資料 4

ICカードについて

2007年10月15日

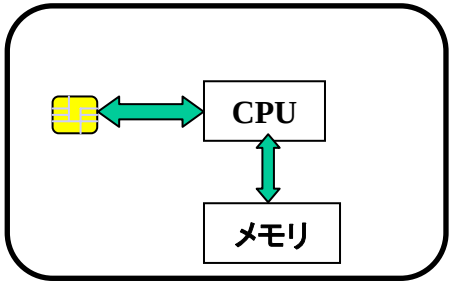
東京工業大学
統合研究院　ソリューション研究機構
谷内田　益義

本日のご説明内容

- ICカードとは？
- ICカードの安全性
  - ICカードの耐タンパー性
  - ICカードの利用条件制御
- ICの応用分野

ICカードとは？

- 一般的には演算装置（CPU)とメモリを内蔵したカード
  - CPU（8～32ビット)、とメモリ（数K～1Mバイト）
  - 偽造が難しい
    - 半導体（IC）と内部メモリ状態のコピー作成は困難
      （磁気カードは、偽造が社会問題化した）
  - 不正使用が難しく、安全性が高い
    - データの保護や安全利用を確保した小型の計算機
    - CPUが入出力を監視し、鍵（パスワード等）でデータを保護している
      - 磁気カードやメモリカードと異なり、鍵によって保護されたデータは簡単に読み出せないので、安全性が高い
    - 安全性が異なるので、メモリカードとは明確に区別されている



ICカードの安全性

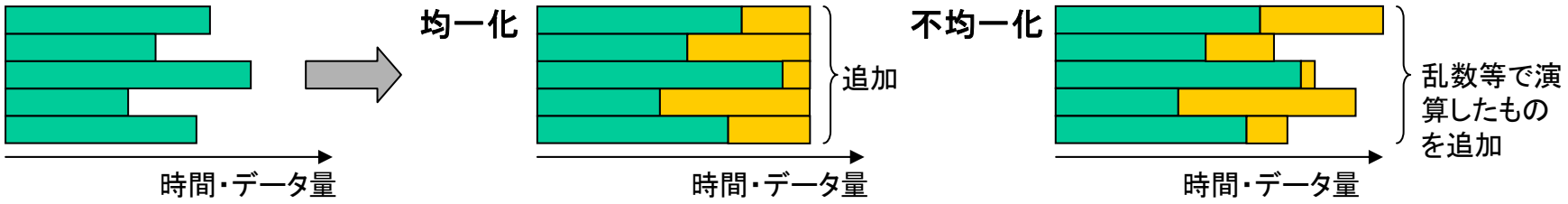
- ICカードは、**耐タンパー性**を有しており不正利用が困難
  - 統計的に考えられる不正な解析や攻撃を防ぐ防御対策をとっている

- ICカードは、**鍵（パスワード等）によって利用制限**が可能
  - メモリ上のデータファイルは、情報を読書き可能
    - 鍵との組み合わせで**ファイルごとに読み書きの利用条件の設定**が可能
    - 正しい鍵を提示した人にのみ、利用権を与える
  - **鍵**は値の設定だけが可能で、製造者・管理者であっても**値を読み出すことができない**
    - 値の照合（暗証番号・パスワード等）や認証（暗号演算）に利用できる
    - 予め設定された回数の照合や認証に失敗すると、鍵の利用を自動的に停止（閉塞）することが可能
  - 磁気カードやICタグは、読取装置があれば、データが読める
    - 磁気カードライターは比較的簡単に入手可能で、偽造も可能
  - メモリカードは、自由に読書き可能
    - USBメモリ、フラッシュメモリ、SDカード等

