情報Ⅰ パスワードによる個人認証

教科書 p.102, 105

認証

・(①　　)

・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

・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: サイバー空間において，本人だけがアクセス（利用可能な状態になること）

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その情報が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

・パスワード認証

・正規の利用者であることを(②　　)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

・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(③　　)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，パスワードの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の組み合わせなどにより機械的に総当たりする

→あまり使われていないような文字列をパスワードとする

・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，できる限り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

・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

・パスワードは超強力で記憶の負担が少なく暗号化されているので安全（?）

・パスキーを用いた認証

・正規の利用者であることを(④　　)により認証する次世代の認証技術

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: パスワードを使わずに安全・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（情報ではなく物）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

・生体認証

・正規の利用者であることを(⑤　　)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: (⑤　　)を示す体の特徴により認証する

4. 評価: 体の特徴の一部のみをコンピュータが読み取るため，他人でも間違えて認証されることがあり危険