情報セキュリティ

情報科学の世界 2
2022 年度前期
佐賀大学理工学部 只木進一

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
  - 民間企業の顧客情報の漏えい
  - 公的機関からの個人情報漏えい
  - 特定個人情報: マイナンバー
- 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
  - ID や PW を窃取される

- 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

情報セキュリティ 10 大脅威 (ICT threats) 2022

順位	個人	組織
1	フィッシングによる個人情報等の詐取	ランサムウェアによる被害
2	ネット上の誹謗・中傷・デマ	標的型攻撃による機密情報の窃取
3	メールや SMS 等を使った脅迫・詐欺の手口による金銭要求	サプライチェーンの弱点を悪用した攻撃
4	クレジットカード情報の不正利用	テレワーク等のニューノーマルな働き方を狙った攻撃
5	スマホ決済の不正利用	内部不正による情報漏えい

https://www.ipa.go.jp/security/vuln/10threats2022.html

質問

インターネットを使っていて、怖いなぁと思ったことはありますか。

個人情報漏洩事案

- 2021/10/3 新生銀行
  - 広告分析等のための委託先に、顧客情報 (カード情報等) 8000 件を流出
- 2020/12/11 駅レンタカーシステム
  - 不正アクセスを受け、25 万件以上のメールアドレス、電話番号を流出
- 2015/5/28 日本年金機構
  - 標的型攻撃
  - 150 万件以上の個人情報漏えい
- 2014/7/9 ベネッセ
  - 760 万件の顧客情報を漏洩
  - 子供と保護者の氏名、住所、生年月日など
  - システムを委託していた系列会社へ派遣されていた社員が持ち出し

個人情報漏洩事案: 佐賀県関係

- 2021/3/2 佐賀市
  - ホームページ上で個人情報を含む画像 1000 件あまりを誤って表示。1 年以上放置。
- 2017/6/20 佐賀銀行
  - 行員が窃盗。共犯者へ大口顧客情報 (169 人) を漏えい
- 2016 佐賀県教育委員会
  - 1 万人の生徒の住所、氏名、電話番号、成績など
  - 県内の少年、高校生が関与

個人情報

- 生存している個人を特定する情報
- 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
- 要するに、本人の属性に関する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
  - http://www.jla.or.jp/library/gudeline/tabid/232/Default.aspx
- 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

- 情報の機密を守る
- 権限のある者だけが、閲覧、変更、削除ができる

完全性：Integrity

- 情報が正しいこと
- 必要とするときに、正しい情報を取得できる

可用性：Availability

- 必要とするときに、情報・装置を利用できること

三つの要素への、対策のバランスが重要

- 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た対策か
- 情報システムの運用の観点
  - システムとして対策を実装できるか
- 費用と効用の評価
- 公開情報にもセキュリティがある

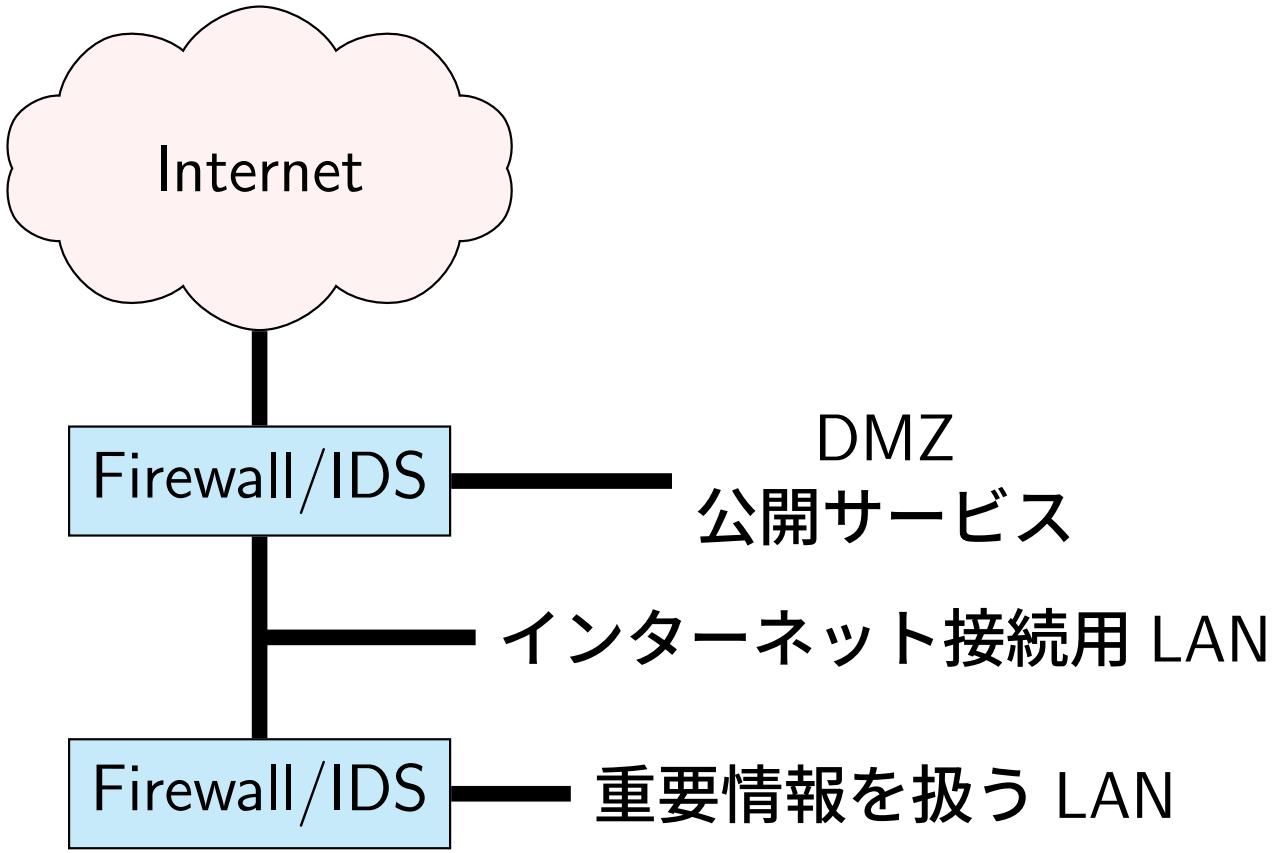
情報セキュリティの対策

- 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
  - DMZ (DeMilitarized Zone) の設置
- 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


Internet
Firewall/IDS
DMZ
公開サービス
インターネット接続用 LAN
Firewall/IDS
重要情報を扱う LAN

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
  - サンドバック: 不審なファイルの動作確認
- メールサービス
  - ウィルス付きメールの隔離と削除
- 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

- HTTPS の利用

- 無線通信の暗号化
- ssh (secure shell): リモートログインの暗号化

技術的対策: 本人確認

- ユーザ名とパスワードによる認証
  - 現状では非常に危険
- 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
  - ログインの記録

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
  - 組織の長がセキュリティ対策の責任者である
  - CSIRT (Computer Security Incident Response Team)

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
  - 閲覧し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
  - 親族にも教えない
- 危ないと感じたら変更する

個人としての安全対策: データを失わない

- データを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の活用

何か変だと思ったら: 相談する

- 総合情報基盤センター
- 学生生活課
- チュータ
- 警察

自分の PC にインストールしているウィルス対策ソフトのログを確認しなさい。