情報セキュリティ　講習会

（職場の情報セキュリティ）

広島工業大学　情報学部　　末次

２００９－０１－２４（土）

目次

はじめに.

1. コンピュータとは何か
2. 被害の種類
3. リスク・脅威の内容
4. セキュリティ対策

資料.

！！

９兆円　（IT犯罪被害総額）

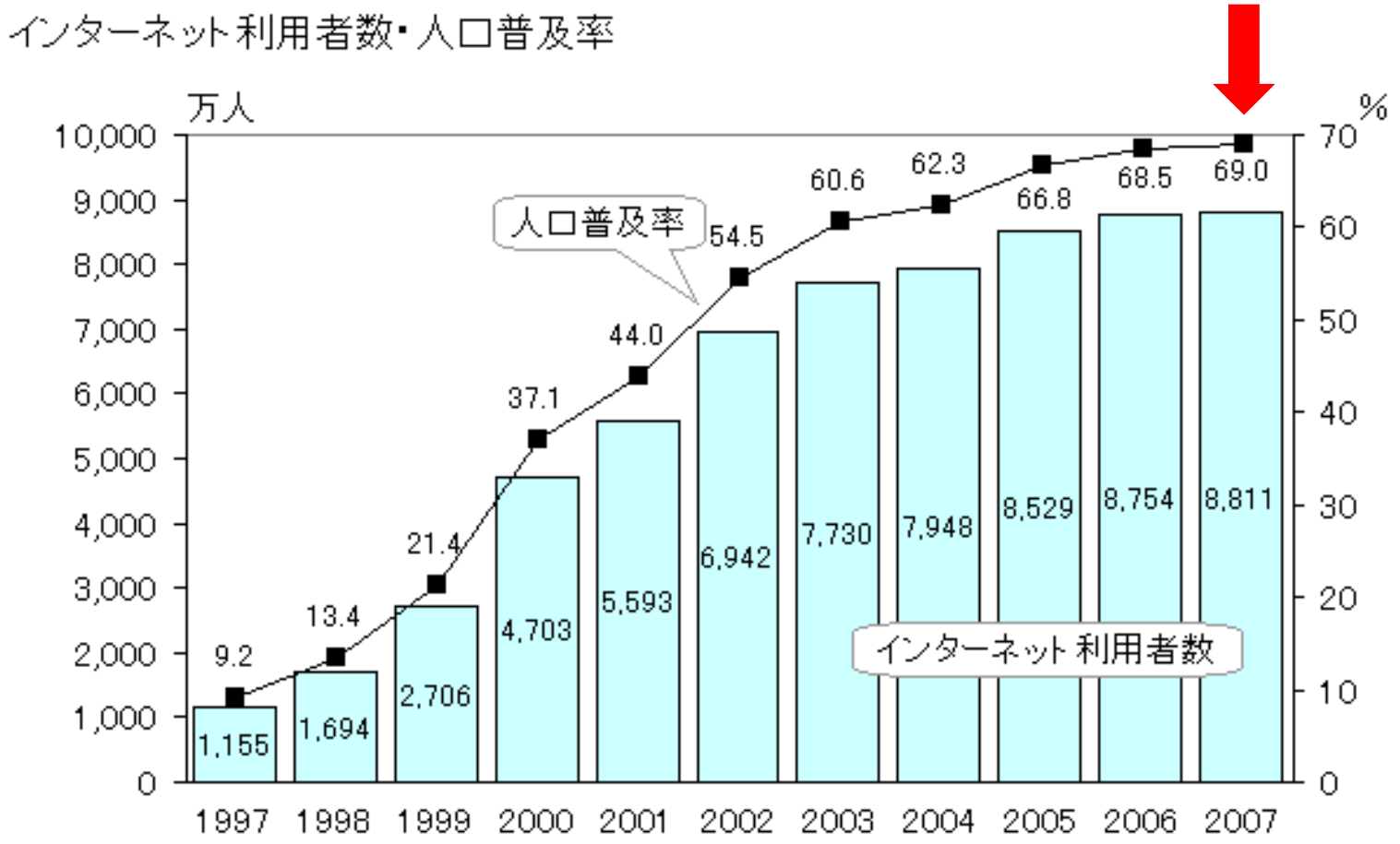
１４億人（ネット利用者数）

１億　　（Webサイト数）

８８００万人

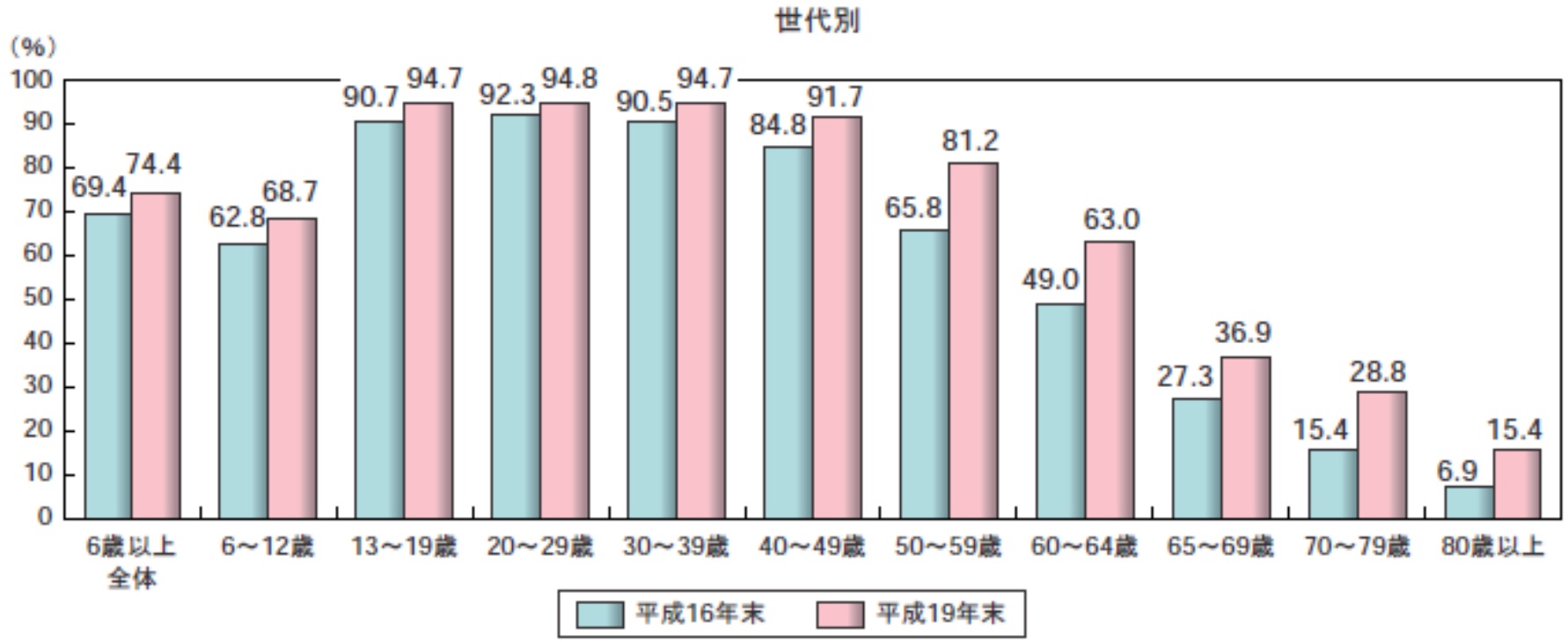
（日本のネット利用者数）

我が国のインターネット普及率A



（注）年末の推計。インターネット利用者数は、パソコン、携帯電話、ゲーム機等のいずれかでの利用者。対象年齢は1999年まで15～69歳、2000年末15～79歳、2001年以降6歳以上。
（資料）総務省「通信利用動向調査」

