2. 電子認証

（暗号利用の認証を除く）

認証

認証（身元確認）方法

1. 本人の記憶

パスワード、暗証番号など

2. 本人の所有物

身元確認用のトークン（社員カード、クレジットカード、運転免許証等）

3. 本人の特徴（Biometrics）

- **身体的特徴**：指紋、虹彩、網膜パターン、人相、掌形など
- **行為的特徴**：声紋、筆跡（署名）、キーストロークパターンなど

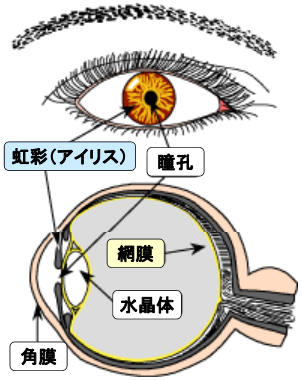
⇩

自分自身と特定のシステム（本人データの保持）との間の身元確認

付. バイオメトリクス認証製品(1)

NECの指紋認証装置
SecureFinger PI300PU-01

沖電気の虹彩認証装置
アイリスパス-S



http://www.jaisa.or.jp/action/group/bio/Technologies/Iris/Irs-f.htm

付. バイオメトリクス認証製品(2)

カメラ部(上)
液晶ガイダンスパネル(下)

富士通の非接触型手のひら
静脈認証装置 PalmGraph

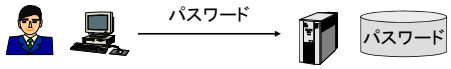
パナソニック電工の顔認証装置
デイリフェイス

http://jp.fujitsu.com/solutions/financial/services/customer/palmgraph/
http://panasonic-denko.co.jp/corp/tech/report/83j/pdfs/83_t05b.pdf

パスワード

パスワード

頭の中のパスワード

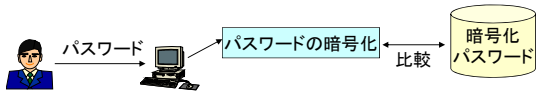


パスワードの欠点

・意味のある文字列、アルファベット文字列、短い文字列にすると解読されやすい
・意味のない文字列、特殊文字を含む文字列、長い文字列にすると覚えにくい
・安全性向上のためには、パスワードの頻繁な更新が必要だが、それが面倒
・パスワードを端末に貼り付けるなどの不注意な利用者を排除することが困難

パスワードの処理と攻撃

パスワードの暗号化



パスワードに対する攻撃

オンライン攻撃：オンラインで推測したパスワードを入力

オフライン攻撃（辞書攻撃）：パスワードファイルを盗み、辞書に基づき、パスワードを生成し、一致性をチェック

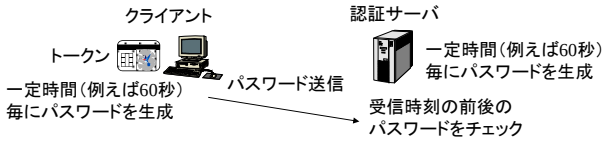
ワンタイムパスワード（1）

ワンタイムパスワード：一度限りの使い捨てパスワード

ワンタイムパスワードの方式

1. **同期方式**
   - ○ 時間同期
   - ○ カウンタ同期
2. **非同期方式**
   - ○ チャレンジ・レスポンス

時間同期方式



付．時間同期方式の例（RSA SecurID）

①入力ウィンドウが表示される

②事前登録のユーザ名を入力

③事前登録のPIN番号とカードに
表示された番号を連続して入力
但し、画面上には表示されない

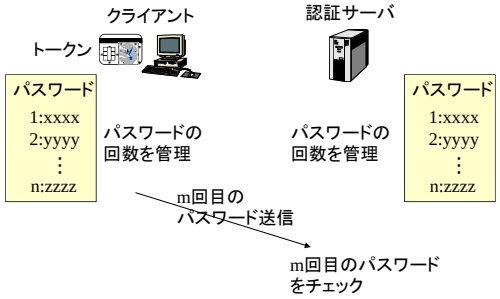
認証中画面

④認証OKなら、画面右下に鍵のマークが表示される

http://www.techmatrix.co.jp/products/security/rsasecurity/securid/example/use2.html

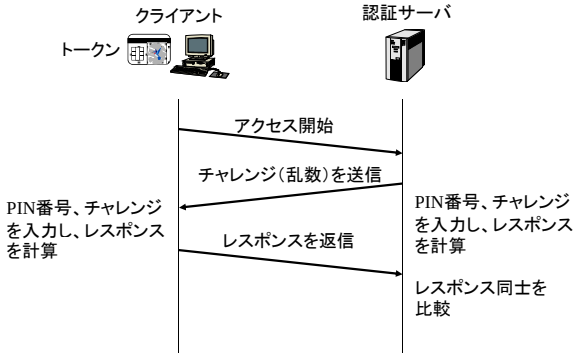
ワンタイムパスワード（2）

カウンタ同期方式



ワンタイムパスワード（3）

チャレンジ・レスポンス方式



（注）PIN: Personal Identification Number

付．S/Key

一方向性関数方式

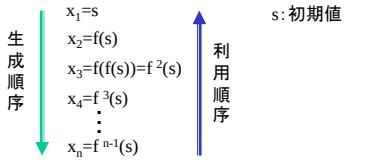
S/Key：Bellcore社によって開発された一方向性関数利用のワンタイムパスワード

一方向性関数　　f(x)としてMD4を使用

$y=f(x)$　容易に計算可能

$x=f^{-1}(y)$　逆関数の計算は困難

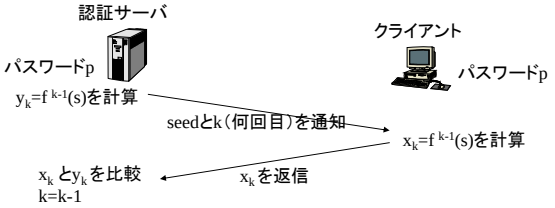
ワンタイムパスワードの生成と利用



s：初期値

付．S/Keyによる認証

S/Keyによる認証手順



関数f の計算