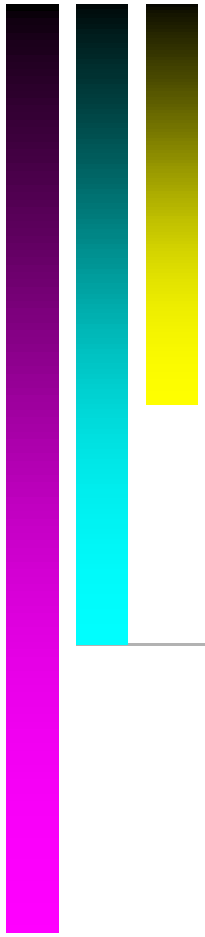


インターネットセキュリティ(2)

Internet Week ‘97

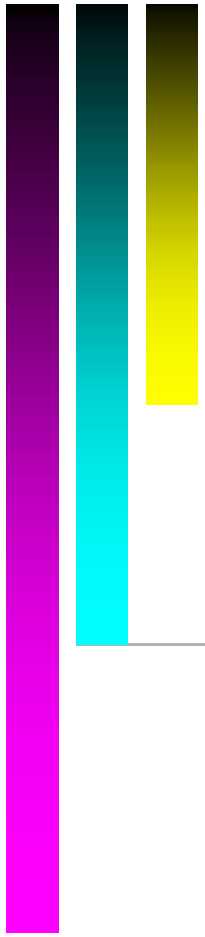
株式会社インターネットイニシアティブ
歌代 和正 <utashiro@iij.ad.jp>
PGP fingerprint: 6B 8F B8 3A 51 1F 2D A2 A7 EA E6 E7 58 73 71 97

Agenda

- ✓ インターネット上のセキュリティ的脅威
- ✓ 不正アクセスの事例
- ✓ 最近の代表的な攻撃手法
- ✓ セキュリティポリシー
- ✓ ファイアウォールの構築技術
- ✓ 商用ファイアウォール
- ✓ 使い捨てパスワード
- ✓ 暗号技術の応用
- ✓ 転んだ後のセキュリティ

Not in Agenda

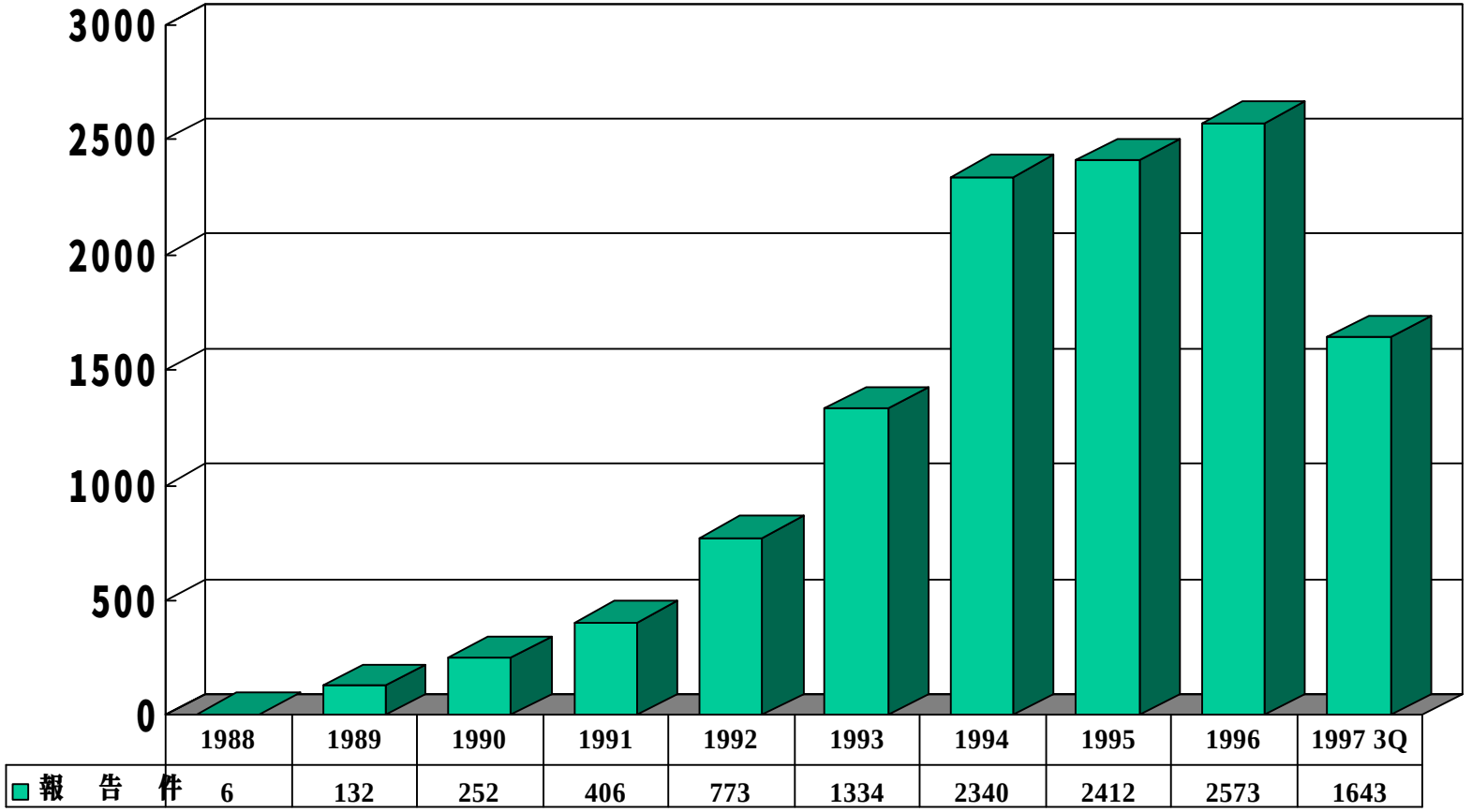
- ✓ ウィルス
- ✓ 電子商取引
- ✓ IPSEC
- ✓ IPv6



インターネット上の
セキュリティ的脅威

CERT/CC への報告件数

(http://www.cert.org/pub/cert-stats/cert_stats.html より)



JPCERT への報告
1996年10月1日 ～ 1997年3月31日

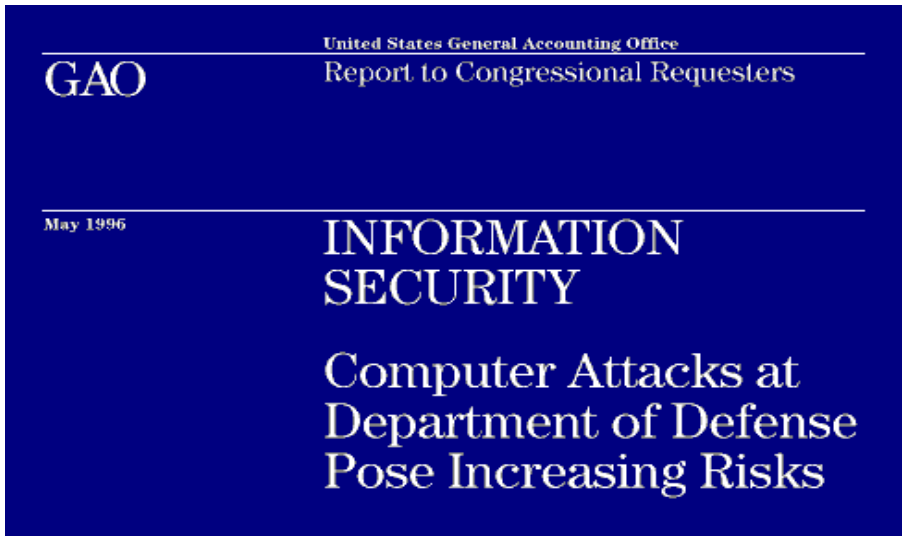
- アタックの内容
  - sendmail 攻撃 (131件)
  - INN による攻撃 (49件)
  - パケット盗聴 (7件)
  - 電子メールの不正な中継
  - Web サーバの CGI を利用した攻撃
  - トロイの木馬
  - パスワード破り
  - ルート権限の搾取

JPCERT への報告
1997年4月1日 ～ 1997年6月30日

- 主なアタック
  - ネットワークニュース・サーバ (INN) を悪用した攻撃
  - 電子メールの不正な中継と電子メール爆撃
  - システムへの不正侵入
  - Web サーバーの cgi-bin プログラムを悪用した攻撃
  - パケット盗聴プログラムによる攻撃
- 傾向
  - 既知の手口の繰り返し
  - SPAM 問題の深刻化

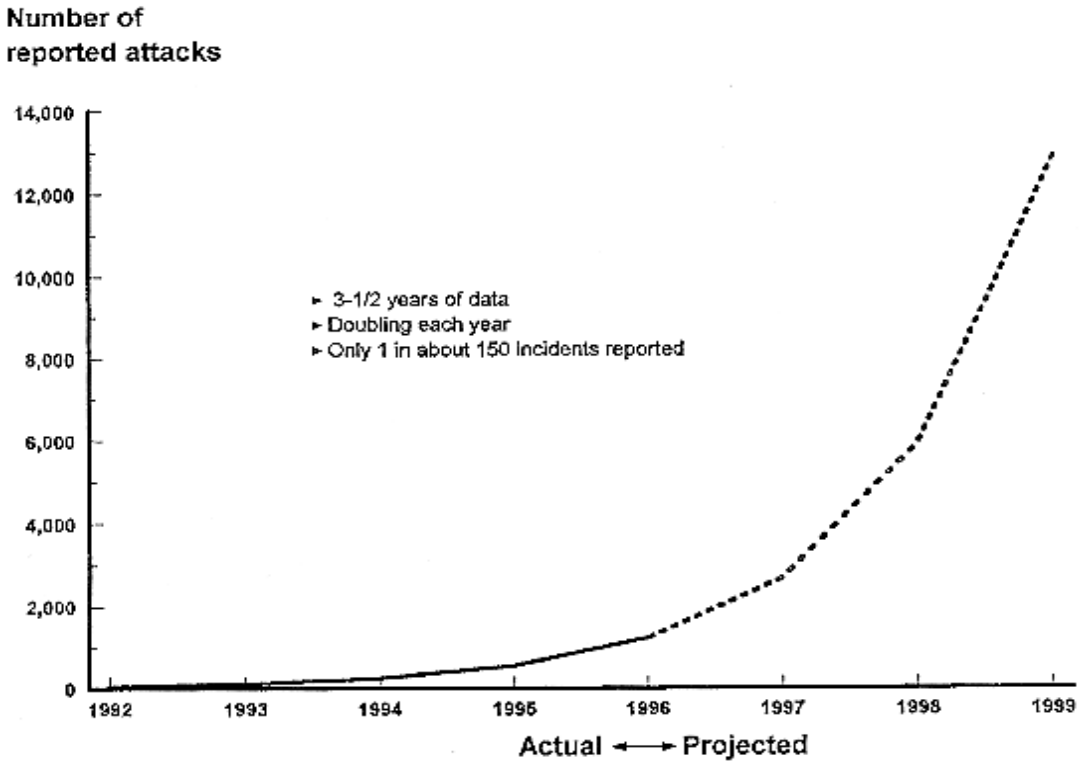
U.S. General Accounting Office Report

- Computer Attacks at Department of Defense Pose Increasing Risks, AIMD-96-84
- Computer Hacker Information Available on the Internet, T-AIMD-96-108

