ファイアウォール 基礎から応用

Internet Week 2006　T9

二木 真明
CISSP　**住商情報システム㈱**

Rev. 1.2

ファイアウォールを体系的に学ぶ

- ネットワークに繋がれた情報資源を守るには
  - ネットワークのアクセス制御とファイアウォール
- ファイアウォールの基本方式
  - パケットフィルタとProxy、それらの発展型
- ファイアウォールの付加的機能
  - VPN、攻撃防御、ウイルス対策とコンテンツフィルタ
  - UTMとは
- ファイアウォールの導入設計
- ファイアウォールの運用とログの管理・監視

ネットワークの守り

- 実はネットワークに繋がっている「資源」を、ネットワーク経由の攻撃から守ること
- 個別に守るのか、一括して守るのか
  - 答えは両方！！　(階層的防御モデル)
    - (レベル1) そのネットワークにいるすべての資源に対して行われる必要がない通信はネットワークレベルで止めてしまおう
    - (レベル2) ネットワーク内の通信で許可、禁止が必要なもの、より細部のチェックが必要なもののみ個々の機器 (ホスト) で制御しよう
    - 場合によっては、二重に防御するような場合もありうるかもしれない (フェイルセーフ的発想)

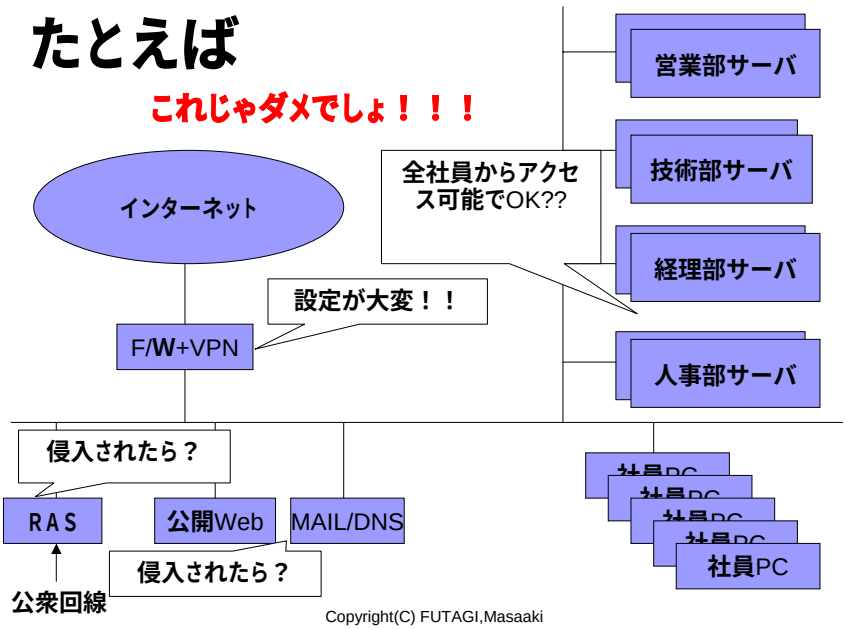
ネットワークレベルでの「守り」

- あるネットワークと他のネットワークの境界 (perimeter) に関所 (gateway) を設けて、必要な通信のみを通すこと
  - 通信の宛先 (ホスト、サービス) による制御
  - 通信の発信元による制御
  - 通信の内容による制御

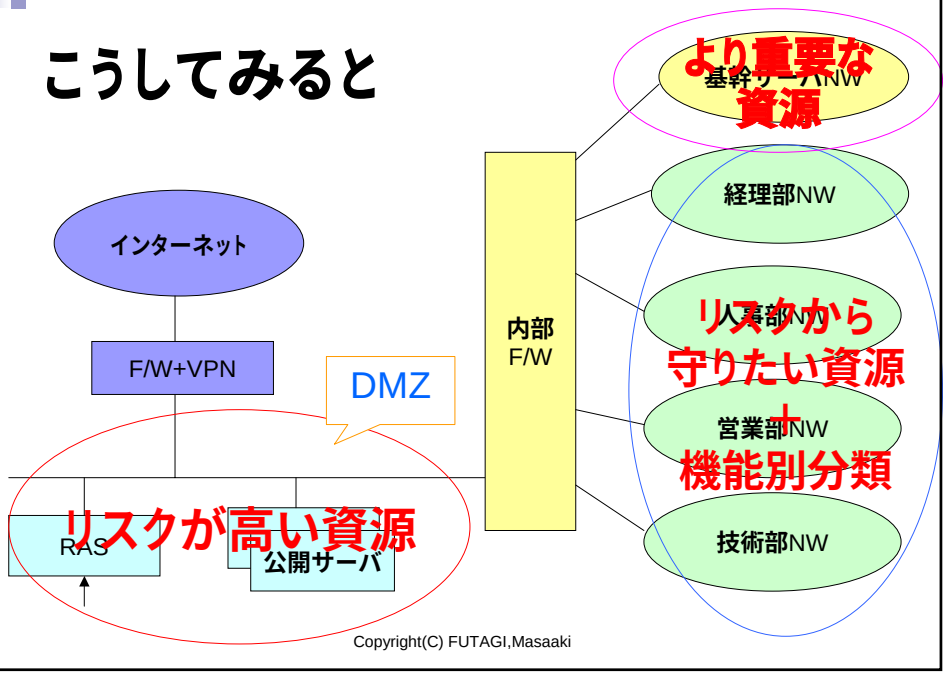
ネットワークの整理は重要

- 境界で守りやすいネットワークとは
  - 目的･機能別に分けられたネットワーク
  - 価値、重要度別に分けられたネットワーク
  - 危険度（リスク）別に分けられたネットワーク
- Perimeter Defense（境界防御）の考え方
  - 機能･目的別のネットワーク構築
  - それぞれの運用ポリシーの確立
  - 境界におけるアクセス制御

たとえば



こうしてみると



公開サーバ保護とDMZ

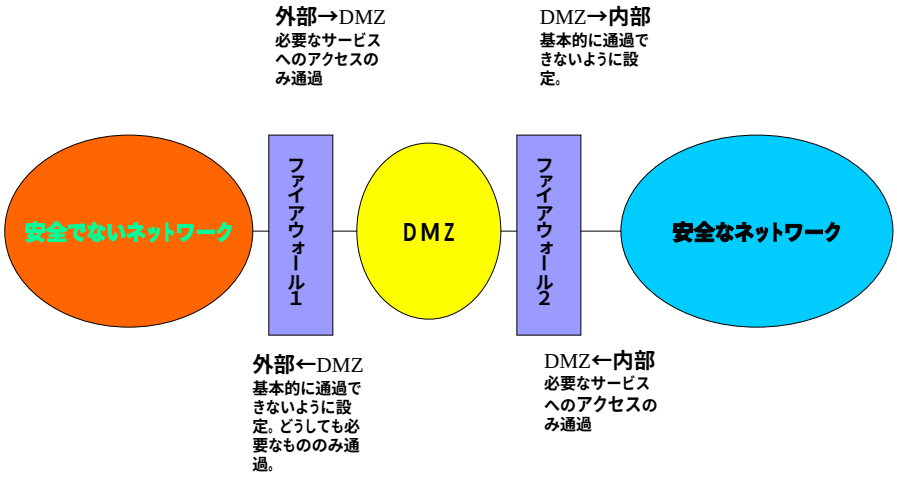
- DMZの意味合い
  - もともとは軍事用語
  - De-Militarized Zone = 非武装地帯（直訳）
    - 隣接する敵対国間の偶発的衝突を避け、また敵対行動に対する抑止の意味から、互いの中間線の両側に「立ち入り禁止区域」を設け、そこへの立ち入りに対しては侵犯行為と見なして攻撃を行うという取り決めのもとで設置される緩衝地帯（例：朝鮮半島の韓国、北朝鮮国境など）
  - 直接侵入を防ぐための「緩衝地帯」的意味合いが強い（決して「非武装＝無防備」ではない）
  - 攻撃により制御を奪われる危険が高いサーバを「保護しつつ」より重要な資源から隔離するもの
  - 公開サーバではサービスを外部に公開する以上、そのサービスの脆弱性などが原因で制御を奪われる可能性がある点考慮したもの