我が国のインターネット普及率B

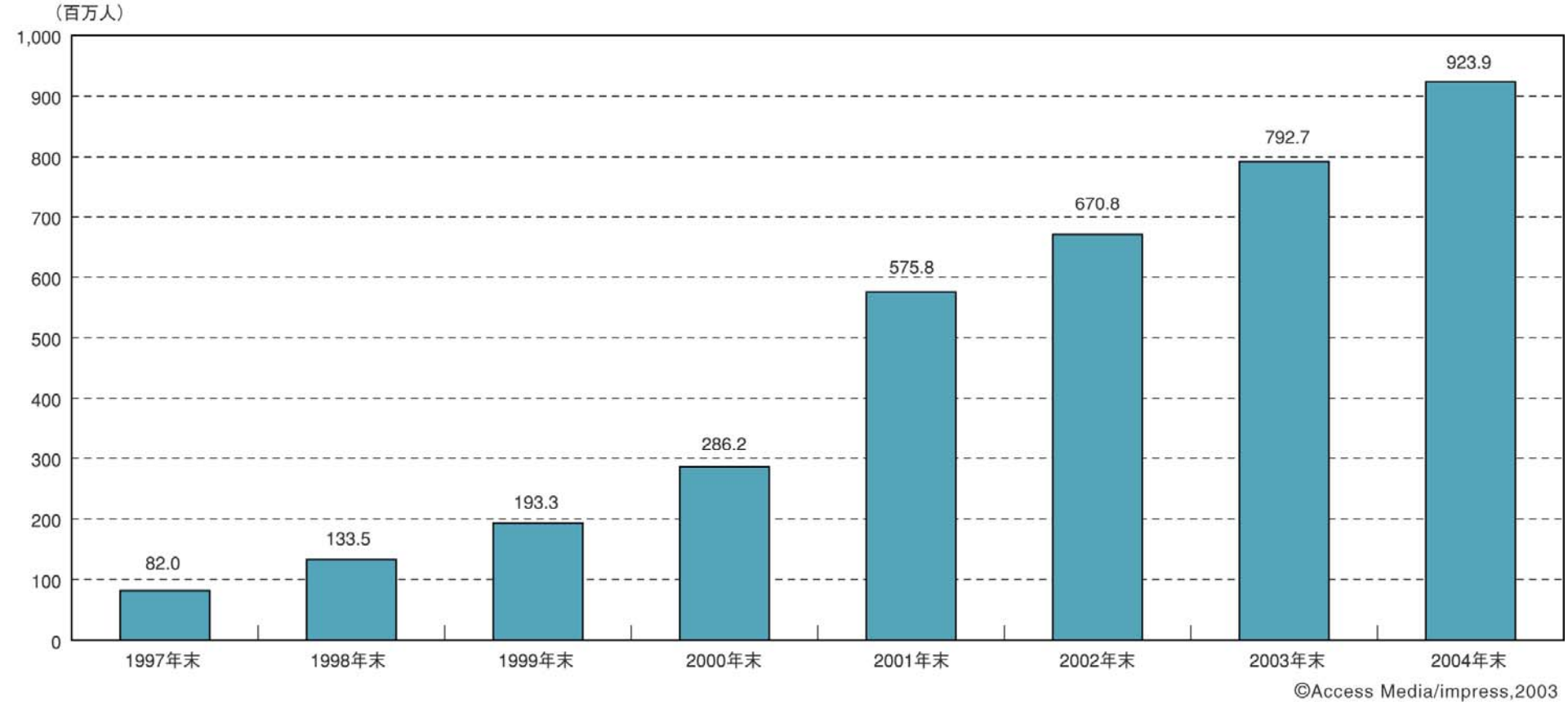


（H20　情報通信白書）

世界のインターネット利用者数

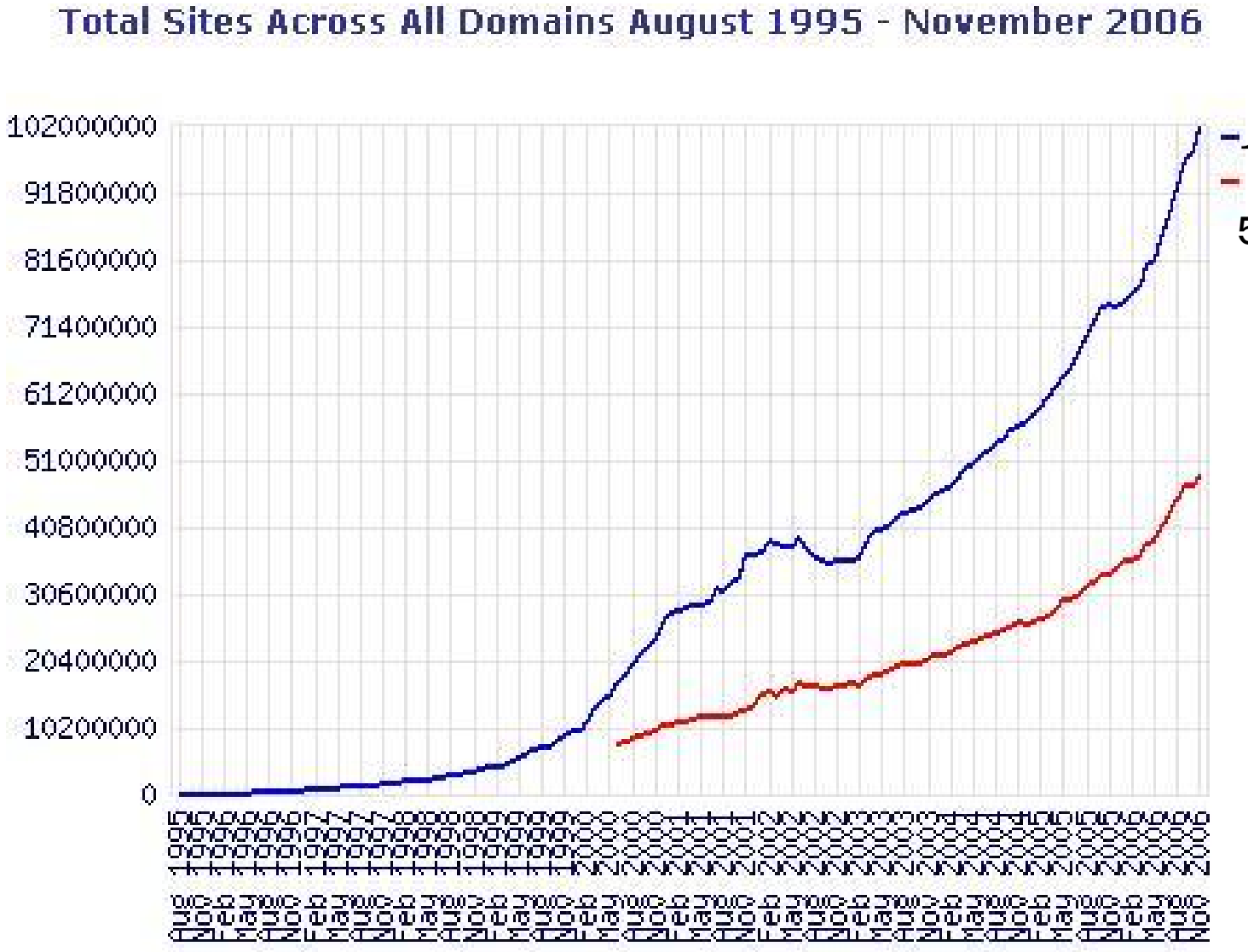
2003年末で、8億人。　2003年末で、14億人以上。

資料4-1-1　世界全体のインターネット利用者数推移予測（1997年-2004年）



出典　インプレス「インターネット白書2003」

世界のWebサイト増加推移



100万（1997）

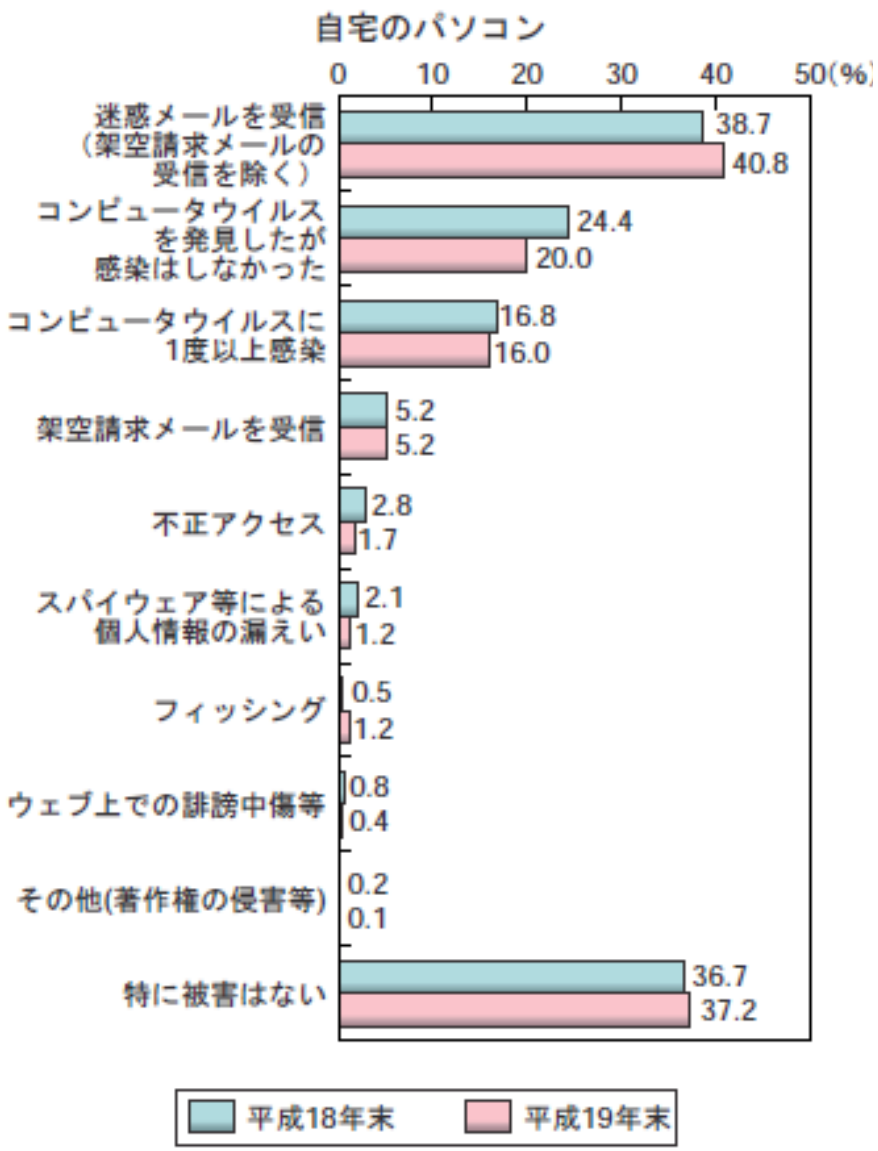
1000万（2000）

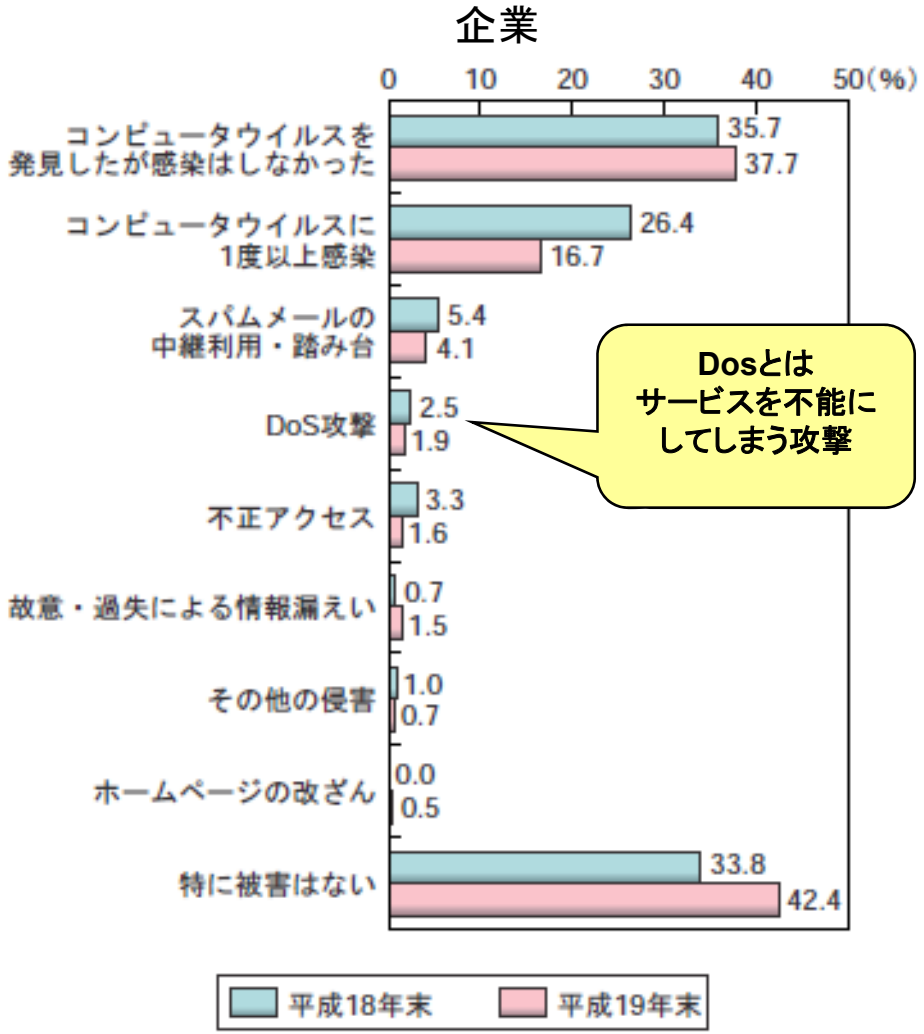
5000万（2004）

1億（2006）

（出典　英Netcraft ）

被害経験





（H20　情報通信白書）

コンピュータ・ウィルスによる被害額

中小企業、大手・中堅企業それぞれについて、次の考え方で、被害額が生じた企業の平均的な被害額を参考値として計算すると、それぞれ以下のとおりとなった。

	中小企業（被害発生企業数 95 社）	大手・中堅企業（被害発生企業数 110 社）
被害額（参考値）	約 4.3 百万円／社	約 130 百万円／社

推計される被害額について

直接的な被害額として計上される支出項目として、以下の対策などが挙げられる。

- サーバの再構築作業（OS の再インストール、各種設定等）
- Web アプリケーションの改修作業
- 第三者によるセキュリティ検査（ぜい弱性検査）
- セキュリティ対策システム機器（ファイアウォールや IDS 等）の導入

ヒアリング対象となった社（複数社）のケースをみると、使用されていたサーバの台数（数台～数十台）・プログラム本数（数百本～数千本）であった。これらを踏まえて、復旧作業に要したウェブアプリケーション等の改修費用・検査等の外注費およびファイアウォール等の機器の購入費を推計すると、約 4,800 万円～1 億円程度を要するものと考えられる。

（2006年　情報処理推進機構　調査）

迷惑メールの比率

スパムメール（迷惑メール）が
・電子メールのアカウントを占める割合は、
　　全体の70%に拡大している。

・英国企業に与えた損失は昨年だけで
　　32億ポンド（約5,760億円）
・世界中の国から送られてくる
・規制しても、抜け道を探して送りつける

（出典:© 1999- 2004 JAPAN JOURNALS LTD ）

はじめに.

