常時接続時代のセキュリティ

理学部地球科学科地球物理分野
4年　藤本　剛志　(No.22000091)

はじめに

インターネットウィーク2001
(http://www.soi.wide.ad.jp/iw2001/)のビギナーズチュートリアルのテーマ

- インターネットの基礎知識
- 常時接続時代のセキュリティ入門
- ネットワーク構築･運用の基礎
- IPv6入門
- プロトコル詳説～クリックしてからホームページが表示されるまで～

のなかから一つを選び，学習結果をまとめよ．

常時接続時代のセキュリティ入門

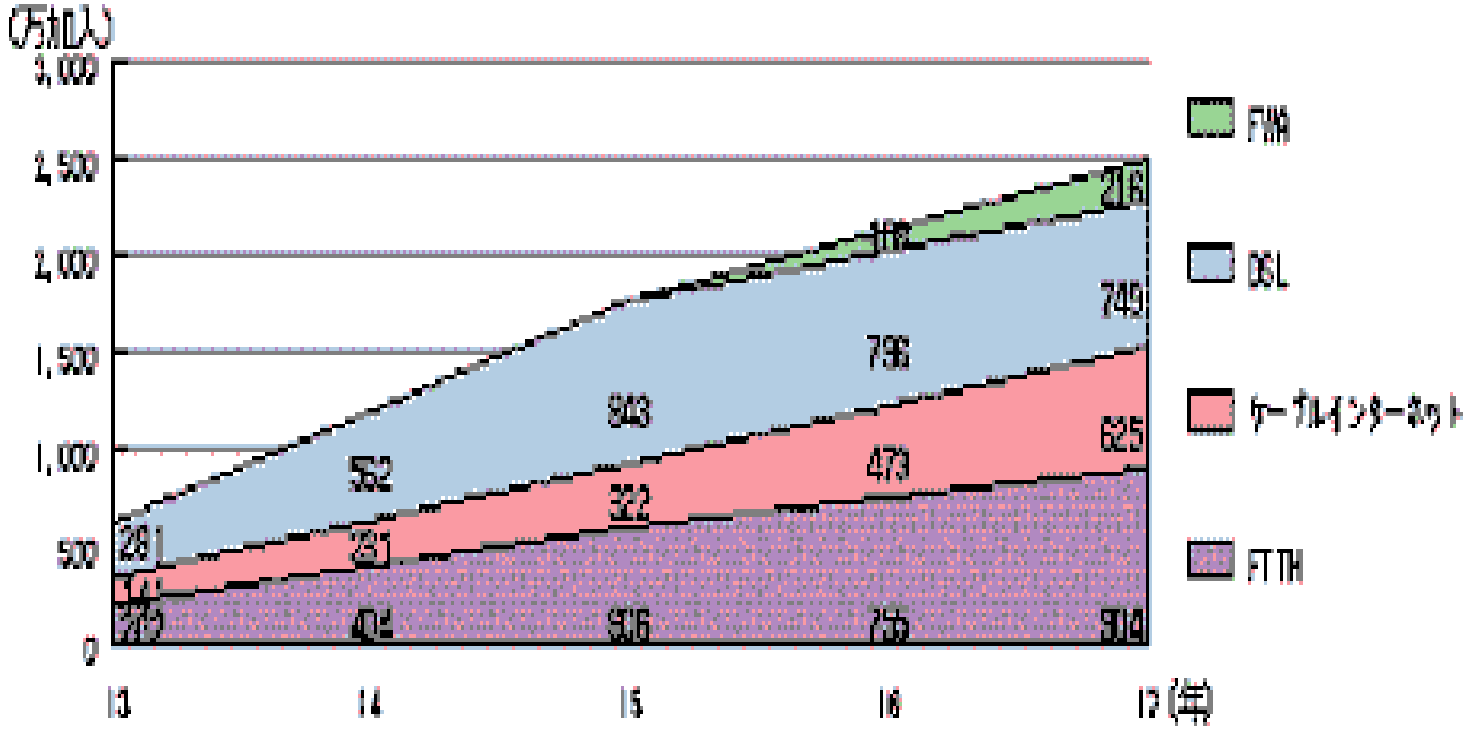
(株)電通国際情報サービス　熊谷誠治 「iw2001，及び2002」

目次

- なぜセキュリティか
  - 常時接続時代に突入
  - 拡大するリスク
- 様々な被害
  - ワームとウイルス
  - 不正アクセス
  - 受動的攻撃
- 対処法
  - 常時接続の実際
  - サーバーの実際
  - 様々なセキュリティ
- 今後の課題

