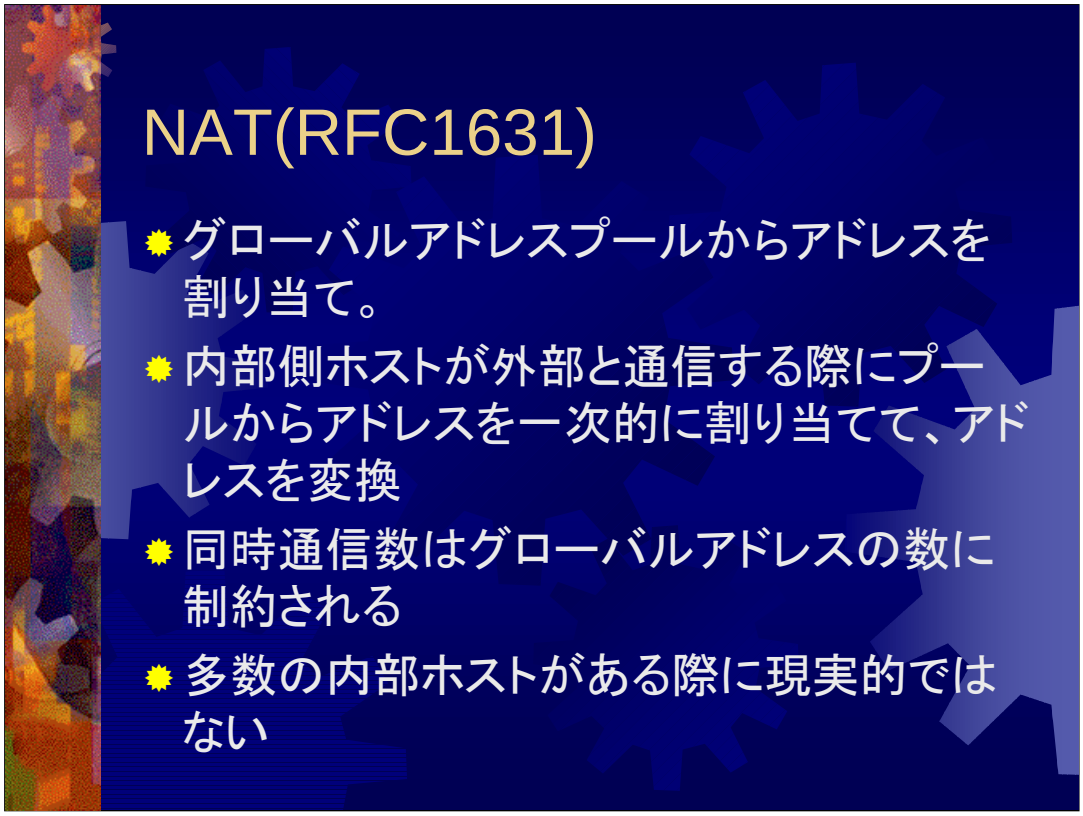
- 1コネクションのみで構成される通信は確実に対応可能
- 複数コネクション／セッションから構成される通信は対応できないものあり。（ストリーミング系の通信など）

ステートフルインスペクション

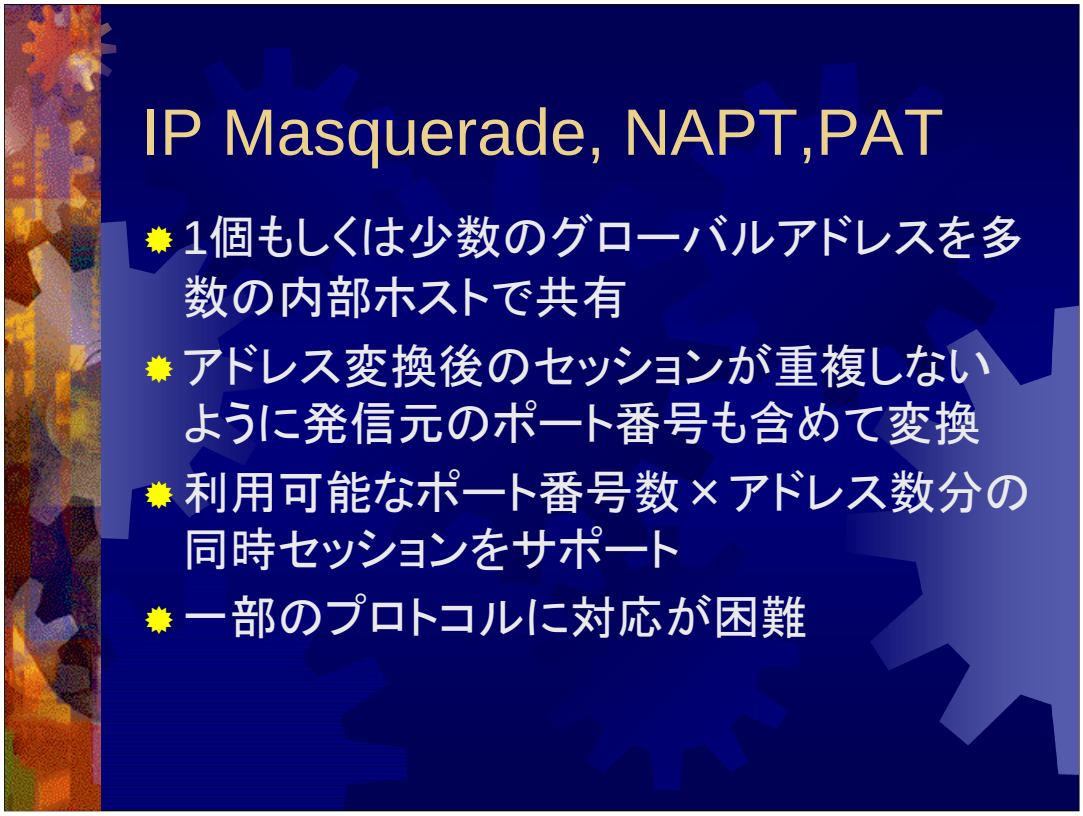
- Checkpoint社オリジナルの用語
  - 本来は、単なるパケットヘッダのみのチェックではなく、アプリケーションレイヤまで、プロトコルをデコードして細部の検査ができる方式のこと。
  - 一般にはダイナミックフィルタと同義に使用されることが多い。C社以外のファイアウォールの場合、厳密にはこの言葉に該当しないものが多いが、ステートフルと称することが多い。



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。



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？)

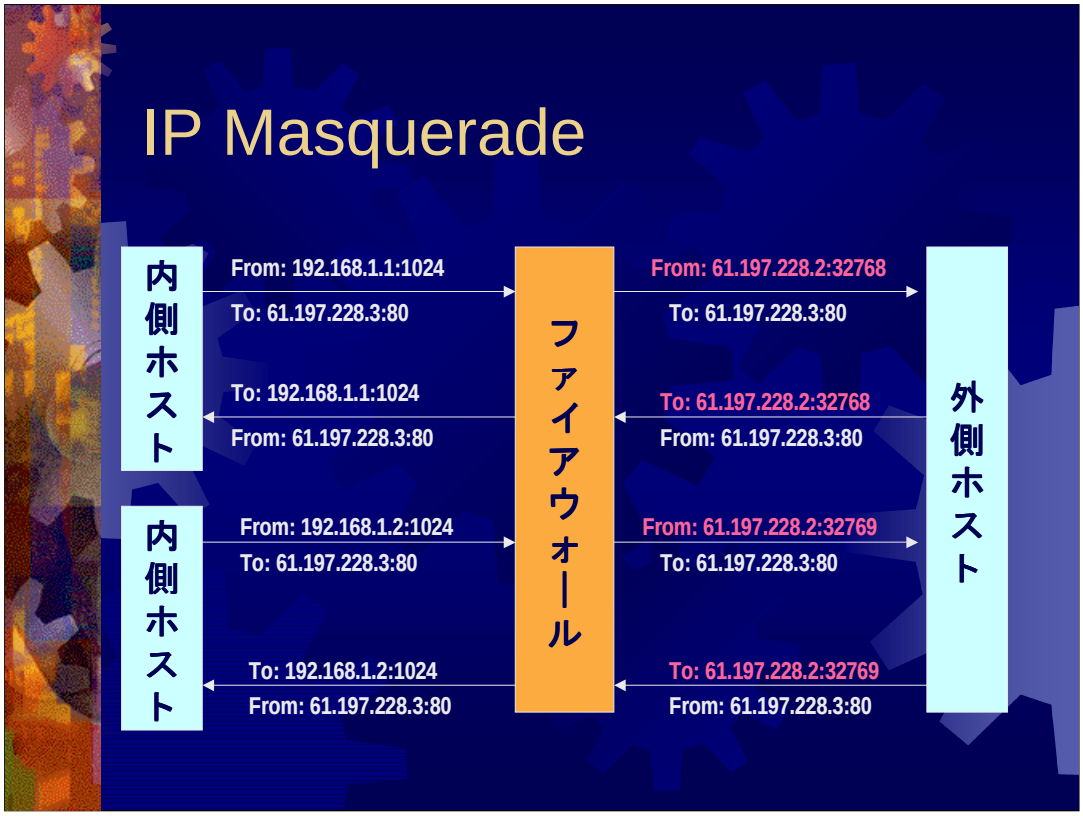


これらの表現は、すべてほぼ同等の機能を表す。

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。

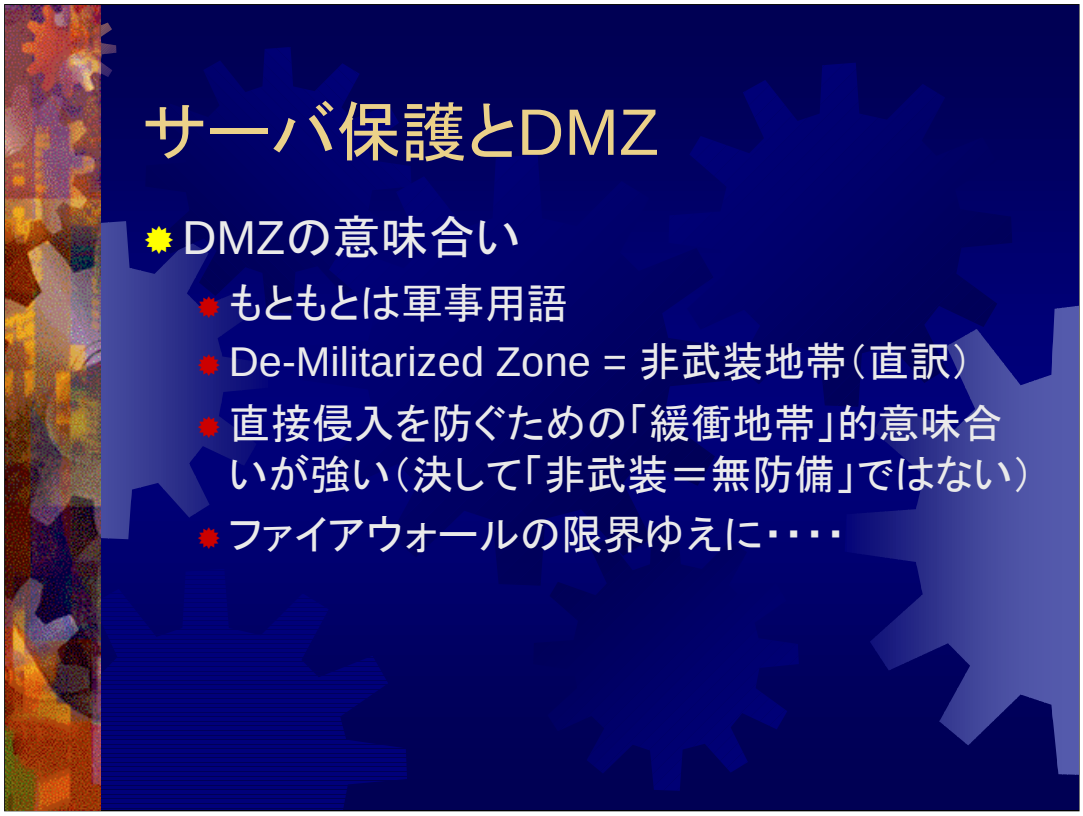
たとえば、一部のリモートアクセスプロトコルなどで、発信元が特権ポートであると扱いがかわるものなどがある。このような場合、特権を使えなかったりする。



