情報システムと情報セキュリティ

サイバー犯罪

1　**不正アクセス行為に関する法律違反**

　他人のID，PWの不正利用や権限のないコンピュータの不正利用などの犯罪

2　**コンピュータ・電磁的記録対象犯罪**

　ホームページのデータを無断で書き換えたり、インターネットを利用して金融機関の他人の口座から自分の口座に無断で預金を移す行為などの犯罪

3　**不正指令電磁的記録に関する犯罪**

　コンピュータ・ウイルスの作成行為、ネット上でウイルスをばらまく行為などの犯罪。

4　**ネットワーク利用犯罪**

　①ホームページ上で他人を誹謗中傷する名誉毀損事件
　②電子掲示板などで犯行予告を行う脅迫事件
　③インターネットオークションでの詐欺事件
　④電子掲示板に販売広告を掲示して覚醒剤を販売した覚せい剤取締法違反事件
　⑤わいせつ図画・児童ポルノ等を不特定の人に閲覧させた事件

サイバー犯罪

5. PCユーザーに対するネットワーク犯罪の例

① 架空請求・ワンクリック詐欺

Webページや電子メールのURLやHTMLメールのリンクをクリックしただけで，契約が成立したかのようなページが表示され，料金を請求することを架空請求という。このような詐欺行為をワンクリック詐欺という。

② フィッシング詐欺

金融機関やクレジットカード会社などを装った偽のウェブサイトに誘導し，IDやパスワード，個人情報を盗む犯罪をフィッシングという。

③ ネットショッピング・ネットオークション詐欺

ネットショッピングやネットオークションでは，代金を支払ったにも関わらず，商品が届かない，あるいは，注文したものと異なるものが送られてくるケースがある。このような，詐欺行為をネットショッピング詐欺，ネットオークション詐欺という。

サイバー攻撃

1. **クラッキング**

不正にコンピュータに侵入し，データを破壊・消去したり，盗み出したりすること。

2. **DoS攻撃**

DoS(Denial of Service attack／サービス拒否攻撃) は，ウェブサービスが稼働しているサーバやネットワークなどのリソース（資源）に対して意図的に過剰な負荷をかけたり，サーバの脆弱性を利用しサービスを妨害したりすること。

演　習

【レポート①】
　一般のネットワーク利用者が，ネットワーク犯罪に巻き込まれる，或いは，加担してしまう事例（新聞などの記事：URLを付記すること）をそれぞれ1つずつ挙げよ。また，それぞれが起きないために必要な手立てを考え，あなたの意見を述べよ。

【レポート②】
国営放送や企業・病院を狙ったサイバー攻撃に関するニュースを調べ，
・攻撃の手法
・脆弱性の種類
・今後必要な対策
について述べよ。
ニュースの出処，参考文献リストをレポートの最後に参考文献リストとして記載すること。

情報セキュリティの確保

1　**技術的な取り組み（認証技術）**

・通常認証
アカウント（ユーザーID）とパスワードの組合せなど
・バイオメトリクス認証（生体情報）
顔，指紋，静脈などの情報
・2段階認証
スマートフォンのSMSやアプリを利用したりしてパスワードと組み合わせた 2 要素認証や，秘密の質問など利用者しか知り得ない情報を利用した2段階認証などが用いられている。

2　**組織的な取り組み（情報セキュリティポリシー）**

次の三つの視点が必要となる。
・機密性：許可された人だけが情報にアクセスできること
・完全性：情報が破壊されたり，改ざんされたりしていないこと
・可用性：情報を使いたいときにいつでも使えること

3　**個人的な取り組み**

情報モラルや情報セキュリティポリシーの遵守や，コンピュータウィルスなどの不正なプログラムに関する知識も必要。

不正なソフトウェア（被害や広がり方）

情報機器の利用者に被害を与えようという悪意をもって作成された不正ソフトウェアをマルウェアという。マルウェアはコンピュータウィルスやランサムウェアなどの上位概念である。マルウェアは大きく次の3つに分類される。

1. **コンピュータウィルス**
   他のプログラムの一部に混入して害を及ぼすもの。別のファイルに感染を広げる。

2. **ワーム**
   独立したプログラムである。ネットワークを介して自身をコピーし，実行することで被害を広げる

3. **トロイの木馬**
   正常なファイルに偽装したプログラム。開くことで攻撃を始める。自分自身のコピーはしない。

不正なソフトウェア（目的や機能による分類）

1. スパイウェア
　ユーザーの操作やパソコンの動作履歴を外部に送信する

2. キーロガー
　スパイウェアの一種で，ユーザーのキー入力の内容を外部に送信する

3. アドウェア
　強制的に広告を表示する

4. ランサムウェア
　機器やファイルを使えなくして，回復のために身代金を要求する

5. ワイパー
　ユーザーのファイルなどを抹消する

6. ドロッパー
　別のマルウェアに感染させる機能をもつ

7. バックドア
　攻撃者による遠隔操作を可能にする「裏口」を作る

8. マクロウィルス
　書類ファイルに含まれるマクロに攻撃用の処理が書かれたもの

9. ルートキット
　コンピュータの制御（権利権限）を奪い，検知を困難にしたり，攻撃をしやすくしたりするプログラムをまとめたもの

10. エクスプロイト
　脆弱性を悪用して攻撃するもの（攻撃行為そのものを指す場合もある）