一般的なDMZポリシー

- 外部からDMZへの通信
  - 公開されているサービスへの通信以外は排除
- DMZから内部への通信
  - **原則禁止（＊）**
- 内部からDMZへの通信
  - 必要に応じて許可
- DMZから外部への通信
  - **どうしても必要なもの以外は禁止（＊）**

（＊）はDMZを構成することの本質

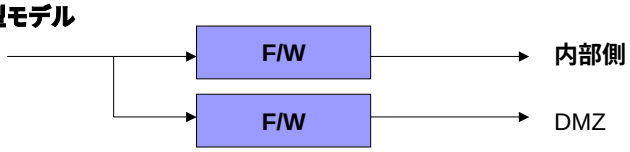
DMZ本来の形



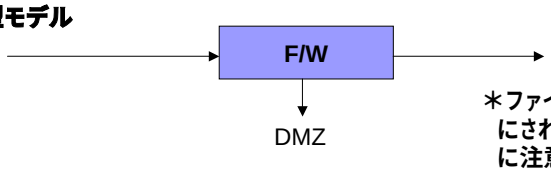
実際のDMZ構成モデル

直列型モデル

並列型モデル



一体型モデル



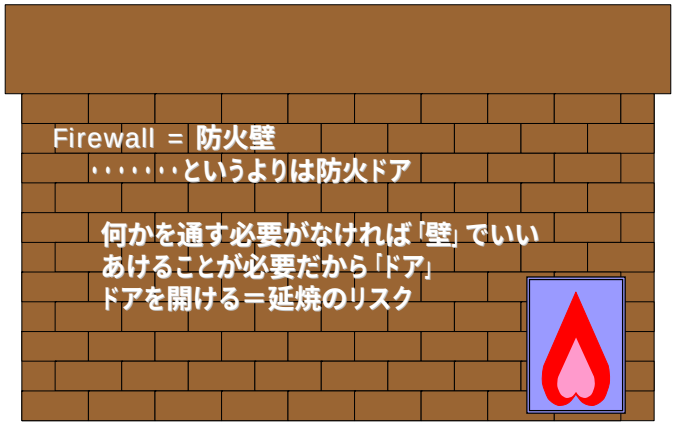
＊ファイアウォール自身が攻撃対象にされた場合のリスクが異なる点に注意

さて、ファイアウォールの話を

- いくつかの疑問
  - ファイアウォールとは何か・・・
  - ファイアウォール製品でなければファイアウォールにはならないのか
  - ファイアウォール製品を買えば、それでファイアウォールはできるのか・・・

ファイアウォールって何さ！？

- つまり‥



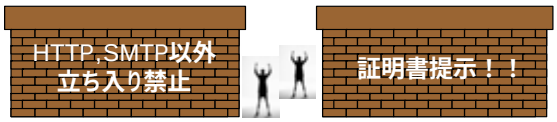
どうして、みんなこの絵を描くのだろう‥‥‥‥‥？？？？？？

ネットワークの検問所

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エイ

それぞれのポリシーを維持しながら通信する
（双方向のアクセスコントロール ＝ 国境検問所）



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）
  - ネットワーク間の物理的接続（ゲートウエイ機能）
  - 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（アクセス制御機能）
  - 危険な兆候の検出と警告（アラーム機能）
  - 通信の許可、不許可状況などの記録の保存（ログ機能）

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防御機能
    - 検出した不正な通信をブロックする機能
- UTM（Unified Threat Management）化の流れ
  - 上記のようなゲートウエイで動作すべきセキュリティ機能を１つのデバイスに集約したもの

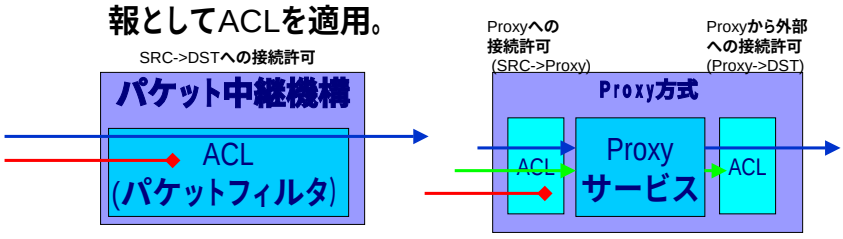
通信の中継機能

- 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
  - Proxy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
    - 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。

*

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。
    - Proxy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。



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
  - ＲＦＣ違反の検出
- 不正な通信内容（アプリケーションレイヤ：付加的機能）
  - ウイルス等が含まれた通信
  - セキュリティホールへの攻撃など
    （IDS・IPS 的機能）

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
- たとえば・・・・
  - 基幹業務サーバをファイアウォールで保護し、通信ログを取得、定期的に検査する→内部統制上の要請にも合致

ファイアウォール関連用語･概念

- Ingress／Egressフィルタ
- ダイナミックパケットフィルタ
- ステートフルインスペクション
- アプリケーションゲートウエイ
- NAT (Network Address Translation)
  - (類) IP Masquerade, NAPT, PAT etc.
- 透過型proxy
- L2ファイアウォール (ブリッジモード、透過モード)
- UTM (Unified Threat Management)

＊

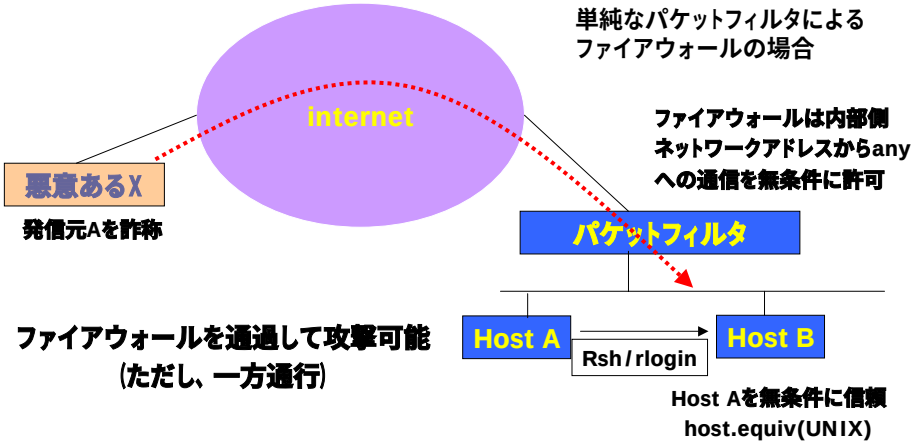
パケットフィルタの特性

- **IP詐称攻撃に対する本質的な弱点**
  - 内部側ネットワークアドレスの詐称
  - 信頼しているネットワークアドレスの詐称
  - 発信元IPアドレスの詐称は容易
  - 一方通行でも有効な攻撃手法もある