１. コンピュータとは何か

２. 被害の種類

３. リスク・脅威の内容

４. セキュリティ対策

資料.

いろいろなコンピュータ

・動く原理はすべて同じである。

（大型コンピュータ）

（スーパーコンピュータ）

（サーバー）

（ワークステーション）

（デスクトップ型パソコン）

（ノート型パソコン）

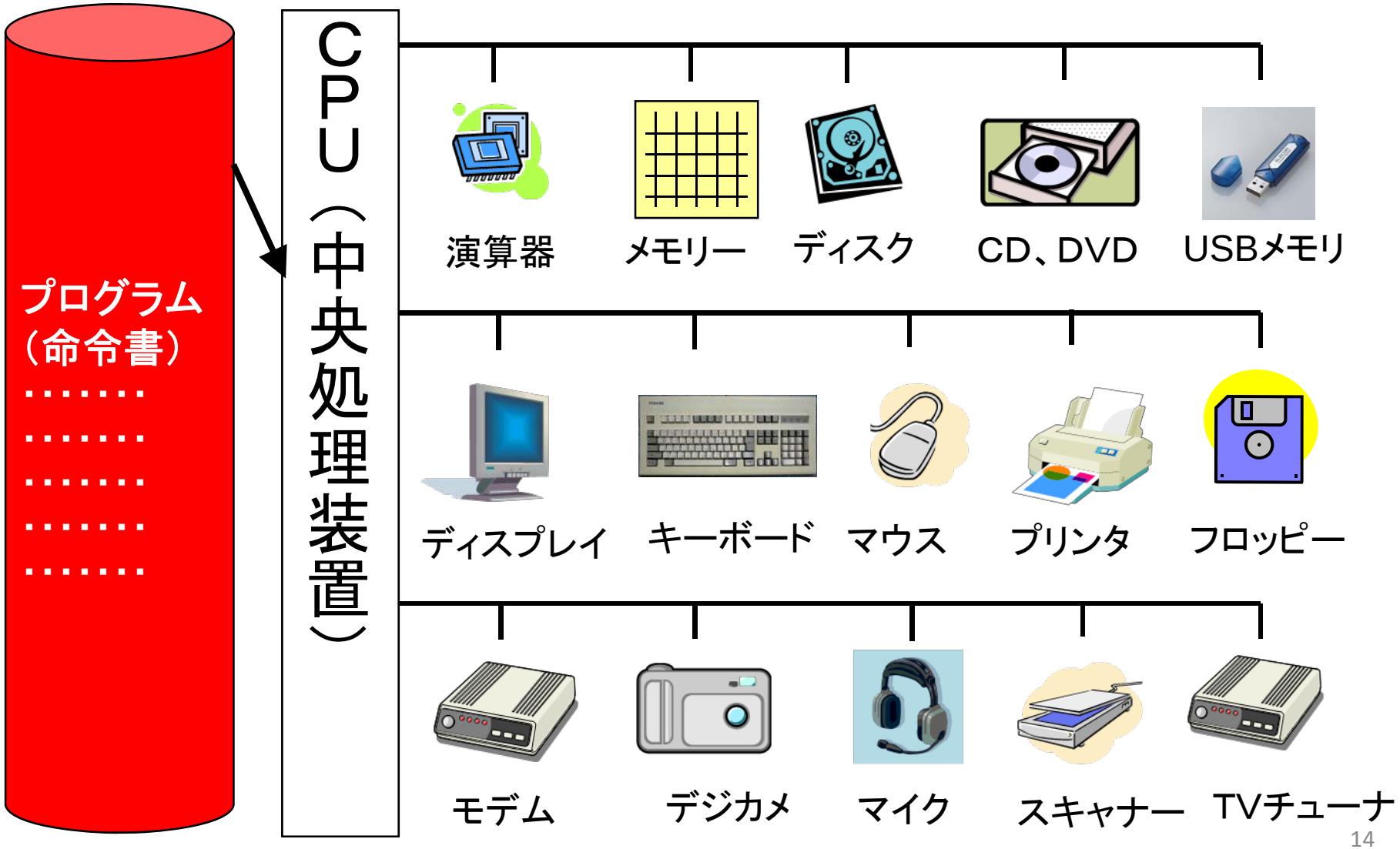
（ミニノート型）

（パームトップ）

（携帯電話）

プログラムが全てを動かす

CPUが、命令書（プログラム）通りに、1行ずつ、各装置に実行を指示。



プログラムの事例1（有用）

```
/*   duration time   */
#include <time.h>
#include <stdio.h>
int main(void) {
     time_t time1, time2;
    double i;
    time(&time1);
    for (i=0; i<5*10000*10000; i++);
    time(&time2);
    printf("duration-time is %6.0lf sec¥n", difftime(time2,time1));
    printf("i=%15.0lf¥n",i);
    return 0;
}
```

1を5億回ほど加算する時間を計算しなさい。

結果は5秒でした。

プログラムの事例2

```
<HTML>
<HEAD>
<meta http-equiv="Content-Type" content="text/html;
    charset=Shift_JIS">
<TITLE>aki-demo1.html</TITLE>
</HEAD>
<BODY BGCOLOR="black">
<applet code="Softaki.class" width="1000" height="700">
</applet>
</BODY>
</HTML>
```

実は、これが
ウィルスの実行を
指示している !!

ウィルスの事例

```
import java.applet.*;
import java.awt.*;
import java.util.Random;
import java.awt.event.*;
public class Softaki extends Applet implements Runnable,KeyListener{
        final int HOSI = 1000;
        int hx[] = new int[HOSI];
        int hy[] = new int[HOSI];
        int hz[] = new int[HOSI];
        boolean loop;
        int head=0;
        public void init(){
                requestFocusInWindow();
                addKeyListener(this);
                loop = true;
            .
            .
            .
```

これが
ウィルスの本体プログラム

結果は、

プログラムには２種類ある。

有用なプログラム

不正なプログラム

・コンピュータ・ウィルス
（マクロ、ワーム、ボット）
・不正を目的のプログラム
（ワンクリック、フィッシング、
スパイウェア等）

はじめに.

１. コンピュータとは何か

２. 被害の種類

３. リスク・脅威の内容

４. セキュリティ対策

資料.

コンピュータウィルスによる被害１.

いたずら、愉快犯

数は多いが、
もはや古典的

- 不快な内容が表示される
- 改ざん（データ書換え）
- ファイル破壊
- パソコンが使用不能
- 悪事への加担者（加害者）にされる
  （メール発信、ｻｰﾊﾞｰ攻撃）

コンピュータウィルスによる被害 2.

金銭奪取など悪質化・専門化

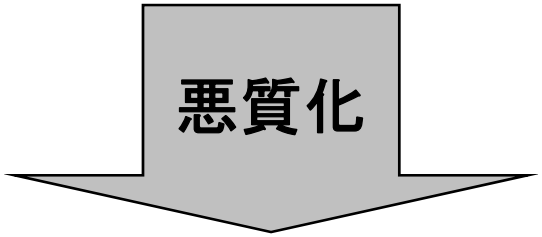
- 情報の盗難
  （名簿の転売目的、ゆすり）
- 金銭を盗まれる
  （キャッシュカードを使われる）

現在では、
典型的な経済犯

迷惑メールによる被害

金銭奪取など悪質化・専門化

- 削除にムダな時間がかかる
- 迷惑メールで通信料金が増える



- ワンクリック詐欺にかかる（金銭の要求）
- 偽装Webサイトに連れて行かれる（フィッシング）
  （個人情報を入力させられる）
  （キャッシュカードを使われる）

スパイウェアによる被害

金銭奪取など悪質化・専門化

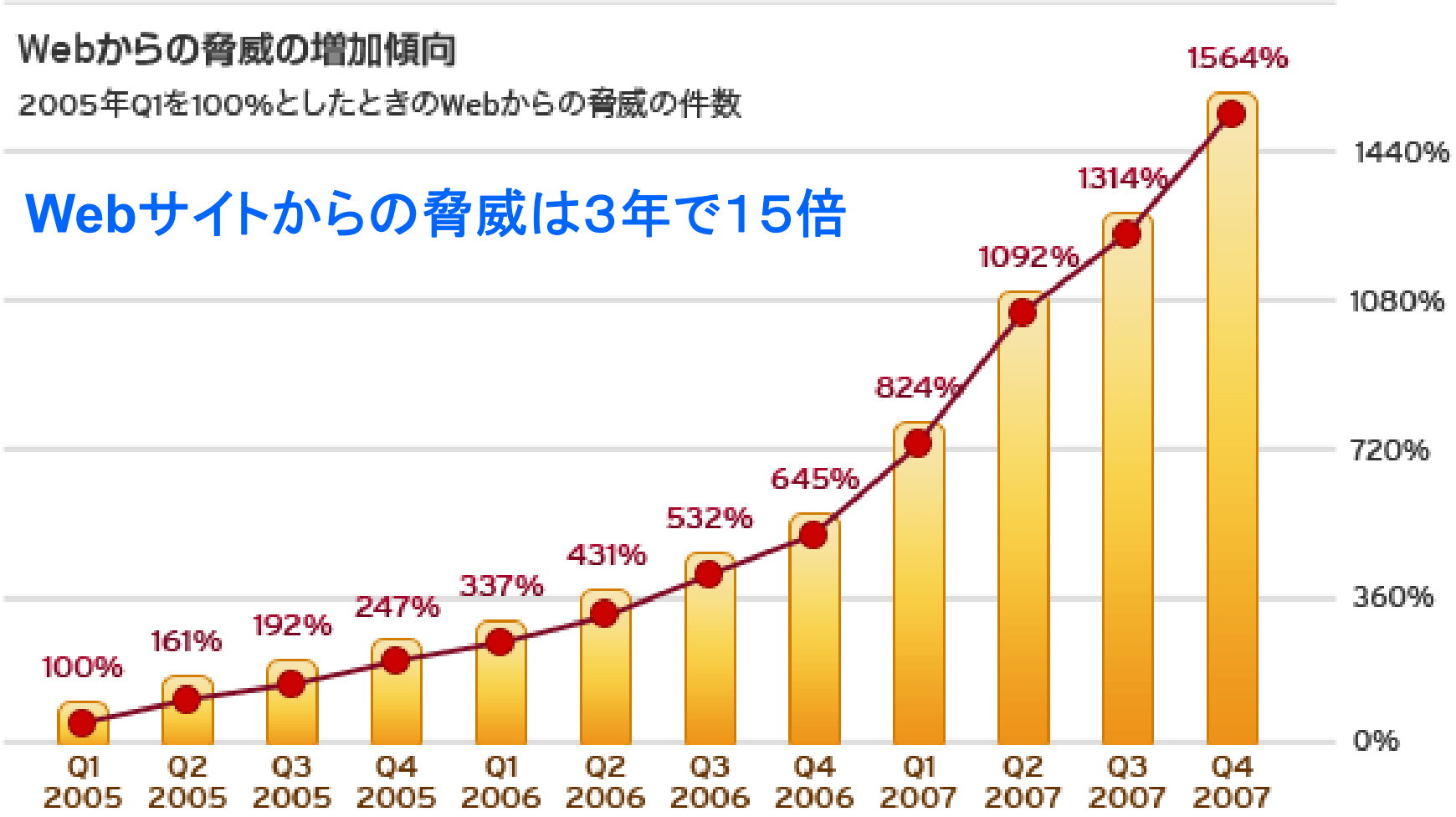
- 個人のパソコン情報の収集（OSの種類）
- パソコンの操作内容（企業のマーケッティング）

