最低限 Unix (Linux) I
～ Linux 入門 ～

情報実験 第 2 回 (2019/04/19)

北海道大学 大学院理学院
宇宙理学専攻 修士 2 年
吉田 哲治

目次

1. Linux とは

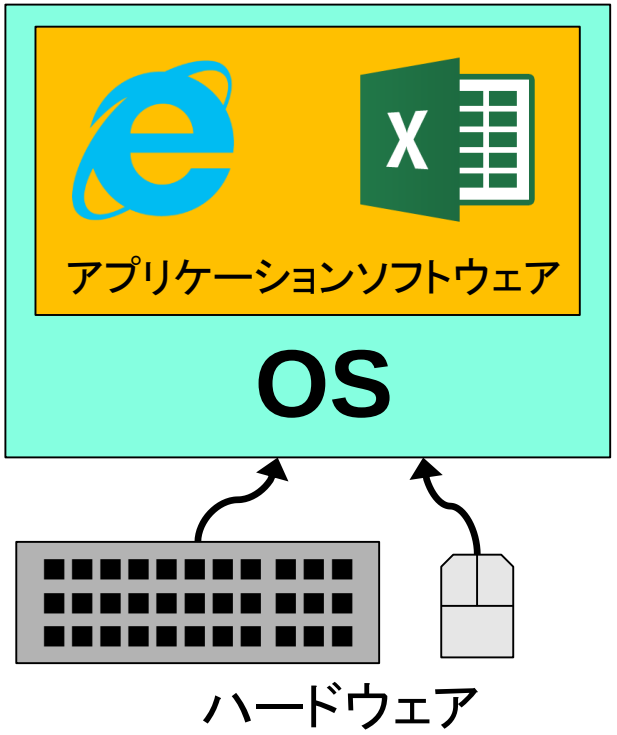
はじめに

- あなたの周り(家)のパソコンを思い浮かべてください
  そのパソコンで使っている OS は何でしょう?
  - Windows
  - macOS
  - Linux
  - iOS
  - Android
  - その他
- INEX では Linux を使います…

そもそも OS って何?

OS (Operating System)

- 計算機を管理・操作するための基本ソフトウェア
  - 詳しくは第 3 回参照
- アプリケーションソフトウェアとハードウェアとの仲介を行う
  - アプリケーションソフトウェアとは特定の目的の為に作られたソフトウェアのこと
    例 : Excel,
    Internet Explorer
    (Microsoft edge) など



Linux とは

- Linus Torvalds 氏が大学在学時に開発 (1991)
  - パソコンで動作するUnix-likeな自分専用のOSが欲しかったため
    - 当時 Unix を載せられる計算機は高額
    - 商用 Unix では著作権の関係上，改変が面倒

https://jp.linux.com/news/linuxcom-exclusive/441821-lco2016041801

- Linux の名称の由来
  - Linus + Unix = **Linux**
  - Linux Is Not UniX
  - 諸説あり

2. マルチユーザシステム

マルチユーザシステムとは

- 複数人が同時に計算機を利用できるよう設計されたシステム
  - 複数人で, 1 つの計算機を同時に使用したい
  - 複数人で，情報共有を可能にしたい

  現在でも大型計算機, Unix, Linuxでマルチユーザシステムを継承

安全かつ円滑に利用するために

- システムの利用にはいくつかの手続きと設定がある
  - 計算機を利用する前に, 使用権利の存否を審査する手続きが必要
    - アカウントシステム
  - ファイル・ディレクトリ利用に関する権限の設定
    - パーミッション (Permission)

3. アカウントとログイン

アカウントとは

- アカウント = 権利, または計算機利用者 (User)
  - ここでの権利は「計算機を使用するための権利」を指す
- アカウントの種類
  - **計算機管理者(**または, **root** あるいは**スーパーユーザ)**
    - 計算機内での最高権限者
    - 全権限を行使可能
      - 例：アカウントの新規作成/削除, システムに関わるファイルの編集
  - システムアカウント
    - 各種サービス(プログラム)を運用するアカウント
      - 例: daemon, www-data, など
    - ユーザが直接利用することはない
  - **一般ユーザ**
    - 計算機管理者とシステムアカウント以外のアカウント
    - 計算機の管理権限に制限
      - 例：シャットダウンすら不可能