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）



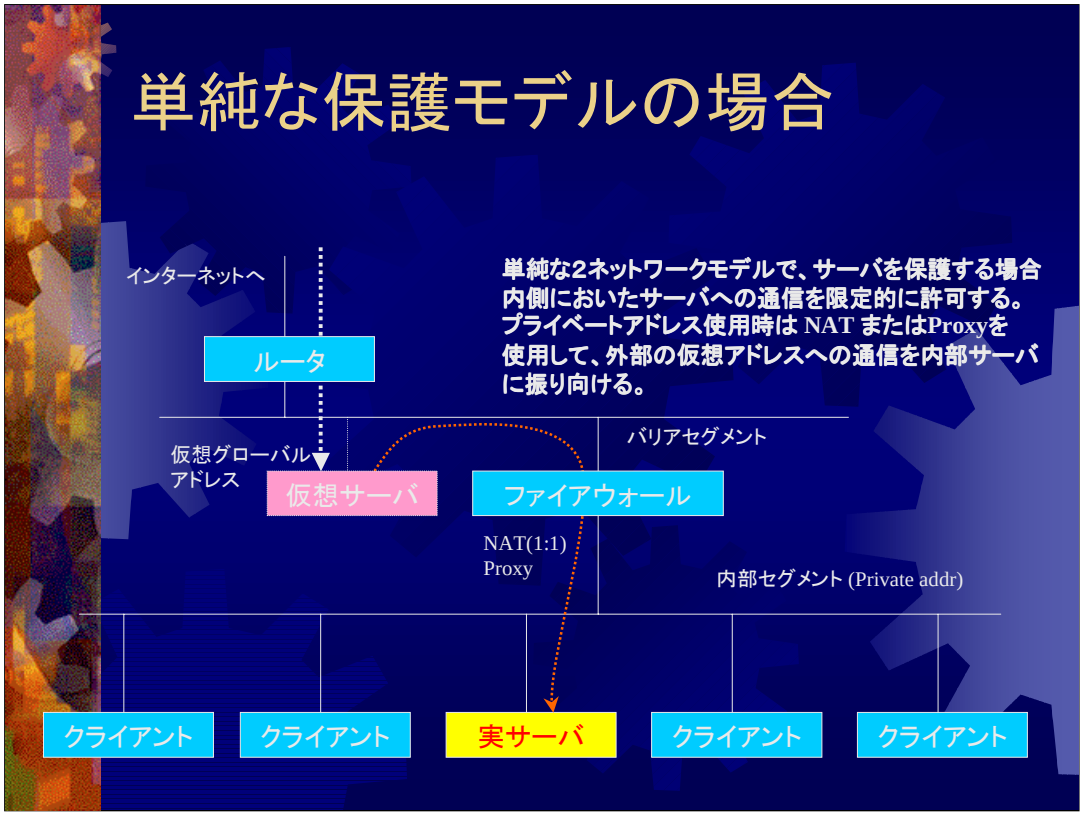
DMZ：誤解のほうが多い言葉

「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。

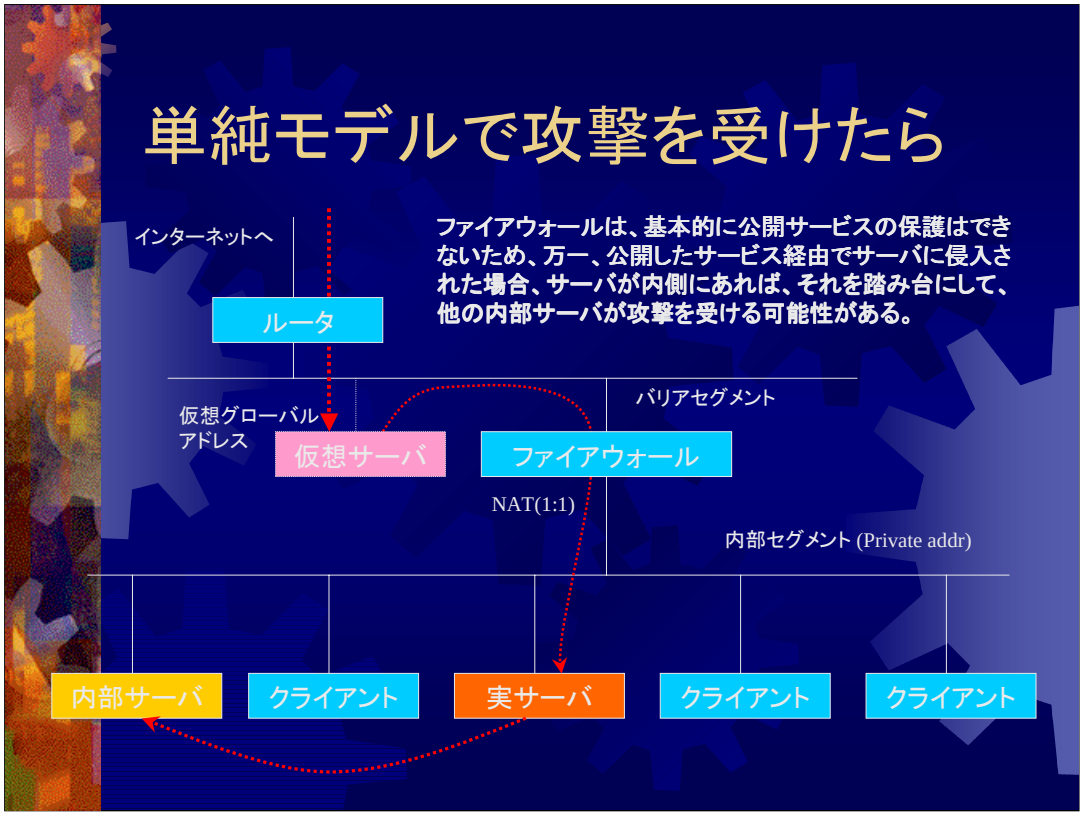
基本的な考え方は、「ファイアウォール」で防げなかった場合の「予防策」

公開サーバの保護

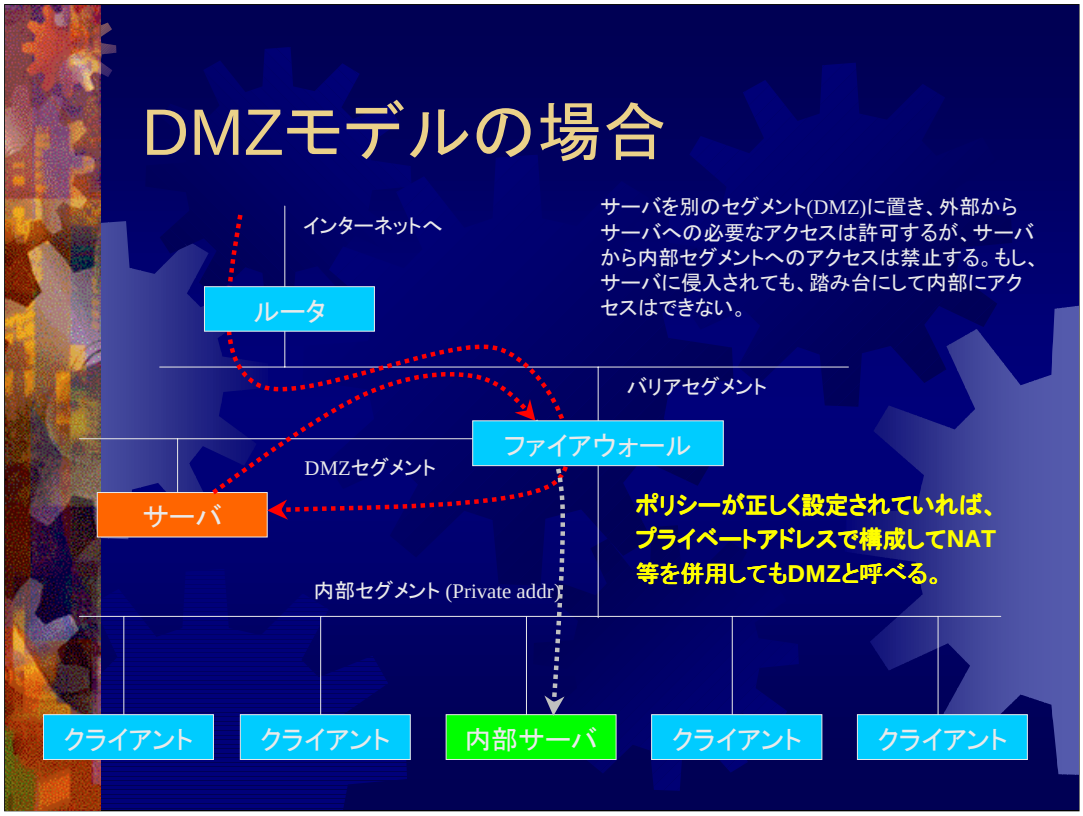
- サーバをファイアウォール下に配置
- 外部からサーバに対して、公開するサービス以外へのアクセスを禁止
- しかし、公開サービスは通さねばならない
  - サーバの公開サービスに脆弱性があると、攻撃、侵入の可能性がある。
  - これをファイアウォールで防ぐことは難しい



