第13章
セキュリティと信頼性

花田　英輔
（このPowerPointは渡辺名誉教授作成のものを花田が一部改編した）

1

コンピュータシステムの安全性への脅威
(教科書13.1)

- 天災：地震、洪水、、
- 人災：テロ、暴動、、
- 建物への不正侵入
- 停電
- 空調不具合
- ハードウェア障害
- ソフトウェア不良
- 操作ミス
- ネットワーク盗聴
- 不正アクセス
- 不正プログラム：ウイルスなど
- 不正ネットワークトラフィック：大量パケット送付

本章では、OSレベルでの対策

より広い対策
⇒戸締り、
電源・空調の多重化、
人的体制、
運用規則整備など

2

安全性に関する特性(教科書13.2)

- 信頼性(Reliability)
  - システムが故障せずに動く特性（正しく機能する、広い概念）
- 可用性(Availability)
  - システムが機能を維持し続ける特性（停止時間が短い）
- 完全性(Integrity)
  - システムに欠陥が無く、機能が意図通りに動く特性（間違いが無い）
- セキュリティ(Security)
  - 故意によるシステムの安全性への脅威への対処
  - 三つの特性⇒機密性、可用性、完全性
    - システムの性能評価(第15章)では「保守性」(Serviceability)を加えてRASISと称する

3

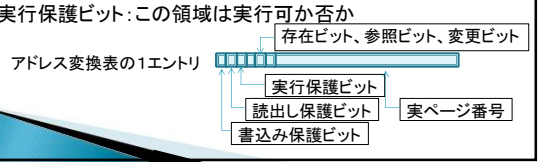
セキュリティの三要素

- セキュリティの三つの要素
  - 機密性(Confidentiality)
    - アクセスを許可された者だけが、情報にアクセスできることを確実にすること（漏れないこと）
  - 完全性(Integrity)
    - 情報及び処理方法が正確であること、および完全であることを保護すること（壊れないこと）
  - 可用性(Availablity)
    - 認可された利用者が、必要な時に、情報及び関連する資産にアクセスできることが確実になっている特性（使えること）

4

記憶保護(教科書13.3)

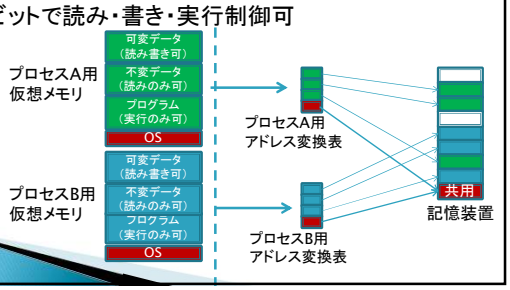
- メモリアクセスを制限
  - OSの領域を応用プログラムからアクセスさせない。
  - プロセスの領域を別プロセスからアクセスさせない。
  - プログラム部分や不変データ部分は変更できない。
- 記憶保護機構（ハードウェア）
  - アドレス変換表のエントリごとにビット付加、アクセス時にチェック
    - 書込み保護ビット：この領域は書込み可か否か
    - 読出し保護ビット：この領域は読出し可か否か
    - 実行保護ビット：この領域は実行可か否か



5

仮想空間の壁による記憶保護

- アドレス変換表にある領域以外はアクセス不可
- 両方の変換表に登録すれば両方からアクセス可能
  - 共用データ領域やOS領域など
  - 保護ビットで読み・書き・実行制御可



6

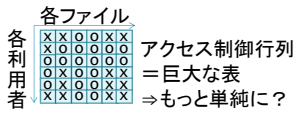
実行モード

- システム全体に影響ある命令（入出力命令等）は非特権モードで使用不可
  - 特権モード(カーネルモード)
    - 全ての命令が実行可能なモード：OSカーネル実行時
  - 非特権モード（ユーザモード）
    - 特権命令は使えないモード：応用プログラム実行時
- 特権モードへの切り替えも保護
  - 非特権から特権への切替え命令は無い（割込みと同時に特権へ）
- 割込み処理プログラムも保護
  - OSの存在する領域を記憶保護

7

ファイル保護(教科書13.4)

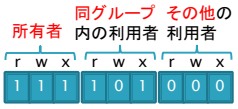
- ファイルの所有者
  - ファイル・ディレクトリを作成した者
  - そのファイル・ディレクトリに対する他人のアクセスを制限可
  - ただしシステム管理者⇒全ファイル・ディレクトリをアクセス可
    - アドミニストレータ（Windows）、ルートユーザ(UNIX)等と呼ぶ
- ファイル保護
  - 読出し許可：その利用者は、そのファイルを読めるか
  - 書込み許可：その利用者は、そのファイルを書けるか
  - 実行許可：その利用者は、そのファイルを実行できるか



