資料２

ADRのオンライン化とセキュリティ

湯淺墾道

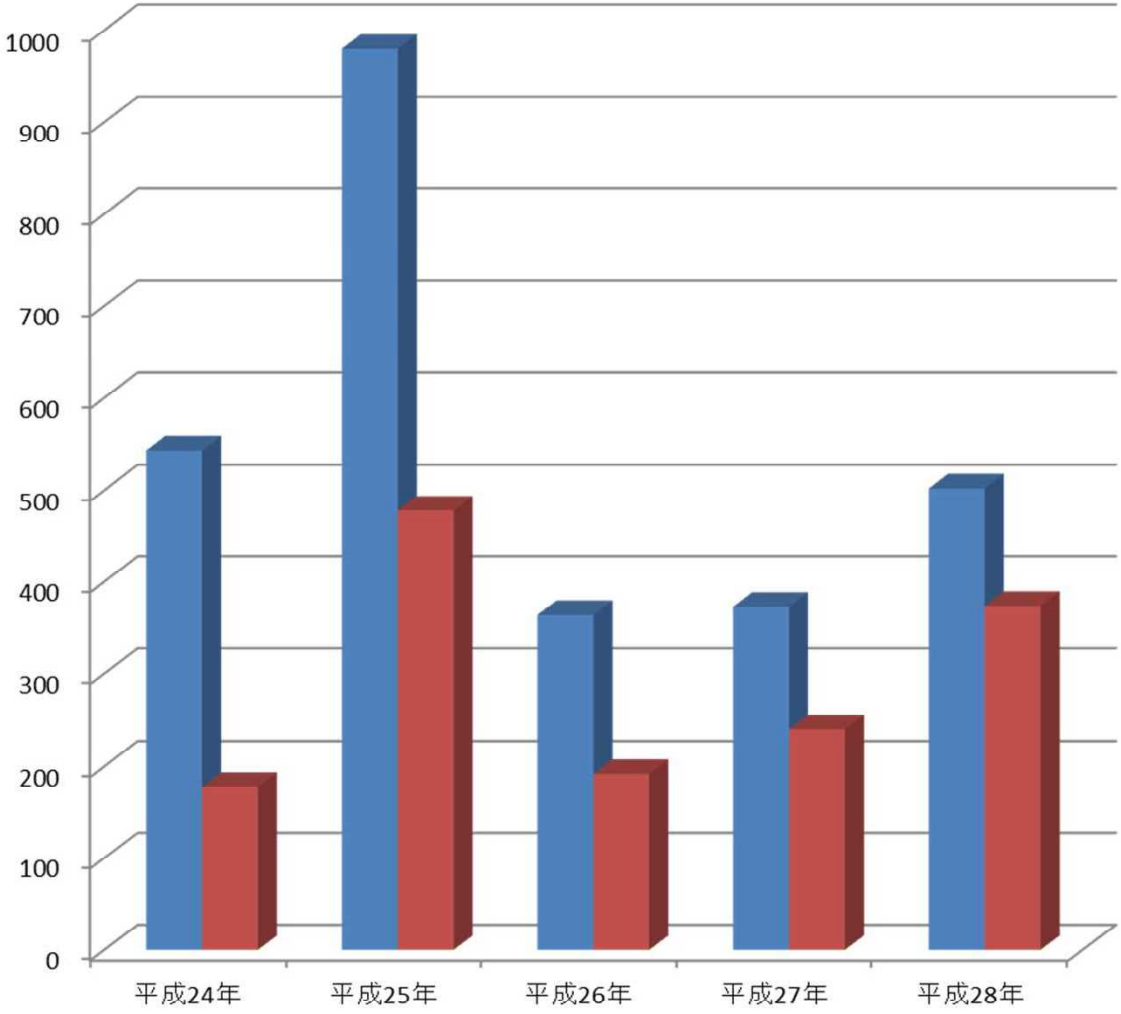
明治大学公共政策大学院ガバナンス研究科

自己紹介

- 1970年生まれ
- 青山学院大学法学部公法学科卒業、同大学院法学研究科公法専攻博士前期課程修了、慶應義塾大学大学院法学研究科政治学専攻博士課程退学
- 慶應義塾大学講師等をへて、2004年九州国際大学法学部専任講師、2005年助教授、2007年准教授、2008年教授、副学長・国際センター長、2011年情報セキュリティ大学院大学情報セキュリティ研究科教授、2012年学長補佐、2020年副学長、2021年明治大学公共政策大学院ガバナンス研究科教授
- 法務省法制審議会民事訴訟法（IT化関係）部会委員、総務省AIネットワーク化推進会議開発原則分科会構成員、総務省情報通信政策研究所特別研究員、総務省投票環境の向上等に関する研究会構成員、経済産業省産業サイバーセキュリティ研究会WG2委員　ほか
- 日本学生支援機構CIO補佐官、神奈川県情報公開・個人情報保護審議会副会長、川崎市情報公開運営審議会会長、渋谷区個人情報の保護及び情報公開審議会副会長、一般財団法人日本データ通信協会諮問委員長、一般財団法人日本サイバー犯罪対策センター理事、ベネッセホールディングス情報セキュリティ監視委員会委員長代理　ほか

セキュリティの現状

サイバー犯罪の推移



■ 不正アクセス禁止法違反（件）

■ コンピュータ・電磁的記録対象犯罪、不正指令電磁的記録に関する罪（件）

※警察庁統計資料による

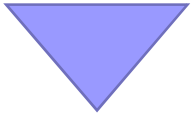
情報漏えいの被害

- 目に見える資産
  - 被害がすぐに発見されやすい
- 目に見えない資産
  - 顧客に関する情報
  - 特許、技術情報、ノウ･ハウ
  - 財務に関する情報
  - 人事に関する情報
  - 戦略や新製品･サービス等の情報