悪質化

- 個人情報の収集、同情報の販売（裏社会）
- 銀行口座番号、パスワードの詐取

Webサイトの脅威

（出典：トレンドマイクロ社）



ウィルスの種類

★ファイル汚染型 ウイルス

拡張子COM、EXE、SYSなどの実行型ファイルに感染するウイルスです。ウイルス単体でプログラムを実行したり複製するのではなく、EXEやCOM等の実行型ファイルに付着して制御を奪い、プログラムを書き換えて感染増殖します

★VBスクリプト型（マクロ型）ウイルス

マイクロソフト社のOffice製品（Word、Excel、PowerPoint、Access）のマクロ機能を利用して感染を広げるタイプのウイルスです。機種やOSに依存せず、かつ汚染されたファイルを開いただけで感染するため、非常に注意が必要です。

★ダイレクトアクション型 ウイルス

以前、世間を騒がせた「Nimda」などのウイルスを「ダイレクトアクション」型ウイルスと呼びます。本来ウイルスはプログラムの一種ですので、起動しなければ感染しません（VBスクリプト型などのマクロウイルスは別です）。しかしこのウイルスはOutlookExpressのセキュリティホールを巧みに突き、ウイルスに感染したメールをOutlookExpressでプレビューしただけで感染します。

平均45分毎に生まれている。

★トロイの木馬

基本的に、ほかのファイルやシステムに感染活動を行わない、つまり増殖を目的としない不正プログラムのことを「トロイの木馬」と呼び、ウイルスと区別しますが、ウイルスの一種と考えても良いと思います。トロイの木馬は一見役に立つプログラムに見えるのですが、実際はセキュリティを侵害し、使用しているコンピュータに大きな被害をもたらすコンピュータプログラムなのです。

★ワーム

ワームとはコンピュータウイルスの様に破壊活動を行うプログラムです。広い意味ではウイルスの一種ですが、一般的なウイルスが何かのファイルに付着して感染を広めていくのに対して、ワームはそれ単体で感染を広めることが可能です。また大量に自己増殖することが可能で、ネットワークの低速化やトラフィックの増大を招くことがあります。

急増中

★ボット

コンピュータを破壊せずに外部から感染したプログラムを利用したり、不正にデータを抜き取ったりするタイプのものです。感染方法はセキュリティーホールなどを突いたり、実行型やマクロ型などのようにメールの添付されてものを実行することで感染することがあります。

悪事の裏組織

（出典：トレンドマイクロ社）

悪事の裏価格情報

インターネット裏社会で行われている犯罪の料金

犯罪サービス	料金
マルウェア*を誰かに1度インストールさせる	アメリカ:30セント、カナダ:20セント、イギリス:10セント、その他の地域で2セント
マルウェアの基本セット	1,000ドルから2,000ドル
マルウェアのオプショナル・サービス価格	20ドルから
エクスプロイト・キット*のレンタル(1時間)	0.99ドルから1ドル
エクスプロイト・キットのレンタル(2.5時間)	1.60ドルから2ドル
エクスプロイト・キットのレンタル(5時間)	4ドルから
AVベンダーに未検出の情報を盗めるトロイ*	80ドルから
DoS攻撃*	1日あたり100ドルから
10,000台の、既に仕掛けが施されたPC	1,000ドルから
盗んだ銀行アカウント情報	50ドルから
最新のe-mailリスト(有効かの確認は未だ)	8ドルから。有効確認済の場合は値段が高い

出典;Sample data from research on the underground digital economy in 2007

はじめに.
１. コンピュータとは何か
２. 被害の種類
３. リスク・脅威の内容
４. セキュリティ対策
資料.

３．リスク・脅威の内容

１）IT がもとから持っている問題
２）インターネットの問題
３）悪意による問題発生

1）IT がもとから持っている問題

① 機械の側面

- IT機械やプログラムには故障やミスがつきもの
- ITの適用範囲が広範囲になったがゆえに、
  停止時の悪影響も甚大になり、社会的な混乱を招く
  （エネルギー、通信、交通、金融 ・・）

② 人的側面

- SEの人材不足
  - SE育成の遅れ（とくに高度IT技術者が不足）
  - 2007年問題（大量退職）による慢性的なSE不足
  - 中国、インドに頼る状況（コトバの壁）
- 急速な技術進歩により、SE育成が追いつかない

（続き）IT がもとから持っている問題

③ 社会的側面

- デジタルデバイド
  - ITが使えない人が不利（雇用時の条件にもなる）
  - 先進国と途上国の格差が広がる可能性
- 人との接触が減少し、人間関係が希薄になる可能性
- 情報の洪水により、必要な情報を見落としがち
- ITによる業務の効率化により、
  - 単純事務作業の職場が減少

④ 文化的側面

- 英語圏中心のソフト
  - 言語の壁
  - 文字コードの制約（自国の文字が使えない）

（続き）IT がもとから持っている問題

⑤ 健康面

- 長時間使用では、電磁波の影響、眼精疲労、腱鞘炎
- ITの単純操作が続くと、脳への悪影響

⑥ パソコンの弱点

- はじめは個人のホビー目的のために開発された
- セキュリティ対策が後手に回った

SEが支えるIT社会

2000年問題

サーバーテロ

通信障害

オンライン停止

デジタルデバイド

情報漏洩

ウィルス

フィッシング

スパイウェア

破壊・改竄

システム・エンジニアだけでは無理

利用者によるセキュリティ対策

補足：IT技術者の不足

日本では、就職難でありながら、SE不足を海外に頼っている。

国策によって、IT技術者が偏る傾向にある。

- 米国（膨大な軍事予算、IT国家目標）
- ロシア（冷戦時の高度な軍事技術の応用）
- インド、中国での大規模なSE養成

  SE数と（大学理系卒業生）：推計

  - 日本　50万人（　1．2万人）、20万人不足
  - 中国　18万人（12万人　　）、42万人不足
  - インド　50万人（10万人　　）

- IT特化政策による国力増進策
  - イスラエル　（先端ソフトウェア、セキュリティ）
  - アイルランド（電子商取引の世界ハブを目標）

2）インターネットの問題

① 管理者不在の世界

- インターネットは、もともとミサイル攻撃を受けた時の迂回通信路確保という緊急対応策として生まれた。
  - 緊急時であり、セキュリティ対策が弱かった。
- 軍事外に適用したのは、研究者間の情報交換が利用の出発点であり、参加者の善意に依存した運営が基本。

その意味では、システム管理者不在の世界であり、ネット犯罪は、そこにつけ込まれている。
- 不正侵入、ウィルス、盗聴、悪徳商法

（続き）インターネットの問題

② ネットシステム技術の検証が弱い

- インターネット新技術を使ったシステム開発は、急ぐあまり、未成熟技術を使った。
- 従来のシステムとは別の開発チームであり、セキュリティ面での検証が弱かった。
- インターネット企業は急成長のあまり、ともすれば内部管理体制が弱く、管理の目が行き届かない面がある。

（続き）インターネットの問題

③ 有害コンテンツ

・世界中では膨大な数のWebサイト（１億）
・しかもインターネットは公道のようなもので誰でも通る
・有害コンテンツサイトは増加傾向
　（犯罪助長、暴力、猟奇、猥褻、自殺志願・・・）

④ 言いたい放題のメール、掲示板

・匿名で利用できるので、
・自由にモノが言える、発想が豊かになるが、
・逆に、無責任な発言がまかり通る （誹謗中傷、無責任な噂）
・言葉だけが一人歩きし、語気、感情、ニュアンスを伝えにくい
　（誤解、行き違い、喧嘩が起きやすい）

（続き）インターネットの問題

⑤ ハイパーリンク

・インターネットが公道である以上、リンクは自由
・しかし、リンク先のWebサイトが有害である可能性がある
（リンクは、いわば、「書物のありか」を示しただけであり、
有害サイトにリンクを張っても、非難はされるが、
罰せられることは無い）
・信頼が置けるWebサイトのみにリンクを張るのが無難

⑥ プライバシーの侵害

・個人情報が大量に、容易に持ち出される。
・コンピュータを使えば、個人情報を蓄積できる。
XX情報、〇〇情報を氏名、年齢、生年月日、
性別、住所で照合（名寄せ、マッチング）すれば、
簡単に結合でき、
しかも短時間で大量にできる。

