ITPASS
Information Training Program
with a Spirit of Self-help

利用者によるセキュリティ –アカウントとパスワード–

神戸大学 理学部惑星学科
地球及び惑星大気科学研究室
B4　藤原 大葵

はじめに

- セキュリティ【security】とは
  - –安全　コンピューターシステムの安全性やデータの機密性を守ること
  - –防犯　悪意のある第三者によるシステムへの不正アクセスやデータの流出・破壊などを防ぐこと

対策が必要

例) パスワードの設定, ←本講義
アクセス権の設定,
ソフトウェアのアップデート
... など

目次

- アカウントについて
- パスワードの重要性
- パスワードクラック
- 悪いパスワード・良いパスワード
- パスワードに関するマナー
- UNIX におけるパスワード管理

目次

- アカウントについて
- パスワードの重要性
- パスワードクラック
- 悪いパスワード・良いパスワード
- パスワードに関するマナー
- UNIX におけるパスワード管理

アカウントについて

- アカウント【account】とは
  - システムを利用する権利
    - 今回の実習では, 計算機を利用するための権利
    - 権利を持った人のことを ユーザ (利用者) と呼ぶ
  - ユーザになるためには事前にシステムに登録 (アカウントを作成) する必要がある
    - アカウント名 (ユーザ名)
    - フルネーム・住所等の個人情報
    - パスワード
      がアカウントの作成には必要

アカウントについて

- UNIX におけるアカウントの種類
  - システム管理者のアカウント (root)
    - システム上のすべてを支配する権限を持つ
      - 例) 新規アカウントの作成
  - 一般利用者のアカウント
    - root 以外のアカウント
    - システムの利用権限に制限がかかる
      - 例) シャットダウンすらできない

アカウントについて

- ログイン / ログアウト
  - システム利用の開始 / 終了の手続き
  - ログインには アカウント名 と パスワード が必要
    - システムは, これらを登録されているアカウント情報と照合し, アクセスを許可するか否かを判断
  - ログインすると, ログアウトするまでユーザとしてシステムを利用できる

アカウントについて

- アカウントを守るとはどういうことか？
  - 自分を守ること
    - ユーザ本人の情報やデータの流出, 破壊, 第三者による悪用を防ぐ
  - 仲間 (他のユーザ) を守ること
    - システムやその中のデータの流出, 破壊, 悪用を防ぐ
    - 悪意のある利用によるシステム運用停止を防ぐ
  - 世界 (インターネット全体) を守ること
    - 乗っ取られたシステムを踏み台にして, 他のシステムが攻撃されるのを防ぐ

目次

- アカウントについて
- パスワードの重要性
- パスワードクラック
- 悪いパスワード・良いパスワード
- パスワードに関するマナー
- UNIX におけるパスワード管理

パスワードの重要性

☆ パスワードは本人確認のための鍵や暗証番号のようなもの

☆ パスワードを他人に知られてしまうと, アカウントを悪用され, 不正にログインされてしまう可能性がある

- 自分, 仲間, 世界に被害が及ぶ

パスワードの重要性

アカウントはパスワードによって保護されている

アカウントを守る上で

パスワードは最大の砦

利用者全員が

適切にパスワードを設定し，管理しなければならない

目次

- アカウントについて
- パスワードの重要性
- パスワードクラック
- 悪いパスワード・良いパスワード
- パスワードに関するマナー
- UNIX におけるパスワード管理

パスワードクラック

- クラック（クラッキング）【cracking】とは
  - 悪意をもって他人のコンピュータに侵入して, データやプログラムを盗んだり, 改ざん, 破壊などを行うこと
  - ちなみに... ハッキング【hacking】とは（本来は）
    - コンピュータについて高い技術を用いて調査研究すること
- パスワードクラックとは
  - 他人のパスワードを解析し, 探り当てること
  - インターネット上では, パスワード解析プログラムが配布されている
  - パスワードを不正に収集し販売する業者もある

