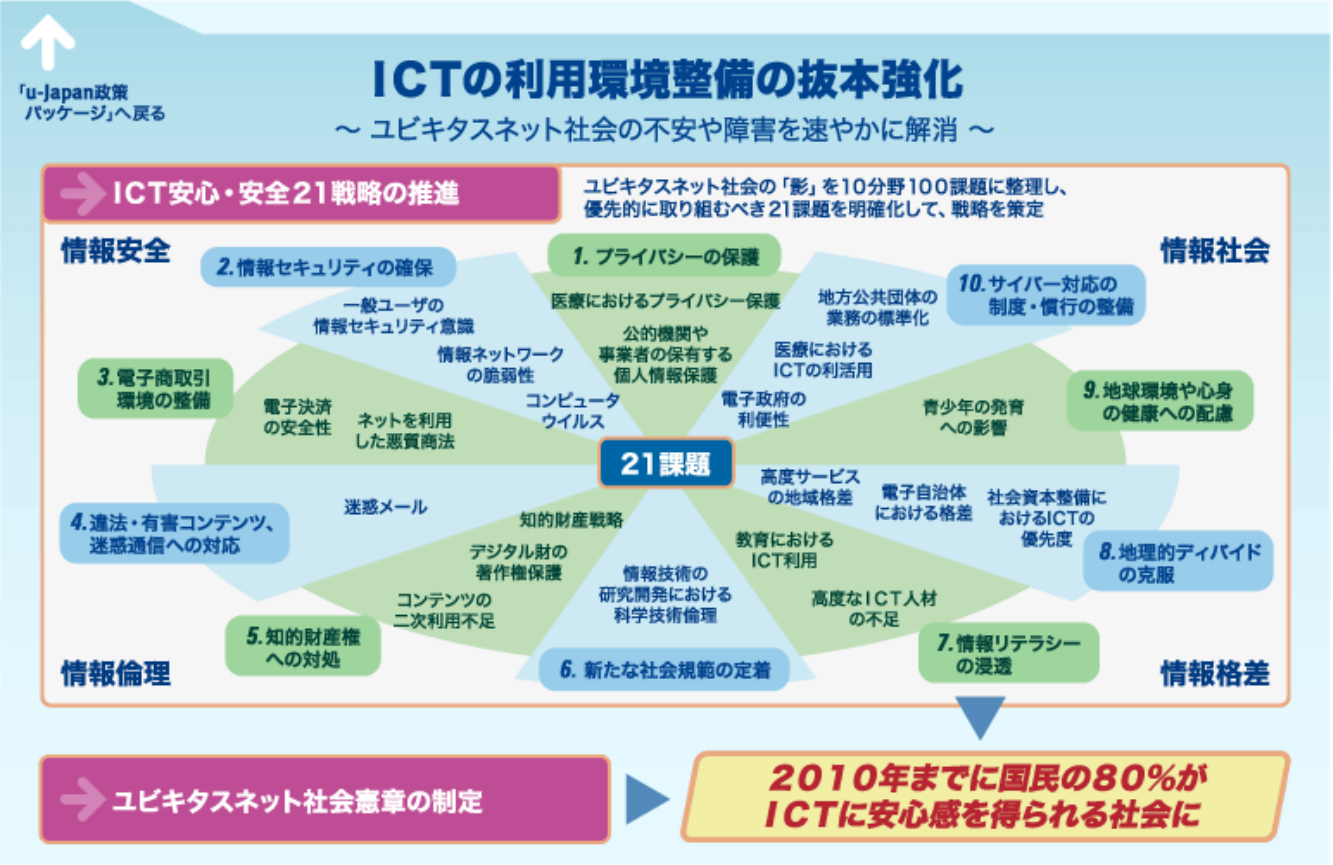
急増する脅威！防げ、不正アクセス！

山田正雄ゼミナール
2008年　法桜祭　学生フォーラム
中村　研人　　土田　郷
中川　貴文　　齋藤　徹

目次

1. はじめに
① 参考資料(ICT利用環境整備の抜本強化)



出展:総務省HP　政策ズームアップ　u-Japan政策より

1. はじめに
② 研究の目的

- 不正アクセスは、様々なコンピュータ犯罪の準備行動として行われる。
- その不正アクセスは急増している。
- では、実態はどうなっているのか？
- そして、どうすれば減らすことができるのか？

2.1 不正アクセスとは

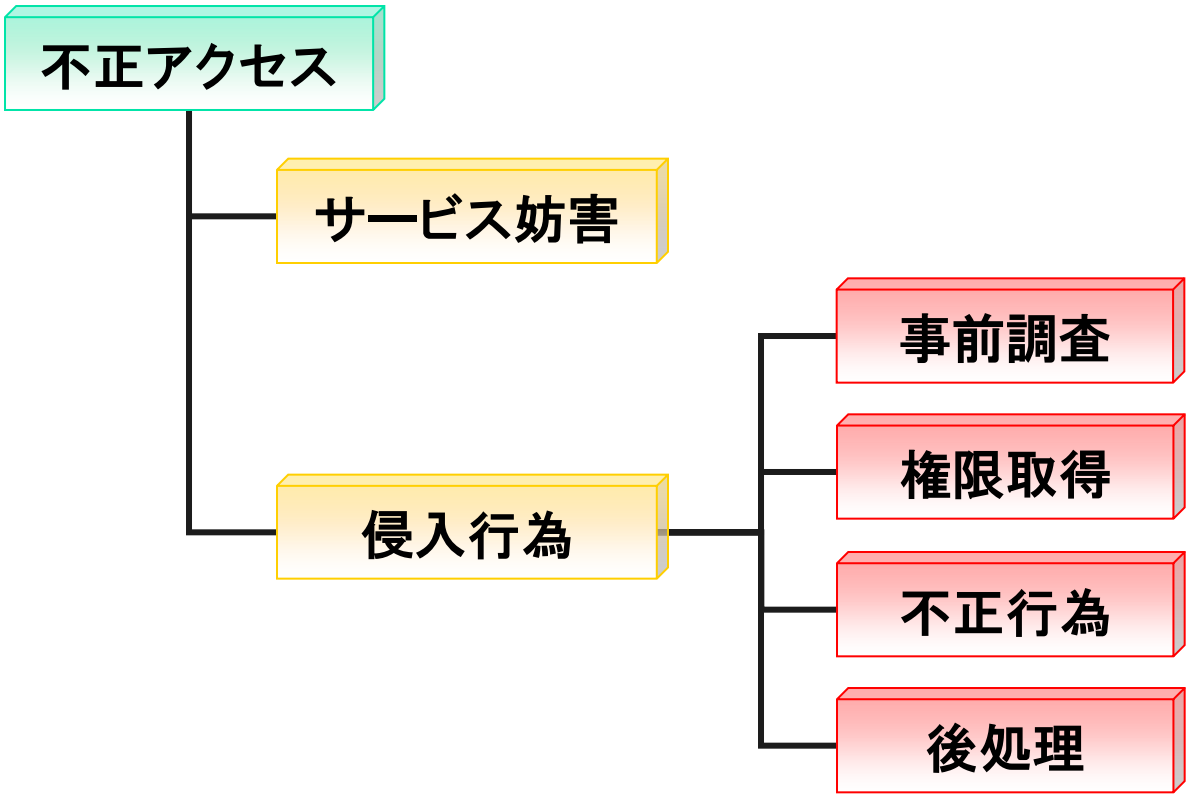
アクセスが制限されている、または許可されていないコンピュータまたはネットワークに接続すること。

1. 他人のIDやパスワードを勝手に使って、システムを利用する行為。(識別符号窃用型)

2. セキュリティ・ホールなどを利用し、通常のアクセス制限を回避するような操作を行い、システムを利用する行為。(セキュリティ・ホール攻撃型)