なぜセキュリティか
～常時接続時代に突入～

- 常時接続時代
  - つねにインターネットに接続
  - 利用のたびに接続する必要無し
  - ブロードバンド時代
    - 高速
    - 固定料金
  - e-Japan
    - 3000万世帯で高速インターネット接続
    - 1000万世帯で超高速インターネット接続

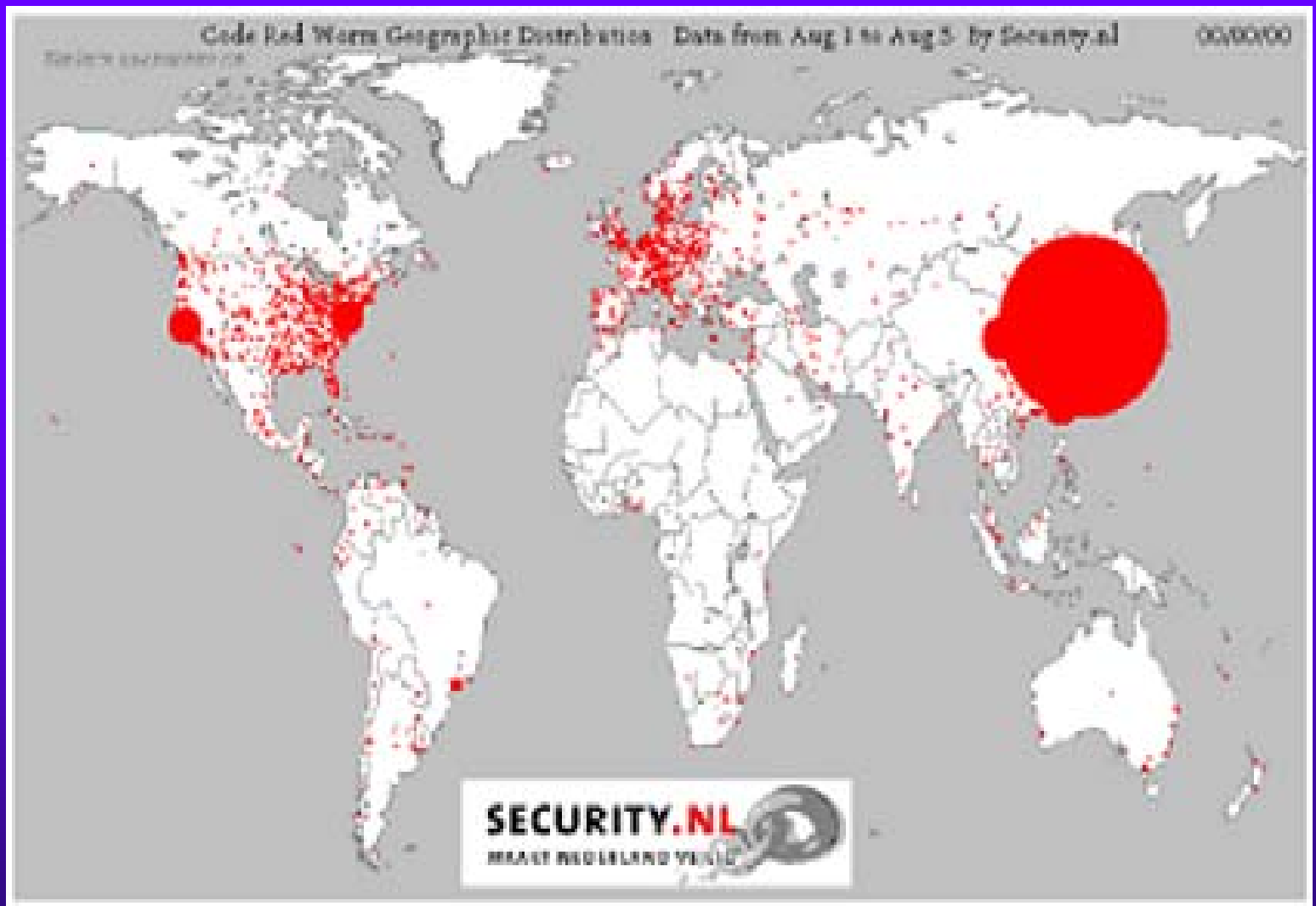


(図1) 2005年までを試算したブロードバンドを導入・利用する世帯数の推移. (平成12年12月「21世紀における情報通信ネットワーク整備に関する懇談会」第2次中間報告による.)

