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
  ◦ 機密性: 情報を部外者からは見られないように秘密にし，許可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

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
・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
・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
・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 を利用しての通信は異常であり，
      制限するなど
・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あり，暗号化する

  前の元の文を(①　　)，暗号化された文を(②　　)，

  暗号文を平文に戻すことを(③　　)という

  ◦ 暗号化や復号に使われる規則を(④　)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
・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
・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(⑤　　)で暗号化したもの（デジタル署名）を，

    受信者が(⑥　　)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
    ▪ 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
    ▪ 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
・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
・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