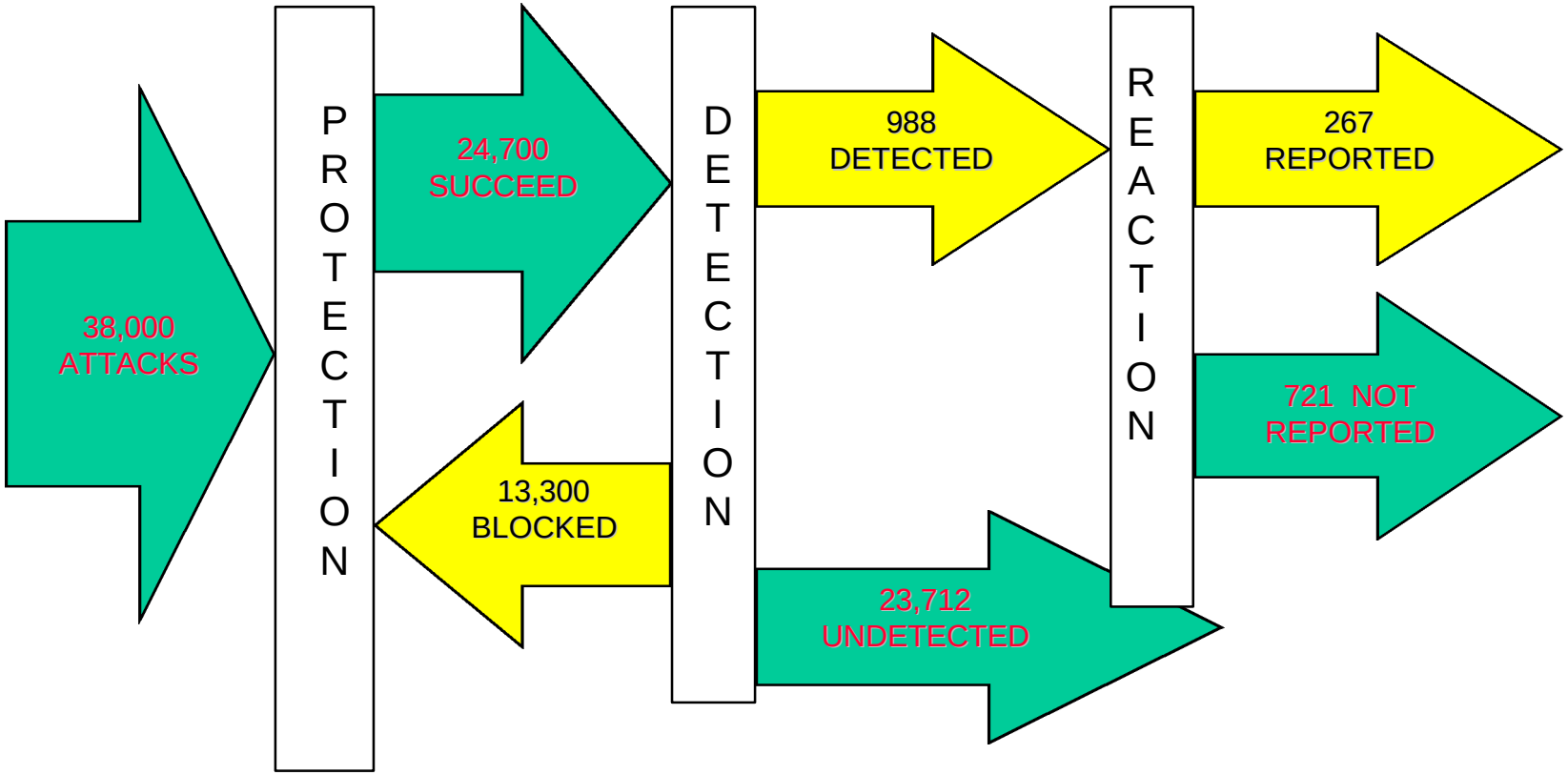


不正アクセス件数は確実に増加

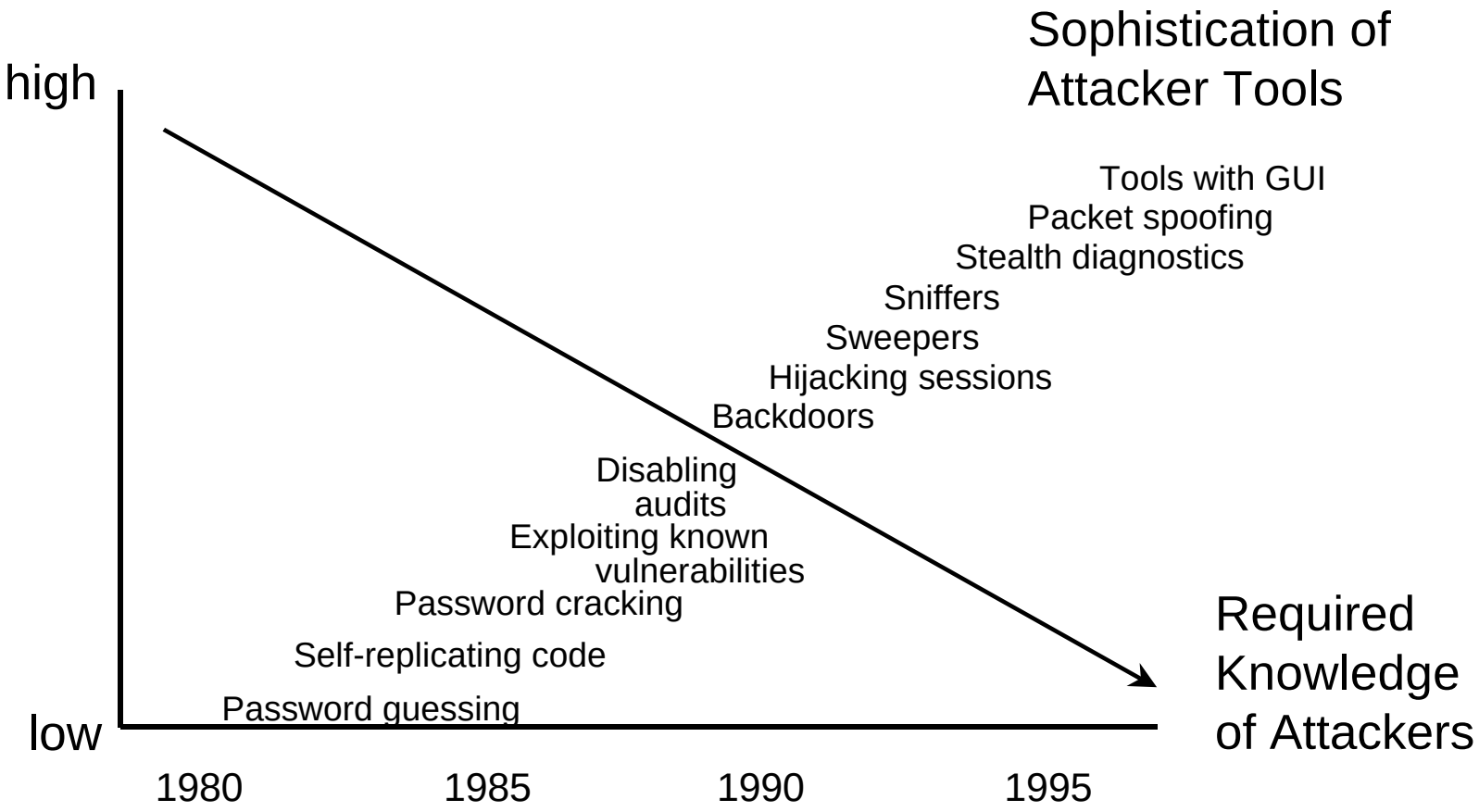
- Dense Security Information Agency に対して
  - 1995年 250,000 件の攻撃



不正アクセス発見の難しさ



高度化する技術


Sophistication of
Attacker Tools
high
low
Tools with GUI
Packet spoofing
Stealth diagnostics
Sniffers
Sweepers
Hijacking sessions
Backdoors
Disabling
audits
Exploiting known
vulnerabilities
Password cracking
Self-replicating code
Password guessing
Required
Knowledge
of Attackers
1980
1985
1990
1995

目的

- 情報の搾取
- 運用の妨害
- 資源の搾取/浪費
  - 計算機資源
  - 回線資源
  - 人的資源
- 社会的権威の失墜
- 自己顕示

攻撃の方法
情報犯罪的手法

- 情報の盗聴
- 情報の改竄
- 情報の捏造
- 権限の取得
  - 総当たり法、辞書アタックなどによるパスワード破り
  - システムプログラムのバグを攻撃
  - トロイの木馬

攻撃の方法
サービス不能攻撃

- Denial of Service Attack
- 相手のサービスを妨害するのが目的
  - 運用の妨害や停止
  - 回線容量の浪費
- 完全に防ぐのは困難
- 比較的簡単に実現できるのが問題

不正アクセスの事例

1988 Internet Worm

- 全世界規模のインターネットワーム事件
  - Morris worm とも呼ばれる
  - 異常に気づいた管理者がインターネットとの接続を絶ったため混乱の回復に時間がかかった
  - セキュリティの重要性を認識
  - CERT 設立のきっかけ

1994 Internet Sniffer **攻撃**

- インターネット上での大規模な盗聴
  - ISP のサーバが被害
  - インターネット上でのパケット盗聴
  - 数千に及ぶパスワードが漏洩

1994-1995 Kevin Mitnik

- 1994 Christmas / 1995 St. Valentine’s Day
- TCP ハイジャック
- システムへの不正侵入と情報の搾取
  - WELL や Netcom などの著名な ISP が被害

1996 日本国内 ISP の被害

- サーバへの侵入
- サーバの稼動を妨害
- 数日間にわたり業務停止
- 警察の介入

Web サーバへの攻撃 (1996.7)

- CIA のサーバが侵入されデータをいたずらされる
- CGI による攻撃

  http://www.news.com/News/Item/0,4,3648,00.html

国内放送局ホームページ書き換え

- 天気予報のホームページの画像が猥褻なものに置き換えられた
- 容疑者は逮捕
- 電子計算機損壊等業務妨害罪が適用

DNS データ偽造攻撃

- 内容
  - 1997.07
  - Internic の root サーバのデータを偽造
  - bind 4.9.6 以前のセキュリティホール
- 情報
  - CERT Advisory CA-97.22
- 対策
  - bind 4.9.6 できればバージョン 8 以上を利用

最近の代表的な攻撃手法

TCP SYN 攻撃

- 内容
  - TCP の SYN パケットを大量に送信
  - OS 内の資源が浪費させられて新たな通信ができなくなる
  - TCP/IP が持つ本質的な問題
- 対策
  - ベンダーパッチ
  - 本質的な解決は難しい

TCP Out of Band 攻撃

- 内容
  - NT のあるポートに特殊な TCP パケットを受け取るとシステムがハングアップ
- 対策
  - NT 4.0 SP3 は安全か?
  - Port 137-139 は通さない
  - 危険なシステムは使わない

Ping o’ Death

- 内容
  - 不正な ping (ICMP ECHO) パケットを送信して相手のホストを妨害
- 情報
  - CERT Advisory CA-96.26
  - http://www.dfm.dtu.dk/netware/pingod/ping.html
- 対策
  - OS のバージョンアップ

UDP Echo 攻撃

- 内容
  - UDP Echo サービスとChargen を組み合わせて、無限に回線を使い尽くす攻撃
  - UDP パケットのアドレスの偽造は簡単
- 対策
  - 不要なサービスは提供しない

CGI を利用した攻撃

- 内容
  - Apache httpd のセキュリティホールを攻撃
  - 任意のコマンドを実行
- 情報
  - JPCERT-E-INF-97-0003-01
    - 緊急報告 - phf CGI プログラムを悪用したアタック
  - CERT Advisory CA-97.07
    - Vulnerability in the httpd nph-test-cgi script
  - CERT Advisory CA-96.06
    - Vulnerability in NCSA/Apache CGI example code
- 対策ーバージョンアップ

SPAM

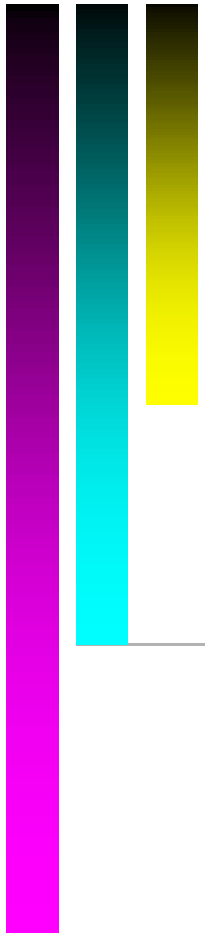
- 内容
  - インターネットを使って大量の情報発信
  - ユーザは不要なメールを受け取る被害
  - ISP の被害が大きい
  - 業務妨害が目的ではない
- ISP の被害
  - サーバの過負荷
  - クレーム処理

SPAM

- 対策
  - 無関係なメールは受け取らない
    - 発信者と受信者のチェック
  - 顧客以外からの SMTP の受信を拒否
    - アドレスによる制御
    - ローミング問題
  - 発信者アドレスによるフィルタリング
    - SPAM リストの利用

SPAM

- 情報
  - http://spam.abuse.net/
  - http://maps.vix.com/
    - MAPS, the Mail Abuse Protection System
  - http://www.jpcert.or.jp/tech/97-0001/
    - 技術メモ - 電子メール配送プログラムの不正利用 (予期しない中継)
  - http://www.Sendmail.ORG/antispam.html
    - Anti-Spam Provisions in Sendmail 8.8



セキュリティポリシー

ネットワークセキュリティの問題点

- 一般に...
  - どんな脅威があるのかわからない
  - 目に見えない
  - 従来のセキュリティと異なる概念
  - 一面的な情報しか流れてこない
- 結果として両極端の反応
  - 過剰反応
  - 無関心

ホストセキュリティと ネットワークセキュリティ

- ホストセキュリティ
  - ホストを守るためのセキュリティ
    - パスワード管理
    - ログ管理
    - セキュリティホール対策
- ネットワークセキュリティ
  - ネットワークを守るためのセキュリティ

セキュリティポリシー

- 何を守るのか
  - 情報？財産？名誉？
- 何を実現すべきなのか
  - インターネットフルアクセス？電子メール？Web？電子ニュース？
- どんな危険が存在するのか
  - 盗聴？偽造？破壊？侵入？盗難？業務妨害？
- 誰から守るのか
  - 外部？内部？スパイ？

