

情報セキュリティと情報倫理

第8回 ホストセキュリティ技術
2022/11/25

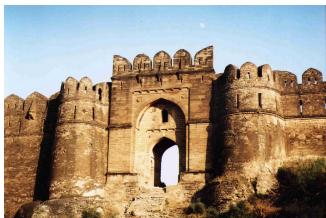
Nov 25, 2022 京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度) 1

第八回

ホストセキュリティ技術

Nov 25, 2022 京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度) 4

ホストセキュリティ技術



- ホスト=城塞
 - サイバー空間と物理空間も原則は同じ
 - 外部との接触は避けられない
 - どうやって攻略を防ぐか?

Nov 25, 2022 京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度) 6

概要

①全学共通科目1年生後期

②金曜日五時限(16:10-17:40)

③担当:

★樹田秀夫・永井孝幸・森真幸(情報科学センター)

④評価方法(予定)

★毎回のミニレポート(20%)

◆出席を前提とした課題内容(予定)

★1回程度の課題レポート(30%)

★期末テスト(50%)



⑤参考書:情報のセキュリティと情報倫理(山田恒夫・辰巳丈)

★ISBN978-4-595-31897-9 C1355 ¥2600E

⑥参考書: IT社会の法と倫理 第二版(サラ・バーズ著)

★ISBN978-4-89471-430-4 C3032 ¥3900E

Nov 25, 2022 京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度) 3

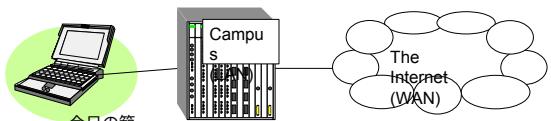
ホストセキュリティ技術

シラバスより

⑦パスワードによるユーザ認証やファイルに関するアクセス制御など、計算機を不正利用から防御する技術について議論する。

第9回 ネットワークセキュリティ技術

⑧インターネットにおける通信の仕組みと不正通信の事例を取り上げ、ファイアウォールやネットワーク侵入検知システムなど不正通信からの防御手段について議論する。



Nov 25, 2022 京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度) 5

防御の考え方

- 入らせない
- 使わせない
- 楽にさせない
- 自由にさせない
- ヒントを与えない



Nov 25, 2022 京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度) 7

最少権限の原則

- 最低限必要な範囲で利用を許可
 - 必要な人にしか利用させない
 - 必要な情報にしかアクセスさせない
 - 必要な通信しか許可しない
 - 必要な工具(プログラム)しか利用させない
 - 必要な機能しか利用させない
 - 必要な操作しか許可しない



Nov 25, 2022

画像: <http://wired.jp/2015/04/30/work-flow-office-pod/>
京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

8 8

今日の話

- 侵入の手口
 - パーソナルファイアウォール
 - ユーザ認証(本人確認の仕組み)
 - アクセス制御(許可したことしかさせない仕組み)
- 被害の拡大防止手段
 - スロットリング,セキュアOS,監査ログ
- ハッカーとクラッカー

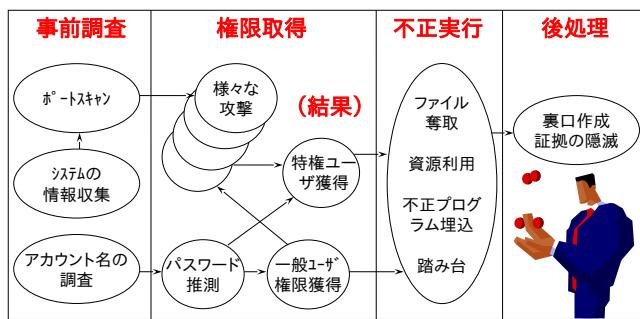
Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

9 9

2. 攻撃手法

- 外部からの攻撃(侵入)の流れ



Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

10 10

1) 事前調査

- システム情報の収集
 - IPアドレス
 - サーバ名
 - サーバソフトウェア
 - OSの種類、バージョン
 - 提供されているサービス
 - 侵入検知システム
- Webサイトの調査やポートスキャンを実行

ポートスキャンとは?