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みられるが、「重大な誤解」である。

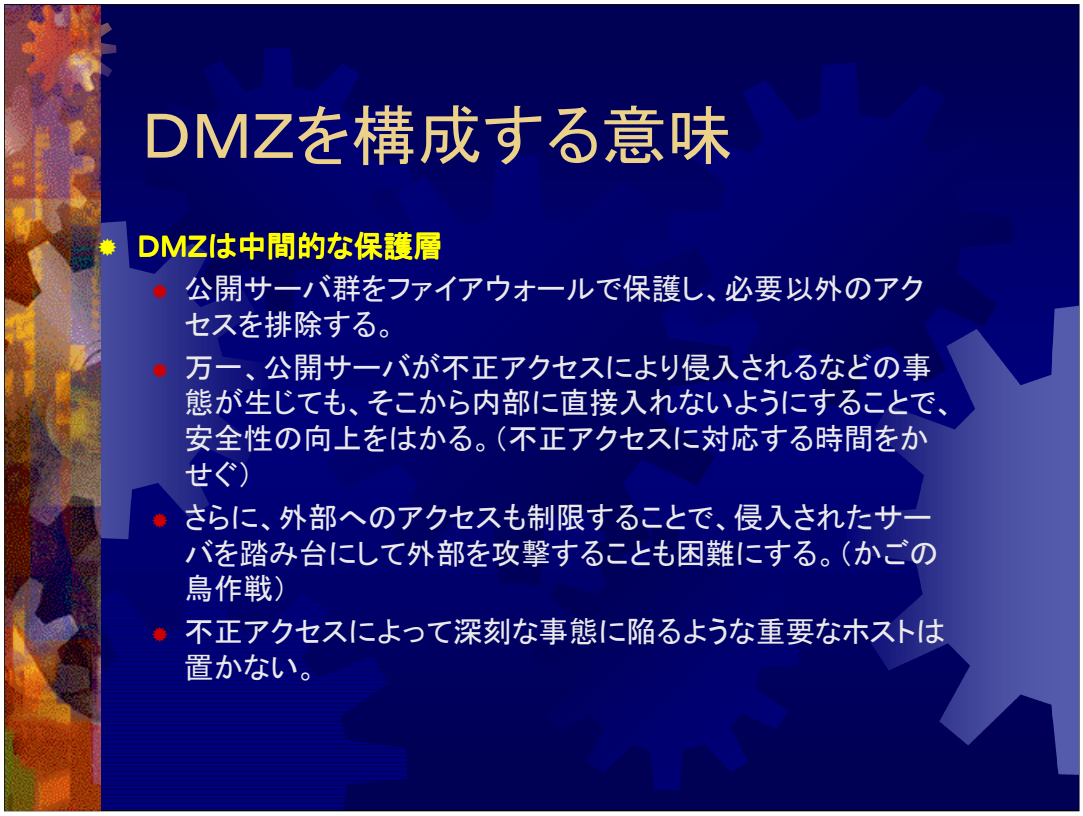


なぜ、「重大な誤解」なのかは、これを見れば一目瞭然。こうならないように考えられたのがDMZの概念だから。



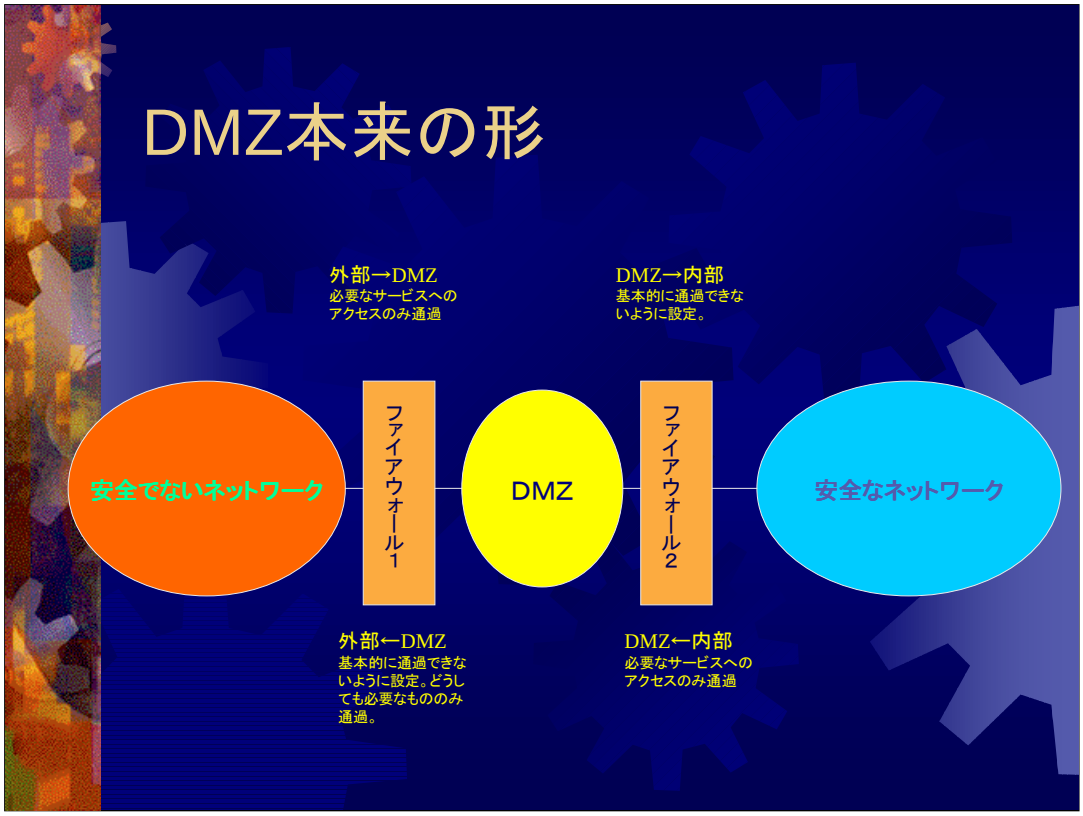
これが、一般的なファイアウォール製品のDMZ構成モデル

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。



原則論はこのとおり。

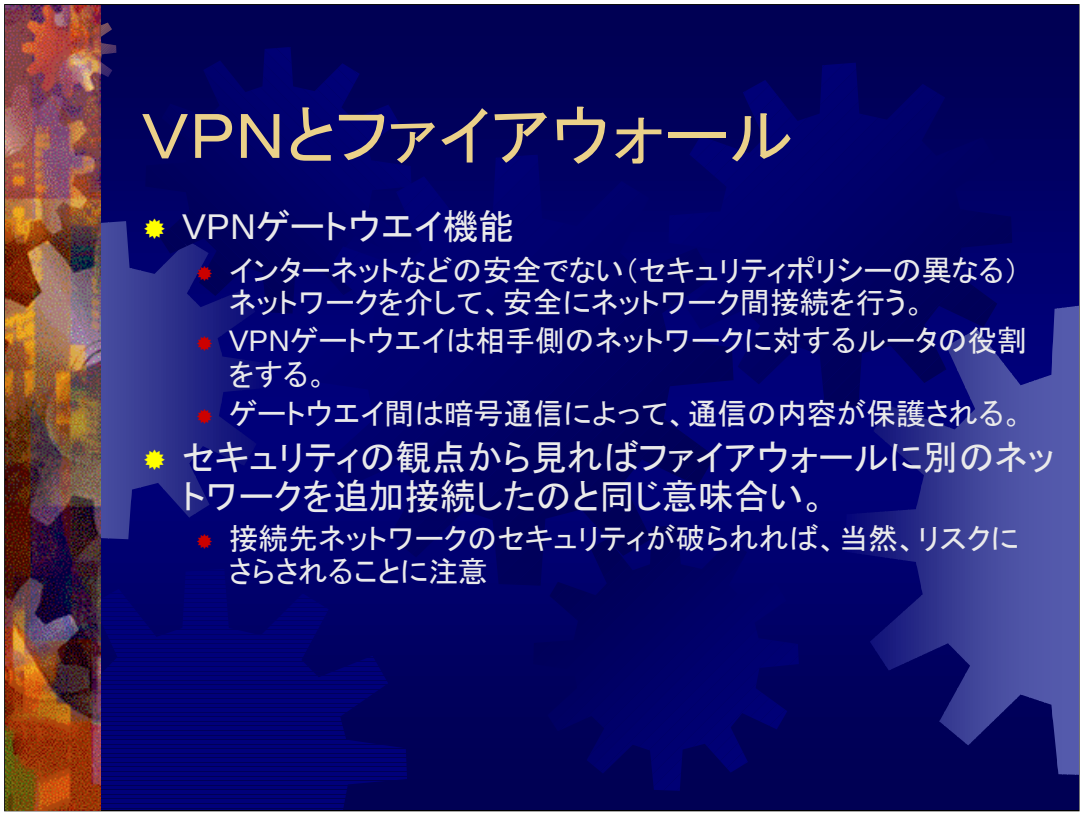
例外を作る場合は、そのリスクを考えて。



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。

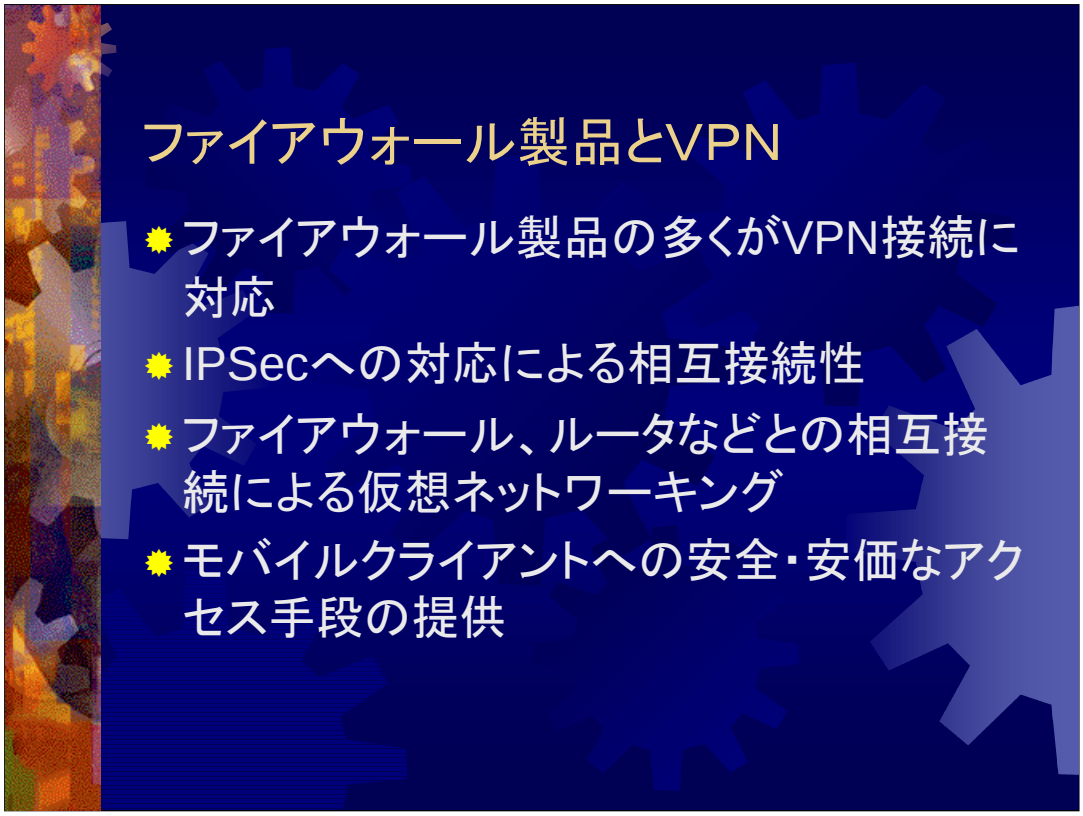
DMZを正しく理解するために

- 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

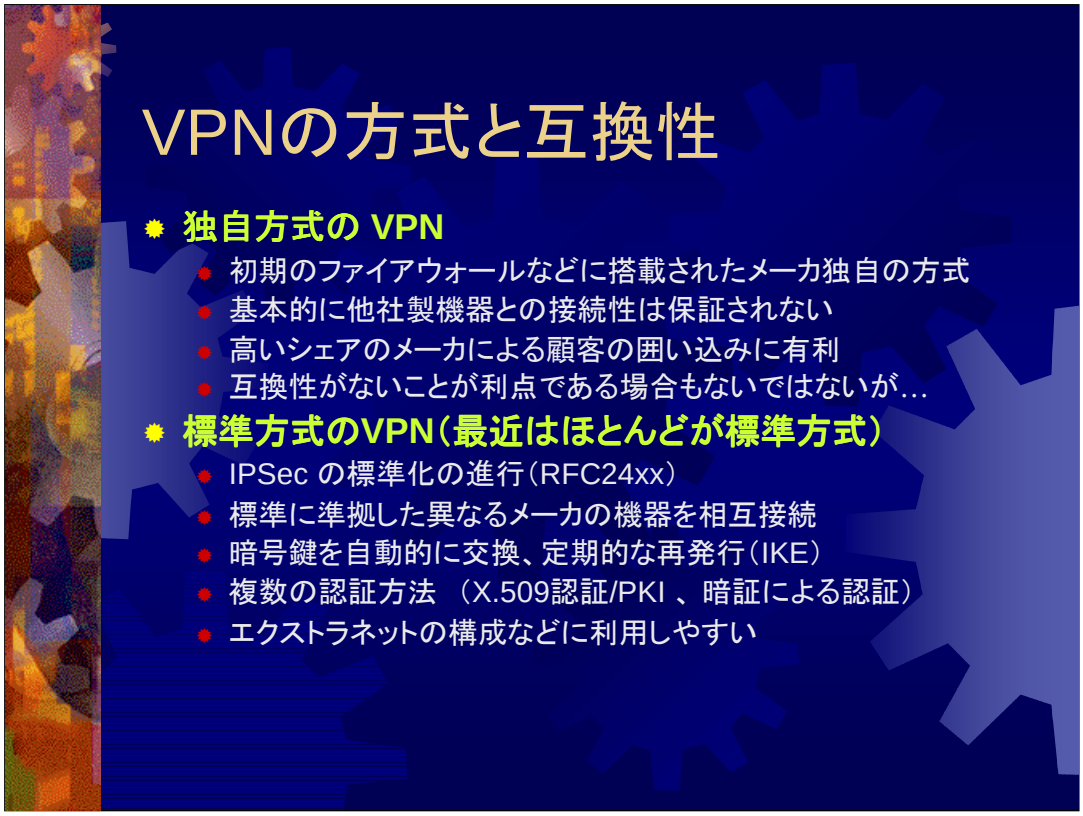


VPN接続は特別な接続ではない。セキュリティ的に考えれば、専用線やダイヤルアップ接続となんら変わらないことに注意。

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。

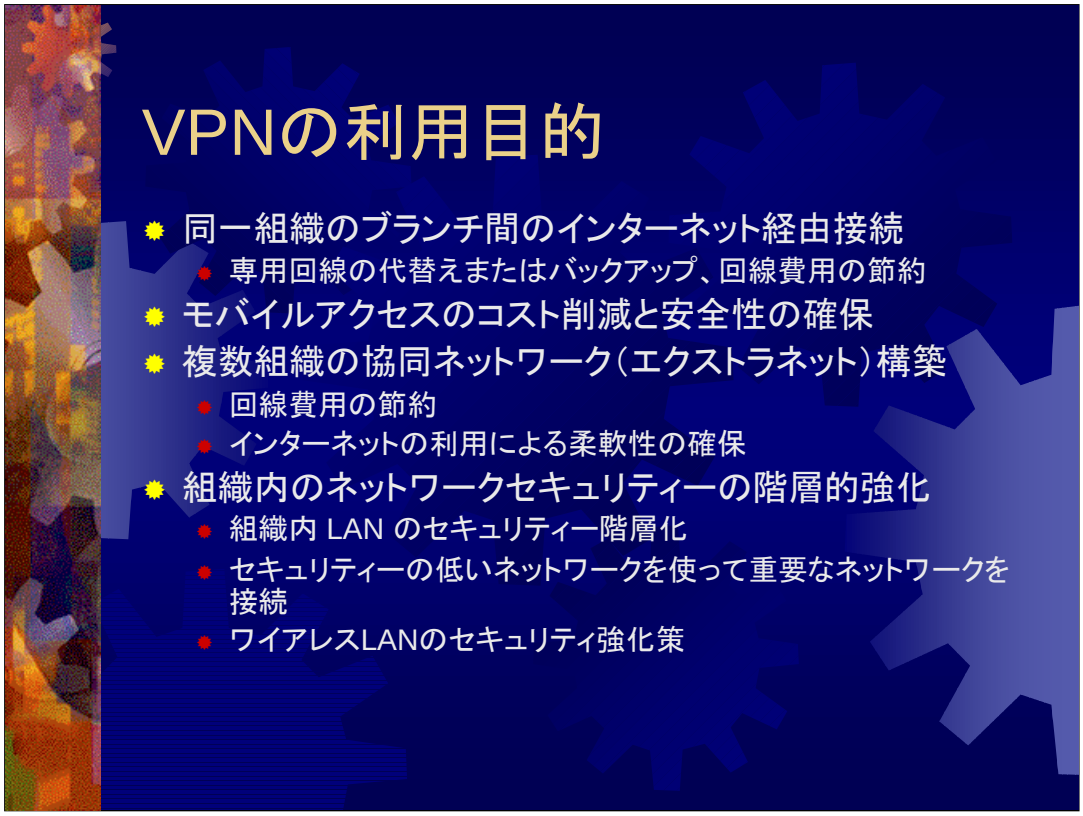


VPN に対応出来る製品はファイアウォール以外にも各種のルータ、専用のVPNサーバなど様々。必ずしもファイアウォールで対応させることが得策でない場合もある。（負荷の問題その他）

