情報セキュリティの概念と理念

情報社会とセキュリティ
2024 年度前期
佐賀大学理工学部 只木進一

Secureの意味

- feeling happy and confident
- likely to continue or be successful for a long time
- guarded and/or made stronger
- 安全や安心に関する広い意味
- 警備なども含む

情報セキュリティの概念

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

integrity:the state of being whole and not divided.

- 情報セキュリティは、「秘密」だけに関わるものではない
  - データやシステムへの信頼を含む
  - 公開情報であっても、セキュリティの観点が必要
- 紙の文書も含む
  - システムの設計図
  - 運用手順書
  - 連絡体制

情報セキュリティの概念: 例

機密性: Confidentiality
個人情報やプライバシー、国家機密など 秘密、取扱注意、その他 3 段階
完全性: Integrity
入試日程、DNS、認証情報など 2 段階
可用性: Availability
ネットワーク、DHCP、公式ホームページなど 2 段階

三つが連動している場合が多い

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 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/vuln/10threats2023.html

ランサムウェア被害

- 2022 年 10 月: 大阪府立病院機構・大阪急性期・総合医療センター
  - 給食の委託先から侵入の可能性
  - 電子カルテシステム停止
  - BCP が無かった
- 2021 年 10 月: 徳島県つるぎ町立半田病院
  - VPN 装置経由の可能性
  - VPN 装置の脆弱性情報に未対応
  - 電子カルテシステム停止
- 閉域網への過信があったのではないか

個人情報漏洩事案

- 2024/3/1 北海道大学
  - 工学部 Web サーバに不正侵入、個人情報 2 万件以上を流出
- 2023/12/19 NTT ビジネスソリューションズ
  - 派遣職員が 900 万件以上の個人情報を持ち出し
- 2023/3/31 NTT ドコモ
  - 委託先 PC より 600 万件の個人情報流出

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

情報資産: 情報に関わる様々な資産

有形のもの

- コンピュータそのもの
- ネットワーク機器: SW、ルータ、FW
- データを保管している媒体: ディスク、テープ
- 紙となった資料や図面

無形のもの

- ソフトウェア
- データ
- ノウハウ

質問

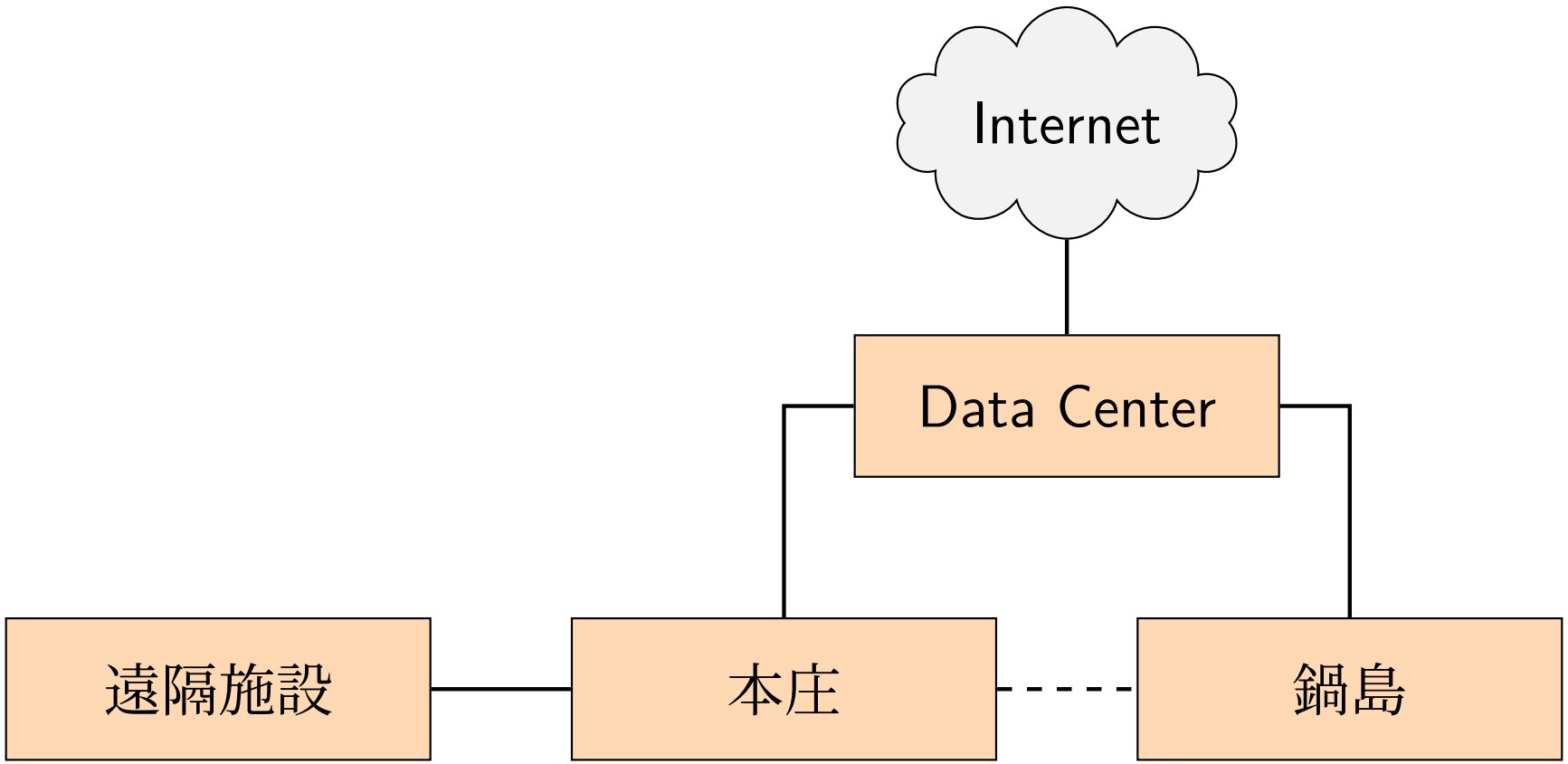
紙になった資料や図面の漏えいや紛失は、どのようなダメージをもたらすでしょうか。明示的でないノウハウの漏えいや喪失は、どのようなダメージをもたらすでしょうか。