セキュリティポリシー

- 管理ドメイン内で一貫したポリシーを持つ
- 一般的なポリシー
  - 個々のホストのセキュリティは信用できない
  - 一般ユーザにネットワーク全体のセキュリティを頼ってはならない
  - 内部のホストは、他の内部のホストやユーザを信用する

セキュリティポリシー

- 一般ユーザがセキュリティを気にしなくても安全にネットワークを利用できる環境が必要
- 実現方法
  - 境界防御
  - 要塞ホスト
  - ファイアウォール

ネットワーク犯罪
ーどう対応すべきかー

- 情報の入手が重要
  - メーリングリスト
  - ニュース
  - ベンダーパッチ
  - CERT (Computer Emergency Response Team)
    - 1988年のワーム事件をきっかけに発足
  - CIAC (Computer Incident Advisory Capability)

ネットワーク犯罪
ー具体的対策ー

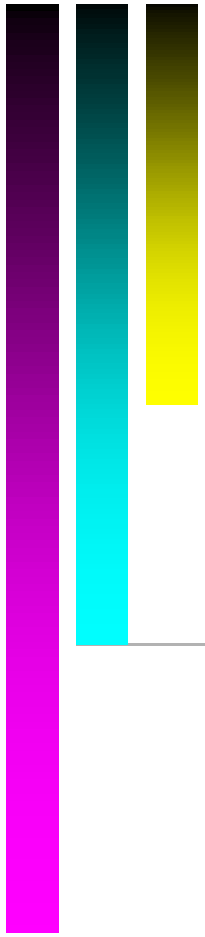
- ファイアウォール (防火壁)
- 使い捨てパスワードの利用
- 通信の暗号化
  - メッセージレベル - PEM, PGP, PET
  - データグラム - Secure IP, 暗号化ルータ
  - データリンク
- 利用状況/利用履歴の監視
- システムの正当性検査
- ユーザ教育

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

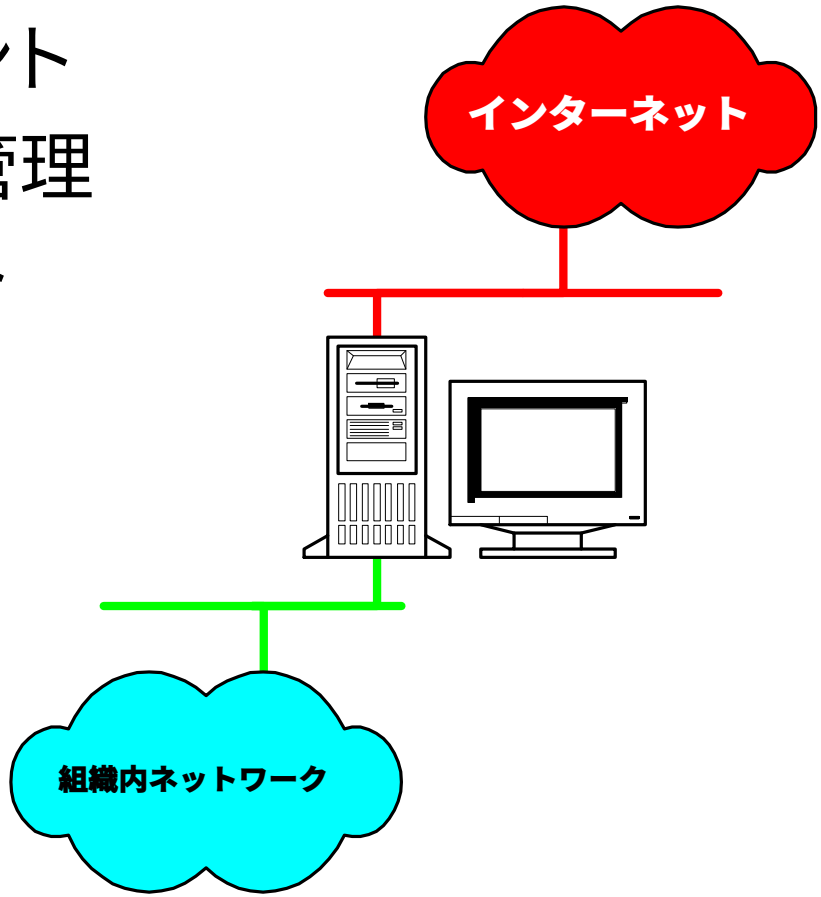


ファイアウォールの構築技術

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

- **Single Strong point**



ファイアウォール

- 要塞ホスト+ Proxy ゲートウェイ + パケットフィルタ
  - 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
もう一つの役割

- 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

ファイアウォール構築ツール

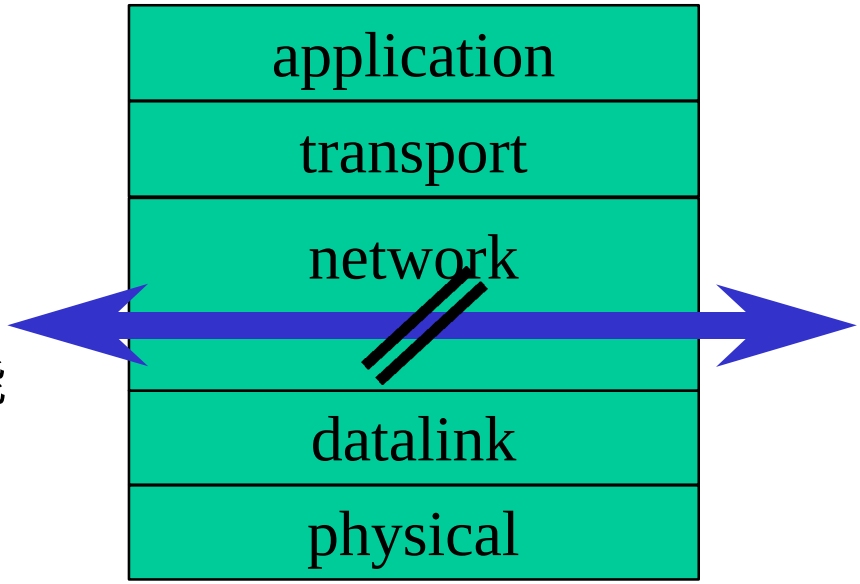
- 何種類かのツールの組み合わせ
  - ホストセキュリティの強化
  - サービスの中継
  - 関連ツール

