

## 2.2.5 パスワード・クラック

password cracking                      - パスワードを解析して探り当てること

**実習)** ファイルにパスワードをかけてみよう, システムのパスワードファイル?

**関連)** パスワードが必要となる(正当な?)理由を考えてみましょう



対象

- ・オンライン                      ← 対策: 入力ミスに対してアカウントロック
- ・オフライン                    ←

解読方法

- ・ **システムの脆弱性を使う**
  - 前回の話題
- ・ **総当り攻撃 (brute force attack)**
  - PC・ネットワークの高速・高性能化
  - すべての組み合わせを1つずつ総当りで試す

**関連)** パスワードの文字数と強度(解読時間)

アルファベット 26 文字, 数字 10 文字, 記号 などの組み合わせ

2 文字 =  $26 * 26 = 676$

キャッシュカードの番号の場合は?

- ・ **辞書攻撃**
  - 人間が使うパスワードは覚えやすいものが選ばれる傾向あり
  - よく使う単語・文字を中心に解読

**実習)** よく使われるパスワードは?

- ・ **rainbow クラック**
  - 基本的には総当り攻撃と同じ
  - あらかじめ計算・準備しておいたハッシュ値 (rainbow table) と比較することで解読

**関連)** ハッシュ値, ハッシュ関数とは? 整理しておきましょう

- ・ **盗聴による取得**
- ・ **パスワードリスト攻撃**
  - パスワードの使いまわし



**関連)** よいパスワードとは? パスワードを管理するには?

**関連)** ワンタイムパスワード (OTP) とは?

## 2.2.6 盗聴

スニッファ sniffing

→ インターネット技術についての復習

Man in the Middle 攻撃 (MITM, 中間者攻撃)

通信の間に割り込んで盗聴

キーロガー

key logger

入力した文字がすべて記録される ← インターネットカフェなどでの事例

その他

→ ショルダーハッキング [ソーシャルエンジニアリング]

→ War Driving [無線 LAN の脆弱性]