基礎現代文化学
情報技術演習　第12回

情報セキュリティ

http://www.kyoto-su.ac.jp/~iyori/info/

情報セキュリティとは

- 明確な定義は定まっていないが、「情報資産の機密性・完全性・可用性を確保する」との意味で用いられる。

- コンピュータ上にある重要な情報（近年では特に個人情報）に対する不正なアクセス、情報の盗難、データ漏洩や破壊などから守るための方策を理解し、実践することが重要である。

パスワードによる認証

- パスワード（password）：特定のシステムを利用する正規ユーザの暗証コード。
- コンピュータへのログイン、特定のシステムの利用などに幅広く用いられるユーザ認証の方式で、通常は英数字の組み合わせからなる。
- パスワードを決定する際には「自分が覚えやすく他人に推定されにくいもの」を重視するとよい。
- また、パスワードは随時変更し、長期間同じものを使用しない方が安全である。

パスワードの強弱

- 弱いパスワード：ユーザの名前や年齢、学生番号、続き数字や意味のある英単語など他人に推定されやすいもの。

- 強いパスワード：以下のような特徴を持つもの。
  ①長さが一定文字数以上(システムによって異なるが、例えば8文字以上)
  ②文字(アルファベットの大文字・小文字)、数字、記号(!,#,$,%,&,^,¥,@,:,;等、ただしシステムによっては使用できる記号に制限があり)の組み合わせ
  ③本人が記憶しやすい(一定回数間違えてしまうと、再発行の手続きを要するシステムもある)
  ④他人から推定しにくい

バイオメトリクス認証（生体認証）

- 生体特有の情報を事前に登録し、ユーザのものと一致するかどうかによって認証をおこなう。近年開発が進んでおり、建物への入室管理、銀行のATMシステムやPCへの導入もおこなわれている。ただし認証精度や不正対策が万全とは言えず、パスワード等との併用によって安全性を高めておく必要がある。
- 主なバイオメトリクス認証方式

  ・指紋

  ・静脈

  ・虹彩

  ・網膜　など

不正アクセス

- 不正アクセス：コンピューターを使って、利用を許可されていないシステムにアクセスすること。

- 「不正アクセス行為の禁止等に関する法律」における定義

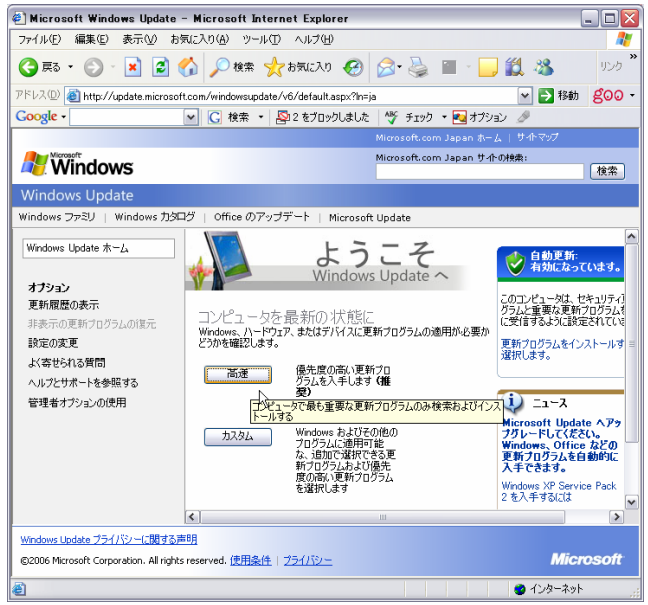
（1）他人のIDを利用して、本来与えられている権限以上の情報の閲覧または利用をすること。

（2）脆弱性などを利用して、制限されている行為を行うこと。

（3）他のネットワーク機器を利用して、制限されている行為を行うこと 。

システムの脆弱性

- システムの**脆弱性**：悪意のあるユーザーがシステムに対して、不正な行為を行う際に利用するセキュリティ上の問題箇所。
- ソフトウエアの設計・設定ミスによって生じた問題箇所を「セキュリティホール」と呼ぶ。
- 脆弱性が発見された場合は速やかに（開発者から提供される）修正プログラム等でシステムの更新をおこなう。定期的にシステムの診断、修正をおこなうとよい。