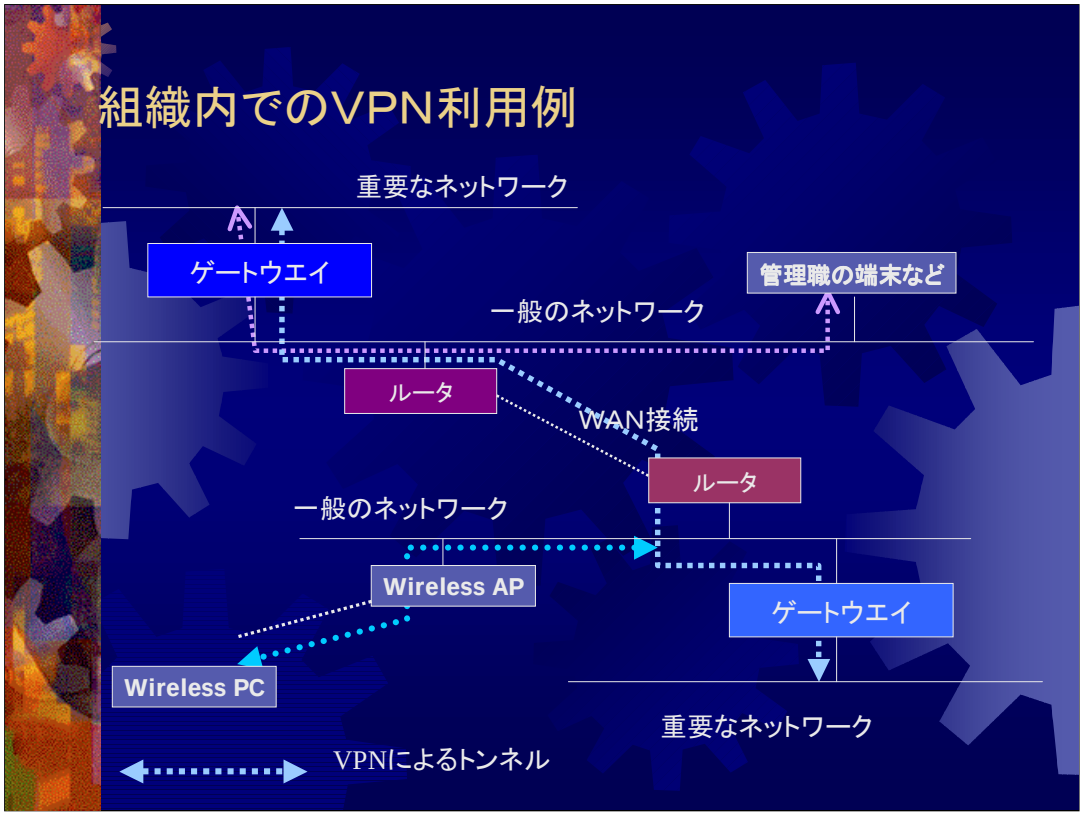


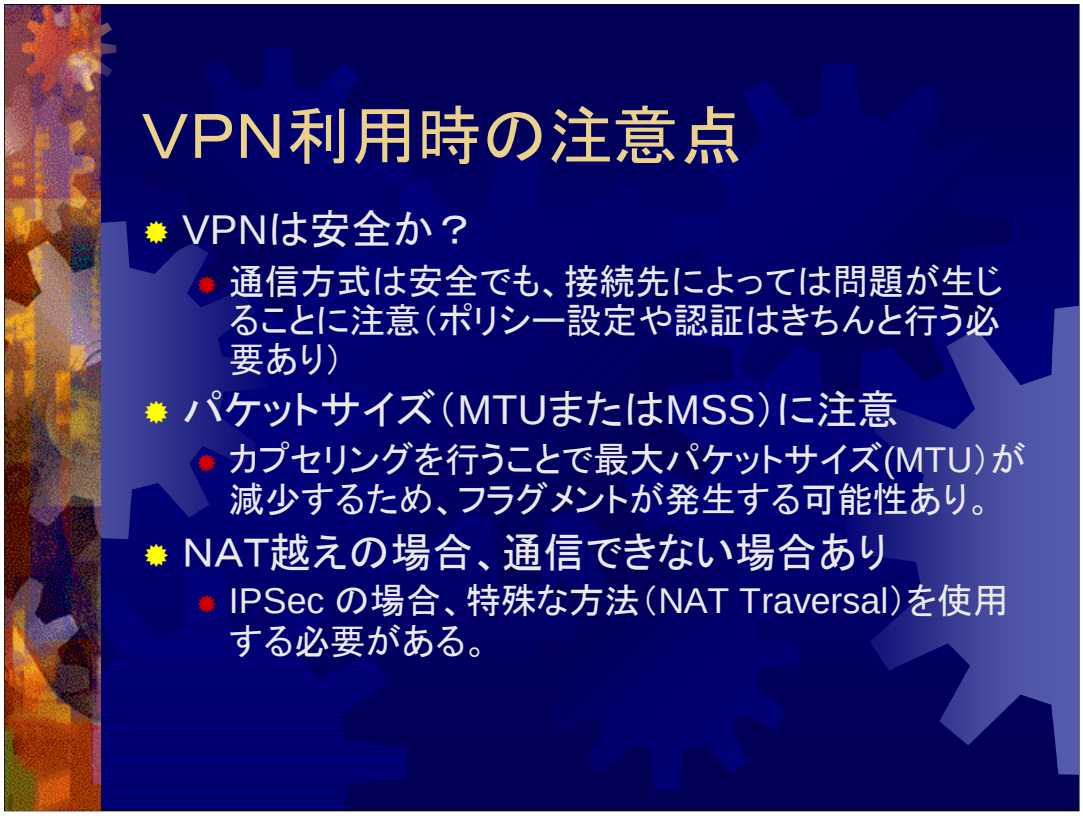
最近は標準方式がほとんど。しかし、標準方式といえども必ずつながるわけではない。

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。

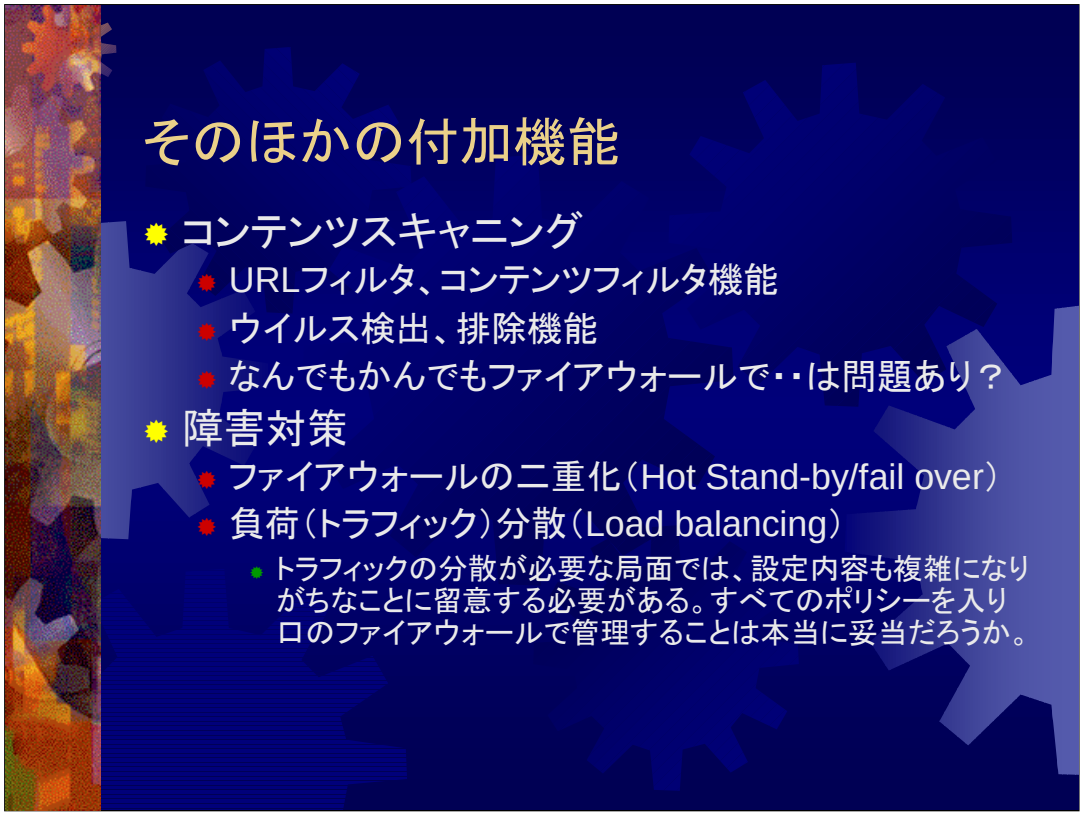

組織内でのVPN利用例
重要なネットワーク
ゲートウエイ
管理職の端末など
一般のネットワーク
ルータ
WAN接続
ルータ
一般のネットワーク
Wireless AP
ゲートウエイ
Wireless PC
重要なネットワーク
VPNによるトンネル



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。

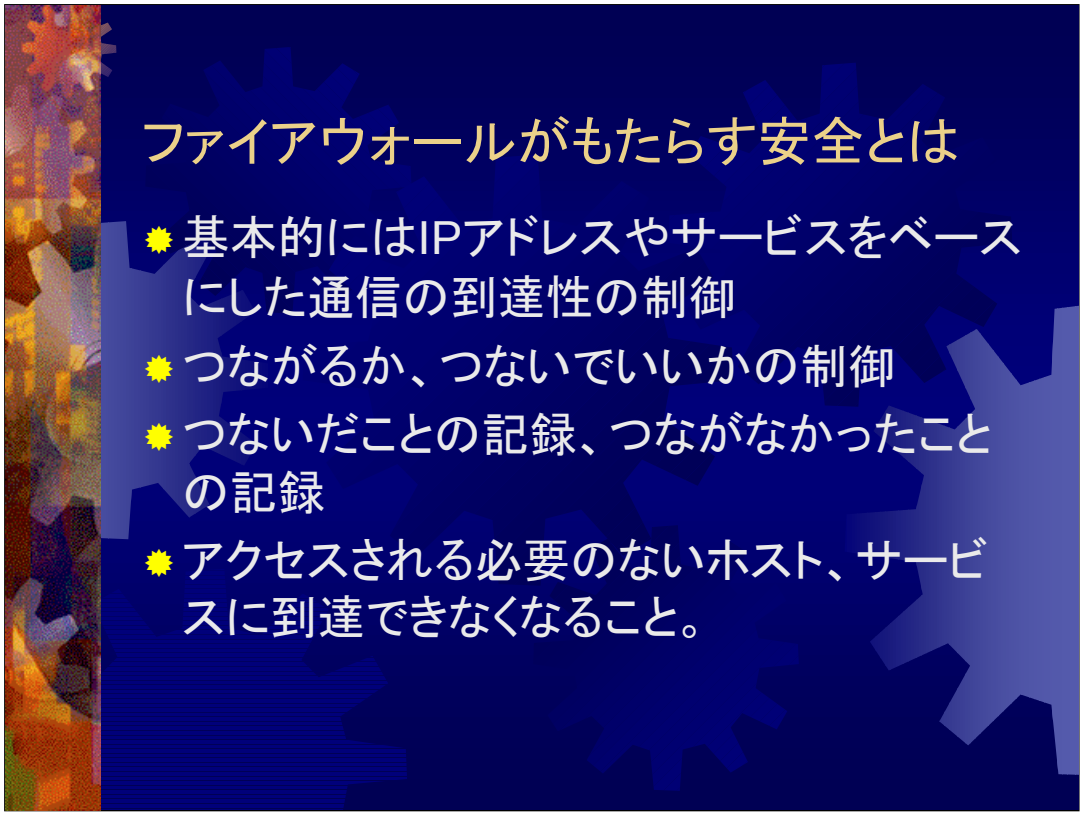
ここでは、IPSec のみを紹介したが、他にも L2TP, PPTP などがあるので、たとえば、個人（ユーザ）ベースでの認証や、クライアントへの内部アドレスの割り当てなどが必要な場合、これらを使うことも考えられる。