～拡大するリスク～

- 攻撃力の向上
  - 回線速度が100倍
    - 1分間に5回しかできなかった攻撃が500回可能に
  - 1日24時間常時接続
    - 1日1時間接続しているときより24倍の攻撃の機会
- Codered
  - 常時接続がもたらした被害拡大
    - 韓国から世界中に
  - 無差別

だからセキュリティ

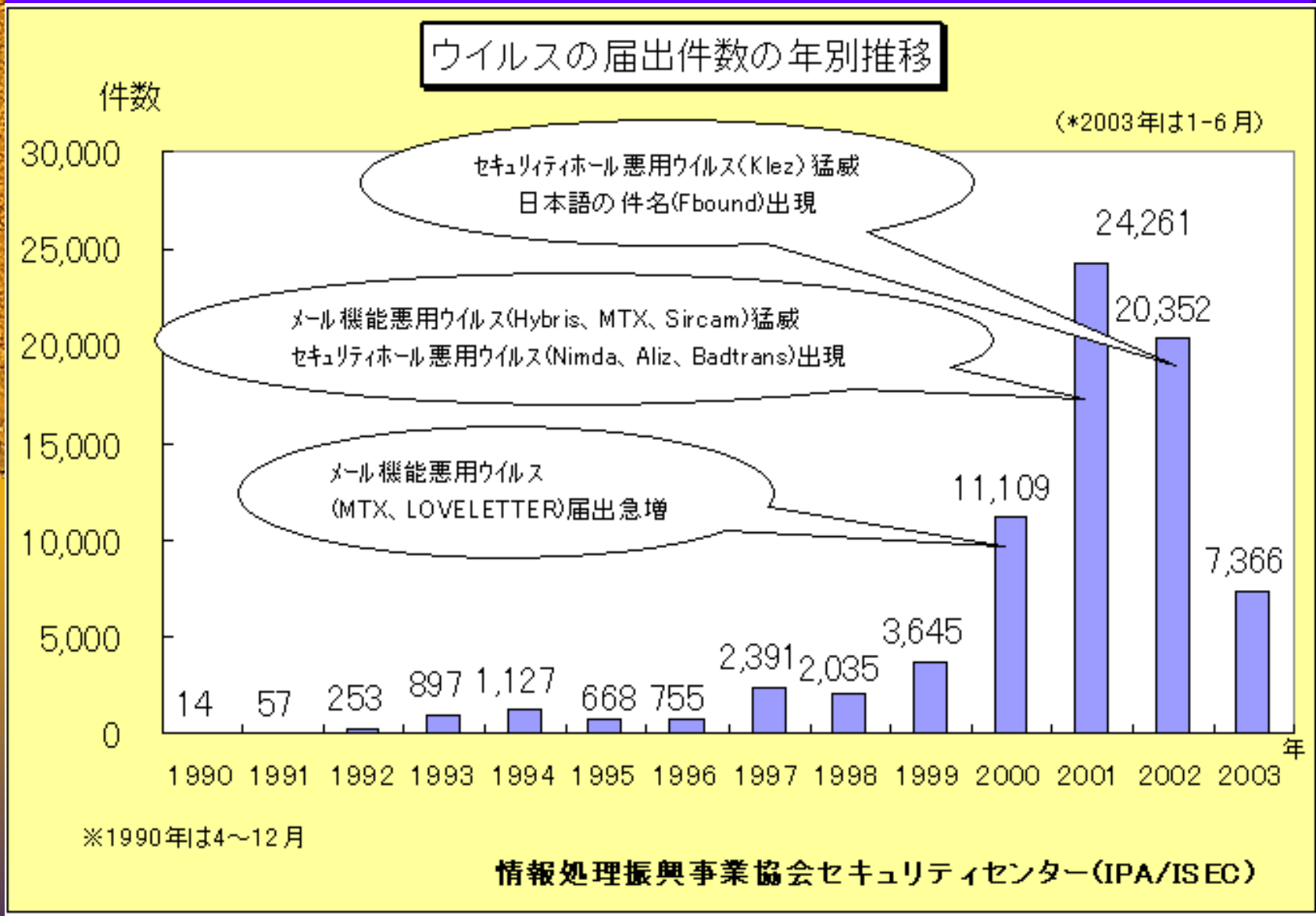


(図2) Coderedの被害状況．赤丸が被害の分布を示す．
(http://www.security.nl/misc/codered-stats/より引用．)