ICカードの耐タンパー性

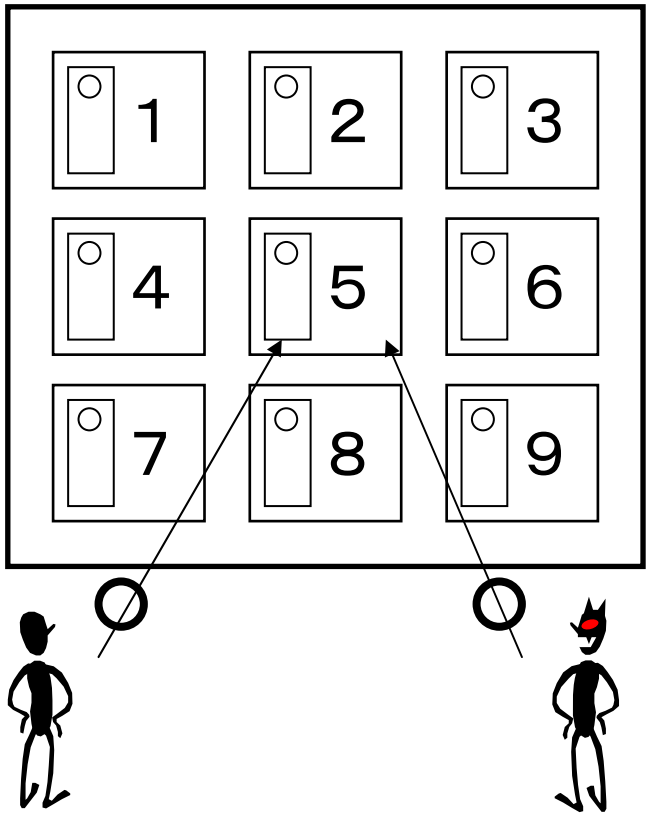
- ICチップを取り出した物理的、電気的解析に対する対策
  - ICチップ取り出しが困難な構造（樹脂による封入）
  - ICチップの多層化による物理解析の困難化（顕微鏡などの観察妨害）
  - 異常検出センサによる電気的解析の困難化（データの消去や機能停止）
  - メモリ素子の配置のランダム化による解読困難化

- ICチップの行う演算処理の消費電力や処理時間など信号の変化を測定して情報を推定する攻撃に対する対策
  - 消費電力や処理時間の均一化、不均一化による信号解析の困難化