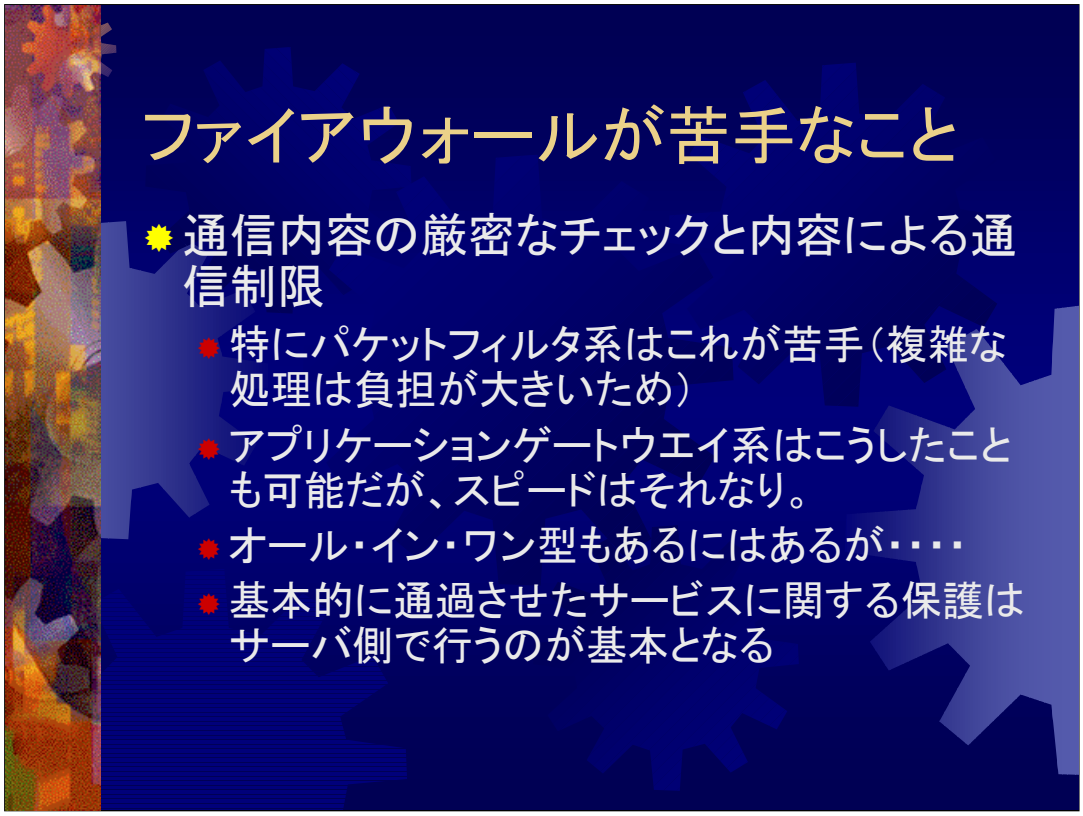
二重化、負荷分散には様々な方法がある。

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）

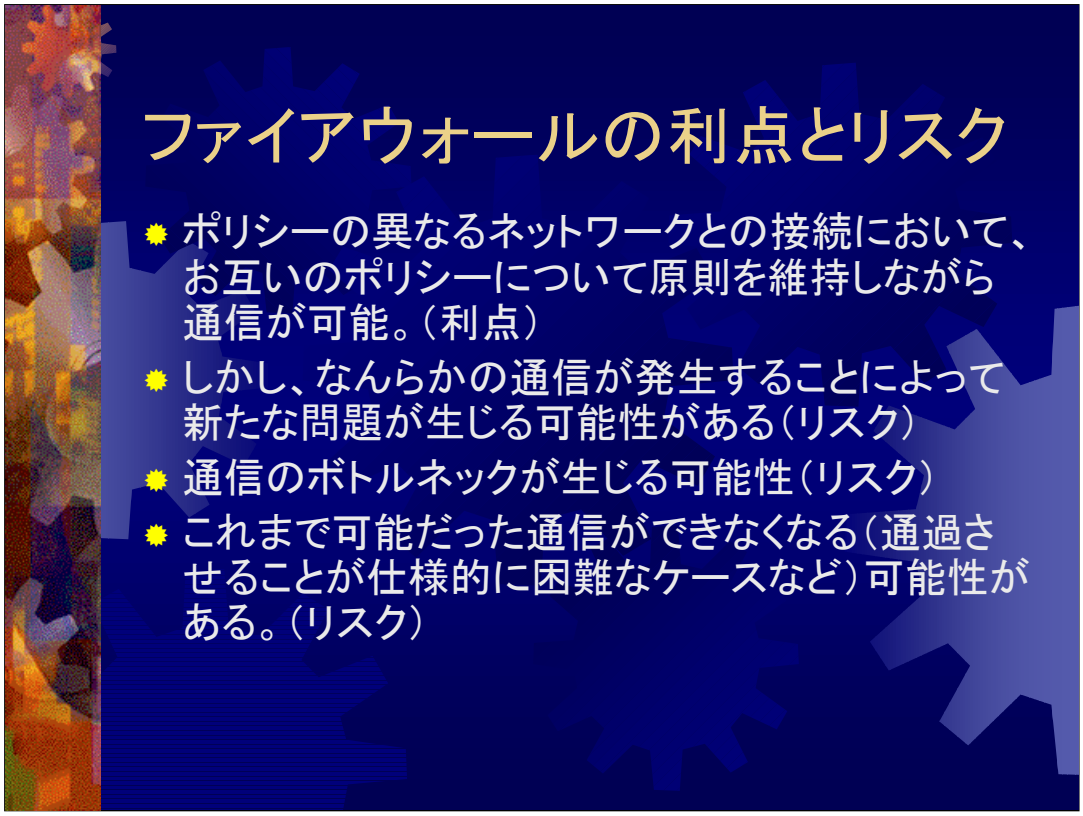

☺ちょっと休憩 ☺



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。

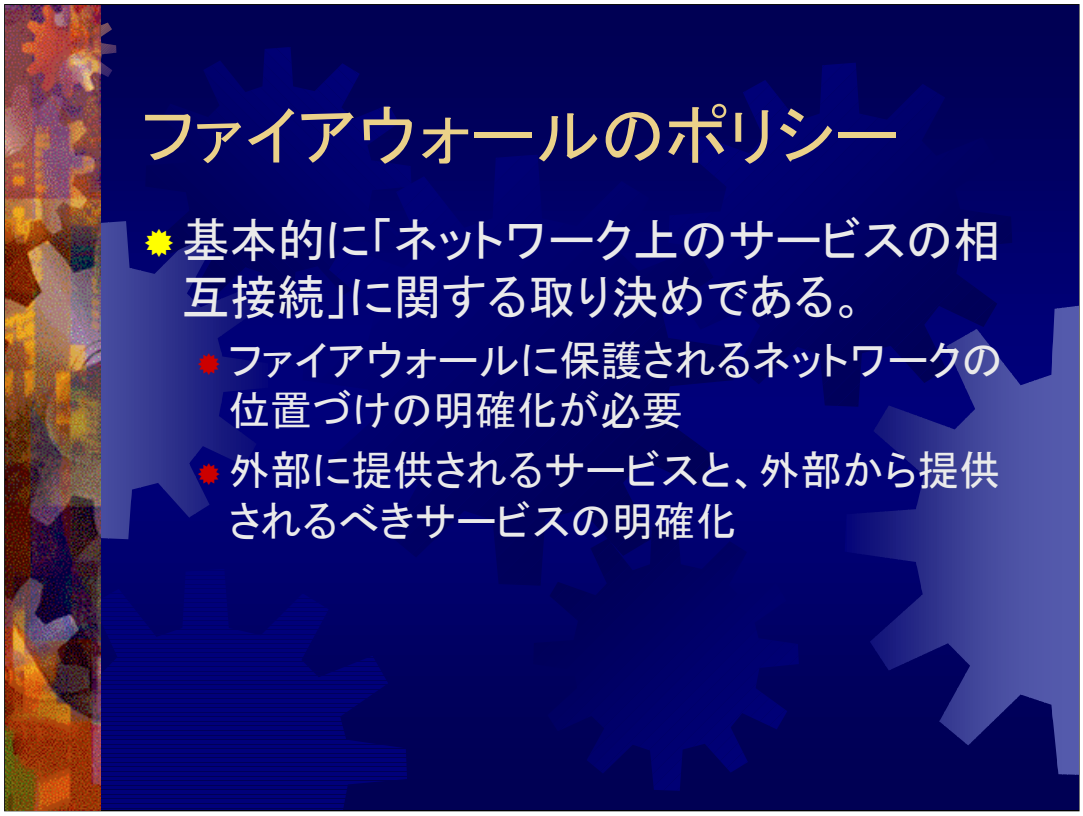


機能と性能のトレードオフに注意

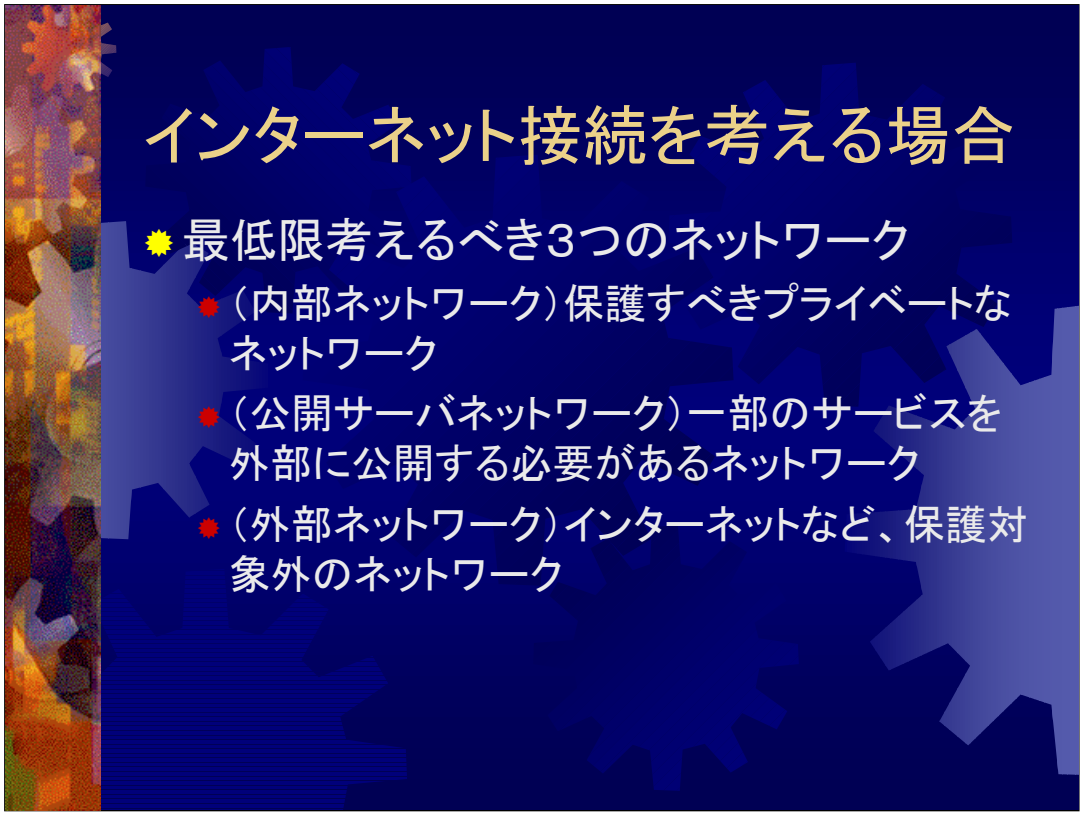


「繋がない」が一番安全。

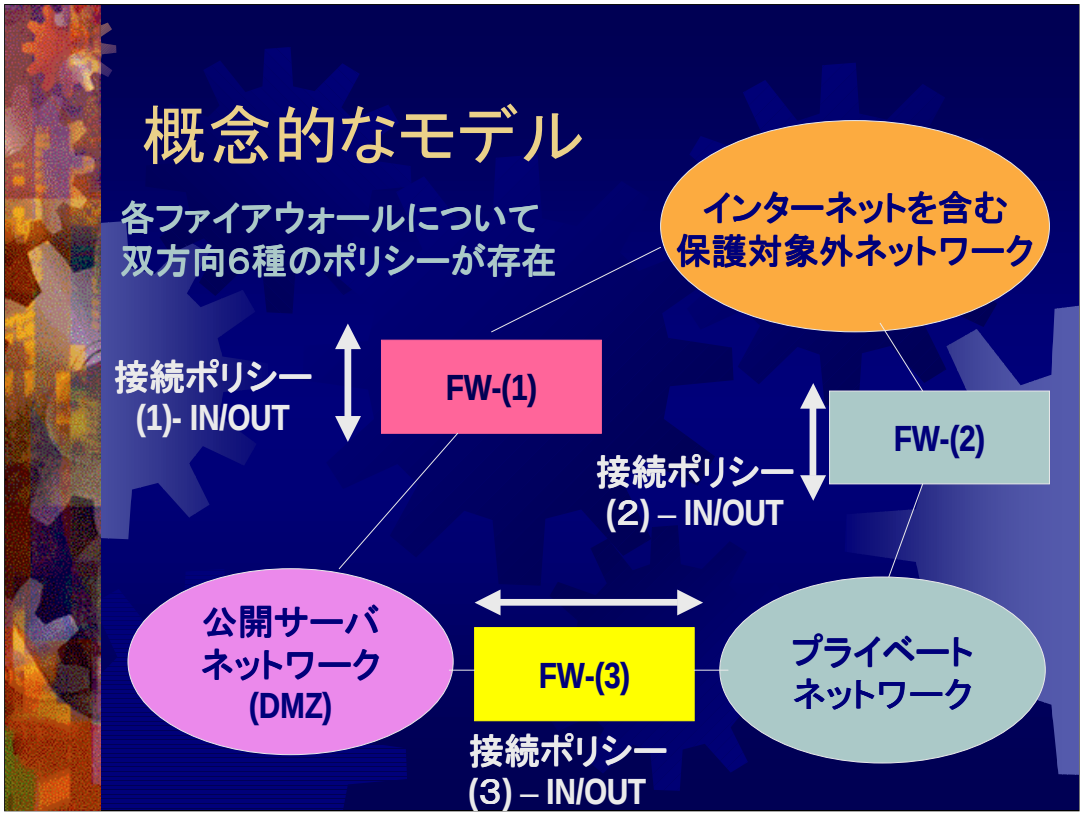
繋ぐ必要があるとしたら・・・・・



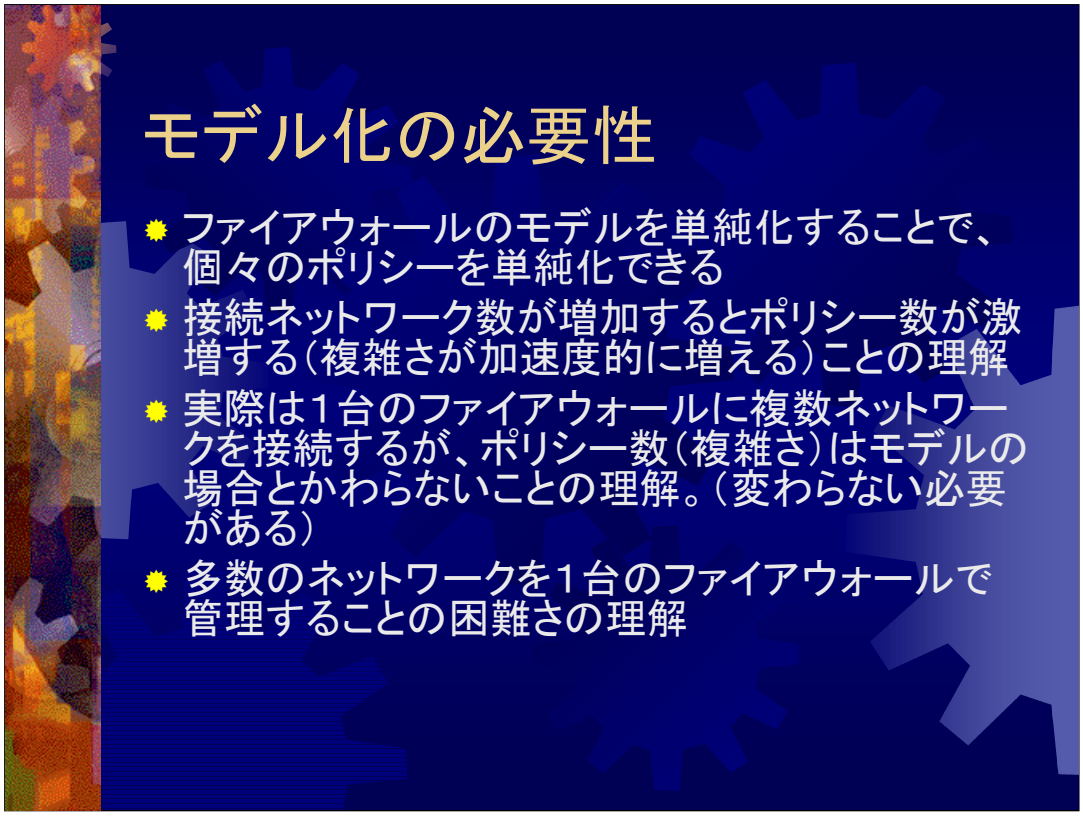
ファイアウォールの「ポリシー」は、いわゆるセキュリティポリシーのサブセットである。サブセットの意味は、「ネットワーク間の相互接続性」に限定された・・・という意味。



