情報化の光と陰

（情報と社会　第１３回）

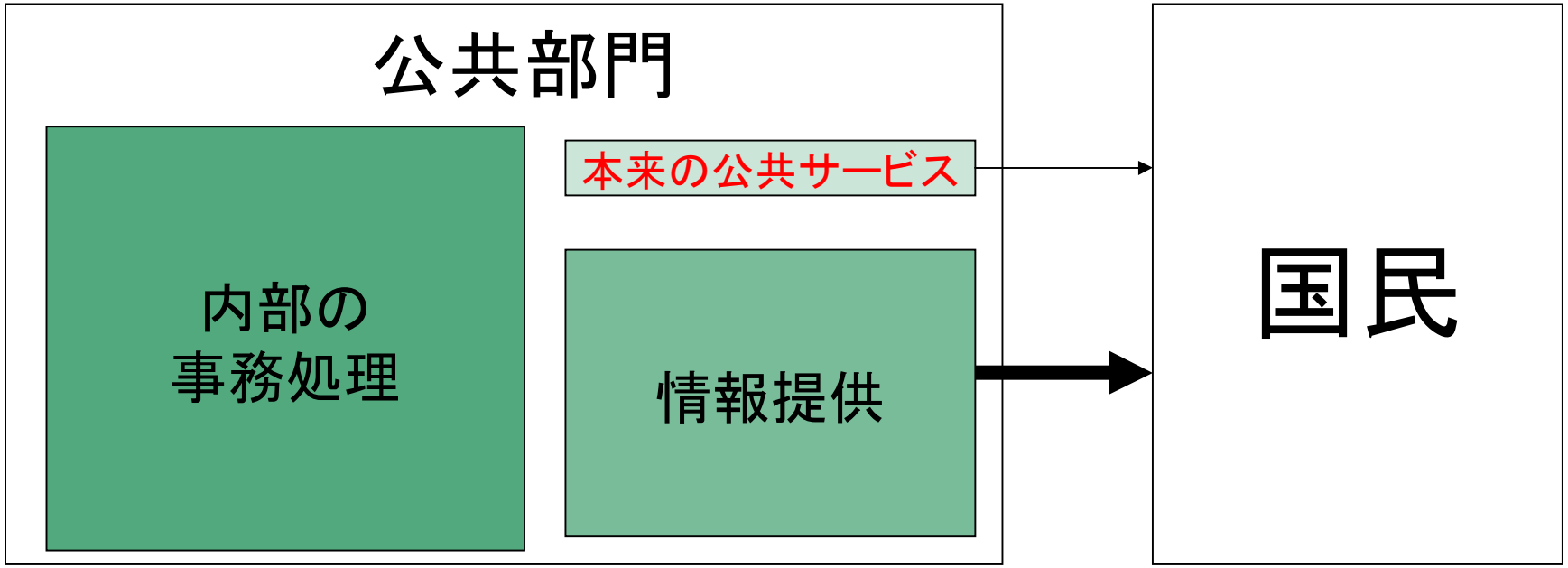
URL　http://homepage3.nifty.com/suetsuguf/

Email　fwhy6454@mb.infoweb.ne.jp

作成者　末次文雄

復習：公共部門のシステム化段階

- 部門内の事務処理のIT化は進んでいる。
- 国民への情報提供も急速に進んできた。
- 「本来の公共サービス」面は、今からの状況。
- 医療、教育、行政への適用の遅れが目立つ。



復習：ユニバーサルデザインの特徴

・発想の原点は、
「すべての人が人生のある時点で何らかの障害をもつ」
・はじめから、
障害の有無、年齢、性別、国籍、人種等に
かかわらず多様な人々が気持ちよく使えるように
あらかじめ、都市や生活環境を計画する考え方である。

・障害といっても、視覚、聴覚、肢体、体力、知的など、
さまざまな障害がある。
・同じ障害でも程度の差がある。
・また誰もが、怪我などで一時的に障害をもつ。
・言葉のわからない土地に行けば言葉不自由者となる。

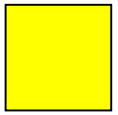
（参照：UDコンソーシアム　http://www.universal-design.co.jp/udc/udc.html
UD社　http://www.universal-design.co.jp/index.html　）

復習:「どこでもコンピュータ」の事例

ユビキタス

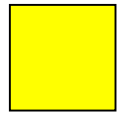
- 携帯電話機
- 携帯端末(PDA)
- 家電製品
- 自動車、カーナビ
- いずれ、全てのものに付く
  - ・商品全てに付く(生産履歴、注意事項)
  - ・音楽CD、映画DVD(試聴、使い方)
  - ・文化財、美術品(鑑賞案内)
  - ・道路、ビル、公園、名所、案内板・・・・

復習：日本で電子政府が進まない理由



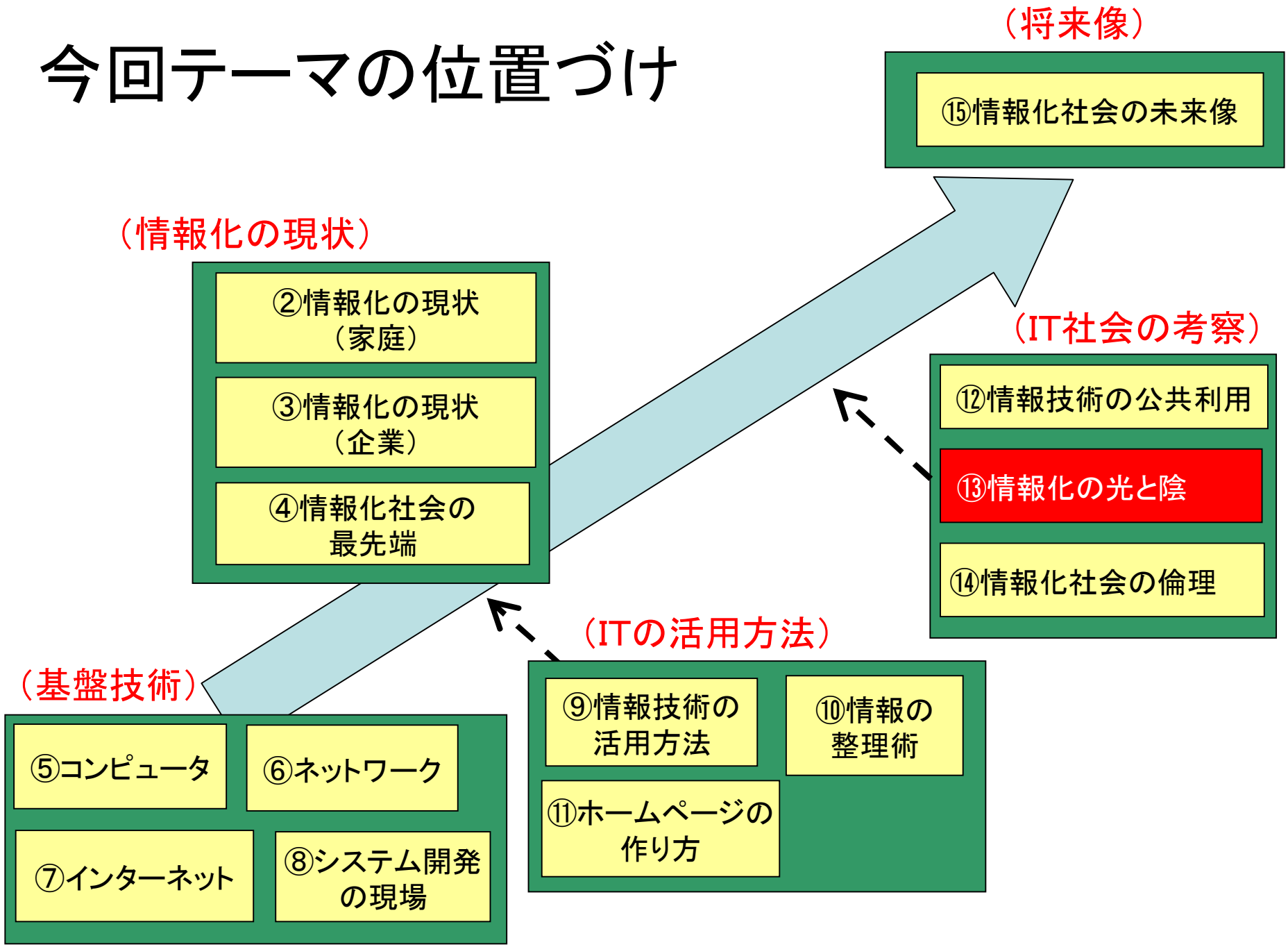
- 行政上の手続きがもともと複雑
  - 現在の複雑な手続きそのままで、電子化している。
  - まず、行革、簡素化が先決である。
  - 費用対効果の視点が無い（全ての行政手続きの電子化は無用）
- 推進部門が複数あり、省庁間で縄張り争い
  - 総務省vs経済産業省など
  - 例示：　自動車税は地方税であり、今は電子納付対象外
    電子パスポート申請時、別途、戸籍謄本を郵送必須
  - 中央省庁、地方公共団体では、電子証明の方式が異なる
- 完璧さを求め過ぎ、利用者の視点からみると、使い易くない
  - 例示：本人の確認方法が簡単でない。（ICカードの使用）
    専用のパソコンが必要となる。
- 法令を行政が提案することが慣習
  - 行政・官庁に都合の悪い法令はでてこない。
  - 国会は、法令審議だけでなく、立法権を駆使すべき。

