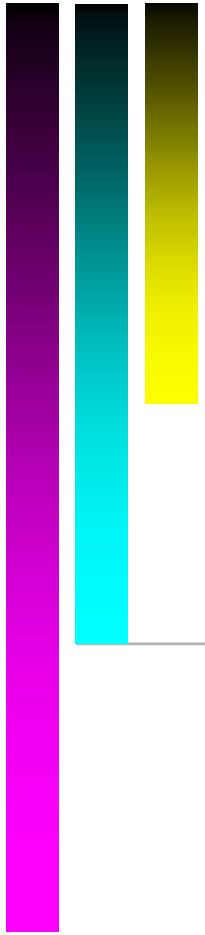


セキュリティ・ゼミナール
ファイアウォール構築技術

歌代 和正 <utashiro@iij.ad.jp>
株式会社インターネットイニシアティブ
PGP fingerprint: 6B 8F B8 3A 51 1F 2D A2 A7 EA E6 E7 58 73 71 97

1998年12月

内容

- ファイアウォールのアーキテクチャ
- 商用ファイアウォール
- 暗号技術の応用
- 侵入検知システム

ファイアウォールの役割

- 境界防御を実現する仕組みの総称
- 要塞ホスト + Proxy ゲートウェイ + パケットフィルタ
  - これらの1つ以上の組み合わせ
  - 2つの相反する機能を実現しなければならない
    - 厳格なセキュリティ管理
    - サービスの中継
- 内部のホストにはインターネット接続レベルでのセキュリティを要求しない
- ユーザには利用しやすい環境を提供

ファイアウォールの役割

- プライベートアドレス運用ネットワークからのアクセス
  - ネットワークアドレス空間の不足
  - 内部ネットワークの構成が外に出ないという副次的効果
  - 最近はルータの機能が向上してきているため、ファイアウォールに対する要求は薄れてきている

境界防御
Perimeter Defense

- セキュリティ境界
  - 共通の管理方針によって管理される領域をとりまく境界
  - 統一的なセキュリティポリシーを共有
- 同一セキュリティ境界の中を矛盾なく管理することが重要

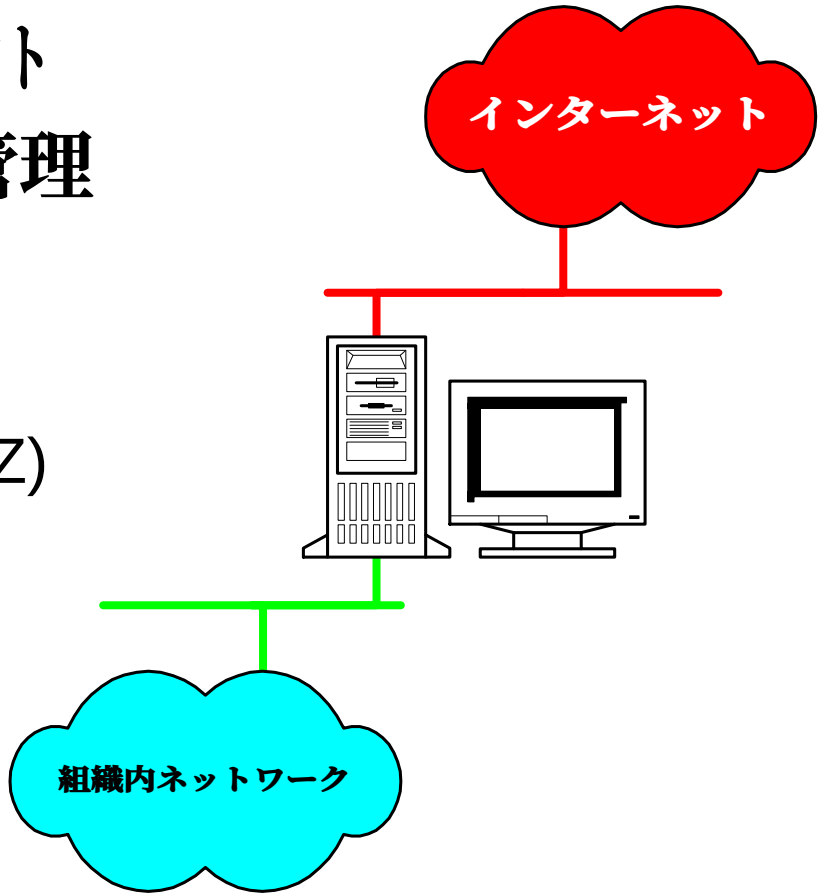
境界防御
矛盾したセキュリティ境界

- バックドア
- モデムアクセス
- 組織内からのダイアルアップ接続
- 物理的なセキュリティ対策
  - 建物のセキュリティ
  - 計算機室のセキュリティ
  - 居室のセキュリティ

要塞ホスト
Bastion Hosts

- インターネットとの接続ポイント
- 厳格なホストセキュリティの管理
- 一般にデュアルホームホスト
  - 複数のネットワークに接続
  - 最近は3つ以上の場合も (DMZ)

- **Single Strong point**



ファイアウォール構築ツール

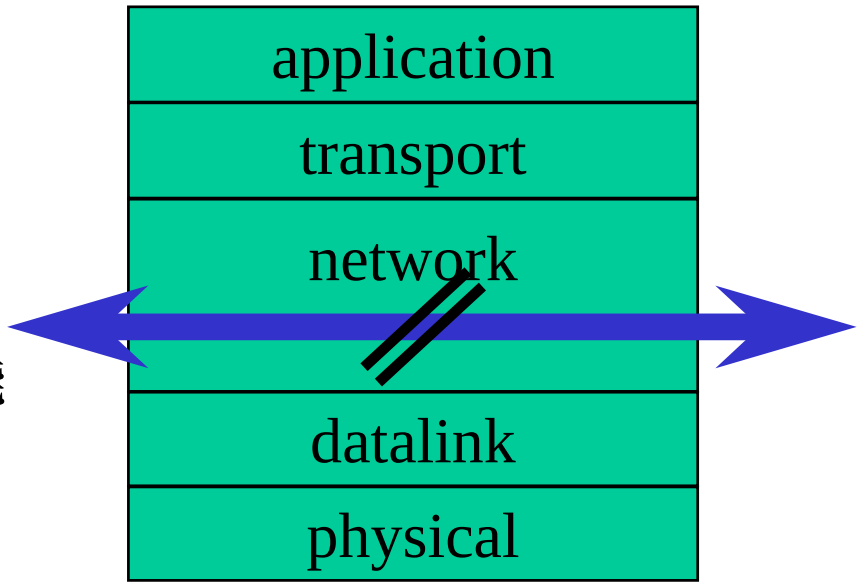
- 何種類かのツールの組み合わせ
  - ホストセキュリティの強化
  - サービスの中継
  - 関連ツール

セキュリティ強化ツール

- アクセス制御
  - 発信元、送信先のアドレス、サービスの種類に基づいてアクセスを制御
  - 利用者や時間帯による制御
  - 利用履歴を管理
  - xinetd, tcp wrapper 等
- セキュリティホールの検査 - システムが正しく設定されていることを検査
  - cops, crack
  - ISS, SATAN, TripWire

パケットフィルタリング

- IP パケットレベルでの制御
  - 専用ルータ
  - ワークステーションベースプロダクト
    - Altavista Firewall
    - FireWall-1
  - フリーソフト
    - screend
    - IP Filter
    - FreeBSD, Linux 等で利用可能



パケットフィルタリング

- アドレスによるフィルタリング
  - 接続を許すホストからのパケットだけを通す
- サービスによるフィルタリング
  - 利用を許すサービスのパケットだけを通す
- 接続方向によるフィルタリング
  - 外に向かう接続だけを可能にする