（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。



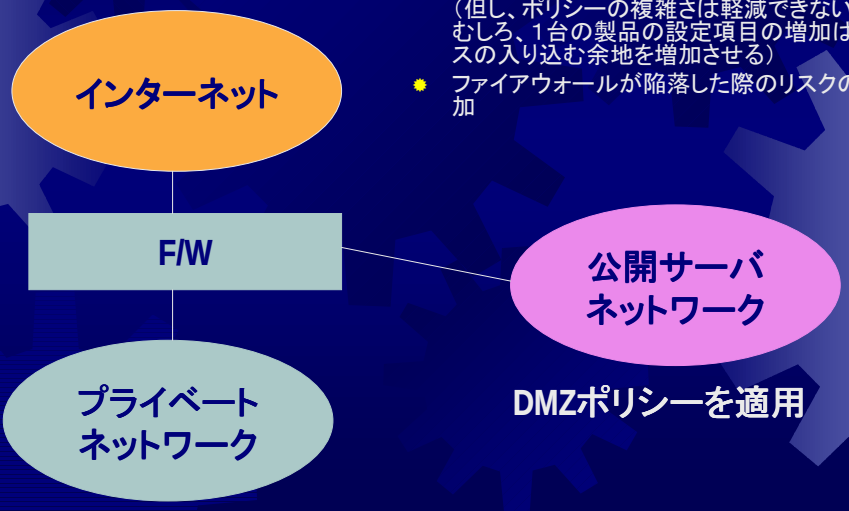
このように複数のファイアウォールを使ったモデルにおきかえて考えると個々のポリシーが考えやすい。



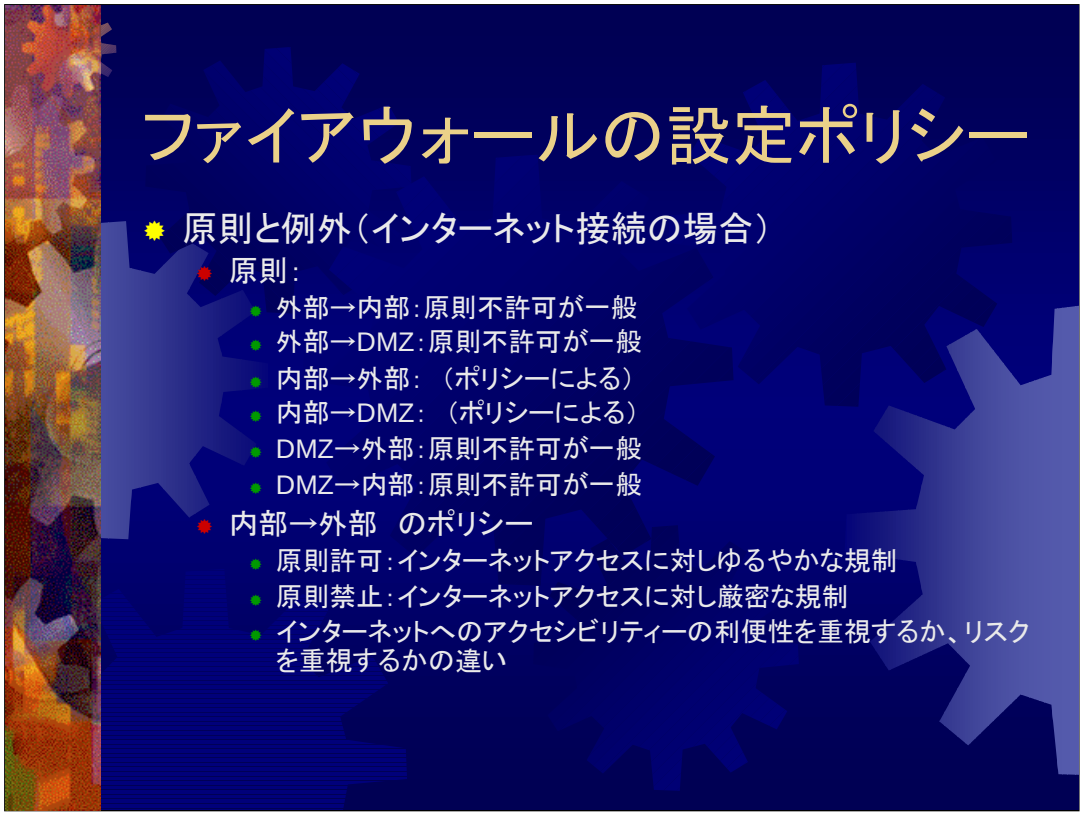
たとえば、多ポートのファイアウォールのポリシー設定は非常に煩雑になる。きちんと整理しないと必ず間違いが起きる。

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



DMZポリシーを適用

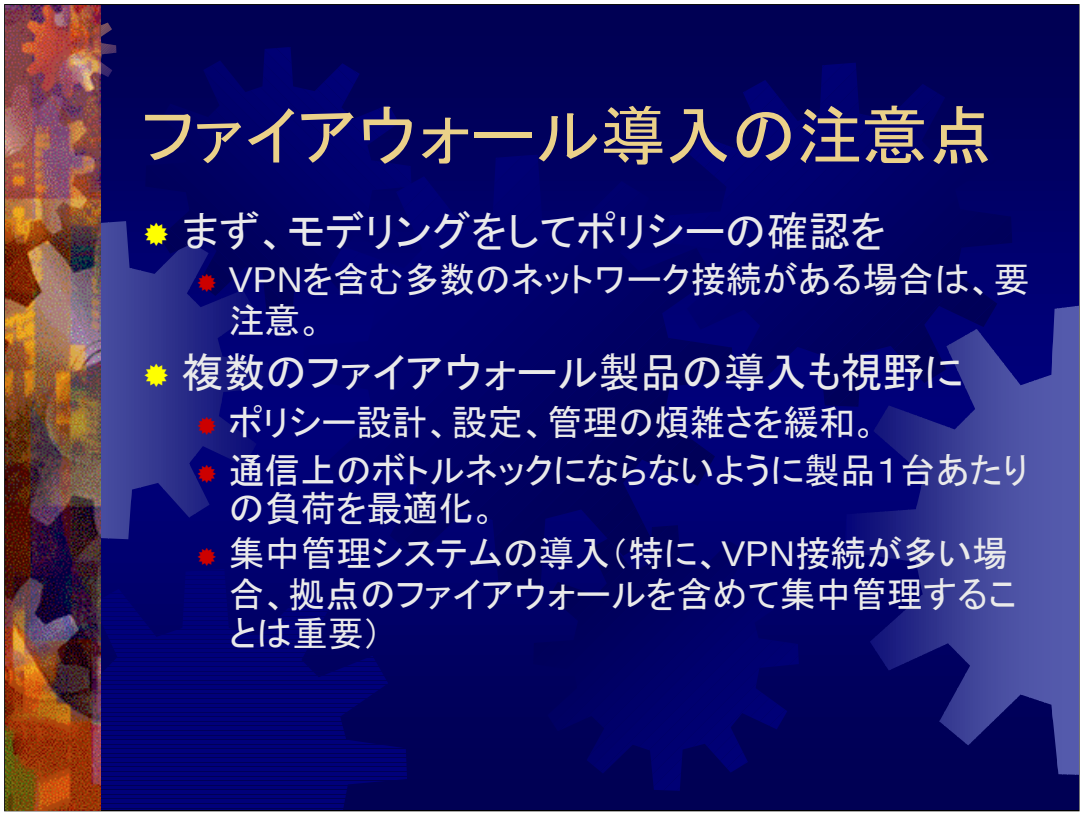


原則を決め、必要に応じて例外を設ける。ただし、原則が骨抜きになってしまわないよう、必ずリスクを考えて例外を設けること。

ファイアウォールの設定ポリシー

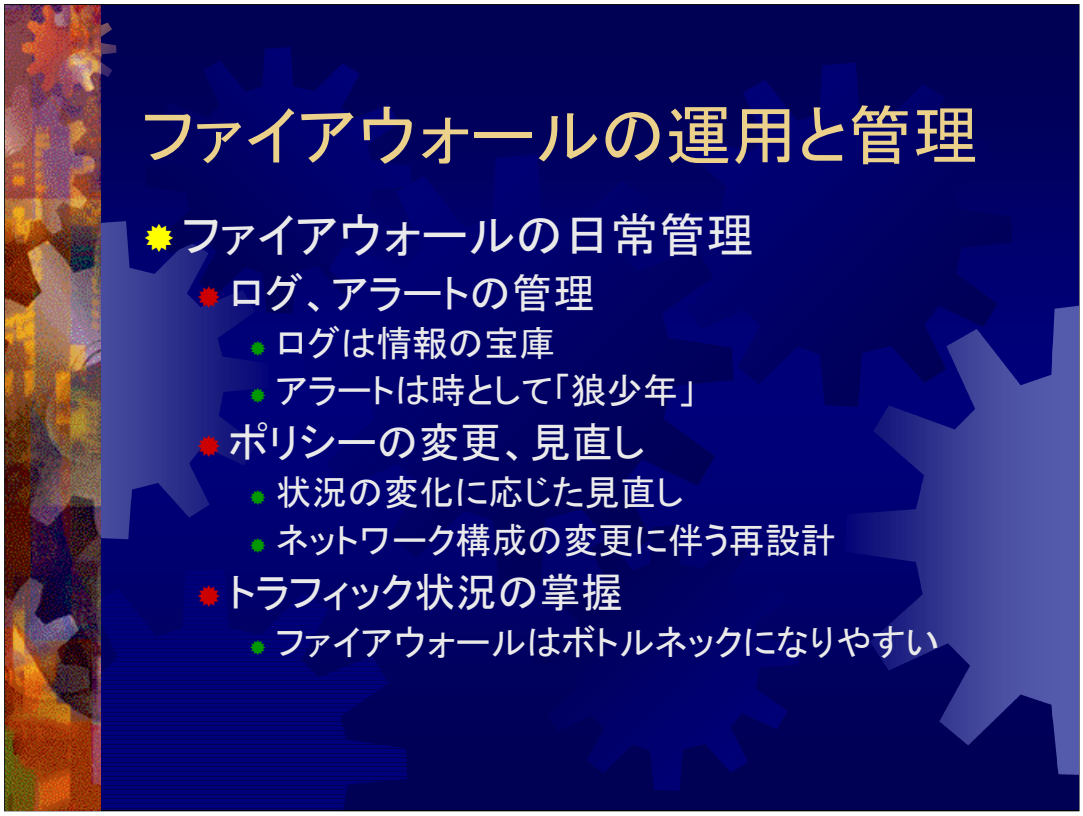
- 原則と例外（インターネット接続の場合）
  - 例外
    - 外部→内部：一般に例外はつくらないほうがよい
    - 外部→DMZ：公開サービスを例外として許可
    - DMZ→外部：運用上必要なもののみ例外として許可
    - DMZ→内部：運用上必要なもののみ例外として許可(*)
    - 内部→外部/DMZ：原則に対し、変更が必要なものを許可または禁止

