サイバーセキュリティの課題と展望

菊池　浩明
明治大学

本日の内容

- インターネット上の脅威
- セキュリティの基本要素
- セキュリティ対策

インターネット上の脅威

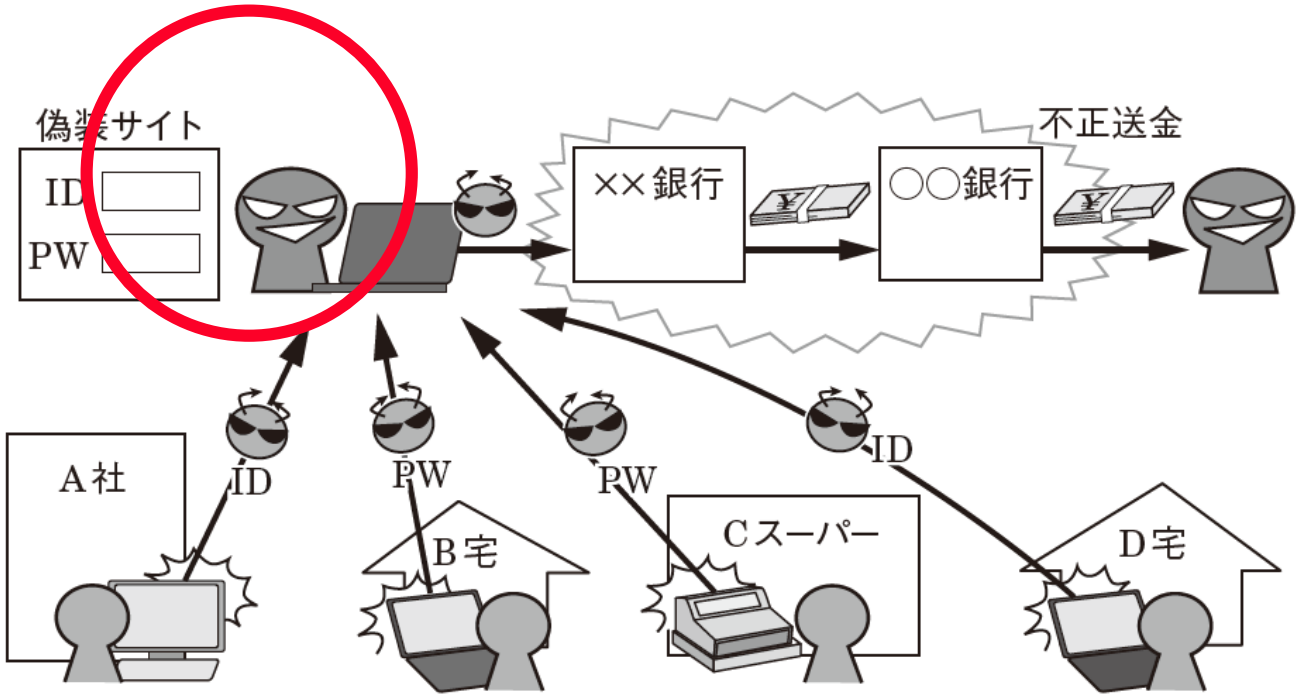
サイバーセキュリティの今

IPA「情報セキュリティ10大脅威」

2016年度版

1位	
2位	標的型攻撃による被害
3位	ランサムウェアを使った詐欺・恐喝
4位	ウェブサービスからの個人情報の窃取
5位	ウェブサービスへの不正ログイン
6位	ウェブサイトの改ざん
7位	審査をすり抜け公式マーケットに紛れ込んだスマートフォンアプリ
8位	内部不正による情報漏えいとそれに伴う業務停止
9位	巧妙・悪質化するワンクリック請求
10位	脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加