復習：e－JAPAN戦略Ⅱの重点



・医療　　：患者を中心に、各医療機関が連携する安価・安心・安全な医療体制をつくる。
・食　　：産地と食卓を情報で結び、安心とおいしさに確かな信頼の絆を取り戻す。
・生活　　：高齢者が安全で快適に暮らせるようなIT化。
・知　　：ITを活用した遠隔教育の推進、コンテンツ産業の国際競争力向上。
・就労・労働　　：ITによる在宅就労、求人・求職情報の効率的な活用などを支援。
・中小企業金融：事務手続きのオンライン化などにより、資金調達環境を改善。
・行政サービス：24時間・365日の行政サービス実現など、電子政府をより充実させます。

今回テーマの位置づけ


（将来像）
⑮情報化社会の未来像
（情報化の現状）
②情報化の現状
（家庭）
③情報化の現状
（企業）
④情報化社会の
最先端
（IT社会の考察）
⑫情報技術の公共利用
⑬情報化の光と陰
⑭情報化社会の倫理
（ITの活用方法）
⑨情報技術の
活用方法
⑩情報の
整理術
⑪ホームページの
作り方
（基盤技術）
⑤コンピュータ
⑥ネットワーク
⑦インターネット
⑧システム開発
の現場

はじめに

・情報技術は、社会を望ましい方向に変革したり、
個人の生活をより便利にする力があります。
しかしながら、もともと技術は人間が発明し、
その技術の利用方法も人間が考えだしたものです。
・従って、技術には弱点もあるし、その使い方によっては、
大きな問題点があります。

これらのことを良く理解して情報技術を使うために、

・ITがもとから持っている弱点に起因する問題発生
・悪意をもってのIT使用による問題発生
・問題点への対応策について

述べてあります。

これらの内容を参考にして、自分が被害者とならないように
「ITによる問題発生への対応策をとる」きっかけに
していただければ幸いです。

目次（情報化の光と陰）

１．ITの光の部分（効用）

１．１　効果が出てきた点

１．２　ITによる社会変革の可能性

１．３　技術は、その適用で評価

１．１　効果が出てきた点

- ITはもともとは軍事技術（最高機密）であったが
  - ・高射砲、ロケットの弾道計算
  - ・敵国の暗号解読など
- 研究、ビジネスに使われ、効果が広がった
  - ・効率化、コスト削減
  - ・流通革新（少ない在庫でタイムリーな商品供給）
  - ・ビジネスや研究開発のスピードアップ
- パソコンの出現で、考えをまとめる道具になった
  - ・情報交換、アイデアのまとめ
- インターネットの普及で、生活の幅が広がる
  - ・コミュニケーションの媒体が増えた
  - ・情報収集、ホビー、友人つくり
  - ・起業が容易になった
  - ・個人の活動範囲が拡がった（容易に世界中を相手）

１．２　ITによる社会変革の可能性

・すでに企業を変えてきた、将来も同様
　　・（雇用、効率（仕事の方法、会議、出張）、スピードアップ）
・地域の活性化、経済発展の可能性
　　・（周回遅れでもトップに立てる）
・個人の仕事の形態が変わる
　　・（テレワーク（遠隔勤務、在宅勤務）、複数、SOHO、起業）
・教育、医療が変わる
　　・（e-ラーニング、電子カルテ、遠隔診断・・・）
・コンテンツビジネスはオンデマンドに移行
　　・（個別の媒体や販売店が不要になる）
　　（ソフト、音楽、映画、放送、新聞、書籍）
・直接民主制への接近
　　・（選挙の電子投票、電子国民投票・・・）

１．３　技術は、その適用で評価

- ITはあくまでも技術であり、道具である
- 技術の適用先によっては、不幸な社会になる

・原子力（平和利用 ⇔ 原子爆弾）
・遺伝子（難病治療 ⇔ 人造人間）
・IT　　（民生利用 ⇔ 無人攻撃機
　　サイバーテロ
　　犯罪
　　統制、監視社会）

人間同士の殺し合いの無い、民主的な社会でしか、
適用先の吟味、審査、決定は、困難である。

２．ITの陰の部分（問題点）と対策

２．１　西暦2000年問題の衝撃

２．２　ITが内包する問題点

２．３　悪意による問題の発生

２．４　統制社会への危惧

２．１　西暦2000年問題の衝撃

コンピュータの利用開始以来、コンピュータが原因で、
世界中の人々を震撼させた初めての出来事であった。

① 原因

・世界的にコンピュータの大小を問わず、
西暦の下2ケタだけで
日付の判別をする習慣があった。
（日付は、コンピュータで扱う重要データであるが、
メモリ容量、ディスク容量を節約するために、
西暦の4桁でなく、下2桁のみを扱う方法を長年採用してきた。）

・そのため2000年以降は00年、01年となり
日付の逆転現象が起きる。

② 悪影響が懸念されたヶ所

・日付を扱う情報システム全て
（軍、政府、自治体、企業、組織、個人のシステム）

・日付を扱うマイクロチップが組み込まれた機器全て
（エネルギー・水道・通信・交通等の社会インフラ、および
軍事、建物、製造、病院、家電などの機器）

２．１（続き） ２０００年問題の衝撃

③ 対策

・問題のある情報システムの修正、

・および設備・機械のマイクロチップの確認・交換（数十億のチップ）

④ 結果

・世界中の全ての関係者による
事前のシステムの修正、
マイクロチップの確認、修正により、
大きな問題の発生を食い止めることができた。

⑤ 将来に課題を残した

・この２０００年問題の経験から、

世界中の人々を震撼させる可能性が一つ増えたという認識。

・広範囲な電磁波障害による人工衛星、航空、
コンピュータ、通信などで異常発生の可能性

（原因）・太陽のフレア活動による磁気あらし

・大規模な地震、火山活動による地磁気異常

・電磁波兵器の実用化

・大規模なサイバーテロによる情報システムの麻痺

２．２　ITが内包する問題点

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
  - 2007年問題（大量退職）による慢性的なSE不足
- 急速な技術進歩により、SE育成が追いつかない