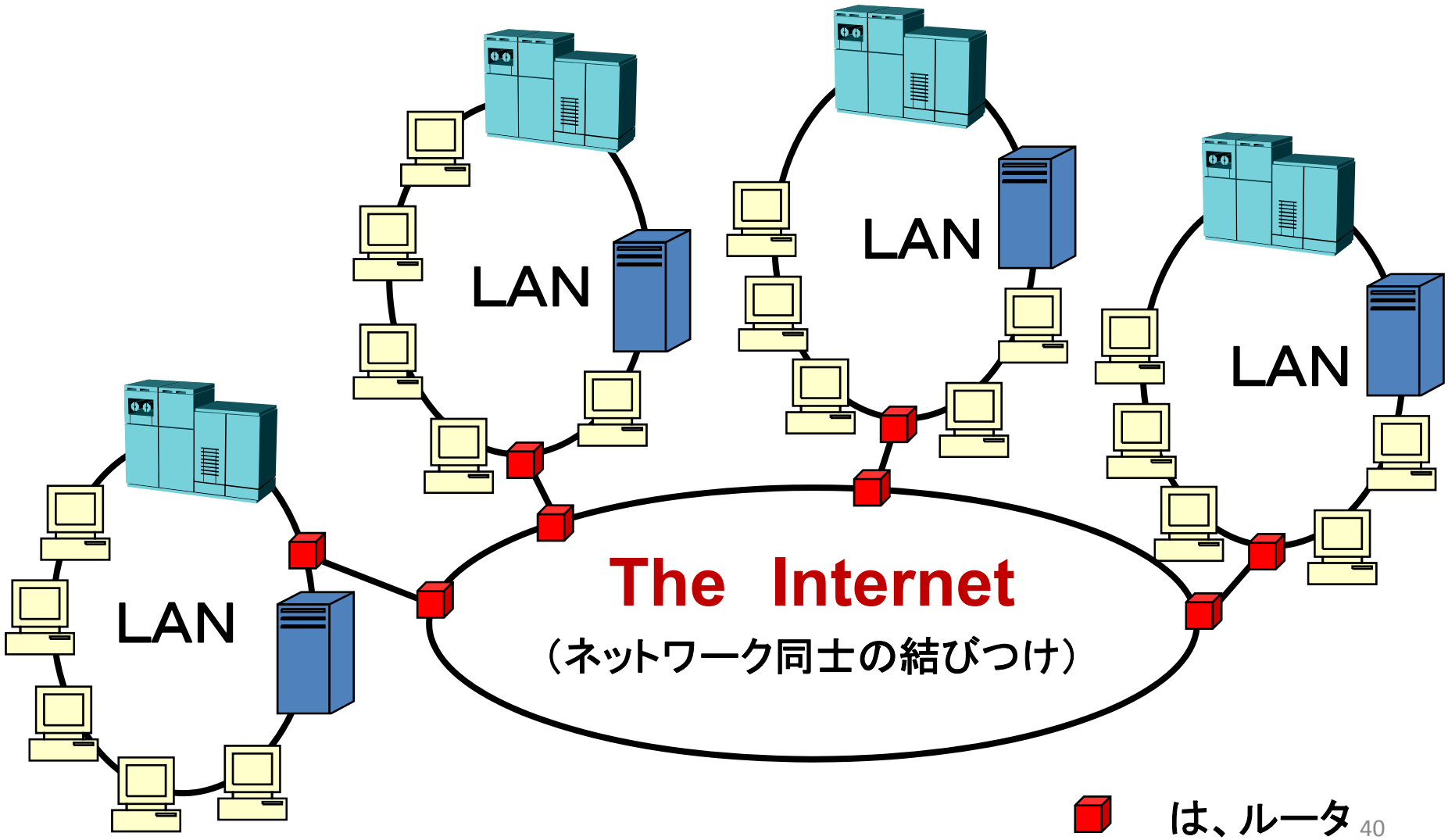
（続き）インターネットの問題

⑦ 知的所有権の保護

- 簡単にコピーできる、コピーしても減らない。
- マスコミのようなデスク、編集者のチェックが無く、知的所有権を保護しにくい領域である。

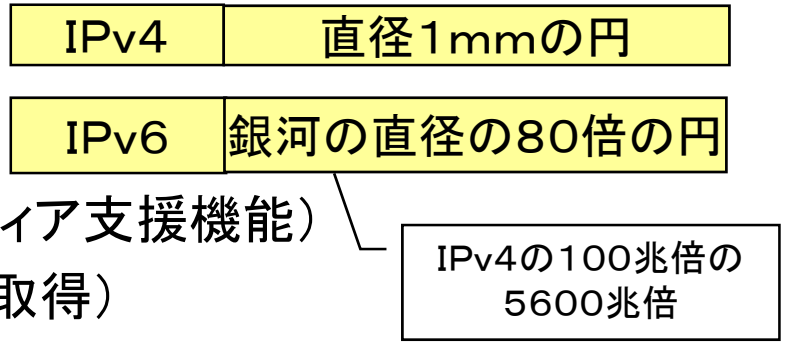
補足： インターネットの定義

・世界的規模で、通信ネットワーク同士を結んだもの
・通信ネットワークのネットワークとも言う（通信網のひとつである）



補足：IPv6とは

- 現行のインターネット・プロトコル第4版（IPv4）は、
  - ドメインの上限が、2の32乗（43億）→2008年前後にパンク
  - 暗号化／復号化機能なし
- 第6版（IPv6）では、
  - 2の128乗まで可能（43億の4乗）
  - 認証、データ暗号化を持つ
  - パケットのリアルタイム処理（マルチメディア支援機能）
  - プラグアンドプレイ接続（ドメインの自動取得）



- 128ビットの割り振り方
  - TLA（Top Level Aggregation）、13bit、世界規模のISP識別
  - NLA（Next Level Aggregation）、24bit、ISP傘下の組織用
  - SLA（Site Level Aggregation）、16bit、組織内のサブネット用
  - ｲﾝﾀｰﾌｪｲｽID（固有のアドレス）、 64bit

（参照：IPv6のビデオ紹介 http://contents.pr.v6pc.jp/
ITスクウェア IPv6オンラインジャーナル http://www.sw.nec.co.jp/IPv6/ ）

3）悪意による問題の発生

① 悪意による問題の特徴

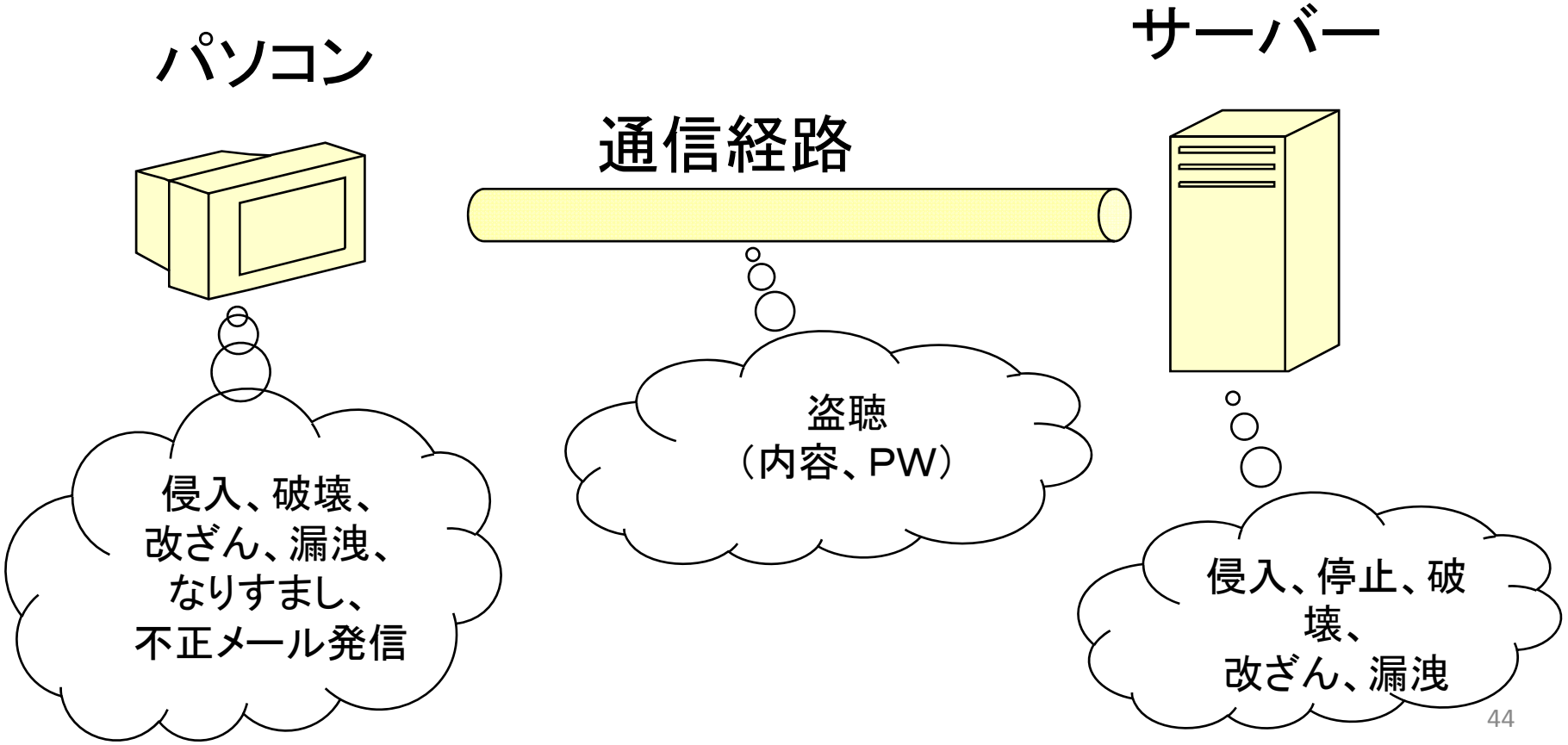
- 電磁的な手段の犯罪は、気が付きにくい
  - ・カードの偽造、指紋の偽造
  - ・取り締まる法令が、後追いになる
- インターネットは自由空間であり、統制しにくい
  - ・無法地帯になりがち（ネット詐欺などの悪徳商法）
  - ・有害Webサイトの増加（暴力、残虐、アダルト・・・）
- IT犯罪には国境が無い
  - ・通信やインターネットには、もともと国境が無い。
  - ・海外からITを悪用した大規模な犯罪が発生
    - ・ロシア、中国、インド、ブラジル発が多い

- 犯人は、捜査当局以上の専門知識を持つ
  - 並外れたIT技術を駆使（クラッカー（破壊者））
  - 破壊活動（サイバーテロ）、盗聴、通信傍受
  - 何重にも他人のコンピュータを介して攻撃するので、
    突き止められるのはマレ。
- 犯罪の規模が非常に大きい
  - 大規模な個人情報漏洩、
  - 広範囲なネット詐欺
- 組織的犯罪に変容している
  - 個人から、専門化集団になり、役割分担で動く
  - 強いて言えば、オレオレ詐欺集団や麻薬組織に類似

