情報セキュリティ informaticsI-031

教科書 pp.102-113

情報セキュリティの3要素

- 情報セキュリティとは
  機密性(Confidentiality),
  完全性(Integrity),
  可用性(Availability)
  を確保することである

情報セキュリティの3要素

- 機密性:
  情報を部外者からは見られないように秘密にし,
  情報を見ることが許された人のみがアクセスできる状態
- 完全性:
  情報が破壊, 改竄(書き換え)または
  消去されていない状態
- 可用性:
  情報にアクセスできる人が,
  アクセスしたいときにアクセスできる状態

サイバー犯罪

- コンピュータやネットワークを利用した犯罪の総称
  - 不正アクセス禁止法:
    他人のアカウント・パスワード等を利用することなど
  - コンピュータ・電磁的記録対象犯罪:
    コンピュータを不正に操作したり,
    データの窃盗・書き換え・破壊などを行うことなど
  - ネットワーク利用犯罪:
    ネットワークを利用してさまざまな犯罪を行うこと

主に機密性に関わる技術

- ユーザIDを用いたパスワードによる認証
  - ユーザIDがあり，それに対応するパスワードを知っている人は情報へアクセスできる

主に機密性に関わる技術

- フィルタリング
  - インターネットなどの通信情報を監視し，
    有害とされるサイトへのアクセス制限や
    職場・学校の私的利用の制限などに用いられる
    - アクセスしてはいけないサイトやカテゴリを指定する
      ブラックリスト方式と
      アクセスしてよいものを指定する
      ホワイトリスト方式などがある
  - 保護者がアクセス内容等を管理する場合は
    ペアレンタルコントロールと呼ばれる

主に機密性に関わる技術

- アクセス制御
  - ネットワークの利用において誰がどんな権限で
    アクセスするかをコントロールすること
    - IPアドレスなどにより,
      情報にアクセスできるかできないかを判別する
    - 生徒は成績データにアクセスできないが,
      教員は成績データにアクセスできる

主に機密性に関わる技術

- ファイアウォール
  - ネットワークの出入り口にソフトウェアとして設置し，データが内部に入ったり外部に送信されたりするデータを制限する
    - IPアドレスとプロトコルを確認して制御を行う
      - (HTTPS通信のみを用いる)Webサーバに SMTPを利用して通信のは異常であり，制限するなど

主に機密性に関わる技術

- 暗号化
  - 情報を送信するとき，
    データが盗聴されても内容がわからないようにする技術で，
    暗号化する前の元の文を**平文**，暗号化された文を**暗号文**，
    暗号文を平文に戻すことを**復号**という
  - 暗号化や復号に使われる規則を**鍵**という
    - 共通鍵暗号方式
      - 暗号化と復号に同じ鍵を使う方式
    - 公開鍵暗号方式
      - 暗号化はネットワーク上に公開鍵，
        復号にはある特定のものだけが持つ秘密鍵の二つを
        用いる方式

主に機密性に関わる技術

- SSL/TLS（HTTPS）
  - Webページ上での情報のやりとりで用いられる暗号化技術
    - SSL/TLSで暗号化されたWebページのURLは「https://」から始まっていて，この通信プロトコルをHTTPSという

主に機密性に関わる技術

- VPN
  - HTTPSを用いて，インターネットなどを経由して外部のLANにつなぐ仕組み
    - 暗号化してつなぐため盗聴されず使用者がLANへ直接つないでいるような状態を実現する技術

主に完全性に関わる技術

- デジタル署名
  - 受け取ったデータが，
    本当にそこに書かれている送信者のものであるかを
    確認する技術
    - 送信者が送信するデータの要約文を
      秘密鍵で暗号化したもの（デジタル署名）を，
      受信者が**公開鍵**で復号して得られる要約文と，
      受信したデータ（平文）から作られる要約文が
      同一であるかによって本人であることを確認する

主に完全性に関わる技術

- 受信者が利用する公開鍵が，
  公開鍵に添付した電子証明書を用いて，
  送信者の秘密鍵に対応するものであることを，
  第三者が証明する技術を電子認証という

主に可用性に関する技術

- バックアップ
  - プログラムやデータが壊れたり紛失したときに備えて，別の記録メディアに保存しておくこと
- UPS
  - 無停電電源装置のことであり，停電してもある一定の時間電源を供給するシステム

マルウェア対策

- マルウェアまたはウイルスと呼ばれる悪意のあるソフトウェアへの対策
  - マルウェアは
    ウイルス, トロイの木馬, ワームなどに分類される

マルウェア対策

- ウイルス:
  自分自身で増殖し,
  ほかのファイルやシステムに影響する
- トロイの木馬:
  自分自身では増殖せず,
  普通のプログラムのように振る舞いながら
  不正な動作をする
- ワーム: 自分自身で増殖し, 単独で活動する
- その他には,
  情報を勝手に送信するスパイウェア,
  意図しない広告を表示するアドウェア,
  ファイルを暗号化して金銭を要求するランサムウェアなどが
  存在する

マルウェア対策

- ウイルス対策ソフトウェア
  - ウイルスを取り除くソフトウェア
    - すでに知られているウイルスのデータ(定義ファイル)を確認して，コンピュータ内のウイルスを発見・駆除する

マルウェア対策

- ソフトウェアの更新
  - セキュリティホール(ソフトウェアの欠陥)から
    ウイルスが入り込むことが多いため,
    OSやアプリの更新で
    過去に見つかったセキュリティーホールを減らす

情報セキュリティポリシー

- 企業に起こりうる情報セキュリティの脅威には
  さまざまなものがある。
  これらの脅威から情報を守るための方針や行動指針を
  情報セキュリティポリシーという。
- 通常, 基本方針・対策基準・実施手順の三つの階層で
  記述されている