
帝塚山学院大学
 TEZUKAYAMA GAKUIN UNIVERSITY

情報セキュリティ論(5) 認証(2) パスワード


中野秀男
 帝塚山学院大学非常勤講師
 大阪市立大学名誉教授、堺市情報セキュリティアドバイザー


1 情報セキュリティ論 認証(2) 2020/6/5

1

今日の話

- ▶ パスワードの歴史
- ▶ Good Password/Bad Password
- ▶ パスワードが破られると
- ▶ パスワードその後
- ▶ SSO, OpenID
- ▶ ウェブのセッション認証
- ▶ 議論




▶ 2 情報セキュリティ論 認証(2) 2020/6/5
 
帝塚山学院大学
 TEZUKAYAMA GAKUIN UNIVERSITY

2

パスワードの歴史


- ▶ ログイン/オンとパスワード
- ▶ アクセス制御のためのパスワード
 - ▶ WEBのアクセス制限など
- ▶ UNIXの8文字のパスワードからPGPのパスフレーズへ
 - ▶ 中野のパスワード
 - ▶ 中野のPGPのパスフレーズ
- ▶ CPUパワーのアップでパスワードの危機
 - ▶ 辞書アタック, CRACKプログラム
- ▶ 防御
 - ▶ Aging, 他の要素との併用、複数化
 - ▶ 今は二要素認証、ワンタイムパスワード(OTP)

▶ 3 情報セキュリティ論 認証(2) 2020/6/5
 
帝塚山学院大学
 TEZUKAYAMA GAKUIN UNIVERSITY

3

Bad/Good Password

- ▶ **Bad Password**
 - ▶ 辞書に載っている単語は使わない
 - ▶ 英語、日本語、人名(アイドル)、専門用語
 - ▶ CRACKソフトによるパスワードチェック
- ▶ **Good Password**
 - ▶ 2つの単語並べて間に記号や数字(実は危ない)
 - ▶ 文章の単語の頭文字に数字記号を挿入
 - ▶ tnsy7kbyn:
 - トンネルを抜けるとそこは雪国(川端康成)




4 情報セキュリティ論 認証(2) 2020/6/5 帝塚山学院大学 TEZUKAYAMA GAKUIN UNIVERSITY

4

パスワードを破られると

- ▶ 破られた事件は昔から、今でも
- ▶ 自分のファイルが破壊されるだけでなく
 - ▶ 利用される踏み台攻撃
- ▶ 組織内では適正な指導を
 - ▶ 簡単なパスワードの人は指導
- ▶ パスワードの見えるtelnet,ftp
 - ▶ なまパスワードはネットワークを通さない
- ▶ 他人がパスワード入力時は離れるのが礼儀
 - ▶ 少なくとも横を向く
 - ▶ 盗もうと思えば




5 情報セキュリティ論 認証(2) 2020/6/5 帝塚山学院大学 TEZUKAYAMA GAKUIN UNIVERSITY

5

パスワードその後(1)

- ▶ システム管理者やっていると多くのパスワード
 - ▶ 普通の人でも最近はいくつかのパスワード
 - ▶ 三つぐらいがいいのでは
 - ▶ 私の場合は
- ▶ これからはパスワードとIDカードか?
 - ▶ セキュリティレベルに応じて身体情報も
- ▶ 増える One Time Password(OTP)
 - ▶ Secure Card: ユーザとホストが乱数を共有
 - ▶ S Key: ランダムに生成した乱数を最後から使用
 - ▶ 一方向性関数で生成
 - ▶ ネットバンキングなど




6 情報セキュリティ論 認証(2) 2020/6/5 帝塚山学院大学 TEZUKAYAMA GAKUIN UNIVERSITY

6

パスワードその後(2)

- ▶ パスワードだけは、もうダメなので多重認証
- ▶ 多くはパスワードや暗証番号以外に他の認証も
 - ▶ 二重認証、多重認証




- ▶ 例
 - ▶ 他の端末でも認証
 - ▶ 番号を送る(One Time Password)
 - ▶ ログインをしたことを知らせて、おかしければアクションを
 - ▶ 暗証番号とカードの代わりにカードと生体認証
 - ▶ いずれは体にマイナンバーを埋め込むのなあ！

7 情報セキュリティ論 認証(2) 2020/6/5 帝塚山学院大学 TEZUKAYAMA GAKUIN UNIVERSITY

7

SSOとOpenID

- ▶ SSO
 - ▶ Single Sign On
 - ▶ 組織内のいろいろなサービスのサーバに
 - ▶ 最初のログインだけで入れる仕組み
 - ▶ WindowsのActive Directory
 - ▶ LDAP
- ▶ OpenID
 - ▶ 特定のベンダーのユーザ名とパスワードで
 - ▶ 他のベンダーのサービスが使える仕組み




8 情報セキュリティ論 認証(2) 2020/6/5 帝塚山学院大学 TEZUKAYAMA GAKUIN UNIVERSITY

8

ウェブのセッション認証

- ▶ httpはショートセッション
 - ▶ 一回のやりとり
 - ▶ 見かけ上ロングセッションにするために必要な認証
 - ▶ URLに識別情報を含めて認証
 - ▶ 識別情報を含めたURLがコピーや改変されるとまずい
- ▶ クッキー
 - ▶ サーバがクライアントにクッキーを送ることで
 - ▶ クライアントを認証
 - ▶ クッキーが盗まれるとまずい



9 情報セキュリティ論 認証(2) 2020/6/5 帝塚山学院大学 TEZUKAYAMA GAKUIN UNIVERSITY

9

議論

- ▶ 認証はどうなっていくのでしょうか
 - ▶ 緩やかな認証: IDではなく組織やコミュニティの認証は?
- ▶ 信頼関係も考えてみましょう
 - ▶ PGP的に: 友達の友達は友達モデル
 - ▶ 「いいね」の代わりに「信頼している」マーク
 - ▶ 警察的に: 友達の友達は友達でない



▶ 10

情報セキュリティ論 認証(2)

2020/6/5



10