（続き）悪意による問題の発生

②　不正はどこで起きるか

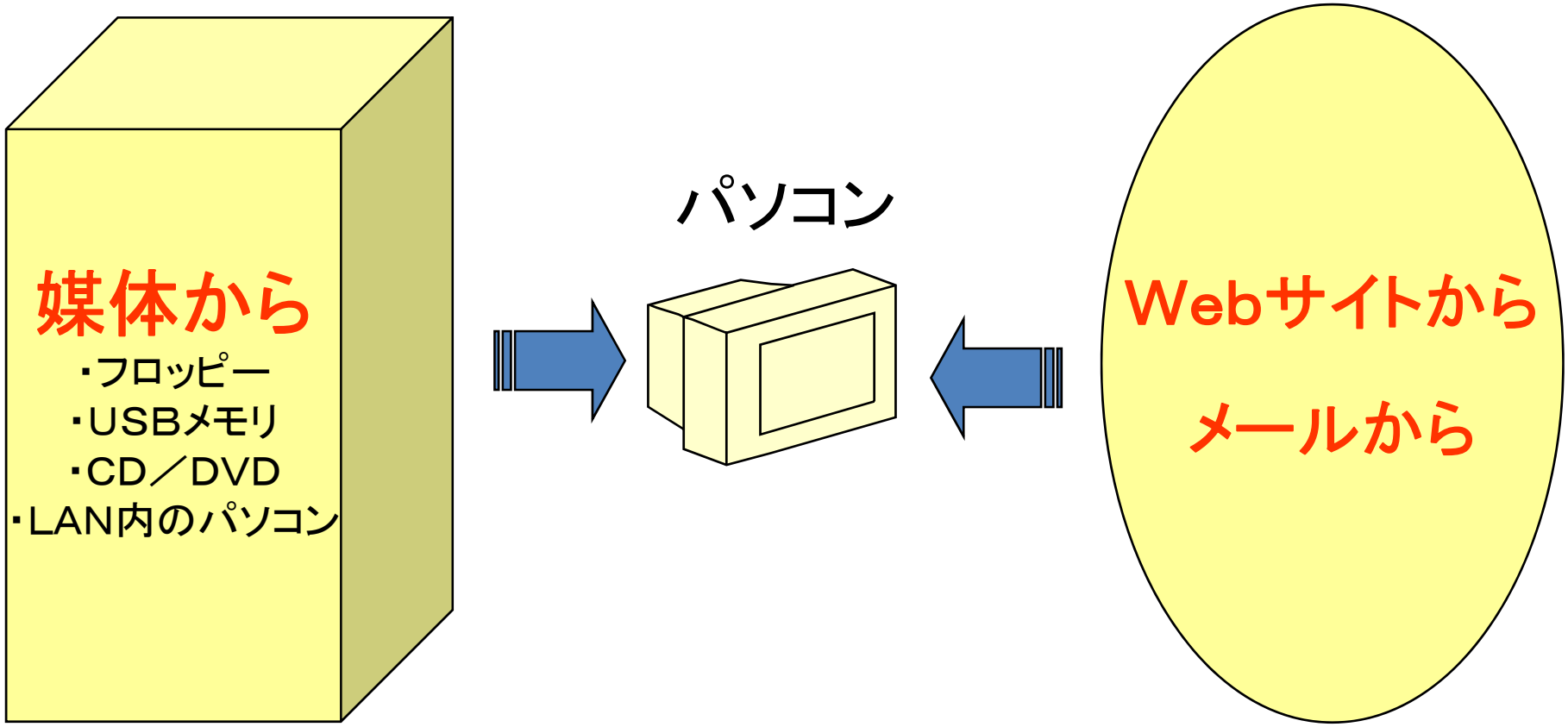
データの入力から経路、処理までの全てで起きる可能性がある



（続き）悪意による問題の発生

③ ウィルスははどこから入るか

媒体とインターネットから入ってくる。



（続き）悪意による問題の発生

④ ウィルスはどうやって入るか

- ソフトは人手で作成しており、欠陥が狙われる
- この欠陥は、鍵が無いドアや窓のようなもの
  - OS（Windowsなど）
  - ブラウザ（インターネットネットエクスプローラ）
  - メールソフト
  - Officeソフト（Word、Excel，PowerPointなど）

  - マイクロソフト社以外のOSやソフトにも欠陥はあるが、利用者が少なく、つまりマーケットが狭いので、それほど狙われていないだけ。

スパムメールが入口

- 突然メールが送られてくる。
- これが、不正の入口になっている。
  - 個人情報収集
  - スパイウェア
  - ワンクリック詐欺
  - フィッシング詐欺
- 収集した個人情報は、業者間でたらいまわし。
- 非常に巧妙な手段が講じてある。
  - 当選しました、50万円さしあげます
  - メールが不要なら、〇〇まで返信して下さい
  - 疑問は、△△までお問合わせ下さい
  - このメールは不審なメールではありません
  - 詳しくは、このホームページをご覧下さい
- この手のメールは、無視し、すぐに削除

補足:送信者を隠す方法

- メールの送信者名を任意に変える
  メールソフトの設定で容易に変えられる
- 無料メールを使う
  一時的に使われた場合は、追跡が困難
- インターネット喫茶からメールする
- 外国のプロバイダを経由する
- 善意のリメーラーを間に介す
  （本来は言論弾圧がある国向けのボランティア用）

（補足）その他 悪徳商法の手口

- 仕事の紹介－－－－ホームページ制作など
- 商品販売－－－－－欠陥商品の売りつけ
- マルチ商法－－－－ネットでネズミ講のさそい
- オークション－－－－商品違い（旧式、模造品）
- ワンクリック詐欺－クリックだけで入会料金を請求
- フィッシング詐欺－金融口座のID、PW入力指示
- 当選通知詐欺－－手付け金、車両登録費用、運送費の詐欺
- 個人情報収集－－メール受信拒否の返信をさせる
- 出会い系サイト－－言葉たくみに他所に呼び出す
- アダルト－－－－－国際回線への自動接続（法外な料金）

知らない人から、
うまい話が自分
に回ってくるわけ
が無い　!!

上記は、詐欺であり不正行為ではあるが、ウィルスとは言わない。

補足：ウィルス

・コンピュータウィルスの略称
・ネットワークや電子媒体を通してコンピュータに入り、
　ディスクの内容などを破壊するプログラムである。
・感染経路は、
　・Webサイトや、メールの添付ファイル
　・HTML形式のメールの本文
　　（危ないサイト→無名の無料スクリーンセーバー、音楽ダウンロード、
　　無料のオンラインゲーム、ポルノ、賭博など ）
　・電子媒体（USBメモリ、CD－ROM、フロッピーディスク）
・ワクチンプログラムで防御可能だが、間に合わない場合あり。

補足：ワンクリック詐欺

- ホームページで画像、入口などクリックしただけで、
  会員として入会した扱いになり、料金請求画面が出る
- よくあるWebサイト
  - 出合い系、ポルノ系（最近では情報提供系も）
- 手口が巧妙
  - 気が付きにくい個所に細かな入会案内あり
  - 個人情報取得済みの画面が出る
  - スパイウェアが入り込むWebサイトもある
  - メール、掲示板、ブログでWebサイトに誘う
- 個人情報は取られていない
  - 実際は、IPアドレス、プロバイダ名程度であり、
  - 特定できる個人情報では無い
- 絶対に個人が分かる情報を送らないこと
  - 確認、問い合わせ、入金をしない
  - 無視するのが一番

補足：フィッシング詐欺

- 本物そっくりの偽メールや偽サイトを使って
  ユーザーをだまし、
  - パスワードやクレジットカード番号、個人情報
    などを盗み取るオンライン詐欺

本物のメール、本物のホームページを見抜く知識が必要

パスワードなどを入力させる本物のブラウザ画面では、
通常、右下の鍵マーク（電子認証付き）があり、安心できる

補足：スパイウェア

・元来は、アフターサービス向上のために、パソコンを使うユーザの操作、
　OS情報、個人情報などを収集するソフトであり、
　得られたデータはマーケティング会社などに送られる。
・米国で、個人情報保護の観点から、問題視されはじめた。
・近年は、金融関係のID、パスワードを盗むなど悪質なものが増えている。

設置手段：
　・スパイウェアは他のアプリケーションソフトとセットで配布され、
　・インストール時にはそのソフトと一括して利用条件の承諾などを求められる。

稼動：
　・ウィンドウなどを表示せずにバックグラウンドで動作するため、
　・ユーザはスパイウェアがインストールされていることに気づきにくい。
　・悪質なものは、入力情報を盗み、他に送る（銀行口座番号、パスワードなど）

違法では無い：
　・利用条件の承諾する場合は、スパイウェアの活動は違法とまでは言えない
　　（ほとんどのユーザはスパイウェアに気づいていない。）
　・ただし、個人情報、パスワードなどを盗むことは、違法

対策：スパイウェア駆除のためのフリーソフトがある。
　・Spybotのダウンロードhttp://enchanting.cside.com/security/spybot1.html
　・最近のウィルス対策ソフトでは、スパイウェア駆除機能が追加され始めた。
　・スパイウェア情報サイト　http://enchanting.cside.com/security/spyware.html　）

補足：ファイル交換ソフト

・P2P形態でのコンピュータ資源利用方法のひとつ（peer　to　peer）
　・本来は、対等の人同士の資源共有化（ファイル、プリンタなど）
　・ファイル共有ソフトともいう
　・楽曲の相互ダウンロード利用で爆発的に普及した
　　・欧米：Napster、Gnutella（グヌーテラ）
　　・日本：Winny
　　・共有してもよいファイルのみを、個人間で交換できる
　著作権侵害であり、利用禁止、刑事処分の動き
・このソフトに、以下の悪条件が重なれば、重大な情報漏洩を引き起こす
　・P2Pソフトにウィルスが入り込む
　・しかも、業務上の機密情報をパソコンに保存している
　　（私用パソコンには、普通は、この手の情報は持っていないハズ）
・情報漏洩事件が続発
　・2005年12月、関西電力、原発の安全基準、技術資料
　・2006年2月、陸・海・空自衛隊、訓練文書、コールサイン、模擬テスト、隊員名簿
　・2006年3月、各地の県警、捜査資料
　私物パソコンを業務に私用せざるを得ないことが原因！！

目次

４．セキュリティ対策

１）個人による対策
２）組織による対策

もともとの問題点への対応策

この問題は、政治、経済、社会的な観点から解決すべきものである。

問題点	解決策
①故障、バグ	代替マシン、テスト充実、コスト負担
②SE問題	海外SEの活用、アウトソーシング、 退職者の再雇用、e-ラーニング
③デジタルデバイド	ユニバーサルデザインの実現 機器の貸与、通信料金の無料化
④英語中心の世界	自動翻訳の実用化、文字コード豊富
⑤健康	電磁波の遮蔽技術、脳の活性化策
⑥インターネット	暗号化、電子認証、自衛手段 通信回線の専用線化、複線化 有害サイト遮断、IPv6への早期移行

１）個人による対応

悪意を持ったIT専門家に個人で対抗するのはそれほど簡単なことではない。

しかしながら、脅威をゼロにはできないが、
損害を小さくはできる。

悪意による問題への対応策

	問題の発生	対策
①不正侵入 （ｸﾗｯｶｰ）	侵入、破壊、改ざん、 漏洩、なりすまし	・OSの更新 ・ファイヤウォール ・パスワードの工夫 ・データのコピー、BU
②ウィルス、 ワーム	破壊、改ざん、 不正メール発信	・OSの更新、対策ソフト ・不審なメール、HPを無視 ・データのコピー、BU
③盗み、盗聴	情報漏洩、 スパイウェア	・キャッシュカードを使わない ・データの暗号化、対策ソフト
④悪徳商法	詐欺、フィッシング 個人情報入手	・うまい話に乗らない ・不審・有害なメール・HP無視
⑤いたずら	誹謗、中傷される 迷惑メール	・不審掲示板に書かない ・実名、住所を明かさない

容易に出来ることを習慣づける1.

・ファイヤウォール（ソフト防火壁）

・WindowsXPから標準装備

・フリーソフト（Sygate　Personal　Firewall）

・アンチウィルスソフト

ネット接続の有無にかかわらず。

・プロバイダのセキュリティサービスに加入

（有料、ウィルステーブルの更新不要）

・ウィルスバスター、Norton、マカフィ（有料）

・カスペルスキー、ESET（有料）

・AVG Anti-Virus（無料）、　avast！4（無料）

容易に出来ることを習慣づける2.