攻撃・侵入の前段階として、標的のコンピュータの各ポートにおけるサービスの状態を調査すること。

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

11 11

2) 権限取得

- ツールなどを使用し、パスワードを強引に解読して権限を取得 = パスワードクラッキング
- パスワードクラッキングの手法
 - ブルートフォース攻撃
 - 辞書攻撃
 - 特殊な辞書を使用して照合

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

12 12

3) 不正実行

- さまざまな不正行為を実行する
 - 盗聴
 - 改ざん
 - なりすまし
 - 破壊
 - コンピュータ不正利用
 - 不正プログラムの埋め込み
 - 踏み台

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

13 13

4) 後処理

- ・証拠隠滅
ログの消去などにより侵入の形跡を消す
- ・バックドアの作成
次回の侵入を容易にするための裏口を設置

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

14 14

まずやること

- ・ヒントを与えない

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

15 15

6) パーソナルファイアウォール(1)

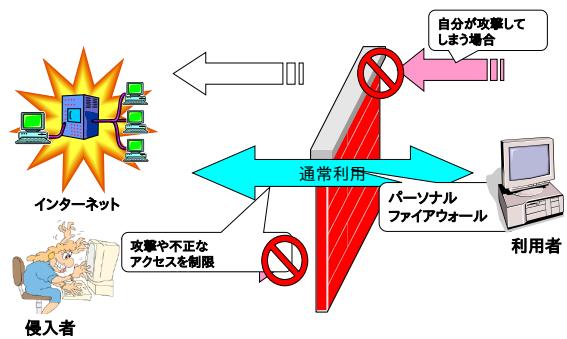
- ・インターネットに常時接続する個人ユーザに効果的
- ・さまざまな製品が発売されている
 - ウィルス対策ソフトウェアと組合せたもの等
- ・Windows の(簡易)ファイアウォール機能
 - Windows Defender

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

16 16

6) パーソナルファイアウォール(2)



Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

17 17

脆弱性

- ・脆弱性が入り込む場所
 - 作成したソフトウェア本体
 - 利用しているライブラリ(ソフトウェア部品)
 - 通信方式・データ形式
 - 入出力処理
- ・脆弱性を使った攻撃
 - バックドア、権限昇格、サービス拒否

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

18 18

脆弱性の具体例

- ・初期・デフォルトパスワード未対策
 - ・境界値チェック・入力値チェック不良
 - ・バッファオーバーフロー・オーバーラン
 - ・メモリリーク
 - 等々
- ・ c.f. <http://www.ipa.go.jp/security/awareness/vendor/software.html>

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

19 19

ネットワークアプリケーション

- プロトコル(通信規約)を決めて相互に通信
 - 決められたデータ形式・手順で送受信
- プロトコルの動作確認は難しい
 - 異常状態は無数に存在する

```
S: 220 xen02.dsm.cis.kit.ac.jp ESMTP Postfix
C: hello myserver.example.jp
S: 250 Nice to meet you !
C: mail from <h-masuda@kit.ac.jp>
S: 250 2.1.0 Ok
C: to <h-masuda@kit.ac.jp>
S: 250 2.1.5 Ok
C: data
S: 354 End data with <CR><LF>,<CR><LF>
C: From: h-masuda@kit.ac.jp
C: .....
C: 250 2.0.0 Ok: queued as BBB28531F
C: quit
S: 221 2.0.0 Bye
```

メール転送プロトコルの例

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

20 20

プロトコル実装の難しさ

- 通信バッファ
 - 相手から送られてくる文字列データの保存領域
 - データが送られてくる前に領域確保
 - 必要以上に確保→性能劣化
 - 必要量に不足 →通信エラー
- 保存領域を超過したデータを未チェックで受信
 - バッファオーバーフロー
- データを送るふりをする
 - DoS (Denial of Service)を誘発
- 不要になった領域の解放忘れ
 - メモリリーク

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

21 21

プロトコルの脆弱性は厄介

- 一度プロトコルが普及すると修正困難
 - 既に出回っているアプリケーションの改修
 - 変更による影響の調査
- 情勢にあわせてプロトコルの拡張
 - 拡張による影響の調査
 - 組合せ(旧-旧,旧-新,新-新)の増加→調査不足

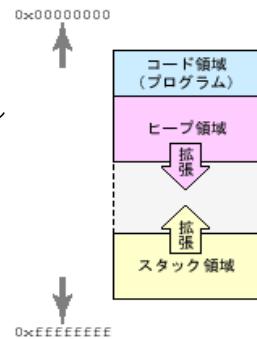
Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