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**

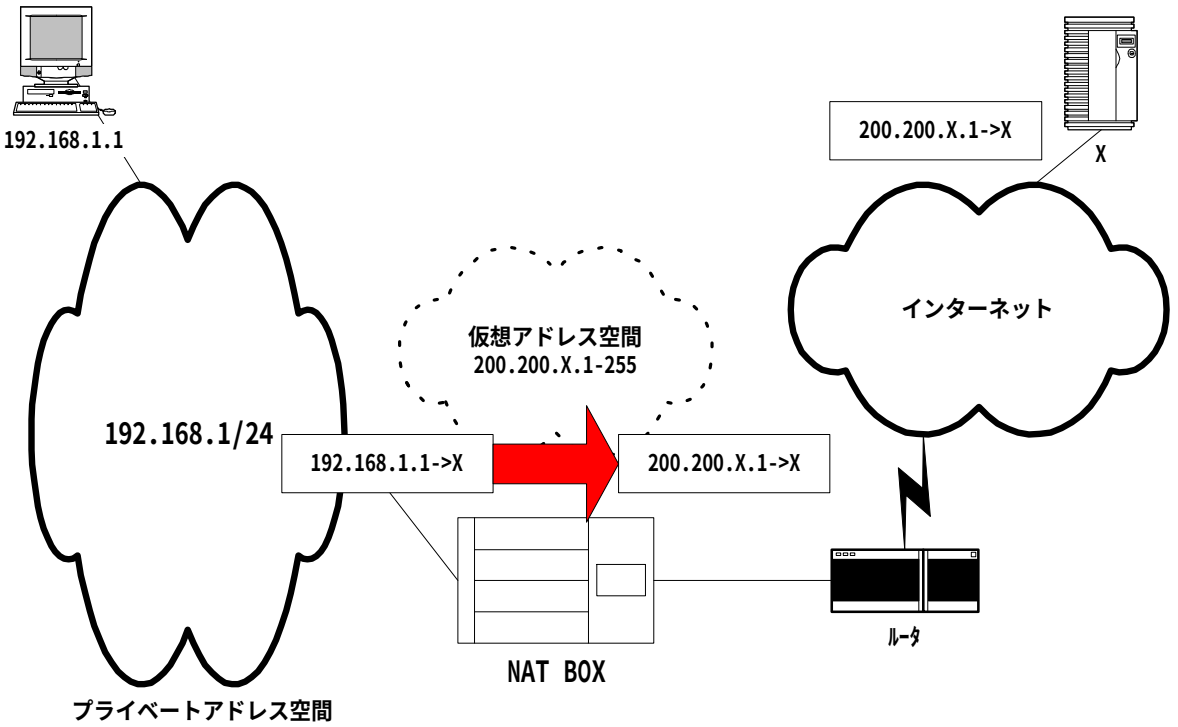
☹通したくないものを通さない

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

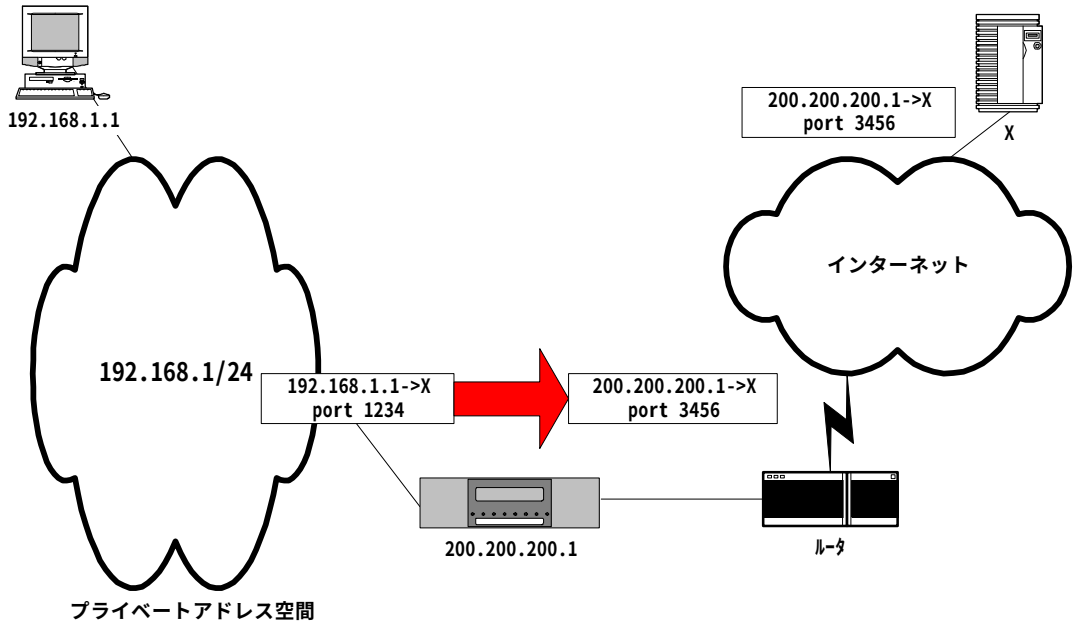
NAT
Network Address Translation

- 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



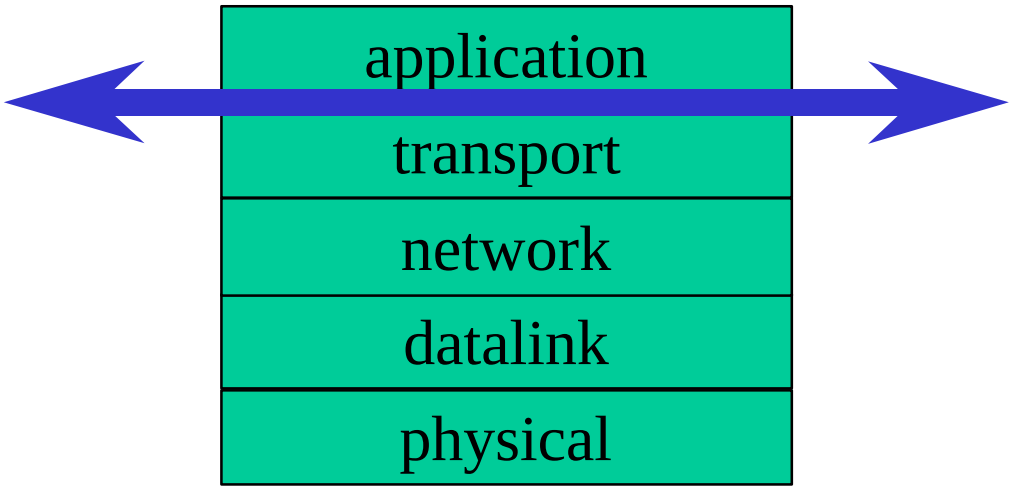
IP masquerade

- IP masquerade の場合には、アドレス変換ルータのアドレスだけを使用する
- ポート番号も変換する



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

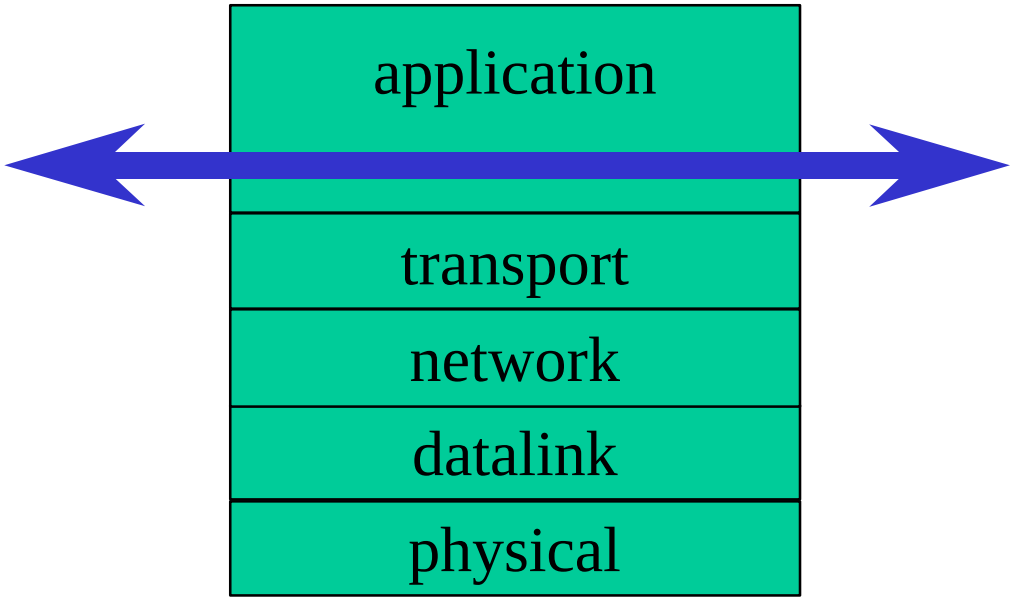


サーキットゲートウェイ

- 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

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

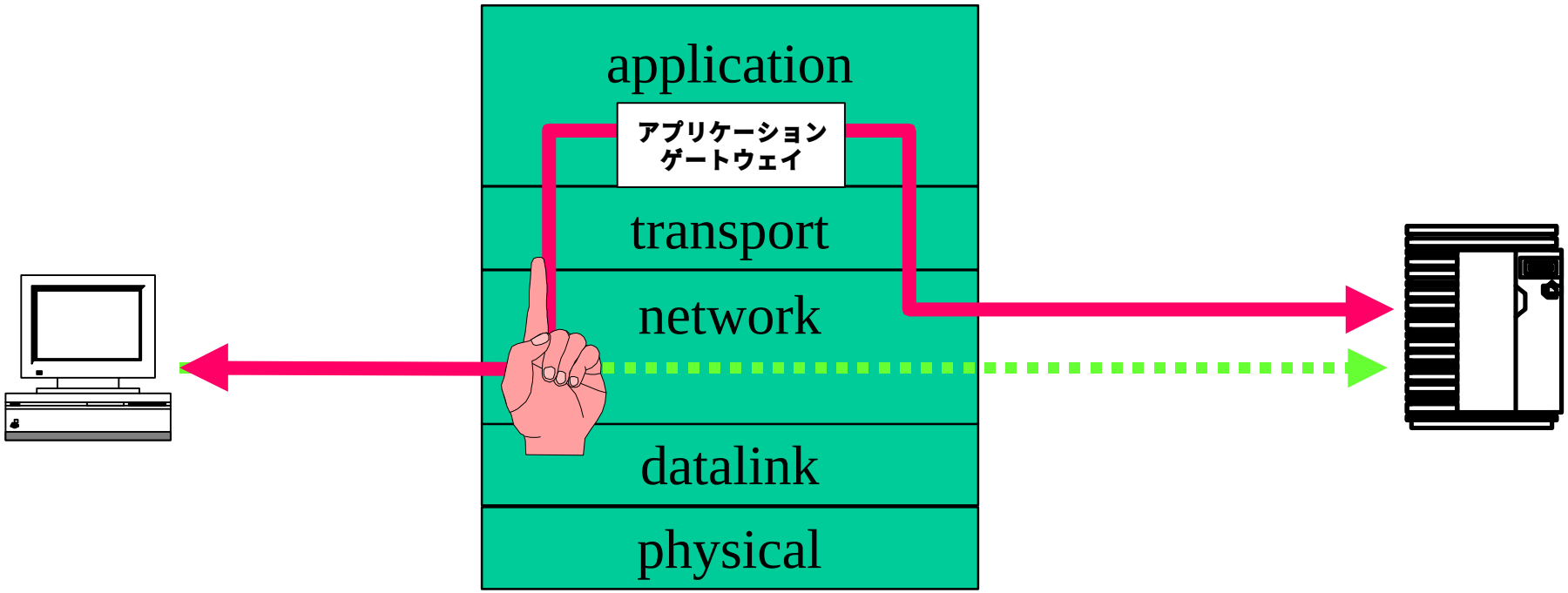


アプリケーション ゲートウェイ

- 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...

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

TIS Firewall Toolkit

- Trusted Information Systems
  - インターネット上でフリーに配布
  - アプリケーションゲートウェイの集合
  - 汎用ライブラリを利用した共通プラットフォーム
  - Unix + socket 環境で動作
- 設計思想
  - バグがあったとしてもシステム自体が重大な被害を受けない
  - 特権モードで動作するプロセスは外部と対話しない
  - サービスは可能なかぎり小規模で、単純であるべきである
  - システムの正当性を検証する手段がなくてはならない

TIS Firewall Toolkit
特徴

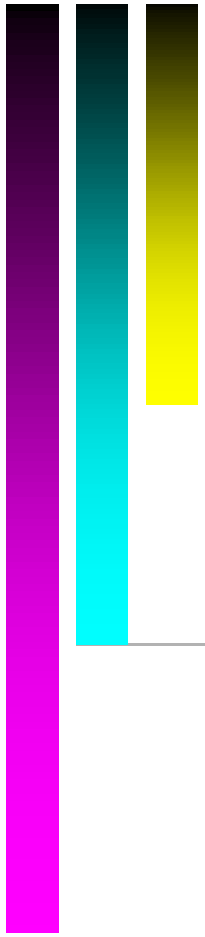
- 共通のアクセス制御ファイル
- 個々のアプリケーションに対応したゲートウェイ
- バックエンド変更可能な認証システム
- 通常のクライアントが使用可能
- 個々のツールは非常に小規模
- ユーザ権限で動作

TIS Firewall Toolkit
特徴 (Cont'd)

- chroot によって、事故が発生した場合の被害を最小限に抑える
- 「許したもの」以外は許さない
- Bastion (要塞) Host によるファイアウォール
  - Dual-Homed ゲートウェイ
  - Screened Host ゲートウェイ
  - Screened Subnet ゲートウェイ

TIS Firewall Toolkit
ゲートウェイツール群

- Smap: SMTP ゲートウェイ
- Netacl - アクセス制御
- Ftp-Gw - ftp 用ゲートウェイ
- Telnet-Gw - telnet 用ゲートウェイ
- Rlogin-Gw - rlogin 用ゲートウェイ
- Plug-Gw - 汎用 TCP ゲートウェイ
- HTTP-Gw - HTTP, Gopher+ ゲートウェイ
- X-Gw: X Window ゲートウェイ



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
Altavista Firewall

- Digital Equipment Corporation
- Unix ワークステーション＋パケットフィルタリング

商用ファイアウォール
FireWall-1

- Checkpoint Software Technologies
  - パケットフィルタリングで不正アクセスを防御
  - GUI による集中管理および監視
  - ユーザに対して透過的環境を提供
  - ネットワークの構成、プロトコル、アプリケーションに柔軟に対応
  - UDP の仮想的な接続をサポート
  - 他のファイアウォールプロダクトと組み合わせて利用可能

商用ファイアウォール
CyberGuard Firewall

- CyberGuard Corporation
- 安全性の高いオペレーティングシステム
  - MVSE: Multiple Virtual Secure Environments

商用ファイアウォール
BorderWare Firewall Server

- Secure Computing Corporation
- All-in-One 的アプローチ
  - インターネットサーバ ＋ ファイアウォール
  - 小規模オフィス向きか

商用ファイアウォール
Gauntlet

- Trusted Information Systems
- Firewall Toolkit ＋ …
  - 付加機能
    - RealAudio, SQL...
  - コンサルティング
  - ドキュメンテーション
  - 管理ツール
  - レポートツール
  - ソフトウェアアップデートサービス

商用ファイアウォール
IIJファイアウォールサービス

- TIS Gauntlet を利用するが、ツールがサービスの中で占める重要度は半分程度
- 残りの半分は
  - コンサルティング、トレーニング
  - インストレーション、サポート
  - アップデートサービス
- レンタル (IP接続の付加サービス)
- PC互換機＋BSD/OS＋Gauntlet＋ α
- 暗号機能の実装

その他のファイアウォールプロダクト

- InterLock (ANS CO+RE Systems, Inc.)
- Eagle (Raptor Systems, Inc.)
- Portus (Livermore Software Laboratories, Inc.)
- Sidewinder (Secure Computing Corporation)
- SunScreen (Sun Microsystems, Inc.)
- etc...

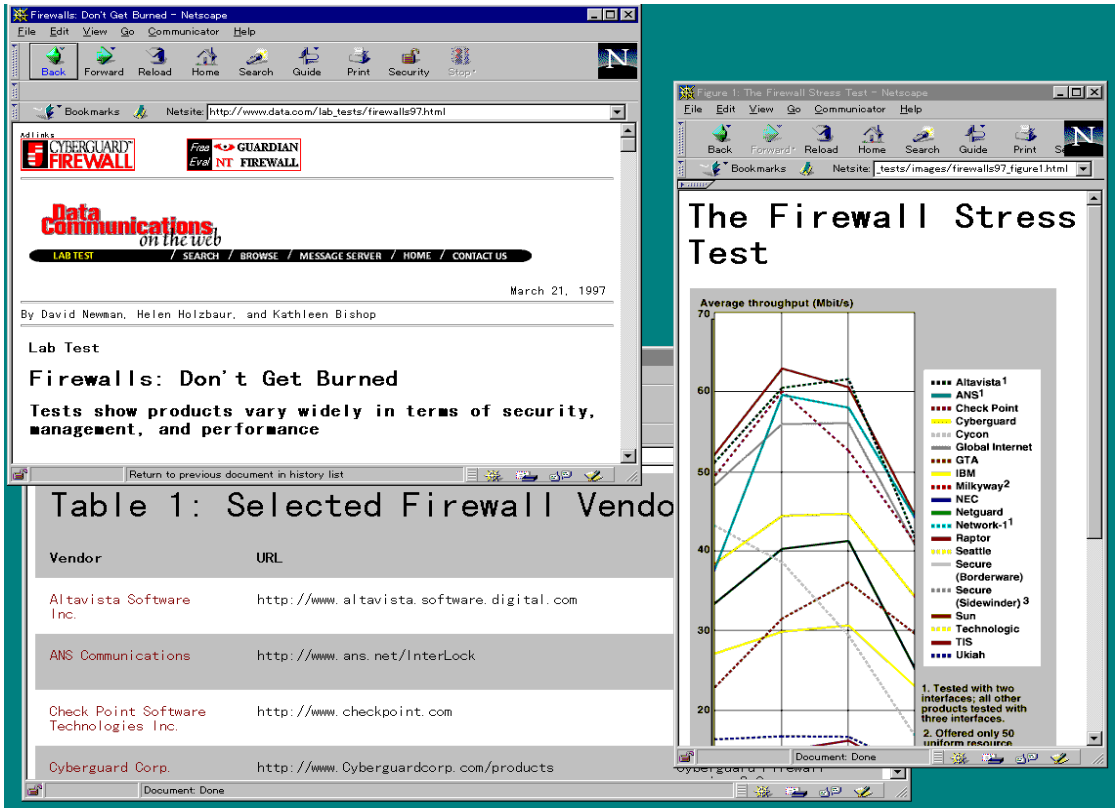
NCSA Firewall Certification Program

- http://www.ncsa.com/fpfs/
- 3COM, ANS Communications, Ascend, Bull S.A., CheckPoint Software Technologies, Inc., Cisco Systems, Cyberguard Corp, Digital Equipment Corporation, Global Technologies Associates, IBM, Internet Device, Isolation Systems Ltd, Livermore Software Laboratories, Milkyway Networks, NetGuard, Network-1, ON Technology Corporation, OpenROUTE Networks, Radguard Ltd., Raptor Systems, Secure Computing Corporation, Sun Microsystems, Technologic Inc., Trusted Information Systems, Ukiah Software, Watchguard Technologies

  (今年の 8月のリストと比べても結構変化がある)

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

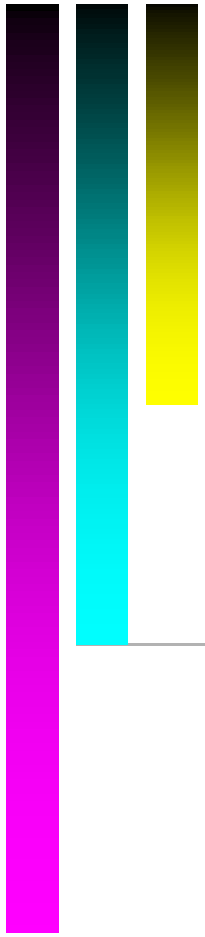
- 必要なアプリケーションは使えるか
- 拡張性はあるか
- 処理能力は十分か
- ソースコードが必要か
- サポート体制は
- 管理のためのコストをいくらかけられるか
- 動作環境
- 費用はいくらかけられるのか

商用プロダクトー何を基準に選ぶか
個人的意見

- 機能は遅かれ早かれ似たようなものになる
  - 機能よりもサポート重視
  - 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
- ブラックボックスは嫌だ
  - オペレーティングシステム
  - アプリケーション
- バグの多いプラットフォームは嫌だ
- どうせベンダーは責任を取ってはくれない
  - 自分で納得できる選択を!

