情報I パスワードによる個人認証

教科書p.102, 105

認証

- **利用者やデバイスが本物であることを証明すること**
  - 学校では, 生徒の顔などや生徒証明書などで
    その生徒がその学校の生徒であることを証明している

認証

・サイバー空間において
1. 問題: 対面のように相手の声や顔を確認することで
   本人であるか確認できず，
   適切なサービスを利用できない
2. 目的: 本人だけがアクセス
3. 目標: ①本人だけが知っていること
   ②本人だけが持っているもの
   ③本人であることそのもの
   により証明すればよい
4. 評価: ①流出したら意味がない
   ②持ち物を盗まれると危険
   ③認証が突破される技術があると価値がなくなる

認証

- パスワード認証
  - 正規の利用者であることを
    本人だけが知っていることにより認証する
  - ユーザIDとパスワードを使って認証を行う
    - ユーザID
      - 正規の利用者であることを識別するための
        記号列
    - パスワード
      - 本人だけが知っていることにより，
        本人であることを確認するための記号列

認証

- 危険性と対策
  - ユーザIDやパスワードを他人に知られると，
    他人が別の人を装ってアクセスするなりすましなどが起こる
    - ソーシャルエンジニアリング
      - 入力しているところを盗み見る
      - 入力されているところを見られないようにする
      - 個人情報を基にパスワードを推測する
      - 推測されづらいパスワードを作成する
    - 総当たり攻撃
      - 入力可能文字のすべての組み合わせを総当たりする
      - 入力可能文字を増やしたり，桁数を増やしたりする
    - 辞書攻撃
      - よく使われている文字列を機械的に総当たりする
      - あまり使われていないようなパスワードとする

認証

・パスワードの付け方の例(理想)
  ・英字だけでなく数字と記号を含み,
    ランダムにして他人が推測できないようにする
  ・本人だけが覚えやすいものにする
  ・ほかで利用しているパスワードを使い回ししない

認証

・パスワードマネージャー

・パスワードを安全に管理するソフトウェア

1. 問題: パスワードが多く覚えられず,
   弱いパスワードを使い回す
2. 目的: すべての強力なパスワードにして
   安全に管理し, 覚える負担をなくす
3. 目標: パスワードはランダムに生成し,
   ソフトウェアでパスワードを管理する
4. 評価: パスワードは強力であり覚えなくてよいが,
   それを利用するための認証が突破されると危険

認証

・パスワードは超強力
　・英字・数字・記号を含み，ランダムで長い
・記憶の負担が少ない
　・パスワードマネージャーを利用するための
　　マスターパスワードのみを覚えていればよい
・暗号化されているので安全（？）
　・紙のメモ等と違い，紛失したり盗まれたりしない

認証

・パスキーを用いた認証
  ・正規の利用者であることを
    本人だけが持っているものにより認証する
  1. 問題: ユーザの負担を減らすことと
     不正ログインをなくすことはトレードオフ
  2. 目的: 安全・簡単に本人であることを証明する
  3. 目標: 本人だけが持っているものを利用する
  4. 評価: 覚える必要もなく,
     なりすましも起きづらく安全

認証

・生体認証
  ・正規の利用者であることを
    本人であることそのものにより認証
    ・指紋認証, 顔認証, 虹彩認証
  1. 問題: パスワードはめんどくさいし
     他人にバレやすい
  2. 目的: パスワード不要で素早く安全委ログイン
  3. 目標: 本人であることそのものを示す
     体の特徴により認証する
  4. 評価: 他人でも間違えて認証されることがある