パスワードクラックの手口 その1

- 総当たり攻撃【brute-force attack】
  - パスワードとして可能な全ての組み合わせを力ずくで試す
    - brute = 獣のような
  - 長いパスワードほど, クラックは困難
  - ➢ 株式会社ディアイティが 2012 年(古い)に行った試算
    - アルファベット (大文字・小文字), 数字, 記号の合計 93 文字を利用できるとして計算
    - PC (CPU : Intel Core i7, システムメモリ : 8 GB, GPU : GeForce GTX 680, OS : Windows7 (64bit)) → 45 億パターン/秒
      - 4 文字 (7481 万通り) : 1 秒以下
      - 6 文字 (6470 億通り) : 2 分 24 秒
      - 8 文字 (5596 兆通り) : 14 日
      - 10 文字 (4840 京通り) : 341 年

このデータは古い！
この試行時間に安心してはいけない
桁数を増やせばそれだけ試行回数が天文学的に増える

パスワードクラックの手口 その1

- HYVE SYSTEMS(アメリカ)が 2020 年に行った試算
  - ハッシュ関数MD5を用いて保存したパスワードの総当りに要する時間
  - GPUはRTX 2080 を用いており、約370 億ハッシュ/秒　で計算

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	61tm years	100tn years	7qd years

(https://www.hivesystems.io/blog/are-your-passwords-in-the-green?utm_source=tabletext)

パスワードクラックの手口 その2

- 辞書攻撃【dictionary attack】
  - パスワードに使われそうな単語を収集し, クラッキング用の辞書を作成
    - 専門用語や趣味の用語まで網羅
  - 大/小文字・数字の変換, 簡単な組み合わせにも対応

■ 例 : Open Wall
  - パスワードクラックツールを開発
  - 4000 万語の単語が載っている辞書ファイルを販売 ($27.95)

パスワードクラックの手口 その3

- ソーシャルエンジニアリング【social engineering】
  - ソーシャルハッキング, ソーシャルクラッキングとも
  - システムではなく, 人を狙った攻撃

■例：

- 肩越しに覗く（shoulder hacking）
- ゴミ箱から収集する（trashing）
- 管理者を装って聞き出す
- メールなどのURL
- 内通者に聞く

…など

パスワードクラックの手口 その4

- パスワードリスト攻撃
  - 何らかの方法によりあらかじめ入手した ID とパスワードを利用
  - 同じ ID・パスワードの組み合わせを複数のアカウントで登録していると, 被害に遭いやすい

◆事例：

- ニコニコ動画不正アクセス事件 (2014 年)
- ディノス・セシール不正ログイン事件 (2015 年～2017 年)
- 楽天ポイント・龍角散爆買事件 (2017 年)

前半のまとめ

- アカウントとは
  - システムを利用する権限
  - パスワードによって守られている
- パスワードは最大の砦
  - パスワードは厳重に管理する
  - アカウントを乗っ取られると, 自分だけでなく仲間や世界にも被害が及ぶことを意識する
- パスワードクラックの手口
  - 総当たり攻撃
  - 辞書攻撃
  - ソーシャルエンジニアリング
  - パスワードリスト攻撃　　などなど

目次

- アカウントについて
- パスワードの重要性
- パスワードクラック
- 悪いパスワード・良いパスワード
- パスワードに関するマナー
- UNIX におけるパスワード管理

悪いパスワード

氏名：森 祥介, アカウント名：hoge
住所：神戸市灘区六甲台町1-1, 電話：078-881-12**

次のようなパスワードはダメ！

- アカウント名, 本名, 関係者の名前
  - hoge, mori, ishikawa
- 電話番号, 住所, 生年月日など個人情報から推測できるもの
  - 07888112, rokkodai
- 上記から簡単に作れるもの
  - Ymori, Mori078, mori07
- 上記を「s を $」，「o を 0」，「i を 1」など単純な規則で変えたもの
  - $m0r1

悪いパスワード

次のようなパスワードもダメ！

- 人名, 固有名詞, コマンド
  - nakata, tsurukabuto, bonobono, passwd
- 辞書に載っている単語
  - favorite, wine
- 単語の羅列, 繰り返し, 逆綴り
  - winecheese, favoritefavorite, etirovaf
- 専門用語
  - Archimedean principle (アルキメデスの原理)
- 全て数字や同じ文字
  - 111111, aaaaaa
- 10 文字未満

悪いパスワード

WORST PASSWORDS OF 2017　TOP 100

- セキュリティ企業 splash data より -

1 位 … 123456
2 位 … password
3 位 … 12345678
4 位 … qwerty
5 位 … 12345
6 位 … 123456789
7 位 … letmein
8 位 … 1234567
9 位 … football
10 位 … iloveyou