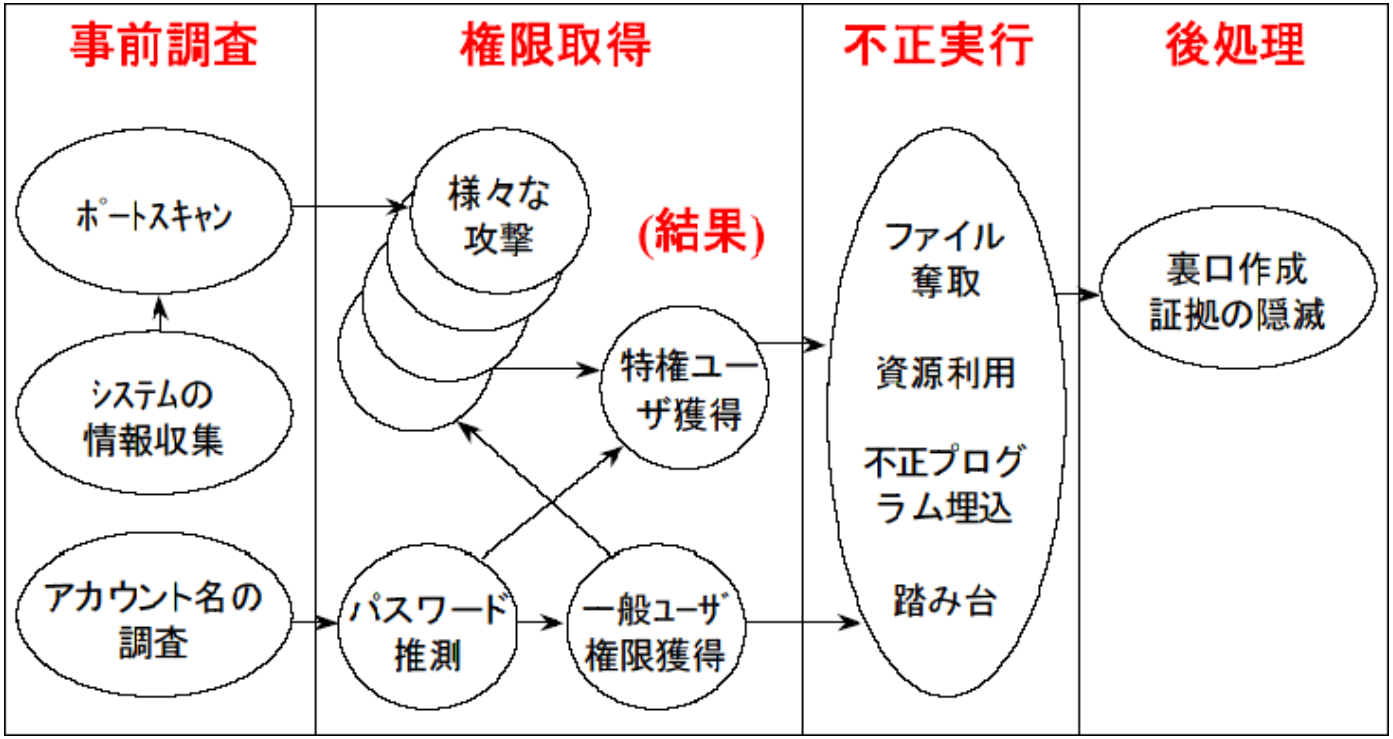
不正アクセス行為の禁止等に関する法律　第三条より

2.2 類型
① 被害別類型



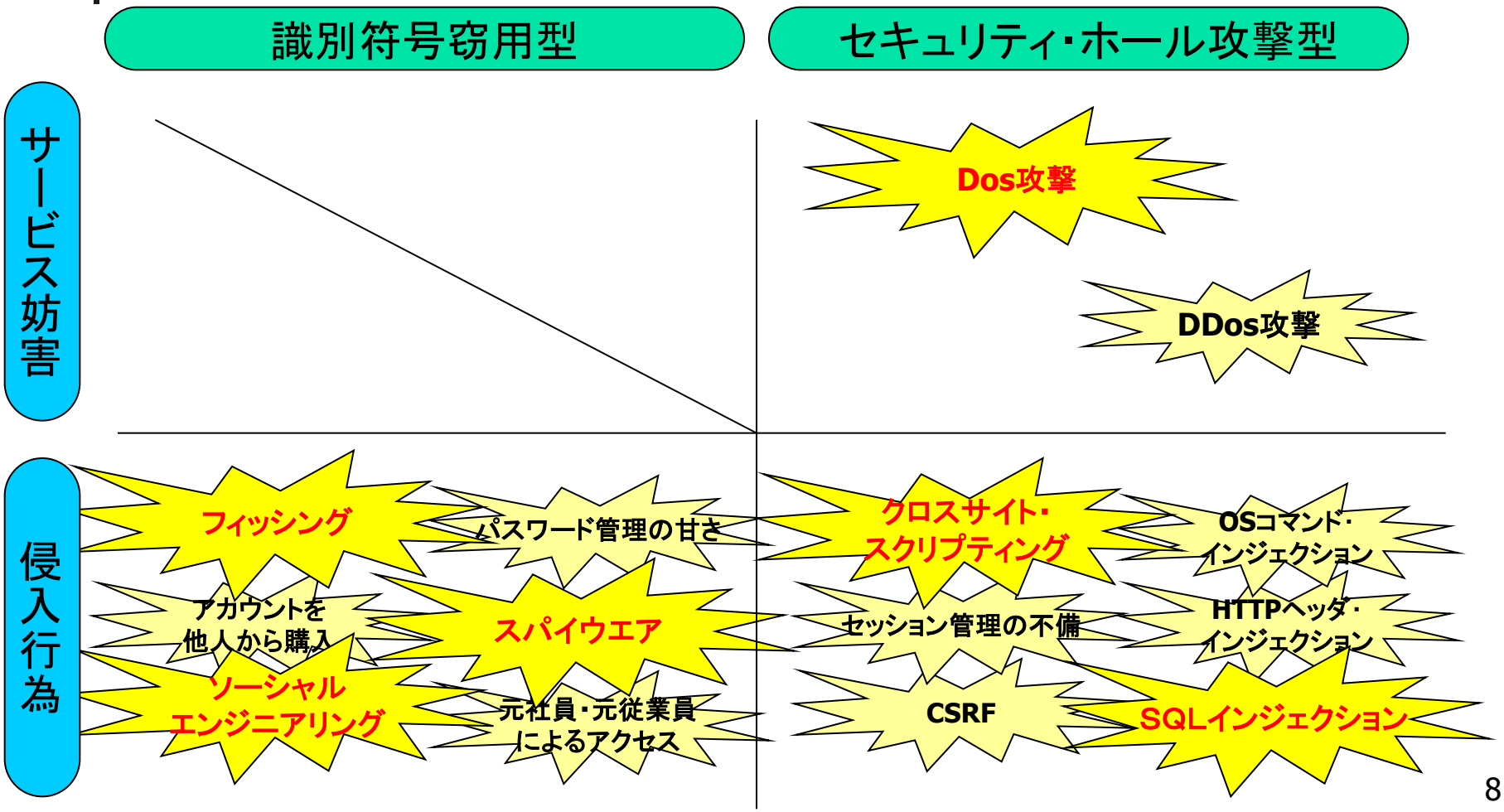
IPA『情報セキュリティ読本』実教出版より作成

2.2 類型
② 侵入行為の流れ

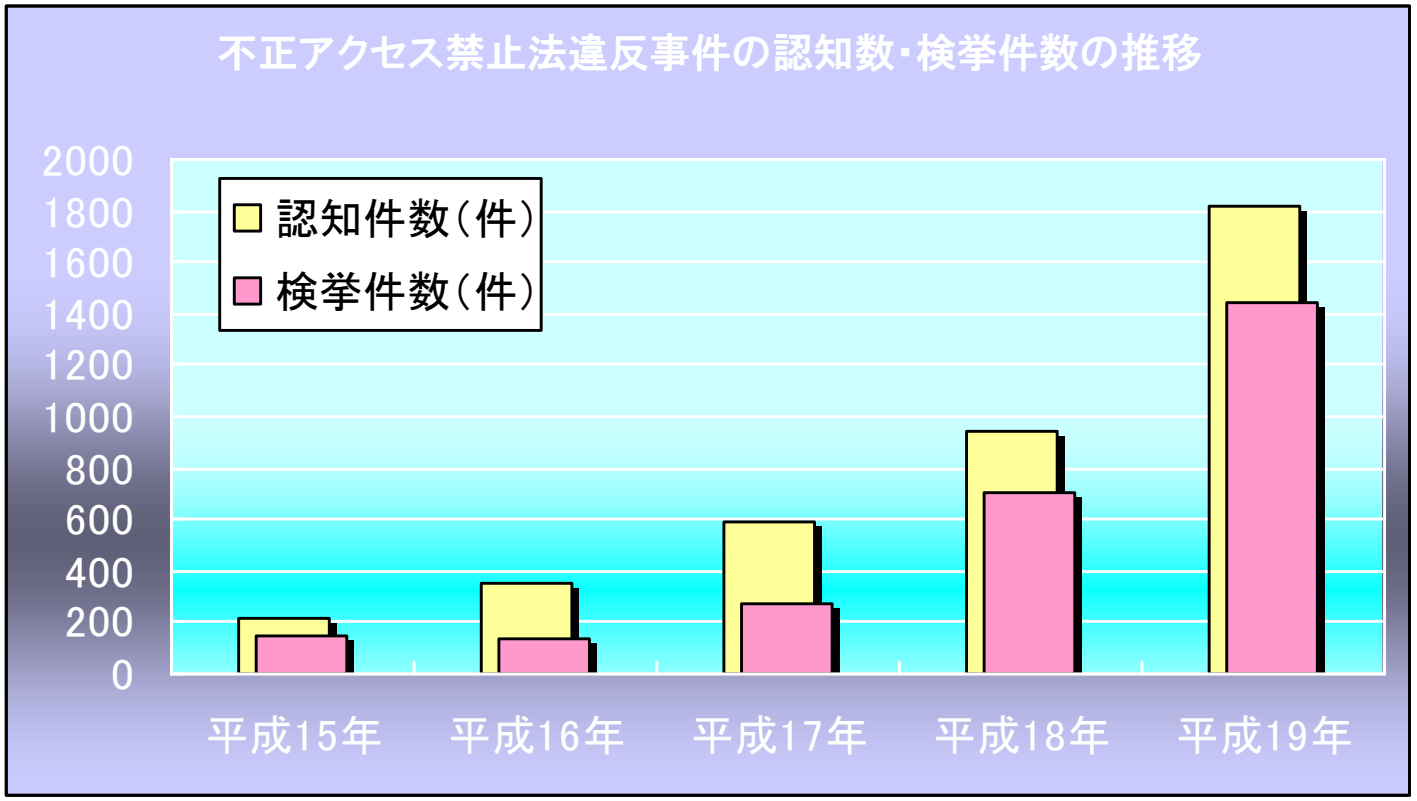


出典：IPA『情報セキュリティ読本』実教出版

2.2 類型
③ 類型のまとめ

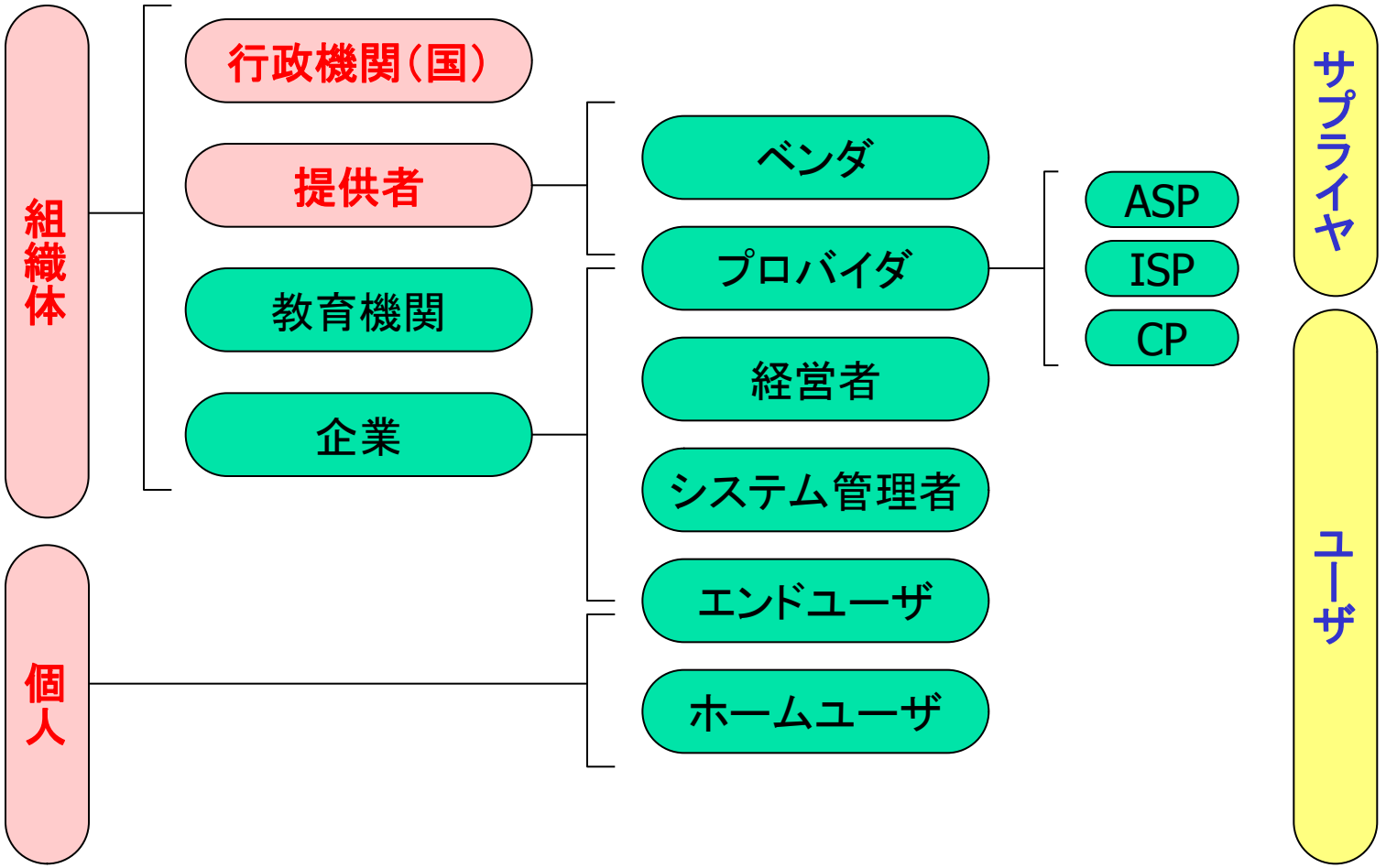