様々な被害
～ワームとウイルス～

- 電子メール、ファイル閲覧などを介して拡大
  - かつてはCD-ROMやフロッピーを介してた
- 凶悪化
  - メールを読む、開くだけで感染
  - 知人から送られてくることも

- LOVE LETTER, Happy99, Codered, Codered2, Nimda, Klez, MSBlaster, など



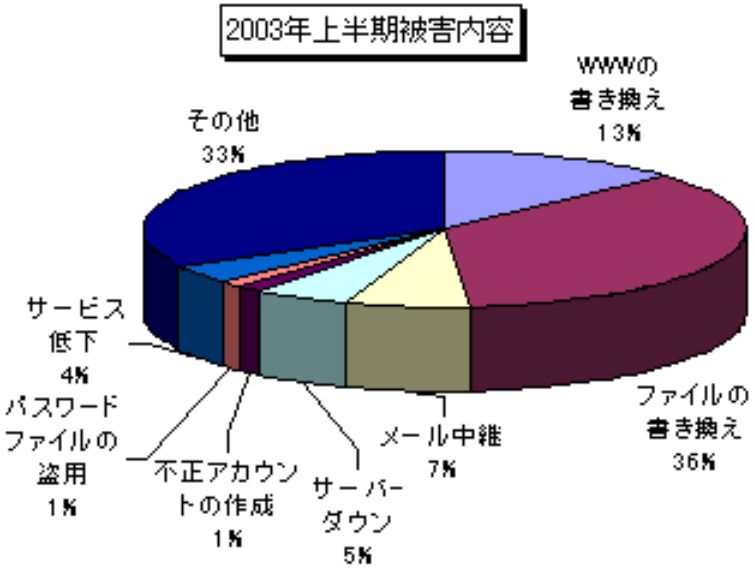
(図3) ウィルスの届出件数の年別推移
(http://www.ipa.go.jp/security/txt/2003/07-1.htmlより引用)