＊IP詐称攻撃

インターネットのルーティングは発信元アドレスを意識しない。従って詐称されたパケットでも、相手方までは届く。しかし、応答は詐称されたアドレスに送られるため、攻撃は一方通行となる。

IP詐称攻撃の例（内部側ネットワーク詐称）



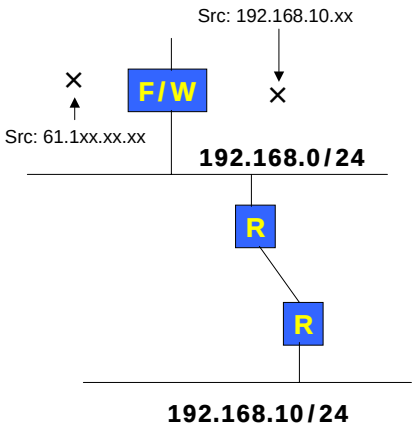
パケットフィルタの特性を補う機能

- 方向性フィルタ
  - パケットがどのネットワークインターフェイスから入ってきたか（出ていくか）を区別
  - 内部側アドレス詐称対策
- ダイナミックパケットフィルタ
  - コネクション／セッションの認識と管理
  - 応答パケットを自動的に認識して通過させる

Ingress/Egressフィルタ（詐称防止策）

- 方向性フィルタを利用
  - パケットの通過方向によって制御を行う。
- 境界ルータで詐称と思われるパケットを阻止
  - 内部側アドレスを発信元に持つパケットが外部から着信した場合（外部者の内部アドレス詐称）
  - 内部にないアドレスを発信元に持つパケットが内部から出ていく場合（内部者の外部側アドレス詐称行為）
- 詐称対策としての限界はある
  - 外部の特定アドレスへのアクセス許可に対する詐称

Ingress/Egressフィルタの例

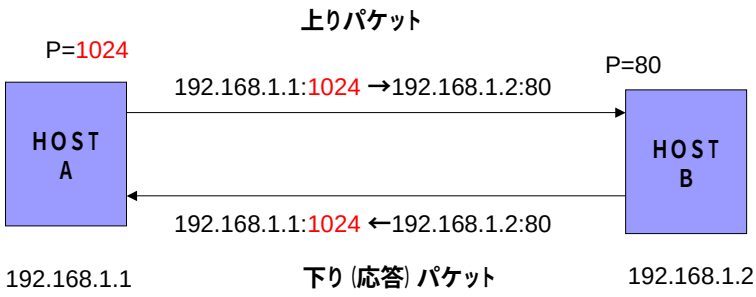


- Ingress フィルタ
  - 発信元が 192.168.0 または 192.168.10となるパケットの外部→内部への通過を禁止
- Egress フィルタ
  - 発信元が 192.168.0または 192.168.10以外のパケットの内部→外部への通過を禁止
- ファイアウォールの直下のセグメントのみでなく、内部側のすべての経路を考慮

ダイナミックパケットフィルタ

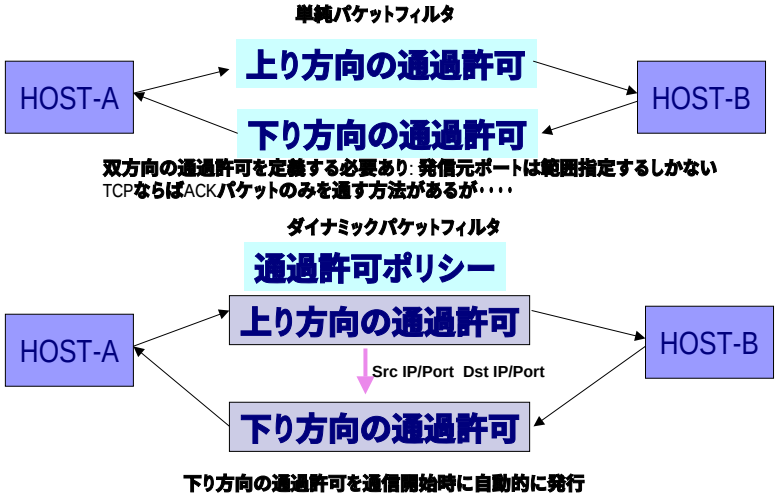
- ファイアウォール製品とルータやS/WのACL機能の最大の相違点
  - 通過を許可した通信パケットへの応答や付随する他のセッションなどを総合的に管理、自動通過処理を行う。
  - 発信元ポートがダイナミックに変わる通信に的確に対応可能。
  - ポリシー設定を単純化できる。（許可するセッションの方向のみ定義）

TCP or UDP／IPでの通信

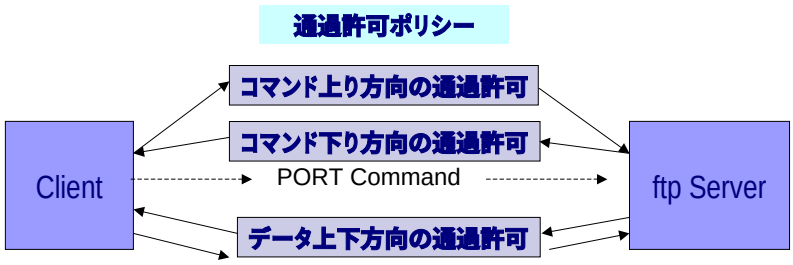


発信元ポート番号は一定ではない。毎回変化する。（any >= 1024）

単純パケットフィルタとの比較



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。

ダイナミックパケットフィルタの特徴

- 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、VoIPなどは要注意）
- ＴＣＰではコネクション切断時に許可取り消し可能だが、UDP, ICMPなどではタイムアウト待ちで取り消される

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パケットフィルタと同義に使用されることも多い。

アプリケーションゲートウエイ

- Proxy方式の一種（高級版？）
  - たとえばHTTPのリクエスト内容やFTPのコマンドなどのレベルでの検査、許可設定ができるなどアプリケーションレイヤでの通信制御が可能なもの
- （対）サーキットレベルゲートウエイ
  - ポートフォワーディングとも呼ばれ、単純に内容を中継するだけのProxy