Windows Updateの画面

暗号化

- 暗号化：許可された者だけが情報を読むことができるよう、一定の規則に従って情報を変換すること。機密性を要する通信などにおいて広く用いられている。

- **共通鍵暗号方式**：暗号化した情報の送り手と受け手が同じ暗号鍵を使用する方式。処理が高速であるが第三者に鍵を知られないように管理する必要がある。
- **公開鍵暗号方式**：送り手と受け手が異なる鍵を用いる暗号化方式。「公開鍵」と「秘密鍵」のセットからなり、公開鍵で暗号化した情報は秘密鍵でのみ、秘密鍵で暗号化した情報は公開鍵でのみ解読（復号）できる。

※鍵とは暗号化の手順を制御するためのデータのこと。

SSL（Secure Socket Layer）

- 公開鍵と共通鍵の2つの暗号化方式を組み合わせて情報を送受信する方式で、ブラウザを使用した個人情報の送受信、金銭の決済のためのクレジット情報の送受信などに使用されている。

- https://　ではじまるWebサイトはSSLを使用したもの。

- SSL通信ではまず公開鍵方式によるサーバ認証をおこない、その後にサーバークライアント間で共通鍵を生成する方式をとる。

参考

http://www.verisign.co.jp/repository/faq/SSL/

コンピュータウイルス

- 通商産業省が制定した「コンピュータウイルス対策基準」による定義

第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を一つ以上有するもの。

（1）自己伝染機能
自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能

（2）潜伏機能
発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、条件が満たされるまで症状を出さない機能

（3）発病機能
プログラムやデータ等のファイルの破壊を行ったり、コンピュータに異常な動作をさせる等の機能

コンピュータウイルス（2）

- ウイルスの感染経路：フロッピーディスク等のメディア
  →ネットワーク（電子メール、Webサイト等）中心に変化
- ウイルスへの対応：
  ◆定期的なシステム更新、脆弱性への速やかな対応
  ◆ウイルス対策ソフトの導入
  ◆覚えのない電子メールを開かない（特に添付ファイルを実行しない）、不必要なWebサイトを閲覧しない
- 感染した場合、または感染が疑われる場合は速やかに対策ソフトを用いて駆除をおこなう。可能であればネットワーク接続は切っておいたほうがよい。

著作権の保護

- 著作権：著作物に発生する権利。著作権法上の著作物は「個人の思想や感情を創作的に表現したものであって、文学、学術、美術、又は音楽の範囲に属するもの 」と定義される。
- ネットワーク上ではテキスト、画像、映像、音楽などの複製が容易であり、またデジタルデータは劣化が少ないことから著作権の保護は重要な課題となってきている。
- 著作権の保護にはDRM（Digital Rights Management）と呼ばれるデジタルコンテンツ保護のための技術のほか、法整備や倫理の周知など様々な側面が重要となる。

著作権の保護(2)

- 電子透かし:通常の視聴では判別できないような形で著作権情報を埋め込み、著作者の所在を明確にするための技術。不正コピーをはじめ、一部を切り取ったり加工してもデータが失われないようになっている。

参考

http://softplaza.biglobe.ne.jp/text/1999sp/dwmark/dwmark-index.html

http://www.jpo.go.jp/shiryou/s_sonota/hyoujun_gijutsu/denshi_sukashi/

情報セキュリティと法制度

- 不正アクセスの禁止や個人情報の保護などについて、日本でも法律の整備が進んでいる。代表的なものは下記参照。

http://www.soumu.go.jp/joho_tsusin/security/kiso/k05.htm

http://www.kantei.go.jp/jp/it/privacy/houseika/hourituan/

参考リンク

- 国民のための情報セキュリティサイト
  http://www.soumu.go.jp/joho_tsusin/security/index.htm

- セコムトラストネット
  http://www.secomtrust.net/secword/index.html

- 情報処理推進機構：セキュリティセンター
  http://www.ipa.go.jp/security/