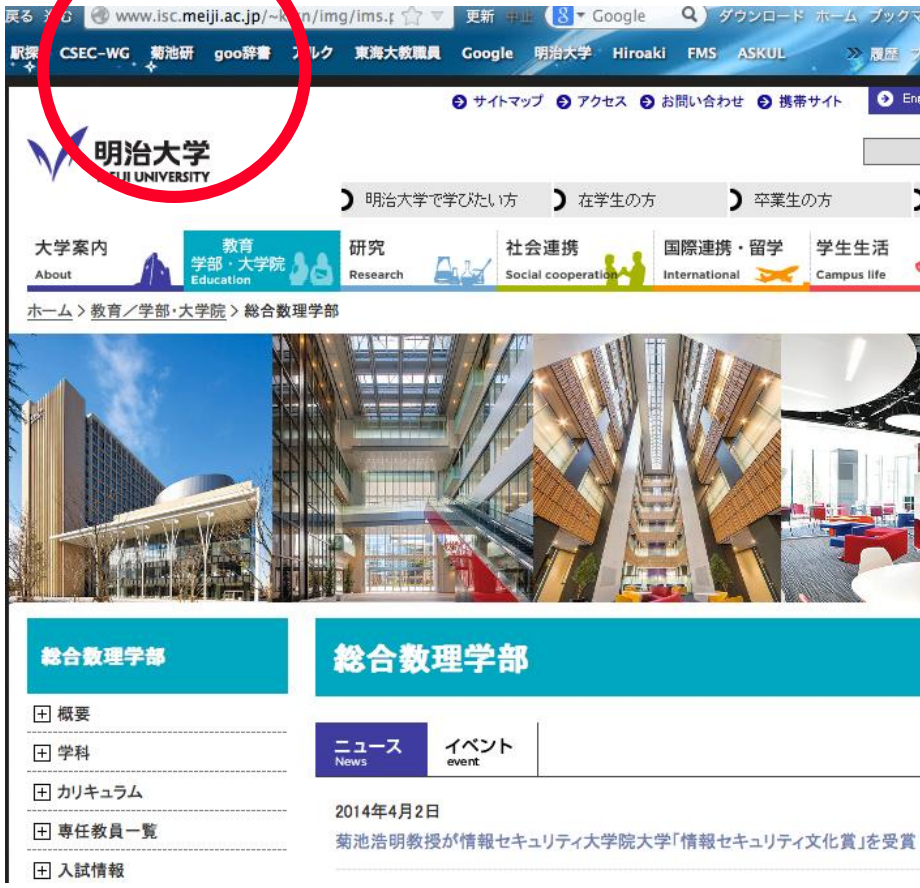
1位 インターネットバンキングやクレジットカード情報の不正利用



どちらが本物でしょう？

www.meiji.ac.jp/ims

www.isc.meiji.ac.jp/~kikn/ims.png

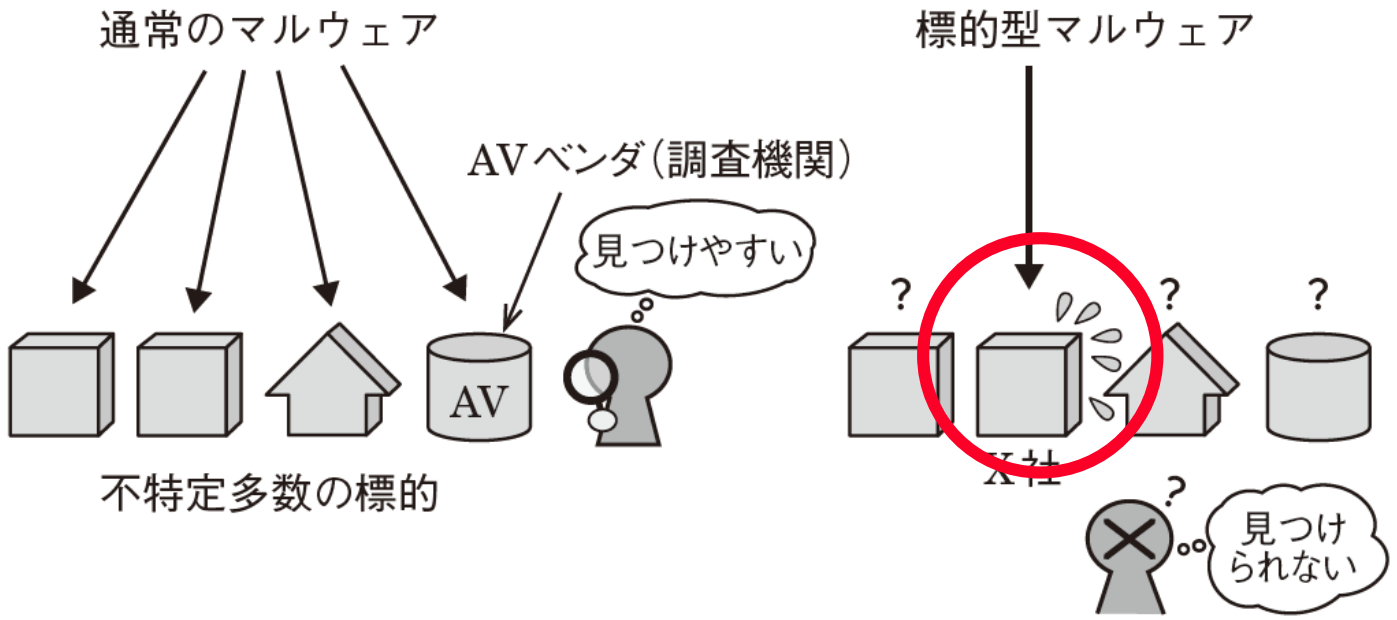


2位 標的型攻撃による情報流出

- 2015年6月2日
  - 日本年金機構から，氏名，基礎年金番号など125万件が流出
  - 5月8日に電子メールの添付ファイルで感染（遮断せず業務継続)
  - 5月19日警視庁相談
  - 5月28日NISCが外部と不正な通信を検出.