2.3 不正アクセスの現状

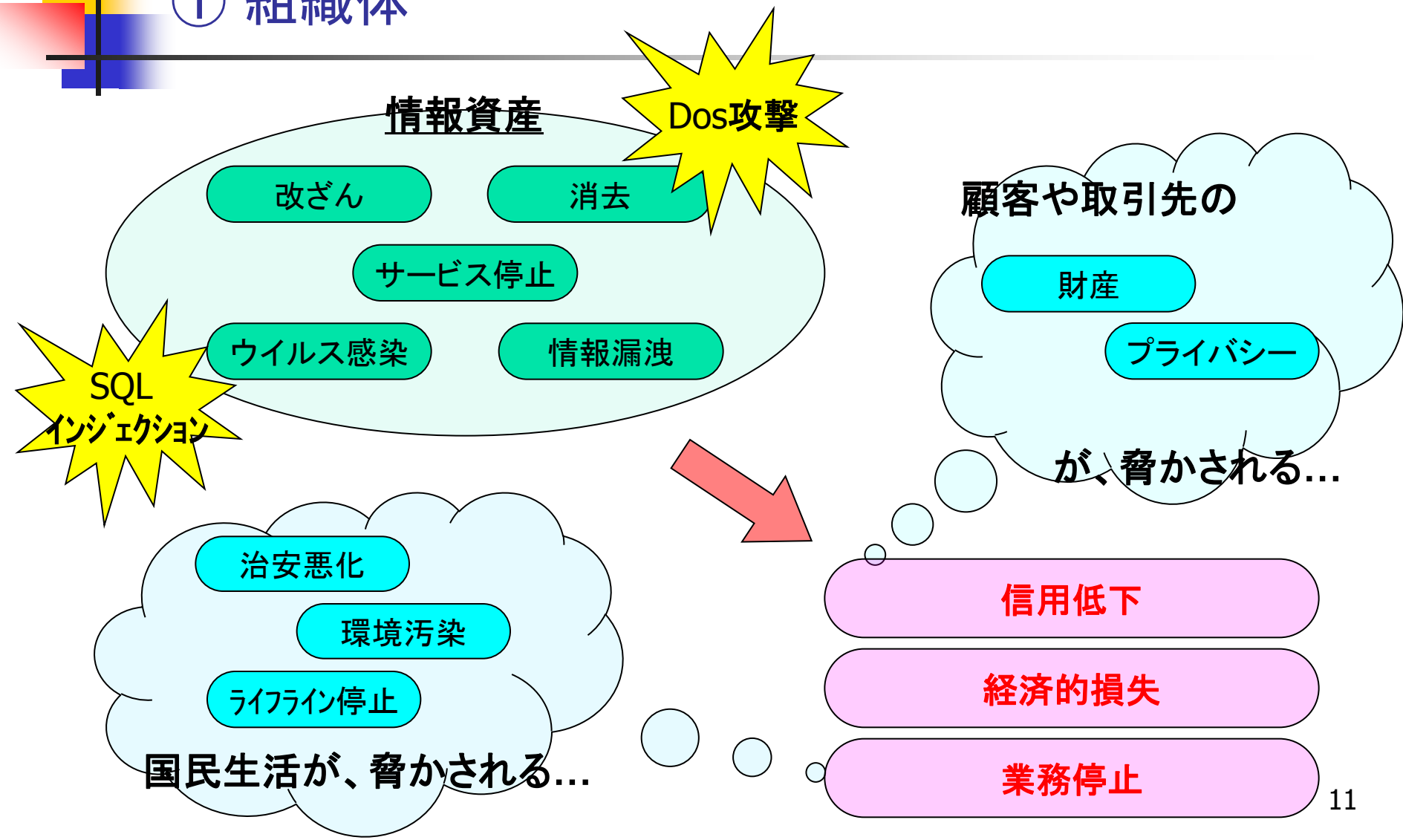


平成19年度　国家公安委員会・総務大臣・経済産業大臣
「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」
（不正アクセス禁止法第7条第1項に基づく公表）より作成

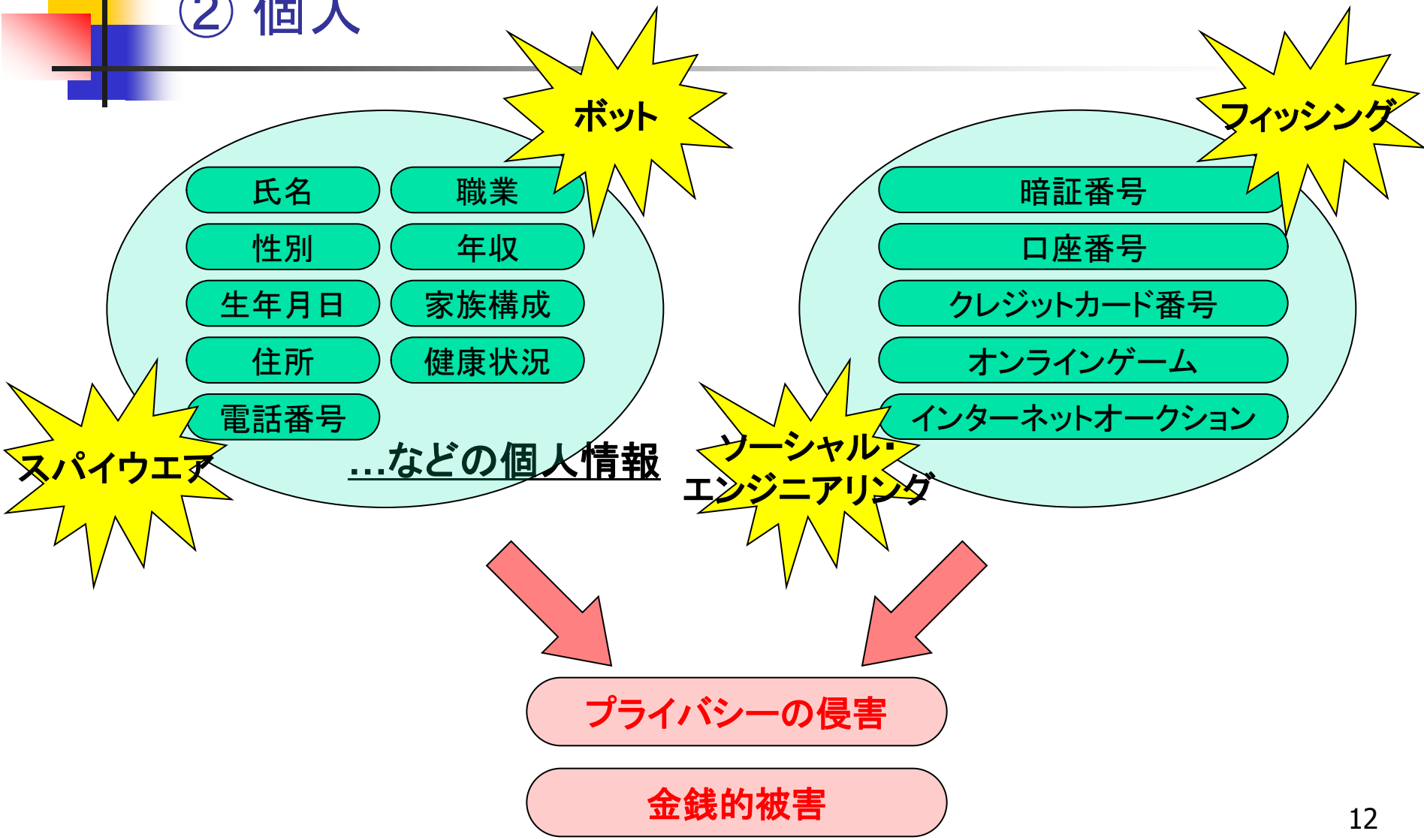
3.1 被害対象


組織体
個人
行政機関（国）
提供者
教育機関
企業
ベンダ
プロバイダ
経営者
システム管理者
エンドユーザ
ホームユーザ
ASP
ISP
CP
サプライヤ
ユーザ