～不正アクセス～

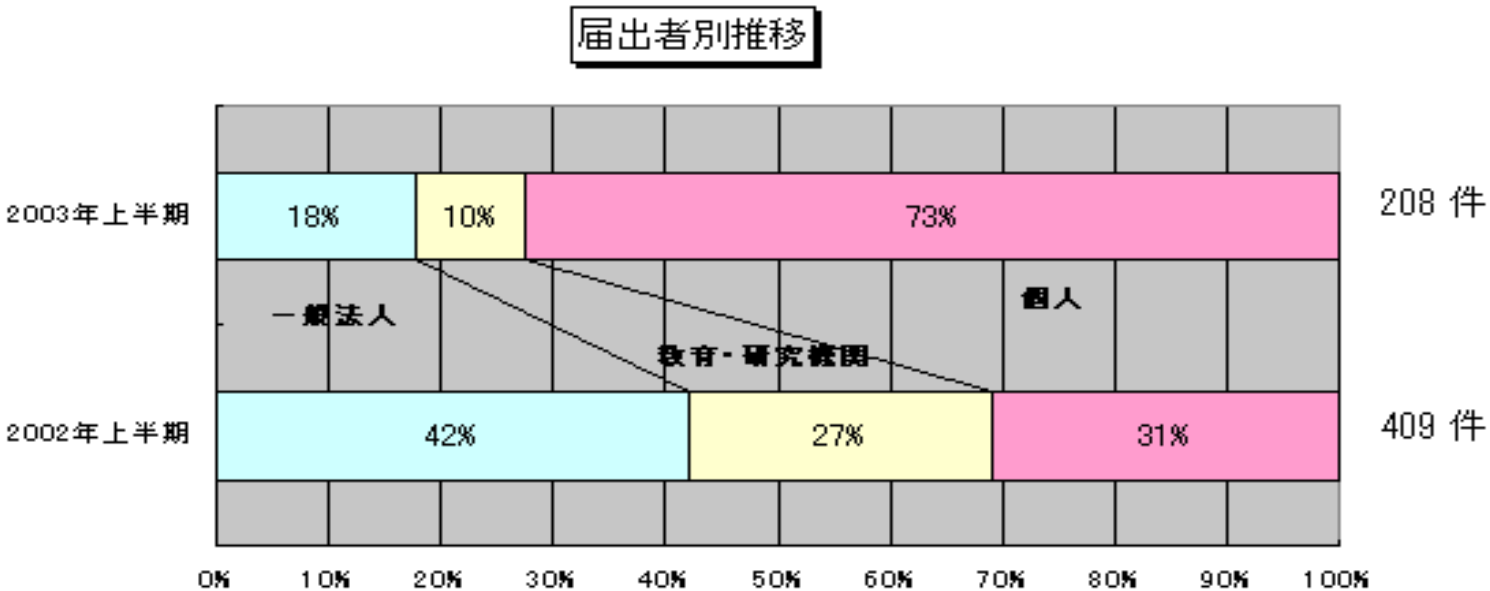
- 一般的な概念

「システムを利用する者が、その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うこと」

- ファイルの改ざん
- 踏み台(被害の拡大、DDoS攻撃)
- サーバーダウン
- 盗聴



届出種別	2003 年 上期	2002 年 上期
WWW の書き換え	10	13
ファイルの書き換え	27	46
メール中継	5	12
サーバーダウン	4	2
不正アカウントの作成	1	9
パスワードファイルの盗用	1	6
サービス低下	3	5
オープンプロキシ	0	0
その他	25	58
合計	76	151



(図4) 2003年上半期の不正アクセス被害内容と2002年上半期との被害者別推移の比較
(http://www.ipa.go.jp/security/crack_report/20030703/03_1st_half.html/から引用)

