

情報リテラシー（第3回 後期）

サイバーセキュリティ1

今日のねらい

- 情報セキュリティの3要素（CIA）を理解し、その重要性を説明できる
- サイバー犯罪の実態を知り、具体的な対策を説明できる
- マルウェアの種類と対策方法を理解できる
- 不正アクセスを防ぐための認証技術を説明できる

情報セキュリティの3要素 (CIA)

情報セキュリティの基本原則

機密性 (Confidentiality)

- **意味**：許可された人だけが情報にアクセスできる
- **具体例**：学籍番号、成績、個人のメール、パスワード
- **脅威**：情報漏洩、盗聴、不正アクセス

完全性 (Integrity)

- **意味**：情報が改ざんされていない、正確である
- **具体例**：レポートの内容、銀行の残高、ニュース記事
- **脅威**：データ改ざん、ウイルス感染、不正な書き換え

可用性 (Availability)

- **意味**：必要な時に情報にアクセスできる
- **具体例**：大学のシステム、メールサーバー、クラウドストレージ
- **脅威**：システムダウン、DoS攻撃、機器故障

サイバー犯罪の実態

身近なサイバー犯罪の種類

- **個人情報窃取** → 氏名、住所、電話番号、クレジットカード情報の悪用
- **アカウント乗っ取り** → SNS、メール、ゲームアカウントの不正利用
- **金銭被害** → ネットバンキング不正利用、偽サイト詐欺
- **なりすまし** → 他人になりすましてメッセージ送信、詐欺行為

被害の特徴

- **気づきにくい** → 発見が遅れ、被害が拡大しやすい
- **連鎖的被害** → 一度の漏洩で複数のアカウントが危険に
- **回復困難** → 一度流出した情報は取り戻せない
- **金銭的損失** → 直接的な金銭被害に加え、信用の失墜

実際の被害事例

事例1：SNS乗っ取りによる連鎖被害（2024年）

1. 攻撃者が友人Aのアカウントを乗っ取り
2. 乗っ取られたAから「SMS認証番号を教えて」とメッセージ
3. 善意で認証番号を教えた結果、自分のアカウントBも乗っ取られる
4. BからCへ同様の手口で被害が連鎖

→ 認証番号は絶対に他人に教えない！

事例2：大手企業へのランサムウェア攻撃

2. 窃取したアカウントで社内システムに侵入
3. ランサムウェアを展開し、システム全体を暗号化
4. 約25万人分の個人情報が漏洩

→ 個人も企業も日常的な警戒が不可欠

マルウェアの種類

- **ウイルス**：他のファイルに感染し、破壊や不具合を引き起こす
- **ワーム**：ネットワーク経由で自己拡散、感染を拡大
- **ランサムウェア**：ファイルを暗号化し、身代金を要求
- **スパイウェア**：個人情報を盗み出し外部送信
- **トロイの木馬**：正規ソフトを装い侵入、遠隔操作を可能にする

演習1：マルウェア感染シミュレーション

件名：【重要】大学システムからのお知らせ

送信者：system-admin@university-notice.com

本文：

全学生は添付ファイルの更新プログラムを実行してください。

期限：本日中

添付：system_update.exe

このメールの何が危険？どう対処すべき？

演習1の解答

1. 送信者ドメインが不自然
2. 実行ファイル (.exe) の添付
3. 緊急性を煽る ('本日中' など)
4. 不安を装う ('セキュリティ強化' など)

→ 添付を開かず、公式サイトで確認する習慣をつけよう

マルウェア対策

- **ウイルス対策ソフト**：リアルタイム保護・定義ファイル更新・定期スキャン
- **OS更新**：セキュリティパッチ適用・自動更新有効化・古いOSの使用禁止
- **安全な利用習慣**：不明なファイルを開かない・信頼サイトからDL・USB注意
- **感染時対応**：ネットワーク遮断→スキャン→パスワード変更→復元

不正アクセスと認証

不正アクセスの手口

- パスワードクラック／フィッティング／セッションハイジャック／SQLインジェクション

認証の3ステップ

1. 認証 (**Authentication**) : 本人確認
2. 認可 (**Authorization**) : 権限に応じたアクセス許可
3. 監査 (**Auditing**) : アクセス記録の保存・分析

多要素認証（MFA）

- **知識要素**（知っているもの）→ パスワード、PIN
- **所持要素**（持っているもの）→ スマホ、ICカード
- **生体要素**（本人の特徴）→ 指紋、顔認証

→ パスワードが漏れても突破されない！

演習2：フィッシングメールを見分けよう

件名：【緊急】Amazonアカウント停止のお知らせ
送信者：security@amazon-support.com
<http://amazon-security.com/verify>

件名：重要：Microsoft アカウントにサインインしました
送信者：account-security-noreply@microsoft.com
<https://microsoft-security.net/signin>

怪しい点を3つ以上見つけよう！

演習2の解答

フィッシングメールの怪しい点（例）

1. 送信元ドメインが偽物

- `@amazon-support.com` や `@microsoft-security.net` は公式ではない
- 公式は `@amazon.co.jp`, `@microsoft.com` など

2. URLのスペルミス

- `amazon-security.com` や `microsoft-security.net` など、1文字違いに注意

3. 緊急・恐怖を煽る表現

- 「アカウント停止」「緊急」「今すぐ」などの言葉で焦らせる

4. 不自然なリンク構造

- URLの一部に「login」「verify」「security」などが含まれる場合は注意

メール内リンクは開かず、必ず公式サイトやアプリから確認する！

フィッシング対策

- 緊急・恐怖を煽る表現に注意
- URLのスペルミスを確認
- 偽ドメイン使用に警戒
- 公式サイトを直接開く
- 多要素認証を設定

ファイアウォールとフィルタリング

- **ファイアウォール**：不正通信を遮断（パケット／アプリ制御）
- **ステートフルインスペクション**：通信状態を記憶して判断
- **ブラックリスト方式**：危険サイト遮断（利便性高）
- **ホワイトリスト方式**：安全サイトのみ許可（高セキュリティ）

VLAN (Virtual LAN)

- 同じ物理ネットでも論理的に分離
- **VLAN ID**で管理し、通信範囲を限定
- 効果：情報漏洩防止、負荷分散、柔軟な管理

情報セキュリティポリシー

- 組織の基本方針（パスワード規定、権限管理、報告手順）
- 個人の行動規範（強いPW、更新習慣、バックアップ）
- **3-2-1ルール**：3コピー・2媒体・1外部保存
- **現実的で継続可能なルールを設定**

まとめ

- CIA三要素がセキュリティの基本
- 多要素認証・ファイアウォール・VLANで防御を多層化
- フィッシング・マルウェア対策は日常の注意が鍵

感想をチャット欄に書こう！