8

UNIXのファイル保護

- ファイルごとに9ビットの情報を保持
  - iノード（ファイルインデックス保存領域）に



例：

```
- rwx --- --- ：自分だけ読み・書き・実行可　700(111 000 000)
- rwx r-x --- ：上記＋グループメンバは読み・実行可 750(111 101 000)
- r-x r-x r-x ：誰でも読み・実行可 555(101 101 101)
```

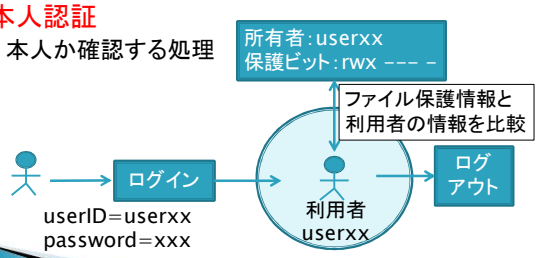
設定変更コマンド(UNIX) chmod

```
chmod 700 file1 :file1を自分だけ読み書き実行可能に
chmod g+x file1 :file1にgroup executeを付加
chown userxx file1 :file1の所有者をuserxxに変更
```

9

利用者の認証(教科書13.5)

- セキュリティ確保には利用者を限定
  - 利用者ID（アカウント名）を付与
  - 利用者の管理もOSの仕事
- 本人認証
  - 本人か確認する処理



10

本人認証

- 利用者が提示されたIDで表される本人かを確認すること
- 主な方法
  - 本人だけが知っている情報で＝パスワードなど
  - 本人だけが持っている物で＝IDカードなど
  - 本人だけの身体的特徴で＝指紋など（バイオメトリック認証）

11

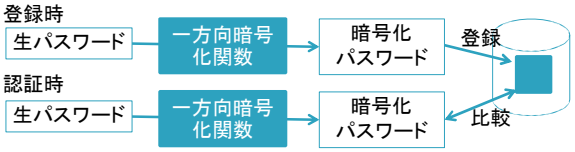
本人認証

- パスワード⇒多く利用
  - 特別な装置が不要で手軽
- カード＋パスワードの組み合わせ等も（銀行ATM等）
- 本人認証以外にも
  - サーバ認証＝接続先のサーバは本物か？
  - クライアント認証＝接続してきたクライアントは本物か？
  - これら実現にはSSL等の仕組みがある

12

パスワードの保護

- OS側の処置
  - 何度か誤ったら失敗として打ち切る
  - 裸のパスワードをシステム内に持たない
    - 必ず暗号化して持っている



13

パスワードの保護

- 利用者側がすべき処置
  - 他人から類推されないものにする
  - 英字、数字、特殊記号を含めた、長いものにする
    - 通常は8文字以上
  - 辞書上の単語やその組合せ、規則性文字列は避ける
    - 総当たり攻撃に耐えうるものに
  - 他人に教えない。自分では忘れない
  - インターネットを介して裸のパスワードを送らない＝暗号化送信手順を
  - 使いまわしをしない＝異なるシステムで同じパスワードを使わない（特に金銭が絡む場合）

14

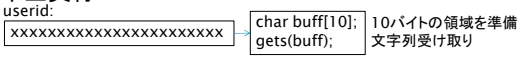
ネットワークセキュリティ(教科書13.6)

- インターネット接続の普及に伴い、重要な課題に
  - 不正アクセス
  - 不正プログラム
  - 盗聴
  - その他、多様なトラブル
- 詳細は別講義で

15

不正アクセス

- 利用の権限が無いシステムの利用
  - パスワード不正取得やソフトウェアのバグ利用等で侵入
  - 情報漏洩、システム破壊、他システム攻撃拠点等に利用
  - セキュリティホール（Security Hole）
    ＝侵入に利用できるシステムの欠陥
    - バッファオーバーフロー　入力バッファ領域を溢れさせ不正実行



- 対策
  - パスワードが漏れない対策
  - バグの早期修正（パッチ、アップデートを適切に）

16

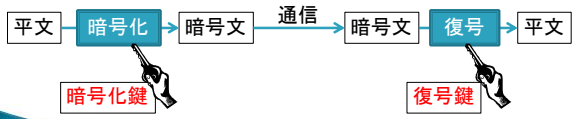
不正プログラム

- 利用者の意図しない振舞いをする、意図的に作成された悪質なプログラム
- 総称＝マルウェア（malware）
  - ウイルス＝感染機能・潜伏期能・発病機能を持つもの
  - キーロガー＝キーボード入力を記録
  - トロイの木馬＝有用プログラムの外見で悪意を含む
  - ワーム＝セキュリティホールを介して自動的に感染
  - ボット＝外部からの指令に従う常駐プログラム
    巨大なボットネットが存在、一斉攻撃等に使用
- 対策
  - ウイルス対策ソフトを導入
  - パッチ、アップデートを適切に
  - ファイル持ち込みを慎重に、メール添付は安易に開かない

