第1章
情報社会

3節　情報社会の課題と対応
1-3-3　セキュリティ確保

情報セキュリティの3要素

関連：p130

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[ユーザ認証]

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：[デジタル署名]

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[二重化]・データ[バックアップ]

機密性を保つ対策1　ユーザ認証

関連：p131

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

機密性への攻撃(認証突破)方法例

関連：p132,136-141

- ●**ソーシャルエンジニアリング**（社会工学的手法）p140,141
  - 話術や盗み見等で保安上重要な情報を入手する。
- ●**キーロガー**（入力履歴を記録するソフトやハード）p138
  - ネットカフェの不特定多数が使用するPC等で注意。
- ●**スキミング**（読み取り装置をスキマーという）p138
  - 磁気カードの情報を複製してしまう。
- ●**不正アクセス**（クラッキング）p137
  - 脆弱性（セキュリティホール）を突いたり，マルウェアを利用したり・・。

キーロガー

関連：p138

キーボードの入力履歴を記録するソフトやハード
ネットカフェのような不特定多数が使用するPCでは，キーロガーによる情報漏洩が気になる。ソフトウェア型とハードウェア型がある。

スキミング（装置：スキマー）

関連：p138


before


after


小型


after


before

不正アクセス

関連：p132,136-141

不正アクセス（クラッキング）　個人や企業のコンピュータを不正に利用すること。
※不正アクセス禁止法：1999公布，2000施行。

侵入方法：
- 脆弱性（セキュリティホールを突く）
- マルウェアを使った，パスワードクラック等

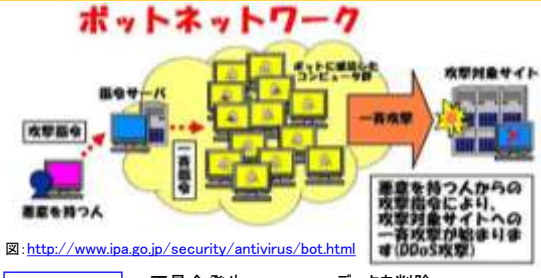
マルウェア（広義のウイルス）　トロイの木馬　スパイウェア　ボット　等

個人情報等を収集し，ネット上に送信してしまう。

侵入方法：
- ネットで配布されるソフトウエアについてくる。
- ウェブページを閲覧すると侵入してくる。

マルウェア　補足（ボットネットワーク）

関連：p128-129



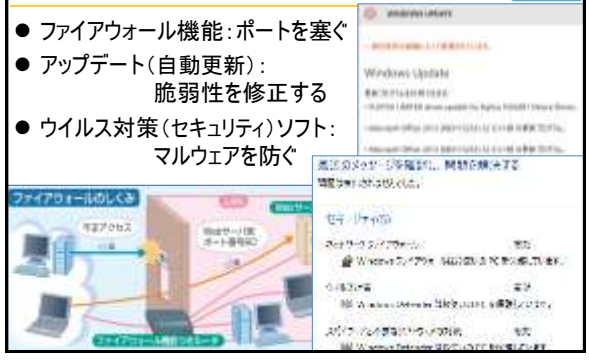
図：http://www.ipa.go.jp/security/antivirus/bot.html

ボット感染後の症状
- 不具合発生。
- データを削除。
- データやウィルスをメールで無作為に送信。
- 一斉攻撃（DoS攻撃，DDoS攻撃）等。

機密性を保つ対策２：侵入手段遮断

関連：p132

- ファイアウォール機能：ポートを塞ぐ
- アップデート（自動更新）：脆弱性を修正する
- ウイルス対策（セキュリティ）ソフト：マルウェアを防ぐ



情報の暗号化　機密性・完全性のために

関連：p133-134

暗号技術の必要性
- 携帯電話：無線で通信・・・盗聴の危険性
- インターネット：個人情報等を送る場合あり

暗号方式の例（換字法）

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。　例：シーザー暗号

ABCDE・・・
DEFGH・・・

●文字の出現頻度などをもとにして解読されやすい。

暗号文の例（シーザー暗号）

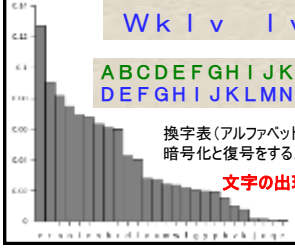
関連：p133-134

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：p133-134

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。

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？

ハイブリッド暗号方式（例：SSL/TLS）

関連：p135

① 共通鍵暗号方式：処理が速い。
② 公開鍵暗号方式：鍵の管理が容易だが処理複雑。

SSL/TLS

最初だけ②の方式を使って①用の鍵を渡す。
以降，①で暗号化して通信する。

次は暗号の応用へ・・・

- URLが https:// ・・・ならば，SSL/TLSが使われている。

ディジタル署名（電子署名）完全性のため

関連：p133-135

公開鍵
誰に渡してもよい。

秘密鍵
自分専用。

問い：私の**秘密鍵**で暗号化した場合，復号によって情報を確認できる人は**だれか？**
情報確認に加えて次のこともわかる・・・**それは何？**

私の**公開鍵**を所有できる**誰でも**，私が作った情報を確認できる。
同時に「**私が作った情報**である」と証明された。
（証明：私の**秘密鍵**で暗号化した。暗号化できるのは私だけ。）

ディジタル署名　鍵が印鑑・サインの役割を果たす。

ディジタル証明書（電子証明書）

関連：p135

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。

可用性を高める方法の例

関連：p130,140

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。

電源の対策（補足：可用性）

無停電電源装置（UPS）