２．２ （続き）ITが内包する問題点

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）

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

２．２ （続き）ITが内包する問題点

⑥ インターネットの弱点

・利用者の善意に頼る構造であり、
悪意に対抗する力が弱い

・ベスト・エフォートの原則で運営され、
通信の必達責任が無い

・コンピュータの番地不足

・IPv4ではドメインの数は、４３億が限界

・これでは、「どこでもコンピュータ」は実現不可能

⑦ 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なっている

内包する問題点への対応策

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

補足資料の一覧

・システム障害事例
・IT技術者の不足

・デジタル・デバイド
・デジタル・デバイドの克服策

・文字コードの乱立
・文字コード標準化の経緯
・日本語文字コードの扱い
・文字集合と文字符号化方式
・アジアの文字が一番の問題
・漢字と異体字の存在

・健康への悪影響

・インターネットの弱点

・IPv6とは
・IPv6への移行計画

補足：システム障害事例

- 2001年8月9日、JAL、発券、搭乗手続き停止で国際線ダイヤが大幅遅れ（ソフトのミス）
- 2001年12月28日、第一勧業銀行、振込みが1月4日にずれ込み（単純ミス）
- 2002年4月1日、みずほ銀行、ATM利用不能、未払いでも残高が減少、自動引き落としの処理遅れ（テスト不足）
- 2003年4月28日～5月8日、ジャパンネット銀行、ネット取引障害（データベース制御、回線制御ミス）
- 2003年 7月14日、日銀、決裁遅延（システムミス）
- 2004年4月8日、東京航空管制システム障害で120便に遅れ（ソフトのミス）
- 2005年5月6日、りそな銀行のATM停止（日付の設定ミス）
- 2005年8月29日、JASDAQ、取引停止（プログラムのミス）
- 2005年8月以降、楽天証券のシステム障害（テスト不足）
- 2005年11月1日、東証のシステム停止（システム移行ミス）
- 2006年1月18日、東証のシステム停止（処理能力限界）
- 2006年3月31日、NTT西、光IP電話39万回線で接続トラブル

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
情報化社会
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

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）

補足：　デジタルデバイド

- デジタルデバイドとは
  経済力の差によって、
  →パソコンやインターネット等のIT利用能力の差、
  →有用な情報にアクセスする機会を持つ者と
  持たざる者との間に情報格差が生じ、
  →ますます経済力、生活力の差が生じる
  という問題である。
- 先進国と途上国、都市と地方、年齢、人種、教育の差に起因する経済力の差は、ITとは別問題だが、
- デジタルデバイドの克服により、
  ますます差が拡がることを解消すべく
  国連が主導して各国とも対策中。
- 要注意な人（好奇心が薄い人、時間に余裕が無い人）

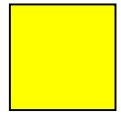
補足：デジタルデバイドの克服策

① 国連
- 世界情報社会サミットで、格差是正を最優先議題。（2003年～）

② 米国
- 1999年、商務省調査、年収7万5000ドル以上の世帯は、最低所得層の世帯に比べ
  - インターネットにアクセスできる比率が20倍以上、
  - パソコン所有率も9倍以上の差
- クリントン政権は2000年1月、社会的弱者の就業機会の増進のため、以下を提唱
  - インターネットの利用機会を提供
    （学校、図書館、テクノロジーセンター（1，000ヶ所）等にて）
  - 教員の再訓練

③ 日本政府
- e-Japan戦略の重点施策
  - 設計段階からのユニバーサル・デザイン
  - 情報処理機器のアクセシビリティ指針（入力の改良、簡単な操作）
  - 情報リテラシー教育（児童、学生、社会人、高齢者）

補足：文字コードの乱立



コンピュータは、全ての文字を2進数に置き換える。

（問題点１）世界には、文字の符号化方式が多数存在

→文字コード間で、煩わしいコード変換が必要

→変換できない場合は、文字化けする

（問題点２）世界中には300以上の文字体系が存在するが、文字コード化できてるのは100程度。

→彼らは、自国の文字を使えない

→外国語が使えないと、コンピュータが使えない

（問題点３）ISOのUnicodeが符号化の世界標準の方向

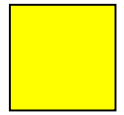
→移行作業は、「2000年問題」に匹敵

従って、外国人との情報交換は、

・英語を使いこなすか、

・文字コード変換に煩わされるのを我慢するしか無い。

補足：文字コード標準化の経緯



1962　米国規格協会(ANSI)がASCIIコードを規格とする。
1969　日本工業規格(JIS)が「JIS X 201」を制定する。（漢字はまだ使えず）
1978　JIS X 208を制定する。第一水準・第二水準
1982　MS-Kanjiコード(シフトJIS)が三菱電機MULTI16に搭載。
1983　JIS X 208-1983　‘78年のコードを改訂する。→新JIS
1990　JIS X 212」が制定される。補助漢字として5801字収録。
1991　EUCの制定。（Extended　UNIX　Code）
1992　Unicode ver1.1が完成。
1993　国際標準規格がUnicodeを規定。（ISO/IEC 10646）
1995　JIS X 0221にUnicodeを規定する。
1996　Unicode ver2.0、UTF-8が制定される。
1997　「JIS X 208-1997」の改訂。→シフトJISに関する規定。
1998　Unicode ver2.1が制定される。
2000　JIS X 0213」を制定する。新たに第三、第四水準の文字を規定。
　　Unicode ver3.0リリース
2002　Unicode ver3.2リリース。

参照：（愛知大学 http://taweb.aichi-u.ac.jp/saitom/mojicode.htm）

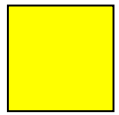
補足：日本語文字コードの扱い

	文字の符号化方式					
JIS文字集合	JIS標準	ASCII	S－JIS	EUC－JP	ISO－2022J	UCS－2
制御文字（半角）	○	○	○	○	○	○
ローマ字（半角）	○	○	○	○	○	○
カナ（半角）	○	X	1バイト	2バイト	○	？
漢字第1水準	○	X	○	○	○	○
漢字第2水準	○	X	○	○	○	○
補助漢字	○	X	X	3バイト	？	？
漢字第3水準	○	X	○	？	○	○
漢字第4水準	○	X	○	？	○	○
オープン領域	－	X	X	－	－	－

Unicodeの一種

・半角カナは変換できないことが多い。
・Windows95はS－JIS、それ以降はUnicodeを採用
・Unicodeでは、CJKV統合漢字になる（China、Japan、Korea、Vietnam）

補足：文字集合と文字符号化方式



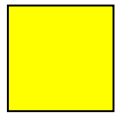
文字集合：　目的をもって幾つかの文字をあつめたもの

例示：日本語では、ローマ字
カナ文字
漢字第一水準、第2水準・・・・・
英語では、　英数字（アルファベットとアラビア数字）
特殊記号（，：　＋など）
制御文字（改行、改頁、通信制御用）
中国語では、簡体字（中国の省略漢字）
繁体字（香港、台湾で使われる漢字）

文字の符号化方式：文字集合をコード化する方法のこと

例示：ASCII（ANSI）、EBCDIC（IBM）、EUC（UNIX用）、
JIS、シフトJIS（MS社）、MS漢字コード、CID（Adobe社）
Unicode、ISO（国際工業規格標準）

