

ICT リテラシー (情報技術論) A

-- 第 05 回 : セキュリティ --

栗野 俊一

講義内容の静止画・動画での撮影、及び SNS 等への転載を固く
禁じます

2022/10/14 ICT リテラシー (情報技術論) A

伝言

私語は慎むように !!

□ 席は自由です

- できるだけ前に詰めよう
- コロナ対策のために、ソーシャルディスタンスをたもとう

□ 色々なお知らせについて

- 栗野の Web Page に注意する事

<http://edu-gw2.math.cst.nihon-u.ac.jp/~kurino>

- google で「kurino」で検索

前回 (第 04 回) の復習

ICT リテラシー (情報技術論) A

前回 (第 04 回) の復習

講義内容の静止画・動画での撮影、及び SNS 等への転載を固く禁じます

前回 (第 04 回) の復習

□ 前回 (第 04 回) の復習

○ 講義内容：最近の情報社会のキーワード

- ▶ ユビキタス社会 (Text P.13, 1.3 節)：どこでもコンピュータとネットワークが使える社会
- ▶ IoT (Text P.14, 1.4 節)：モノがインターネットに接続する
- ▶ Web 2.0 (Text P.15, 1.5 節)：双方向サービスによる新しい利用形態(8:2の法則)

今週 (第 05 回) の概要

ICT リテラシー (情報技術論) A

今週 (第 05 回) の概要

講義内容の静止画・動画での撮影、及び SNS 等への転載を固く禁じます

今週 (第 05 回) の予定

□ 今週 (第 05 回) の予定

- 前回の残り: 資料も前回のものを利用する
 - ▶ 人工知能 (Text P.17, 1.6 節) : より人間に近いサービスを提供する
- 講義 : セキュリティ
 - ▶ ネットワークセキュリティ (Text p.32, 2.8 節)
 - ▶ パーソナルセキュリティ (Text p.33, 2.9 節)
 - ▶ 暗号化 (Text p.37, 2.10 節)

今週 (第 05 回) の目標

□ 今週 (第 05 回) の目標

○ 講義

- ▶ セキュリティに関する基本的な概念を身に付ける
- ▶ セキュリティに関する技術的知識(ファイヤーウォール, 公開鍵暗号)を知る

今週 (第 05 回)

- 前回 (第 04 回) の課題
 - Web Class「小テスト-3」
- 今週 (第 05 回) の課題
 - Web Class「小テスト-05」

セキュリティ

ICT リテラシー (情報技術論) A

セキュリティ

講義内容の静止画・動画での撮影、及び SNS 等への転載を固く禁じます

セキュリティ

□ セキュリティとは

○ セキュリティ (security) そのものの意味は、「安全」、「保全」、「保護」

▶ 何かを守り、安心してサービスが受けられる状態

○ 「情報セキュリティ」

▶ How : 暗号や防御のためのソフトウェア、アクセスの制限などを用いる

▶ Which : データやシステム、通信経路などを保護する

▶ What : 機密漏洩や外部からの攻撃、改ざんなどの危険を排除する

○ 「何を守る」かで利用される技術が異なる (共通のものもある)

▶ サーバを守る : ネットワークセキュリティ

▶ 個人の情報を守る : パーソナルセキュリティ

○ 保険の考え方

▶ (セキュリティ)事故が起きないようにする(防御)の他に、起きた後の被害を軽減する

▶ 例 : バックアップ

ネットワークセキュリティ

□ ネットワークセキュリティとは

- サーバ：サービスを公開するために、ネットワークから匿す事ができない

 - ▶ インターネット(危険)とサーバ(守る対象)の間(のネットワーク上)に守る仕組みが必要 => ファイアーウォール

□ ファイアーウォールの役割

- ネットワーク上の通信を監視して、危険なパケットを遮断する

 - ▶ フィルタリング (パケットの類別)

□ DMZ (DeMilitarized Zone)

