第13回 サイバー攻撃と情報セキュリティ

2026/07/22

今回やること

1. 情報セキュリティの基本
2. 情報セキュリティの脅威
3. 情報を守るための技術

1. 情報セキュリティの基本

情報セキュリティとは

- 個人や企業、組織の大切な情報を守ること。
  - ✓個人情報や機密情報など
    （例：顧客名簿、クレジットカード情報）
- 多くの情報機器は、ネットワークでつながっている。
  - ✓このつながりを利用して、外部からのハッキングが可能になる。
- 従業員などによる無断の情報持ち出しなども考えられる。
- 技術、教育、法整備などの様々な観点から情報を守る必要がある。

情報セキュリティの3要素

- **機密性**
  - ✓許可された人だけが、情報にアクセスできる。
  - ✓例：パスワードによる保護、暗号化
- **完全性**
  - ✓情報が正しく保たれている。
  - ✓例：データの改ざん防止、アクセス権の設定
- **可用性**
  - ✓必要なときに、情報が利用できる。
  - ✓例：サーバーダウン対策、サーバーの冗長化

アルバイトが見えないはずの顧客情報が見えるぞ…

Wordの情報が勝手に書き換えられた！

課題を提出したいのにUNIPAにアクセスできない！

情報セキュリティ 最近の追加要素

- 真正性
  - ✓情報の発信元や利用者が正当である。
- 責任追跡性
  - ✓誰が何をしたかを記録し、確認できる。
- 否認防止性
  - ✓自分の行為を否定できないようにする。
- 信頼性
  - ✓情報やシステムが安定して正しく動作する。

正当なユーザであると確実にする。
例：ユーザ認証

ログや受領通知などで管理する。

バグなどがなく、意図したとおりに動く。
例：システムメンテナンスなど

演習1：セキュリティの7要素

演習

1. UNIPAからxxxx_13.docxをダウンロードする。
   ✓ xxxx部分を学籍番号に変更すること。
2. 演習1の問題を読み、解答すること。

2. 情報セキュリティの脅威

マルウェアとは

- 第三者によって、意図的に被害を及ぼすように作られたプログラムやソフトウェア
- 様々な種類がある。
  ✓ウイルス、ワーム、スパイウェアなど。
- 感染経路も様々である。
  ✓電子メールの添付ファイルやリンクを開く。
  ✓悪意あるWebサイトにアクセスする。
  ✓不正なソフトウェアをインストールする。
  ✓脆弱性を持つソフトウェアの隙をつく。

感染するとどうなるか

- PCの動作が重くなる。
- デバイスが勝手な動作をする。
  ✓メール送信する。
  ✓起動する。
- 変なポップアップ広告が表示される。
- 個人情報が抜かれる。
- 個人情報を人質に、お金を請求される。
- ネットワーク内のほかの機器に感染させる。

ウイルス

- コンピュータウイルスのこと。
- 自己伝染機能、潜伏機能、発病機能のいずれか1つ以上の特徴を持つ。
  ✓自己伝染機能
    ➢ 自らのプログラムを他のプログラムにコピーする。
  ✓潜伏機能
    ➢ 何らかの条件が満たされたときに、症状が出る。
  ✓発病機能
    ➢ プログラムやデータを破壊する。

ワーム

- 自身を複製して感染させていくマルウェア。
- ウイルスとは違い、ほかのプログラムを必要としない。
  ✓ネットワークに接続しただけで、感染するのもある。
  ✓一般的には、メールを介して感染することが多い。
    ➢ メールについてる添付ファイルとか。

トロイの木馬

- 有名なギリシャ神話が名前の由来となる。
- 一見、問題のない画像や文書ファイル、アプリなどに偽装して、デバイスの内部に侵入する。
- 外部から命令を受けると、その指示に従って、デバイスを操る。

スパイウェア

- 本人が気付かないうちに、デバイスにインストールされて、そのまま気付かれずに使われ続けるのが特徴。
- ユーザの個人情報や、アクセス履歴などを収集する。
  - ✓顧客情報を多く持つ企業やサービスでは、注意が必要。

キーロガー

- PCのキーボードでタイピングしたキーやスマートフォンでのタッチ操作を記録する機能。
  - ✓本来は、ソフトウェア開発時のデバック作業に役立てるための便利ツール。
- スマートフォンやATMなどに不正に設置されることで、パスワードやクレジットカード情報の不正利用につながる。
  - ✓見覚えのない機械が付いているATMで、情報を入力しない。