補足：アジアの文字が一番の問題



・世界には約3000～7000の言語、約300の文字体系
・話者数の世界上位100位までの言語のうち、
　・62言語がアジアの言語で、それらに19種の文字体系が使われている。
　・この様にアジア地域の言語・文字文化は多種多様である。
・アジアの文字コード体系が進まない理由
　・ アジアの文字の構造が複雑で、その取り組み方が色々ある。
　　位置により文字が変わる（アラビア文字）、結合文字（インドの一部）
　　異体字の存在など
　・ 従って互換の取り難い色々な文字コードが開発される。
　・場合によっては、1つの国に種々の
　　文字コード体系が存在する。(以前の日本もそうであった)
　・大手のソフト業者は、このマーケットに関心が薄い。
　・語学学者とインターネット関係者が乖離
　　各国現地文字のコード化・標準化の必要性を一番感じている
　　インターネット関係者は、言語・文字や国際規格に対する造詣が
　　深くないので、なかなか有効な発言ができない。

（参照：三上喜貴氏 「文字符号の歴史（アジア編）」（共立出版社刊））

補足：漢字の異体字の存在

問題の例示：

- 住民基本台帳システムでは、異体字などの扱いは、各自治体が外字扱いしている。
- 外字は、他システム、他機種では互換性が無い
- 日本、中国、台湾、韓国、ベトナムでの統一が困難

異体字の例示：

（日本） 竜　龍　龔

（中国） 龙　竜　龍

（台湾） 龍　龔　竜　[illegible]　[illegible]　[illegible]　[illegible]　[illegible]　[illegible]　[illegible]　[illegible]　[illegible]　龏

補足：健康への悪影響

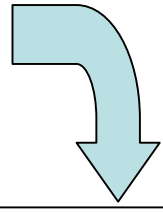
電磁波による悪影響

- 医療器具の誤動作を誘引
- 脳、内蔵への影響の可能性
- 海外では規制が常識（日本？）

脳の活動への影響

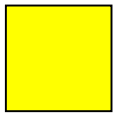
- 考えたり話したり書いたりする場合に比べて、
- パソコンやゲームを操作する場合は、

視覚野、運動野（運動神経）が活発に動き、
人間の知的能力の源泉である
脳の前頭葉連合野の活動が少ない



考える＞音読＞読み書き、計算＞パソコン操作

補足：インターネットの弱点



ⅰ）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技術であり、
・緊急時ということで、セキュリティ対策が弱かった。

ⅱ）軍事目的から民間利用に転換した際には、
はじめは研究者同士の情報交換であり、
・オープンで、参加者の善意で成り立っていた。

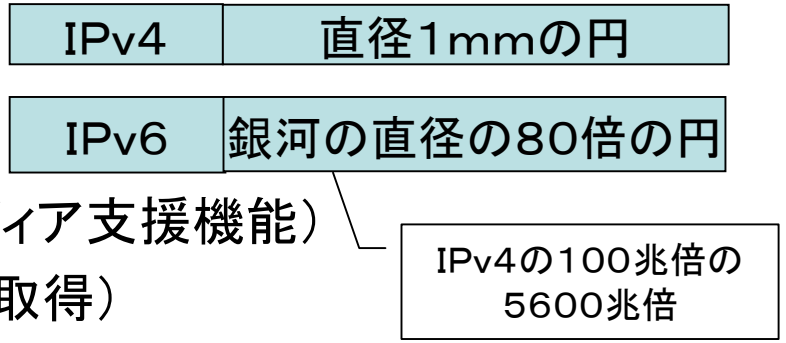
ⅲ）このように、もともとセキュリティに問題を持ったままのインターネットと
個人のホビー用のパソコンが結びついて急速に用途が広がり、
セキュリティ対策が後手になった。
・パソコンは、はじめは個人のホビー目的のために開発された。
・Windowsも、はじめは個人の範囲内での利用を目的。
・しかも、そのWindowsを使って、情報発信だけでなく、重要情報を
入力するシステムがビジネス目的に安直に構築された。
（キャッシュカード情報、個人情報など）

ⅳ）インターネットなど新技術を使ったシステム開発は、未成熟技術を使った。
従来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。

ⅴ）インターネット企業は急成長を続けており、ともすれば、
内部管理体制が弱く、管理の目が行き届いていない。

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年前後にはパンク
  - 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）

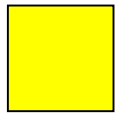


- 128ビットの割り振り方
  - TLA（Top Level Aggregation）、13bit、世界規模のISP識別
  - NLA（Next Level Aggregation）、24bit、ISP傘下の組織用
  - SLA（Site Level Aggregation）、16bit、組織内のサブネット用
  - ｲﾝﾀｰﾌｪｲｽID（固有のアドレス）、 64bit

（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/ ）

補足：IPv6への移行計画



・移行が必要な箇所
  ・DNS（ドメイン・ネーム・サーバー）
  ・ルーター
  ・ハブ
  ・OS （WindowsXP、ソラリスは対応済み）
  ・プロバイダ
・日本の移行推進団体
  ・Ipv6普及・高度化推進協議会（http://www.v6pc.jp/jp/index.html）
  ・会長　村井 純（慶応大学）
  ・構成　官民あげての推進体制（IIJ、日本IBM、トヨタほか350団体）
  ・移行領域のWG（4つ）
    大企業・自治体、ISP 、SOHO、家庭
・e-JAPAN戦略の計画では、2005年を目標（？）
  「2005 年までにすべての国民が、場所を問わず、自分の望む情報の入手、処理、発信を安全・迅速・簡単に行えるIPv6が実装されたインターネット環境を実現する。」
・ 米国国防省、2008年に移行完了目標

