# インターネットとセキュリティ

情報ネットワーク工学入門

只木進一（理工学部）

# セキュリティインシデントは他人事ではない

- 個人情報の漏えい
  - 民間企業からの顧客情報の漏えい
  - 公的機関からの個人情報漏えい
- 信用してアクセスしたサービス
  - 乗っ取られていて、不正プログラムを押し込まれる

# セキュリティインシデントは他人事ではない

- 個人のPCやスマートフォーンからの情報漏えい
  - 自分の情報だけでなく、他人の情報
- 様々なサービスのID
  - 乗っ取り、なりすまし
- 自分のデバイスが、攻撃の足場に使われる

# 最近起こっているインシデント

- 突然PCの画面の色が変わり、遠隔操作アプリを導入され、金銭を要求される
- 宅配便到着SMSを開くと、ウィルスをダウンロード
- 宅配便到着SMSを開くと、何かのIDとパスワードを要求

# 情報セキュリティ10大脅威(ICT threats)2020

| 順位 | 個人 | 組織 |
|---|---|---|
| 1 | スマホ決済の不正利用 | 標的型攻撃による情報流出 |
| 2 | フィッシングによる個人情報等の詐取 | 内部不正による情報漏えい |
| 3 | クレジットカード情報の不正利用 | ビジネスメール詐欺による金銭被害 |
| 4 | インターネットバンキングの不正利用 | サプライチェーンの弱点を悪用した攻撃の高まり |
| 5 | メールやSMS等を使った脅迫・詐欺の手口による金銭要求 | ランサムウェアによる被害 |

https://www.ipa.go.jp/security/vuln/10threats2020.html

# 個人情報漏洩事案

- 2019/11/11 室蘭工業大学
  - サーバ設定ミスで、1187件の学生情報が外部から閲覧可能に
- 2019/11/7 トレンドマイクロ
  - 従業員が12万人の個人情報を持ち出し
- 2019/10/29 鈴鹿市
  - 教諭が生徒情報の入ったUSBを紛失

# 個人情報・プライバシーとその管理

- 個人情報：生存している個人をそれだけで特定する情報
  - 氏名や住所は重要な要素だが、それだけではない
  - 個人の属性から特定できる場合がある
    - 職業、出身大学、電話番号などの組合わせ

- プライバシー
  - 以下の三つの要件を満たす
    - 個人の私的生活の事実
    - 公知でないもの
    - 公開を望まない
  - 本人の属性に関する情報のうち、他人に知られたくないもの

# プライバシーの例

- 図書館は利用者の秘密を守る
  - 何を読んだか、借りたか
  - 図書館の自由に関する宣言
- 購買履歴
- 病歴、投薬履歴
- 友人関係

# 情報セキュリティの構成要素

- 機密性：confidentiality
  - 秘密であること
  - 許可された人だけが利用できる
- 完全性：integrity
  - 正式で正しいものであること
- 可用性：availability
  - 必要なときに利用できること

- 三つの要素のバランスが重要
  - 情報システムとしてのバランス
    - システムの目的に合致しているか
  - 情報システムの運用の観点
    - システムとして運用できるのか
  - 費用と効用の評価
- 公開情報にもセキュリティがある
- 情報システムは手段に過ぎない

# 情報セキュリティの対策

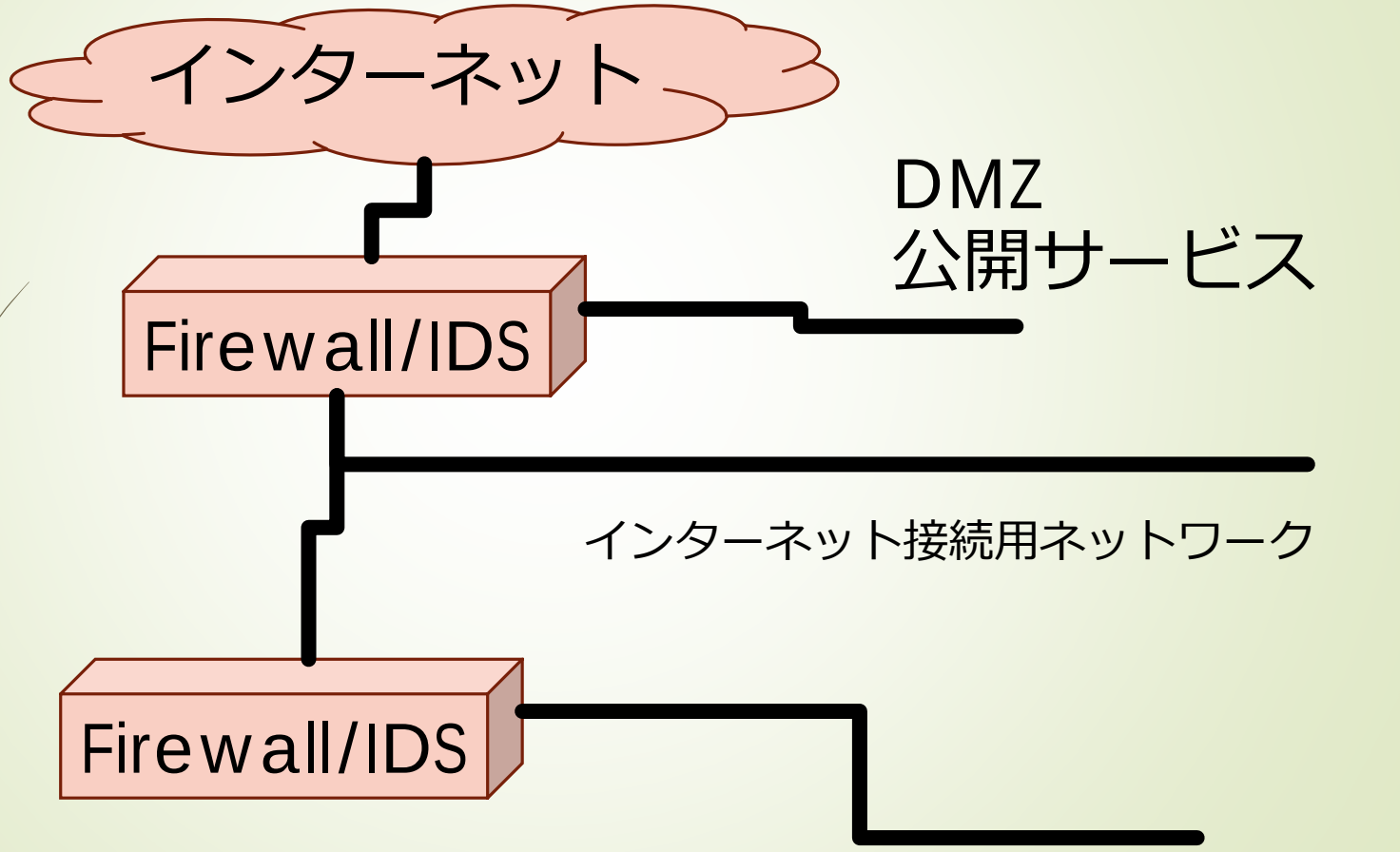
- 問題が発生しないための対策
  - 不正通信が起こらないように
  - ウィルスが入り込まないように
  - 不正侵入が起こらないように
- 問題の発生を想定した対策
  - 不正通信の確認と遮断の方法
  - 重要情報の暗号化
  - 重要情報の分散