11 位 … admin
12 位 … welcome
13 位 … monkey
14 位 … login
15 位 … abc123
16 位 … starwars
17 位 … 123123
18 位 … dragon
19 位 … passw0rd
20 位 … master

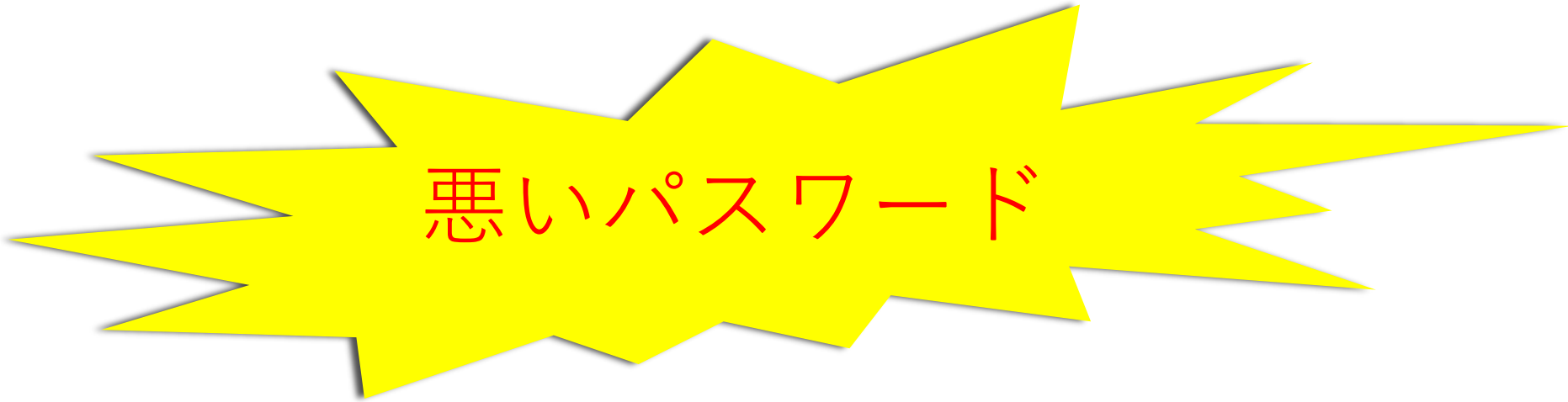
⋮

(比較的) 良いパスワード

無意味で, しかし自分では忘れない

- 文章や詩などの頭文字を並べてみる
  - Boys be ambitious! – W. S. Clark. → Bba!wsc.
  - Aki no Tano Kariho no Iono Toma wo Arami Waga Koromodeha Tuyu ni Nuretutu → atkitawktn
- できるだけ, 「大文字と小文字」, 「記号」, 「数字」を混在させる
  - Bba!wsc. → B6a!*wsc.
  - atkitawktn → Atk1t@Wktn

もちろん, ここで挙げたパスワードは全て



である！！

えっ、なんで？

良いパスワードの条件

- 頑丈であること
  - 十分な長さ (= 10 文字以上) があること
  - 英数字, 大文字, 記号 が混在していること

- 自分にとって 覚えやすい・忘れにくい こと
  - ただし, 同じパスワードを使い回さない

  - 「基本フレーズ + サービス名など」
    でパスワードの使い回しを避ける

    というのは、最近では破られやすいらしい...

パスワードに関するマナー

- 人が入力しているところは見ない
- アカウントの貸し借りはしない
- 決して人に教えない
- できるだけ頭にしまっておく
- メモするなら, 見せない・捨てない・なくさない
- 同じパスワードは使い回さない
- 初期パスワードは最初のログイン時に変更する
- ~~定期的に変更する~~
  - 定期的な変更はセキュリティ効果が薄い
    - 定期的に変更しようとするとパスワードが簡単になりがち

(総務省：安全なパスワードの管理)

目次

- アカウントについて
- パスワードの重要性
- パスワードクラック
- 悪いパスワード・良いパスワード
- パスワードに関するマナー
- UNIX におけるパスワード管理

UNIX におけるパスワード管理 (1)