22 22

バッファへの攻撃

- 必要以上に確保させる
 - 性能劣化
 - DoS攻撃
 - 例: 団体予約の当日キャンセル
- 必要量に不足
 - 通信エラー
 - バッファオーバーラン



Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

23 23

バッファオーバーラン

- 変数領域よりも大きなデータを読み込ませる
 - スタック上のリターンアドレスを書き換え
 - 別関数へ

```
12 int main()
13 {
14     char linebuf[1024];
15     FILE *fp;
16     long mark1 = 0x11111111;
17
18     vuln(linebuf);
19
20     void vuln(const char* line)
21     {
22         char msg[20];
23         long mark2 = 0x22222222;
24     }
25 }
```

画像出典: http://www.irasutoya.com/2015/06/blog-post_972.html

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

24 24

バッファオーバーラン防止方法

- 入力値のチェック
 - 最大長を超えるデータを棄却
- バッファ書き換えチェック
 - 変数間にチェックデータを挿入
 - これが書き換えられていたら異常と判断
- スタック上でのコード実行の禁止
 - NXビット(No eXecute)
 - 関数コードの投入を禁止
- コード配置アドレスのランダム化



Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

25 25

インジェクション

- ・入力データに命令を紛れ込ませる攻撃
 - SQLインジェクション攻撃
 - ・意図しないデータベース操作を実行させる
 - XSS(クロスサイトスクリプティング攻撃)
 - ・意図しないWebコンテンツを表示させる
 - ・意図しないJavaScriptを実行させる

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

26 26

例:ロボット制御のプログラム

- ・「右に□コマ進め」
 - □には何マス分右に進むかを入力
- ・普通の人:□に3を入力→「右に3コマ進め」
- ・攻撃者は□にこう入力する:
3コマ進め」「下に4
→結果:「右に3コマ進め」「下に4コマ進め」

入力チェックが甘いと命令を自由に実行できてしまう

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

27 27

サニタイジング(無害化)

- ・例:「右に3コマ進め」「下に4コマ進め」

1. 入力中の「」は無視する

- 結果:「右に3コマ進め下に4コマ進め」

2. 元からあった「」と入力中の「」を区別

- 結果:「右に3コマ進め』『下に4コマ進め」



検査項目:データの最大長,特殊文字,
文字コード,書式,etc

出典 http://www.irasutoya.com/2017/04/blog-post_544.html

出典 http://www.irasutoya.com/2014/11/blog-post_736.html

28

28

クロスサイトスクリプティング (XSS)

- ・例:Web掲示板

- 投稿された文字列をそのまま表示

入力:ども

A:ども

- この文字列にHTMLタグが入っていた場合

・タグで文字に色をつけられる

入力:ども

A:ども

・<script>タグで好きなJavaScriptを実行できる(危険!)

- 危険な入力:

<a href = “javascript:void(window.open(
'http://www.example.com',
'foo'))”>abc

特定のWebページが勝手に開かれる

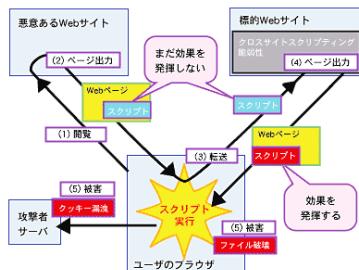
Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

29 29

強制ページ表示の何がまずい?

- ・「ウイルス感染」ページへの強制誘導
 - ページを表示しただけで感染



出典 https://www.ipa.go.jp/security/awareness/vendor/programmingv1/a01_02.html

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

30

防御手段

- ・パーソナルファイアウォール

- 省略(後の回で取り上げる)

- ・ユーザ認証

- 本人確認の仕組み

- ・アクセス制御

- 許可したことしかさせない仕組み

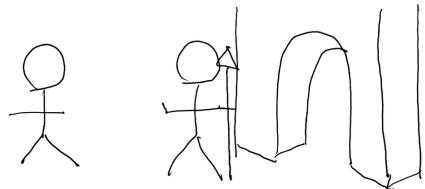
Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

31 31

ユーザ認証

- 正当な利用者であることの確認



Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

32 32

4) さまざまな認証方式

- 本人しか知らない情報を入力
 - パスワード
- 本人固有の持ち物を使用
 - トークン(ワンタイムパスワード生成装置)
 - スマートカード等
- 本人の身体的特徴で識別
 - バイオメトリック認証(指紋、顔など)