（＊）あまり推奨できないが・・・・



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。

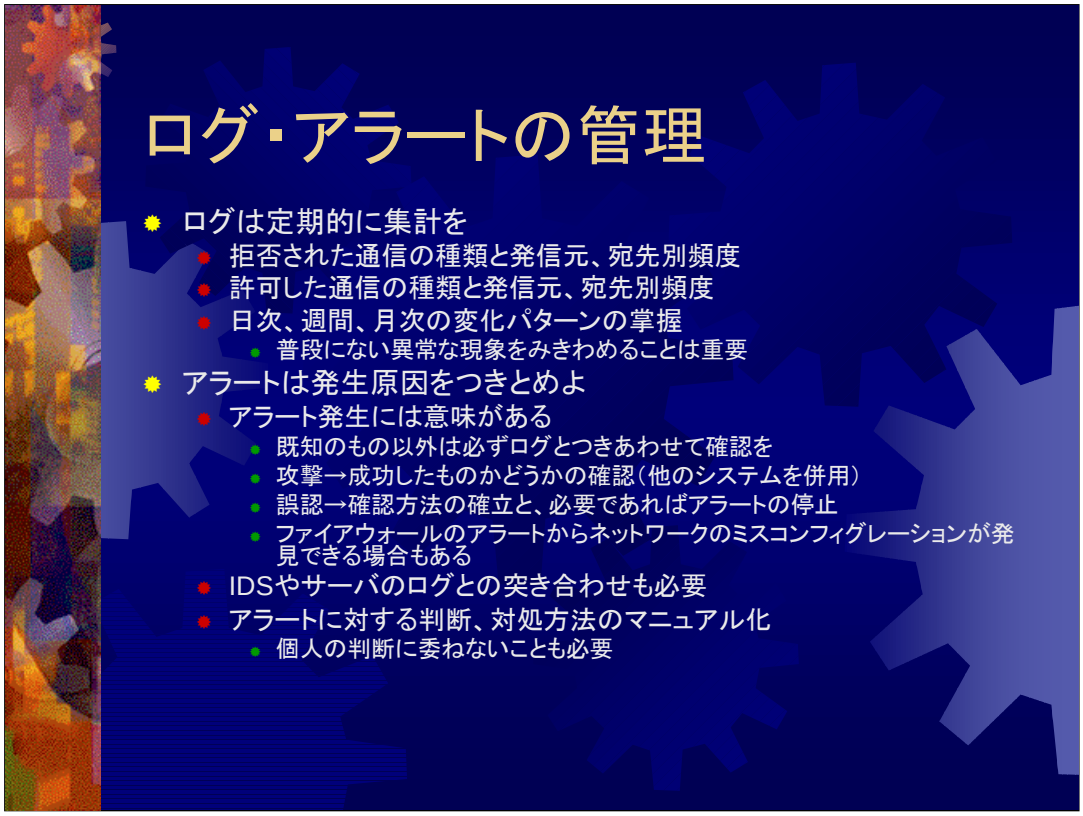
VPNは、集中管理ツールを使うとうまく管理できることがある。



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。

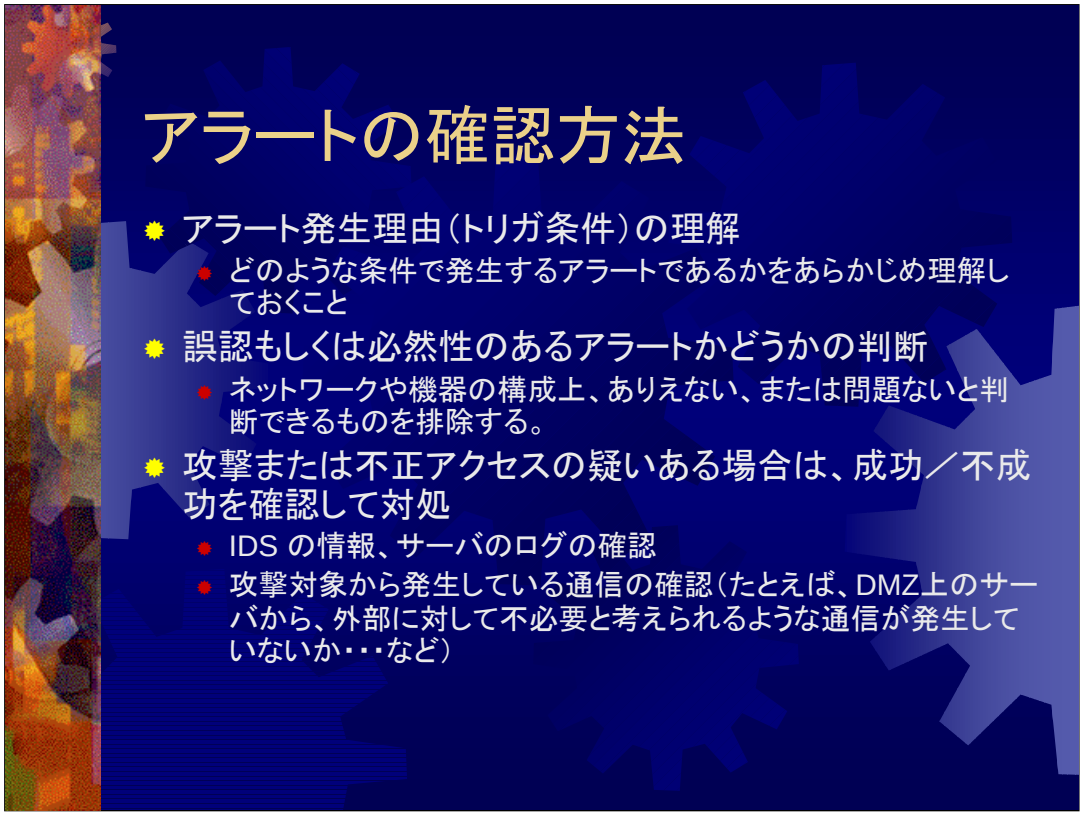
セキュリティのみではなく、トラフィックも重要な管理項目。



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）

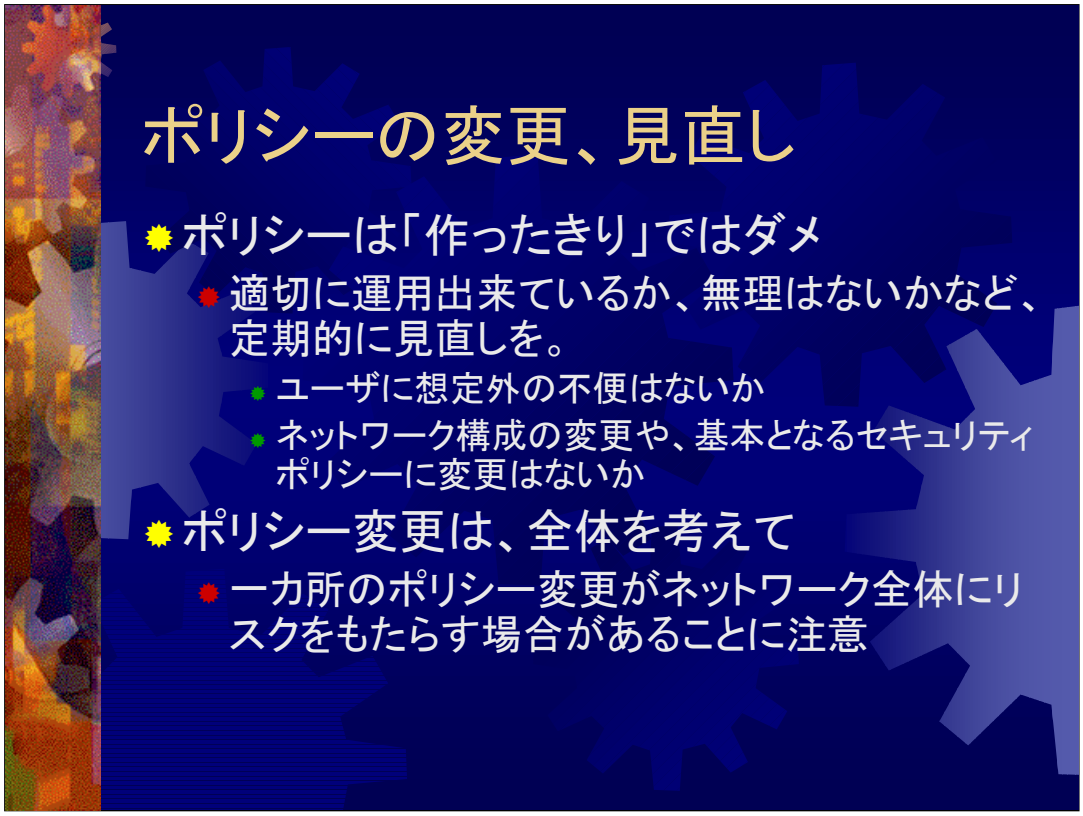
リアルタイムに転送できなければ定期的にバックアップを。

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と、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）



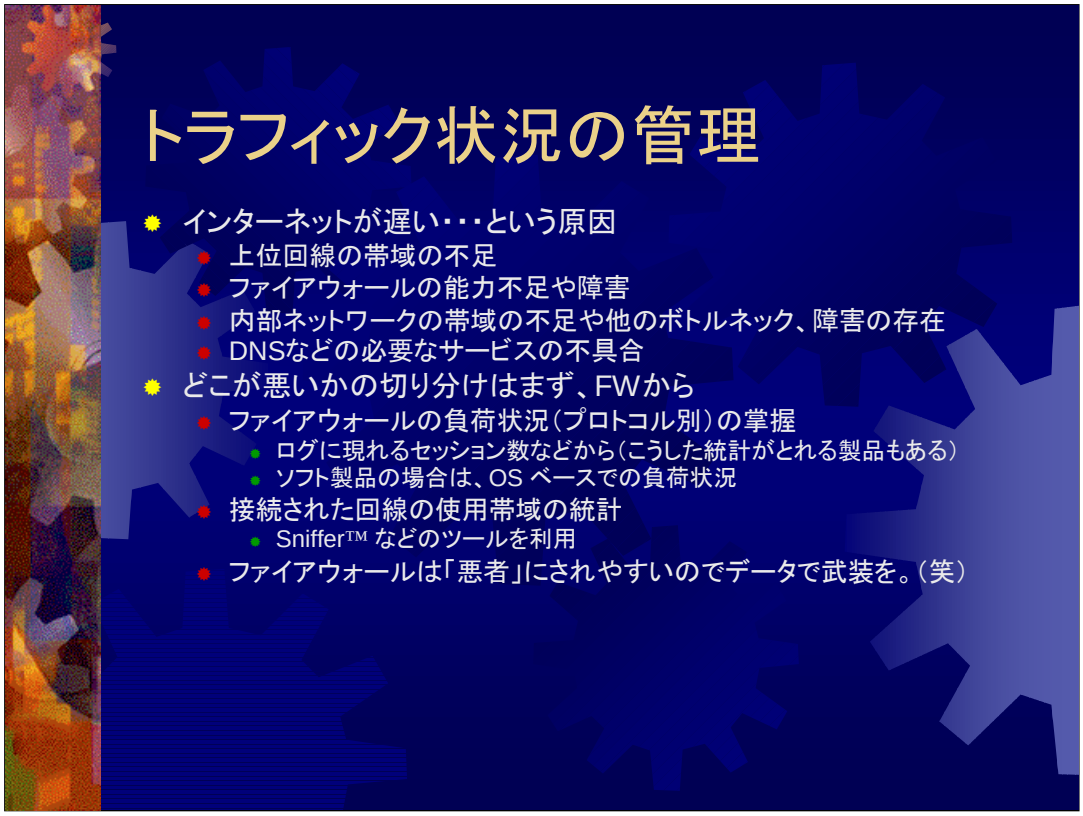
確認はさぼらずに行う。
誤認とわかっているアラートは、排除すべく設定変更や環境の変更を行うことも必要。

なによりも、「狼がきた・・・」にならないことが重要。



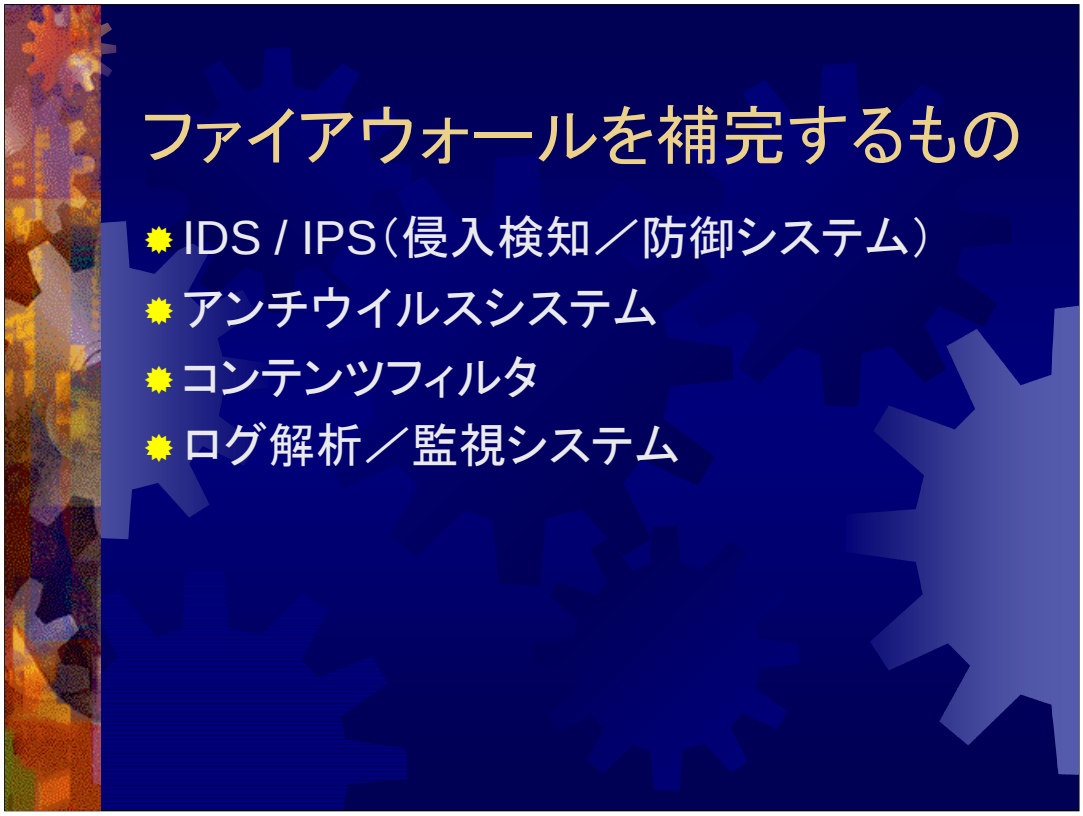
ネットワーク構成を変更した場合は、ポリシーも見直しを。

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。



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。

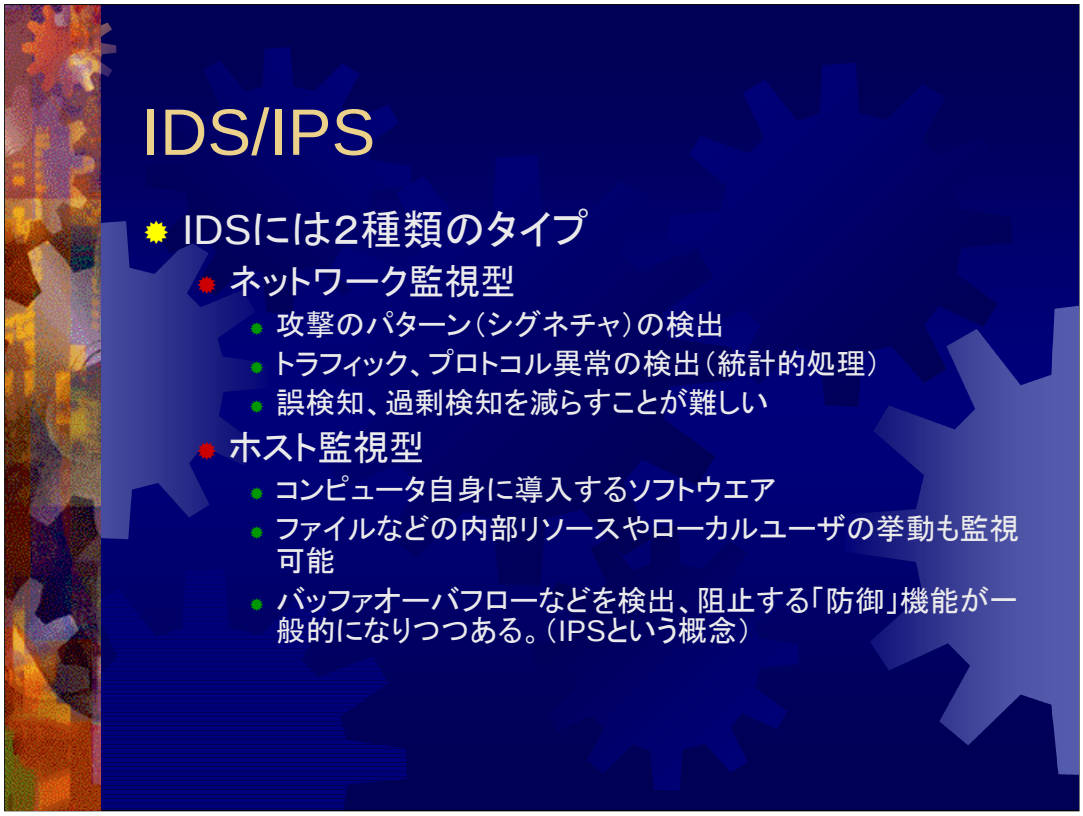
ファイアウォール製品のサポートには、当然として周辺の機器やネットワーク構成についての知識が必要。きちんと切り分けて、まず、ファイアウォールかどうかをユーザに示すことができないと、泥沼に引きこまれることになりかねないので注意が必要。