3.1 被害対象
① 組織体

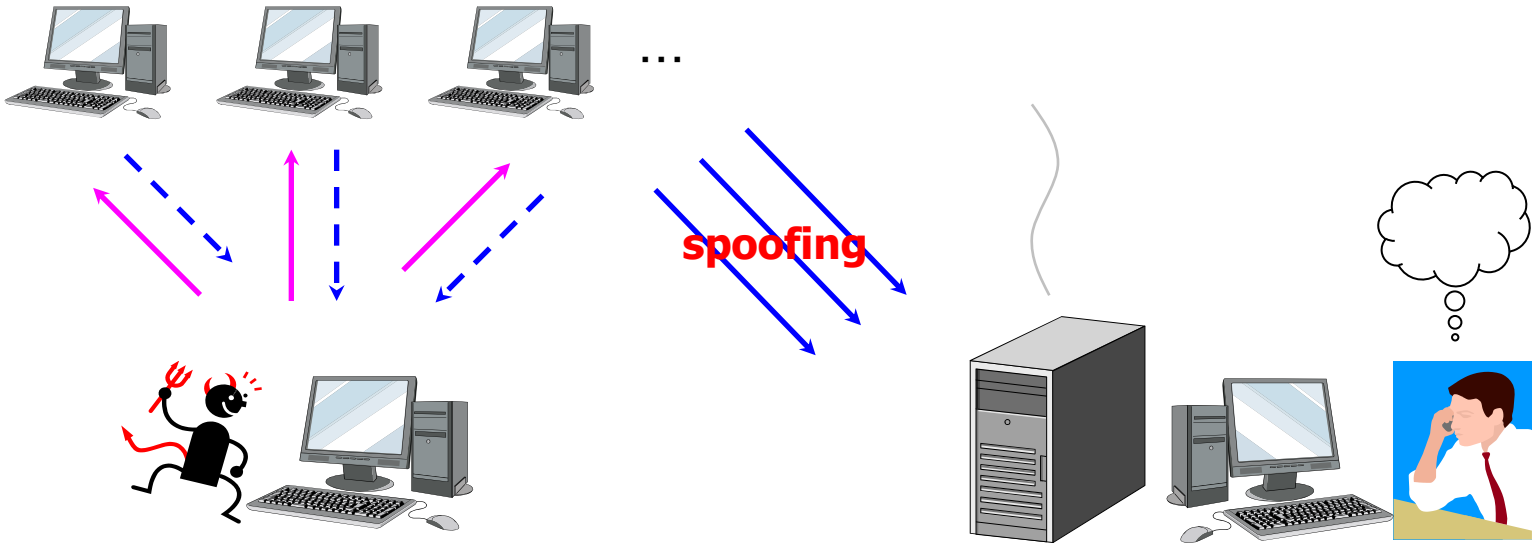

情報資産
Dos攻撃
改ざん
消去
サービス停止
ウイルス感染
情報漏洩
SQL
ｲﾝｼﾞｪｸｼｮﾝ
顧客や取引先の
財産
プライバシー
が、脅かされる…
治安悪化
環境汚染
ﾗｲﾌﾗｲﾝ停止
国民生活が、脅かされる…
信用低下
経済的損失
業務停止

3.1 被害対象
② 個人


ボット
フィッシング
氏名
職業
性別
年収
生年月日
家族構成
住所
健康状況
電話番号
暗証番号
口座番号
クレジットカード番号
オンラインゲーム
インターネットオークション
スパイウエア
…などの個人情報
ソーシャル・
エンジニアリング
プライバシーの侵害
金銭的被害

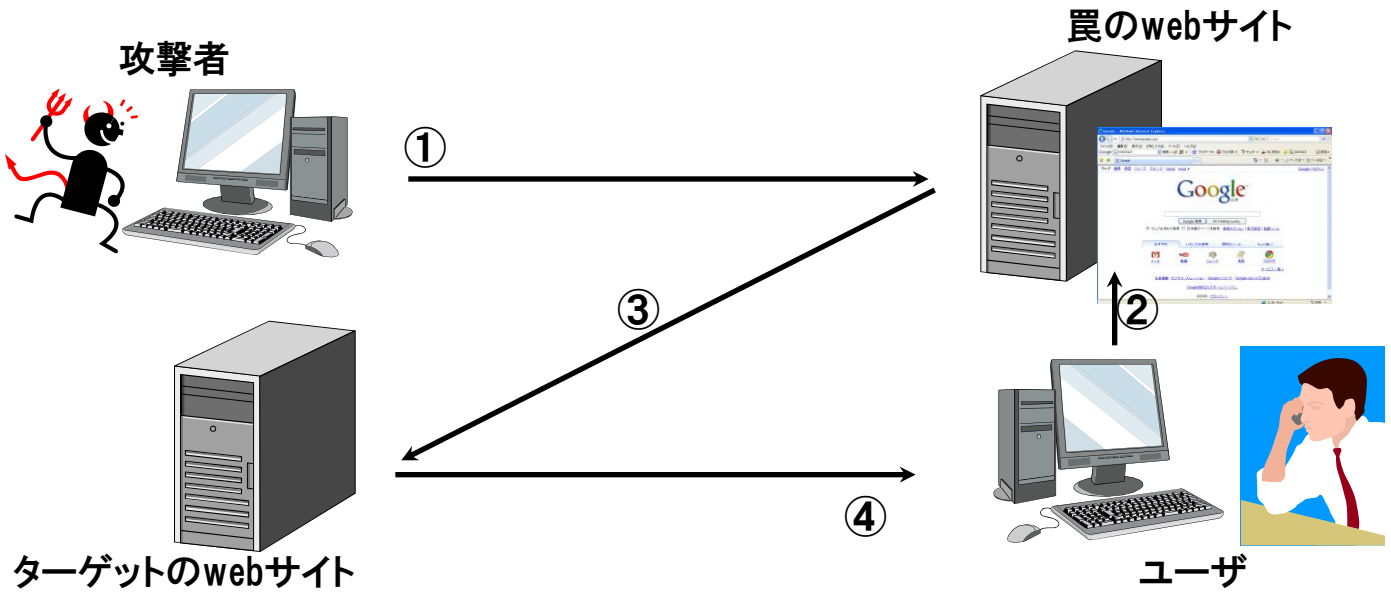
3.2 被害事例
① DoS (Denial of Service)攻撃

サーバに大量のデータを送って過大な負荷をかけ、サーバのパフォーマンスを極端に低下させたり、サーバを機能停止に追い込んだりする攻撃のこと。



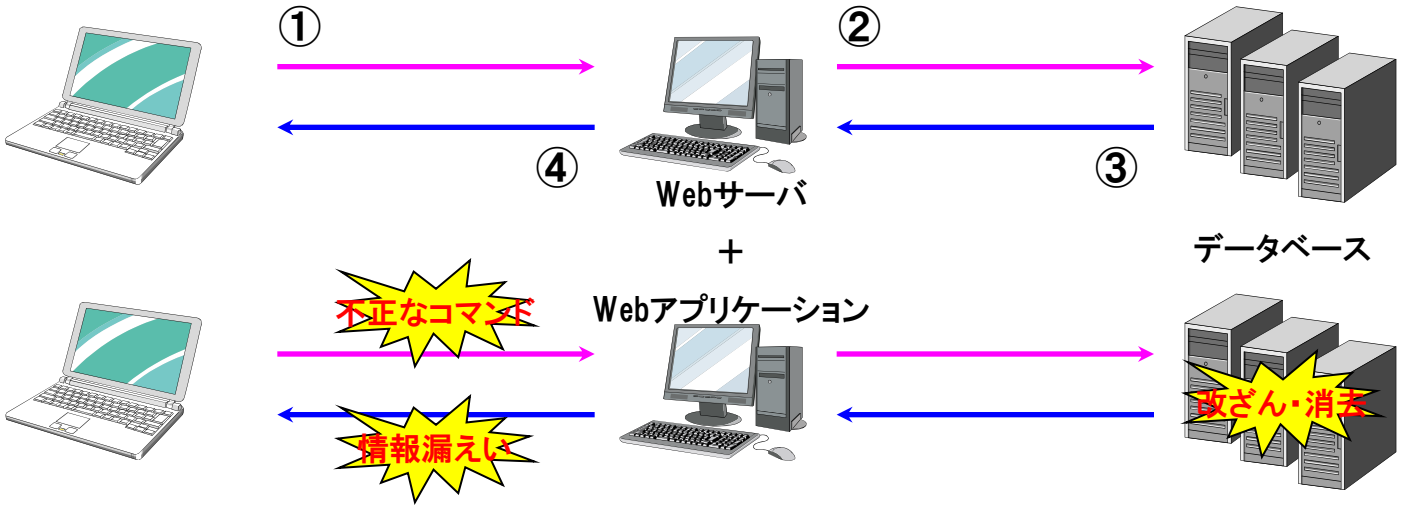
3.2 被害事例
② クロスサイトスクリプティング

ユーザがうっかり(罠が仕掛けられた)リンクをクリックすると、別のサイトへ強制的に飛ばされ、用意されたスクリプトが実行されて被害にあう。



3.2 被害の事例
③ SQLインジェクション

webサーバへの攻撃手法のひとつ。Webサイトにおいてデータベースへの問い合わせや操作を行うSQL文に不正なコマンドを挿入し、データを改ざん・消去したり、取得したりする。