原則

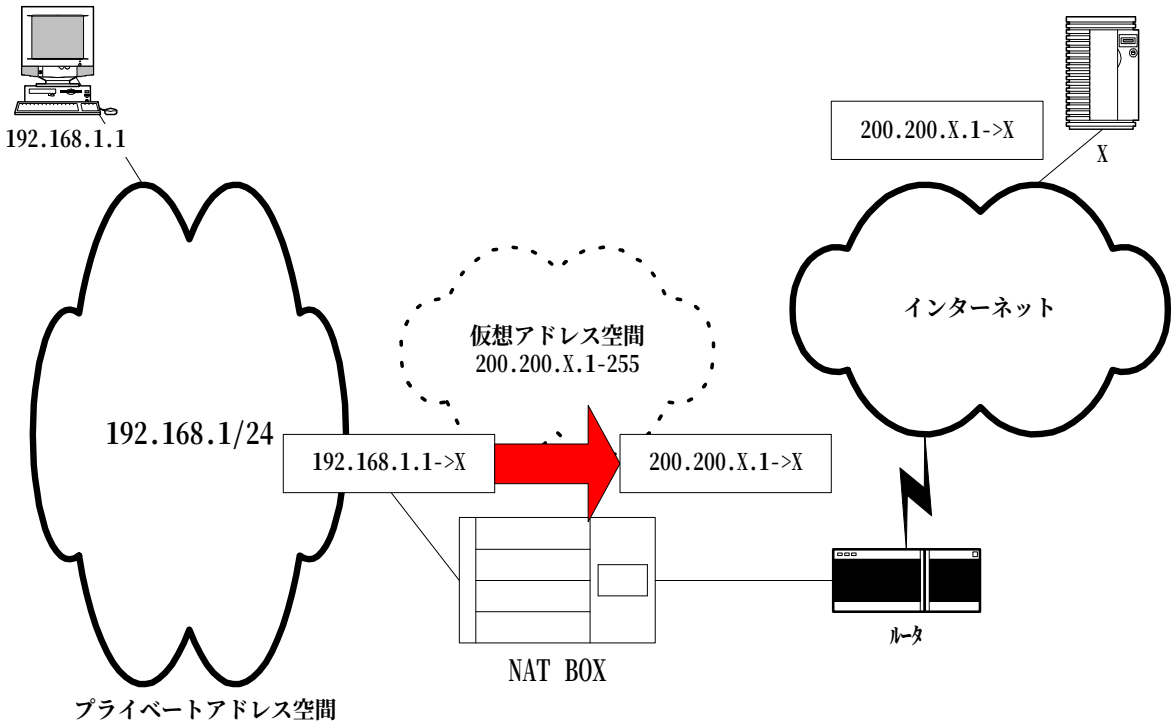
- 通したいものだけを通す
- 通したくないものを通さない

NAT
Network Address Translation

- RFC-1631
- **背景**
  - IP アドレスの不足
  - **インターネットへの直接の接続を必要としないネットワークの増加**
- **プライベートアドレス空間** (RFC-1918) **の発信元、送信先アドレスをグローバル空間にマッピング**
- **結果として内部ネットワークの構造を隠蔽し、アクセスを制限する効果がある**

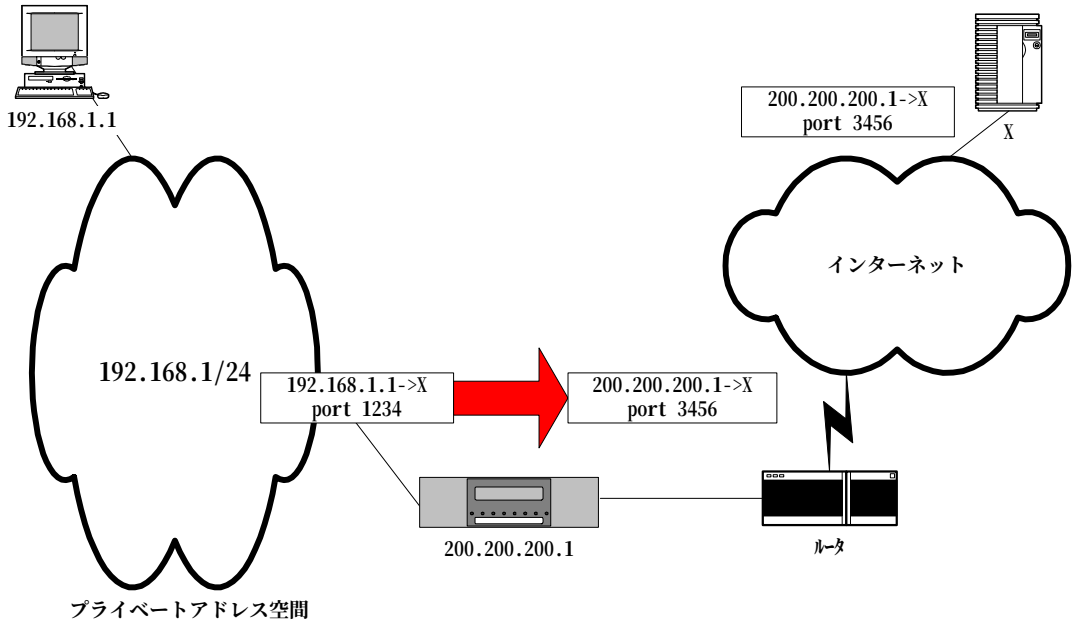
NAT
Network Address Translation

- プライベートアドレス空間を確保されたグローバルアドレス空間にマッピング
  - 静的対応
  - 動的対応
- ポートは触らない



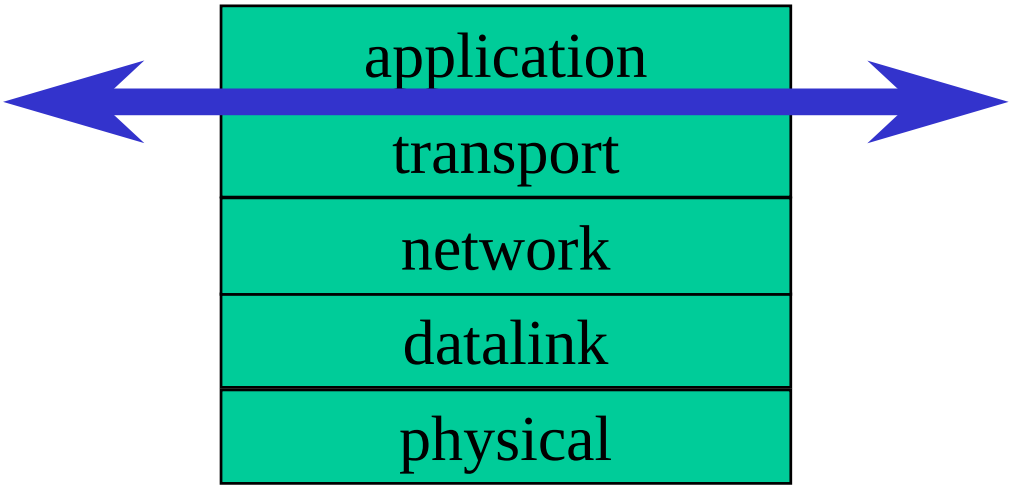
IP masquerade
(NAPT: Network Address Port Translation)

- ポート番号も変換する
- アドレス変換ルータのアドレスだけで運用可能
  - 端末型ダイアルアップでの利用が可能



サーキットゲートウェイ

- アプリケーション層で動作するが、アプリケーションプロトコルは理解しない
- トランスポートレベルゲートウェイということもある

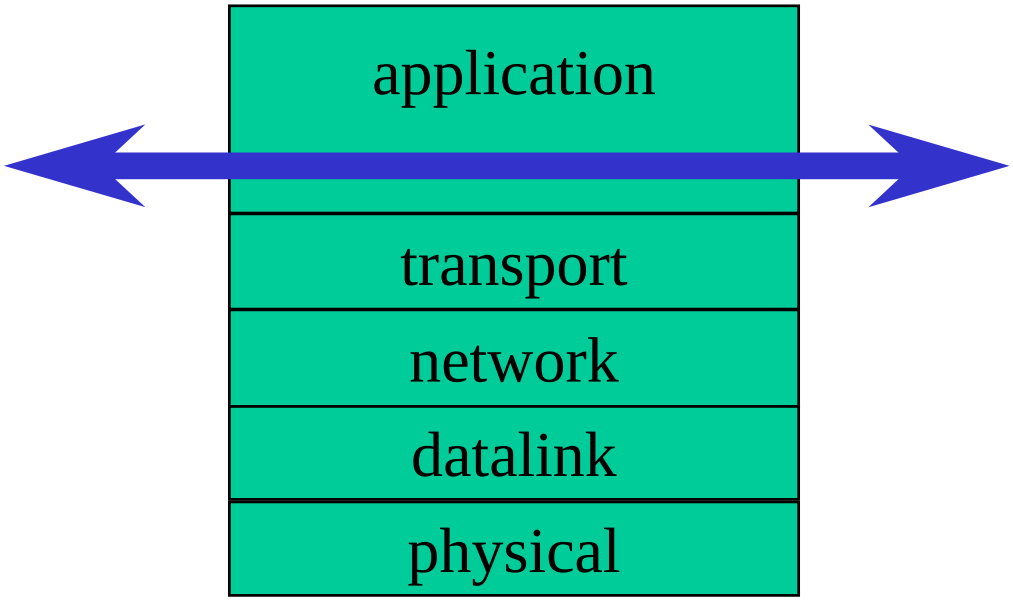


サーキットゲートウェイ

- socks
  - 汎用 TCP Proxy ゲートウェイ
  - クライアントでの対応が必要
- udprelay
  - 汎用 UDP Proxy ゲートウェイ
- plug-gw
  - TIS Firewall Toolkitに含まれるサーキットゲートウェイ