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



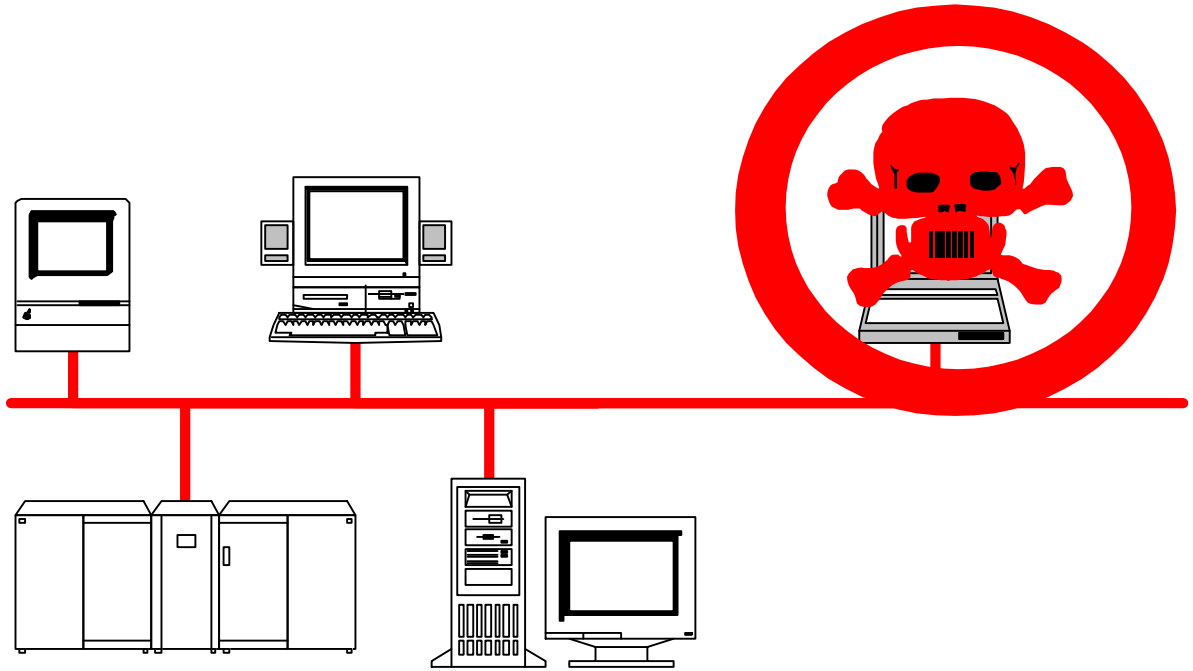
使い捨てパスワード

パスワード盗難の危険性

- 通信回線の盗聴
- 無線LANの盗聴
- プロバイダのホストが侵入されて、盗聴プログラムが仕掛けられる可能性も
- Shoulder Surfing

パスワード盗難の危険性

- Ethernet などのブロードキャスト型のネットワークではデータはすべて丸見え



パスワード盗難の危険性

- 盗聴はインターネット上よりも、ローカルネットワークの方が危険
  - インターネットカフェ
    - 他の客、店員
  - オフィス内
    - 訪問客、侵入者、社外作業スタッフ、社員
  - 校内ネットワーク
    - 学生、その他いろいろ
  - コンファレンスの端末ルーム
    - 他の参加者

使い捨てパスワード

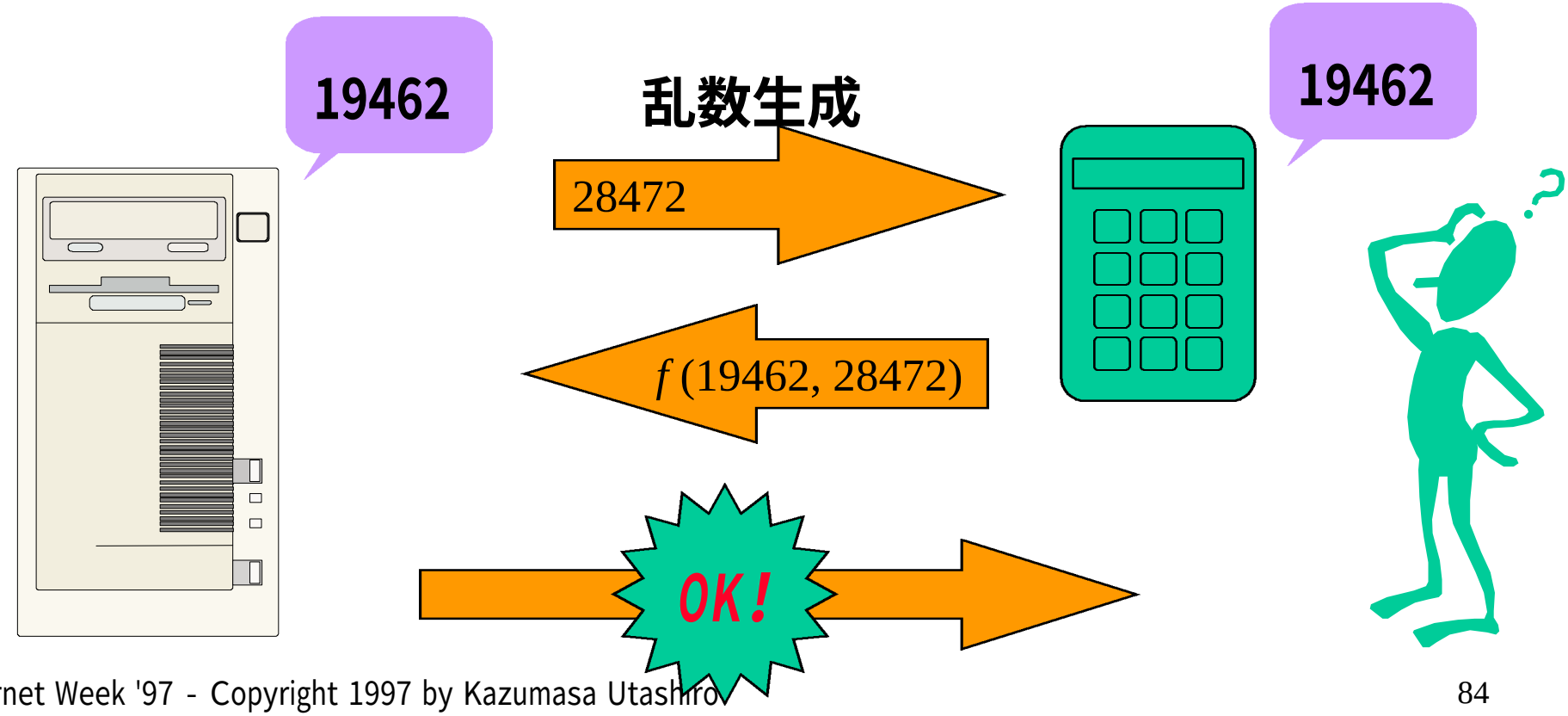
- 毎回異なるパスワードを利用する仕組み
  - one-time password
  - disposable password
  - challenge/response
  - 等と呼ばれる

使い捨てパスワードの方式

- Challenge/Response
  - 非同期式 (Asynchronous)
  - 誰何/応答
  - 合言葉方式
- 同期式 (Synchronous)
  - サーバとクライアントの間で同期が必要
  - カウンタ同期式
- 時刻同期式　(Implicit challenge)

Challenge/Response

■ ホストと端末デバイスの間で秘密の情報を共有



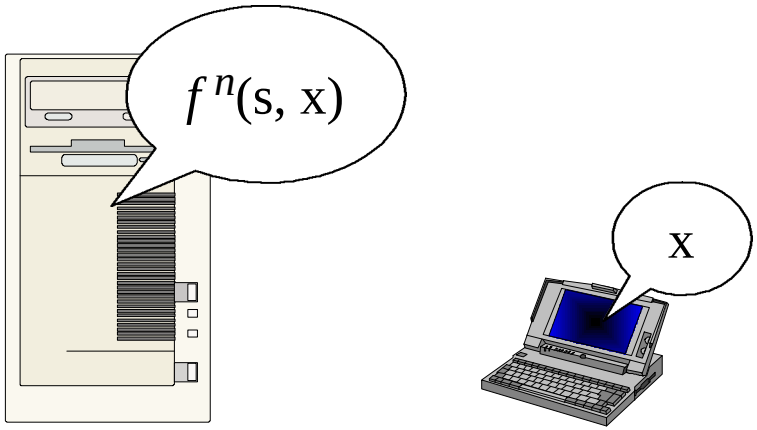
同期式と非同期式の違い

- 両者とも秘密を共有する必要がある
- 同期式
  - 操作が簡単
  - パスワードの系列があらかじめ決まっている
  - パスワード系列を盗難される可能性がある
- 非同期式
  - チャレンジコードを入力しなければならないため、操作が面倒
  - 時刻同期式では入力する必要がないが、乱数性に欠ける

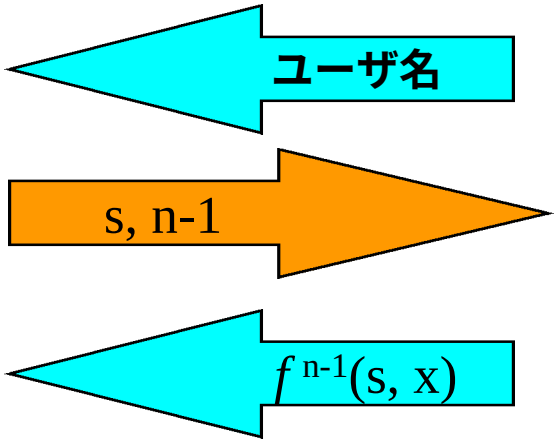
S/Key

- Bell Communication Research で開発
- 目標
  - 盗聴からの保護
  - 使いやすい環境
  - 自動管理
  - 秘密のアルゴリズムに頼らない
  - 秘密のデータに頼らない
- IETF で標準化作業
  - OTP: One-Time Password

S/Key の仕組み



- f : ハッシュ関数 (MD4, MD5 等)
  - $y = f(x)$
  - $y = f(x')$ となる x' を求めるのは困難

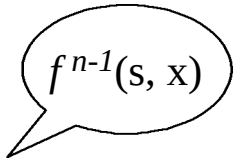


$f(f^{n-1}(s, x)) == f^n(s, x)$?

YES!