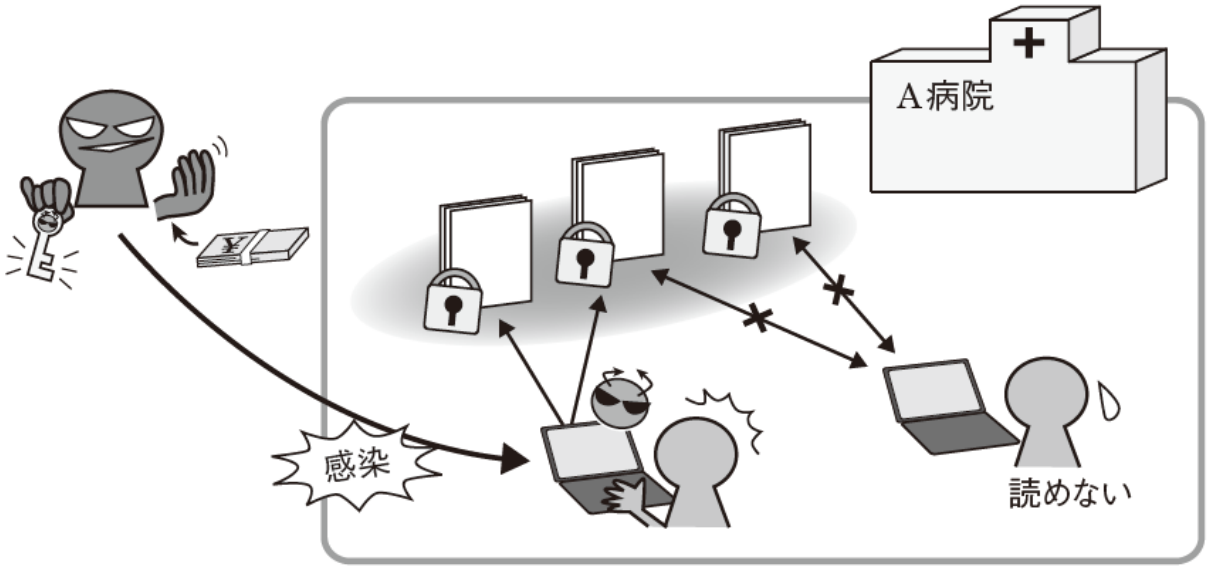
標的型攻撃 (targeted attack)

- Malicious (悪意のある)+ware (ソフトウェア)



3位 ランサムウェア

- Ransom (身代金）＋ware（ソフトウェア）



制御システムを狙うマルウェア

- Stuxnet (2010)
  - イランの核燃料再処理プラントPLC
- Havex (2014)
- BlackEnergy (2015)
  - 変電所管理SCADAソフトの脆弱性
    - » 監視を停止，ファイル消去，コールセンターに禍荷電
  - 2015年12月，ウクライナ西部を6時間に渡り大規模停電，40万人が影響

サイバー攻撃の傾向

- 現実世界とサイバー空間の距離が近づいた
  - 電子送金が普及し，経済的に大きな影響を与える
  - 車や発電所などが狙われ，現実の戦争の道具とみなされる
- 完全に安全な技術はない
  - 標的を絞って専用のマルウェア
  - 不特定多数と通信しなければならない業務
- 新しい技術に新しい脆弱性
  - スマートフォン，IoT機器
  - 仮想通貨ビットコインの悪用

情報セキュリティの基本要素

セキュリティの様相

情報セキュリティとは？

- セキュリティ＝安全？　安心？
  - 安全：　システムなどで物理的に確保すること
  - 安心：　心の安らぎ
- セキュリティ security
  - 幅広い脅威に対応し，事故発生時に損害を最小化するために行う組織的，社会的な防衛
  - 情報セキュリティ・物理的セキュリティ・国家セキュリティ

情報セキュリティの3要素

C I A

- CIA (Central Information Agency) 米国中央情報局

秘匿性 (Confidentiality)

- 情報を不適切な対象に見せないこと
  - 「機密性」とも言う
- 例）
  - ネットワークの盗聴
  - 不正コピー
  - 個人情報漏えい（氏名，年金番号，マイナンバー）