ランサムウェア

- 会社のPCやサーバに侵入し、保存されているファイルを勝手にロックした上で、元に戻す代わりに身代金を要求するプログラム。
  - ✓身近な例）アサヒグループのサイバー攻撃
- お金を払ったとしても、データが戻ってくる保証はない。
- テレワークの普及によるVPN機器やリモートデスクトップの脆弱性が狙われる。

脆弱性

- システムやソフトウェア、ネットワークに存在する弱点のこと。
- 脆弱性を入り口に、マルウェアを仕掛けたり、不正アクセスを行う場合がある。
- 普段からいくつも発見されており、定期的に修正パッチとよばれる修正プログラムが配布されている。
  - ✓WindowsやMacでも、定期的に配布されているため、アップデートが重要。

マルウェアの対策方法

- 脆弱性の解消
  - ✓定期的なソフトウェア更新・アップデート
- コンピュータウイルス対策
  - ✓アンチウイルスソフトを有効に活用。
    - ➢ 更新もする。
    - ➢ セキュリティ機能は安易に止めない。
  - ✓IoT機器もセキュリティ対策が必要
- 不用意なアプリケーションのインストール防止
- 情報のバックアップ

演習2：マルウェアの事例

演習

1. 演習2の問題を読み、以下を行え。
2. 授業内で扱ったマルウェアから、好きなものを1つ選ぶ。
3. そのマルウェアに関する実際に起きた事件や事例などを調べて、概要を書くこと。
   ✓ その際、参考にしたURLなども記載すること。

3. 情報を守るための技術

ユーザ認証

- 不正なアクセスを防ぎ、適切な権限のもとにシステムを運用するための仕組み。
  - ✓ログイン(ログオン)：システムを利用可能にする。
  - ✓ログアウト(ログオフ)：ログイン状態を打ち切る。
- ユーザ認証の方法
  - ✓ユーザIDとパスワード
  - ✓生体認証（指紋や虹彩、声紋など）
  - ✓ワンタイムパスワード（使い捨てのパスワード）

パスワードのお約束

- 推察が容易なパスワードは使用しない。
- 使いまわさない。
  - ✓パスワードの定期変更はあまり意味がないらしい。
- 紙に書いて保存や管理しない。
- パスワードの適切な運用は変わったりするので、こまめに確認しておくとよい。

- 最近では、ID・パスワードに加えて、SMSや認証アプリで発行されるコードを使って認証する、**2段階認証**が一般的。

アクセス権の設定

- 社内や学内の共有ファイルを閲覧・編集できる人を設定する。
  - ✓「読取」、「修正」、「追加」、「削除」がある。
  - ✓ファイルやディレクトリに応じて、ユーザごとに設定。
- 例：UNIPA
  - ✓学生アカウントでは、情報リテラシーⅠの受講者名簿は見えない。
  - ✓教員アカウントでは、受講者名簿がすべて閲覧可能。

暗号化と復号

- 暗号化
  - ✓情報を、第三者に読まれない(読まれても問題ない)ように変換する技術。
  - ✓例：Add(加える)→Bee(蜂)
- 復号
  - ✓暗号化された情報を、元の状態に戻す処理。
  - ✓例：Bee→Add
- 暗号化は、鍵とよばれるものを用いて行われる。
  - ✓例：1文字アルファベットをずらす。

ソーシャルエンジニアリング(1)

- 脅威となるのは、ウイルスだけではない。
- 攻撃を行ったり、攻撃の原因となるものを作り出す人間も、脅威の1つ。
  - ✓内部関係者、愉快犯、詐欺・故意犯など…
- 重要書類を持ち出したり、置き忘れたりしない、パスワードを放置しないなど、人間に対する教育が重要。
  - ✓これを、ソーシャルエンジニアリングという。
- フィッシング詐欺など、人を使った脅威はたくさん存在する。
  - ✓まずは事例を知ることが大事。

ソーシャルエンジニアリング(2)

- なりすまし
  - ✓電話やSNSで誰かになりすまし、情報を引き出す。
  - ✓社内ルールなどを厳密化することで防げる。
    - ➢ 電話では情報を教えない、など
- ショルダーハッキング
  - ✓パスワードなどを肩越しにのぞき見する。
  - ✓電車やカフェなどでは、極力パスワードを入力しない。
- トラッシング
  - ✓ゴミ袋をあさって、捨てられた資料から情報を見る。
  - ✓シュレッダーや溶解処理などを行う。

情報セキュリティのまとめ

攻撃方法	対策方法
ソフトウェアの脆弱性	ソフトウェア更新
マルウェア感染	セキュリティソフトの利用
パスワード窃取	パスワードの管理・認証の強化
詐欺などの誘導	脅威・手口を知る