第3章
情報通信ネットワークと情報社会

第1節　コンピュータネットワークのしくみ
第2節　情報システム
第3節　情報社会と安全性

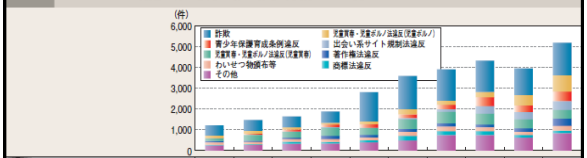
サイバー犯罪の現状(h13-22)

関連：p.-

サイバー犯罪　コンピュータやネットワークを利用した犯罪

http://www.npa.go.jp/hakusyo/h23/honbun/html/1-toku2_1_1.html

図-2　ネットワーク利用犯罪の検挙件数の推移(平成13～22年)



区分＼年次	13	14	15	16	17	18	19	20	21	22
合計（件）	1,209	1,471	1,649	1,884	2,811	3,593	3,918	4,334	3,961	5,199
詐欺	485	514	521	542	1,408	1,597	1,512	1,508	1,280	1,566
児童買春・児童ポルノ法違反（児童ポルノ）	128	140	102	85	136	251	192	254	507	783
青少年保護育成条例違反	10	70	120	136	174	196	230	437	326	481
出会い系サイト規制法違反	–	–	8	31	18	47	122	367	349	412
児童買春・児童ポルノ法違反（児童買春）	117	268	269	370	320	463	551	507	416	410
著作権法違反	86	66	87	174	128	138	165	144	188	368
わいせつ物頒布等	103	109	113	121	125	192	203	177	140	218
商標法違反	31	37	95	82	109	218	191	192	126	119
その他	249	267	334	343	393	491	752	748	629	842

情報セキュリティの3大要素

関連：pp.68-69

情報セキュリティ　コンピュータやネットワークを危険から守る

機密性　認可された者だけがアクセスできるようにすること
（不正アクセスや情報の漏えいがない）
- ●対策の例：IDとパスワード等による<u>ユーザ認証</u>

完全性　情報やその処理方法が正確・完全であること
（改ざんされていない・間違っていない）
- ●対策の例：<u>デジタル署名</u>

可用性　必要時には確実にアクセスできること
（紛失・破損・システム障害等がない）
- ●対策の例：ネットワーク回線<u>二重化</u>・データ<u>バックアップ</u>

マルウェア（コンピュータウイルス）の概要

関連：pp.70-71

●マルウェア（コンピュータウイルス）とは？
- 悪意をもって作られたプログラム。
- データやプログラム，電子メール，Webページ，USBメモリ等から広がる。

●マルウェアの機能
① 自己伝染機能：　他のシステムに自らの機能をコピーすること
② 潜伏機能：　ある時期まで，被害を及ぼさずに待機すること
③ 発病機能：　被害を及ぼす動作（ファイル破壊，データ流出，機能低下等）

●マルウェアの分類（厳密な分類はない）

マルウェア（広義のウイルス）
- ウイルス(狭義)　ファイルに寄生（例：マクロウイルス）
- ワーム　単独のファイルとして存在

マルウェア（広義のウイルス）
トロイの木馬　スパイウェア　ボット　等
スパイウェアは一般に下記①の機能をもたない

機密性を保つ対策1　ユーザ認証(個人認証)

関連：pp.72-73

認証　利用する権利の有無を確認すること
- ユーザIDとパスワード（望ましいPWは？・・・考察せよ）
- 生体認証(バイオメトリクス)：
  指紋・虹彩・網膜・静脈・掌形・顔・音声等

問い：　8文字でPWを作る。それぞれ何通り？
(1) 数字だけなら？
(2) 数字とアルファベット小文字なら？
(3) 数字とアルファベット大文字小文字なら？
(4) 1秒に200万パターン試した場合にPWを見つける最大時間は？

青少年科学館より

暗号文の例（シーザー暗号）

関連：p.72

シーザーが，部下に暗号文を送ったとする。何が書いてあるか？想像してみてください。

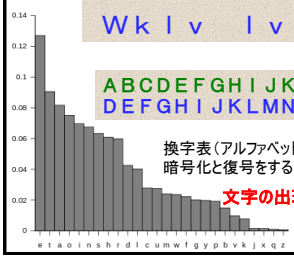
●解読するには，アルファベット3文字，前にずらすとよい。

This is a pen.