コラム-1
“webサイトの脆弱性”

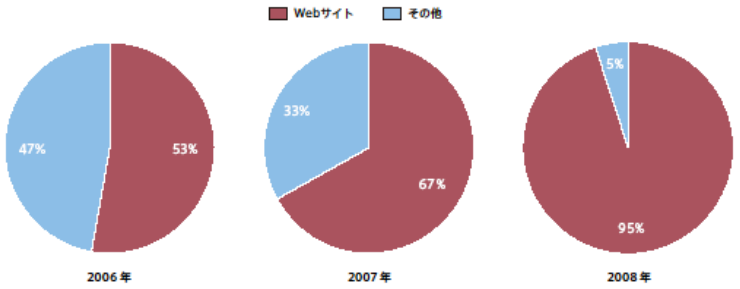


図1　重要インシデントのターゲット

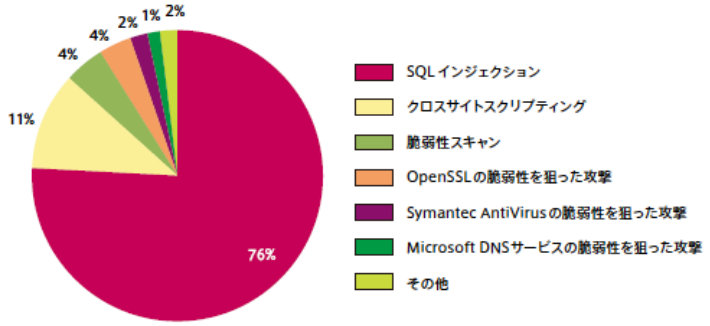


図2　重要インシデントの内訳（2008 年）

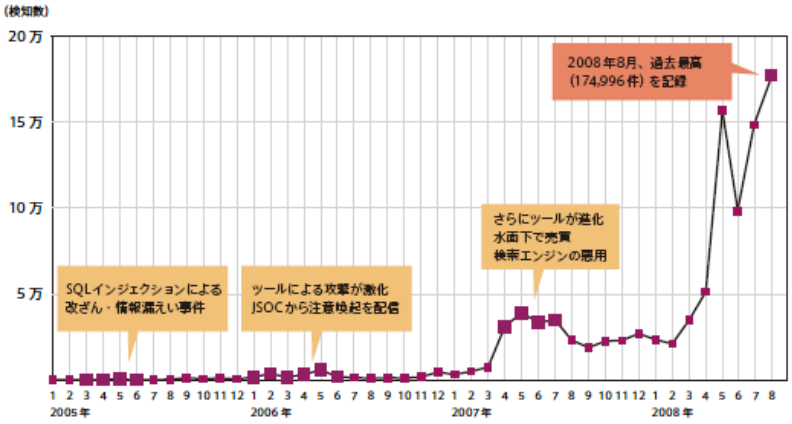


図3　SQL インジェクションの検知件数（2005 年～ 2008 年）

JSOC　侵入傾向分析レポートvol.11　より

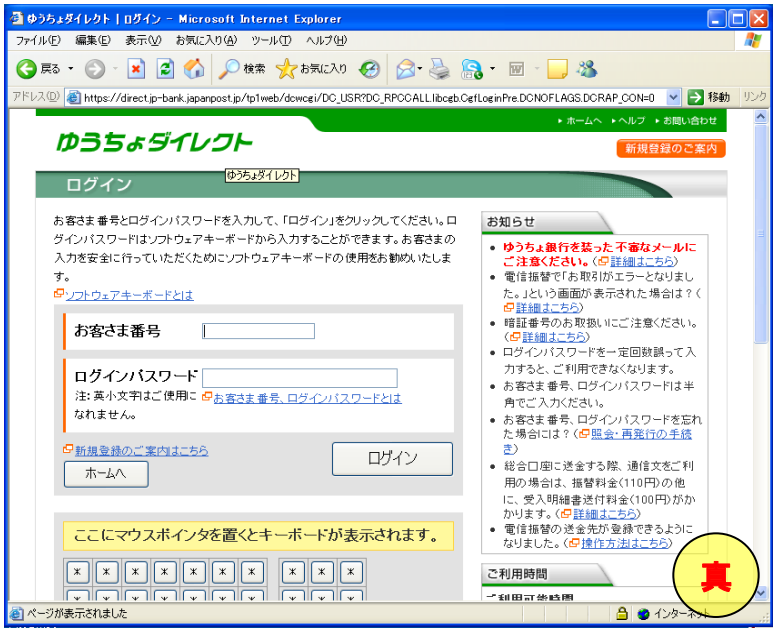
3.2 被害の事例
④ フィッシング

偽のウェブサイトへ誘導し、ユーザ自身の手で個人情報を漏洩させる。

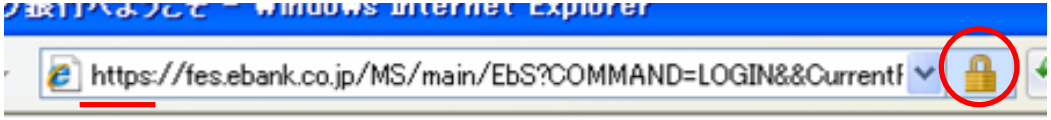
ゆうちょダイレクトをご利用頂き有難うございます。

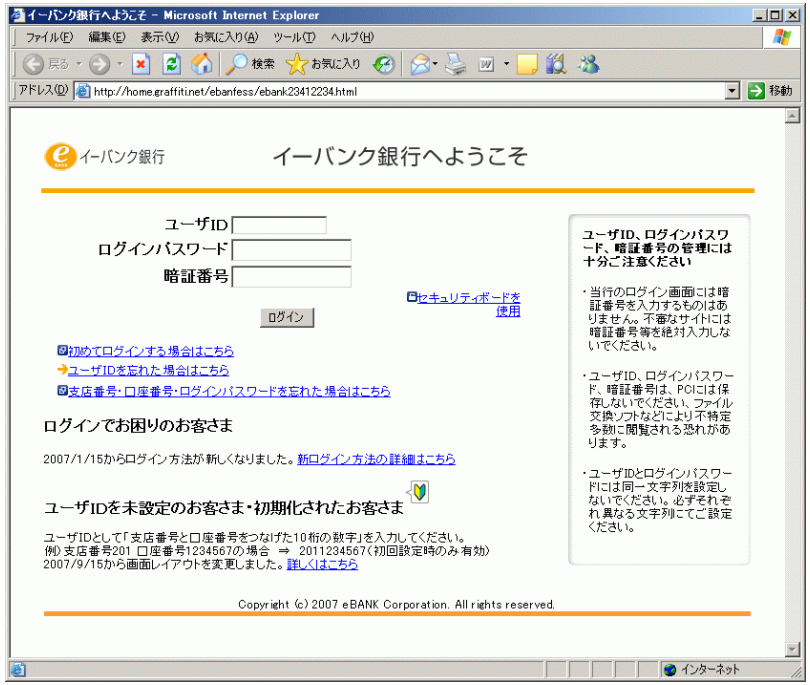
お客様へ重要なお知らせです。
詳しくは下記より必ずご確認下さい。
http://japanpost.weblike.jp/form.php