アプリケーション
ゲートウェイ

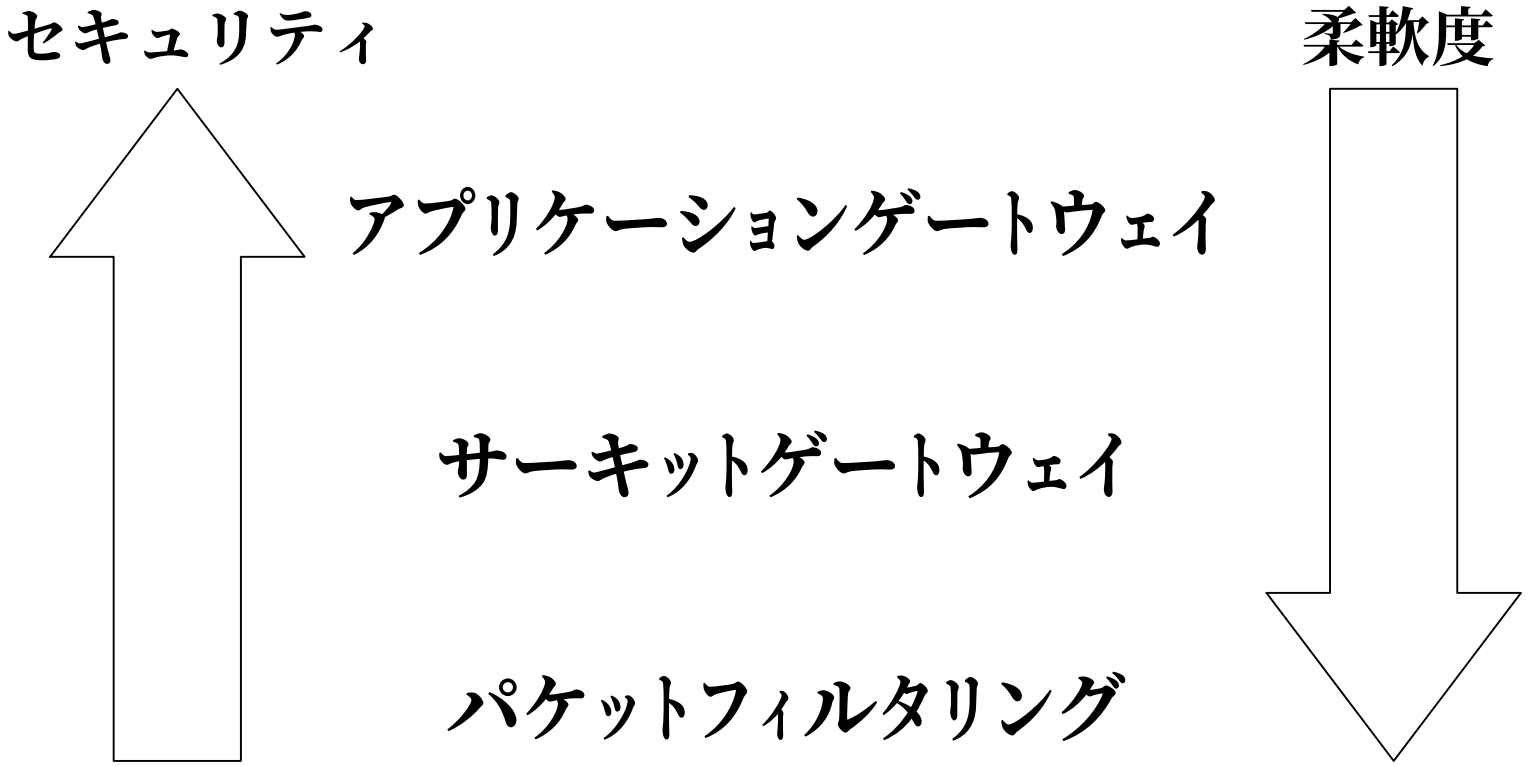
- アプリケーションプロトコルレベルでのデータの中継
  - プロトコルに応じた制御や監視情報の取得が可能
  - ユーザ認証が可能



アプリケーション ゲートウェイ

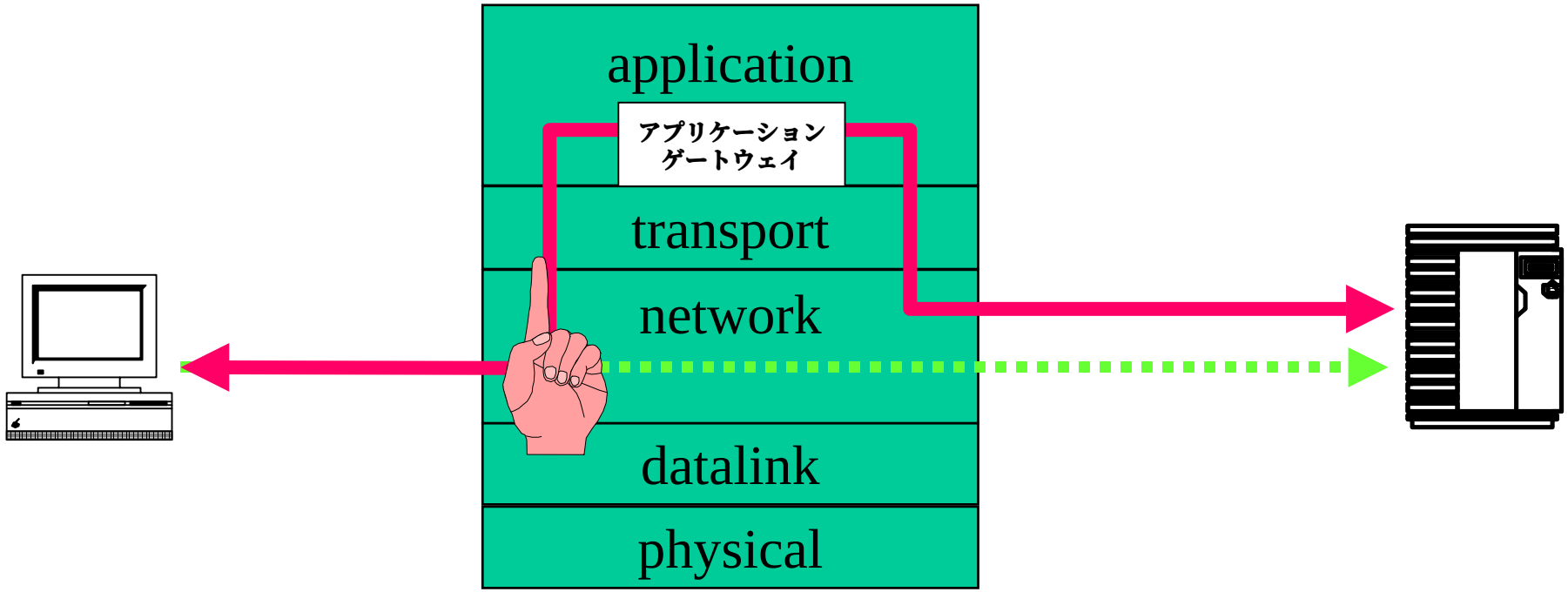
- 本来ゲートウェイ機能を持つソフトウェア
  - sendmail
  - INN, C-News
  - NTP
  - Named
- 専用中継プログラム
  - HTTP, Gopher...
  - telnet, ftp...
  - RealAudio, StereamWorks...