２．３　悪意による問題の発生

① 悪意による問題の特徴

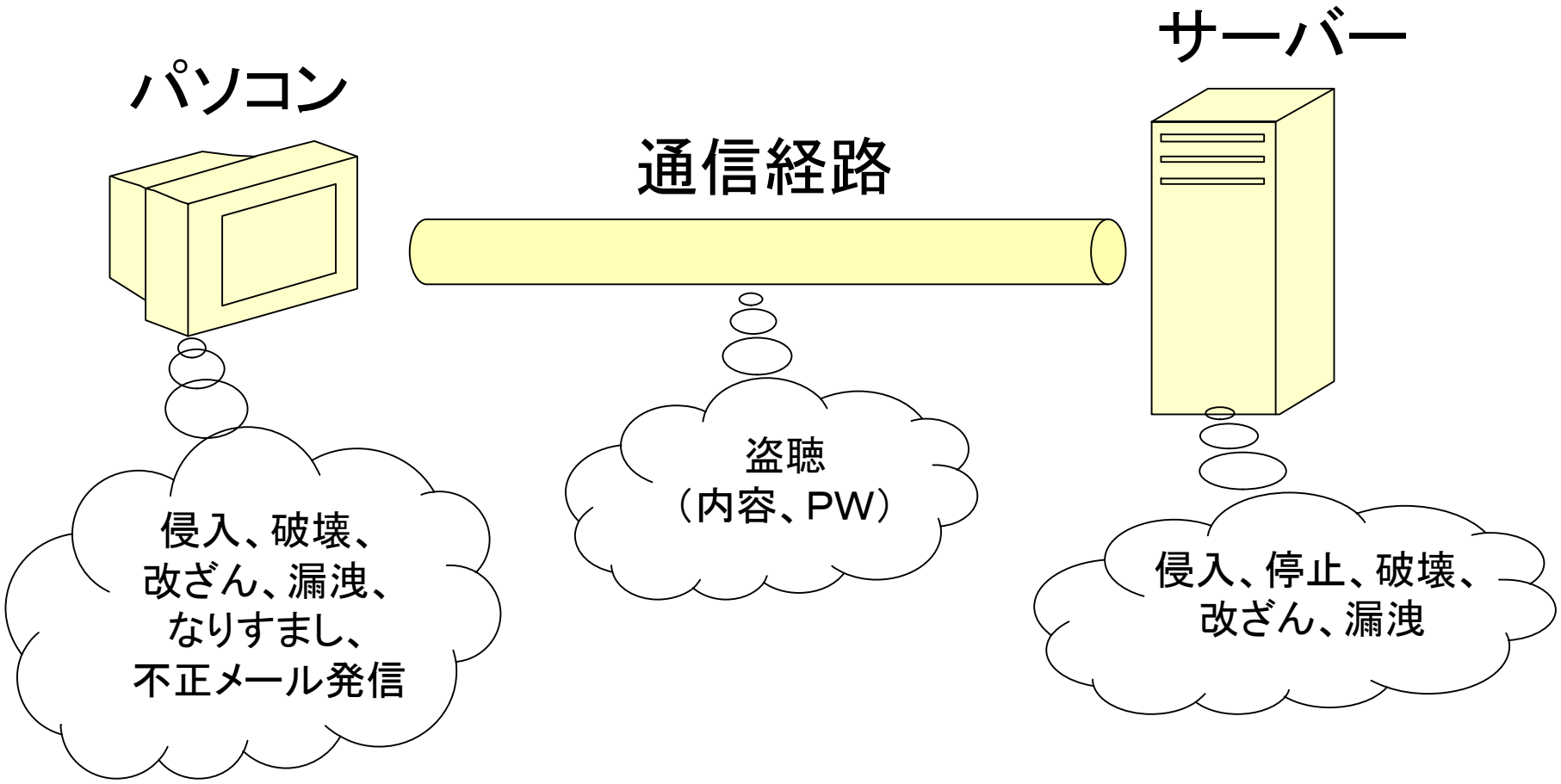
- ソフトは人手で作成しており、欠陥が狙われる
  - Windows、IE、メーラーの欠陥
  - コンピュータ・ウィルス（破壊プログラム）
- インターネットは自由空間であり、統制しにくい
  - 無法地帯になりがち（ネット詐欺などの悪徳商法）
  - 有害Webサイトの増加（暴力、残虐、アダルト・・・）
- 電磁的な手段の犯罪は、気が付きにくい
  - カードの偽造、指紋の偽造
  - 取り締まる法令が、後追いになる
- 犯人は、捜査当局以上の専門知識を持つ
  - 並外れたIT技術を駆使（クラッカー（破壊者））
  - 破壊活動（サイバーテロ）、盗聴、通信傍受
- 従来に比べて、犯罪の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

② 犯罪の形の変化

- コンピュータ、インターネットが普及したから
  犯罪が増えたのでは無いが、
- 悪事をはたらく犯罪の形が変わり、
- 犯罪の規模が大きくなった。
  - 情報漏洩は、電子媒体により膨大になった。
    （1枚のDVDに数百万人分の個人情報）
- 手段や道具は、使い道により犯罪になる
  - 郵便　通信　⇔　架空請求ハガキ
  - 電話　通信　⇔　振り込め詐欺
  - メール　通信　⇔　ウィルス潜入
  - ホームﾍﾟｰｼﾞ　情報発信　⇔　フィッシング詐欺
    ワンクリック詐欺

③　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



④ 受けるダメージ

- パソコンが使用不能
- ファイル破壊、改ざん（データ書換え）
- 掲示板で個人攻撃される（誹謗、中傷）
- 迷惑メールで通信料金が増える
- 悪事への加担者にされる（メール発信、ｻｰﾊﾞｰ攻撃）
- 情報の盗難（名簿の転売、スパムメールのターゲット）
- 詐欺にかかる（不用品の購入、金銭の支払い、脅し）
- なりすまし（キャッシュカード使用）

いたずら、愉快犯 → 金銭奪取など悪質化

⑤ 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

補足資料の一覧

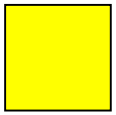
・ハッカー、クラッカー
・クラッカーによる侵入事例
・サイバーテロへの備え

・ウィルス、ワーム
・ウィルスの被害状況
・ファイル交換ソフト
・情報漏洩の事例

・悪徳商法の手口
・送信者を隠す方法
・スパムメールが入口
・ワンクリック詐欺
・スパイウェア
・フィッシング詐欺

・ネット犯罪の相談窓口
・IT安心会議

補足：ハッカー、クラッカー



- ハッカーの原義は、
  - 並外れた能力を持つプログラマ
  - 転じて、権力を持つ政府、大企業に対抗して
    システム内に侵入して、不正を暴く人

- クラッカーは、
  - その並外れた能力を悪用する人で、
  - システムの破壊者

資料：クラッカーによる侵入事例

- 2005年6月、米国、カード決済会社で4000万件の個人情報流出疑惑
  - ・米カードシステムズ・ソリューションズ
  - ・影響が世界中のカード利用者に波及
  - ・カード不正使用が、6ヶ月間も分からなかった
- 2001年3月9日、米連邦捜査局(FBI)の発表
  - ・米国で、1年間に、
  - ・100万を超えるクレジットカード番号が盗み出された。
  - ・ロシアとウクライナの組織的なクラッカー集団のしわざと言われている。
- 2000年1月10日、
  - ・米国、CDなどのネット販売店（CDユニバース）から、
  - ・顧客30万人分のクレジットカード情報を盗み出した。
  - ・東ヨーロッパのクラッカー
- 2000年9月11日、
  - ・米ウェスタン・ユニオン社のウェブサイト・サーバーから、
  - ・1万5700人のクレジットカードとデビットカードの情報を盗んだ。
  - ・どこのクラッカーかは不明
- 2000年1月24日、日本、中央省庁のホームページ改ざん（科技庁ほか）

補足：IT犯罪には国境が無い

- インターネット、電子商取引が盛んな国々は、対策中。
  - ・米国、欧州、日本など
- それほど対策を講じていない国々が多い。
  - ・ロシア、中国、インドなど
- 通信やインターネットには、もともと国境が無い。
- 従って、海外からITを悪用した大規模な犯罪が発生。
  - ・スパイウェアなど、ロシア、中国発が多い。

補足：サイバーテロへの備え

大規模なコンピュータ・システムに侵入して破壊し、
主要な機能を麻痺させる。
政府・軍部・大企業が狙われる可能性が大。
最も影響が大（通信企業、エネルギー、交通、金融決済
日本の備えの遅れが目立つ。

方法：　　クラッカーまたは破壊用ウィルス対策
日本の予算：　235億円（米国の10分の1以下）
対策要員：　日本　77人
米国　数千人
英国　300人以上
韓国　300人以上

補足：ウィルス、ワーム

- ウィルス（＝コンピュータウィルス）
  - 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
      （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（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。
- ワーム（ウィルスの一種）
  - メールの添付ファイルを開く操作によって動作する。
  - アドレス帳を使って、メールを出し他のコンピュータにも拡がる。
  - 急速に被害が拡大し、メールサーバーが麻痺する被害。
- ウィルス、ワームとも、MS社のWindowsがターゲット。
- 携帯電話に侵入するウィルスも出現
  - 例：Cabir（カビル）、シンビアンOSが対象
- 自分のIT技能の誇示、仲間内での競争、愉快犯・いたずら。