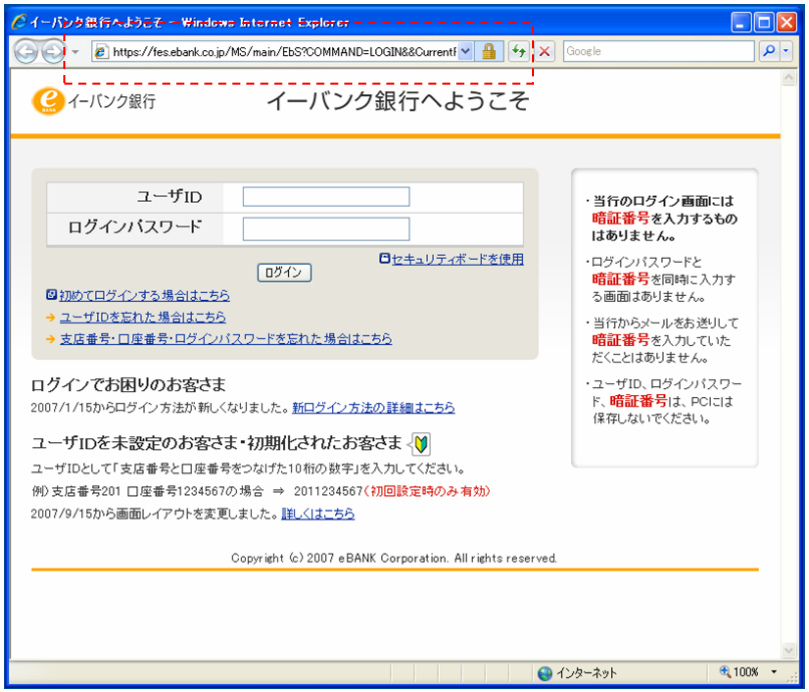
株式会社ゆうちょ銀行



コラム-2
フィッシングサイト

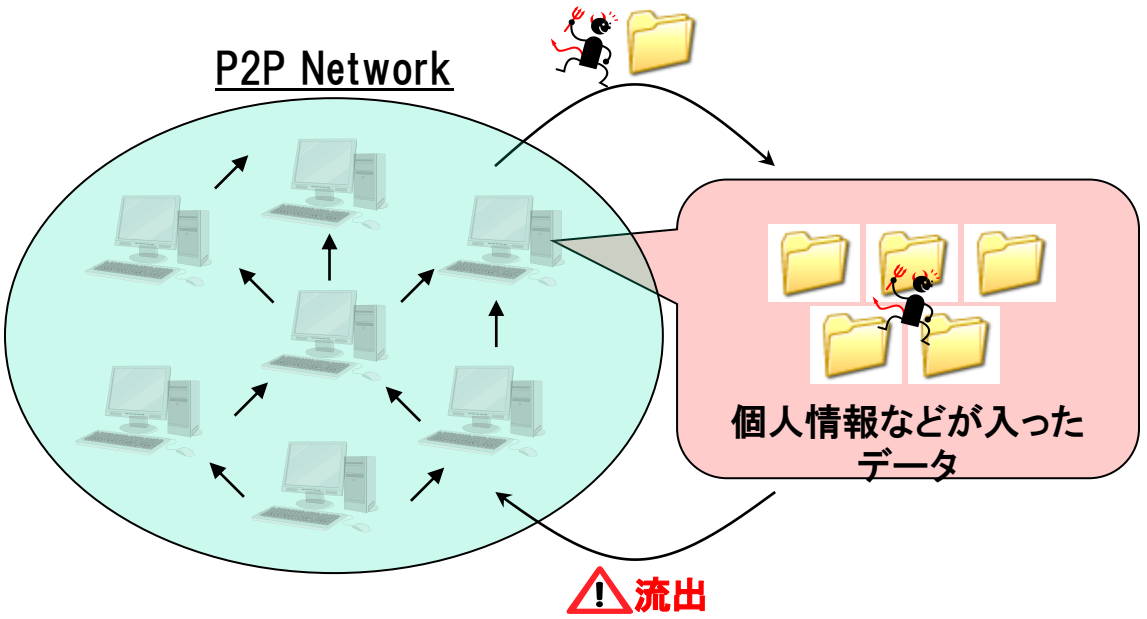






3.2 被害事例
④ スパイウエア

ユーザの気づかないうちにコンピュータへ侵入し、インターネットに対して個人情報やコンピュータの情報などを送信するソフトウエアのこと。



3.2被害の事例
⑥ ソーシャルエンジニアリング

人間の心理的隙をつく攻撃方法。ネットワークシステムへの不正侵入を達成するために、必要なIDやパスワードを、物理的手段によって獲得する行為を指す。

4.1 国の対策
①法律

関連法制定の変遷

1987年	刑法改正 [電子計算機損壊等業務妨害罪(刑法第234条の2) 電磁的記録不正作出及び供用罪(刑法第161条の2) 電子計算機使用詐欺罪(刑法第246条の2)]
2000年	不正アクセス行為の禁止等に関する法律施行
2001年	電子署名及び認証業務に関する法律施行
2005年	個人情報保護法施行

4.1 国の対策
② 制度

- 制度
  - 情報セキュリティ監査制度
  - コンピュータ不正アクセス対策基準
- 国際標準
  - ISO/IEC15408(JISX5070)
  - ISO/IEC17799(JIS5080)
  - ISO/IEC27001　　…など

4.2 提供者の対策

- ベンダの対策
  - セキュリティ対策ソフトの作成
  - 修正プログラム（パッチ）の作成・配布
  - ITセキュリティ評価及び認証制度
- プロバイダの対策

ウイルス対策

主な感染源であるメールウイルスをサーバー上でチェックするほか、パソコン内をリアルタイムでスキャン・駆除。常に最新のウイルス対策で、安心・安全なインターネットライフをお届けします。

フィッシング詐欺対策

偽のサイトにクレジットカード番号などの個人情報を入力させて、盗もうとするフィッシング詐欺。疑いのあるサイトにアクセスした際に、警告画面を表示するなどの機能が有効です。

不正アクセス対策

独自のファイアーウォール機能をはじめ、セキュリティセンターと接続してデータを暗号化するなど、セキュリティホールを利用した不正アクセスから総合的にネットワーク環境を守ります。

スパイウェア対策

ウェブサイトの閲覧やダウンロードの際に、いつの間にかパソコンに忍び込み、不正にユーザー情報を収集・・・。見過ごしがちなスパイウェアをリアルタイムで検出し、すみやかに駆除します。

無線LAN侵入対策

無線LANを通じて個人情報を盗んだり、無線LANにただ乗りするなどの不正行為対策として、定期的にパソコンやネットワーク機器を検索。不正侵入がないかどうかを確認します。

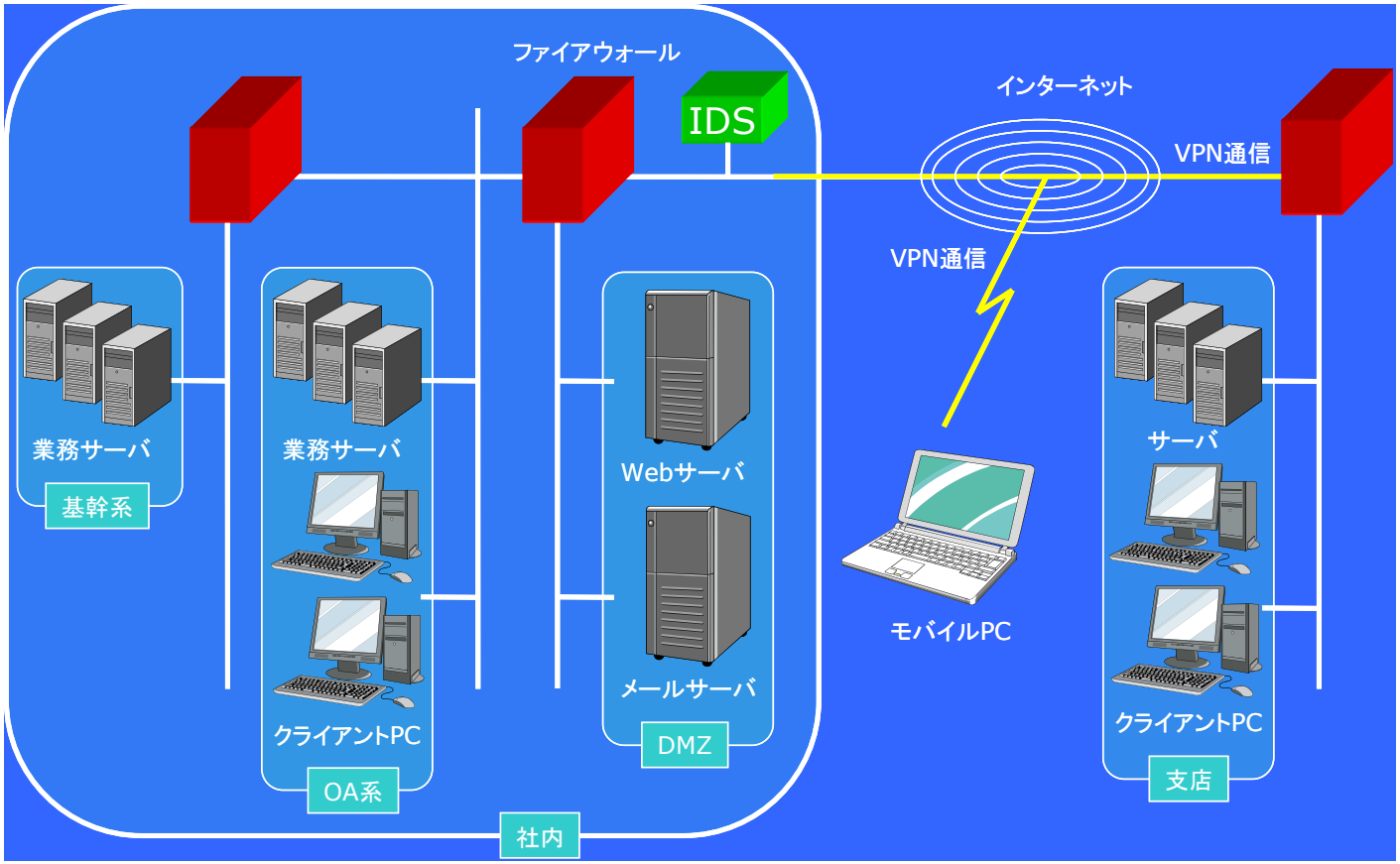
4.3 利用者の対策（組織体）
①基本的な考え方

- IDやパスワードの厳重な管理及び設定
- 不必要なポート及びサービスの閉鎖
- 外部からのアクセスに対して不必要に過剰な情報を提供しない
- セキュリティ･ホールの解消
- ルータやファイアウォールなどの設定やアクセス制御設定
- こまめなログのチェック

4.3利用者の対策（組織体）
② 具体的なシステム導入事例

- 制度的対策
  - セキュリティ･ポリシーの策定
  - 国際標準（ISO/IEC）･国内基準の適用(JIS)
- 技術的対策
  - ファイアフォール
  - DMZ (DeMilitarized Zone)
  - IDS (Intrusion Detection System)
  - IPS (Intrusion Prevention System)
  - VPN (Virtual Private Network)
  - IPsec (Security Architecture for Internet Protocol)
  - SSL (Secure Sockets Layer)

4.3利用者の対策(組織体)
③ 対策モデル例



4.4 利用者の対策（個人）
①　基本的な考え方

- Windows Update やOffice Update など、OS やアプリケーションソフトのアップデート
- パスワードの設定と管理（複雑化、定期的に変更、安易に他人に教えないなど）
- 無線LAN やPC 共有についてのセキュリティ設定確認
- ルータやパーソナルファイアウォールの活用