実装方式の比較



透過型 Proxy

- 本来自分宛てでない接続を横取りする
- クライアントは相手と直接通信しているように見える

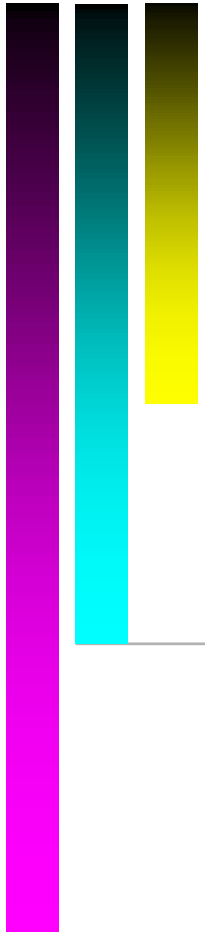


透過型 Proxy

- 原則として TCP レベルでの中継
- IP パケットレベルで中継はしないので、NAT や IP Masquerade とは本質的に異なる
- 一般的にはうまく働くが、特殊な状況ではトラブルの原因になることもある

SOHO でのファイアウォール

- サーバを運用するのであれば、ネットワークの規模には関係なくファイアウォールが必要
- 外部からのアクセスの必要がなければ、ルータで内向きの接続を制限してしまえばよい
- サーバのアウトソースサービスを利用することで単純なファイアウォールが実現可能
  - DNS サーバ、メールサーバ、Web サーバ
- ただし、端末のセキュリティ確保も重要
  - ダイアルアップも同様



商用ファイアウォール

商用ファイアウォールサービス

- コンピュータやネットワークが専門ではないユーザの増加
  - サポートや管理サービスの必要性
- 安全に手軽にインターネットを利用できる環境が必要
  - turn-key システムの必要性
- 攻撃手法の高度化
- インターネットサービスの複雑化
  - 専門家以外の対応の限界

商用ファイアウォールサービス

- ツールを組み合わせるだけでは、ファイアウォールを安全に運用できない
- 様々なツールやサービスの統合
  - パケットフィルタ
  - アプリケーションゲートウェイ
  - コンサルティング
  - 構築サービス
  - 教育/セミナー

商用ファイアウォールサービス

- nトレンド
  - – NT ファイアウォール
    - • ＯＳの基本機能のセキュリティに注意
  - – 管理サービス
    - • ファイアウォール製品の複雑化
    - • さらにアウトソーシング指向
  - – ハイブリッド型ファイアウォール
    - • パケットフィルタ ＋ アプリケーションゲートウェイ
  - – All-in-One 型マルチサーバ

代表的商用ファイアウォール

- Altavista Firewall
  - Digital Equipment Corporation (Compaq)
- FireWall-1
  - Checkpoint Software Technologies
- CyberGuard Firewall
  - CyberGuard Corporation
- Gauntlet
  - Network Associates

代表的商用ファイアウォール

- Eagle
  - Raptor Systems, Inc.
- Portus
  - Livermore Software Laboratories, Inc.
- Sidewinder
  - Secure Computing Corporation
- SunScreen
  - Sun Microsystems, Inc.

etc...

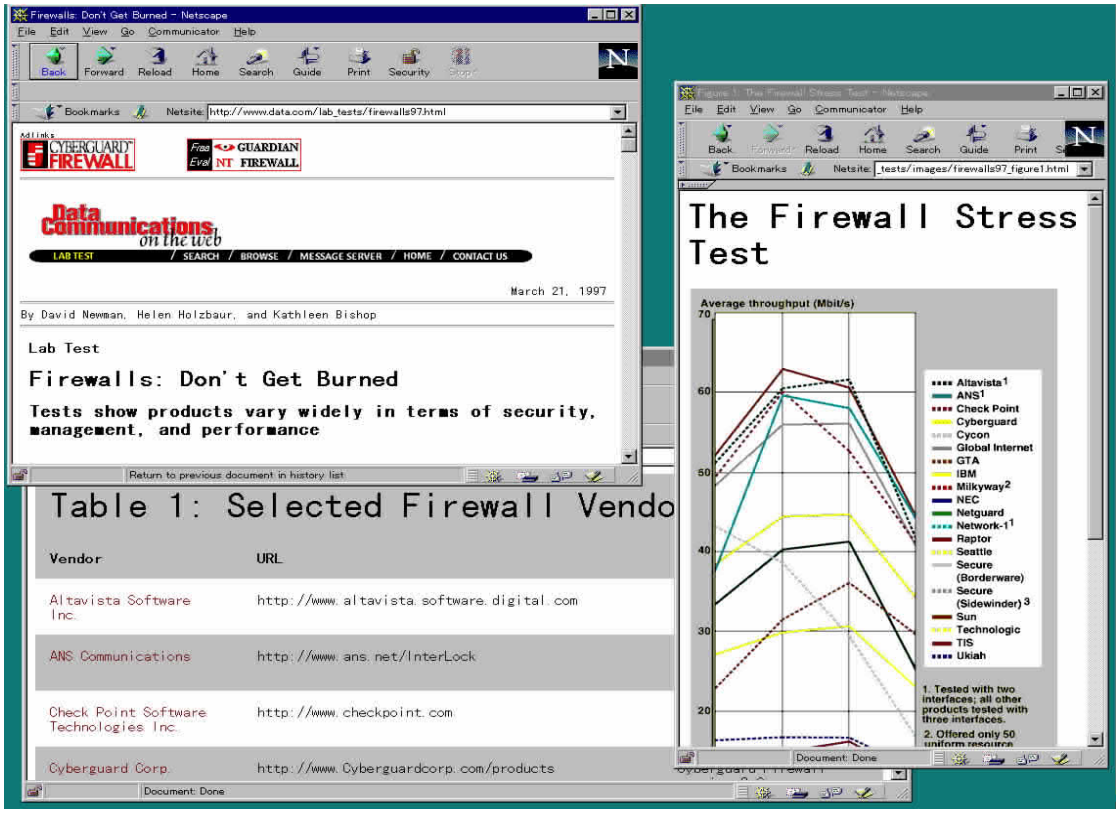
ICSA Firewall Certification Program

- http://www.icsa.net/services/consortia/firewalls/certified_products.html
- 3COM, ANS Communications, Ascend, Bull S.A., CheckPoint Software Technologies, Inc., Cisco Systems, Cyberguard Corp, Digital Equipment Corporation, Elron Software, Global Technologies Associates, IBM, Internet Device, Isolation Systems Ltd, Livermore Software Laboratories, Lucent Technologies, Milkyway Networks, NetGuard, Network-1, Radguard Ltd., Raptor Systems, Secure Computing Corporation, Sun Microsystems, Technologic Inc., Trusted Information Systems, Ukiah Software, Watchguard Technologies

(※ 98年1月にNCSAから名称変更。)

ファイアウォール製品の比較

Data Communications Magazine Firewalls Lab Test



- http://www.data.com/lab_tests/firewalls97.html

商用プロダクト－何を基準に選ぶか

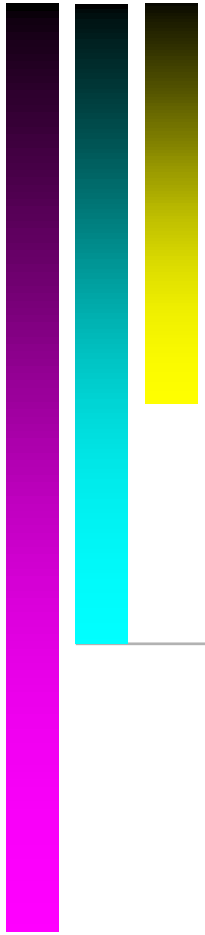
- 必要なアプリケーションは使えるか
- 拡張性はあるか
- 処理能力は十分か
- ソースコードが必要か
- サポート体制は
- 管理のためのコストをいくらかけられるか
- 動作環境
- 費用はいくらかけられるのか

商用プロダクト－何を基準に選ぶか (別の側面)

- 機能は遅かれ早かれ似たようなものになる
  - 表面的な機能よりもコンセプト重視
  - 新しい機能をいち早く取り入れるシステムはむしろ不安な場合も
  - プロダクトそのものよりもサポートが重要

ネットワーク以外の対策も重要

- 物理的セキュリティ
  - ビル、居室、計算機室
  - バックアップメディア
  - 計算機
  - 線路
- 情報管理
  - 業務フロー
  - 文書管理
  - 設備管理



暗号技術の応用

情報セキュリティの要件

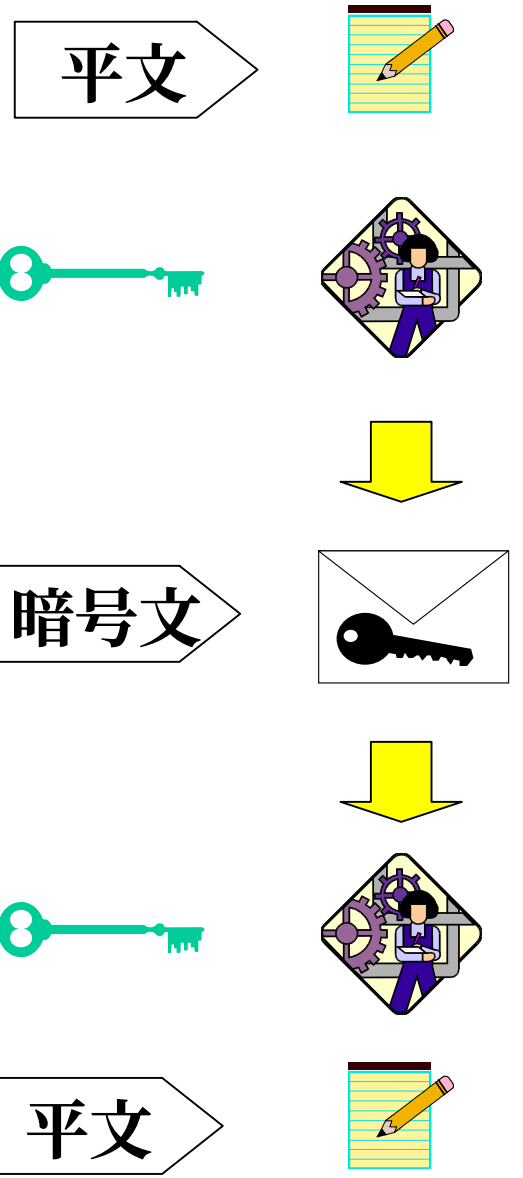
- Confidentiality: **秘匿性**
  - **秘密の保持**
- Integrity: **完全制**
  - **内容の保証**
- Authentication: **認証**
  - **正しい通信相手を認識できる**
- Non repudiation: **否認防止**
  - **通信の事実を保証できる**

