情報セキュリティの3要素

関連:p60

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認証

完全性 情報やその処理方法が正確かつ完全であること
（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:回線の二重化やバックアップ

情報セキュリティ(機密性)を保つ対策

関連:p61

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:指紋・虹彩・静脈・顔・音声等

- 認証突破の方法例
  - ◆ ソーシャルエンジニアリング(社会工学的手法)
  - ◆ キーロガー

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？

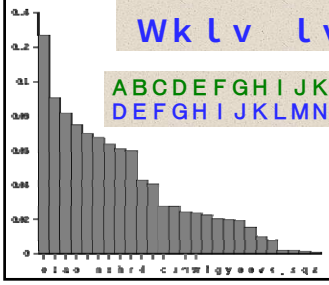
青少年科学館より

暗号の例

- 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



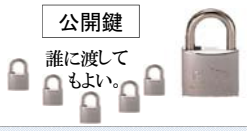
公開鍵暗号を例えると・・・

関連:p62

公開鍵暗号方式 ● 二つの鍵を用意する。

- ● 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。

問い： 私の公開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。

ディジタル証明書(電子証明書)

関連:p62

問題点：CがAだと名乗って秘密鍵を作り，公開鍵を公開しても通用してしまう。

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。