資料：ウィルス被害状況

- 国内企業の被害総額は推計値で約3025億円
- １事業所あたりの被害額は約28万円

独立行政法人「情報処理推進機構（IPA）」の調査
（ 5000の事業所や自治体を対象）

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
  ・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6月、三菱電機プラントエンジニアリング、電機設備保守情報
  ・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
  ・2006年3月、富士宮信用金庫、顧客の手形決済情報
    私物パソコンを業務に私用せざるを得ないことが原因！！

資料：情報漏えいの事例

- 2006年6月、KDDI、顧客情報流出（399万人）
- 2006年4月、第一生命、顧客情報記録のマイクロフィルム紛失（21万人）
- 2005年6月、米カード決済センター、4000万件以上のカード情報流出疑惑
- 2004年6月25日、米AOL、顧客メールアドレス、元従業員（9200万件？）
- 2004年6月29日、お茶の水女子大、パソコン5台とディスク10枚盗難（3000人分）
- 2004年4月8日、コスモ石油、カード会員情報（92万人）
- 2004年4月6日、日銀札幌支店、登録者全員のメールアドレス配信（単純な操作ミス）
- 2004年3月24日、奈良県内の病院、ノートパソコン5台の盗難事件、
  約7500人分の患者らの個人情報あり。
- 2004年3月9日、ジャパネットたかた、顧客情報（66万人）
- 2004年2月25日、Yahoo！BB、加入者情報、DVDで漏洩（470万人）
- 2004年2月21日、三洋信販、顧客データ（32万人）
- 2004年2月12日、マイクロソフト社、Windows2000のソースコードが流出
- 2003年11月19日、ファミリーマート、メールマガジン購読者情報（19万人）
- 2003年8月8日、信販会社アプラスの会員情報（8万人）
- 2003年6月26日、ローソン、カード会員情報（56万人）
- 2003年3月18日、Yahooオークション、他人のIDで11億円の買い物
- 2003年2月20日、ネブラスカ州キャッシュカード処理会社、
  カード番号盗難（800万枚）、クラッカーのしわざ
- 2002年12月28日、福島県岩代町の全町民9600人分の個人情報を収めた
  マイクロテープが盗難
- 1999年5月21日、宇治市、住民基本台帳データ（約21万件）

（情報漏洩事件の一覧表　http://www.it-hoken.com/cat_aeieoieioeie.html　）

情報の悪用

・個人情報売買

・預金引出し

・脅迫

・自慢話

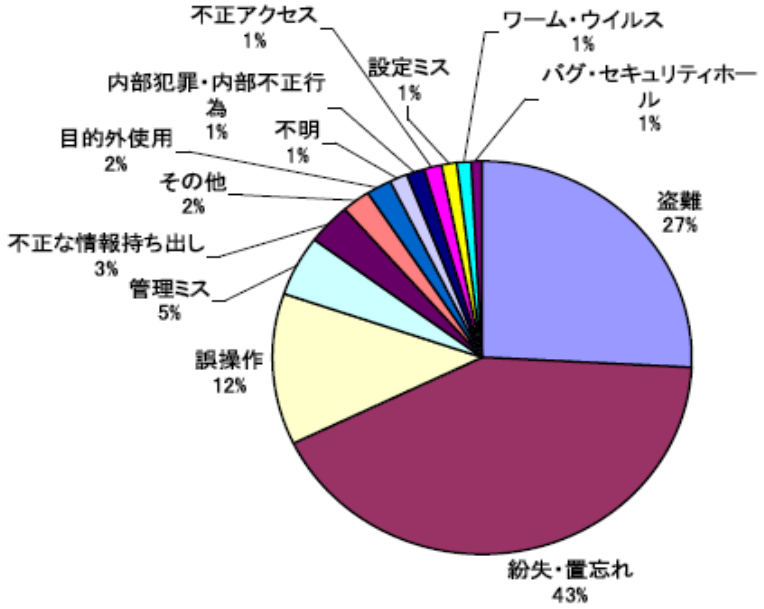
資料：情報漏えいの状況

・2004年1月1日、金融庁、改正貸金業規制法で、消費者金融業者での顧客情報の漏えいは、業務停止処分の対象とする。

・情報漏洩件数

	2002年	2003年	2004年	2005年
件数	62件	57件	366件	1，032件
被害者数	41万人	155万人	1，043万人	881万人

（原因）



（出典：NPO　日本ネットワークセキュリティ協会）

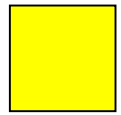
補足：悪徳商法の手口

従来の電話、FAX、街での勧誘と同様で、
方法がIT利用に変わってきた。
（電子メール、Webサイト、掲示板）

・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－－－ネズミ講のさそい
・オークション－－－商品違い（旧式、模造品）
・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
・ワンクリック詐欺－クリックだけで入会料金を請求
・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　!!

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）

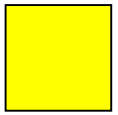
補足：スパムメールが入口

- 突然メールが送られてくる。
- 悪徳商法の入口になっている。
  - 個人情報収集
  - ワンクリック詐欺
  - フィッシング詐欺
- 収集した個人情報を、業者間でたらいまわし。
- 非常に巧妙な手段が講じてある。
  - 50万円さしあげます、当選しました
  - メールが不要なら、〇〇まで返信
  - 疑問は、△△まで問合わせ下さい
  - 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：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:スパイウェア



・元来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。
・最近は、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: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
・ウィルス対策ソフトに、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)

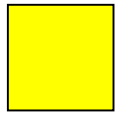
補足：フィッシング詐欺

- 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技が必要

パスワードなどを入力させるブラウザ画面では、
通常、右下の鍵マークがあり、証明書付きで
安心できる

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

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）

２．４　国家による統制社会への危惧

①　インターネット利用規制

・一部の国では、政府が特定のWebサイトの
閲覧を禁止している。（中国、イランなど）

例示：IBB（米国、国際放送局）のWebサイト
：政府批判の掲示板、ブログは、閉鎖される。
：政府に都合が悪い投稿は拒否される。
：米ネット企業が中国当局に協力（Yahoo、MS、Google）

・企業でも、業務に結びつかないWebサイトの
閲覧を禁止している。

・モニタリング
・アクセス制限の措置

②　国家機関による監視、盗聴

・合法的な盗聴ではあるが、電波、ケーブルを使う通信は、
　通常、全て盗聴対象になる。
　　・電話、携帯電話、FAX、電子メール、特定Webサイト検索
・世界規模の盗聴システムの存在が疑われている。
　　・エシュロン（アメリカ、イギリスほか）
　　　・世界中の通信を傍受（電話、FAX、無線、インターネット）
　　・ほかにも、ロシア、フランス・・・・？
　　・英国の盗聴法
　　　・テロ予防のため、電子 メール盗聴装置をプロバイダーに義務づけ
・日本、1999年、盗聴法（通信傍受法）成立
　　・法令成立前でも、公安・警察で実行していたと言われているが、
　　・法案は、その目的、範囲、を限定しており、無法状態よりは一歩前進。
・各国とも、公安機関による監視、盗聴が行われている。
　　・国際テロ、破壊活動団体などが対象

補足：匿名の世界ではない

- 「インターネットは匿名の世界」はウソ。
- メール、掲示板、電子会議、Weblogなど、
  通信は、全て記録してある。
- したがって、後から追跡調査が可能である。