共通鍵暗号と公開鍵暗号

- 共通鍵 (秘密鍵) 暗号
  - 通信する両端で、あらかじめ秘密の同じ鍵を持っていることを前提とする
  - 暗号化と複合化には同じ鍵を使う
- 公開鍵暗号
  - 2つの鍵を使う
  - 一方の鍵で暗号化したデータは、もう一方の鍵でしか複合できない
  - 秘密鍵と公開鍵

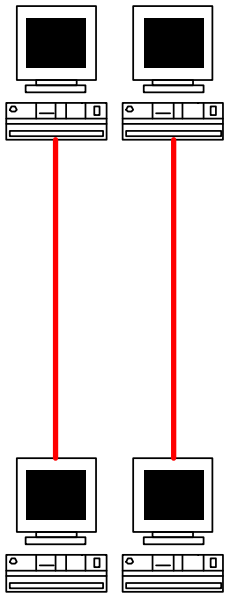
共通鍵暗号

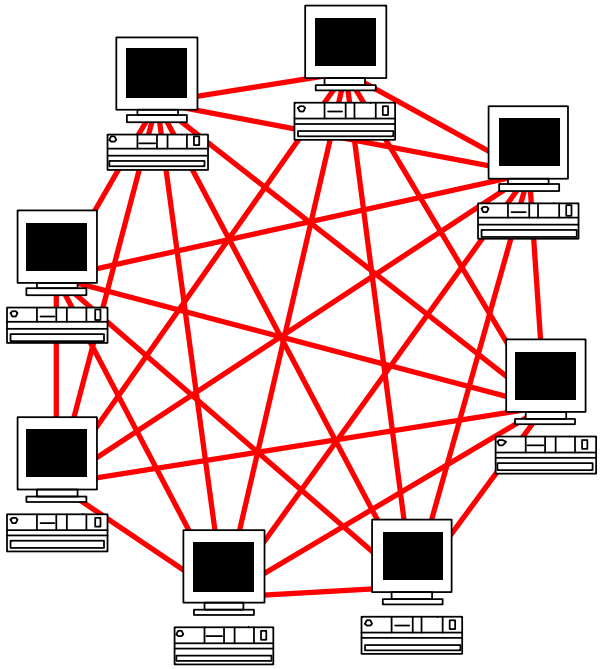
- 暗号鍵と複合鍵が同一
- 両者で共通の秘密情報を共有する
- 高速
- 例
  - DES, FEAL, RC2, RC4, IDEA...



共通鍵暗号

- n 少数の特定の相手との通信には問題は少ない
- n 通信相手が多くなると、鍵の管理が複雑化



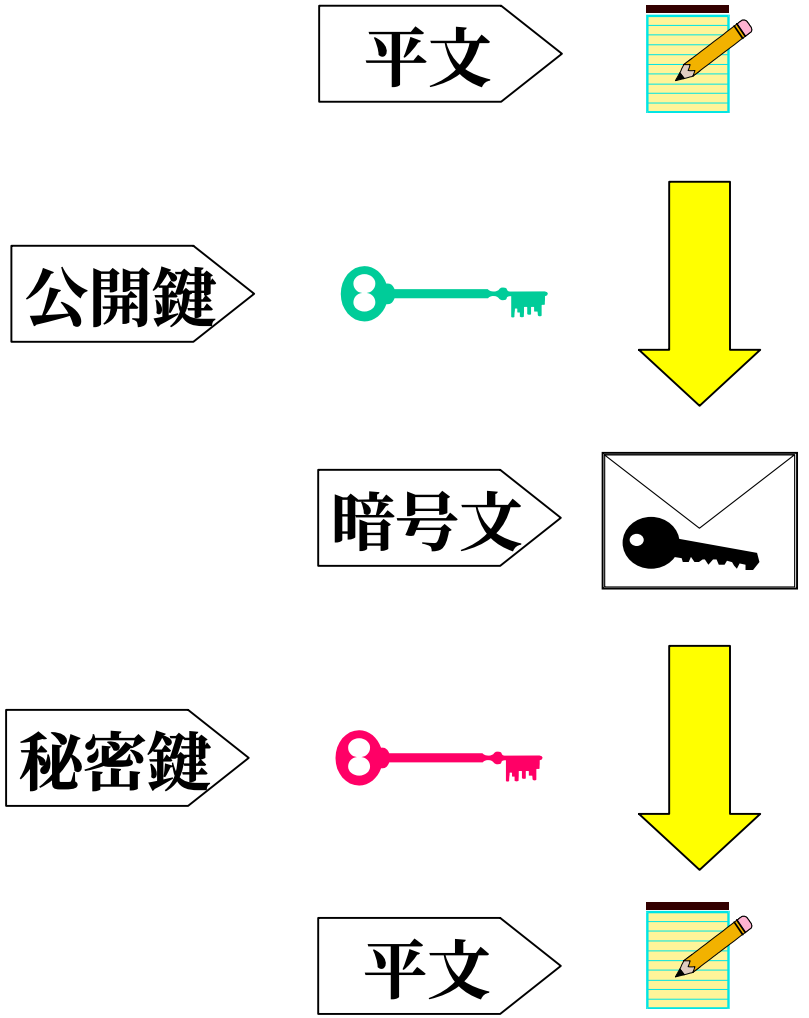


公開鍵暗号の特徴

- 不特定多数のユーザ間で暗号化通信が可能
  - 秘密鍵は本人だけが持つ
  - 公開鍵はすべて公開
  - 相手の公開鍵で暗号化すれば、本人にしか読むことができない