個人情報漏えい

年間の漏えい人数	496万0063人
年間のインシデント件数	799件
一件あたりの漏えい人数	6578人

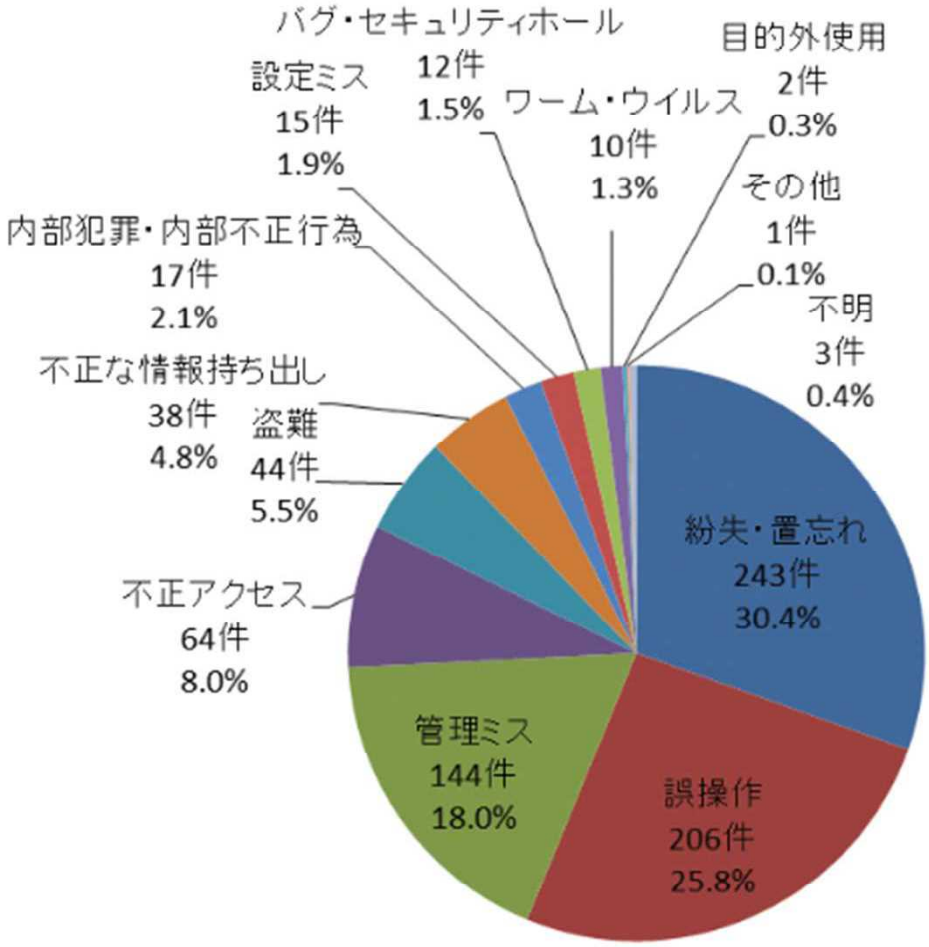
- 報道や企業のウェブページ等で公開されている情報のみ



- 実数はもっと多いと想像される
  - 日本ネットワークセキュリティ協会「2015年 情報セキュリティインシデントに関する調査報告書【速報版】」（2016年）

漏えいの原因

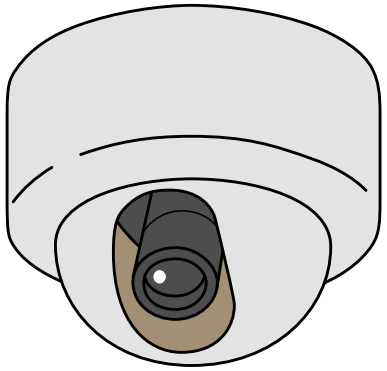
不正アクセス、盗難、不正な情報持ち出し、内部犯罪、ウィルスによるものが1/4



- 日本ネットワークセキュリティ協会「2015年 情報セキュリティインシデントに関する調査報告書【速報版】」(2016年)

どこから漏れる?

- 不正侵入、マルウェア感染
- 利用権者のパスワード設定・管理の甘さ
  - 使い回し、初期設定のまま
  - administrator　password等の安易なもの
- その他


多様なサイバー攻撃

- 膨大な量のメールを送付、大容量の添付ファイルをつけたメールを送付
- クラッキング（ウェブサイトに侵入、データを改竄する）
- フィッシング（ユーザーを偽のWebサイトへ誘導して、IDやパスワードを窃取する）
- ガンブラー攻撃（悪意あるプログラム＝マルウェアをダウンロードさせる）
- ゼロデイ攻撃（ソフトウェアにセキュリティ上の脆弱性が発見されたとき、問題の存在が公表される前にその脆弱性を突いて攻撃する）

- トロイの木馬（バックドアを設置する）
- ボット（他のユーザーのPCを遠隔操作可能にする）
- ボットネット（ボットを多数設置してネットワーク化）
- DDos（特定のWebサイトに一斉にアクセスすることで機能不能にする）
- 標的型電子メール
- APT (Advanced Persistent Thread)
- SNSを標的にした攻撃

中小事業者がサイバー攻撃を受けやすい理由

- セキュリティ対策が不十分でセキュリティの専門家がいない
- 委託先に任せっぱなしになっている
- 情報システム担当者がいない、担当者以外はよくわからない
- サイバー攻撃を受けたことに気づかない
- 1台のパソコンを共用している、多目的に使っている
- 保有している情報資産の価値、サプライチェーンにおける位置に気づかない