- f^n(s, x) **は盗まれても安全**

f^{n-1}(s) **を記憶**

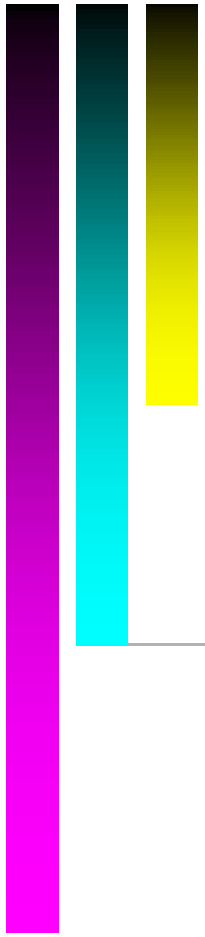


商用使い捨てパスワードの例

- SecureNet Key
  - Challenge/Response
  - DES
- SafeWord
  - Challenge/Response
  - 同期式
  - DES
- SecurID
  - 時刻同期式
  - アルゴリズム非公開

認証デバイスの効用

- 見えないセキュリティを目に見える形に変換できる
- 従来のセキュリティとのアナロジー
  - 誰かに貸してはいけません
  - なくしてはいけません
  - いつも持っていなさい
- 定型的な管理が比較的容易



暗号技術の応用

情報セキュリティの要件

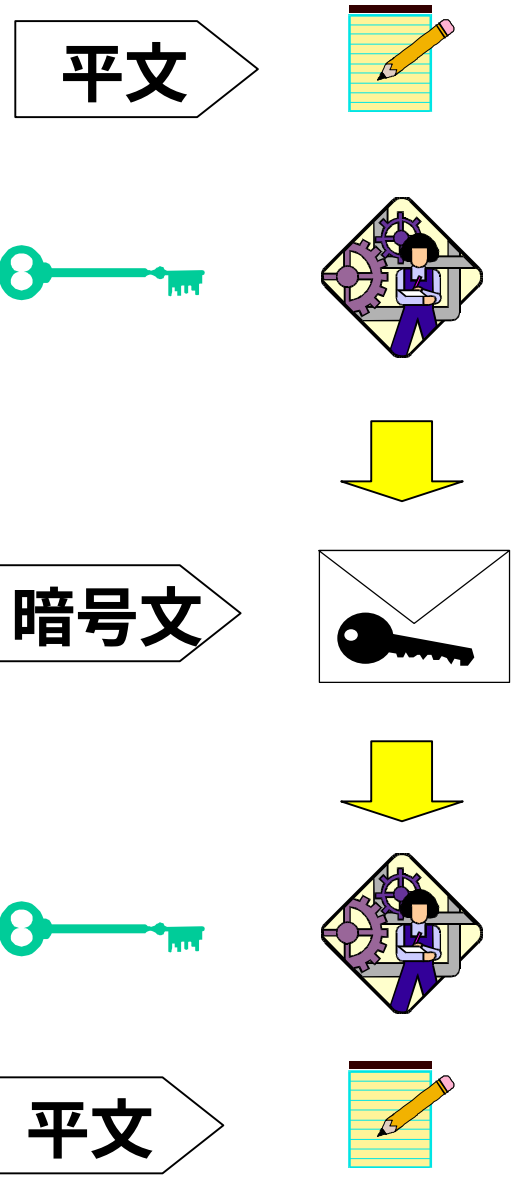
- Confidentiality: 秘匿性
  - 秘密の保持
- Integrity: 完全制
  - 内容の保証
- Authentication: 認証
  - 正しい通信相手を認識できる
- Non repudiation: 否認防止
  - 通信の事実を保証できる

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

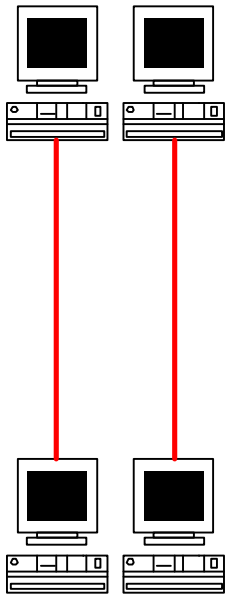
共通鍵暗号

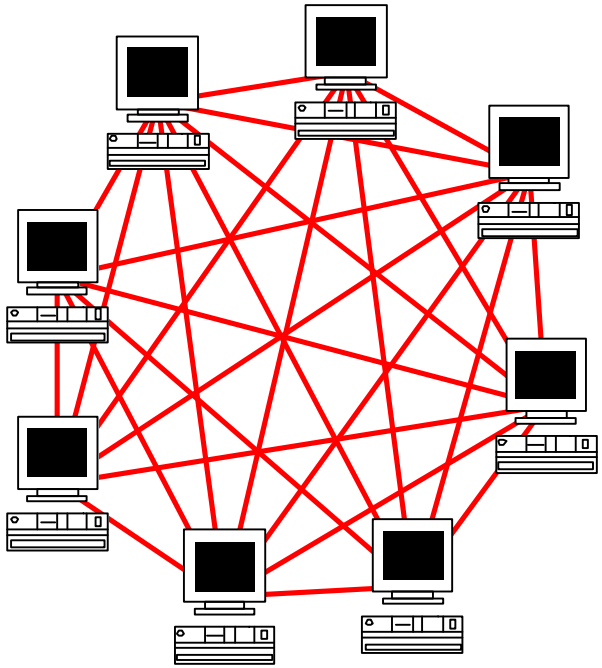
- 暗号鍵と複合鍵が同一
- 両者で共通の秘密情報を共有する
- 高速
- 例
  - DES, FEAL, RC2, RC4, IDEA...