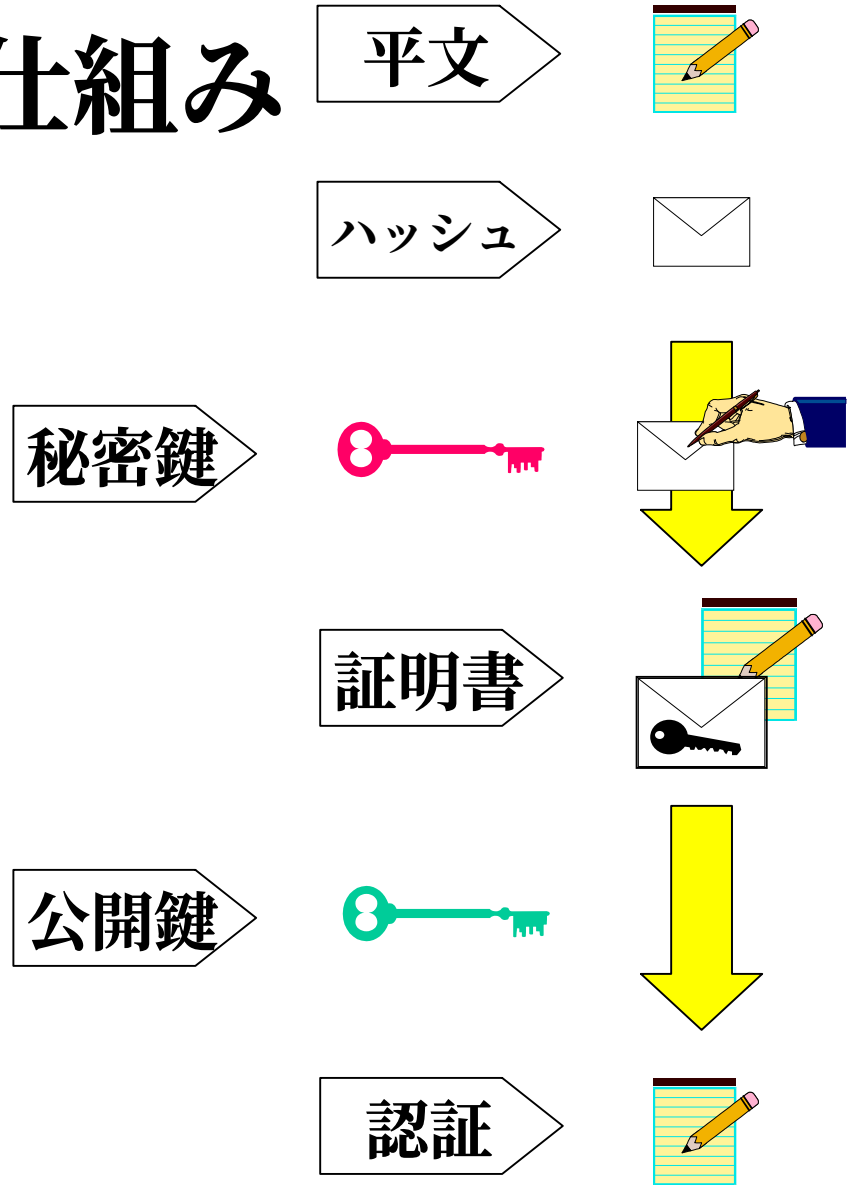
公開鍵暗号の動作

- 公開鍵で暗号化すると、対応する秘密鍵でしか、復号できない
- 各ユーザは、一組の鍵だけを管理すればよい



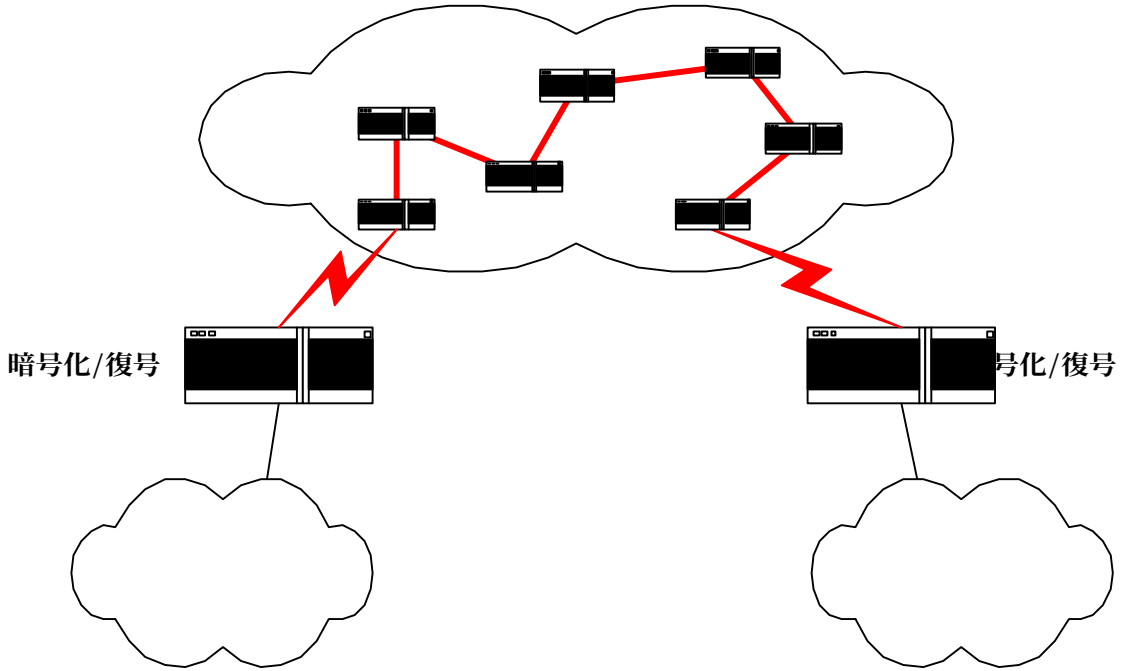
公開鍵による認証の仕組み

- デジタル署名
  - データの一方向ハッシュ値を自分の秘密鍵で暗号化して添付
    - 公開鍵で複合化したものとデータが一致すれば認証



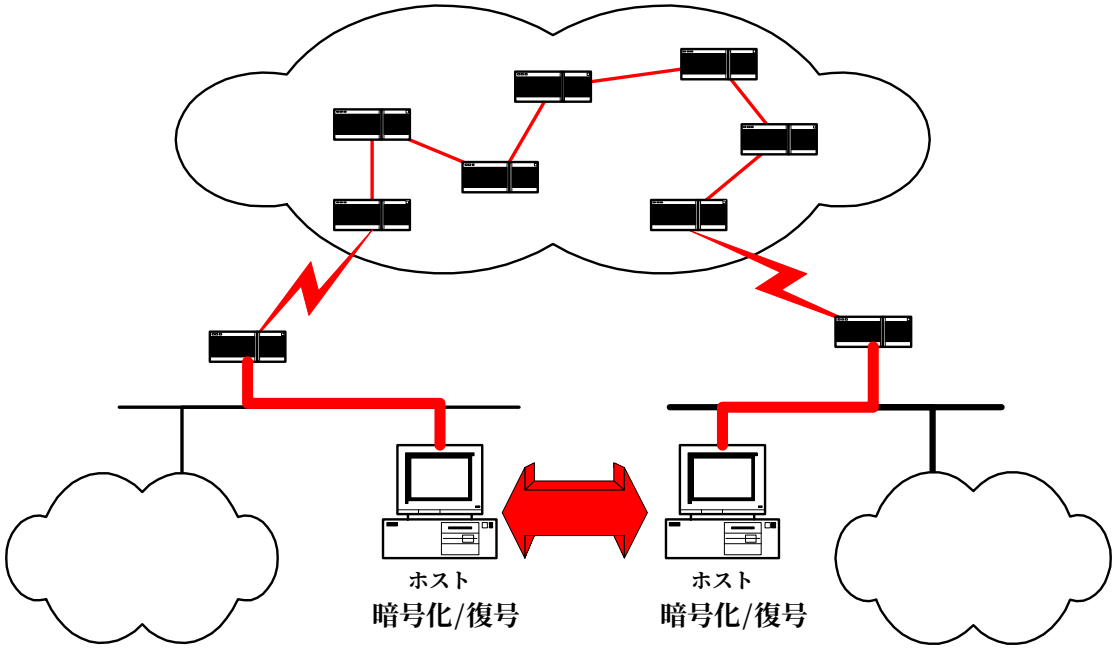
通信経路の暗号化

- 公衆網を流れるデータを暗号化することによって、安全性を確保する



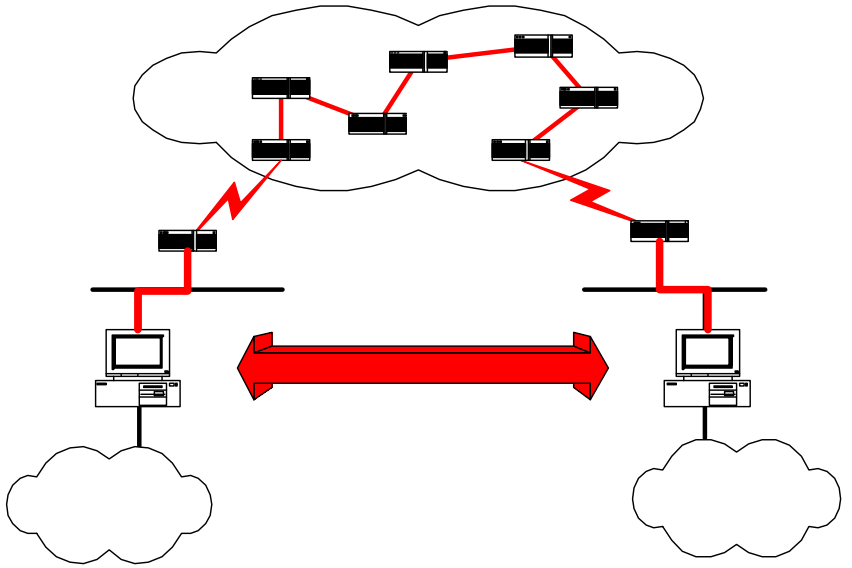
ホスト間の暗号化

- ホスト間を流れるデータを暗号化することによって、安全性を確保する



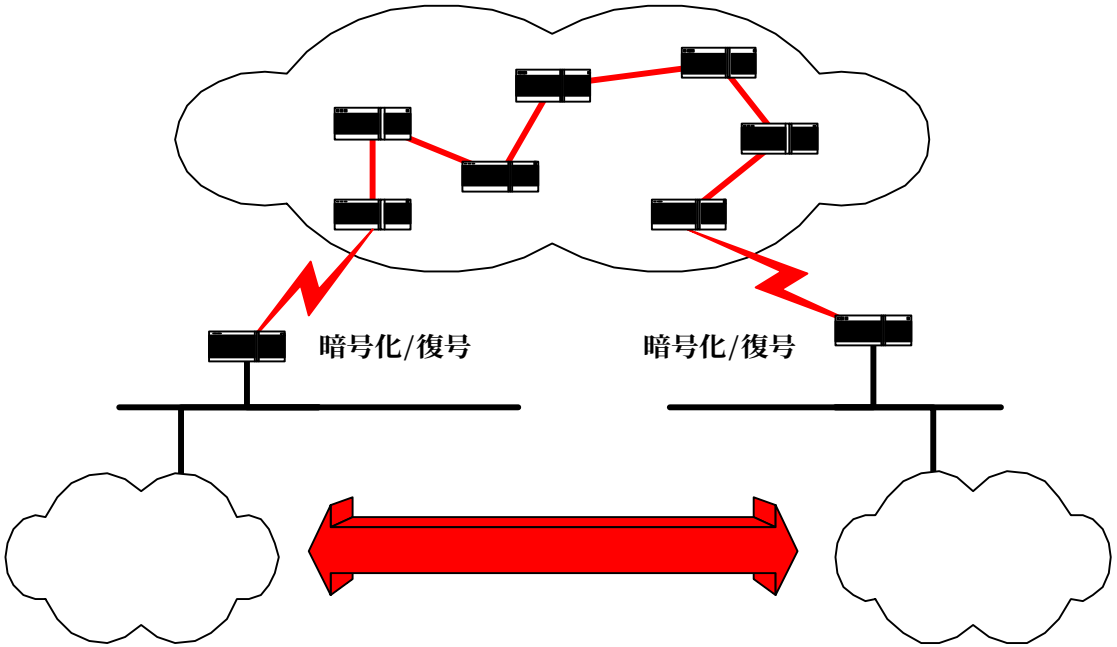
ファイアウォールでの暗号化

- ファイアウォール間を流れるデータを暗号化することで、安全性を確保する
- ファイアウォールの機能をそのまま保ち、特定の相手との安全な通信経路の確保



