

# 情報セキュリティ

23j1-222

教科書P98-99

# この時間の目標

- 情報セキュリティ
- S 情報セキュリティについてよく理解でき、配慮して活用しようと思った
- A 情報セキュリティについてよく理解できた
- B 情報セキュリティについて理解できた
- C 情報セキュリティについて理解できなかった

# 35 情報セキュリティ

# 情報の機密性, 完全性, 可用性

- 情報セキュリティの目的
  - 機密性 (Confidentiality)
    - 認められた人だけがアクセスできる
  - 完全性 (Integrity)
    - 壊れたり改ざんされていない
  - 可用性 (Availability)
    - 必要なときに利用できる
- セキュリティポリシーを定める
  - 情報を扱うときの手順やルール
  - 結局は人が一番心配

# 情報の機密性を守る技術

- 個人認証

- 個人を特定して利用範囲を定める
- IDとパスワード
- 生体認証や多要素認証

- 暗号化

- 一定の規則に従ってデータ変換
- 変換ルールが分からないと内容が読み取れない

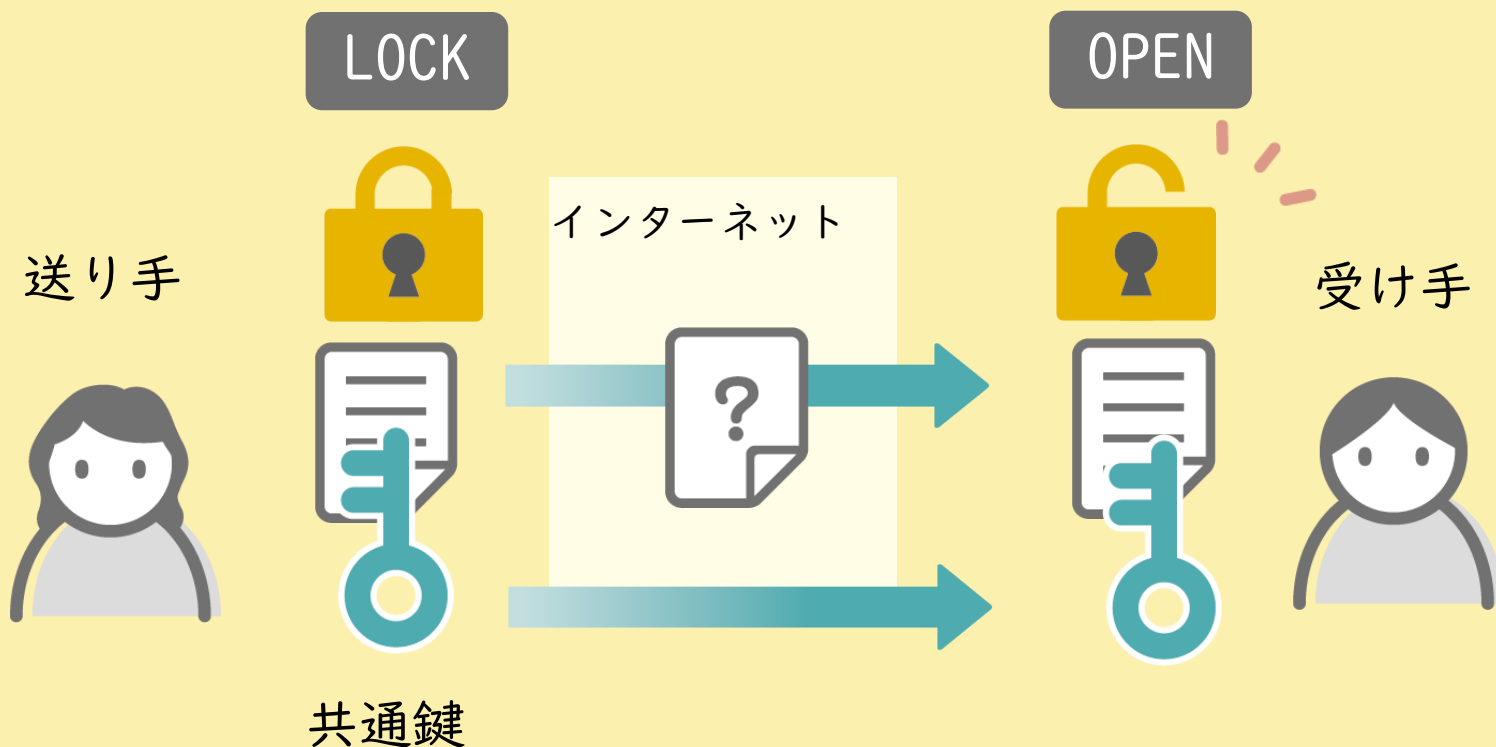
# 情報の機密性を守る技術

- 暗号の基礎要素
  - 共通鍵暗号
  - 公開鍵暗号
  - ハッシュ関数

# 情報の機密性を守る技術

## • 共通鍵暗号

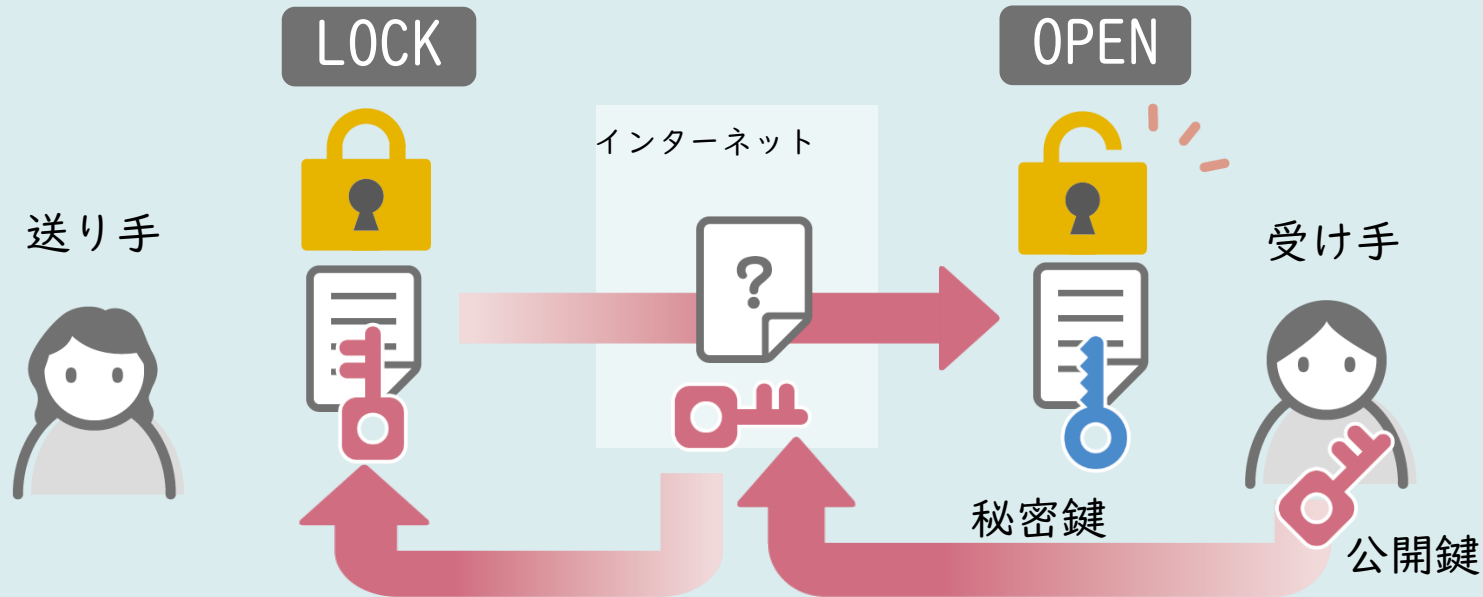
暗号化に使った鍵も相手に渡す。



# 情報の機密性を守る技術

## • 公開鍵暗号

鍵を掛けるときと開くときに異なる鍵を使う。  
送り手は受け手の公開鍵で暗号化し、  
受け手は秘密鍵で開ける。