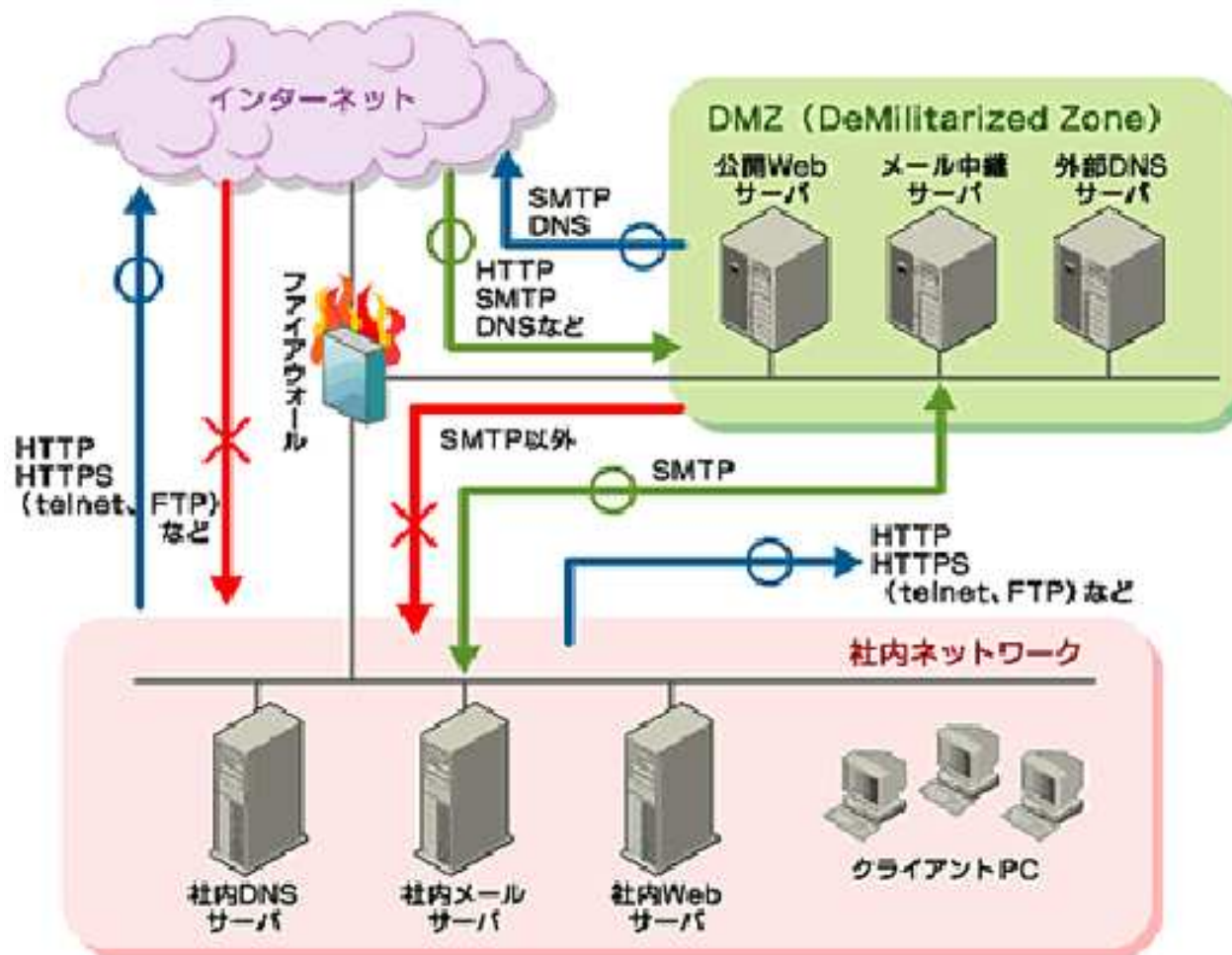
- 信頼できないネットワークと信頼できるネットワークの中間に置かれるネットワーク領域のこと

- ファイアーウォールを二つ組み合わせて作る

 - ▶ 信頼できないネットワークと信頼できるネットワークの通信を仲介

 - ▶ 信頼できないネットワークと信頼できるネットワークの直接の通信を避ける

ネットワークセキュリティの概念図



(c)

パーソナルセキュリティ

□ パーソナルセキュリティ

○ 個人の利用する PC や携帯電話を防る

- ▶ 基本クライアントなので、守りやすい (ファイアーウォールの内側に置く)
- ▶ 公共の WiFi 等はリスクが高い

□ パーソナルセキュリティの技術

○ ウイルス対策ソフト

- ▶ パターンファイルを用いて、コンピュータウイルスを発見し、駆除する
- ▶ 新しいウイルスに対応するには、パターンファイルの更新が必要

○ OS のアップデートとバックアップ

- ▶ OS のバグ(誤り)を利用してウイルスが感染する
- ▶ 誤りの修正が必要 (OS のアップデート)