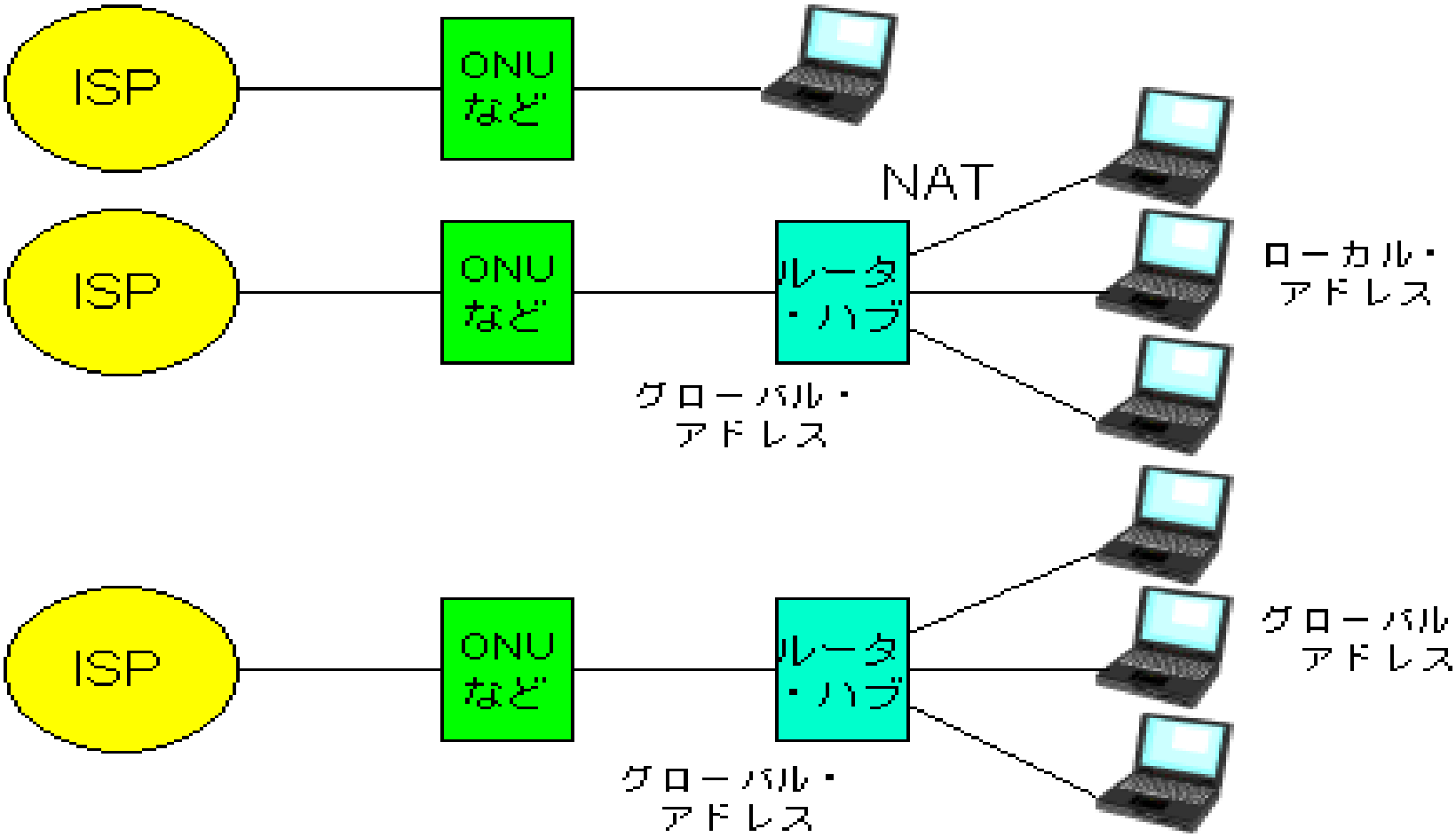
～受動的攻撃～

- 自らが外部をアクセスして被害
  - ファイルのダウンロード
  - Webページを見ただけでも
    - ファイアウォールが機能しない
- 所謂「変なサイト」でなくても危険
  - Webサイトを不正アクセスにより改ざん

今後拡大する被害と予想される。

対処法
～常時接続の実際～

- **接続方法**
  - CATV, DSL, FTTH
    - **ケーブルモデム**、DSL**モデム**、ONU(Optical Network Unit)**に**Ethernet**端子**
      - 128kbps**～**30Mbps, 512kbps**～**50Mbps, 100Mbps**～**
  - FWA
    - **固定無線アクセス**
    - 22GHz, 26GHz, 38GHz**の周波数を使用**
      - **数**Mbps**～数十**Mbps



（図5）常時接続の構成例

NAT・・・一つのグローバルアドレスを複数のローカルアドレスで使う技術

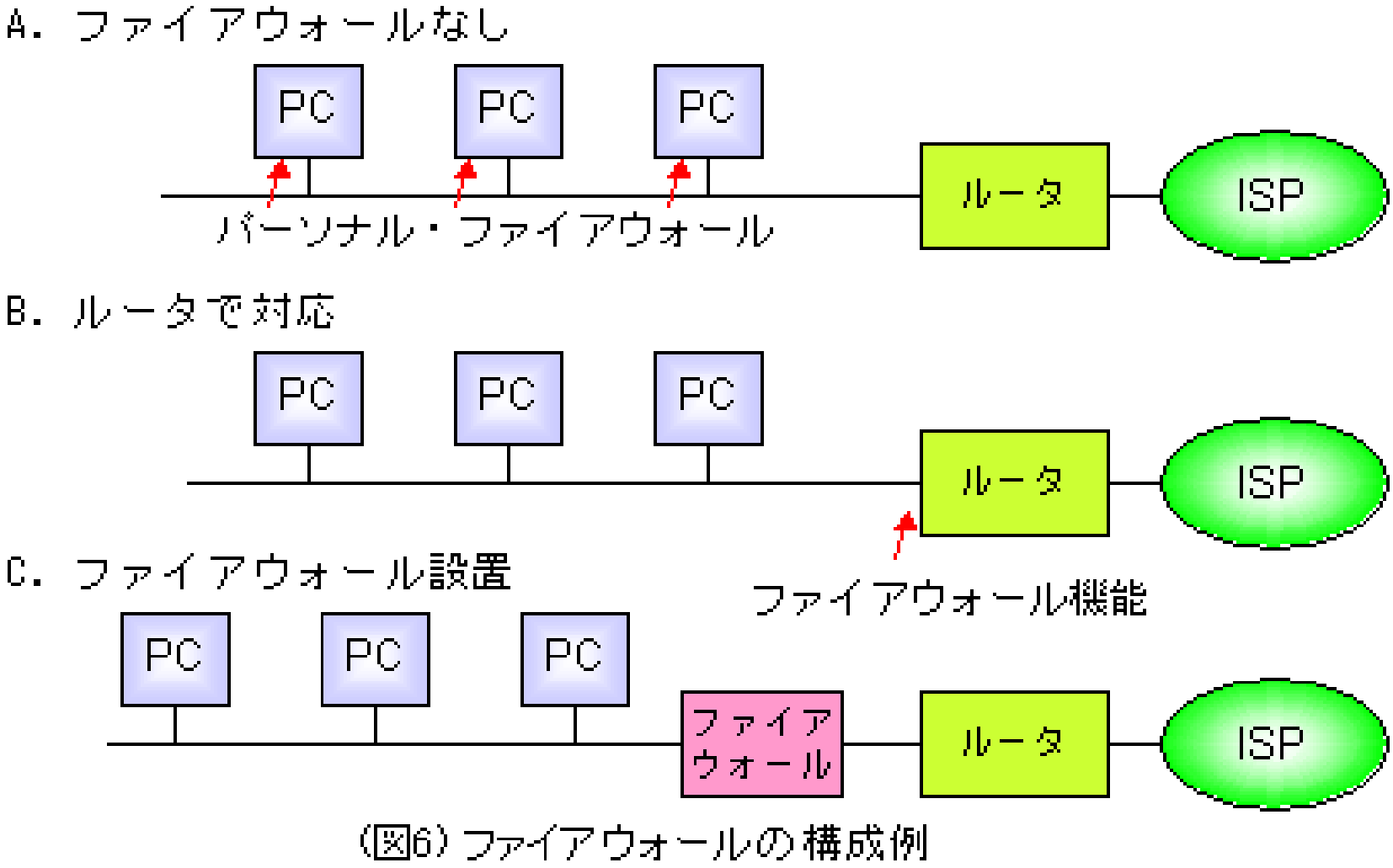
- 集合住宅
  - NATを使用
    - 多数で使用すると個々の性能が落ちてしまう
  - 他人と同じネットワークを使用
    - シェアードハブという、他のポートにも情報が流れ、アクセスも可能な構造をしたハブは注意
  - それぞれが別のネットワークになるような構造をしたVLAN機能付きのハブを使用する