# 情報の機密性を守る技術

- ハッシュ関数

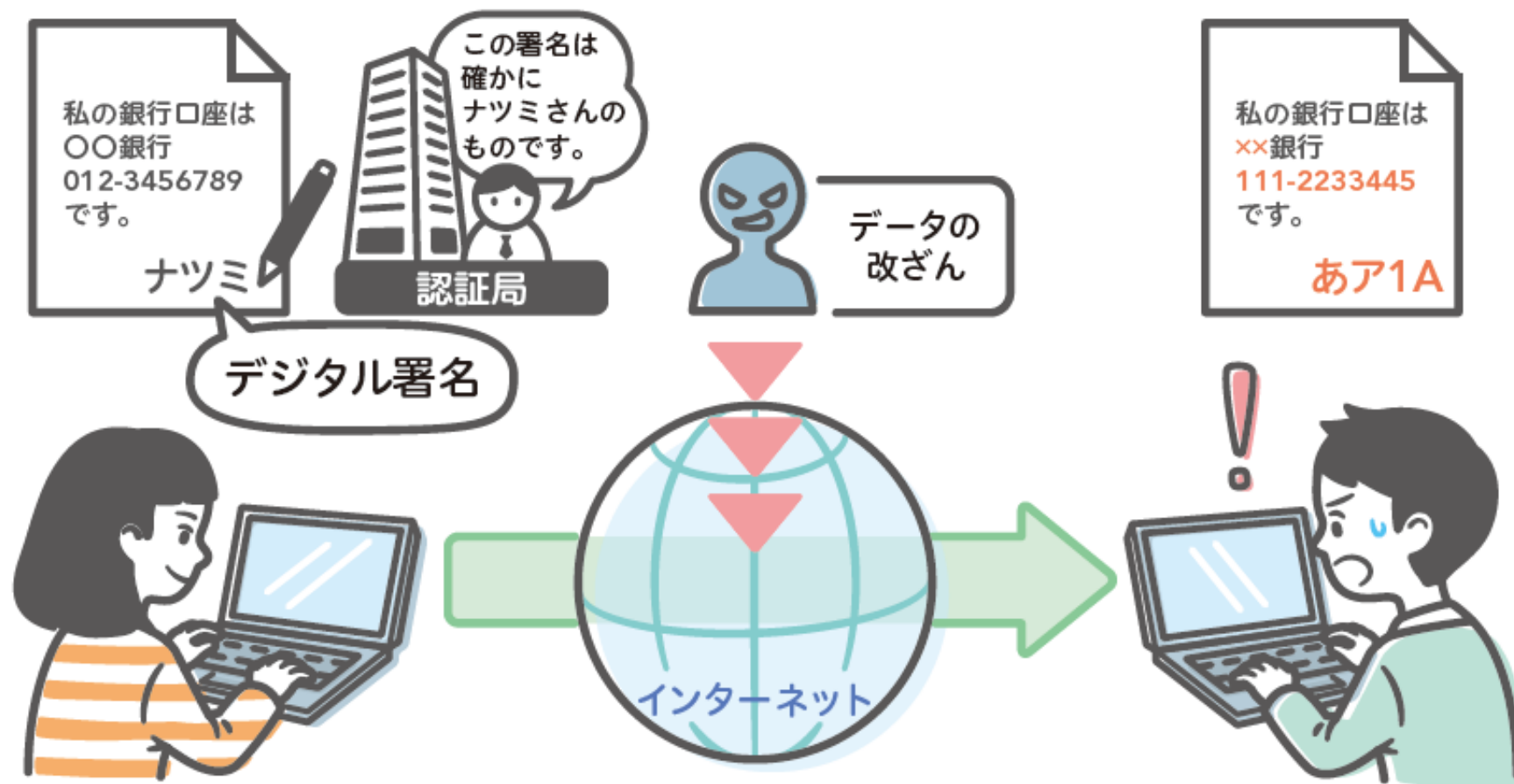
- 任意のデータを一定の長さに変換
- 同じ文字列→同じハッシュ値が得られる
- ハッシュ値から元の文字列は求められない

- Sha256の例

- 123123123:  
932f3c1b56257ce8539ac269d7aab42550dacf8818d075f0bdf1990562aae3ef
- 123123122:  
be5fd759fa07c0221a752f24c39cc11f55ce4ae78c77b8e39aaef9faf32a305

# 情報の完全性を守る技術

## • デジタル署名や電子認証



# 情報の可用性を守る技術

- バックアップ
- 冗長化(二重化・多重化)
- 不正アクセス等の防御
  - ファイアウォール
  - ウイルス対策