情報に関わるリスクとインシデント

リスク (risk): 情報資産を失う (漏らす) 可能性 × 失ったときの損失

- 重要なデータは、破損 (漏洩) 時のリスクが大きい
  - ファイルサーバ等を使って破損リスクを低減
    - RAID (Redundant Arrays of Inexpensive Disks)
  - 暗号化によって漏洩時のリスクを低減
- 使用しなくなった古いデータの漏えいリスク
  - 外部媒体に保存し、定期的に破棄
  - 廃棄時にはデータ消去や媒体の物理的破壊
- 対外接続回線は、停止すると大きな機会損失
  - 冗長構成としてリスク低減

佐賀大学の対外回線冗長化: 可用性向上例



SINET (Science Information Network) の冗長化

https://www.sinet.ad.jp/static/844d19d7b1eec0e67be088757b6c79e0/SINET6-2022_j.pdf

- メッシュ状にすることで、冗長化

情報に関わるリスクとインシデント

- インシデント (incident): 情報資産を棄損した状態、機密情報が漏洩した状態
  - 機密性の高い情報が漏えいした
  - 完全性の高い情報が改ざんされた
  - 可用性の高いサービスが停止した
- リスクとコスト、そして利便性のバランスが必要
  - 機密性の高い情報はオフライン ⇒ 紙で扱う?
  - 完全性の高い情報は書き換え不能の媒体で提供 ⇒ 更新時は?
  - 可用性の高いサービスは多重に ⇒ 幾つ用意すれば十分?

質問

成績証明書は、プライバシーレベルの非常に高いものです。適切な本人確認の下でしか、提供することはできません。
卒業後に成績証明書が必要になった時に、どうやって発行するのが良いでしょうか。

外部のリスク要因

- マルウェア (malware)
  - ウィルス、スパイウェア、ボットなど悪意あるプログラムの総称
  - 数は 2005 年ころにピーク
  - 悪質化
- 不正アクセス
  - 攻撃用ツールの流通
  - 侵入後の不正行為: 盗聴、改ざん、破壊、マルウェア埋め込み、踏み台
- サービス妨害
  - DDoS (Distributed Denial of Service): ボットなどを使って多地点から攻撃
  - メール攻撃

内部のリスク要因

- 情報システムの技術的脆弱性
  - OS、DB、Web クライアント、Web サーバなど
  - 脆弱性を突いた攻撃
  - 古い OS やアプリケーション
  - 設定不備
- 組織の脆弱性
  - 情報資産の持ち出しによる、紛失・盗難
  - 誤公開、誤送信
  - 内部犯行
  - 運用体制不備
  - 保守契約なし

情報セキュリティの検討と守るべき価値

- 例えば、自由、安全、プライバシーの観点から
  - 情報技術によって、新しい可能性を通じた自由の拡大
  - 情報技術の悪用によって、安全が脅かされる
  - 情報システムを通じて、プライバシーの侵害・漏えいが発生する
- 技術、法制度、市場、モラルの観点から妥協点を探る必要
  - Google Street View は便利だが、自分の家の周りの様子が解り不安
  - 安全確保のための通信監視は、プライバシー侵害にならないか
  - プライバシー保護を強調しすぎると、データ活用が進まない

- 個人情報の保護と利用
  - マイナンバーによる納税者情報の一元管理による行政の効率化
  - 行政に情報を把握されることへの不安
  - 提供した個人情報を活用した、個人に対応したサービス
- 企業内における従業員のやる気と監視
  - 従業員が使用する PC からの情報漏えい
  - 従業員が使用する PC の不適切な利用（勤務時間中に株取引をするなど）
  - 監視や制限をきつくすると、士気が下がる

立場や技術力に応じた多様な視点

- 個人としての一般ユーザ
- 組織に属する者としての一般ユーザ
- 組織等の技術的管理者
- 組織等の非技術的管理者
- 経営者や組織の長
- 研究者や技術者

一般ユーザの視点

- 自らが加害者とならないための対策
  - OS やウィルス対策ソフトのアップデート
  - 危険なメールへの対応
  - 危険なサイトへの対応
  - SNS との適切な付き合い方
- 組織の一員としての対策
  - 組織の情報セキュリティ方針に従う
  - 内部情報の管理
    - オンラインに、その情報を書き込んで大丈夫か
    - SNS、chatGPT、メール
  - 公私の区別

管理者

- 技術的管理者
  - 担当システムのモニタリング
  - 技術情報の収集と報告
  - 技術的対応
  - インシデント対応
- 非技術的管理者
  - 情報セキュリティの重要性の理解
  - 部下への指導
  - インシデント対応

経営者や組織の長

- 情報セキュリティの重要性の理解
- 情報セキュリティ対策への投資
- 情報セキュリティ要員の確保
- 情報セキュリティ対策のための体制整備

研究者や技術者

- 関連法の理解
- 倫理への配慮
- 技術の影響への配慮

課題

皆さんが所有しているPCのディスクの中には、様々な情報があります。その情報に発生するリスクは何でしょう。漏えいだけでなく、喪失のリスクも考えましょう。
そのリスクを軽減するための対策は何でしょう。