～サーバーの実際～

- 企業だけでなく家庭にもサーバーを
  - 自分のウェブページを自宅で運用
  - 家庭内の情報を外出先から利用
- 攻撃の標的
  - 外からのアクセスを待ち受けている
    - ポートスキャン
    - 不正アクセス
    - 踏み台
- 多くの知識が必要
  - よく分からなければサーバーを立ち上げない

～様々なセキュリティ～
ファイアウォール

- 防火壁
- 外部からの侵入を食い止めるシステム
- そのようなシステムが組み込まれたコンピューター
- 必要な通信のみを通す



(図6) ファイアウォールの構成例

- A,B,Cを組み合わせる
- SPI(Stateful Packet Inspection)

ウイルスチェックソフト

- ウイルスに感染したファイルを検知、修復
- メールに添付されてくるウイルスに有効
  - シェアウェア
    - Trendmicro社のウイルスバスター
    - Symantec社のNorton Antivirus
  - フリーソフト
    - GRISOFT社のAAVG
- 2重3重にソフトを導入

Windows update

- Windowsは弱い？！
  - 狙われやすい
  - いつまでたってもセキュリティホール
    - プログラム規模が大きすぎ
    - セキュリティに対する意識が薄かった
- セキュリティ・パッチを随時更新
- 毎日のようにセキュリティ・パッチ
  - 最近は減った？
- バージョンアップでパッチが元戻り