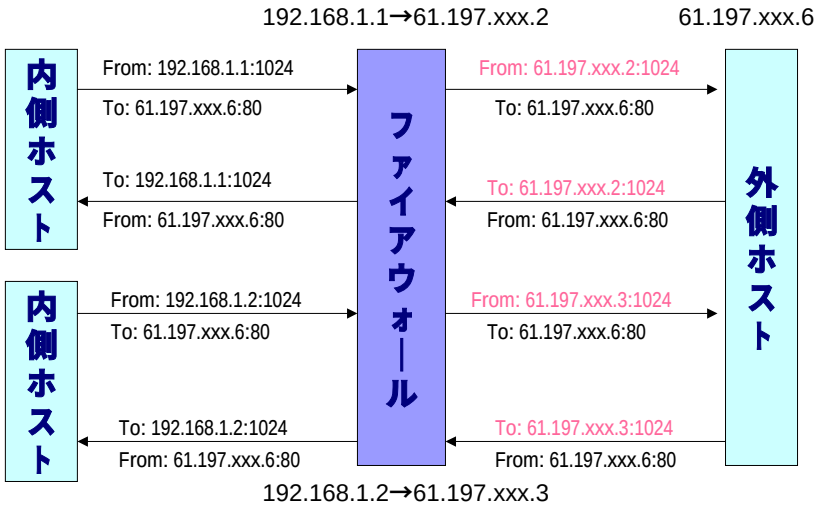
NAT（Network Address Translation）

- 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パケットフィルタ系ファイアウォールを置く場合に必須。
- 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。
- 一般にNATと呼ばれるものにはいくつかのタイプがある
  - ＲＦＣ２６６３で、ＮＡＴの様々な形を整理しようとする試み

固定(Static / 1：1)NAT

- 内部側1ホストに対して固定で1個の変換用アドレスを割り振る方法
- DMZをプライベートアドレスで構成する際や外部との通信で1個のグローバルIPを占有する必要がある場合などに利用される
- 内部ネットワークにいるホストをこの方式でインターネットに公開すると危険 （DMZの意味の復習を）

NAT（1：1変換）



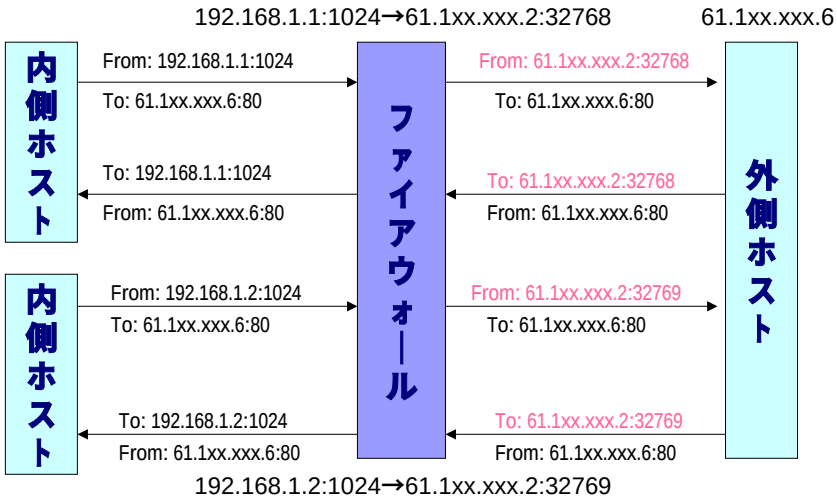
NAT(RFC1631)

- グローバル（変換用）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
- 同時通信数は変換用に用意したアドレスの数に制約される。（通信中の1クライアントが1IPを占有する）
- 多数の内部ホストがある際に現実的ではない。

NAPT, IP Masquerade, 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

NAPT (N:1変換)



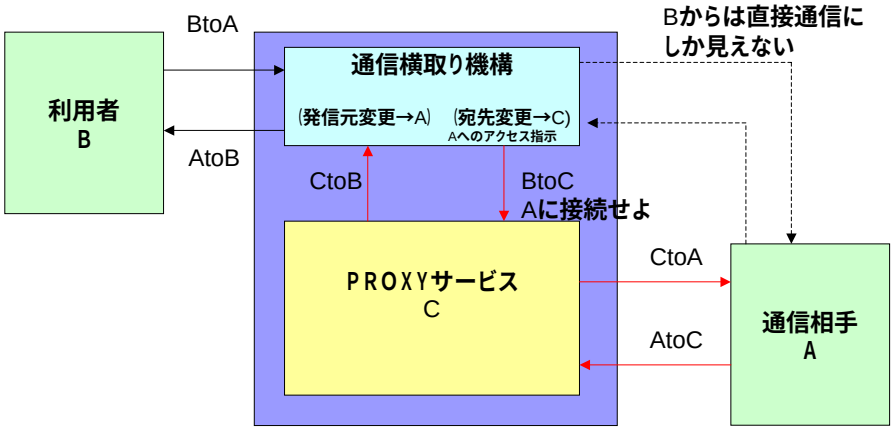
NAT使用上の注意点

- 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/AHなど)

透過型（Transparent）Proxy

- Proxyの煩雑さ
  - 直接相手と通信せず、一旦Proxyに接続してから、目的の通信を要求する必要がある。
  - たとえばWebブラウザではProxy設定で使用するProxyサーバを指定しておく。
- 透過型Proxyでは、（みかけ上）利用者は直接相手方と通信できる。

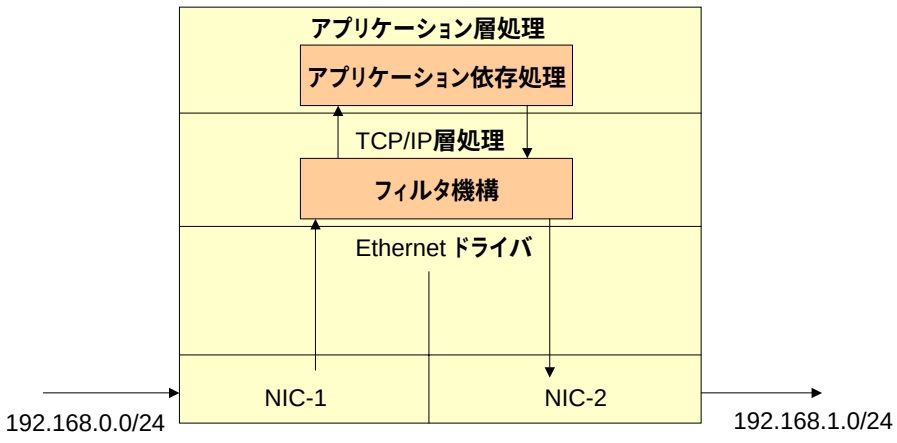
透過型Proxyの原理



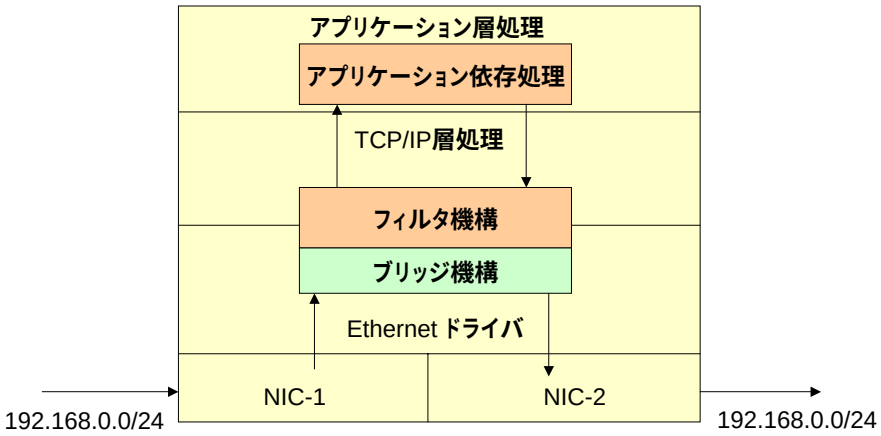
L2ファイアウォール

- ブリッジモードともいう
- メーカーによっては透過モードという言い方も
  - 透過型 Proxyと紛らわしいので注意
- 簡単に言えば「ハブ」にファイアウォール機能を持たせたようなもの
- ファイアウォールの前後でIPネットワークがかわらないので、後から導入する際、ネットワーク構成を変えなくてすむ