- ユーザの基本情報, パスワードに関する情報は, /etc ディレクトリの passwd, shadowファイルに保存されている

- /etc/passwd ファイル
  - ユーザの基本情報を記録
  - root ユーザだけでなく, 一般ユーザも閲覧可能
    - パスワードは /etc/shadow ファイルで管理する

UNIX におけるパスワード管理 (1)

- /etc/passwd ファイルの内容例

```
hoge:x:501:501:HOGE:/home/hoge:/bin/bash
alis:x:502:502:Alice:/home/alis:/bin/bash
bob:x:1202:1201:BOB:/home/bob:/bin/bash
```

✓ 「:」で区切られた 7 つのフィールドで構成

	項目	説明
1	ユーザ名	ユーザ名を記述
2	パスワード	• 「x」: **パスワードは暗号化され**, 「/etc/shadow」 ファイルで管理されている • 「*」: 一時的にユーザのアカウントを無効化する場合に設定 • 「」 **(設定なし)** : パスワードが設定されていない状態
3	ユーザ ID	ユーザの ID を記述
4	グループ ID	ユーザが所属している主グループの ID を記述
5	コメント	フルネームや役割などのコメント情報を記述
6	ホームディレクトリ	ユーザのホームディレクトリの場所を記述
7	ログインシェル	ユーザがログインした際に割り当てられるシェルを記述

UNIX におけるパスワード管理 (2)

- /etc/shadow ファイル
  - 暗号化/ハッシュ化されたパスワードと, パスワードに関連する情報などを記録
  - ログイン時には入力されたパスワードを暗号化/ハッシュ化し, それが /etc/shadow ファイルの内容と一致するか確認する
  - 一般ユーザは閲覧できず, root ユーザのみ読み書き可能
    - 一般ユーザは, 暗号化/ハッシュ化されたパスワードを参照することさえできない
- 暗号化：復号可能な可逆変換
- ハッシュ化：復号不可能な非可逆変換

UNIX におけるパスワード管理 (2)

- /etc/shadow ファイルの内容例

```
hoge:EV7RndYXv5pHs:11941:0:99999:7:::0
alis:$1$wpkFeWyW$dRnpRo1XDyGJQkc1IM3CT1:10907:0:99999:7:::0
```

  - ✓ 「:」で区切られた 9 つのフィールドで構成

	項目	説明
1	ユーザ名	ユーザ名を記述
2	パスワード	暗号化/ハッシュ化されたパスワードを記述
3	最終パスワード変更日	最後にパスワードが変更された日を, 1970年1月1日からの経過日数で記述
4	パスワード変更可能日数	パスワードが再度変更可能になるまでの日数を記述
5	パスワード有効期間	パスワードの変更が必要になるまでの日数を記述
6	パスワード変更期間警告通知日	パスワード有効期限切の警告を何日前から通知するかの日数を記述
7	パスワード有効期限経過後, アカウント使用不能になるまでの日数	有効期限経過後にパスワードを変更しなかった場合にアカウントが使用不可になるまでの日数を記述
8	アカウント有効期間	アカウントが使用不可になるまでの日数を, 1970年1月1日からの経過日数で記述
9	予約フィールド	現在は使用されていない

UNIX におけるパスワード管理 (3)

- パスワード文字列の変換に用いられる方法

① 古くは DES (Data Encryption Standard) を用いていた

DES → 64bit単位のデータを暗号化（パスワードは8文字以内）

② 現在はより安全な SHA-512 (Secure Hash Algorithm 512) が用いられている

SHA-512 → (ほぼ)任意の長さのデータを512bitにハッシュ化

```
hoge:EV7RndYXv5pHs:11941:0:99999:7:::0                          -①
alis:$6$wpkFeWyW$dRnpRo1XDyGJQkc1IM3CT1:10907:0:99999:7:::0     -②
```