4.4 利用者の対策（個人）
② パスワード設定・管理

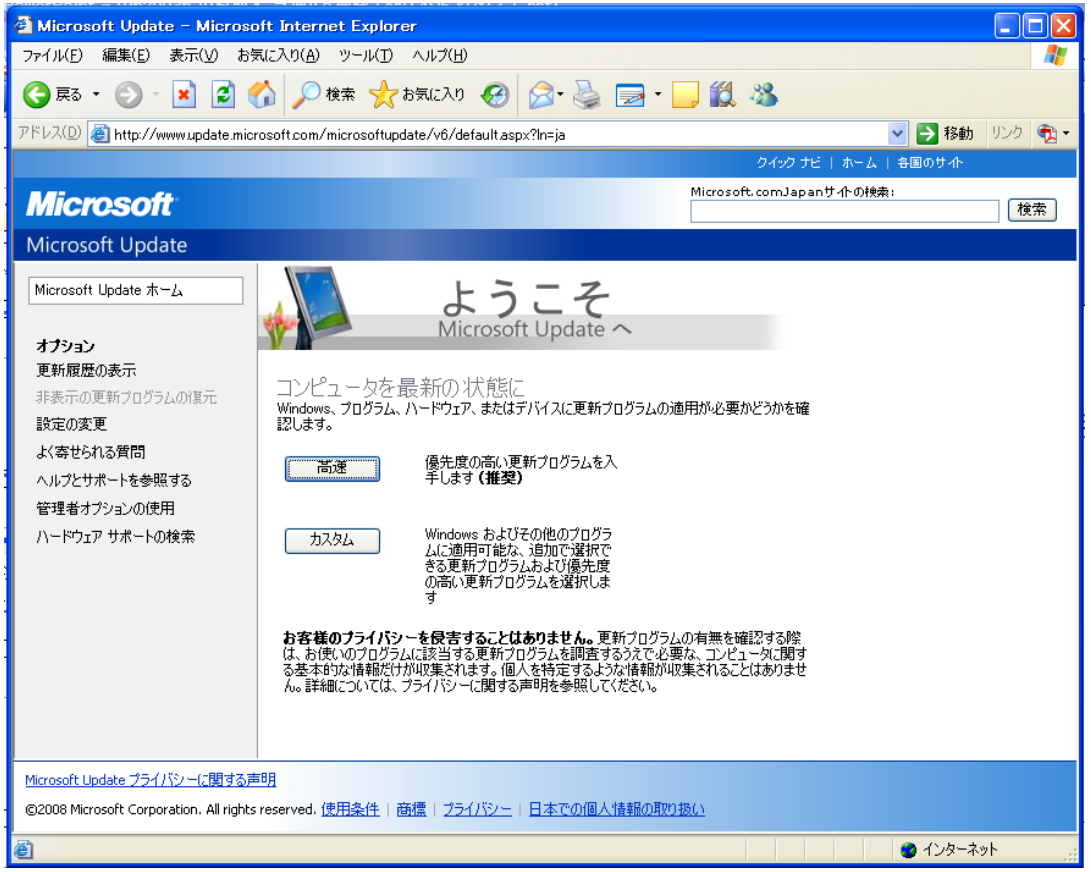
- パスワード設定の注意点
  - (1) 大文字・小文字・数字・記号の組み合わせ
    記号(!、＃等)、数字、英字を適当に織り交ぜる
  - (2) 長いパスワード
    最低8 文字以上
  - (3) 推測しづらく自分が忘れないパスワード
    無作為で意味を持たない文字列であること
- パスワード管理の注意点
  - (1) 定期的にパスワードを変更する
  - (2) 紙に書き留めない
  - (3) パソコンに保存しない
  - (4) 人に教えない

4.4 利用者の対策（個人）
③ 文字数と入力桁数によるパスワードの最大解読時間

使用する文字の種類	使用できる文字数	最大解読時間			
		入力桁数			
		4桁	6桁	8桁	10桁
英字(大文字、小文字区別無)	26	約3秒	約37分	約17日	約32年
英字(大文字、小文字区別有)＋数字	62	約2分	約5日	約50年	約20万年
英字(大文字、小文字区別有)＋数字＋記号	93	約9分	約54日	約1千年	約1千万年

※すべての組み合わせを試すために必要な時間を計算。記号は31文字使用できるものとした。使用パソコンOS:Windows Vista Business 32bit版、プロセッサ:Intel Core 2 Duo T7200 2.00GHz、メモリ:3GB

4.4 利用者の対策（個人）
④ セキュリティパッチの適用



4.4 利用者の対策（個人）
⑤ 統合セキュリティ対策ソフトの導入

- 統合セキュリティ対策ソフトの導入

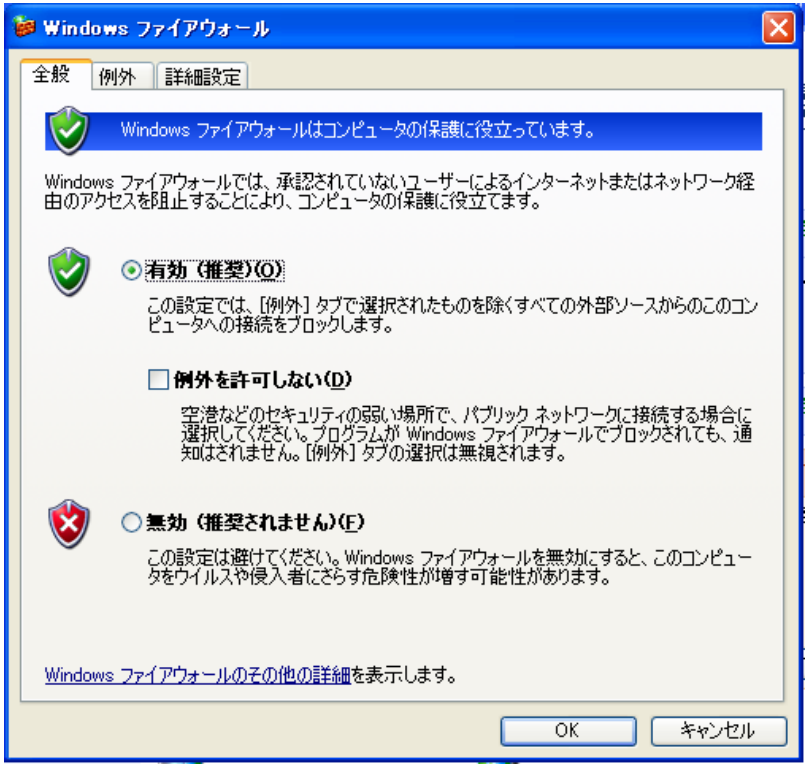
　総合セキュリティソフトとはアンチウイルス、アンチスパイウェア、ファイアウォールなどパソコンのセキュリティ対策に必要な機能が一つにまとまったソフトである。
　操作も簡単なものが多く、価格の面から見ても、必要なソフトをバラバラと購入するよりも安く済む。

http://www.the-hikaku.com/security/index.html

4.4 利用者の対策（個人）
⑥ ファイアウォールの設定

- パーソナルファイアウォールの設定

Windows XP SP2以降では、「Windowsファイアウォール」と呼ばれるパーソナルファイアウオールが標準で搭載された。



※画面はWindows XP Home Edition

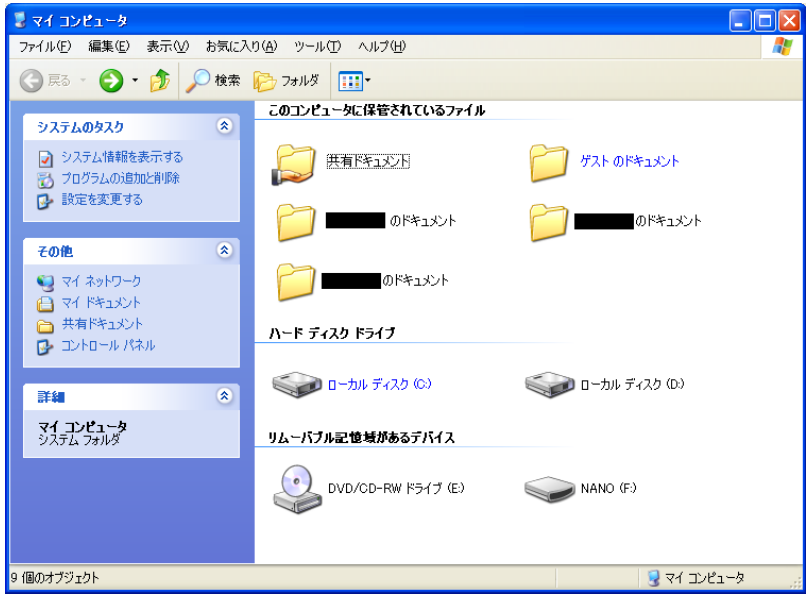
4.4 利用者の対策（個人）
⑦ 無線LANのセキュリティ設定

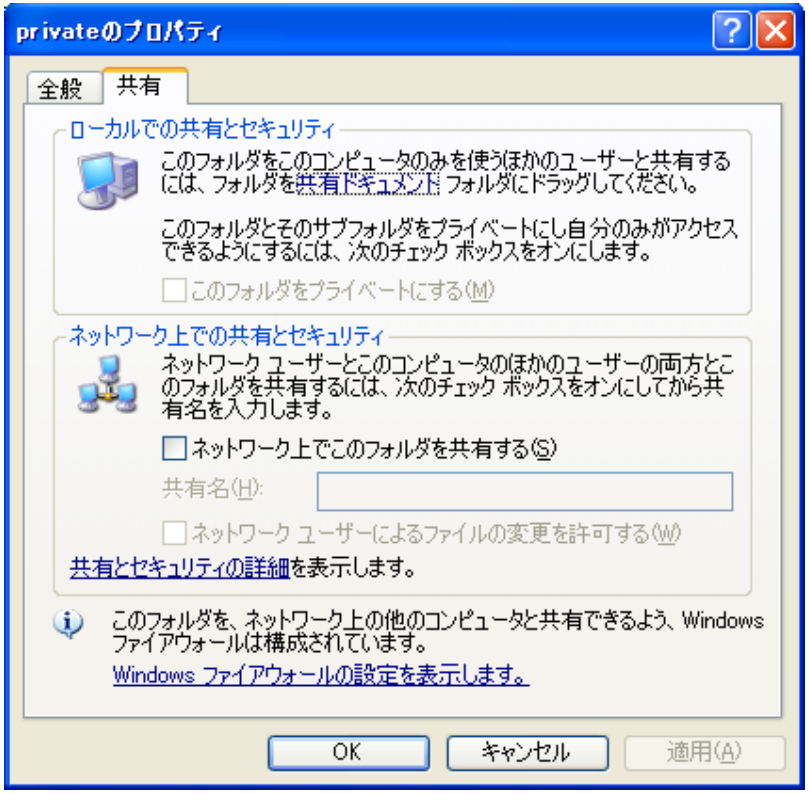
- 無線LAN アクセスポイント（親機）
  - WPA2/WPAを設定する

    ※WEPにはぜい弱性が発見されている。
  - SSIDを設定する
  - MAC アドレスによるフィルタリングを設定する
  - 空白又はANY 端末からの接続を拒否する

