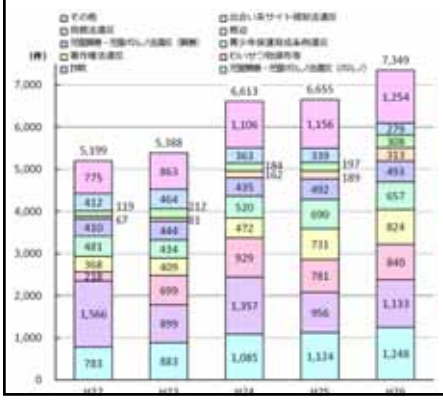
サイバー犯罪の現状(h22-26)

関連:p60



(https://www.npa.go.jp/kanbou/cybersecurity/H26_jousei.pdf)

情報セキュリティの3要素

関連:p60-65

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>

機密性を保つ対策2:侵入手段遮断

関連:p60-61

- 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

共通鍵暗号と公開鍵暗号

関連:p64

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?

ディジタル署名(電子署名) 完全性のため

関連:p65

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。

可用性を高める方法の例

関連:p61

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。