オンライン化とセキュリティ

セキュリティのCIA

- 1992年　OECD情報セキュリティガイドライン
  - Confidentiality（機密性）
  - Integrity（完全性）
  - Availability（可用性）
- 日本産業規格（旧・日本工業規格）JIS Q 27002
  - 「情報の機密性、完全性および可用性を維持すること」、「さらに、真正性、責任追跡性、否認防止および信頼性のような特性を維持することを含めてもよい。」

- Confidentiality（機密性）
  - JIS Q 27002「情報へのアクセスを認められた者だけが、その情報にアクセスできる状態を確保すること」
- Integrity（完全性）
  - 情報および処理方法が正確かつ完全であることの保護 。
  - 情報の不正な改竄がないこと、情報処理結果の誤りがないこと、情報に欠損がないこと

- Availability（可用性）
  - JIS Q 27002「情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること」

手続の電子化の考え方

検討項目	検討内容
法令の要求	要求される手続内容の明確化。
実現手段	法令等の要求を遵守しつつ、電子的に代替する手段の技術的検討。
関係者の確定	当該手続に関わる関係者の確定と、それに基づくアクセス権限の設定。
リスク・脅威	当該手続に関わるリスクや脅威の分析。サイバー攻撃、システムの脆弱性、内部要因（人的要因）等を総合的に分析。 業務委託先（利用サービス）における障害等のリスクの想定。
セキュリティ対応策	リスクや脅威への対応策の事前策定。 多様なセキュリティ対策技術、各種サービスの中から適切な対策の選定。
被害発生時の対応	被害拡大の防止。 文書が滅失した、秘密とすべき情報が漏えいした等の被害が実際に発生した場合の対応手続の明確化。

検討すべき点

- 利便性と秘密保持等を衡量した適切なセキュリティ水準の設定
  - 従来の手続における水準との比較
- 個人情報保護の取扱いとプライバシー保護
- 本人確認とアクセス制限
- 民間事業者の提供するシステムを利用する場合
  - 約款、バックアップ、SLA、当該事業者が当事者となる場合の措置、ベンダロック

- 例：本人確認
  - 従来の手続（対面確認）
    - 何を、何によって、どうやって確認していたのか？
    - 対面ではどの程度の厳格性が求められていたのか
  - オンライン化
    - 対面確認では行われていた「何を、何によって、どうやって」のうち、オンラインでは行えないものは何か？
    - 対面時にはなかった新たな要素は何か？
    - 対面＞オンライン　対面＝オンライン　対面＜オンライン　をどう考えるべきか

当事者（個人）レベルでのセキュリティの留意点

- 紛失、盗難
- OS等を最新版にアップデートする
- アプリの出所に注意する
- 遠隔ミーティングツール
  - チャットに表示されるURL
  - 背景
- パスワードの管理
  - パスワードの使い回しの危険性


15:46
今忙しい？
大丈夫です
近くのコンビニで
BitCash カードを何枚か
買ってきて欲しいんだ
けどいいかな？

いくらぐらいですか？

5万円分のを1枚買ってきて欲しい

買ってきたらどこに郵送すればいいですか

お金は明日あげるよ。

買ったら裏面のひらがなIDを削って写真でfacebookを送ってくれ

写真でFacebook？

はい。

民間サービス利用時の留意点

- 2021年4月
- 「政府機関・地方公共団体等における業務でのLINE 利用状況調査を踏まえた今後のLINE サービス等の利用の際の考え方（ガイドライン）」
  - 公的業務、公共性を有する業務における民間サービス利用時に参考になる点が多い
  - ADR事業者の従事者や関係者への注意喚起に参考になる点が多い

なお、要機密情報を含む業務連絡等でメッセージアプリを利用する場合は、ISMAP に基づきセキュリティ対策が確認されたメッセージサービスを、各行政主体のセキュリティポリシーに合致することを確認しつつ契約し、利用することが推奨される。

- ISMAPとは
  - 政府情報システムのためのセキュリティ評価制度（Information system Security Management and Assessment Program: ISMAP）
  - 政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準を確保