ネットワーク間の暗号化

- ネットワーク間を流れるデータを暗号化することによって、安全性を確保する

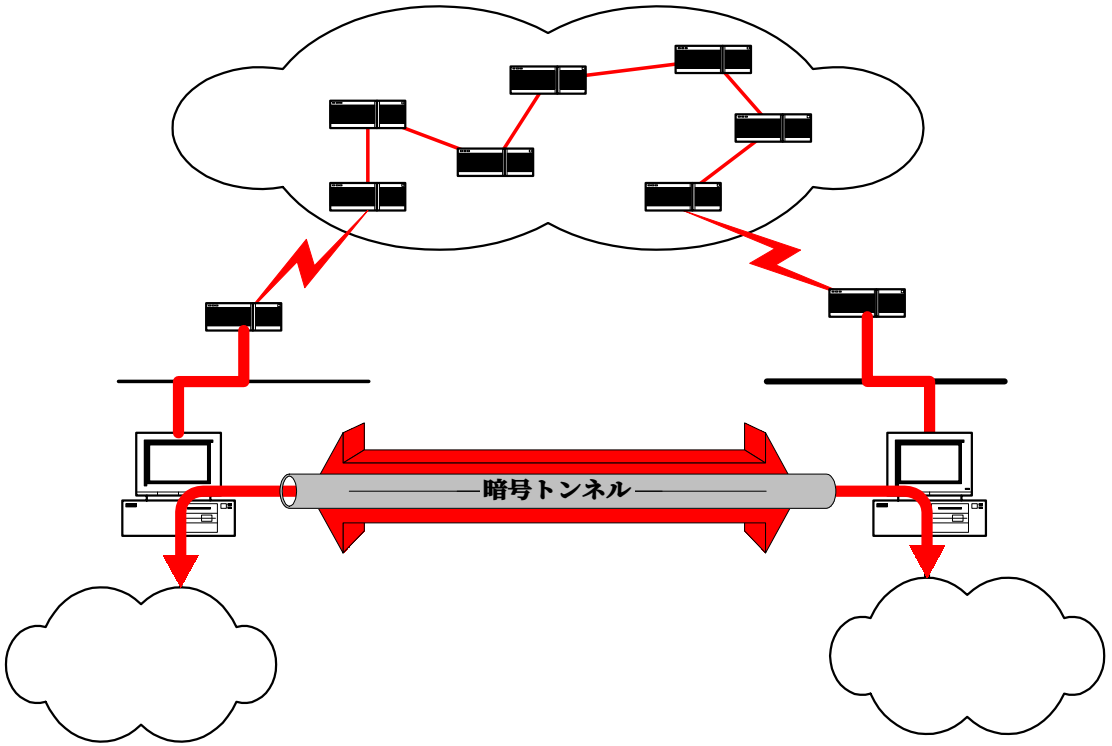


VPN
Virtual Private Network

- ネットワーク間のパケットをカプセル化して、インターネット上を配送
- プライベートアドレスを運用するネットワークをインターネットを介して相互接続が可能
- インターネットを使って、仮想的に専用線で接続されたのと同等なネットワーク環境を構築
- 本当の意味でのプライベートネットワークであるためには、通信経路における安全性の確保が不可欠

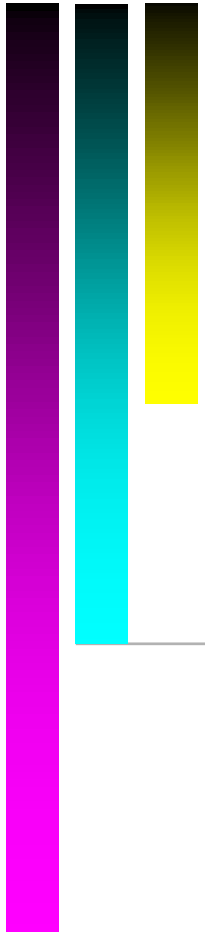
VPN
Virtual Private Network

- 注意：VPN はファイアウォールとの機能的関連性は薄い



トランスポート／アプリケーション層での暗号化

- SOCKS
- SSL
- SSH
- PGP
- S/MIME

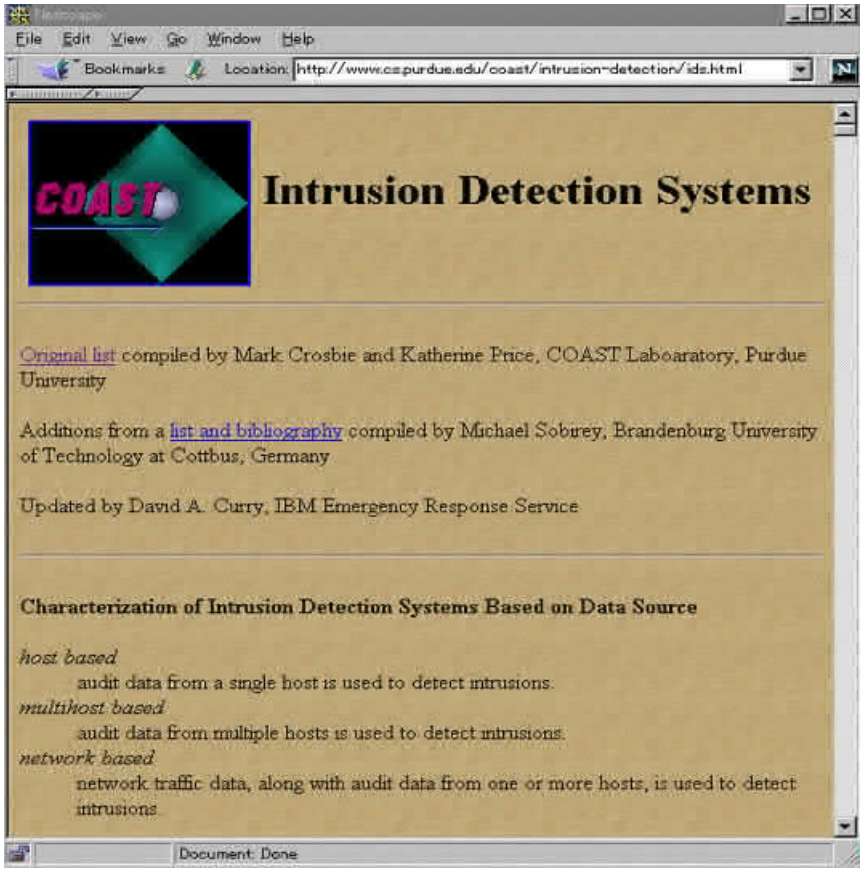


侵入検知システム
Intrusion Detection System (IDS)

ファイアウォールでは...