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

33 33

1. アカウント、ID、パスワード

- 1) パスワードの重要性
- 2) パスワードクラッキング
- 3) パスワードを保護するための対策
- 4) さまざまな認証方式

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

34 34

1) パスワードの重要性

- ID: ユーザが誰であるかを識別
- パスワード: 本人であることを確認
- 大原則「パスワードは本人しか知らない」
- パスワードが漏えいした瞬間から、システムやネットワークが脅威にさらされる
- パスワードは、ユーザが思っている以上に重要なもの

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

35 35

2) パスワードクラッキング

- パスワードクラッキングの種類
 - 本人から入手(ソーシャルエンジニアリング)
 - パスワードを推測
 - パスワードファイルを解析する(不正なツールを使用)
 - 辞書攻撃、ブルートフォース攻撃など
 - 盗聴する

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

36 36

ソーシャルエンジニアリング

- 人間心理や社会の盲点を突いて情報入手
 - 言葉巧みにパスワードを聞き出す
 - 廃棄物から重要情報を読みとる
 - 社員になりすまして盗み見や盗み聞きをする



Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

37 37

パスワードクラックのコスト

- パスワードの総数

桁数	総組合せ
数字4桁	1万
数字8桁	1億
英数字(26*2+10) 8文字	約200兆

- 攻撃速度

攻撃手法	所要時間
辞書攻撃	100万語 × 1μs/回 = 1秒 (100万語+数字4桁) × 1μs = 10000秒 < 3時間
総当たり(ブルートフォース)	200兆 × 1μs/回 = 約6.3年 100台で並列化→約23日 10000台で並列化→約5.5時間 百万台で並列化→約3分

Nov

38

39

Unixのパスワードファイル例

- /etc/shadow
 - ユーザ名の後ろにあるのがパスワードハッシュ
 - 入力パスワード文字列のハッシュ値と比較
 - /etc/shadowの内容と一致すれば認証成功

```
root:$1$29Ep0BC$m051yEGCj.xaf5x1W6TTU8:0:0:0:Charlie &:/root:/bin/csh
root:*:0:0:0:Bourne-again Superuser:/root:/bin/sh
daemon:*:1:1:0:0:The devil himself:/sbin/nologin
operator:*:2:5:0:0:System &/usr/guest/operator:/sbin/nologin
bin:*:3:7:0:0:Binaries Commands and Source:/sbin/nologin
games:*:7:13:0:0:& pseudo-user:/usr/games:/sbin/nologin
postfix:*:12:12:0:0:& pseudo-user:/var/spool/postfix:/sbin/nologin
named:*:14:14:0:0:& pseudo-user:/var/chroot/named:/sbin/nologin
ntp:*:15:15:0:0:& pseudo-user:/var/chroot/ntp:/sbin/nologin
sshd:*:16:16:0:0:& pseudo-user:/var/chroot/sshd:/sbin/nologin
_pflogd:*:18:18:0:0:& pseudo-user:/var/chroot/pflogd:/sbin/nologin
```

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

40

41

パスワードは定期変更すべき?

- 「その方が安全」と思っていたが…
 - 期待: パスワードがばれても新パスワードは無事
 - 実際: 思ったほど効果なし

「あなたのパスワードは半年間変更されていません。すぐに変更してください」
「えー、すぐにメール送らないといけないのに…」
「前のパスワードの後ろに123つけとこ」
「過去のパスワードによく似ているものは使えません。再入力してください。」
「前のパスワードの後ろに123123つけとこ」
「パスワードの変更が完了しました。」

さてこの新パスワードは安全か?

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

42

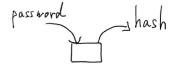
43

パスワードの保存形式

- 平文(原文)をそのまま保存するのは論外
- ハッシュ値を保存
 - 一方向関数($f^1(x)$ の計算が困難な関数)を使用
 - 攻撃耐性のあるハッシュ関数を使うこと
 - MD5関数はもう使わないこと(攻撃法が既知)

- ハッシュ値の例

- 平文:kumamon
- md5: 4832912896b858d84628d9ca04fc4b0
- sha256: 5bb6b2c15630635b72d317a7d724c5715d690a116fe52d1a022d1a7dc0f1b438



Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

39

3) パスワードを保護するための対策

- 強度が高い(推測しにくい)パスワードを使用する
 - 長くする、生年月日・電話番号・愛称などは避ける
 - 大文字・小文字・数字・記号を組み合わせる
- パスワードは適切に保管・利用する
- 絶対に人に教えない
 - 管理者などから問われることはない
 - アカウントの貸し借りはしない
- パスワードの使い回しをしない