完全性 (Integrity)

- 情報が完全な形で保たれ，改ざん・破壊されない
- 例）
  - データの改ざん
  - フィッシングサイト（本物サイトの偽装）
  - メールの偽造（送信者の偽り）

可用性 (Availability)

- 情報や資源がいつでも利用できること
- 例）
  - システムの破壊，ファイルの暗号化 (ランサムウェア）
  - サービス利用不能攻撃 Denial-of-Service (DoS)

情報セキュリティの要素 まとめ

	要素	説明	例
C	秘匿性 (Confidentiality)	情報を不適切な対象に見せない	・ネットワークの盗聴 ・不正コピー
I	完全性 (Integrity)	情報が完全な形で保たれ，改ざんや破壊されない	・データの改ざん ・偽造
A	可用性 (Availability)	情報や資源がいつでも利用できる	・サービス利用不能攻撃(DoS) ・破壊

演習問題 1.2

- 次の例は，CIAの脅威のどれに該当するか？
  - 正規の従業員が，顧客情報を持ち出して名簿業者に売却してしまった.
  - マルウェアに感染したホストを何百台も操り，特定のウェブサイトをダウンさせた
  - コップに残留した指紋を取得して指を偽造し，他人になりすまして部屋の鍵を開錠した.

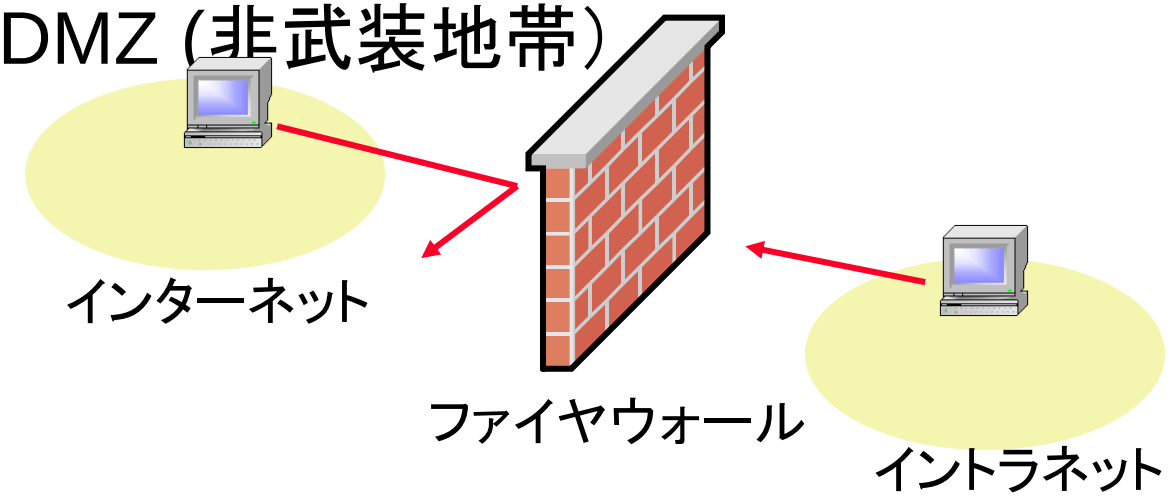
セキュリティ対策

セキュリティ技術

ファイアウォール　（防火壁）

C I A

- 機能
  - 1. パケットフィルタリング
  - 2. NAT (アドレス変換）
  - 3. DMZ (非武装地帯）



アンチウィルスソフト

C I A

- Anti Virus (AV)
- パターンデータベース
  = シグネチャー
  - サイズ小さく
  - 変種への適応
  - 誤認識低く

  - 更新し続ける必要性

暗号技術

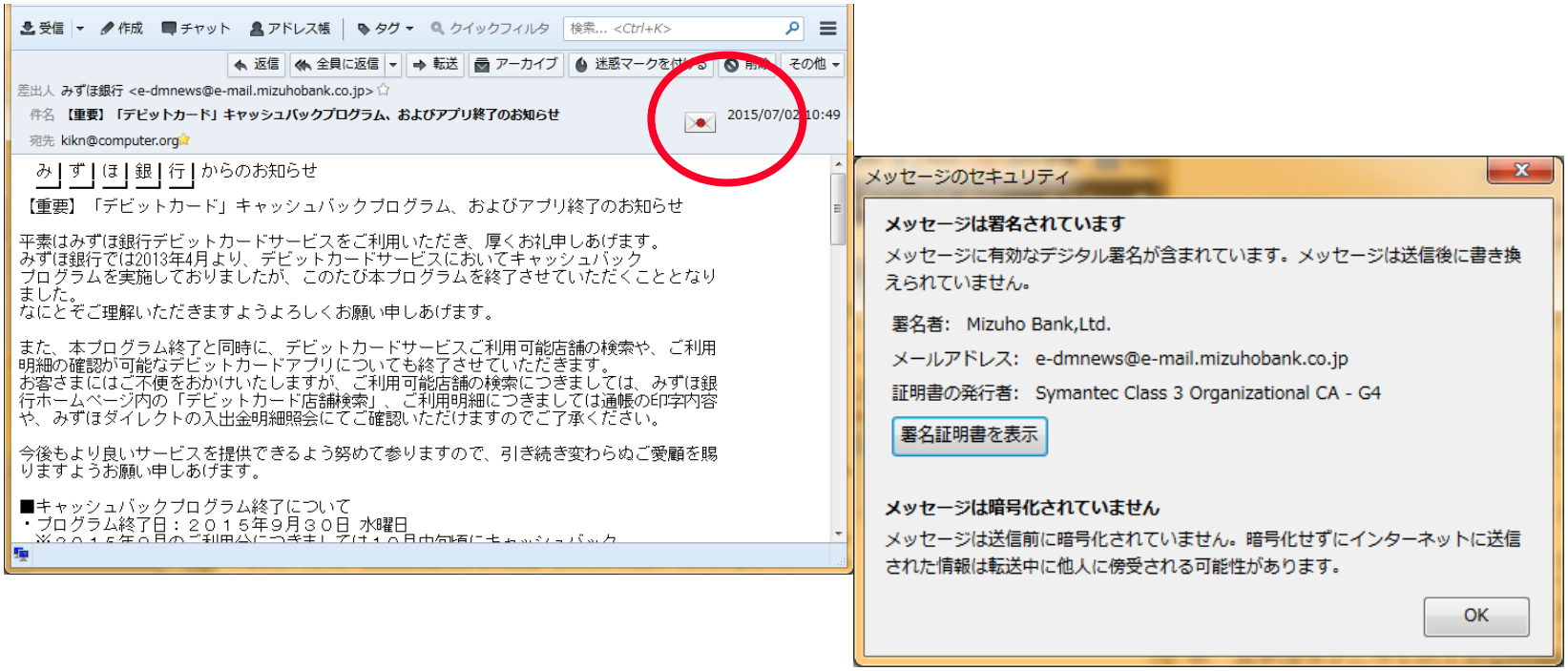
C I A

- ビジネル暗号 (Vigenere Cipher)
