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
2024 年度後期
佐賀大学理工学部　只木進一

1. 序論: Introduction
2. 個人情報とプライバシー: personal information and privacies
3. 情報セキュリティの構成要素: Elements of information security
4. 情報セキュリティの対策: Information security measures
5. 個人としての安全対策: Personal security measures

セキュリティインシデントは他人事ではない

- 通信など情報基盤が停止する
  - スマートフォンが使えない
  - キャッシュレス決済ができない
- クラウドサービスが止まる
  - オンライン授業に参加できない

- 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
  - フィッシングメールの増加
- 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
- Teams の停止
- 携帯キャリア障害

ランサムウェア: Ransomware

- 感染すると、PC 内のファイルに暗号がかかる
- 金銭を要求、特に電子通貨を要求
- 払っても、解除されるか不明
- 企業への大規模攻撃の事例: 事業継続への脅威
- 病院システムへの攻撃事例: 診療継続への脅威

https://www3.nhk.or.jp/kansai-news/20221107/2000068014.html
https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html
https://www.asahi.com/articles/ASP592PNYP58ULFA008.html

情報セキュリティ 10 大脅威 (ICT threats)2023

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	サプライチェーンの弱点を悪用した攻撃
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	標的型攻撃による機密情報の窃取
4	クレジットカード情報の不正利用	内部不正による情報漏えい
5	スマホ決済の不正利用	テレワーク等のニューノーマルな働き方を狙った攻撃

https://www.ipa.go.jp/security/10threats/10threats2023.html

個人情報漏洩事案

- 2023/10/17 NTT 西日本子会社
  - 派遣社員が媒体を使って個人情報を持ち出し。すでに名簿屋等に流出か？
- 2022/8/18 徳島大学
  - 改修時の設定ミスにより 7000 人以上の学生情報漏えい
- 2020/11/10 慶應義塾大学
  - 不正アクセスで 3 万件以上の学生情報漏えい
- 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

- 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

個人情報保護に関する法律

- 「個人情報」とは、生存する個人に関する情報
- 個人識別符号が含まれるもの
  - 個人の身体の特徴をデジタル化したもの
  - サービスや商品と関連して割り当てられるカード番号など
- 「要配慮個人情報」
  - 本人の人種、信条、社会的身分、病歴、犯罪の経歴、など

https://elaws.e-gov.go.jp/document?lawid=415AC0000000057

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
- 「要配慮個人情報」と重複

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

情報セキュリティの概念: 4 つの新要素

真正性: Authenticity
なりすましや虚偽の情報でないことが保証されている。
責任追跡性: Accountability
アクセス記録等から、ユーザやシステムの振る舞いや責任を説明できる。
信頼性: Reliability
システムが矛盾なく正常に動作する。
否認防止: Non-Repudiation
事後になってから事実を否定できないように証拠が残っている。

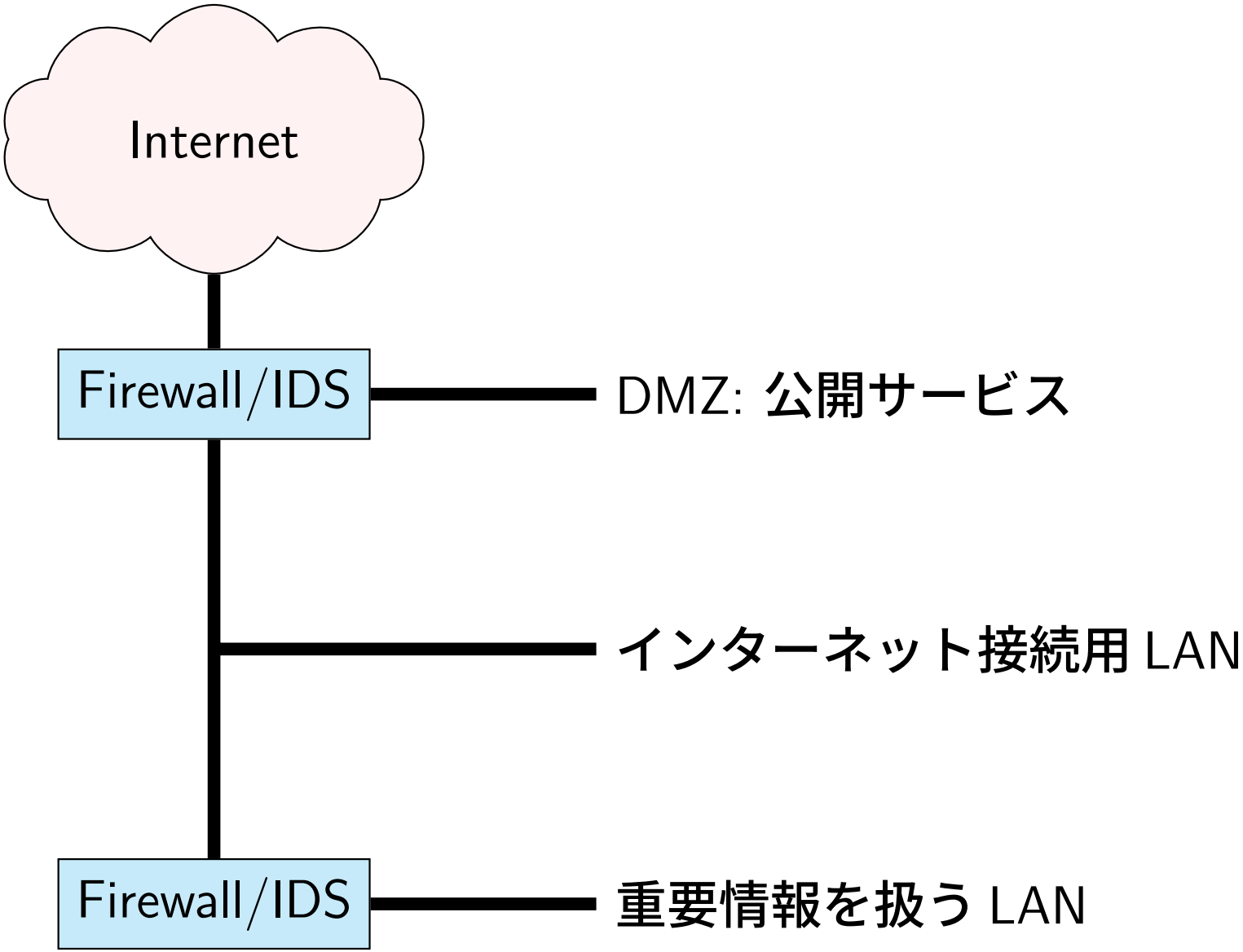
情報セキュリティの対策

- 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
- 証明書の提示
  - 真正なサイト、無線サービスであることの証明

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
  - 複数の認証要素の組合せ
- 証跡管理
  - 認証の記録を残し、点検する

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
  - 自己の行動の振り返り
- 訓練
  - 疑似攻撃への対応
  - インシデント発生時の対応
- 体制整備
  - 責任
  - 連絡
  - 事後処理

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
  - 本当に必要なのかを考える
- 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
  - 親族にも教えない
  - 教えた場合、「不正利用」とならない可能性
- 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

課題

IPA「情報セキュリティ 10 大脅威 2023」のページを読みなさい。
https:
//www.ipa.go.jp/security/10threats/10threats2023.html