L3ファイアウォールの処理



L2ファイアウォールの処理



ファイアウォール製品の付加的機能

- 攻撃防御機能
  - いわゆるIPS,IDPS的な機能。通信に含まれる既知の攻撃手法を検知してブロックする
- ウイルス防御機能
  - 通信に含まれる既知の不正プログラムやスクリプトを検知してブロックする
  - 主にhttp, ftp, smtp, pop2などが対象
- コンテンツ、URLフィルタなどの機能
  - 主に http が対象、接続先のURLやページの内容によってブロックする機能
- VPN機能
  - 遠隔拠点間、モバイルPC等のインターネット経由暗号通信によるネットワーク接続機能。IPsec, L2TP, PPTPなどのプロトコルが一般にサポートされる

最近流行のＵＴＭ

- Unified Threat Management
  - 単一の「ゲートウエイ」デバイスで、あらゆる脅威に対応しようという考え方
  - かつての「All-In-One」ファイアウォールを格好良く言っただけ！？
  - ネットワークアクセス制御、脆弱性への攻撃防御、ウイルス（マルウエア）検査など、従来、個別のゲートウエイデバイスを使って行っていた処理を、相互に有機的に結合し、集約する
- H/W処理性能向上で、実用的な製品が可能になったことが大きい
- ネットワーク機器（S/W等）との統合、モジュール化の動きも顕著

☺ちょっと休憩 ☺

ファイアウォールの導入設計

- ネットワーク設計もしくはその見直し
- ネットワーク境界におけるポリシーの決定
- トラフィック予測と性能設計
- 障害対策の設計
- ログ管理に関する設計

ネットワーク設計のポイント

- インターネット接続の場合
  - DMZを構成するか（単一or複数、直列or並列or一体型）
- 内部側をいくつのネットワークに分けるか
  - 単一のファイアウォールで構成するか、複数で構成するか
  - 既存ネットワークへの導入の場合、ネットワーク（アドレス）を変更するか否か
- プライベートアドレスを使うかグローバルアドレスを使うか
- 特定のネットワーク（アドレス）を隠蔽するか

既存FWをリプレースする場合

- ネットワーク構成やポリシーを変えないのが簡単だが‥
- この際だから、よりよい構成にならないか見直してみる手もある
  - 内部側の分割
  - DMZ構成の見直し
  - 新しいプロトコルやアプリケーション、セキュリティポリシーの変化に応じたファイアウォールポリシー見直し
  - ‥‥など

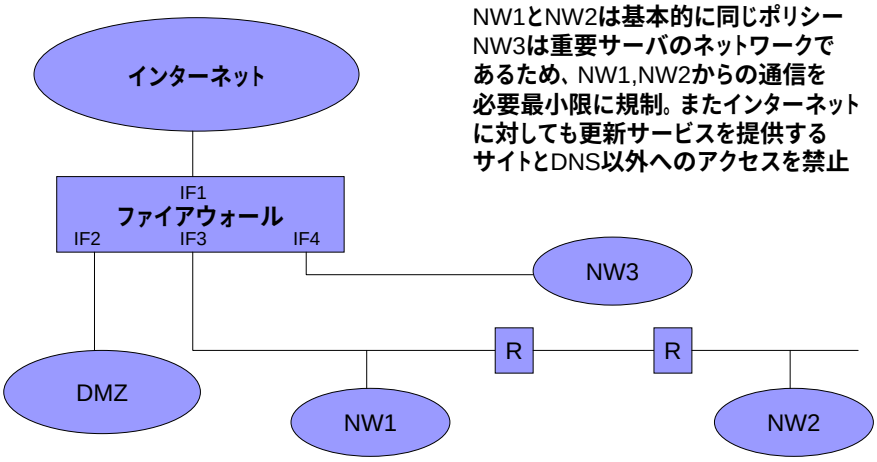
ファイアウォールポリシー設計

- まず、ネットワークをグループ化しておこう
  - たとえば、ある事業部に属するネットワーク、ある重要度以上にランクされている社内業務用サーバセグメント‥‥など、同じポリシーが適用されそうなものを一通り、グループ化しておく
- サービスもグループ化を
  - たとえば、メールサービスとして、SMTP,POP3,IMAP4をグループ化しておけば、メールサーバへのアクセス制御を考えやすい

ファイアウォールポリシー設計

- 各ネットワークグループ間で相互に通過させる、もしくはブロックするサービスやサービスグループを決める。(ポリシー)
  - デフォルトを通過とするかブロックとするか。安全なのはブロックだが、内部ネットワーク間では通過を基本する場合も考えられる
  - 設定する際の前後関係に注意を
- 決めたポリシーをファイアウォールを通過する通信の向きで整理する

ある会社のネットワーク



NW1とNW2は基本的に同じポリシー
NW3は重要サーバのネットワークで
あるため、NW1,NW2からの通信を
必要最小限に規制。またインターネット
に対しても更新サービスを提供する
サイトとDNS以外へのアクセスを禁止

ネットワークとサービスのグループ化

INTN-G	ANY
DMZ-G	DMZ
SERVER-G	NW3
CLNT-G	NW1　NW2

CLNT-OUT	HTTP HTTPS FTP
DMZ-OUT	DNS SMTP
DMZ-IN	SMTP DNS HTTP HTTPS
SERVER-IN	DNS FTP HTTP HTTPS NETBIOS(TCP/UDP 135-9)

ファイアウォールポリシー

	To	IF1 INET-G	IF2 DMZ-G	IF3 CLNT-G		IF4 SERVER-G
From		INTERNET	DMZ	NW1	NW2	NW3
IF1 INET-G	INTERNET		DMZ-IN	NONE		NONE
IF2 DMZ-G	DMZ	DMZ-OUT		NONE		NONE
IF3 CLNT-G	NW1	CLNT-OUT	ANY			SERVER-IN
	NW2					
IF4 SEVER-G	NW3	NONE	ANY	ANY		

トラフィック予測と性能設計

- 設計のポイント
  - トラフィックの掌握
    - 現状の掌握と次の再検討時期まで（3から5年程度）の推移の予測
  - 性能設計
    - 選択する機器の能力や特性を正しく掌握する
    - 付加機能を使用する際の負荷や性能特性の変化を考慮する