○ ソーシャルハックへの対応

- ▶ 利用者を勘違いさせて、悪意あるプログラムを取り込ませる (トロイの木馬)
- ▶ 公共端末でのトラップ (キーロガー)

○ WiFi と暗号化

- ▶ 無線は、盗聴のリスクがあるので、より強い暗号化技術を用いるべき
- ▶ VPN (Virtual Private Network) で通信経路を暗号化する

○ 認証とパスワード管理

- ▶ 自分と他を分けて、安全な環境で、データを操作するための基礎

パスワード管理

□ パスワード管理

○ パスワード：通信相手に「自己」を示すための情報

- ▶ 「パスワードが盗まれる」=「自分自身が盗まれる」
- ▶ EcoLink のパスワードがバレる：勝手に科目登録されたら
- ▶ NuAppsG のパスワードがバレる：自分の名前で、悪口メールを送られたら
- ▶ 銀行講座の暗唱番号がバレる：勝手にネット注文され...

○ パスワードの共有はしてはいけない (他人に自分を委ねる行為..)

□ 良いパスワード/悪いパスワード

○ 悪いパスワード

- ▶ 個人情報から安易に推測できるパスワード (渾名や、生年月日)
- ▶ キーボードのキーの並びや、英単語

○ 良いパスワード:自分しか知らない情報(Key)と規則的変換(乱雑化)の組み合わせ

- ▶ 例1: 情報:最近、自分が好きになった人、3名/変換規則:頭文字(2文字)と生年(下2桁) => $(2+2) \times 3 = 12$ 文字のパスワード
- ▶ 例2: 情報:10 Word 程度の文章/変換規則:基本 Word の先頭を取るが、3 Word 毎に、Word の長さにする
- ▶ パスワードジェネレータを使い、パスワードリストを管理

暗号化技術

ICT リテラシー (情報技術論) A

暗号化技術

講義内容の静止画・動画での撮影、及び SNS 等への転載を固く禁じます

暗号化技術

□ 暗号とは (Text P.37, 2.10 節)

○ 通信内容(平文[ひらぶん])を、一定の規則で書き換え(暗号化)、第三者に読めなくする技術(暗号文)

▶ 通信相手には、暗号文から平文へ戻す(復号化)手段が与えられている

▶ 通信内容の盗聴だけでなく、ファイルの盗用による情報流出をさけるためにも利用可能

□ 暗号形式の種類

○ 秘密鍵(対称鍵/共通鍵)暗号：暗号化と復号化の鍵が共通な暗号方式 (例:シーザ暗号)

▶ 通信の送り手と受け手が同じ鍵を保持する必要がある(鍵の配付問題)

○ 公開鍵暗号：暗号化の鍵(公開鍵:public key)と復号化の鍵(個人鍵:private key)が別になっている暗号方式 (例: RSA)

▶ 暗号化の鍵(公開鍵)を一般に公開する事ができる(配付の問題がない)

▶ 個人鍵を秘匿する事により、認証にも利用できる

□ 電子署名

○ 個人鍵で暗号化する(と公開鍵で復号化できる..)事により、「電子署名」が可能

▶ 電子署名を利用する事により、色々な事を「保証」できる (cf. ビットコイン)

PKI : 公開鍵暗号基盤

□ PKI (Public Key Infrastructure : 公開鍵暗号基盤) とは

- 個人と個人鍵を結び付ける仕組み (電子証明書の発行)
 - ▶ CA (Certificate Authority: 認証局) に公開鍵を登録して、保有を証明してもらう

□ PKI の役割

- 誰でも、暗号通信が可能になる
 - ▶ 個人と公開鍵が対応付けられるので、それで暗号化が可能
- 誰でも、電子署名が可能になる
 - ▶ 自分の個人鍵を利用した電子署名が可能に

□ https の仕組み

- Web サーバが、CA 局から、電子証明書を発行してもらう
- 通信をする時に、この電子証明書にある鍵を利用して通信
 - ▶ 暗号通信だけでなく、本人証明も可能になる

おしまい

ICT リテラシー (情報技術論) A

おしまい

講義内容の静止画・動画での撮影、及び SNS 等への転載を固く禁じます