③　国民総背番号制との関係

電子政府の進展によって、

・国民の了解、合意ができていない段階で、

・国民総背番号制が裏で始まる可能性あり。

裏でやるよりは、国民が決める問題であり、国会で明確にすべき課題　（好嫌や善悪の問題ではなく必須である）

（参考：氏名、住所、性別、生年月日をキーに名寄せすれば、簡単に下記を結合できる。）

運転免許証番号

健康保険証番号

旅券番号

年金の受給者番号

住民基本台帳
（住民票コード（11桁））
（氏名、住所、性別、生年月日）

銀行の口座番号

メールアドレス

病院の患者ID

納税者番号（未実施）

金融の個人信用情報

民間の各種ユーザーID

犯罪履歴情報

3. 個人でできる対応策

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、脅威は無くならないが、
損害を小さくはできる。

①　簡便な対策

容易に出来ることを習慣づける

- データのコピーとバックアップ
- 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）
  - パスワードを頻繁に変える
  - 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絶対に開かない
- メールはテキスト形式で読む設定（HTMLメールは防御が脆弱）
- 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）
- 脆弱性を補強
  - Windows　Updateの励行
  - OS、ブラウザのバージョンアップ（IE6　SP1以上）
  - メールソフトのバージョンアップ
- 信頼できるサービス事業者を利用
- インターネット喫茶利用時は、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で埋める。

② ソフトで予防する

- 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
  - 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）
  - AVG Anti-Virus（無料）、 avast！4（無料）
    - http://free.grisoft.com/freeweb.php/doc/2/lng/us/tpl/v5
    - http://www.iso-g.com/
- OSを変える手もある
  - 世界中のほとんどがWindowsであり、集中攻撃
  - Linux（ほかにKnoppixは1CDーLinux）
  - Lindows（Windows対応ソフトが動くLinux）

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。

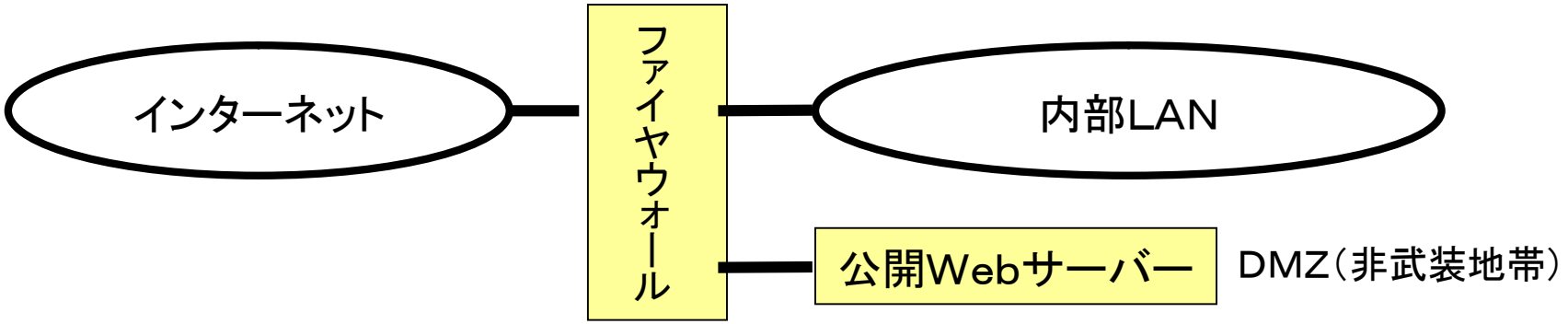
①パケット・フィルタリング方式

・ネットワーク層で動作

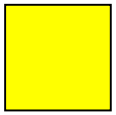
・送信元や送信先のIPアドレス、ポート番号などで判断する

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



補足： スパイウェア対策ソフト



- 最近は、アンチウィルスソフトに対策機能が含まれている場合がある。
- プロバイダ提供もある。
- 無料ソフトでも有効
  - Spybot

    http://enchanting.cside.com/security/spybot1.html

  - AD－Ware

    http://www.forest.impress.co.jp/lib/inet/security/antiadspy/adawarese.html

③　電子認証

「盗聴、改ざん、なりすまし」を予防

電子認証は、三つの手段を組み合わせる

ⅰ）暗号encryption

・一定の規則により暗号化し、同じ規則で復号する（解読）

・この規則のことを「暗号化ロジック」または「鍵」という

・ハガキよりも封書、書留にあたり、盗聴、改ざんを防止する

ⅱ）電子署名（デジタル署名）Digital　SignatureまたはCertificates

・本人自身であることを証明する電子的なデータのこと

・サインや実印にあたり、なりすましを防止する

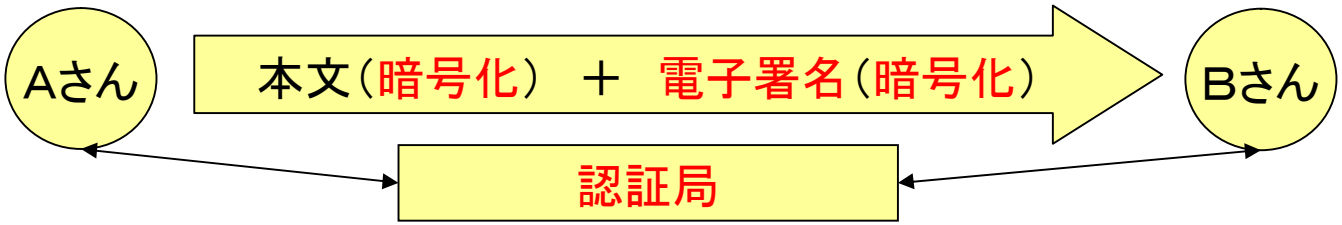
ⅲ）電子署名の認証electronic authentication（電子証明書）

・電子署名が、有効であることを証明すること。

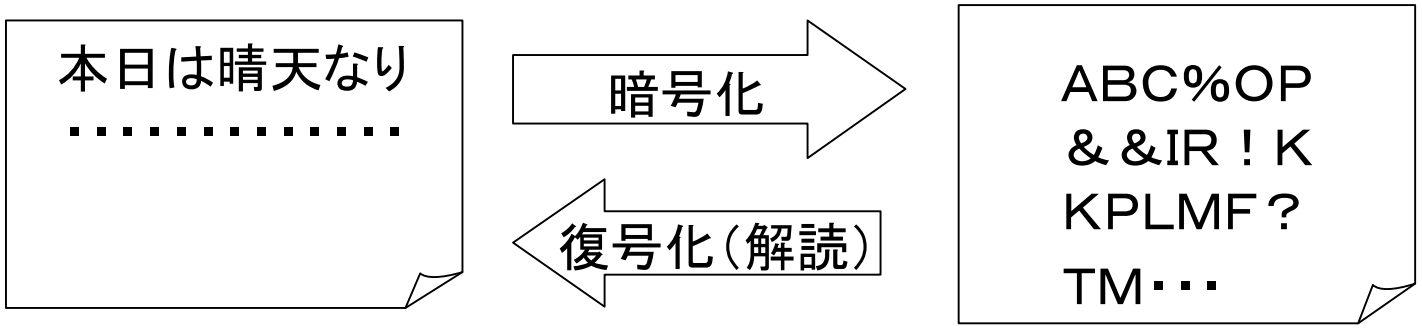
（名前、メールアドレス、公開鍵、有効期限がセットになっている。）

・民間の認証局が証明する（CA：Certificate　Authority）

・実印の印鑑証明書にあたる



補足：暗号化の種類



ｉ）共通鍵暗号方式（一つの鍵）（ドアの鍵と同じ）

- 一つの鍵で、暗号化、解読をする
- この鍵を使う人が多いと漏れる（1:n、n:n）
- 鍵の保管、伝達が非効率で、普及せず

ii）公開鍵暗号方式（二つの鍵）

- 公開鍵と秘密鍵のペアをつかう
- 秘密鍵で暗号化した文書は、公開鍵でしか解読できない（デジタル署名付きメール）
- 逆に公開鍵で暗号化された文書は、秘密鍵でしか解読できない（暗号化メール）