トラフィック掌握のための要素

- インターネット接続の場合
  - 目的別のトラフィックを考える
    - 社員のインターネット利用傾向
      - 通常のWeb参照頻度
      - ダウンロード頻度
      - マルチメディア系通信の利用頻度と業務上の重要性
    - 外部からDMZ公開サービスへのアクセス
      - 期待するアクセス数など
      - バースト的なアクセス増加の可能性
    - VPNのトラフィック
      - 拠点間（利用頻度と帯域保証の要否）
      - モバイルユーザの数とアクセス頻度
  - どちらかといえば、まずアクセス回線の容量を決めるほうが先
    - ファイアウォールの性能問題はそれほどシビアではない

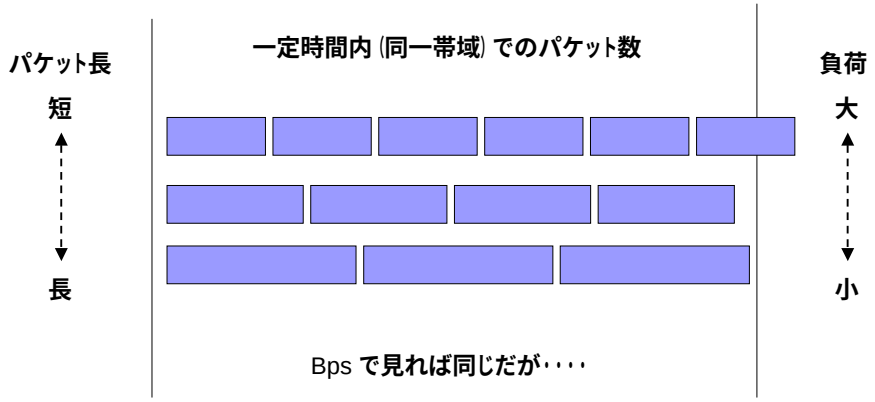
トラフィック掌握のための要素

- 内部ネットワークのファイアウォールの場合
  - 現状のトラフィックパターンの掌握
    - トラフィックアナライザなどでの分析
      - 帯域消費量の推移
      - サービスの利用頻度
      - サービスごとのパケットサイズ分布
  - 将来予測
    - 中期的な情報システムの整備計画などをもとにトラフィックの増減を予測

製品の性能評価ポイント

- スループットの罠
  - カタログ記載のbps値の意味
    - 測定条件がメーカーによって異なる
    - 多くの場合、最もいい値が出る条件で測定
  - パケットサイズ分布の影響が大きい
    - パケットフィルタベースのファイアウォールの負荷はパケット数で決まる
    - 同じ帯域でも、パケットサイズ分布によって負荷が大きくかわる点に注意が必要

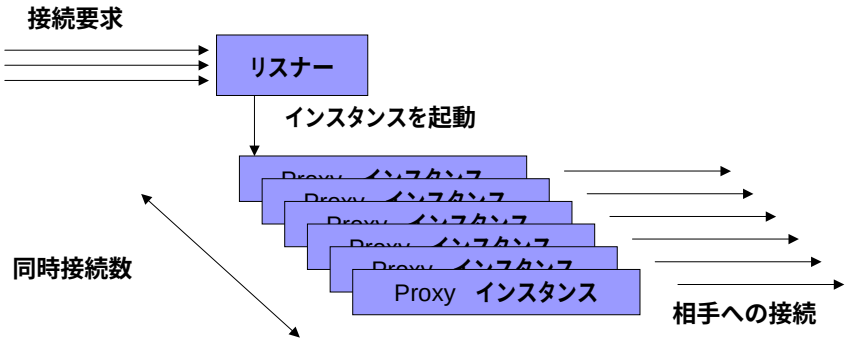
パケット長とファイアウォールの負荷



Proxy の場合の考え方

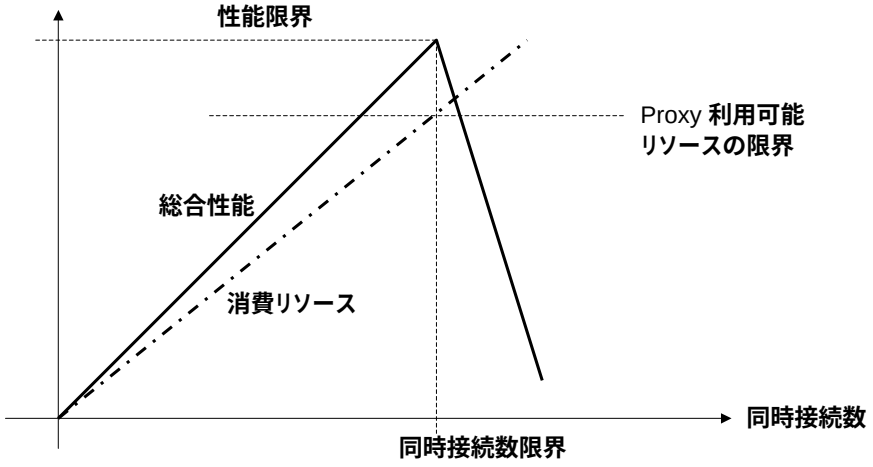
- 同時接続数と性能の関係に注意
  - 接続1個に対し、一定量の資源を消費
  - ファイアウォール内の資源に限りがある点に注意
  - 一定数以上の同時接続許可はかえって性能を低下させる
- 同時接続数はメーカー推奨値を中心に微調整

ファイアウォール内でのProxyの動作



同時接続数を制限し、順次処理。同時接続数を超える接続要求は、どれかの接続が終わるまで待たされる。（考え方は、Webサーバ等と同じ）

同時接続数と総合性能



付加機能と性能

- 負荷の高い機能
  - ウイルス検査機能
  - コンテンツ検査機能（URL、コンテンツフィルタ、SPAMフィルタなど）
  - 侵入検知・防御機能
  - VPN（強度の高い暗号をソフトウエア処理する場合）

ウイルス・コンテンツ検査の特性

- 通信で授受されるコンテンツに対して、内容を検査する
  - ウイルス（マルウエア）感染の有無
  - 特定のキーワード、パターンの合致など
    - Webサイトのコンテンツフィルタ
    - スパムメールフィルタなど
- 最新のパターンファイル供給が必要
  - インターネットからのダウンロード、もしくは更新サーバへのアクセスを定期的に行う必要がある

ウイルス･コンテンツ検査の特性

- どちらかといえばProxy的な動作となる点に注意
  - 同時処理が多ければリソースを食いつぶし、性能の極端な低下を起こす（制限が必要）
  - 少なからず遅延が発生するため、ユーザが「遅い」と感じる原因になる
- Proxy系のファイアウォールを使ったほうが無難
  - 負荷が上がったときに、全体が不安定になりにくい
  - 最近のUTMでは、こうした機能だけProxy的な処理を行っている場合が多い

侵入防御機能（IPS機能）の特性

- Signature による検知
  - 特定の脆弱性攻撃に固有のパターンを通信から検出する
  - 誤検知（false positives）の可能性もあるが、最近の製品ではかなり改善
- Anomaly（異常）検知
  - DoS攻撃などのトラフィック異常を検知
  - 検知は確率的、誤認を排除できない

