利用者によるセキュリティ

アカウントとパスワード

用語解説(1) アカウント

システムを利用する権限

UNIX におけるアカウントの種類

- システム管理者 (root)
  システム上の全てを支配する権限を持つ
- 一般利用者
  各人を識別するアカウント名(ユーザ名)

用語解説(2) ログイン/ログアウト

システムの利用開始/終了手続き

ログイン(利用資格の確認)

- アカウント名とパスワードの組み合わせによる本人認証

パスワードはアカウントを守る唯一の砦

パスワードの重要性

アカウントを守ることは
- 自分を守ること
- 仲間を守ること
- 世界を守ること

あなたのアカウントを使って行われた不正行為の責任は<あなた>にあります

パスワードクラック

他人のアカウントを守るパスワードを盗み出すこと

- 総当たり攻撃，辞書攻撃
- ソーシャルエンジニアリング

パスワードクラックの手口 (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試す
- 長いパスワードほどクラックするのに時間がかかる

アルファベット・数字・記号を利用の場合
(日経パソコン 2010.12.13)

5 文字	→	13.5分	6 文字	→	22時間
7 文字	→	87日	8 文字	→	23年

パスワードクラックの手口 (2)

辞書攻撃 (Dictionary Attack)

- クラッキング用の辞書を使った総当たり攻撃
  - 様々なソースから単語を拾集
  - 専門用語や趣味の世界の単語も含む
- 大文字/小文字/数字の変換などにも対応

辞書に載っている単語を使ったパスワードは
ほとんど一瞬でクラックされる

パスワードクラックの手口 (3)

ソーシャルエンジニアリング
(Social Engeneering)

- 肩越しに情報を盗み見る
- ゴミ箱から情報を盗む
- 権威ある人になりすまして情報を聞き出す
- 仲間のふりをして情報を聞き出す

悪いパスワード

- アカウント名，人名，地名
- 電話番号，生年月日
- 固有名詞，辞書に載っている単語
- 全部数字，全部同じ文字
- ８文字未満

The Top 500 Worst Passwords of All Time

http://www.whatsmypass.com/the-top-500-worst-passwords-of-all-time

1 123456	11 letmein	21 6969
2 password	12 baseball	22 jordan
3 12345678	13 master	23 harley
4 1234	14 michael	24 ranger
5 pussy	15 football	25 iwantu
6 12345	16 shadow	26 jennifer
7 dragon	17 monkey	27 hunter
8 qwerty	18 abc123	28 fuck
9 696969	19 pass	29 2000
10 mustang	20 fuckme	30 test

(比較的)よいパスワード

無意味で，しかし自分は忘れない

- 文章や詩などの頭文字を並べる
- 大文字/小文字，記号，数字を混在させる

例：春はあけぼの

頭文字を抽出	→	Hrhakbn
数字/記号を追加	→	Hrh@k6n
８文字にする	→	Hrh@k6nX

パスワードにまつわるマナー

- 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
- 他のアカウントと同じにしない
- 初期パスワードは最初のログイン時に変える
- たまに変更する

まとめ

アカウント
- システムを利用する権限

パスワード
- アカウントを守る最後の砦
- パスワードの適切な管理はシステム利用者の義務