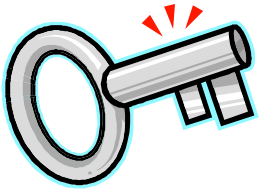
補足：秘密鍵で暗号化(デジタル署名付きメール)

Aさん

①Aさんが、Aさんの秘密鍵を使って暗号化したデジタル署名と文書を送る（デジタル署名のみの暗号化でも可能）

②Aさんは、Bさんに、メールと一緒に電子証明書（公開鍵含む）を送る

Bさん



秘密鍵

暗号化

デジタル署名

暗号文

解読

公開鍵

認証局

③Bさんは、認証局にデジタル署名の正しさを確認する。

④正しければ、Bさんが、渡されたAさんの公開鍵を使って文書を解読する

解読できるということは、間違いなくAさんからの文書であることの証明。

補足：公開鍵で暗号化（メールの暗号化）

Aさん

①Aさんが、事前に、Bさんにメールで電子証明書で公開鍵を渡しておく

Bさん

②Bさんが、Aさんの公開鍵を使って文書を暗号化して送る

秘密鍵

解読

暗号文

暗号化

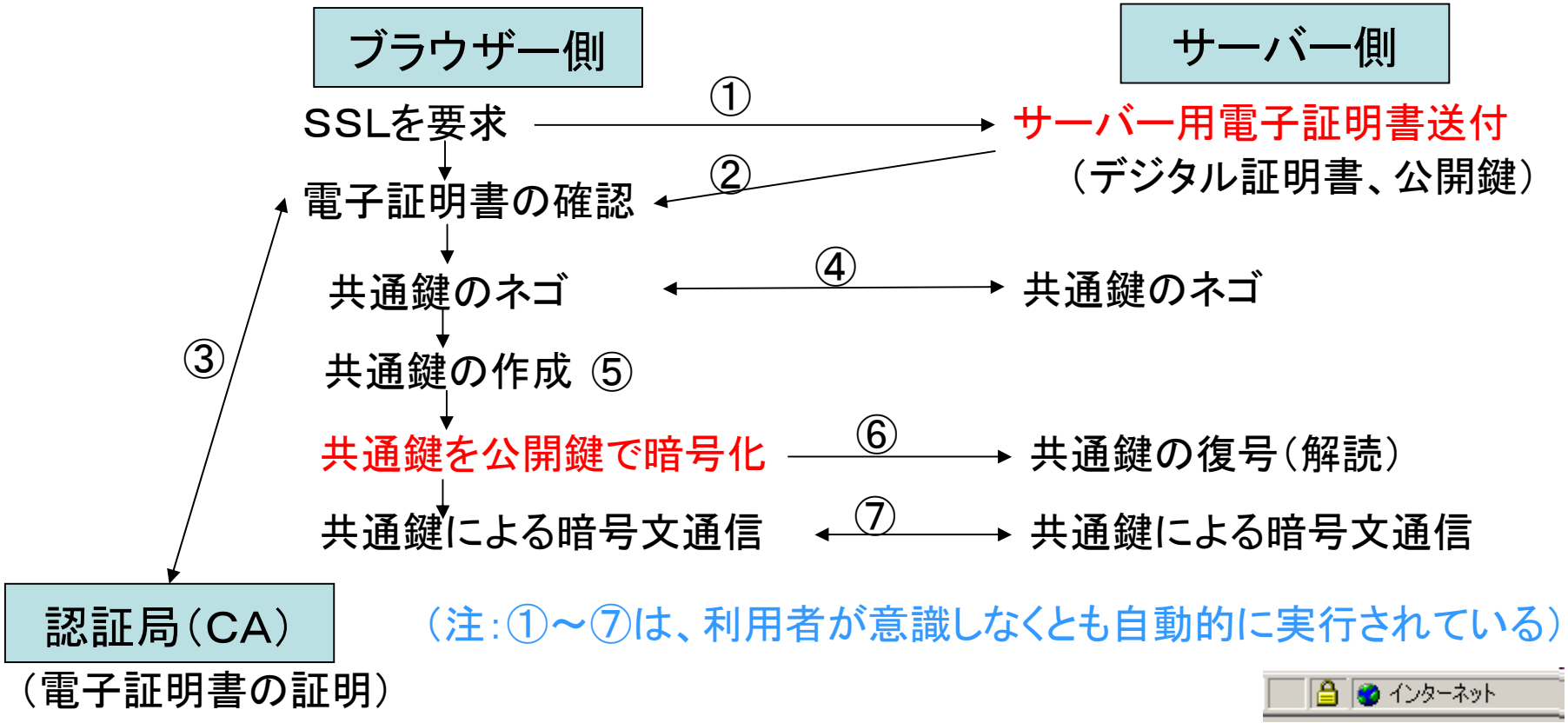
公開鍵

③Aさんが、自分の秘密鍵を使って文書を解読する。

（秘密鍵はAさん以外は知らないので、他人は文書を解読できない。）

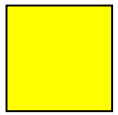
補足：インターネットの安全確保

- SSLにより、ブラウザ～Webサイト間の個人情報の保護を自動実行
- Secure Sockets Layer （セッション・レイヤ、HTTSというプロトコル）
- ソケットレベルで、認証と暗号化を行う（ソケット＝IPアドレス＋ポート番号）
- 個人情報、キャッシュカード情報の送信に使われる
- 公開鍵方式（安全）と共通鍵方式（高速）の長所の組み合わせ



（注：①～⑦は、利用者が意識しなくとも自動的に実行されている）

補足：電子証明書の種類



- Webサーバー用
  - ・これが一番、普及している
    （日本ベリサイン、日本ジオトラスト、日本ビートラステッドジャパン・・・）
- 個人用
  - ・私的な個人電子証明書
    - ・必要ではあるが、費用がかかり、非常に少ない
  - ・公的な個人電子証明書
    - ・住民基本台帳を基盤に自治体で取り扱う
- 法人用
  - ・私的な法人電子証明書
    - ・各企業が認証局を開設できる
  - ・公的な法人電子証明書
    - ・法務省が商業登記認証局を設置

4. 企業のセキュリティシステム

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。
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

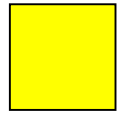
・異動時、退職時は削除

４．（続き）

⑥ その他の対策

- 情報漏えい防止ソフトウェア
- 監視カメラ設置（心理的効果）
- アクセスログ（記録）は長期保管
- 外部とのアクセス管理（ファイヤウォール）
- 企業用の電子認証システムの導入
- ネットワークに繋がない
  （最高機密用コンピュータ）
- 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）
- 公的なセキュリティ認定を受ける

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

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 ）

５．レポート課題

- 以下の点について、まとめをレポートで提出
- 内容

①メールやインターネットを利用する場合、
自分が被害者とならないために
・気をつけるべき点
・およびその理由を
レポートにまとめよ。

- 形式　　A4、１枚程度
- 提出方法　メール（添付も可）、またはペーパー
  TO：fwhy6454@mb.infoweb.ne.jp
- 提出期限　次回の授業開始までに。

６．参考書、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
・小暮　仁「教科書　情報と社会」 日科技連
・Y2プロジェクト 「超図解　インターネットテクノロジー＆
セキュリティ」　エクスメディア社
・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