侵入防御機能（IPS機能）の特性

- 誤認を排除するためのチューニング期間が必要
  - 導入後、一定期間は「検知機能」のみを動作させ、誤認が激しいSignatureについて、改良または停止する。
  - その後、「防御機能」を起動して本運用に入る
- 最新のSignatureを導入する手段が必要
  - 自動更新または手動でインストール・・・
  - Signature更新にあたっては、追加されたSignatureと変更されたSignatureについて、動作確認が必要になる場合もある。

付加機能は「おまけ」か？

- 最近のＵＴＭでは必ずしもそうではないが・・・
- 負荷の高い、大組織ではファイアウォールから分離して運用した方がいい場合もある
  - メールサーバやWebキャッシュとウイルス対策専用サーバ、コンテンツフィルタ、SPAMフィルタの連携など専用システムの利用
  - IPS(侵入防御システム)、アプリケーションファイアウォールの利用
  - VPN専用サーバの利用

製品評価、検証も必要

- 実際の利用状況に耐えられるかどうか
  - 重要なネットワークに使う場合は、擬似的な負荷を与えた性能検証が必要な場合もある
  - 検証できない場合でも、カタログ値をうのみにせず、実際に近い数値や利用事例などの情報提供をベンダに要求してみよう（言えば出てくるケースが多い・・・）

障害（故障）対策

- 止められない、なくせないファイアウォール
  - インターネットからの情報がとまると・・・・・
  - インターネットへの情報提供や対話がとまると・・・・
  - 社内用ファイアウォールが止まればネットワークが止まる・・仕事が止まる・・・

故障対策のレベル

- ファイアウォールが守っている資源（機器、サービス）の重要度に直結
  - 許容されるダウンタイムやサービスのクオリティ低下に応じた対策が必要
  - たとえば、オンサイト保守のSLA（数時間～2時間程度の対応時間）では満足できない場合は自前で対策が必要に

対策のレベル

- 冗長化が基本だが方法はいろいろ
  - コールドスタンバイ（予備機交換）方式
  - ホットスタンバイ（予備機待機）方式
  - ロードバランサ（負荷分散）方式

コールドスタンバイ方式

- 故障時、ただちに交換できるような予備機を用意しておく方法
  - 数分～1時間以内程度のダウンタイム
  - サービス低下は同じ機器を使う限りはない
- 予備機は基本的に同一機種を同じ設定を投入した状態で準備
  - 機種や設定が異なるとサービス低下や別の障害につながる　(収拾がつかなくなる可能性)

ホットスタンバイ方式

- 予備機を電源投入状態で待機させ、障害時に自動的に (もしくは手動で即時) 切り替える方式
  - ダウンタイムが少ない (数秒～1分程度：機種、方式によって多少差がある)
  - Active – Passive (Stand-by)方式などとも呼ぶ
  - 同じ機器を使う限り性能低下はない

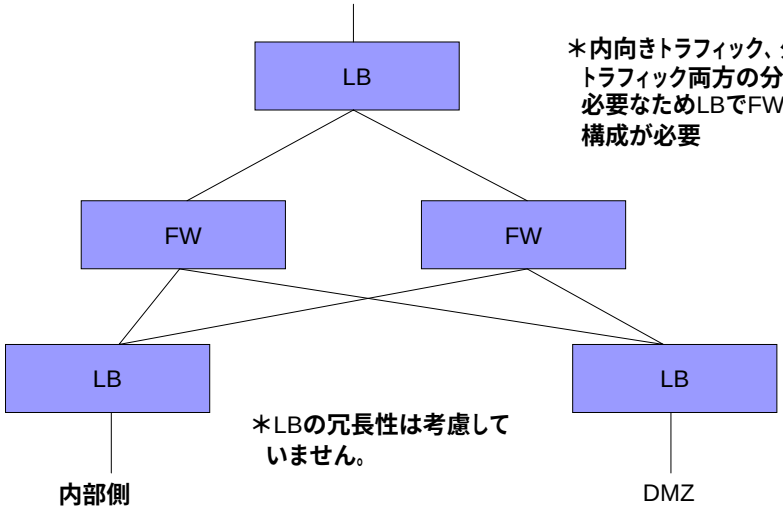
ホットスタンバイ方式の技術

- Heart beat 交換
  - 予備機が稼動機の応答を常時チェック。無応答になった場合に、自分が置き換わる
  - セッション情報を共有している方式では通信（セッション）が切れないが、そうでないと切り替え時に行っている通信は一旦切れることがある。
- 切り替え方式
  - 完全置き換え方式
  - 仮想IPアドレス切り替え方式　（VRRPなどを利用）

ロードバランサ方式

- 複数のファイアウォールをロードバランサ（負荷分散装置）の下で同時使用する方式
  - ダウンタイムは僅か（ほぼ0）
  - 障害時性能低下が発生する（片肺飛行）ため、性能に余力をもたせておく必要がある
  - 使用できるロードバランサは限られる（ファイアウォール用のものが必要）

ロードバランサとファイアウォール



＊内向きトラフィック、外向きトラフィック両方の分散が必要なためLBでFWを挟む構成が必要

＊LBの冗長性は考慮していません。

LB使用時の留意点

- ファイアウォール用LBを使う
  - ダイナミックパケットフィルタによるセッション管理を意識した分散が必要 (persistence)
    - 例）ftp：コマンドコネクションを振り分けたFWに対し付随して発生するデータコネクションも振る必要あり
    - VoIPなど1セッションで多数のチャネルを持つプロトコルを使用する場合は困難な場合も

Active-Active 冗長方式

- ファイアウォール自身の機能でロードバランシングを行う
  - 複数台のファイアウォールが連携して、仮想IPアドレスを管理
  - ロードバランサが不要
  - ロードバランサ方式同様に、ダウン時の負荷を考慮して性能に余裕をもたせておく必要がある

ファイアウォールを何台使うか

- 1台（セット）の製品に多数のネットワークを収容
  - 導入効率は良いが、設定などが煩雑になる可能性もある
  - リスクが一ヶ所に集中する
- 分離を検討すべきケースは？
  - リスクが極めて高いネットワークは独立して管理すべき（たとえば、内部の基幹業務サーバセグメントなど）
  - ポリシー設定数が極めて多いようなネットワークや頻繁に設定変更が発生するようなネットワーク
  - トラフィックが極めて多いネットワーク

ログに関する設計

- ログ取得の機能はファイアウォールの重要機能のひとつ
  - 何を何のために記録しておくか
  - どのくらいの期間保存するか
  - どのような手段で保存するか
- ログ管理の重要性の増大
  - 内部統制上、ログ取得とその監視や定期的検査が必要とされるケースが増加する

ファイアウォールで取得できるログ

- セッション（通信許可）ログ
  - 通信の量に応じて大量のログが発生
  - 通信履歴を取得できるので、利用者の通信利用状況の解析や、インシデント発生時の追跡など利用目的は多様
- 通過拒否ログ
  - 主に外部からの通信拒否状況を記録。
  - 内部からの通信制限をきつくしている場合など、場合によっては大量のログが出る。
  - 主に、不正な通信を発見したり、傾向を見るために利用