Wklv lv d shq.

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC



換字表（アルファベットをずらした一覧表・変換ルール）を参照して暗号化と復号をする。

文字の出現頻度などをもとにして解読されやすい。

共通鍵暗号と公開鍵暗号

関連：p.72

共通鍵暗号方式

- 同じ鍵を送り手と受け手の両方がもつ。
- 暗号化と復号では同じ鍵を使う。

問題点：鍵を受け手に安全に渡さなければならない。

錠・錠前

公開鍵暗号方式

- 二つの鍵（**秘密鍵**・**公開鍵**）を用意する。
  - ・**秘密鍵**で暗号化：**公開鍵**でなければ復号できない。
  - ・**公開鍵**で暗号化：**秘密鍵**でなければ復号できない。

公開鍵

誰に渡してもよい。

秘密鍵

自分専用。

問題点：本当に本人の公開鍵か？

ディジタル証明書（電子証明書）

関連：p.73

問題点：CがAだと名乗って秘密鍵を作り，その公開鍵をAの公開鍵だと偽る。

解決策：区役所の印鑑登録・印鑑証明と類似の方法。

認証機関（認証サーバ）⇨ **公開鍵**が本人のものであることを，第三者が確認・証明するしくみ。

ディジタル証明書（電子証明書）⇨ 認証機関が発行した証明。

このしくみを**公開鍵基盤**（**PKI**：public key infrastructure），公開鍵認証基盤等という。

可用性を高める方法の例

関連：p.75

記憶装置の二重化

●2つのハードディスクに同時に書き込む。
⇒情報の消失を防ぐ。

バックアップ

●データ等を定期的に別の装置に複写する。
⇒ ミス・攻撃への対策。

電源の二重化

●停電、自然災害、電源故障の対策。
⇒ 停止させない。

ネットワーク回線の二重化

●ネットワークの一部に問題が生じても、別ルートでアクセス可能にする。
⇒ 利用可能状態の維持。

ネットワークにおける詐欺

ワンクリック詐欺

サイト閲覧中に突然「会員登録完了。〇日までに〇万円をお支払い下さい。」等の画面を表示する，高額な架空請求詐欺。

フィッシング詐欺

実在企業(銀行・カード会社・SNS運営会社等)を装ったメールを送信して個人のログイン情報(カード情報やパスワード)を取得する詐欺。メールの内容やメール記載のリンクから表示されるログイン画面は，実在するものとよく似ていて見分けがつかない。

ファーミング詐欺

DNSサーバの情報を操作することで，不特定多数の人を偽サイトに誘導して，カード情報やパスワードを不正に入手する詐欺。

URL入力⇒DNSサーバにIPアドレス問合せ⇒ページ表示

例：www.yahoo.co.jp IPアドレス 183.79.131.212 等

ファーミング詐欺は，これらの関連付けを不正に書き換えて行う。

その他　ネット通販詐欺，ゲームアイテム詐欺，偽セキュリティソフト詐欺，・・・

情報技術の発展によって新たに問題が生じる。

⇒ それらに応じた法整備，モラルやマナー，セキュリティ意識が必要。

ネットトラブルへの対応

問題発生時の対応・正しい行動についての 考え方

●ネットでは，常に丁寧な言葉を使う。

●ネットでは相手が明らかに間違っていても，反論しない。
炎上を仕掛ける者，楽しむ者(面白半分の書込み等)は多数！

●ネット上では，相手の表情も声の抑揚も，年齢も性別も，実質**何も見えない**。何にでも**成りすます**ことができる。
基本的に何も信用してはいけない。**会うなんて**とんでもなく愚か。

●本名を名乗った⇒自宅の特定⇒押入に侵入された・・・という事例も不思議とは言えない。
知識不足で他の情報も漏らし続けているかも・・・。