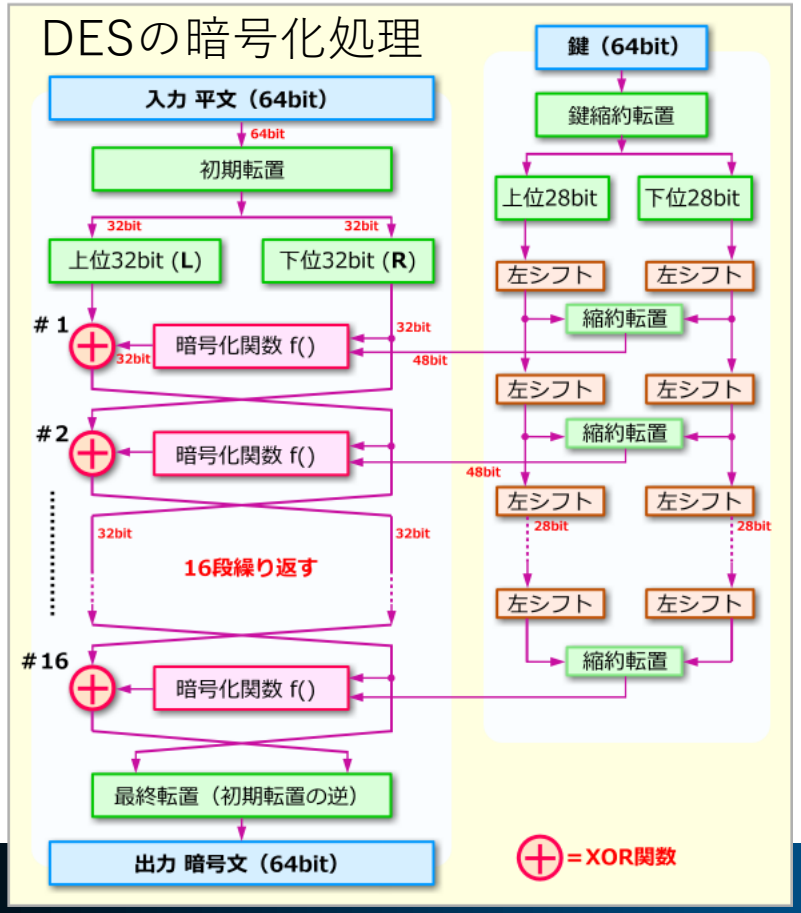
暗号化の種類

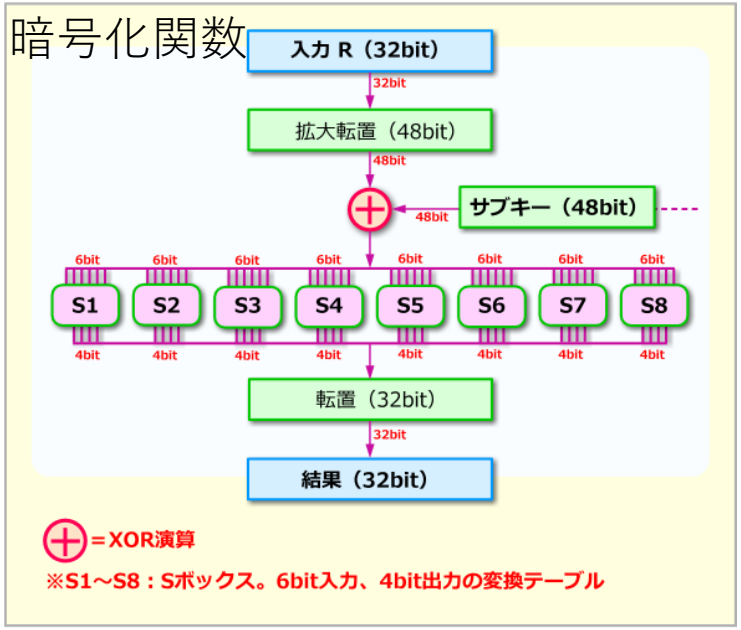
salt (ハッシュ化に利用する乱数)

パスワード + saltをハッシュ化したもの

余談1：DES

- DESでは、64bit単位のデータに対して、ビット位置の変更（転置）やテーブル参照による置き換え（置換）、XOR演算、シフト、繰り返し処理などを組み合わせて、入力されたデータを可能な限り「かき混ぜる」という処理を行っている。



