

 帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

**情報セキュリティ論(4)
認証(1) 基礎**

中野秀男
帝塚山学院大学非常勤講師
大阪市立大学名誉教授、堺市情報セキュリティアドバイザー

1 情報セキュリティ論 認証(1) 2020/5/29

1

今日の話

- ▶ 認証とは
- ▶ 認証のカテゴリー
- ▶ CSモデルなど
- ▶ 認証局(CA)
- ▶ 認証の要素
- ▶ ID
- ▶ 議論



▶ 2 情報セキュリティ論 認証(1) 2020/5/29  帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

2

認証とは

▶ 認証とは

- ▶ 私があなたを中野さんだと認めること
- ▶ ATM端末があなたが正当なバンクカードの持ち主と認めること
- ▶ AがBを正当な相手だと認めること
- ▶ AやBは人(ユーザ)、マシン?
- ▶ 正当の定義は
 - ▶ 人と物では違う
- ▶ どうすれば認めたというか?



▶ 3

情報セキュリティ論 認証(1) 2020/5/29



3

認証のカテゴリー

▶ ユーザ～ホスト間

- ▶ パスワード、暗証番号
- ▶ IDカード
- ▶ 生体情報

▶ ホスト～ホスト間

- ▶ 最近はM2M(Machine to Machine), IoT

▶ ユーザ～ユーザ間

- ▶ メールが典型例
- ▶ シンタックス的認証
- ▶ セマンテック的認証



▶ 4

情報セキュリティ論 認証(1) 2020/5/29



4

CSモデル、クラウド

- ▶ クライアント(マシン、ユーザ)を信用するか
 - ▶ 知識だけがあるユーザが増えた
- ▶ サーバ・マシンを信用するか
 - ▶ CRACK版のコマンド`
 - ▶ にせのホームページ
- ▶ 情報システムのモデル
 - ▶ クライアント/サーバモデル
 - ▶ クラウドコンピューティング(SaaS, PaaS, IaaS)
- ▶ P2Pモデル: Peer to Peer



▶ 5

情報セキュリティ論 認証(1) 2020/5/29

5

認証局

- ▶ CA: Certificate Authority
- ▶ 公証役場をネットで
- ▶ 電子証明書を発行
- ▶ eTaxも電子証明書を利用
- ▶ 民間だとVerisignなど多くの業者
- ▶ Private CA
- ▶ PKI: Public Key Infrastructure(公開鍵基盤)



▶ 6

情報セキュリティ論 認証(1) 2020/5/29

6

認証の要素

- ▶ 身体情報(Something You Are)
 - ▶ バイオメトリクス(指紋、虹彩、顔、音声、筆跡)
 - ▶ マシンの場合は(IPアドレス、MACアドレス)
- ▶ 知っている事(Something You Know)
 - ▶ パスワード、パスフレーズ、暗証番号
- ▶ 持っているもの(Something You Have)
 - ▶ IDカード、RFID(無線タグ)



▶ 7

情報セキュリティ論 認証(1) 2020/5/29



帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

7

ID

- ▶ IDって
 - ▶ 人や物に付与された識別番号、識別情報
 - ▶ 住基カード、クレジットカード、PiTaPa
 - ▶ 物には(人も含めて)RFIDが
 - ▶ 携帯電話もID
- ▶ IDはセンスされる
 - ▶ 映画: Minority Report(網膜認証)
- ▶ IDは一度漏れると一人歩き
 - ▶ 漏洩防止
 - ▶ 漏洩しても犯人がわかる仕組みは?
 - ▶ IDのありかがわかるシステムの構築
- ▶ 知らず知らずのうちにTrackされるIDと情報



▶ 8

情報セキュリティ論 認証(1) 2020/5/29



帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

8

議論

- ▶ 認証はどうなっていくのでしょうか
- ▶ ものの認証は
 - ▶ ものは死なない
 - ▶ ものはコピーで大量に同じものが
 - ▶ ものの中のソフトウェア(ファームウェア)
- ▶ 信頼関係も考えてみましょう

