ファイアウォールの構築

グループ **G5**
末信亨、土田恵司、松浦恵、三瀬邦義、山口恵

セキュリティ

サーバセキュリティとは

- 安全確保の防衛策
  - システム攻撃者からコンピュータを守る
  - 不正アクセスの防止
  - 情報漏洩の阻止
  - システムの安定性保持

セキュリティの必要性

- 個人でのセキュリティ
  - 個人で保有するデータやパスワードなどにおけるセキュリティ
  - 個人の責任で管理すべきである
- ネットワークとしてのセキュリティ
  - ネットワークと外部とのやりとりを制限
- マシンとしてのセキュリティ
  - マシンへのアクセスを制限
  - マシン内のサービスについてもセキュリティを考える必要がある

ネットワーク上のセキュリティ

- SSL
  - 共通鍵暗号方式と公開鍵暗号方式の2つの暗号化技術が利用

- Fire wall
- アクセス制御（access control）
  - ユーザがコンピュータシステムの資源にアクセスすることができる権限・認可をコントロールすることを言う

ファイアーウォールについて

ファイアーウォールとは…

- Fire wall (防火壁)
- 外部ネットワークと内部ネットワークとの境界に設置され、壁の役割を果たすシステム
- 内部ネットワークから外部ネットワークへのアクセスはそのまま通過させるが、外部ネットワークから内部ネットワークへのアクセスは切断するという動作によりネットワーク・セキュリティーを向上

しかし・・・・・

- ファイアウォールを構築するだけでは全ての攻撃を防ぐことが出来ない！
  - メールに添付されているコンピュータウィルスは除去できない
  - 正常なhttpアクセスを装ったDDoS攻撃には対処できない
  - 新しい脅威に対して十分に対処できない可能性がある
- ファイアウォールの運用においては必ず他のセキュリティ技術と組み合わせることが必要

ファイアウォールで・・・

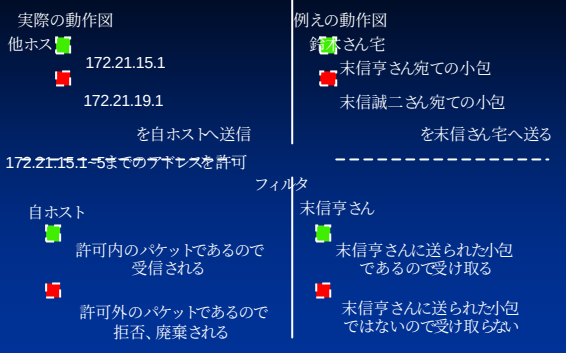
- よく使用されるアーキテクチャ
  - **デュアル・ホームホスト**
  - **スクリーンド・ホスト**
  - **スクリーンド・サブネット・ホスト**
- よく使用される手法
  - **Proxy**
  - **パケット・フィルタリング**
- 今回は、パケットフィルタリングとProxyについて詳しく説明を行う

パケットフィルタリング

パケットフィルタリングとは？

- 内部ホストと外部ホスト間でやりとりされるパケットに対して選択を行い制御することである
- パケットの選択判断材料
  －始点（終点）IPアドレス
  －宛先（送信元）ポート番号

PFの機能図



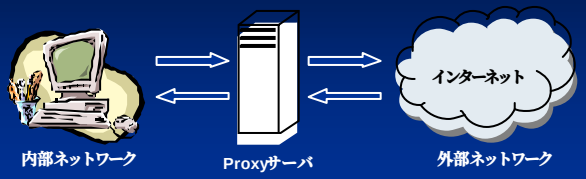
長所と短所

- 長所
  - 転送速度が高速
  - 細かな制御が可能
- 短所：
  - 設定がわかり辛い
  - パケットのデータ自体には無審査

HTTP Proxy

Proxyサーバとは

- 内部ネットワークから外部への中継を行うサーバのこと



Proxyサーバの主な機能

- キャッシュ機能
  - データ取得の高速化
  - サーバ負荷の軽減
  - トラフィックの軽減
- フィルタリング機能
  - アクセス制限
  - データの加工

Squid

- HTTPやFTPに対応したプロキシソフトウェア
- 米コロラド大学で開発され、現在最も利用されている
- キャッシュ機能に特化

今回の実験内容

今回の実験内容

- ファイアウォールの構築
  - –パケットフィルタリング
  - –HTTP Proxy

パケットフィルタリング(1/2)

- ルータの設定
  - – Windows NTを使用
  - – パケットの許可・拒否
  - – 始点IPアドレスが172.21.1X.0を持ち外側→内側へのパケットを拒否
  - – 終点IPアドレスが172.21.1X.2でプロトコルがwwwのパケットを許可
  - – 終点TPアドレスが172.21.1X.2でプロトコルがDNSのパケットを許可
  - – 内側→外側へのパケットはすべて許可

パケットフィルタリング(2/2)

- 確認
  - – 内部マシンから確認
  - – httpアクセス
  - – DNSアクセス
  - – f tpアクセス
  - – telnetアクセス

HTTP Proxyの構築(1/2)

- Squidのインストール
- 設定
  - – squid.conf ファイルを編集
  - – ポート番号・アクセス制限・キャッシュ

HTTP Proxyの構築(2/2)

- 確認
  - – ノートパソコンを使用
  - – プロキシサーバを使用してアクセス

参考文献

- 情報システム工学実験第3・4ネットワークリテラシー

ご静聴ありがとうございました