- 外部のホストに対する攻撃は防ぐことはできない
  - WWW, FTP, etc.
- すでに内部にいる侵入者は発見できない
  - CSI/FBI computer crime survey, Computer Security Journal, 1997 によれば不正侵入の 80% は内部から
- 存在しないホストに対する攻撃は気がつかない
  - port scanning, 回線資源の浪費
- 未知の攻撃は防げない

COAST's Intrusion Detection Information Pages



– http://www.cs.purdue.edu/coast/intrusion-detection

IDS
情報源

- ホストベース
  - 単一のホストの情報に基づく
- マルチホストベース
  - 複数のホストからの情報に基づく
- ネットワークベース
  - ネットワークからの情報に基づく

IDS
侵入モデル

- Anomaly detection model
  - 通常のユーザやシステムの活動とは異なった動きを捜査し、侵入を検出するモデル
- Misuse detection model
  - 既知の侵入手口を用いた形跡、あるいはシステムの弱点(vulnerabilities)をついた活動を捜査し、侵入を検出するモデル

商用 IDS
The Kane Security Monitor

- Intrusion Detection
  - ネットワークベース
  - サーバ、WSのログファイルをチェック
  - 特定のアクションが起こった場合、管理者に通知
    - ログインの試行回数が異常に多く発生した場合など
  - Windows NT用
- http://www.intrusion.com/

商用 IDS
RealSecure

- Internet Security systems
- http://www.iss.net/
  - ネットワークベース

商用 IDS
Stalker シリーズ

- Haystack Labs
  - 97年TISが吸収, TIS は現在 Network Associates, Inc.
- http://www.haystack.com
- Stalker
  - マルチホストベース
  - Sun, IBM,HP 等のUNIXシステムで利用可
- WebStalker
  - WWWサーバに対する不正なアクセス、コンテンツの書き換えをチェック
  - NT版、UNIX (Solaris 2.6, AIX 4.3) 版

商用 Intrusion Detection System NetRanger

- WheelGroup Corporation
  - 98年に Cisco に吸収
- http://www. wheelgroup.com/
  - ネットワークベース
  - Sensor
    - Solaris on Pentium or UltraSPARC
    - ルータのイベント、ネットワークトラフィックを監視、Directorへアラーム転送
  - ルータの制御

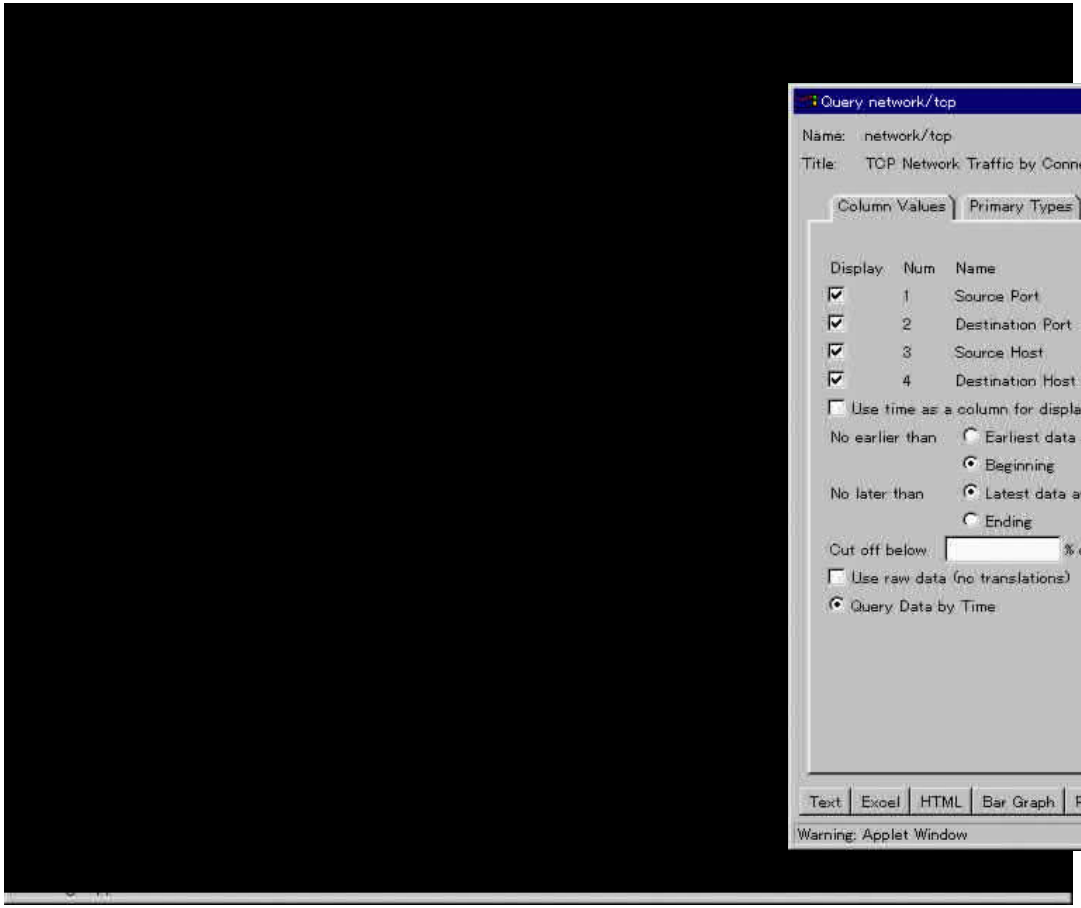
商用 Intrusion Detection System Session Wall-3

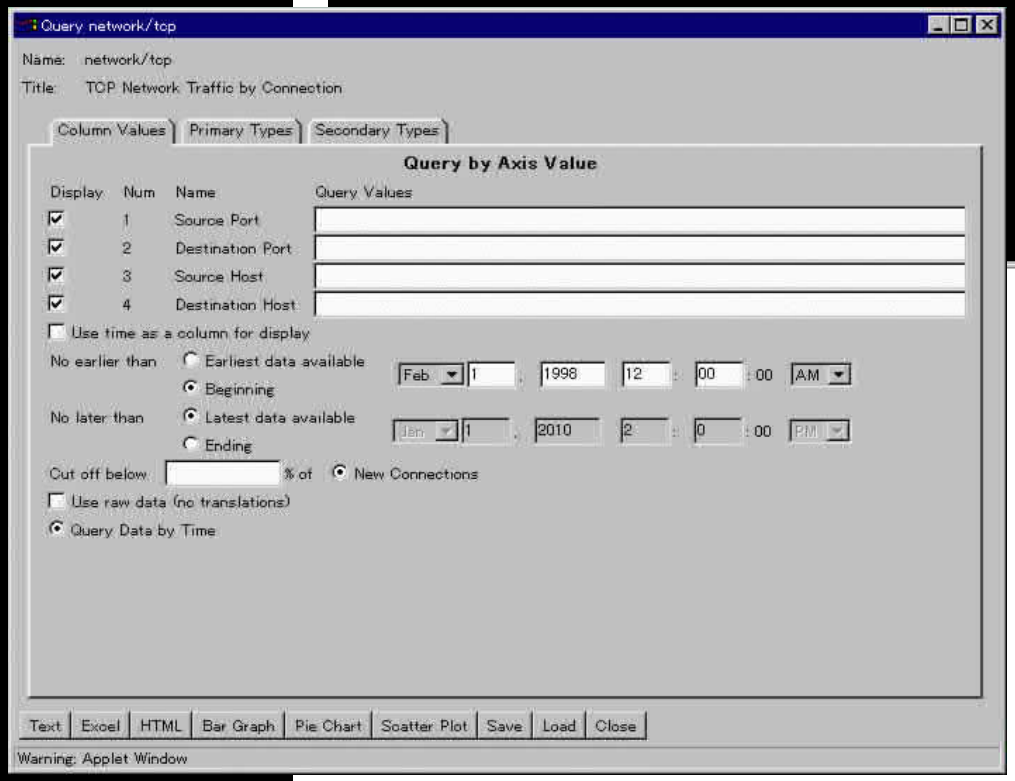
- AbirNet
- http://www.abirnet.com
  - ネットワークベース
  - 内部Firewallの構成、パフォーマンスには影響を与えない
  - PC上で動作、Windows95, NT用
- 比較的安価

商用 Intrusion Detection System
Network Fright Recorder (NFR)

- Network Fright Recorder, Inc.
- http://www.nfr.net/
  - ソースコードのフリー配布
  - ネットワークベース
  - Packet Sucker, Decision Engine, Backend のセット
  - パケット収集&解析
  - プログラミング可能 (N-code)
  - BSD/OS, HP-UNIX, Linux 等で動作
  - Java対応ブラウザで収集データを参照

NFR 操作画面





NFR レポート画面

その他の商用 IDS

- CMDS (Computer Misuse and Detection System) by SAIC
- INTOUCH INSA (Network Security Agent) by TTI
- OMNIGUARD Intruder Alert by Axent
- POLYCENTER Security Intrusion Detector by Digital
- Watch Dog by InfoStream
- etc...