情報セキュリティ

情報科学の世界II

2017年度

只木　進一（工学系研究科）

セキュリティは他人事ではない

- 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

セキュリティは他人事ではない

- 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

個人情報漏洩事案

- 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
- 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

- 2014/4/18 東京医科大学
  - 脳神経外科手術　33例
  - 氏名、性別、生年月日、検査データ
  - 職員がUSBで持ち出し、紛失

- 2011/4/21 ソニー
  - Play Station Networkの顧客情報7700万件流出
  - 住所、ログインID、パスワード、購入履歴など
  - サーバーの脆弱性を突かれ、不正アクセスを受ける

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
  - 例えば
    - どういう食べ物や服装の好みがあるか
    - 病歴、服薬履歴

情報セキュリティの構成要素

- 機密性：confidentiality
  - 秘密であること
  - 制限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
- 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

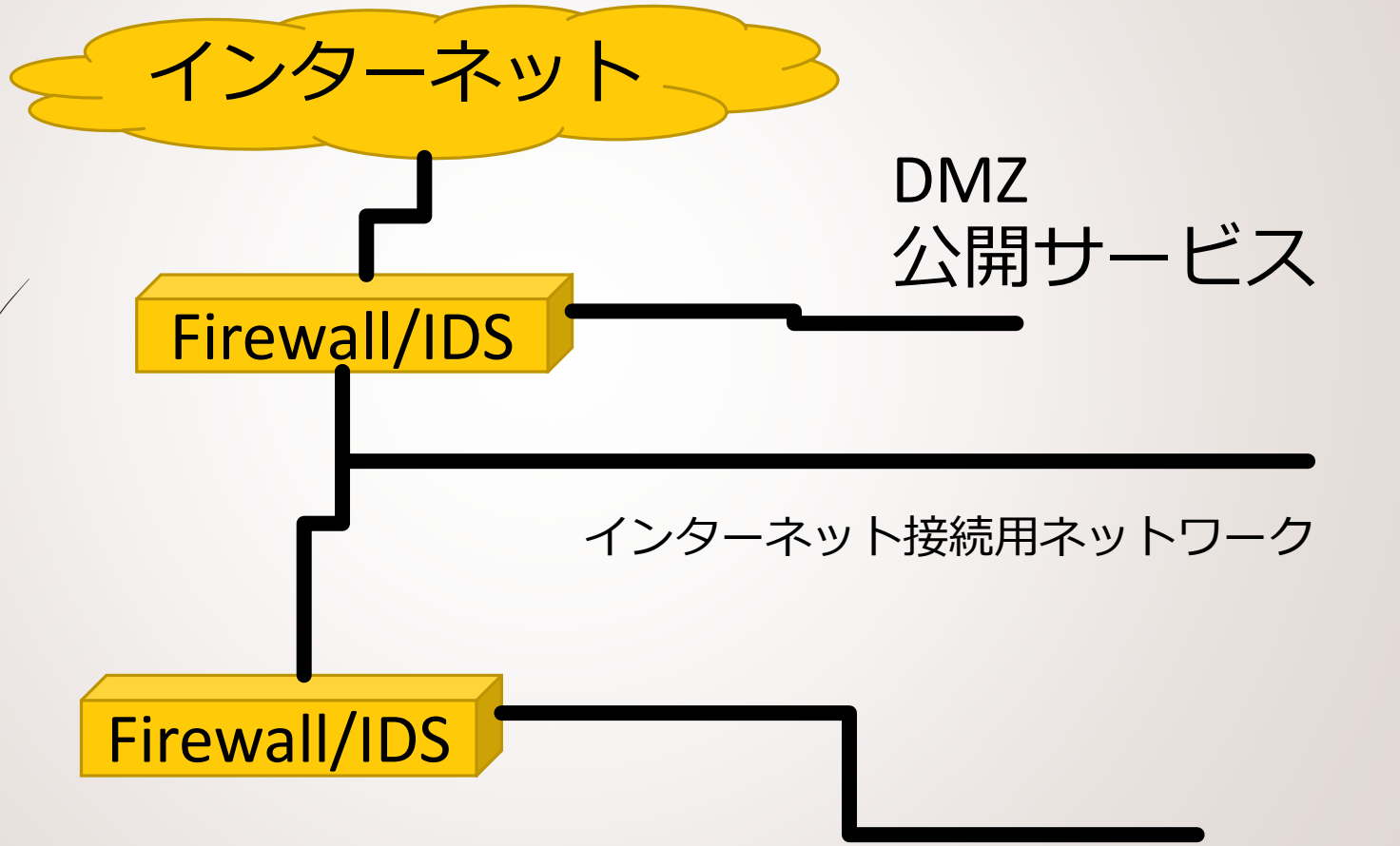
- 問題が発生しないための対策
  - 不正通信が起こらないように
  - ウィルスが入り込まないように
  - 不正侵入が起こらないように
- 問題の発生を想定した対策
  - 不正通信の確認と遮断の方法
  - 重要情報の暗号化
  - 重要情報の分散

- 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

- 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
- ウィルス対策：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

- 本人確認：不正利用防止
  - ユーザー名とパスワードによる認証
  - 多要素認証
    - 持っているもの：ICカードなど
    - 持っているものに一時的なパスワードを送信
  - 生体認証
    - 指紋、虹彩、静脈
  - 証跡管理

暗号化

- 情報を暗号化する
  - 暗号化には、その方法とともに鍵が必要
- 例：Caesarの暗号
  - アルファベットの先頭から鍵の文字列に置き換える
  - 残りは、鍵の終端の後ろに残ったアルファベットを順番に対応させる

- 鍵：JULISCAER
- a b c d e f g h I j k l m n o p q r s t u v w x y z
- J u l I s c a e r t v w x y z b d f g h k m n o p q

- 符号化：Encode, Encipher
  - 元のテキストを暗号テキスト(cipher text)にする
- 復号化：Decode, Decipher
  - 暗号テキストを元のテキストに戻す

- 鍵を送信者と受信者が共有する方法
  - 共通鍵方式
    - 符号化と復号化で同じ鍵
    - どうやって鍵を送る？
- 送信用鍵と受信用鍵が異なる
  - 公開鍵方式
    - 符号化と復号化が異なる鍵

公開鍵暗号方式

- 受信者から送信者へ、符号化用鍵の送信
- 送信者は送信内容を符号化用鍵で暗号化し、送信
- 受信者は、自分だけが持つ復号化用鍵で暗号テキストを復号

SSL (Secure Socket Layer)

- Web 通信で用いる暗号化方式
- Webの信頼性を示す証明書
- 重要情報を送る場合には、確認必須

- クライアントがサーバへ通信要求
- サーバが証明書と公開鍵を送信
- クライアントは、共通鍵を生成して
  サーバから受信した鍵で符号化して送信
- サーバは共通鍵を受信して復号
- 双方が共有した鍵で、暗号通信

復号できない暗号

- パスワード
  - 符号化できるが、復号できない
  - 攻撃手法
    - ユーザ名、名前、生年月日などをヒントに
    - 総当たり

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

個人としての安全対策：ウィルス対策

- 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：ID管理

- 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
  - 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