例: パスフレーズによる設計(好きなフレーズをもとに変換)
パスフレーズ「JINSERIROIRO」 → パスワード「J#NS2R&R」
母音を抜き記号や数字を挿入

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

41

調査報告

- 機械的なルールで修正されたパスワードは推測可能
 - Time to rethink mandatory password changes
 - <https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes>
- 報告内容(2009)
 - 10,000人の被験者に三ヶ月毎のパスワード変更依頼
 - 典型的な「文字置き換えルール」が使われていた
 - 数字を増やす(11→12),似た文字へ置き換え(S→\$)
 - 特殊文字の追加/削除(!!→!!), 文字の入替(u4→u4)
 - 置き換えルールを使って新パスワードを推測
 - 旧パスワードが分かったユーザの17%で成功
 - 旧パスワードハッシュへの攻撃
 - 数ヶ月かけて6割のパスワード解読成功

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

43

トークン・スマートカード

- RSA社SecureID
 - 60秒毎に異なるパスワードを生成
 - サーバ側でも同様の装置がある
 - PIN番号をつけて送付
 - 物理的盗難時の対策
- USBトークン
 - USBキーデバイス
 - 読出し専用
 - パスワードやデジタル証明書入り



Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

44 44

バイオメトリクス認証

- 指紋や眼球奥の虹彩、声紋、静脈パターン等
 - 他人に譲渡できない
 - パスワードのような忘却はない
- アナログ処理なので精度の問題がある
 - FRR:本人拒否率(False Rejection Rate)
 - FAR:他人受入率(False Acceptance Rate)
 - 導入基準: 誤り率(FRR)が1/1,000以下
- 他の認証方式との併用を推奨
 - なしすましの可能性があるため(後述)

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

45 45

バイオメトリクス認証の問題

- **生体情報が流出した場合に取替え不可能**
- チェック方法によっては人工物を排除できず
 - 指摘(松本 勉教授@横浜国立大学)
 - グミによる指紋(なりすまし成功)
 - カラープリンタによる虹彩(なりすまし成功)
 - 大根による静脈パターン



参考 Nov 25, 2022

<http://itpro.nikkeibp.co.jp/free/NC/NEWS/20050701/163801/>

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

46 46

多要素認証

- セキュリティレベルに応じて複数方式で認証
 - 例

要求レベル	認証方式
1	パスワード認証 or トークン
2	パスワード認証 and トークン
3	パスワード認証 and トークン and 生体認証

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

47 47

リスクベース認証

- 高リスクと判定されたアクセスには追加認証
 - 高リスクの判定基準
 - いつもと違う端末からのアクセス
 - いつもと違う場所からのアクセス
 - いつもと違うブラウザからのアクセス,等々
 - 追加認証
 - 暗号トークンの入力
 - 「秘密の質問」
 - SMSコード入力,etc

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

48 48

推奨ルール

- 十分な長さを持った安全なパスワードを使う
- パスワード漏洩が危惧されたら即変更
 - 旧パスワードとは全く別のパスワードにする
- 重要なサービスは多要素認証を設定
- パスワードマネージャを使う方法もある
 - パスワードはランダムに生成
 - パスワード管理はソフトに任せる
 - 管理ソフト起動用のパスワードだけ守る

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

50 50

アクセス制御

- 認可の実現に必要
 - 誰に何の情報へのアクセスを許すか
 - 誰に何の操作を許すか
 - 権限の管理
- 認証は「誰であるか」の確認だけ
 - 認証と認可の両方が機能して意味がある

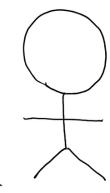
Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

51 51

マルチユーザOS

- ユーザ(グループ)毎に権限を管理
 - 特権ユーザー
 - ・システムに関する全ての操作が行える
 - ・root(UNIX系OS), Administrator(Windows)
 - 一般ユーザー
 - ・システム本体・他ユーザーに危害を加えないよう操作を制限
 - 自分用の設定しか変更できない
 - 自分が起動したプログラムしか操作できない
 - 自分が所有するファイルしか変更できない
 - 他の人のデータ・プログラムは操作できない
 - » 他の人のフォルダ・ディレクトリ内にファイルを作れない
 - » 他の人の実行したプログラムを操作できない