- APの設定に合わせてパソコンを設定する

4.4 利用者の対策（個人）
⑧ ファイル共有設定の無効化



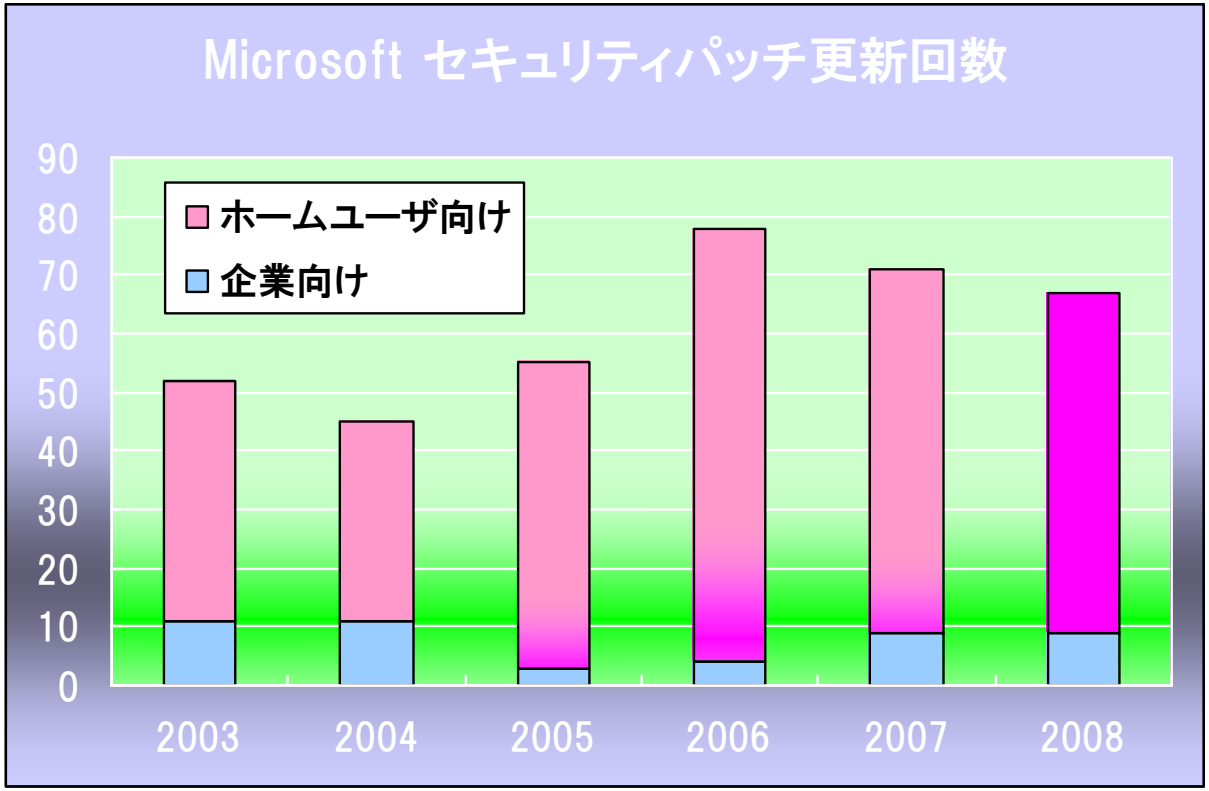


※画面はWindows XP Home Edition

5. おわりに
① 識別符号窃用型の課題

	利点	欠点
知識認証	・ 安価で導入可能(ただし、ワンタイムパスワードの場合、機器の費用がかかる)	・ 漏洩しやすい ・ 忘れる可能性がある
所有物認証	・ 覚える必要がない	・ 機器をなくしてしまう危険がある ・ 機器の貸し借りをする可能性がある
生体認証	・ 覚える必要がない ・ 貸し借りができない	・ プライバシー情報を登録しなければならない

5. おわりに
② セキュリティ・ホール攻撃型の課題



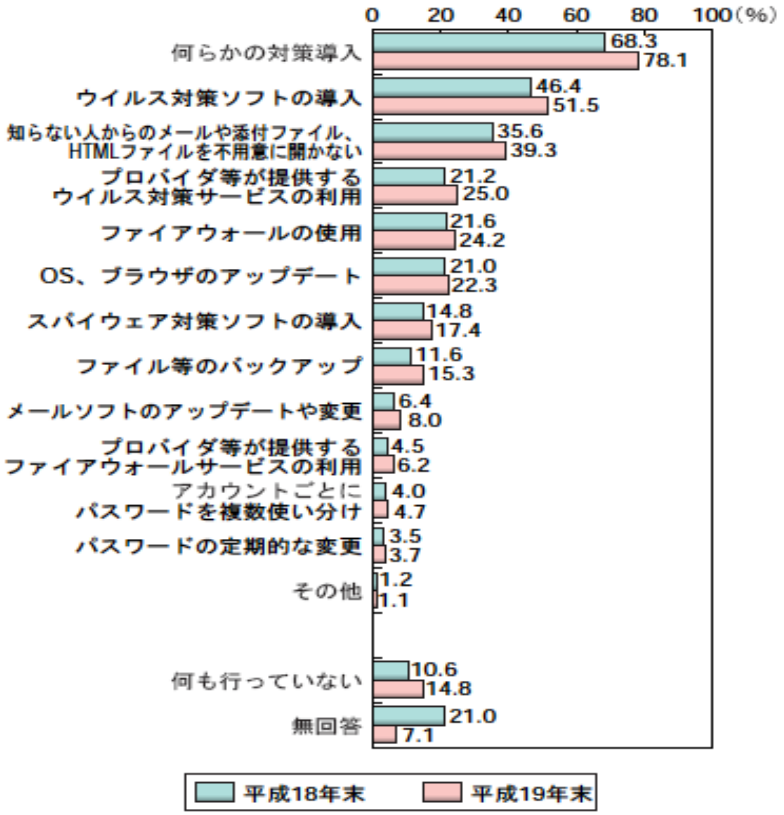
Microsoft ホームページ内

「ITPro 向けに作成されている毎月のセキュリティ更新プログラム情報サマリ」より 作成

※2008年は10月までの更新回数で作成

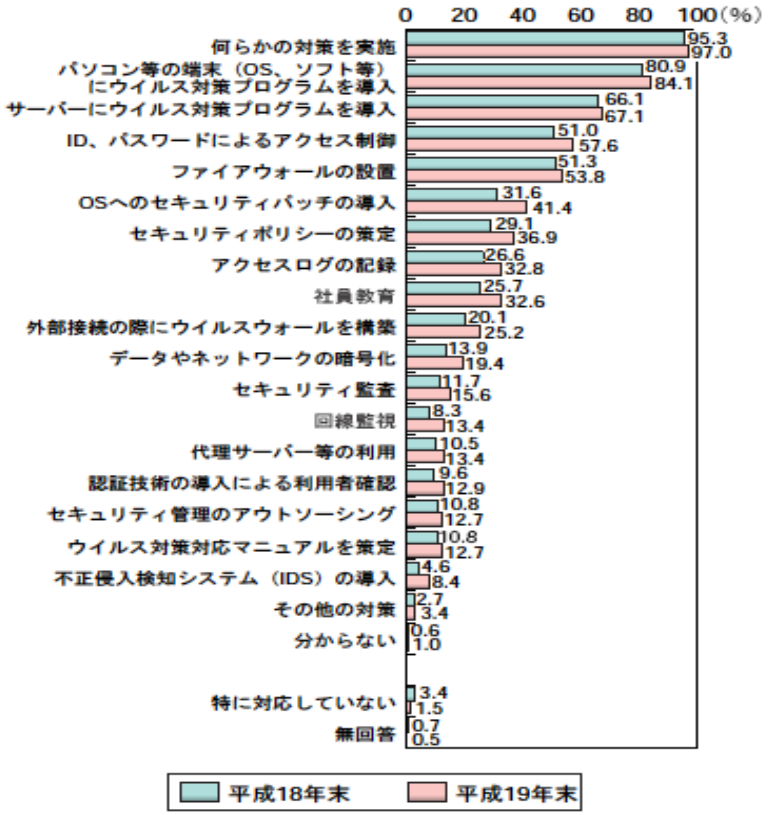
5. おわりに
③ 世帯及び企業のセキュリティ対策実施状況

図表1-3-4-8　世帯におけるセキュリティ対策の実施状況（複数回答）



総務省「通信利用動向調査」により作成

図表1-3-4-9　企業におけるセキュリティ対策の実施状況（複数回答）



総務省「通信利用動向調査」により作成

5. おわりに
④ 結論

- 最終的にコンピュータやネットワークにログインするのはエンドユーザ・ホームユーザである。
- 現在の対策には課題も残るが、実施により被害を最小限に抑えることは出来る。
- しかし、家庭においても、企業においても対策を実施していない現実がある。
- これらの実施水準を引き上げることで不正アクセスを減らすことができるのではないだろうか。
- 「これひとつで完璧！」という対策はないので、様々な対策を組み合わせて、総合的な対策を行う必要がある。