- データのコピーとバックアップ
  - 媒体を変えて複数採る
- 類推しにくいパスワードを設定する
  - 簡単なパスワードにしない（特殊文字も使う）
  - パソコンに起動パスワードを設定
  - パスワード付きのスクリーンセーバ
  - 機密ファイルの保管時にパスワードを設定
- 不審なメール添付ファイルを開かない
- メールはテキスト形式にする
  - HTMLメールは防御が弱い

容易に出来ることを習慣づける

- ・システムの脆弱性を補強
  - ・Windows　Updateの励行
  - ・バージョンアップ
    - ・OS、ブラウザ、メールソフト
    - ・Officeソフト
- ・ネット上になるべく個人情報を置かない
  - ・ハンドルネームにする
- ・信頼できるサービス事業者を利用
- ・インターネット喫茶を利用しない
  - ・個人情報は絶対入力しない
  - ・入力情報は全て盗まれる前提で利用すること
- ・パソコン廃棄時は、データ領域をオールゼロに。

補足:パスワードの設定方法

1） ユーザーIDをむくまないこと
2） 記号を含むこと
3） パスワード破りに使われる頻度が少ない記号を使う {fumio} 〈fumio〉
4） 8桁以内の初めのほうに記号を入れる

理由:長いパスワードを設定しても、Webサービスによっては8桁しか使われていないものがある。

5） 語呂合わせで覚えやすくする

suetsugufumio→stgfm→:stg@fm ＜stg＜fm ！stg！fm

hiroshima→〈hr〈sm {hr{sm [hrsm]

6） 記号が使えなければ、記号部分を、覚えやすい数字に置き換える

9stg9fm

7hr7sm

補足:パスワードの設定方法

【使われない記号を入れる】

記号	割合(%)	記号	割合(%)	記号	割合(%)
-	62.8	'	1.9	,	0.1
$	5.2	:	1.7	]	0.1
@	3.9	(	1.6	~	0.0
#	3.7	)	1.5	<	0.0
!	3.5	+	0.8	>	0.0
%	3.3	?	0.6	|	0.0
^	3.1	;	0.4	{	0.0
*	2.7	"	0.3	}	0.0
&	2.7	=	0.2	[	0.0

この部分の記号を使うと良い

補足：ファイヤウォール（防火壁）

・外部の悪意の侵入者から、コンピュータシステムへの
　侵入を防ぐためのしくみ。（ただし、メールは通す）
・企業では、内部から外部への情報の流出も防止できる。
・決めたルールに基づいて、通過を制御する。

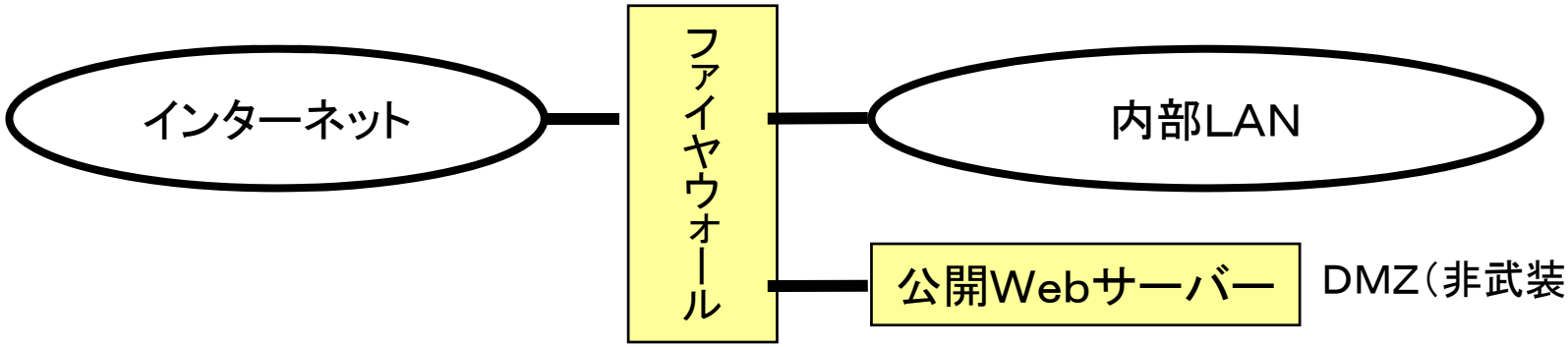
①パケット・フィルタリング方式

・ネットワーク層で動作

・送信元や送信先のIPアドレス、ポート番号などで判断する

②アプリケーションゲートウェイ方式

・アプリケーション層で動作
・通信を中継するプロキシ（代理 Proxy）サーバを設置
・社内ネットワークとインターネットの間で直接通信をできないようにする



2）組織による対策

ポイント：

- 情報資産を、管理状態に置く
  - セキュリティ管理者の設置
    - 情報入手、情報の共有化（メール等で）
  - ネットワーク
  - パソコン
    - 機種選定、ソフト選定
    - ウィルス対策ソフトを全パソコンに設定
    - 同ソフトの更新状況の把握
  - プロバイダのセキュリティソフト使用
  - 定期点検
    - WindowsUpdate実施状況
  - 電源オフの励行
    - 就業後、休日、長期連休

2）組織による対策

その他：

① セキュリティ・ポリシーを規定
- セキュリティを優先する基本方針
- 個人情報保護の方針

② 入室制限（コンピュータ室、事務室）

③ 重要データは、暗号化する。
- データバックアップを採り保管場所を変える。

④ 端末起動時の制限
- パスワード、指紋検証
- パスワード付きのスクリーンセーバ

⑤ データのアクセス権限を制限
- 職務に応じた権限付与、外注先の人も同様
- 重要データは、都度の申請・許可方式
  （常時アクセス権を付与しない、期間限定とする）
- 重要データの利用制限
  - 個人情報、財務情報、機密情報
- 異動時、退職時は削除

（続き）組織による対策

⑥ その他種々の対策

- 社員教育
- 私物パソコンを持ち込ませない
- 監査を受ける（内部監査、外部監査）
- アクセスログ（記録）は長期保管
- 情報漏えい防止ソフトウェア

以下は大組織で考慮要

- 監視カメラ設置（心理的効果）
- 外部とのアクセス管理（ファイヤウォールサーバ）
- 企業用の電子認証システムの導入
- 公的なセキュリティ認定を受ける
- 最高機密用コンピュータはネットワークに繋がない

参考：セキュリティの３要素

- Confidentiality（機密性）
  - 盗聴、漏洩の防止
- Integrity（完全性）
  - 改ざん、なりすましの防止
- Availabirity（可用性）
  - データ破壊、改ざん、停止の防止

補足：ITと法的責任

- 汎用コンピュータと、OS
  - もともと故障、バグがあるのが前提で使用している。
  - 特定目的の製品ではなく、ミスによる損害が起きても責任は問えない。（製造物責任の範囲外）
  - 非難はされても厳密な刑事罰は問えない。
  - 製品スペック（仕様）であると言われれば、それまで。
- 専用のコンピュータ製品
  - 用途が限られるマイクロチップが組み込まれた製品は、ミスによる責任が問われる。（製造物責任あり）
  - 例示：自動車、家電製品、医療器械

ソフト（適用プログラム）は、業務そのものまたはその代行であり、業務上の過失責任が問われる。
（銀行口座残高の消滅など）

資料：公的な倫理規程

以下に、学会などでの倫理規定、倫理綱領の抜粋を示す。
いずれも、知的財産権、プライバシーの尊重を会員向けに規程している。

・情報処理学会
　・他者の人格とプライバシーを尊重する。
　・他者の知的財産権と知的成果を尊重する。
　・情報システムや通信ネットワークの運用規則を遵守する。

・電子情報通信学会
　・他者の権利の侵害が生じることを避ける。
　・他者の権利には、所有の権利、プライバシーの権利等が含まれる。
　・他者の創意工夫を尊重する。
　・著作権、特許権、その他の知的財産権を侵害しない。
　・他者の管理するシステムに許可なく侵入しない。
　・他者の通信に不正にアクセスしない。

・精密工学会
　・他者の尊重と謙虚な姿勢
　・他者の生命，財産，プライバシーを尊重するとともに、
　・専門職務上の主張や判断をする時には、
　・常に事実にもとづいた行動をとることを心がけ、
　・他者の意見，主張，批判などを謙虚に受けとめる。
　・他者の業績である知的成果ならびに知的財産権を尊重する

資料：セキュリティ認定制度

・プラーバシーマーク認定制度
  ・個人情報の管理、体制、責任者のレベルを評価し認定
  ・個人が、業者の管理水準を判断しやすくなる
  ・（財）日本情報処理開発協会
・情報セキュリティ監査制度
  ・製品評価技術基盤機構（NITE）
  ・企業の部分的なセキュリティも評価対象可能
  ・政府調達のIT製品（機器、システム）の認定にも使用
・「ISMS適合性評価制度」の認定業者を選択
  ・（財）日本情報処理開発協会
  ・方針、技術、組織、運営面からセキュリティ総合評価
  ・世界標準、JISに準拠
  ・第三者の審査機関による審査
  ・Infomation Security Management System
    （http://www.isms.jipdec.jp/lst/ind/index.html ）

NITEは今のところ
認定マーク無し

資料：政府のセキュリティ対策

- IT戦略本部のもとに、情報セキュリティ政策会議を設置
  - 『ITを安心して利用できる環境を構築する』
  - 『ITの利便性とセキュリティの両立』
  - IT戦略本部（＝高度情報通信ネットワーク社会推進戦略本部）
  - 情報セキュリティ政策会議は、内閣官房長官が主催
    - 事務局は、内閣官房情報セキュリティセンター(NISC)
    - 政府機関統一セキュリティ基準の設定
    - 有効なセキュリティ対策の実施、監査
    - ４領域の対策強化
      - 政府・自治体、重要インフラ、企業、個人
    - 重要インフラ１０分野へのサーバーテロ対策
      - 電力、ガス、水道、医療、鉄道、航空、物流
      - 金融、情報通信、行政サービス
    - セキュリティ技術推進、人材育成

（米国では、連邦情報セキュリティ管理法を既に設定。FISMA Federal Information Security Management Act ）

資料:IT安心会議

- 政府が、IT戦略会議の元に設置
- 正式名称は、
  インターネット上の違法・有害情報等に関する関係省庁連絡会議
- 2005年2月、発足
  有害コンテンツ、フィッシング詐欺、の横行がきっかけ
- 事務局は内閣官房
  警察、総務、法務、経済産業など関係14省庁の課長級で構成。
- インターネットの普及に伴う
  違法・有害情報の入手の容易化や遭遇機会の増大等が、
  犯罪や財産権侵害、人権侵害等のITに関連する新たな
  社会問題の発生を助長していることへの対応策を検討

- 対策
  フィルタリングソフトの普及策、プロバイダ自主規制、モラル教育、
- ネット利用者にもホームページを通じて情報提供している。
  （http://www.kantei.go.jp/jp/singi/it2/others/itanshin.html）

資料IT基本法の制定

「高度情報通信ネットワーク社会形成基本法」（2001年成立）

1．目的

高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に推進する

2．定義

「高度情報通信ネットワーク社会」とは、
インターネットその他の高度情報通信ネットワークを通じて
自由かつ安全に多様な情報又は知識を世界的規模で入手し、共有し、又は発信することにより、
あらゆる分野における創造的かつ活力ある発展が可能となる社会をいう。

3．基本理念

高度情報通信ネットワーク社会形成の意義

- すべての国民が、高度情報通信ネットワークを容易にかつ主体的に利用する機会を有し、
- その利用の機会を通じて個々の能力を創造的かつ最大限に発揮することが可能となり、
- もって情報通信技術の恵沢をあまねく享受できる社会を実現