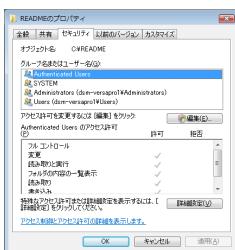
Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

52 52

ファイルのアクセス制御

- ファイルやディレクトリ毎に権限を設定
 - ユーザ別、グループ別に権限を設定
 - read/write/exec/modify/append,etc



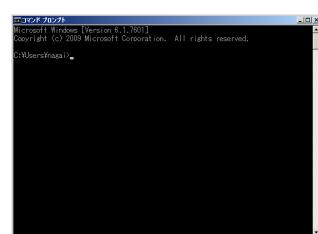
53 53

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

プログラムの実行制御

- 特定のユーザ/グループにだけ実行を許可
 - 例:コマンドプロンプト
 - OSのコマンドを色々実行できてしまう→利用を制限



Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

54 54

特権ユーザーの役割

- システムの保守・管理作業用
 - 設定ファイルの変更
 - アプリケーションのインストールなど
- 保守・管理作業が必要な時だけ利用
 - 普段は一般ユーザーとしてシステム利用
 - 特権ユーザーのまま添付ファイルを開くと危険



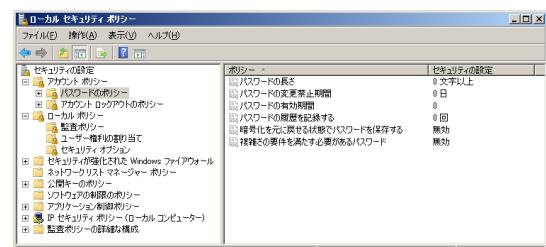
Nov 25, 2022

京者 :情報倫理 (2022年度)

55 55

Windowsの権限管理

- セキュリティポリシーで細かく設定可能



Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

56 56

Windowsの問題点

- 高機能、複雑なので手に負えない
- 管理者権限が必要なアプリケーションが多い
 - 過去の資産(後方互換性 バックワードコンパチビリティ)
- ものぐさな運用形態がよく見られる
 - 全利用者に管理者権限を与えてしまう
 - Active Directoryを使えば権限の集中管理可能
 - 個人利用端末だと一般ユーザが管理者
 - メーカー出荷状態のまま利用
 - 不用意な操作でシステム全体に影響

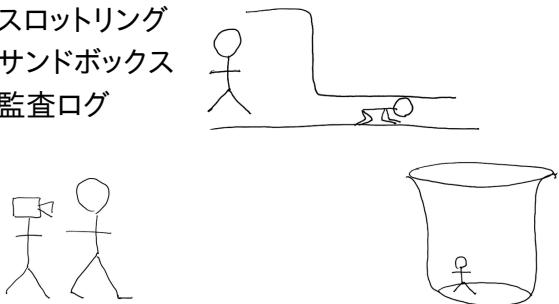
Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

57 57

被害の拡大防止手段

- スロットリング
- サンドボックス
- 監査ログ



Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

58 58

スロットリング(レート制限)

- 攻撃回数を増やせないようにする
 - パスワードを複数回間違ったらロックする
 - 一回の試行で、失敗時には待ち時間を入れる
- 推奨基準
 - 30日で100回の認証失敗しか試行できないよう制限
 - 平たく言えば「1日に3回までの失敗を許す」

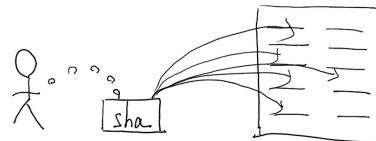
Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

59 59

スロットリングだけでは不十分

- オフライン攻撃
 - パスワードハッシュとパスワード候補を照合
- 逆ブルートフォース攻撃
 - ANAのアカウント乗っ取り事例(後述)



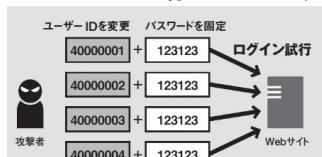
Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

60 60

ANAの事例(2014)

- 出典:危なすぎる数字だけのパスワード、JALとANAがユーザー認証を強化
 - 仕様: Web会員のパスワードは数字4桁/数字6桁
 - 逆ブルートフォース攻撃が成立
 - 分散アクセスされると正規のアクセスと区別できない



Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

61 61

ストレッ칭ング

- パスワードハッシュの計算を繰り返す
 - 通常
 - hash = sha(password)
 - ストレッ칭ング
 - hash = sha(sh(a(sh(...(password)...)))
 - 1,000～10,000回程度繰り返しハッシュ計算した値を使用
- メリット
 - オフライン攻撃に要する時間が増える



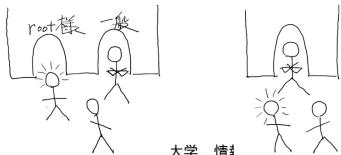
Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

62 62

セキュアOS

- 問題:特権ユーザは強力すぎる
 - rootユーザはアクセス権限チェックが適用されない
 - 全てのファイルを読み書き可能
 - 便利だが乗っ取られた時の危険性が高い
- 解決策:強制アクセス制御
 - 特権ユーザにもアクセス制御をもれなく適用



Nov 25, 2022

大学 情報セキュリティと情報倫理 (2022年度)

63 63

セキュアOS(続き)

- 問題:特権ユーザプロセスは強力すぎる
 - root権限のプロセスはシステムの全ての機能を利用できる
 - 動作中のプログラムが乗っ取られると危険
- 解決策:サンドボックス(最少特権環境)
 - 必要最小限のことしかできない状態でプログラムを実行
 - アクセスできるファイルの限定
 - 通信できるポートの限定



Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

64 64

監査ログ

- 事前調査段階での不正侵入検知
- 侵入された際の被害範囲の特定
- 監査ログは別ホスト・外部媒体で保全
 - ログ自体が改ざん・消去されることも
 - 侵入されたホストのログは信用できない



Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

65 65

ハッカーとセキュリティ

クラッキングとは

- ハッカー (hacker)
 - 非常によく出来た洗練されたプログラムを書く
 - コンピュータの巨匠ともいえる(昔は...)
 - 知的なチャレンジ→エスカレート
- クラッカー (cracker)
 - 卑劣な心を持つハッカー?
 - 盗みや損害を与えるため、権限なくコンピュータシステムに侵入する者?
 - 最近は、金銭目的化

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

67 67

ハクティビズム

- 政治的主張を伴うハッキング(クラッキング)
 - hack(ハック):「合理的で創造的な行為」
 - hacktivism = hack + activism

活動区分	通称	例
法遵守的	ポリティカルコーディング	暗号通信用ソフト開発 P2P通信ソフト開発
法侵犯的	ポリティカルクラッキング	外交機密の暴露 特定団体Webの攻撃

参考 <http://credo.asia/2014/03/22/hacktivism/>

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

68 68

自動車のハッキング

- Charlie Miller&Chris Valasek(セキュリティ専門家)

- [Jeep](#) チェロキーの遠隔操作に成功(2015.7)
 - ・エンジン、ステアリング、ワイヤー
 - [Black Hat USA 2015: ジープのハッキングの全容が明らかに](#)
 - [技術報告書](#)

- 対象車種140万台リコール
 - ソフトウェアのアップデート



<http://www.blogcdn.com/www.autoblog.com/media/2013/02/2014-jeep-cherokee-1.jpg>

Nov 25, 2022

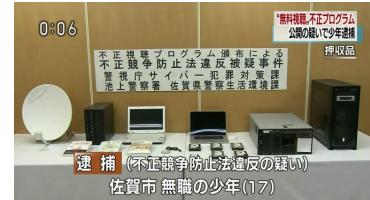
京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

69 69

地上波デジタル放送視聴用ソフト

- デジタル暗号放送の視聴ソフト

- 技術詳細は非公開なのに何故かネット上に掲載
 - この少年はそれを元に地上波デジタル用に改造
 - **B-CASカード無しで無料チャンネルを視聴できる**



Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

70 70

クラッキングの重大性

- 貧弱なセキュリティがある限り問題である.
- CERT(The Computer Emergency Response Team)
 - JPCERT/CC (<http://www.jpcert.or.jp/>)
 - インターネットのセキュリティ問題への対処
 - 情報収集と広報
- 多くの不正侵入は報告されないことが多い
 - 恥の文化(?), 過度の信頼性低下(株価低下?)
 - クラック行為の助長, 信頼性の低下 ...
- Morrisワーム(1988年)
 - インターネットの全システムの10%を停止に
 - 簡単に防げる脆弱性が放置されていることを実証