共通鍵暗号

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



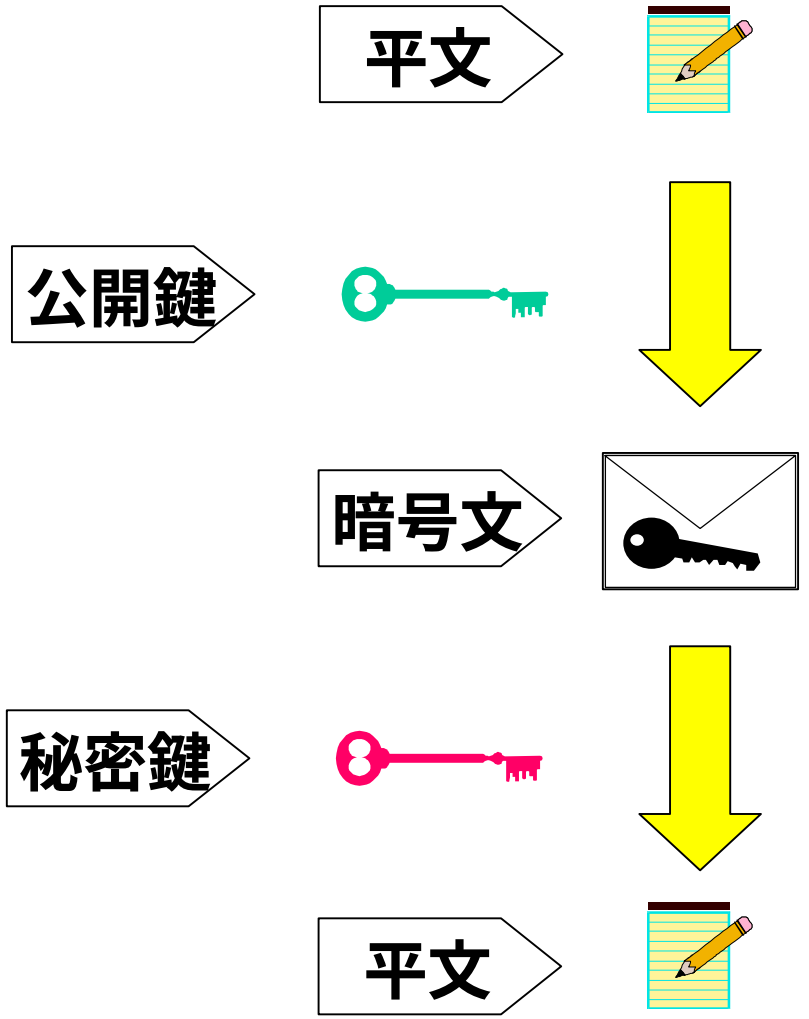


公開鍵暗号の特徴

- 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

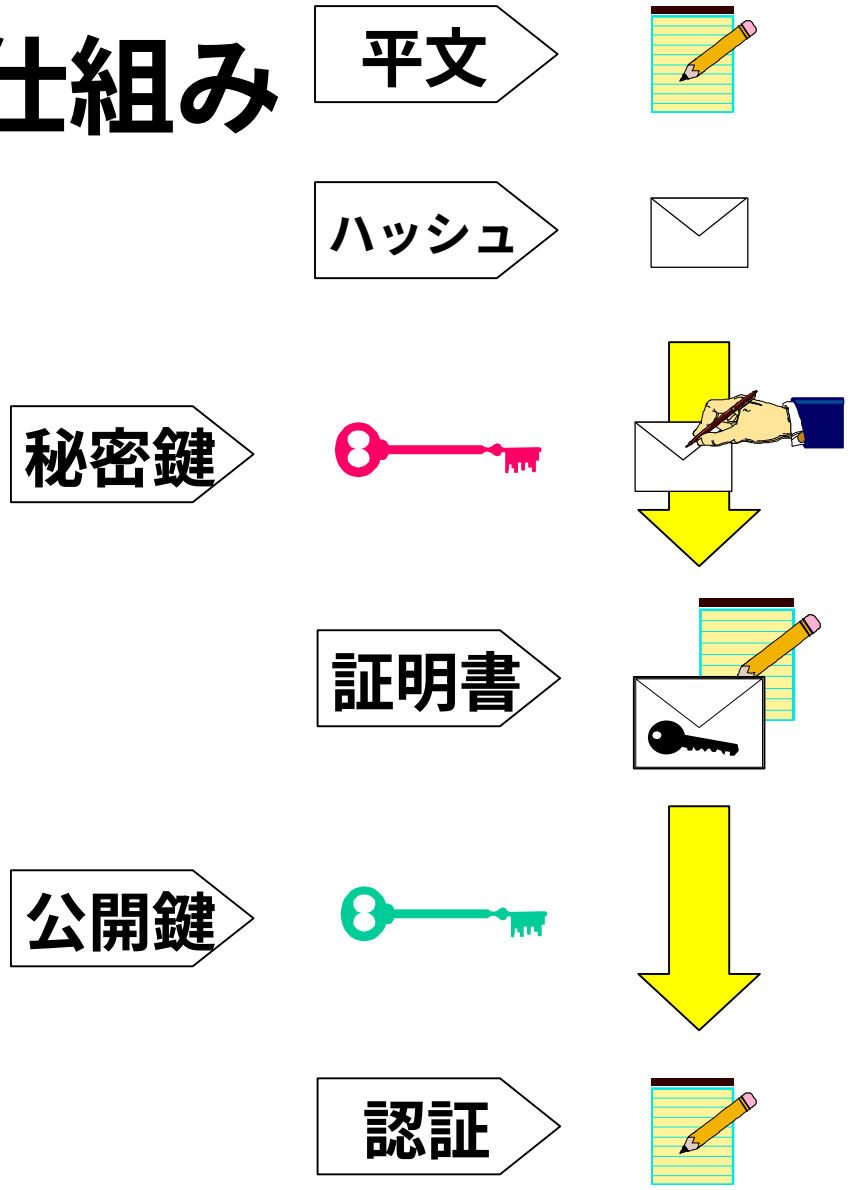
公開鍵暗号の動作

- 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



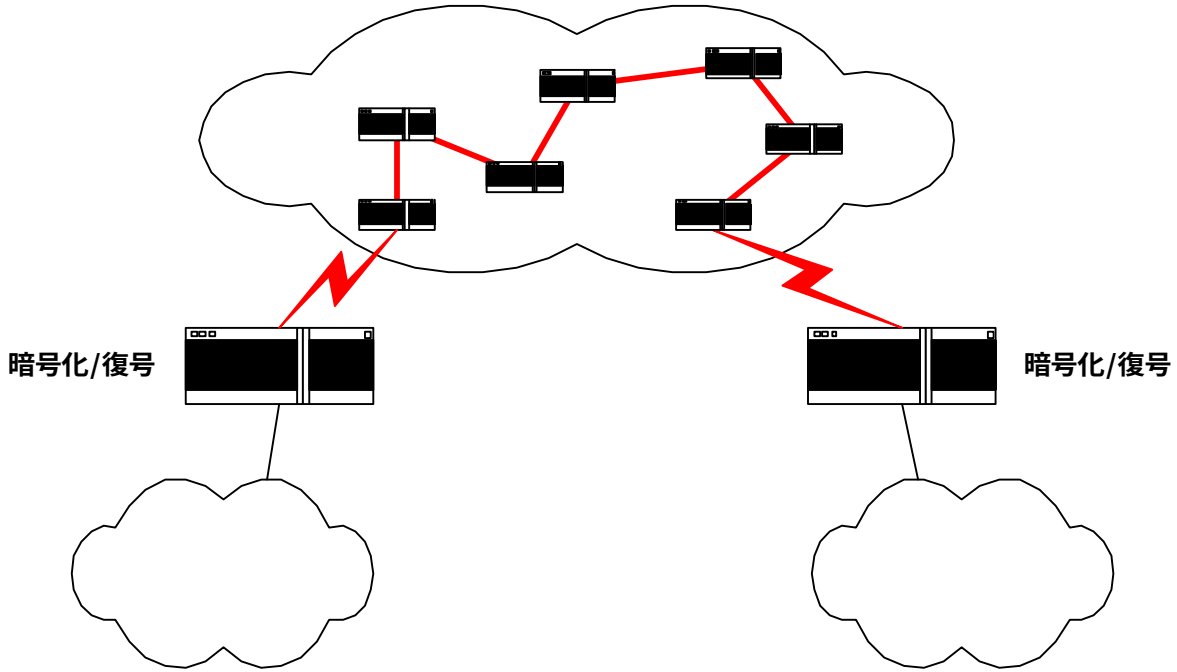
公開鍵による認証の仕組み

- 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



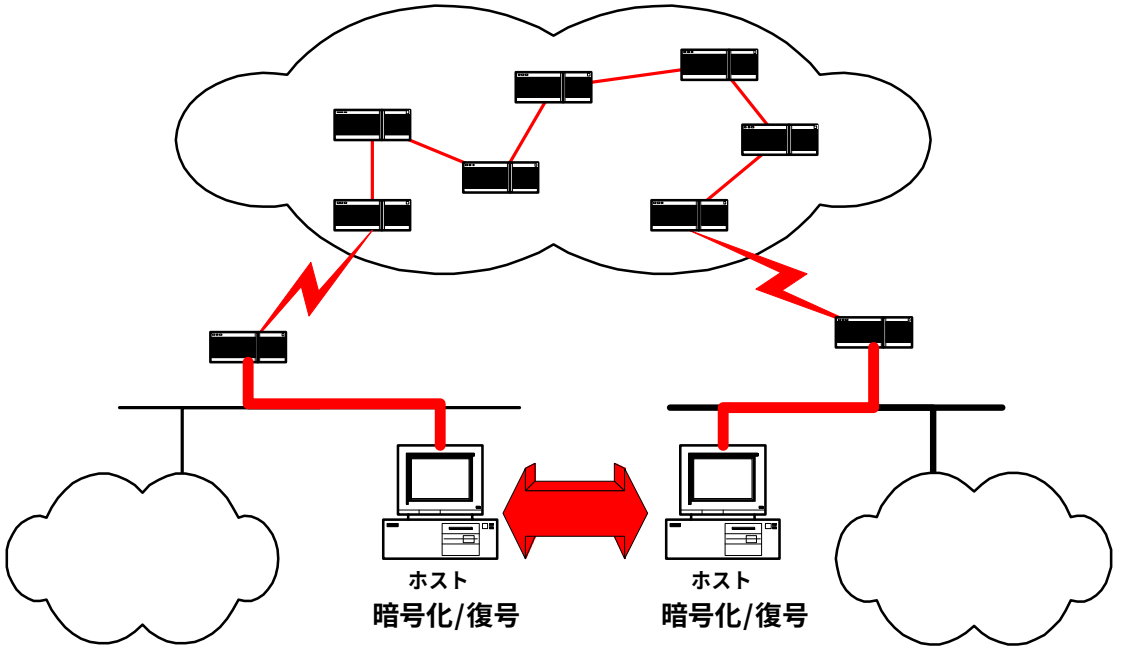
通信経路の暗号化

- 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



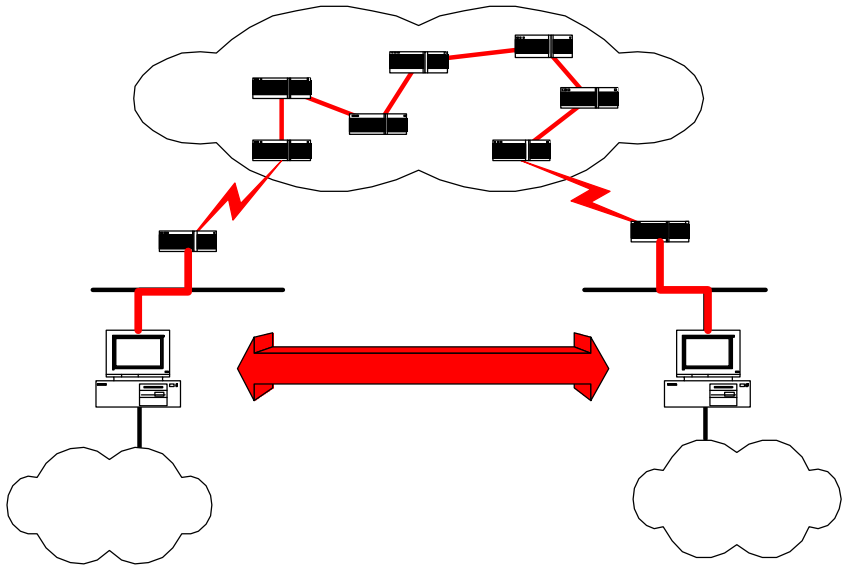
ホスト間の暗号化

- 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



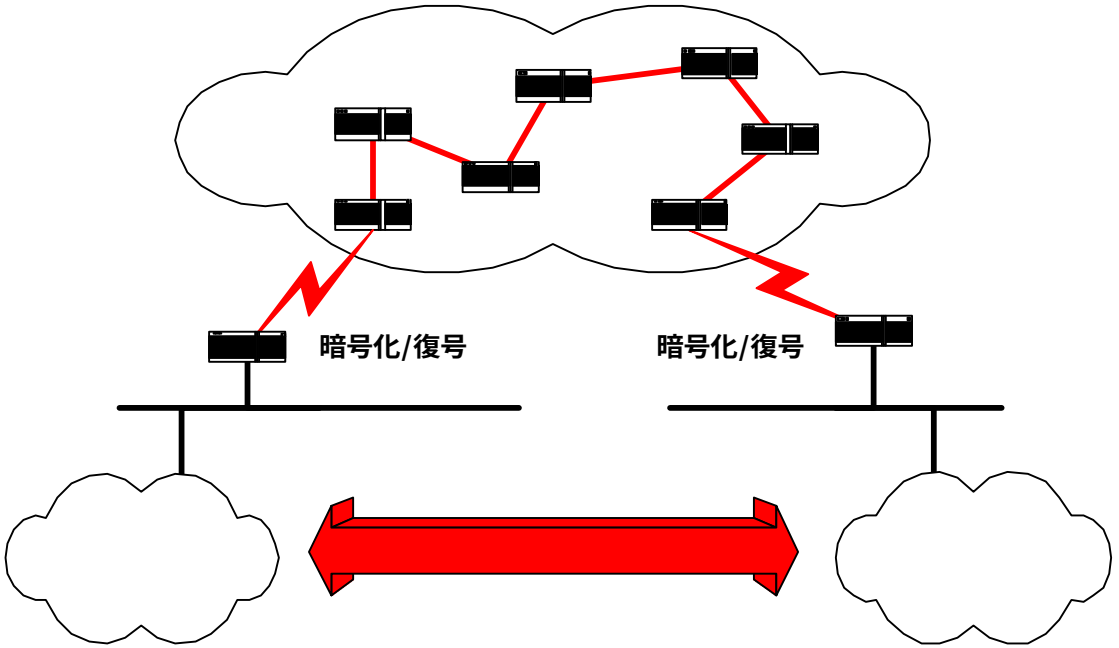
ファイアウォールでの暗号化

- 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

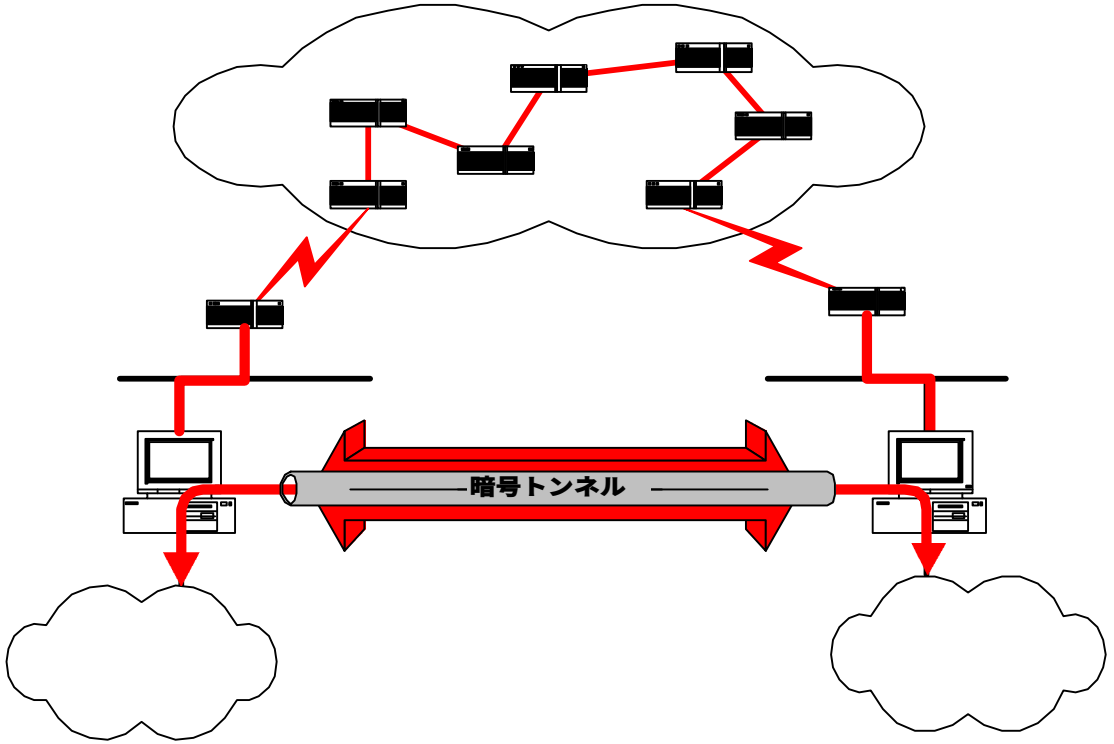


VPN
Virtual Private Network

- 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



アプリケーション層での暗号化
SSH - Secure Shell

- フィンランド・ヘルシンキ大学で開発
- リモートログインプロトコル
- RSA, IDEA, DES
- 多くのプラットフォームで稼動
- Data Fellows 社による商用プロダクト
  - F-Secure シリーズ
- IETF Secure Shell Working Group で標準化

SSH によるアクセス例

```
bbright: {3} % ssh -v bar
SSH Version 1.2.20 [i386-unknown-bsdi3.0], protocol version 1.5.
Standard version.  Does not use RSAREF.
foo: Reading configuration data /etc/ssh_config
foo: ssh_connect: getuid 1029 geteuid 0 anon 0
foo: Connecting to ssh [XXX.XXX.XXX.XXX] port 22.
foo: Allocated local port 1023.
foo: Connection established.
foo: Remote protocol version 1.5, remote software version 1.2.21
foo: Waiting for server public key.
foo: Received server public key (768 bits) and host key (1024 bits).
foo: Host 'bar' is known and matches the host key.
foo: Initializing random; seed file /usr/home/buz/.ssh/random_seed
foo: Encryption type: idea
foo: Sent encrypted session key.
foo: Received encrypted confirmation.
foo: Trying rhosts or /etc/hosts.equiv with RSA host authentication.
foo: Remote: Server has been configured to ignore .shosts.
foo: Remote: Server has been configured to ignore .rhosts.
foo: Remote: Rhosts/hosts.equiv authentication refused: client user 'buz', server user 'buz', client host 'foo'.
foo: Server refused our rhosts authentication or host key.
foo: No agent.
foo: Trying RSA authentication with key 'Kazumasa Utashiro <utashiro@iij.ad.jp>'
foo: Received RSA challenge from server.
Enter passphrase for RSA key 'Kazumasa Utashiro <utashiro@iij.ad.jp>':
foo: Sending response to host key RSA challenge.
foo: Remote: RSA authentication accepted.
foo: RSA authentication accepted by server.
foo: Requesting pty.
foo: Failed to get local xauth data.
foo: Requesting X11 forwarding with authentication spoofing.
foo: Requesting shell.
foo: Entering interactive session.
Last login: Tue Nov 25 02:39:14 1997 from foo

bar %
```

アプリケーション層での暗号化
暗号メール

- PEM, MOSS
  - Historical?
- S/MIME
  - RSA 社が主導
- PGP
  - Pretty Good Privacy
  - written by Philip Zimmermann

アプリケーション層での暗号化
PGP

■ 公開鍵

```
Key for user ID: Kazumasa Utashiro <utashiro@iij.ad.jp>
1024-bit key, key ID 3861D3D1, created 1995/04/17
Also known as: Kazumasa Utashiro <utashiro@wide.ad.jp>
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6.3i

mQCNAi+SS4sAAAEEAMbOKHACUV313TBs4c6hhfenqS58bMWGh7vt9W+C1VAAf5eK
K0IL34FWjG5TGwmllhTVer20Gn5DyDK4sz8OFGHQB55jUMCpStv4jft4FG6pTAox
nM58ERvr9HN5Bn2FSY9llS7ToJJwwEY0da7BaAaTes9dKWQUWuDpOdQ4YdPRAAUR
tCZLYXp1bWFzYSBVdGFzaGlybyA8dXRhc2hpcm9AaWlqLmFkLmpwPokAlQIFEC+S
TNDg6TnUOGHT0QEBUs8D/iEBNlB0ys/DCA7aJ/bM6OTMA3xXH3m0ZsYfA+Jtv8u1
4pKSj7y0bWm0iNCO90j+akRuJruOEK4wZQ4Eg6FdZVEILQ+Iq6j07tTss1x0JwF7
H4YfQcRPG2oeyaW72faU7rOufY9NOccgiz/t0QEf3dYzrXQti5ra0D/wUrZ5rHzw
tCdLYXp1bWFzYSBVdGFzaGlybyA8dXRhc2hpcm9Ad2lkZS5hZC5qcD6JAJUDBRAz
miKX4Ok51Dhh09EBAZ9eA/4urZ/dlPyMemuVmfMpB/wHnq4PyKMO8fRifheCOJd8
bouXjhxJZQAQH1q2yK3RNXDVEU/fgT7/k4tuLq2of61iUHa5j1GfTLTNkEM9FrPW
wT63bJJvcQOYLuB7YqtqZO0GPTbFxeM5Nt55nq+v4433K9Y7eebq9fsst9Zm1a4g
zA==
=Og7A
-----END PGP PUBLIC KEY BLOCK-----
```