基本的視点

- 経済構造改革の推進（電子商取引の促進、新規事業の創出）
- ゆとりと豊かさを実感できる国民生活の実現（低廉・多様な情報サービス）
- 個性豊かで活力に満ちた地域社会の実現（地域における就業機会の創出、多様な交流機会の増大）
- 民間主導を原則としつつ、国等が公正な競争の促進等環境整備を行う適切な官民の役割分担
- 情報通信技術の利用の機会及び活用能力の格差の是正（デバイド対策）
- 雇用等新たな課題への対応

「他の関連法令」

電子署名法、電子帳簿保存法、個人情報保護法

（参考：IT基本法　http://www.kantei.go.jp/jp/singi/it2/hourei/index.html　）

資料：e-Japan戦略と法律

IT社会実現のための最低限必要な法令は、急速に整備が進んだ。
後は、どういう社会にするのか、その促進のための整備が未だ。

- 1999年、住民基本台帳法の改正
  - 住民コードを用いた住民情報の全国的ネットワークの整備
- 2001、IT基本法
  - 全ての国民が情報通信技術の恵沢を享受できる「高度情報通信ネットワーク社会」の形成
- 2001年、電子署名法
  - 電子文書等に記録された情報について本人による一定の電子署名がなされているときは真正に成立したものとする
- 2002年、行政手続きオンライン化三法
  - 書面で行う行政手続は、原則として全てコンピューターシステムを利用して行うことができること
- 2003年、個人情報保護法
  - 個人に帰属、管理責任、流用禁止
- 2005年、電子文書法
  - 財務・税務関係の書類に、電子媒体を認める

資料：　個人情報保護法

- 時期：2003年5月成立、2005年4月から全面施行
- 理念：個人情報は、個人の人格尊重の理念の下に慎重に
  取り扱われるべきものであり、
  その適正な取扱いが図られなければならない。
  - 定義：個人情報とは、氏名、生年月日、身体、職業などの
    ことであり、特定の個人を識別できる情報である。
- 帰属と管理責任：

  個人情報は、「個人のもの」と規定」、
  企業に個人情報を預けてあり、企業には適正な管理責任
- 内容：不正の手段による個人情報の取得の禁止
  本人同意がない「個人データの第三者提供」の原則禁止
  本人からの求めに応じ、開示、訂正、利用停止
- 個別の法令化検討中：
  医療、金融、通信分野は、情報流出時の影響が大きく、
  情報窃盗罪も検討中。

資料：個人情報保護の指針

- 2004年6月、違反は処罰対象
  - 企業が持つ個人情報が流出した際には、
  - 改善命令や罰金など処罰を科す（個人と企業の両罰規程）
- 氏名や住所のデータ、防犯カメラに映った映像などが個人情報に当たると明記
  - 個人の身体、財産、職業などに関する事実情報
  - 評価、判断を表す全ての情報
  - 職員録、従業員名簿も対象
- 「5000人以上の個人情報」を管理している企業が対象
- 社員だけでなく、アルバイト、派遣社員、アウトソーシング先も管理義務を負う。
  - 管理責任者を設置
  - 雇用契約に秘密保持義務を明記
  - 目的以外の利用禁止
- 情報流出時は→経産省が改善勧告→改善命令→懲役、罰金

資料：個人情報保護法の対象

	対象	対象外
名簿	氏名・住所・職業 身体の情報	市販の電話帳
名刺	体系的に整理されたもの	未整理、独自に分類したもの
ﾒｰﾙｱﾄﾞﾚｽ	名前、所属がわかるもの	一連番号などで個人が特定しにくいもの
映像	本人が識別できるもの	不鮮明な映像
アンケート回収用紙	分類されたもの	未整理で全く分類されていないもの

資料:管理責任

組織	基本	その他
国	・保有する個人情報の保護	・所管業界向け指針の作成
地方公共団体	・保有する個人情報の保護	・住民への広報 ・住民からの相談受付
企業・団体	・保有する個人情報の保護	・従業員の啓発

資料：個人情報保護の所管官庁

分野		所管官庁
医療	医療一般	厚生労働省
	研究	文部科学省・厚生労働省・経済産業省
金融・信用	金融	金融庁
	信用	経済産業省
情報通信	電気通信	総務省
	放送	総務省
事業全般		経済産業省
雇用管理	一般	厚生労働省
	船員	国土交通省
警察		警察庁
法務		法務省
財務		財務省
教育		文部科学省
福祉		厚生労働省
職業紹介など		厚生労働省
労働者派遣		厚生労働省
国土交通		国土交通省
農林水産		農林水産省

（出典）内閣府国民生活局企画課個人情報保護推進室「個人情報の保護に係る関係省庁の検討状況」）

資料：　知的所有権の保護法

- 知的所有権の対象
  - 発明、商標、著作物など
  - 人間の知的生産物であり、物理的に支配できない
  - 知的財産権、無体財産権ともいう
- 知的所有権の種類
  - 工業所有権
    - 特許権（発明のこと。特許出願日から20年間有効）
    - 実用新案権（物品の形状・構造。出願日から6年間）
    - 意匠権（物品のデザイン 。登録日から15年間）
    - 商標権（商品識別標識。登録日から15年間。延長可能）
      （商品名、社名、ロゴマーク、芸名、ペンネームなど ）
  - 著作権
    - 著作物が対象
    - 存命中および死後50年間有効
    - 会社名義で公表された著作物は、公表から50年間有効
  - 企業秘密
    - 技術情報、営業情報、顧客情報など
    - 守秘義務がある（合理的で特約があれば退職後も一定期間、継続）

資料：著作権

・著作物に関して、以下の三つの権利の総称
  ・著作者人格権（公表権、氏名表示権、同一性保持権 ）
  ・著作財産権（複製権、貸与権、翻訳権、翻案権、公衆送信権 ）
  ・著作隣接権（実演家、レコード製作者、放送事業者の権利）

注１：他人の著作物をコピーしてホームページに掲載するのは「公衆送信権」を侵害し、禁止されている。

注２：引用は、以下の条件を満たせば、著作権侵害にはならない。

> ・論旨と密接な関係があるなど引用する必然性がある
> ・出所の明示がなされている
> ・自分の著作物が主で、引用が従である
> ・自分の著作物と引用が明確に区別されている（「　　」で囲む等）

注３：個人的使用の範囲であれば、コピーは禁止されない。

・著作物とは、
  ・言語著作物（小説、脚本、論文、講演、ホームページ、メモなど）、プログラム、図形、写真、音楽、映画、美術、地図、建築、舞踏など

・著作権は、
  ・登録の有無には関係なく、著作物の創作によって発生（無方式主義）
  ・ © マークがあれば、方式主義の国でも有効

資料：　その他の法令

① 不正アクセス禁止法

- 他人の識別番号を無断で入力や他人に提供する行為
  （ユーザーID、パスワード、合言葉など）
- セキュリティ・ホールを攻撃する行為

② 電子メール法

- 迷惑メールの発信は、処罰対象

③ プロバイダ責任制限法

- ユーザーの不正な情報を削除できる
- 権利を侵害された人は、発信者の個人情報開示を請求できる

④ プライバシー権

- 個人の情報をみだりに公開されない権利
- 氏名、住所、身体、職業、肖像、容姿、行動
- 依拠：憲法13条（個人の尊重、生命・自由・幸福追求の権利）

資料：　その他の法令

⑤クーリングオフ

・特定商取引法(旧訪問販売法)、割賦販売法 で規定

・ネットショッピング、通信販売はクーリングオフの対象外

⑥刑法

・電子計算機損壊等業務妨害罪

・電子計算機使用詐欺罪

・詐欺、名誉毀損、猥褻物、児童ポルノ禁止法など

⑦民法

・許諾契約違反、損害賠償など

・特定商取引法（価格、引渡し時期、返還方法などの明示）

資料：脳とコンピュータの違い

① コンピュータは、脳を越えられない

・コンピュータは解法を発案できない

・人間は自分で答えの出し方（解法）を考え出せる

・人間の持つひらめき、連想、創造力が、
　どこから生み出されているのか分かっていない。

・人間の脳のメカニズムの研究が先決
　（21世紀中は解決できない）

脳は、意欲で動くコンピュータ

人間は、意欲、欲求が満たされると→→快の感情になり→→知が働き出す。
コンピュータは、最後の「知」の部分の一部自動化をする。

『・人間は、私たちの“意”、すなわち意欲や欲求が満たされると、“快”な情報として受け取ります。反対に欲求が充足されないと、“不快”な情報として受け取り、回避や攻撃といった行動をあらわすようになる。
・この欲求は大きく分けると、第一次、第二次、第三次の欲求に分類できます。
・第一次欲求というのは個体や種族の維持欲求で、食欲とか性欲、睡眠欲と呼ばれる肉体維持の欲求（肉欲）です。さらに、強調したいのは、この肉欲以上に強い第一次欲求（遺伝的欲求）として、「人は自分の存在が他の人から意義深いと思われないと生きることができない」という精神的な欲求（精神欲）をもっているということです。すなわち、精神欲は肉欲以上に重要な原始的な欲求として人にそなわっており、この欲求が満たされないと人は生きられない。
・第二次欲求というのは社会的欲求で、仲間との関係、親子関係、ヒトとヒトの関係に対する欲求です。人間は1人では生きられません。ヒトとの関係で生きるのです。
・第三次の欲求とは知的な欲求です。芸術・科学・文化・哲学など美や知を求める欲求がある。
・これらの欲求が充足されたとき、ヒトは快と思い、充足されないときは不快と思うのです。それによって脳の活性化が調節されていくわけです。』

（出典：工業技術院 、松本元氏
http://www.hitachi-hitec.com/sapiens/002/ajsa0024.html ）

資料：ネット犯罪の相談窓口

- 全国警察ハイテク犯罪相談窓口等一覧
  http://www.npa.go.jp/hightech/soudan/hitech-sodan.htm
- 法律相談センター一覧
  http://www.nichibenren.or.jp/jp/hp/houritu/soudan/index.htm
- Web１１０番
  http://web110.com/
- 電脳ネット犯罪撃退教室
  http://www.joho110.com/index.html
- NPOシロガネサイバーポール（インターネット駆け込み寺）
  http://www.scyberpol.org/
- JPCERT コーディネーションセンター（セキュリティ事象）
  http://www.jpcert.or.jp/
- インターネット法律協議会
  http://www.ilc.gr.jp/index.htm
- 内閣府、国民生活政策ホームページ
  http://www5.cao.go.jp/seikatsu/index.html
- 国民生活センター
  http://www.kokusen.go.jp/ncac_index.html

参考書、参照Webサイト

・坂村　健「痛快！　コンピュータ学」　集英社インターナショナル
・菅野　文友「IT革命の光と影」 日本規格協会
・岡本茂ほか「パソコン用語事典」 技術評論社
・オールアバウト・ジャパン、セキュリティ　http://allabout.co.jp/computer/netsecurity/
・愛知大学　文字コード　http://taweb.aichi-u.ac.jp/saitom/mojicode.htm
・ITスクウェア　IPv6オンラインジャーナル
　http://www.sw.nec.co.jp/IPv6/
・JIPDEC、ISMS適合性評価制度
　http://www.isms.jipdec.jp/lst/ind/index.html
・Web110番　http://web110.com/
・日本ベリサイン社　http://www.verisign.co.jp/
・NDN社、電子認証講座　http://www.ninsho.co.jp/explanation/index.html
・セキュリティ・チェック・リスト　http://www.johokyoku.com/check/security.html