情報リテラシー（第4回 後期）ハンドアウト

サイバーセキュリティ2

---

1. 今日のねらい

- **暗号化の仕組み**と共通鍵・公開鍵暗号方式の違いを理解できる
- **デジタル署名と電子認証**の役割を説明できる
- **SSL/TLS**による安全な通信の仕組みを理解できる
- **電子透かしと誤り検出符号**の目的と使い方を説明できる

---

2. 暗号化の基本と方式

基本用語

暗号化： データを第三者が読めない形式に変換
復号： 暗号化されたデータを元に戻す
平文： 暗号化前のデータ / **暗号文：** 暗号化後のデータ

共通鍵暗号方式

仕組み： 同じ鍵で暗号化と復号
メリット： 高速処理 / **デメリット：** 鍵の配送が困難
代表例： AES（最も安全） / **注意：** DESは使用禁止
利用例： ファイル暗号化、VPN通信、無線LAN（WPA2/WPA3）

公開鍵暗号方式

仕組み： 公開鍵で暗号化 → 秘密鍵で復号
メリット： 鍵配送問題を解決 / **デメリット：** 処理が遅い
代表例： RSA
利用例： メール暗号化、デジタル署名、SSL/TLS通信

ハイブリッド暗号方式

共通鍵でデータ暗号化（高速） → 公開鍵で共通鍵を暗号化（安全）

👉 **HTTPS通信（SSL/TLS）で使用される方式**

---

3. デジタル署名とハッシュ関数

デジタル署名

役割： 電子文書の作成者証明と改ざん検出（紙の文書の「印鑑」に相当）
仕組み： 送信者が秘密鍵で署名 → 受信者が公開鍵で検証

効果： 認証・完全性・否認防止

ハッシュ関数

特徴： 任意データ → 固定長のハッシュ値を生成
性質： 同じデータ → 同じハッシュ値 / 少し変更 → 全く異なるハッシュ値
利用： ハッシュ値を暗号化して署名（データ量削減、高速化）

☞ **効率的で確実な本人確認と改ざん検出**

---

4. 電子証明書とSSL/TLS

電子証明書と認証局

電子証明書： 公開鍵が本人のものかを証明する電子文書（運転免許証のような身分証明書）
認証局： 電子証明書を発行する信頼できる第三者機関
証明書の内容： 所有者情報、公開鍵、有効期限、認証局の署名

SSL/TLS

役割： インターネット通信の暗号化プロトコル
3つの機能： ①暗号化（盗聴防止） / ②認証（本物か確認） / ③完全性（改ざん検出）
HTTP vs HTTPS： HTTP（暗号化なし） / HTTPS（SSL/TLSで保護、URLが「https://」）

SSL/TLS通信の流れ

ハンドシェイク： 接続確立 → 証明書送信 → 検証 → 共通鍵生成・交換
データ通信： 共通鍵で高速暗号化通信

☞ **ハイブリッド暗号方式による安全な通信**

---

5. 電子透かし

電子透かしとは

デジタルコンテンツ（画像、音声、動画）に**見えない情報を埋め込む**技術

目的と特徴

目的： 著作権保護、不正コピー追跡、改ざん検出
特徴： 圧縮・加工に耐える（頑健性）、品質を損なわない（不可視性）

種類と応用

可視型： テレビ局ロゴ、写真サイトの透かし文字
不可視型： 音楽ファイルの著作権情報、機密文書の追跡情報
応用例： 音楽・映画の著作権管理、紙幣・パスポート偽造防止

☞ **デジタル時代の権利保護に不可欠**

---

6. 誤り検出符号

誤り検出符号とは

データ通信や記録時のエラーを検出する技術（検査用ビットを付加）

パリティチェック

仕組み： データのビット数を偶数（または奇数）にする1ビットを追加
例： 1011010 → 10110100（パリティビット0を追加）
検証： 受信側でビット数を確認してエラー検出

特徴

利点： シンプルで実装が容易
限界： 2ビット以上のエラーは検出不可
発展： より高度な検査方式も存在

☞ **シンプルだが効果的なエラー検出方法**

---

7. 演習

演習1：証明書の確認

ブラウザでWebサイトの証明書を確認しよう

確認方法：
HTTPSサイトのURLバー左側の**鍵マーク**をクリック → 「この接続は保護されています」→「証明書」をクリック

確認項目： 発行先（ドメイン名）/ 発行者（認証局）/ 有効期限

演習2：パリティチェックでエラーを見つけよう

偶数パリティで送信された次のデータを確認。エラーがあるものはどれ？

A. 10110100 / **B.** 11010101 / **C.** 00111000 / **D.** 11110000

ヒント：1のビット数を数えて、偶数かどうか確認しよう！

---

8. まとめ

- **暗号化**は共通鍵・公開鍵・ハイブリッドを使い分ける
- **デジタル署名**で本人確認と改ざん検出を実現
- **SSL/TLS**により安全なWeb通信が可能に
- **電子透かし**で著作権保護、**誤り検出符号**でデータの完全性を保証

- 複数の技術を組み合わせた**多層防御**が重要

キーワード： 暗号化、復号、共通鍵暗号、公開鍵暗号、ハイブリッド暗号、AES、RSA、デジタル署名、ハッシュ関数、電子証明書、認証局、SSL/TLS、HTTPS、ハンドシェイク、電子透かし、誤り検出符号、パリティチェック、多層防御