■ fingerprint

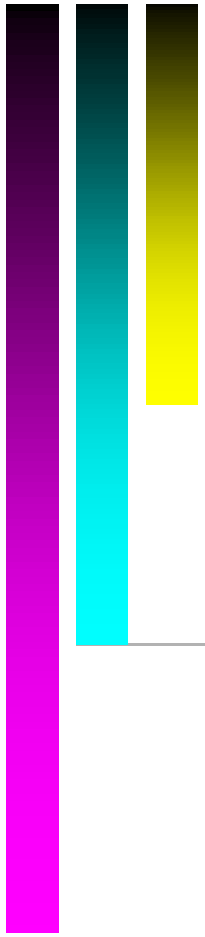
```
6B 8F B8 3A 51 1F 2D A2  A7 EA E6 E7 58 73 71 97
```

トランスポート層での暗号化
SSL - Secure Socket Layer

- Netscape Communications 社による開発
- 汎用のトランスポート層における暗号
- HTTP で広く使われている
- IETF Transport Layer Security Working Group で標準化

トランスポート層での暗号化
SOCKS

- サーキットゲートウェイ
  - アプリケーションプロトコルに依存しないゲートウェイ
- 基本的にアプリケーションの改造が必要
  - 非対応アプリケーションを利用するためのラッパーもある
- Version 5
  - RFC1928, 1929, 1961
  - UDP サポート
  - 暗号、認証機能のサポート
  - http://www.socks.nec.com/



転んだ後のセキュリティ

侵入を受けた時の対応

- 記録
- 証拠の保全
- 関係者への連絡
- 被害状況の把握
- 被害の拡大防止
- 復旧
- 原因の解明

記録

- 人間の記憶は曖昧 (時刻、前後関係、状況...)
- 分単位での記憶は不可能
- とにかくすべての事象を時間情報と共に記録する
  - 何を発見したか
  - 誰に連絡したか
  - 誰から連絡があったか
  - 前後関係はどうだったか
  - 何を行ったか

cf. “An Evening with Berferd” by Cheswick

証拠の保全

- 未加工の情報が重要
  - ディスクの内容を確保
    - 可能なら取り外して書き込み禁止でマウント
    - 失われてしまう情報がある
      - アクセス時刻
      - 消去ファイルの内容
      - 時限トラップの動作
  - ログファイルの保存
  - 未収集データの記録
    - パケットダンプ
    - 詳細なログ情報

ログ情報の種類

- ログイン履歴
  - リモートコマンド等履歴に残らない場合もある
- コマンド履歴
- サーバアクセス履歴
  - Mail (SMTP, POP, IMAP), News, WWW, ftp, RADIUS, Proxy, TCP wrapper, UUCP,
- ホスト管理
  - ARP, DHCP, 経路情報,
- システムメッセージ

関係者への連絡

- 被害を発見したら速やかに関係者に連絡
- タイミングが重要
  - 内容は不十分であってもかまわない
  - 間違いであることを恐れない
  - 新たな情報が入り次第更新

関係者への連絡...

- 管理者が気づかない被害の可能性
  - 利用者、顧客、他の管理者
- 他の組織への被害の拡大を防止
  - 他のホストが同様の被害にあっている可能性
    - 同レベルのホスト―組織内の別のサーバ管理者、他の組織の管理者
  - 踏み台による二次被害の可能性
    - 下流ホスト―組織内の他のサーバホスト、ユーザが利用するホスト、特にホスト認証を行うホストが危険
    - 関係の深い他の組織の管理者

関係者への連絡...

- 攻撃元への通知
  - 一方的な非難は避ける
    - 相手も被害者かも知れない
    - 管理者に罪はない
    - 協力関係が必要
  - 憶測は交えない
  - 客観的データの提供
  - 必要以上の情報は与えないほうが無難
    - 管理者が攻撃している可能性も...
    - 自分の情報を与えたくない場合には IRT による調停を依頼することも有効 (ただし限界はある)

関係者への連絡...

- 緊急対応機関 (IRT: Incident Response Team)
  - 組織内の IRT
  - JPCERT
  - CERT/CC 等海外 IRT (JPCERT 経由も可)
- 司法機関
  - 警察
    - 刑事事件でないと動きにくいので注意

被害状況の把握

- 被害の拡大を防ぐための重要な作業
- 協調作業が重要
- 正確かつ必要十分な情報の収集
  - 情報の根拠を記録
    - 自分で確認したのか、誰かに聞いたのか、憶測が入っているか、証拠となるデータは何か...

被害の拡大防止

- 被害状況に基づいてその拡大防止処置
  - システムの停止
  - 代替機による運用
  - アカウントの消去
  - パスワードの変更
  - ファイルの消去、実行モードの変更
  - 設定ファイルの変更
- 場合によっては処置をせずに様子を見ることが有効な場合もある

復旧

- 気がつかない被害の可能性をなくす
  - バックアップからの復旧
    - バックアップ自体が被害を受けている可能性もあるので注意
  - オペレーティングシステムの再インストール
    - 必要な設定は手作業により復旧

復旧
バックドアの可能性を除去

- 必ず戻って来るためのバックドアを用意する
  - ユーザのパスワードの変更
  - 特定のホストからの認証を抑制
  - 認証プログラムの変更
    - 共有ライブラリを変更することもある
    - チェックサムが偽造されると整合性の検査だけでは不十分
    - カーネルの変更も有り得る
  - 専用プログラムの稼動
    - 特定の時間だけ動くことも
- 再構築以外に絶対的な方法はない

原因の究明

- データを解析して原因の究明を行う
- どれだけ十分なデータが保存されているかが重要
- 何が必要になるかは、必要になってみないとわからない
- できるだけ未加工の生のデータが残っているのが望ましい

原因の究明... 対人関係編

- 多くの場合は人的ミスが原因
  - ミスは必ず起きる。誰がやっても起きる。
  - 起きてしまったことを考えても仕方ない
  - 個人攻撃はしない
  - 知っていることは隠さずに話す
  - **トラブルを楽しむ心の余裕**
    - 深刻になりすぎない
    - 中間管理職的パニック症状の回避
    - 結果オーライ的楽観主義

長期的対策

- 発生した被害による反省を基にして、システムセキュリティの見直しを行い、同様な被害の再発を防ぐ
- 組織内 IRT（プログラム）の編成

JPCERT

- http://www.jpcert.or.jp/
- Info@jpcert.or.jp
  - PGP Key ID
    - ID 1024/2C94D4ED
  - PGP Key fingerprint
    - BA F4 D9 FA B8 FB F0 73 57 EE 3C 2B 13 F0 48 B8

参考資料

資料

- RFC1244, FYI8 Site Security Handbook
- User’s Security Handbook (draft-ietf-ssh-users)
- RFC1281 Guidelines for the Secure Operation of the Internet
- CERT Coordination Center Generic Security Information

資料 (Cont'd)

- インターネットセキュリティガイドライン -インターネットを利用する上での留意事項-
  - 社団法人 日本電子工業振興協会
- コンピュータウイルス対策基準
  - 通産省告示第429号
- コンピュータ・ウイルス等不正プログラム対策指針
  - 警察庁
- 不正アクセス対策基準
  - 通商産業省告示第362号

資料 (Cont'd)

- Common Criteria for Information Technology Security
  - セキュリティ基準の世界標準
  - ISO/SC27/WG3
  - http://csrc.nist.gov/cc/
  - 現在 version 2.0 “beta” が入手可能

通産省

- コンピュータ不正アクセス対策基準
  - 平成 8年 8月 8日
  - 通商産業省告示第 363号
  - http://www.ipa.go.jp/SECURITY/ciadr/crack-gl.txt
- 内容
  - システムユーザ基準
  - システム管理者基準
  - ネットワークサービス事業者基準
  - ハードウェア・ソフトウェア供給者基準

警察庁

- 情報セキュリティ調査報告書 (1997.4)
  - オープンネットワークにおけるセキュリティ上の問題
    - 不正行為
    - 暗号の普及に伴う問題
  - 情報セキュリティ施策の在り方
    - 暗号
    - 法的問題
- セキュリティシステム対策室の設置 (1997.4)
- 情報システム安全対策指針 (1997.9)

郵政省

- 情報通信ネットワーク安全・信頼性基準
  - 昭和62年2月14日付け郵政省告示第73号
- 情報通信ネットワークの安全・信頼性に関する調査研究会
  - 平成9年

メーリングリスト

- firewalls
- fwall-users
- academic-firewalls
- BugTraq
- CERT-Advisory
- risks
- firetalk
- announce@jpcert.or.jp

BUGTRAQ

- セキュリティホール
- クラックツール
- ベンダーパッチ
- IRT レポート
- 解決策
- デマ

- 1850通/年
  - 1996.11-1997.10

玉石混淆

```
Subject:      "LAND" Attack Update
From: Aleph One <aleph1@DFW.NET>
To: BUGTRAQ@NETSPACE.ORG
Date:   Thu, 20 Nov 1997 15:23:29 -0600
Reply-To: Aleph One <aleph1@DFW.NET>
Mime-Version: 1.0
Content-Type: TEXT/PLAIN; charset=US-ASCII
Approved-By: aleph1@UNDERGROUND.ORG
X-UIDL: 76aaca610ad2efc16f23a752343b4f4a

This test where againts the "land" attack. This is _NOT_ about "teardrop".

BSDI 2.1 (vanilla)                      IS  vulnerable
BSDI 2.1 (K210-021,K210-022,K210-024)   NOT vulnerable
BSDI 3.0                                NOT vulnerable
Digital UNIX 4.0                        NOT vulnerable
FreeBSD 2.2.2-RELEASE                   IS  vulnerable
FreeBSD 2.2.5-RELEASE                   IS  vulnerable
FreeBSD 2.2.5-STABLE                    IS  vulnerable
FreeBSD 3.0-CURRENT                     IS  vulnerable
HP-UX 10.20                             IS  vulnerable
IRIX 6.2                                NOT vulnerable
Linux 2.0.30                            NOT vulnerable
Linux 2.0.32                            NOT vulnerable
MacOS 8.0                               IS  vulnerable (TCP/IP stack crashed)
NetBSD 1.2                              IS  vulnerable
NeXTSTEP 3.0                            IS  vulnerable
NeXTSTEp 3.1                            IS  vulnerable
Novell 4.11                             NOT vulnerable
OpenBSD 2.1                             IS  vulnerable
OpenBSD 2.2 (Oct31)                     NOT vulnerable
SCO OpenServer 5.0.4                    NOT vulnerable
Solaris 2.5.1                           IS  vulnerable (conflicting reports)
SunOS 4.1.4                             IS  vulnerable
Windows 95 (vanilla)                    IS  vulnerable
Windows 95 + Winsock 2 + VIPUPD.EXE     IS  vulnerable

Some misc stuff:

Ascend Pipeline 50 rev 5.0Ap13          NOT vulnerable
NCD X Terminals, NCDWare v3.2.1         IS  vulnerable
LaserJet Printer                        NOT vulnerable
...
```

```
int main(int argc,char
{
        struct sockaddr
        struct hostent
        int sock,foo;
        char buffer[40]
        struct ip * iph
        struct tcphdr *
        struct pseudohd

        fprintf(stderr,

        if(argc<3)
        {
                fprintf
                return(
        }

        bzero(&sin,sizeof(struct sockaddr_in));
        sin.sin_family=AF_INET;
```

ニュースグループ

- comp.security.announce
- comp.security.unix
- comp.security.misc
- comp.security.firewalls
- comp.admin.policy
- jp.inet.security.announce
- fj.comp.security
- tnn.internet.firewall

会議

- USENIX
  - Security Symposium
  - System Administration (LISA)
  - Technical Conference
  - System Administration, Networking, and Security Conference (SANS)

会議

- Internet Society
  - Symposium on Network and Distributed System Security
  - INET
- FIRST
  - Computer Security Incident Handling Workshop
- Computer Security Institute
  - NetSec

書籍

- 「インターネット参加の手引き」WIDE プロジェクト編、共立出版
- 「ファイアウォール」Cheswick & Bellovin、ソフトバンク
- 「ファイアウォール構築」、Chapman & Zwicky、オライリー・ジャパン
- 「テイクダウン」下村努 & John Markoff、徳間書店
- 「Network Security」、Kaufman, Perlman & Speciner、Prentice Hall