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。

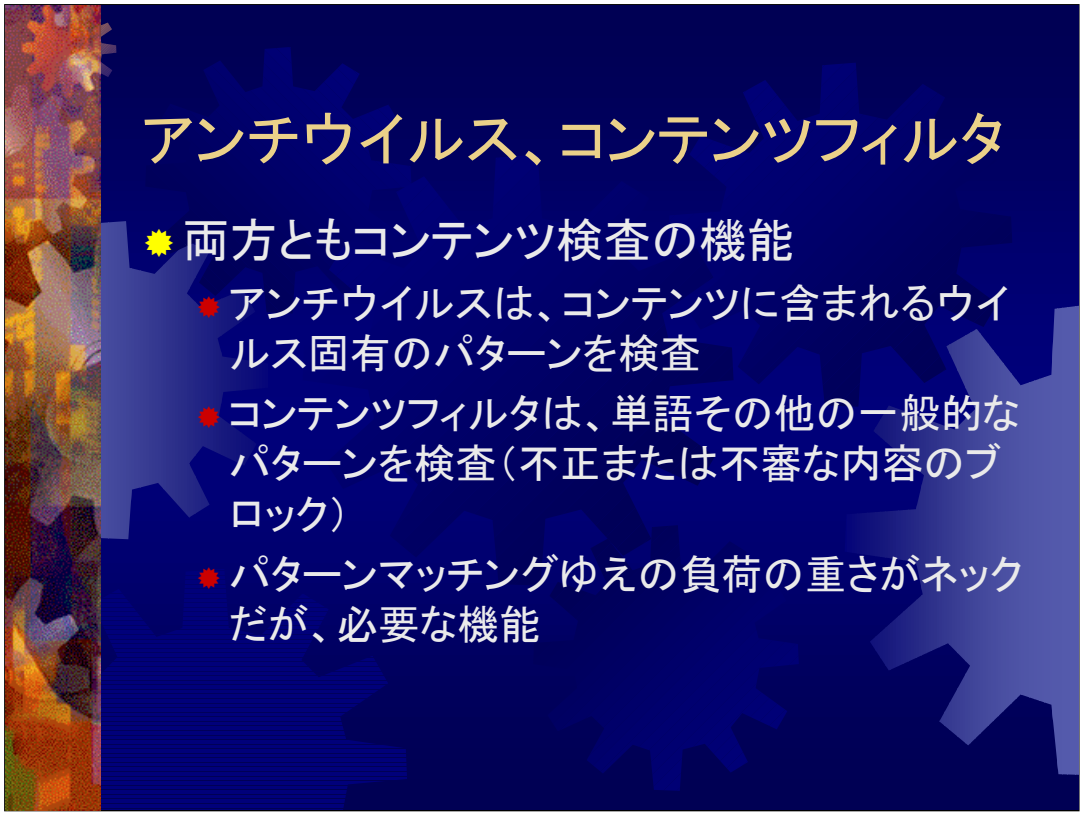
アノマリイ型IDSというものもある（ネットワーク型の一種でもある）。
基本は、トラフィック量を始め、アクセス数、データ転送量など、多くの
パラメータについて統計的に傾向（ベースライン）をもとめ、その傾向
から乖離したような状況が生じた場合に警告するようなタイプのシステム。

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。

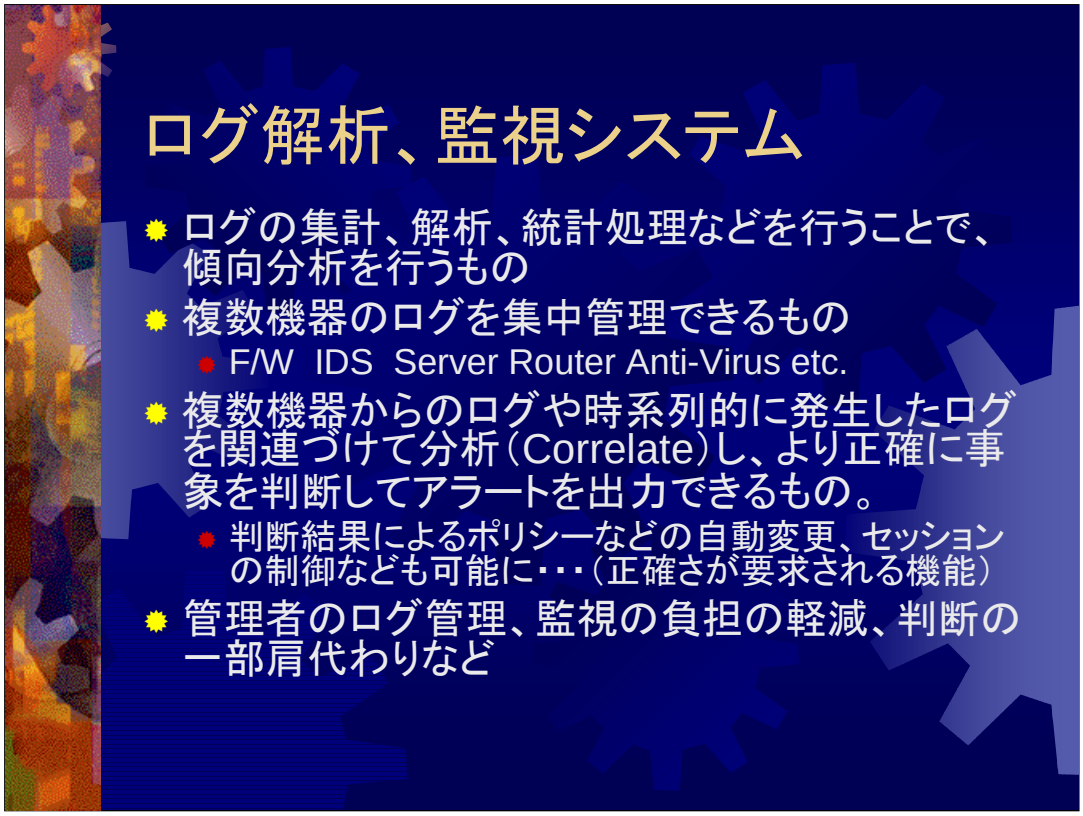
ホスト監視型は、将来的にはアンチウイルスシステムなどと統合されていく可能性が高い。たとえば、リソース（ファイル）監視などにより、未知ウイルスの検出なども可能。

攻撃を検出するだけではなく、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。

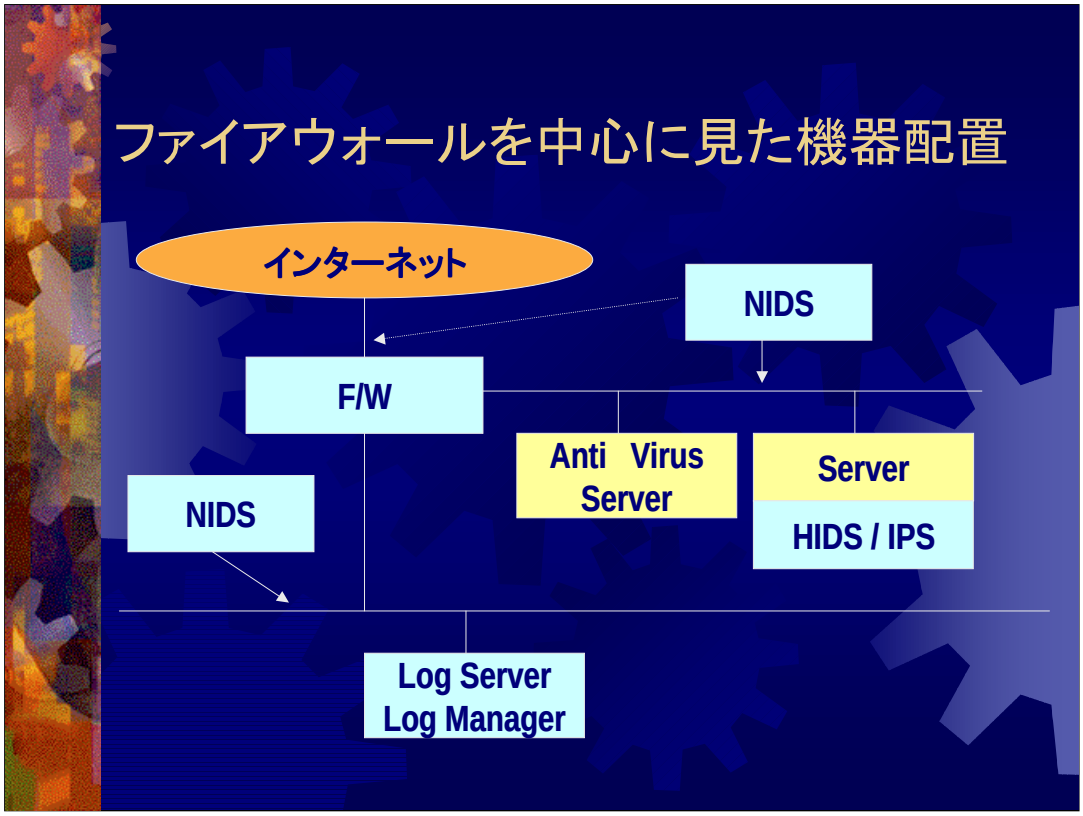
一方、ネットワーク型での攻撃妨害は、誤認との戦い。精度をいかに上げるかがポイント。単独の機器では難しく、複数の機器の情報を相関（Correlate）して、正確な判断を行うようなシステムが必要。

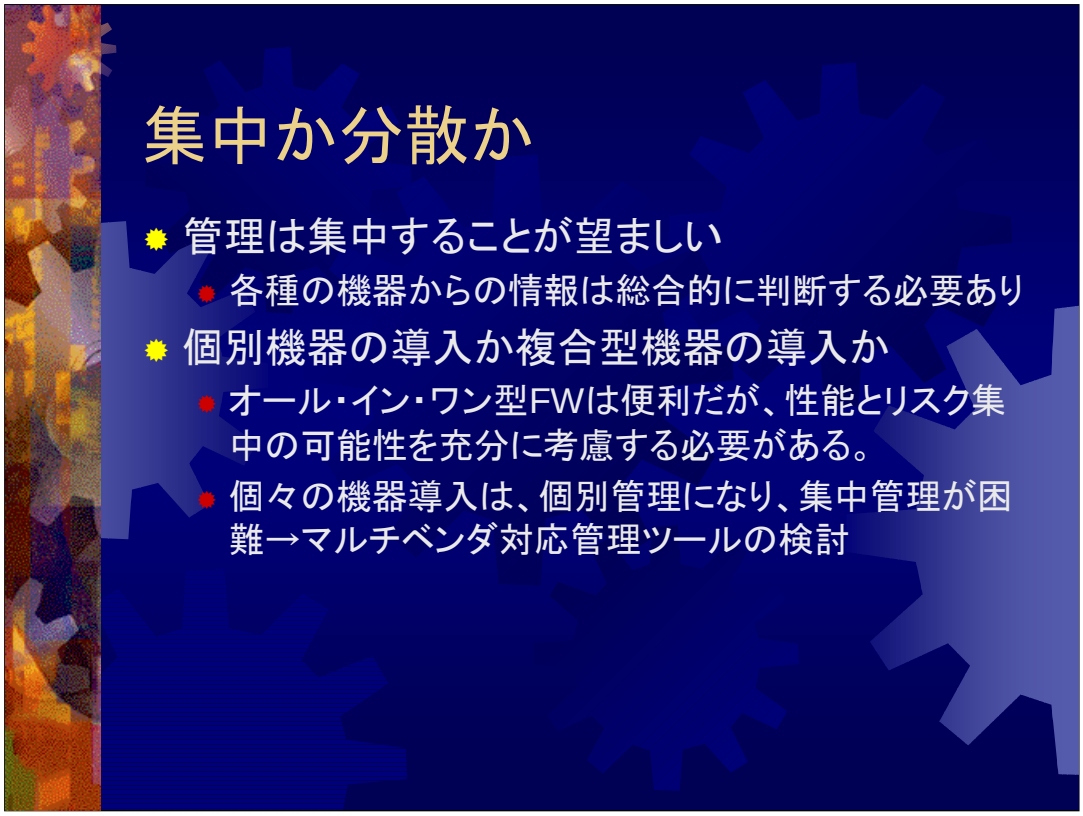


主なアンチウイルスソフトに登録されたパターンは数万種にのぼる。これらをすべてマッチングさせる処理の負荷は想像を絶する。そういう意味では、これをファイアウォールで行うよりも、メールサーバ、Webキャッシュなどの別の部分で行った方が、ファイアウォールが負荷によるボトルネックに陥る危険性が少ない。



同一メーカ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、管理するだけではなく、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くる。


ファイアウォールを中心に見た機器配置
インターネット
NIDS
F/W
Anti Virus Server
Server
HIDS / IPS
NIDS
Log Server
Log Manager



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 からもダウンロード可能です。
  - http://www.kazamidori.jp/SECURITY/
- E-mail: futagi@kazamidori.jp