認証と暗号化

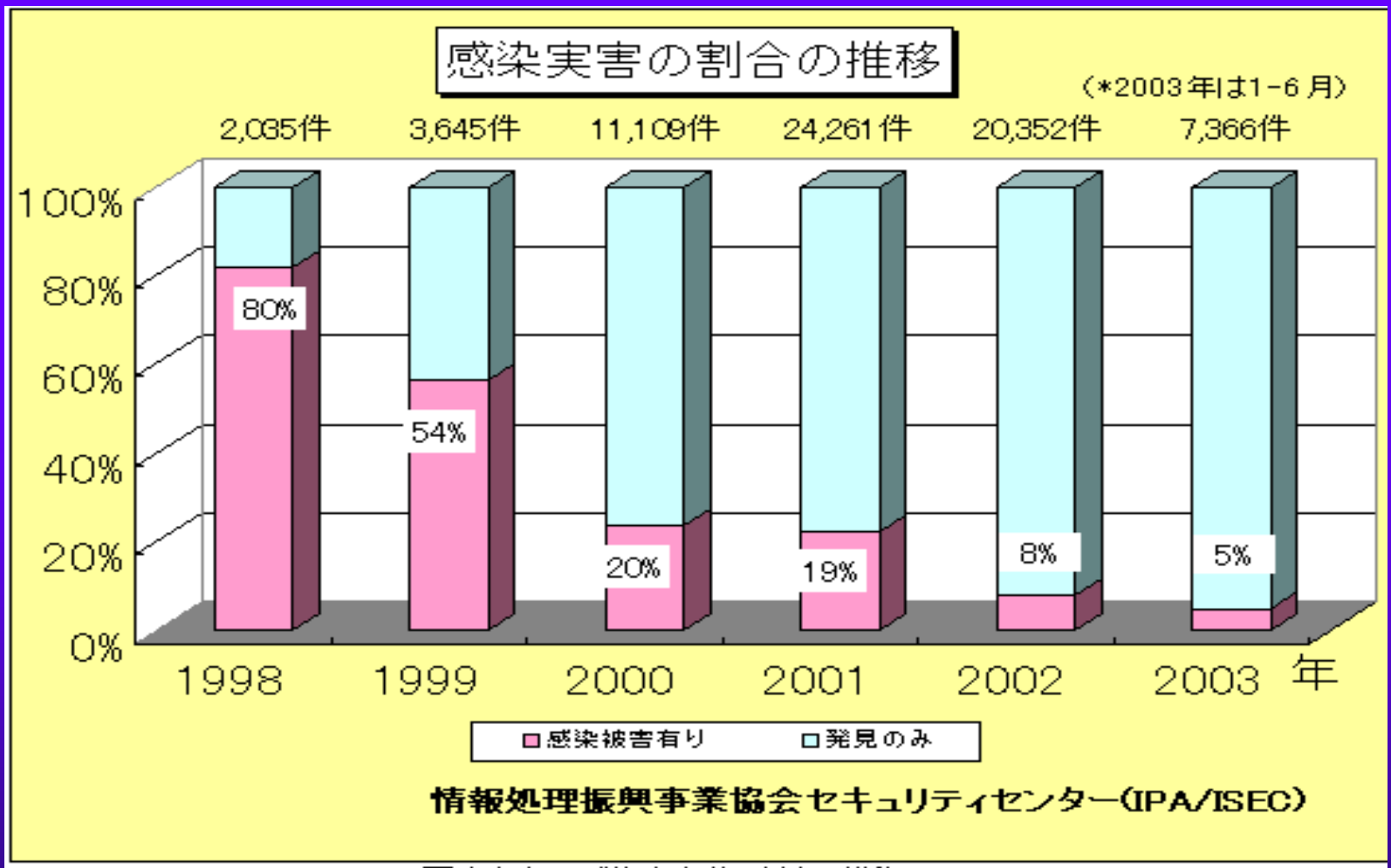
- パスワード
  - 端末からサーバーまでの通信経路を盗聴されたらバレる
- OTP(One Time Password)
  - RSAセキュリティ社のSecurID
    - トークンと呼ばれるワンタイムパスワード生成器がユーザー固有のPIN Numberと時刻の組み合わせからランダムな数字を生成する。これがワンタイムパスワードとなり、1分ごとに変化する。

- SSH(セキュアシェル)
  - TELNETなどのパスワード認証以外のセキュリティ機能の無い通信路の暗号化
- SSL
  - WebブラウザとWebサーバー間での通信内容の暗号化と認証局の署名の入った証明書を使ったサーバーの認証という2つの機能
- 共有鍵暗号
  - 送信者と受信者で同じ鍵を共有
- 公開鍵暗号
  - 送信者に暗号化鍵、受信者は複合化鍵
- 電子署名
  - 文書の作成者を証明し、かつその文書が改ざんされていないことを証明

今後の課題

- 攻撃者の攻撃力の向上
  - ウイルスの凶悪化
  - 不正アクセスなどの巧妙化
  - 受動的攻撃
- 詐欺、プライバシー
  - ネットオークション、ネットショッピング

しかし・・・



(図8) ウイルス感染実害者の割合の推移
(http://www.ipa.go.jp/security/txt/2003/07-1.htmlより引用)

ユーザーのセキュリティ意識の向上

参考資料

- 情報処理振興事業協会セキュリティセンター
  - http://www.ipa.go.jp/security/
- 総務省「ブロードバンド・アクセスの普及」
  - http://www.soumu.go.jp/hakusyo/tsushin/h13/html/D1112000.htm
- SECURITY.nl
  - http://www.security.nl
- 受動的攻撃検証サイト
  - http://zaddik.hp.infoseek.co.jp
- IT用語辞典e-Words
  - http://e-words.jp