17

盗聴

- インターネット⇒通信中のデータが盗聴可能
- 対策⇒暗号化通信
  - 共通鍵暗号方式＝暗号化・復号化に同一鍵
  - 公開鍵暗号方式＝互いに類推困難なペアの鍵
    暗号化の鍵は公開、復号の鍵は秘密
    計算負荷大⇒共通鍵の交換だけ公開鍵利用などの運用方法
    SSLなど



18

OSの信頼性、可用性機能(教科書13.7)

- 信頼性、可用性を向上するためのOS機能
  - 入出力エラー回復
    - 失敗したら何度か繰り返す
  - ファイルシステムのバックアップと回復
    - 全体または一部のコピーを取る・戻す
  - ジャーナリング
    - ファイル処理中の障害に対して復旧を容易にするような記録を残す管理手法
  - 二重化システム
    - 構成要素を二重化(電源、プロセッサ、ディスクなど)
  - 自動運転
    - 操作ミスの回避

19

第14章 システムの運用管理

20

運用管理(教科書14.1)

- 運用
  - 目的通りの機能を日々維持するために必要な業務の実施
- 運用管理
  - 運用のための管理業務
- 管理対象
  - 集中処理大型システム、部門別システム、個人用システム、、
  - ファイルサーバ、プリンタ、PC、ネットワーク、、
- 管理体制
  - 運用管理責任者＝責任を持つ人
  - 運用管理担当者＝実務を行う人
  - アウトソーシング＝運用管理を外部委託(責任範囲は契約で)

21

システムの規模と管理体制

- 組織の共通的処理を担うシステム
  例:総合情報基盤センターシステム⇒センター内に管理責任・管理担当
- 利用者部門の共用システム
  例:研究室共用サーバ⇒特定教員が管理責任、特定教員/学生が運用担当
- 各個人が扱うシステム
  例:個人PC⇒自分で責任、自分で運用

22

運用管理の内容

- 利用者管理
  - 利用者の登録・削除・パスワード管理、利用情報取得
- 構成管理
  - ハード・ソフトの構成設定・更新
- 障害管理
  - 障害予防、障害対処、バックアップ
- 稼動管理
  - 稼動統計、稼働率対策
- 性能管理
  - 所定の性能維持のための作業
- セキュリティ管理
  - セキュリティ維持のための作業
- ネットワーク管理
  - ネットワークについて、上記の管理

23

利用者管理(教科書14.2)

- 利用者と利用者グループ
  - システム管理者と一般利用者
  - システムによっては、特定権限を持つ利用者グループ設定も
- 利用者登録
  - システム管理者の仕事
  - 利用者ID、初期パスワード、所属グループ、その他設定
- 課金
  - システムによっては、使用状況によって課金
  - プロセッサ使用時間、メモリ使用量、ディスク使用量、印刷枚数
- 資源使用量の制限
  - 特定の利用者が過大に利用しないよう設定(時間制限、容量制限)
- システム利用ログ
  - 利用者がいつシステムを利用したかの記録
  - セキュリティ管理等に利用

24

構成管理(教科書14.3)

- ハードウェアの構成
  - ハードウェアの適正化、デバイスドライバの組み込み
- ネットワークの構成
  - ネットワークの適正化、アドレスの設定
- ファイルシステムの構成
  - ファイルシステムの適正化、どのディスクにどう割当て
- プログラムの構成
  - 新たなプログラムのインストール
  - 新たな版への更新作業、セキュリティパッチの適用

25

障害管理(教科書14.4)

- 障害の予防(事前)
  - ハードウェア障害ログによる早期発見:一時的エラーに注意
  - ファイルシステムのバックアップ:キチンと計画しないと無駄に
  - ソフトウェアの更新:バグ対策版への更新
  - 障害時の代替策:予備システム/多重化/手作業手順書
- 障害への対処(事後)
  - 障害状況の記録確保
  - システムの復旧:当面の業務が可能なように
  - ベンダに原因究明と対策を依頼
  - 本対策:機器・ソフトウェアの更新など

26

今回の課題

1. 情報システムの安全性に関する特性に以下の項目がある。それぞれ説明せよ。
   - 信頼性、可用性、セキュリティ、完全性
2. (予習)電子メール等で発生する「文字化け」が起きる原因を調べて記せ

- 今回のファイル名は"学籍番号-OS14.docx"
  (例:24238000-OS14.docx)としてください
- 締切:1月30日(金) 18:00 (遅れた場合は減点)
- 本講義に関する情報は(この講義資料も)次のWebpageに掲載するので、時々参照すること
  https://www.ai.is.saga-u.ac.jp/~hanada/OS/

27