  - 16 century, Blasie de Vigenere

  - `thi sis adu mmy mes sag e`
  - `+ ABC ABC ABC ABC ABC ABC A`
  - `= TIK SJU AEW MNA MFU SBI E`

暗号化メール S/MIME

C I A



様々なセキュリティ技術

脅威	対策	要素技術	講義
不正アクセス	ファイアウォール，認証技術	経路制御技術，IDS	2 ファイアウォール，6 認証技術
マルウェア	アンチウィルス AV	シグネチャー，振舞検知	3 マルウェア
盗聴	暗号技術	共通鍵暗号，公開鍵暗号	4 共通鍵暗号
偽造	暗号技術	電子署名，ハッシュ関数	5 公開鍵暗号
フィッシング詐欺	暗号メール，PKI	S/MIME, SSL/TLS	8 PKI, 9. メール
違法コンテンツ	著作権保護	電子透かし，CPRM	11 コンテンツ保護
標的型攻撃	マネージメント	ISMS, CSIRT	マネージメント

演習問題 1.3

- 次の脅威に効果的なセキュリティ技術を（暗号化，ファイアウォール，アンチウィルス）の中から選べ．
  1. 顧客情報ファイルの漏えい
  2. 外部からのパスワードの総当たりによるメールアカウント侵入
  3. 既知のマルウェアへの感染

まとめ

- サイバー空間が現実社会とより密につながるようになり，サイバー攻撃の脅威がより深刻になってきた.
- 悪意のあるソフトウェアを（　　）という
- 情報セキュリティには，C(　　)，I(　　)，A(　　)の3つの基本要素がある.
- ファイアウォールや暗号などの対策技術があり，どの脅威にどの対策が有効か見極めて活用する必要がある.

課題1

- IPA情報セキュリティ10大脅威 (個人）
  https://www.ipa.go.jp/security/vuln/10threats2018.html　の上位10位（個人）を，C,I,Aに分類し，理由を述べよ．複数該当や，分類困難なものも残してよい．
- 提出
  - Oho-Meiji, PDF形式で提出．