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

71 71

悪意なきハッキング

- 「権限のないコンピュータシステムへのアクセス」に対する(自称無害)のハッカーの主張
 - 損害は発生していない. 無害なレクリエーションであり, 知的な挑戦だ
 - ・管理者からみれば侵入者の意図・活動内容は不明確
 - ・システムのセキュリティの弱点を明示している
 - ・よいセキュリティがないからいけない
 - 弱点をついて弱点を明らかにすることは恩恵か?
 - 情報をコピーする行為は盗みでは無い
 - プライバシー, 知的財産権
 - 通信会社は儲けすぎだから, 少々のただ乗りは問題ない
 - 泥棒は泥棒

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

72 72

Chaos Computer Club



- 目標:あらゆるコンピュータや技術的なインフラへの自由なアクセスを守ること
 - 記事: [セキュリティの欠陥を暴く](#)
- 活動事例
 - 銀行のシステムに侵入し、13万マルク引出し
 - 翌日、返金
 - iPhone 5sのTouchID(指紋認証)の回避

Nov 25, 2022 画像出典: https://commons.wikimedia.org/wiki/File:25C3_Pesth%C3%B6rnchen.jpg

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

機密保持によるセキュリティの維持

- 脆弱性情報をクラッカーから隔離すればよい?
 - 「脆弱性」は現に存在している
 - 情報は暴かれてしまう可能性がある
- 機密保持を考えることは無意味では無い
 - 少なくとも時間稼ぎにはなる
- 倫理的な問題
 - 放置されている脆弱性は知らせるべきか?
 - 放っておけば大勢の被害者, 公開すれば格好の餌食
- **現在の業界ルール**
 - **脆弱性を見つけたらCERTに報告**
 - 開発元が**脆弱性を解決した後に脆弱性を公開**

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

74 74

セキュリティの改善

- セキュリティの確保を主たる設計目標にする
 - (技術面の)安全性を確保する技術はある
 - ex. Firewall, IDS, IPS, 暗号化, 電子署名
- 公開性と容易性 vs. セキュリティ
- 完全なる防衛は存在しない
- ユーザへの教育
 - よいパスワード管理手法
 - 他者に推測されにくく自分では覚えられる長いもの
 - パスワードマネージャの利用

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

75 75

法律による線引き(日本)

- コンピュータへの無権限アクセス
 - 「違法」と明文化されています
 - 悪意の有無は問わない
- 危害を与える恐れのあるプログラムの作成
 - いわゆる「コンピュータウイルス作成罪」
 - 不正指令電磁的記録作成・提供罪として規程
 - 「正当な理由無く」作成・配付すると有罪

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

76 76

セキュリティはなぜ脆弱なのか

- 歴史的原因
 - インターネットは研究者の通信手段としてスタート
 - 自由なアクセス, 利用の利便性, 情報共有の容易性
- 技術的原因
 - 複雑系ゆえの予測困難
 - 常に何らかの誤りはある
 - ネットワーク接続, 利用に必要なスキルの低下
 - より多くの個人情報, 重要情報の蓄積
- 人的原因
 - 快適さの追及、ヒューマンエラー
 - 知的好奇心、自己顕示欲、金銭欲、思想信条、etc.
 - 重大な問題が発生するまで対策をしないことが多い

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

77 77

まとめ

- 脆弱性
- 防御の考え方
 - 最少権限の原則, サニタイジング
 - 代表的な防御手段
- ハッカーとクラッカー

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

78 78

ミニレポート

- Moodle に掲載
- 提出期限: 次回講義開始時

Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

79 79

参考資料

- 情報セキュリティ読本 教育用プレゼン資料
 - <https://www.ipa.go.jp/security/publications/dokuhon/ppt.html>
- SELinuxシステム管理
 - オライリージャパン, ISBN:978-4873112251
- 情報セキュリティプロフェッショナル教科書
 - アスキードットメディアワークス
 - ISBN: 978-4048677820



Nov 25, 2022

京都工芸繊維大学 情報セキュリティと情報倫理 (2022年度)

80 80

参考資料

- DRAFT NIST Special Publication 800-63B
Digital Authentication Guideline (翻訳版)
 - <https://openid-foundation-japan.github.io/800-63-3/sp800-63b.ja.html>
- セキュアOS「LIDS」入門(6)
 - <http://www.atmarkit.co.jp/fsecurity/rensai/lids06/lids01.html>
- OS環境の要塞化とセキュアOS
 - <https://enterprisezine.jp/iti/detail/3806>