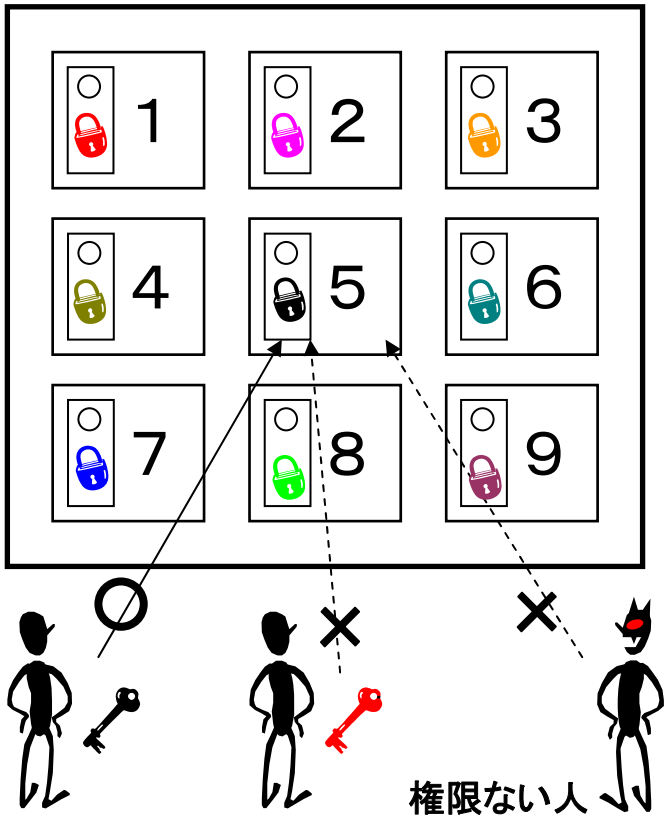
ICカードとメモリカード

メモリーカード



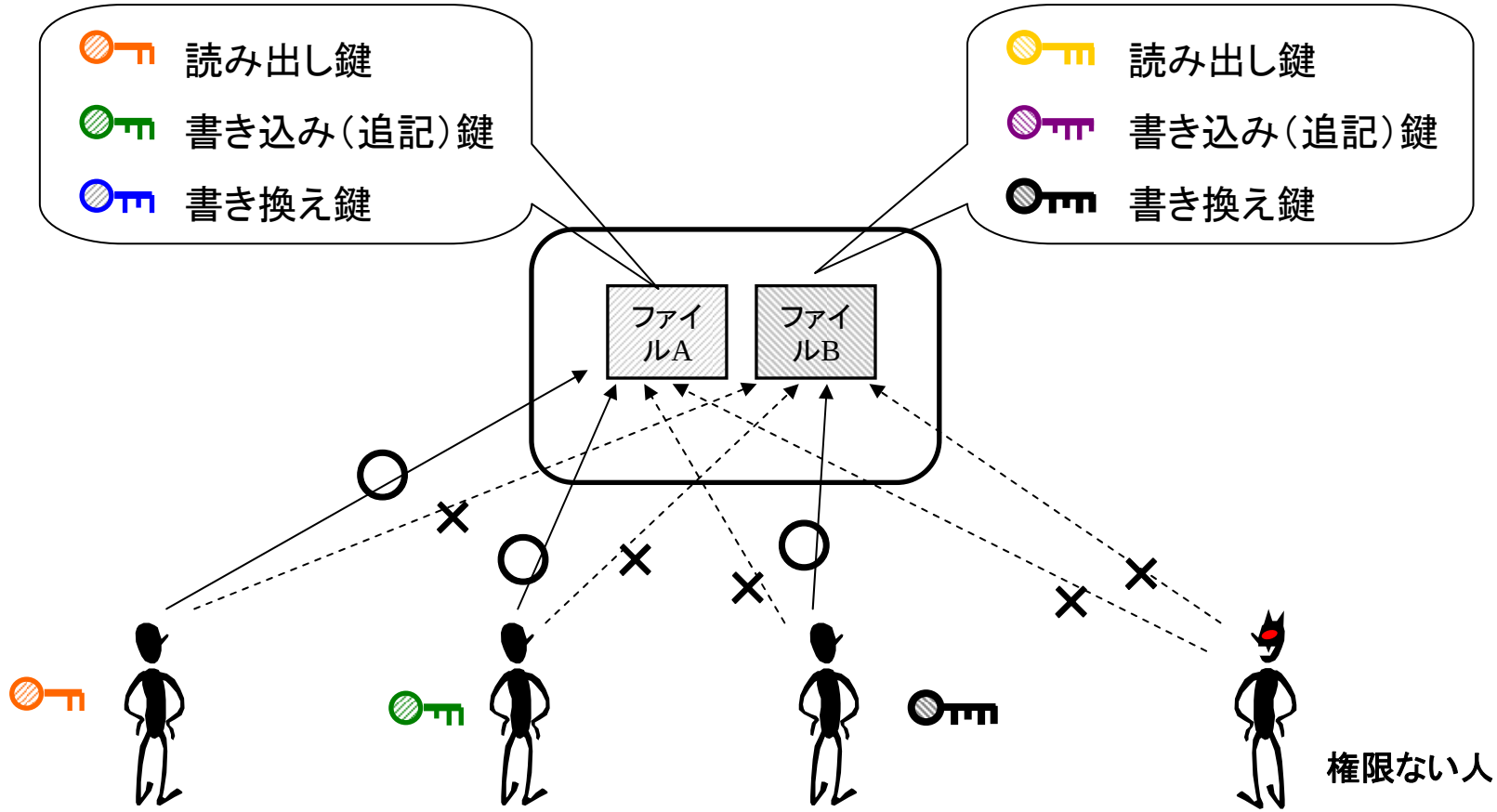
誰でも利用可能

ICカード



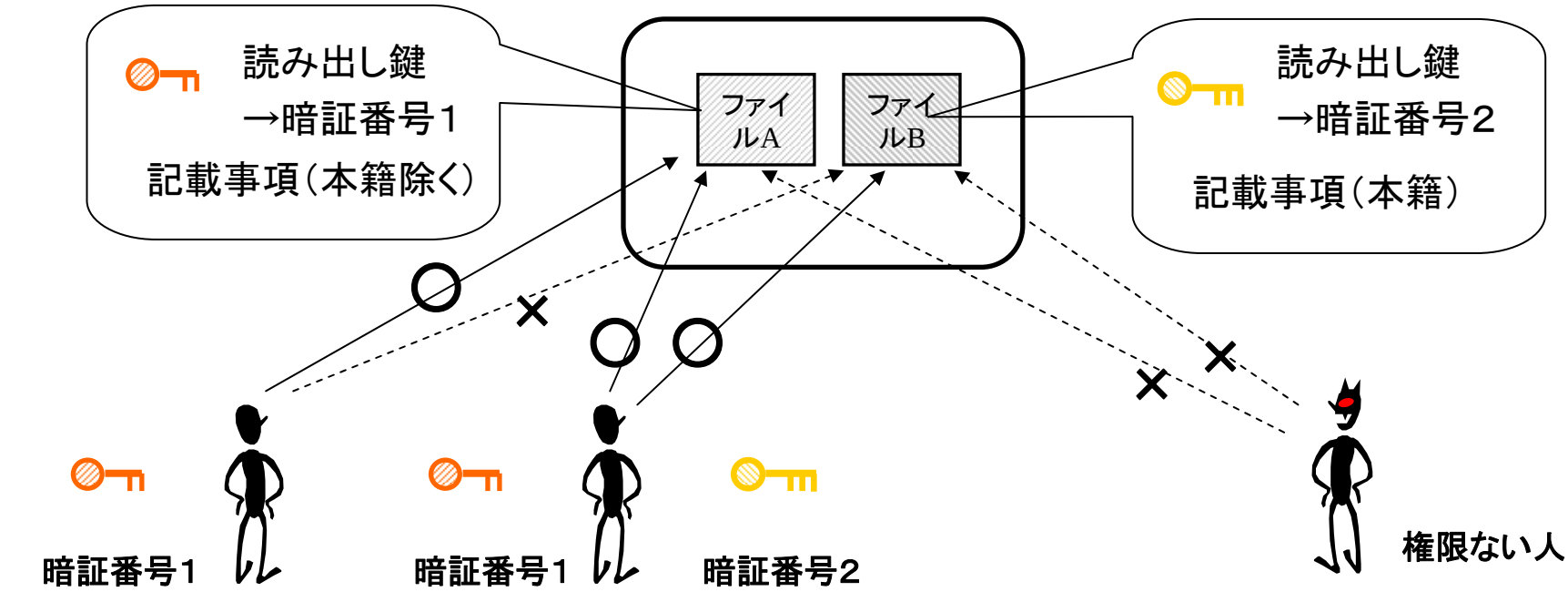
正しい鍵を持った人だけ
が利用可能

鍵による利用条件制御


読み出し鍵
書き込み（追記）鍵
書き換え鍵
読み出し鍵
書き込み（追記）鍵
書き換え鍵
ファイルA
ファイルB
権限ない人
Aは読出し可能
Bは利用不可
Aは追記可能
Bは利用不可
Aは利用不可
Bは書き換え可能
Aは利用不可
Bは利用不可