- 問題が発生した後の対策
  - 緊急退避
  - 連絡・通報・責任体制
  - 影響範囲の迅速な確認方法
  - 適切な公表
- 問題の再発を防ぐ対策
  - 原因の究明と対策
  - リスクとコストの再評価

# 技術的対策：通信路の対策

- ネットワークの分離
  - 重要情報を持つネットワークを切り離す
- Firewall
  - 送受信元、サービスで通信を制限
- IDP(Intrusion Detection System)
  - 侵入の兆候を検知して遮断

# ネットワークの構成例

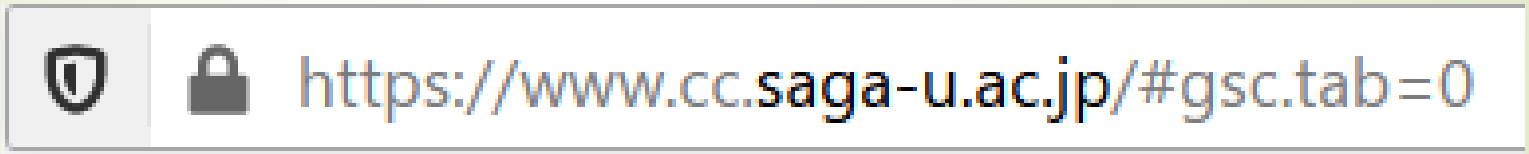

インターネット
DMZ
公開サービス
Firewall/IDS
インターネット接続用ネットワーク
Firewall/IDS
重要情報を扱うネットワーク

# 技術的対策：ウィルス対策

- 通信路
  - ウィルス付メールの遮断
  - 不正なWebサイトへ誘導するメール遮断
  - 不正な活動の検知と遮断
- クライアント
  - ファイルのフィルタリング
  - 不正な活動の検知と遮断

# 技術的対策：重要情報の送受信を暗号化

- Webでの重要情報送受信




- 無線通信の暗号化

# 技術的対策：本人確認

- ユーザ名とパスワードによる認証
- 認証の3要素
  - 記憶：パスワード、秘密の言葉
  - 持ち物：ICカード、スマートフォン
  - 本人そのもの：指紋、虹彩、静脈
- 多要素認証
  - 複数の要素の組合せ
- 証跡管理

# 技術的対策：証明書

- サーバ証明書
  - 通信先が真正であること
  - SSL証明書
- クライアント証明書
  - クライアントが予め登録されていること

# 技術的対策：デバイス認証

- 組織内部にあるデバイスであっても、信用しない
- デバイスを認証
  - MACアドレス、個人認証
- デバイスの挙動のモニタリング
  - おかしい動きをしたら切断

# 非技術的対策

- 教育・研修
  - 情報セキュリティの重要性
  - 対策の必要性
- 訓練
  - インシデント発生時の対応
- 体制整備

# 個人としての安全対策：Webの利用

- 重要情報をできるだけ送らない
  - 正しいサイトであることの確認：証明書
  - 暗号化
  - 本当に必要なのか
- 不正サイトからの攻撃を防ぐ
  - 不要なサイトへアクセスしない
  - 見ただけでウィルスダウンロードの危険性

# 個人としての安全対策：ウィルス・フィッシング対策

- ウィルス対策ソフトの導入
  - ウィルスパターンの更新
  - 定期的な全体スキャン
- 危険なメール
  - 知らない人からの「緊急」「重要」メール
  - 送信元のアドレスがおかしい
  - リンク先のアドレスがおかしい

# 個人としての安全対策：パスワードの管理

- 重要なサービスのパスワードを他のサービスと共有しない
  - 大学のメールアドレスとパスワードの組を外部サービスで使わない
- 他人に教えない
- 危ないと思ったら変更する

# 個人としての安全対策：データを失わない

- バックアップをする
  - CDやBD
  - USB接続のポータブルHD
  - クラウドストレージ

# 何か変だと思ったら

- 総合情報基盤センターに相談する
- チュータに相談する
- 警察に相談する