

### 3.2 ファイアウォール

firewall (おおもとの意味は 防火壁)

ネットワークの境界(内部と外部)などに設置  
不正な侵入を防ぐ or 監視するための仕組みの総称

主な機能

- ・ 隘路(あいろ, CHOKE POINT) - 外部とのやり取り場所を限定
- ・ スクリーン(ルータ) - 外部と内部を仕切る
- ・ 検問(パケットフィルタリング) - 許可されたパケットのみ通す
- ・ 隠蔽(NAT と NAPT) - アドレス変換など
- ・ 代理(proxy) - 外部接続を直接行わないように
- ・ 記録(ログ)

ファイアウォールの種類

- ・ パケットフィルタリング
- ・ アプリケーションゲートウェイ
- ・ その他(NAPT, SPI, WAF, パーソナルファイアウォール)



ファイアウォールの形態

- ・ ネットワーク上で動作 ← ルータの一種
  - ・ ソフトウェア
  - ・ ハードウェア
- ・ PC・サーバ上で動作

話題) 学校の状況は?みなさんの家庭では?

話題) 中国のファイアウォール?

#### パケットフィルタリング

→ 隘路, スクリーン, 検問, 記録

復習) パケット通信, IPアドレス, ポート

パケット情報

- ・ 送信元 IPアドレス, ポート → 送信先 IPアドレス, ポート

ルールを設定してパケットの通過(許可/不許可)をコントロールする

関連) SPI(Stateful Packet Inspection)

関連) DMZ(De-Militarized Zone)

#### アプリケーションゲートウェイ

→ 隘路, 代理(proxy), 隠蔽, 記録

外部との接続を代理で行い、直接接続が行われないようにする

Webの閲覧、メール配送など特定のプログラム(アプリ)に対して適用  
アクセス内容(コンテンツ)フィルタリング可能

関連) 「踏み台」との違いは?

## NAT, NAPT (IP マスカレード)

→ 隠蔽, 記録  
アドレス変換  
限られたグローバル IP アドレスを複数台で利用

復習) プライベート IP アドレス と グローバル IP アドレス  
何か? なぜ必要か? 何に困るのか?

## パーソナル・ファイアウォール

クライアント PC (主に個人所有の PC) に導入  
→ パーソナルコンピュータ向け

話題) Windows のファイアウォール機能

## Web アプリケーションファイアウォール (WAF)

Web アプリケーションに特化したファイアウォール = Web サイトを守る  
復習) XSS, SQL インジェクション

メモ) ファイアウォールがあれば大丈夫・・・というわけではありません

- ・ フィルタルールのアップデートが煩雑
- ・ 正常な通信との区別が難しい
  - ・ マルウェア (ウイルスやワーム)
  - ・ セキュリティホール
  - ・ DDoS
- ・ 暗号化された通信はわからない