鍵による利用条件制御例

- 自動車運転免許証



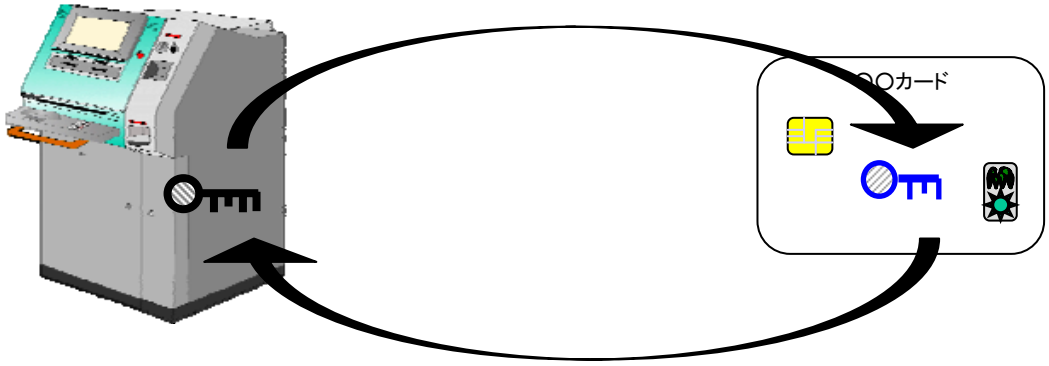
暗証番号１だけでは、
本籍は読み出せない

免許証所持者は
どちらも利用可能

・暗証番号は読み出せない
・暗証番号を3回間違えると読み出せなくなる（警察署等で回復可能）

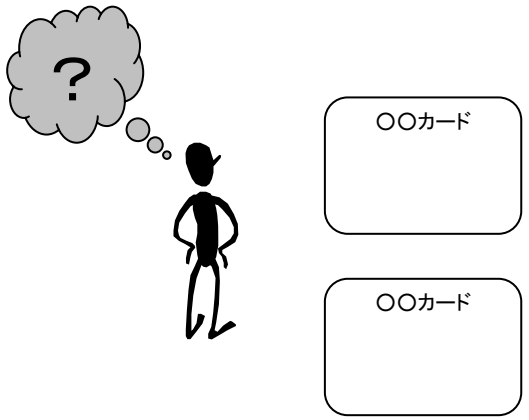
金融サービスでのICカード導入

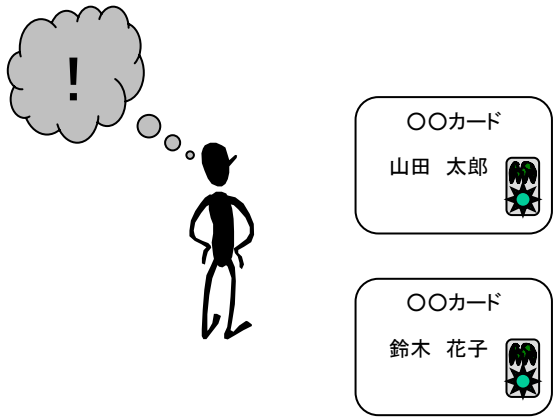
- 安全性向上
  - 偽造、不正使用が困難
    - ICカードの導入によって、フランスの金融カードの偽造変造・不正利用の被害額が1/10に（総取引額の0.27%から、0.023%に）
  - カードと利用する端末の認証
    - カードが端末の鍵を確認することで、不正な端末での利用を防止
    - 端末がカードの鍵を確認することで、不正なカードの利用を防止



カード券面情報の重要性

- 不正な利用を防ぐためには、券面の情報が重要
  - オンラインのサービス利用だけでなく対面での利用がある場合には、券面情報及びセキュリティ情報が重要
    - カードの偽造防止（例えば、クレジットカードのホログラム等や、運転免許証・パスポート等の特殊印刷等）
    - 利用者情報(氏名等）の確認





ICカードを利用したサービス例

- 広くICカードが広く利用されるようになってきた
  - テレホンカード（海外では普及。日本では廃止された）
  - 金融（キャッシュカード、クレジットカード）
  - ETCカード（カードは接点付、車載機が電波で飛ばす）
  - 放送：B-CASカード
  - 鉄道
    - JR東日本のSuica、JR西日本のICOCA、PiTaPa（関西の私鉄）、PASMO（関東の私鉄・バス）等、
    - ロンドン、パリ、シンガポール、香港の地下鉄等、海外でも実績あり
  - 身分証明書
    - 国家公務員証、社員証、職員証、学生証　等
  - 運転免許証、パスポート
    - 既に日本国内だけで数百万枚が発行されている
  - 住民基本台帳カード
    - 住民基本台帳コードの他、電子署名のための公的個人認証サービスも搭載されている

まとめ

- ICカードの安全性
  - ICカードを不正に解析するすべての脅威からの防御対策
    - チップを取り出した信号解析や顕微鏡解析による不正情報取得、消費電力や電圧および処理時間の変化からの情報や鍵の推定などのすべての脅威に対応した対策をしている。
  - 鍵（暗号鍵あるいはパスワード）の設定による利用条件制限
    - 情報が記録されるメモリ上のデータファイルは、ファイルごとに鍵を設定して保護される
    - 正しい鍵が確認された時に、鍵に応じた読み書きの利用権が与えられる
    - 鍵は、設定だけが可能で、読み出しはできない
    - 鍵の確認による正当性の保証が可能
      - パスワード・暗証番号等の照合による利用者の正当性確認・認証
      - 暗号鍵の確認による正しいカードの正当性確認・認証
      - 暗号鍵の確認によるサービス・端末の正当性確認・認証