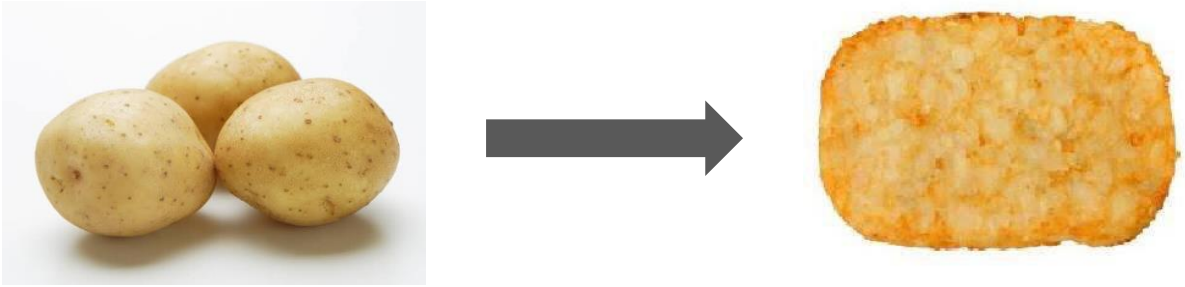


(https://www.atmarkit.co.jp/ait/articles/1505/21/news030.html)

余談2：SHA-512

- SHA-512とは、任意の長さの原文から固定長の特徴的な値を算出するハッシュ関数（要約関数）の1つ。どんな長さの原文からも512ビットのハッシュ値を算出（ハッシュ化）する。

- ハッシュ化 ～ データの非可逆変換（暗号化ではない）



- 暗号化ではなくハッシュ化なので、復号できない。

(http://e-words.jp/w/SHA-2.html)

後半のまとめ

- 推測されやすい「悪い」パスワードはつけない
  - 個人情報, 辞書に載っている単語など
- パスワードに関するマナー
  - 人が入力しているところは決して見ない
  - アカウントの貸し借りはしない
  - 決して人に教えない
  - …
- ユーザの情報はファイルに記録される
  - 基本情報：/etc/passwd
  - パスワード情報：/etc/shadow

参考文献

- 神戸大学 ITPASS 実習　2021 年 3 日目『利用者によるセキュリティ - アカウントとパスワード -』
  - https://itpass.scitec.kobe-u.ac.jp/exp/fy2021/210811/lecture_account/pub/itpass_lecture_account_2021.pdf
- コトバンク　『セキュリティ』
  - https://kotobank.jp/word/セキュリティ
- アカウントとは (account)
  - http://www.toha-search.com/it/account.htm
- パスワードリスト攻撃とは? 被害の原因と対策方法
  - https://cybersecurity-jp.com/security-measures/18665
- splash data 『WORST PASSWORD OF 2017』
  - https://s13639.pcdn.co/wp-content/uploads/2017/12/Top-100-Worst-Passwords-of-2017a.pdf
- /etc/passwd と /etc/shadow ファイルについてのまとめ
  - http://www.server-memo.net/centos-settings/system/passwd_shadow.html

今日の1冊

- 高町 健一郎, 大津 真, 佐藤 竜一, 小林 峰子, 安田 幸弘, 2011, Linuxの教科書ーホントに読んでほしいroot入門講座 [改訂版], 毎日コミュニケーションズ, ISBN-13: 978-4872802788
- Linux の運用について 1 から解説してくれている. システム管理者が主な対象となっている. 少し古い本.
- 第 6 章に「クラッキング対策」としてパスワード管理やセキュリティ対策について解説してくれている.
- 507号室の本棚と自然科学系図書館に置かれている.

実習（8/9 13:00 ~ ）の概要

- 2つの計算機にアカウントを作成します
  - 情報実験機 (joho??) : 目の前の計算機
    - 実習で使う計算機です
  - ITPASS サーバ : 507号室の南側にあります
    - ITPASS グループで運用しているサーバ
    - レポート提出はこのサーバで行います (詳細は後ほど説明します)
    - 通称「ika (イカ) 」 … ちなみに, tako (タコ) もいます

実習に向けて

- 今の講義を参考にして, 考えてきたパスワードを再考して下さい
  - 「悪いパスワード」ではないですか…？
- アカウント名は 英小文字 + 数字で 8 文字以内 (混在でなくて良い)
  - 先頭は英小文字のみ
  - 「-」「_」「@」「.」などは使用不可
  - 学籍番号, 無意味な文字列は避けて下さい
  - 本人であることが分かるものが望ましい
  - ただし、珍しくない姓や名だけは避けましょう (tanaka, yamada など)
- パスワードは 5 個 必要です