ファイアウォールで取得できるログ

- 認証ログ
  - 認証に基づく許可などを行った、もしくは拒否したなどのログ。アクセス履歴管理や不正なアクセス試行などの発見に利用
- 管理者ログイン、設定変更ログ
  - ファイアウォールの設定変更履歴の管理や、不正な変更操作の発見などに利用
- 各種エラーログなど
  - ファイアウォールの動作状況の管理に利用

ログの保存･保全方法

- ログの保存先
  - ファイアウォール自身に保存
  - ファイアウォールの管理サーバに保存
  - Syslogサーバなどに保存
  - その他の監視システムなどに保存
- ログを保全するために
  - ファイアウォール自身のみに保存しない
  - 複数の保存先を作ることが望ましい。(本体＋syslogサーバ) など

ログの容量と保存期間

- セッションログ
  - 最も容量が多い
  - 発生件数はセッション数（利用者トラフィック）に依存。
  - 保存期間は目的によるが、インシデント発生時にトレースする目的ならば、90日程度は保存する必要がある。（サービス事業の場合は必須）
  - Proxy型（アプリケーションゲートウエイ型）は一般に多彩なログが取得できるが、その分容量が大きくなるので注意

ログの容量と保存期間

- 拒否ログ
  - 最も見積もりが難しいもの
  - 一般にトラフィックログよりはかなり少ないが、場合によっては同程度かそれ以上になる可能性もある
    - 世界的なワームの大量感染などが発生した場合
    - 社内で本来許可されないような通信を大量に発生させるような事故が発生した場合など
    - トラフィックログの半分程度～同程度と見積もるのが経験上妥当
  - 傾向を見る目的ならば保存期間は短め（1週間～1ヶ月程度）でもよいが、インシデント発生時にトレースするようなケースでは90日以上が望ましい。
- その他のログ
  - 容量はセッションログの数%程度で一般に十分
  - 保存期間は認証、設定変更ログなどは90日程度が望ましい。その他は適宜

ファイアウォールの運用

- 実際動かし始めたら、それ自体はあまり手がかからない
- 主にログの確認、利用と定期的な設定（ポリシー）見直しが運用の中心

ログの管理、監視

- 通信の傾向掌握
  - 内部利用者の通信利用状況（種別やその傾向、推移）
  - 外部の通信先（サービス別）ランキング（トップN+ボトムN）の取得
  - 通信拒否（内部、外部）状況と拒否される通信種別（ポート番号、プロトコル）ごとの状況
  - 認証エラーなど不正アクセスにつながりうる状況の掌握
  - ログ解析ソフトなどを使用して定期的にレポート作成を

インシデントの発見

- ファイアウォールのログから得られるものは多い
  - 未知ウイルスの感染
    - クライアントからメールサーバを経由しないSMTP通信の抽出（短時間に大量発生ならウイルス可能性大）
  - 未知ワームの感染
    - 外部へのポートスキャン、Ping などが頻発する場合、ワーム感染の可能性は大
  - ボットやスパイウエア発見
    - IRCの通信ログ、普段あまり使用しないポート番号での通信など
  - HTTPトンネル（HTTPに見せかけた別目的の通信）
    - HTTPコネクションの継続時間のチェックなど

午後のT13の話題ですが・・・・・・

*

ファイアウォールのリアルタイム監視

- 稼動監視
  - 正常動作（死活）の監視。障害もしくはその兆候の発見（負荷状況などから）
- ログ監視
  - エラーなどからの障害もしくはその兆候の発見
  - リアルタイムな利用状況推移の掌握
  - 警告メッセージなどからのインシデント発見
  - 複数の事象からインシデントを推測、発見

ファイアウォール監視の手段

- ネットワーク監視システム (NMS) による稼動監視
  - Ping, SNMP などを使用した監視
- セキュリティ情報マネジメント (SIM) システムによる監視
  - ログを多面的に分析、インシデントの兆候を発見
  - インシデントのリスクを分析
- 監視サービス事業者の利用
  - サービス内容をよく確認すること
  - セキュリティ監視の場合は自分側にインシデント対応できる体制がないと宝の持ち腐れになる可能性あり

内部統制から見たファイアウォール管理

- 製品選定過程の透明性確保 (製品評価、レビューの記録などを残す)
- ネットワーク・ポリシー設計の文書化とレビュー、責任者による承認 (の記録)
- ポリシー変更手順の文書化と変更作業の承認者の明確化、変更履歴の管理
- ポリシー変更設計者と変更作業者の分離もしくは、第三者による作業確認など
- ログ管理手順の明確化、ログ管理者とファイアウォール管理者の分離

ファイアウォールの今後

- 枯れた分野だが・・・・
  - 決してなくならない。（ネットワークがある限り、「境界防御」の考え方は残る）
- ファイアウォール製品の多機能化と他システムとの有機的結合
  - メーカーの生き残り戦略による周辺領域侵犯の激化
  - 他の製品との統合管理、監視（M&Aの影響？）

ファイアウォール技術者のスキル

- ネットワーク構築に関するスキル
  - ファイアウォールはネットワーク機器である！！
- セキュリティ全般についての知識
  - ファイアウォールを使う（ユーザ）、構築する（SIer）はセキュリティ全般をある程度知っていないと困る。（FWポリシーはセキュリティポリシーの「実装」であるから）
  - 入れた後の使い方を考える際に必須である
  - セキュリティ資格の取得に挑戦を
- そしてファイアウォールの知識と構築経験

ファイアウォールを切り口にセキュリティを知ろう　(Your next step!)

- セキュリティポリシー、リスクアセスメント
  - ネットワークのアクセスコントロール実装
  - ファイアウォールのポリシーとリスクの関係
- インシデントレスポンス
  - ファイアウォールからインシデントを見つける
  - ファイアウォールからインシデントを追う
  - ファイアウォールでインシデント拡大を止める

参考図書

- 情報セキュリティプロフェッショナル教科書
  - 秀和システム刊
  - 日本ネットワークセキュリティ協会執筆
  - http://www.shuwasystem.co.jp/cgi-bin/detail.cgi?isbn=4-7980-0880-X

Q&A

- Contact Info.
- **二木真明**
  - futagi@kazamidori.jp
  - futagi.masaaki@scs.co.jp

資料集URL:
http://www.kazamidori.jp/SECURITY/

講師自己紹介

- **二木 真明**
  - **所属： 住商情報システム株式会社**
    - **ネットワーク・セキュリティソリューション事業部**
      - **営業統括部　担当部長　(技術担当)**
      - **海外セキュリティ製品の技術評価、調査等を担当**
    - **情報システム部 (兼務)**
      - **情報セキュリティ担当、部長付**
      - **社内セキュリティ監視基盤整備、IT全般統制担当**
  - **元プログラマー**
    - **FreeBSDベースのファイアウォール製品の開発に従事 ('96～'99)**
  - **情報セキュリティアドミニストレータ、CISSP**
  - **NPO　日本ネットワークセキュリティ協会　幹事・技術部会長**