計算機を利用するための事前準備

- 計算機を利用するためには, 事前にアカウントを計算機管理者 (root) に作成してもらう必要がある
- 作成に必要な情報 (アカウント情報)
  - **アカウント名**
  - **パスワード (認証用の合言葉)**
  - 氏名
  - 住所 等々…

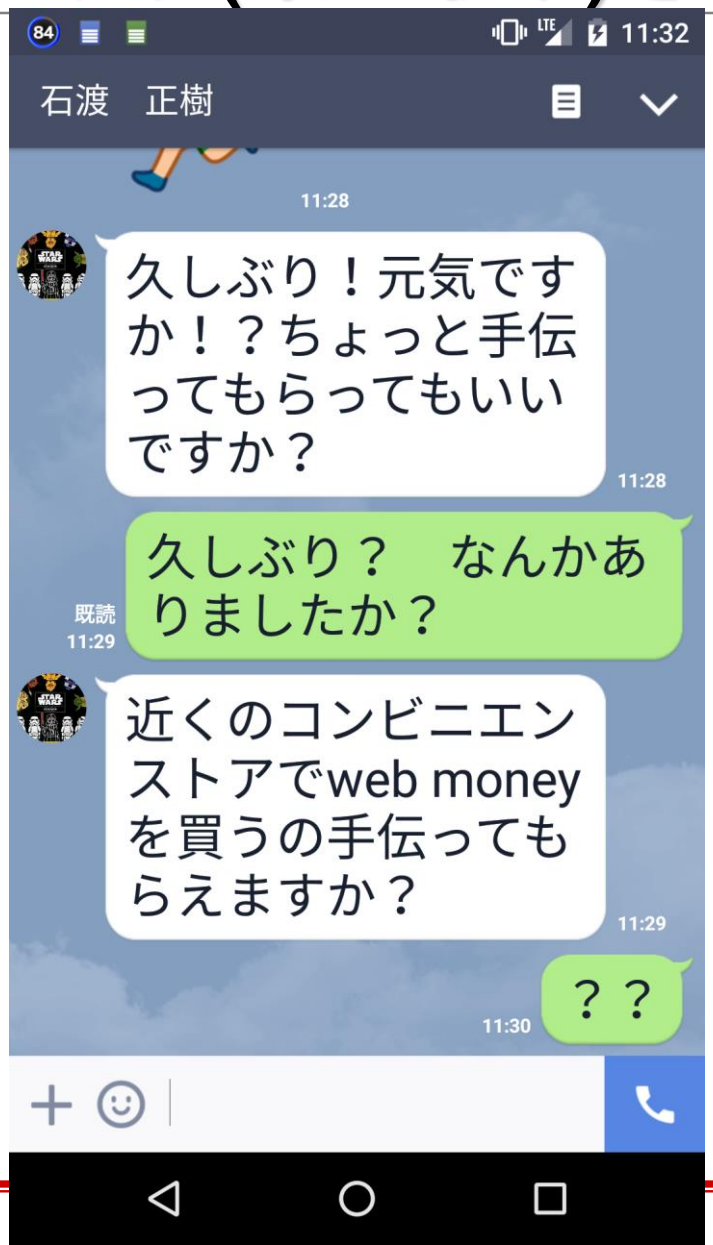
アカウント作成後,
計算機に**ログイン**できるようになる

ログインとは

- 事前に登録したアカウント情報を用いて，認証した後に, コマンド等を利用できる状態にすること
- 必要入力事項は「アカウント名」＋「パスワード」 のみ
- アカウントを持つ人は**パスワードを守る責務**がある
  - アカウントクラック (アカウント名＋パスワードを盗むこと) しようとする輩はあなたを常に狙っています！

4. アカウントクラックの手法と想定される問題

アカウントクラック(乗っ取り)された例



この乗っ取りはフィクションです.

アカウントクラック(乗っ取り)された例

この乗っ取りはマジです. 2018/03/23

S さんとのやりとり 1

S さんとのやりとり 2

その直後できたグループ

アカウントクラックの手法 1

- Social Attack (または Social Engineering)
  - ネットワークを介さず, 社会的手段 (話術・覗き見など)を用いて, 不正行為に必要な情報を得る行為
    - ユーザー名, パスワードを入力している様子を覗き見 (**ショルダーハッキング: Shoulder Hacking**)
    - 計算機管理者を装い, 電話などで利用者に問い合わせ, パスワードなどを取得
    - ゴミ箱に捨てられているメモ用紙などから情報を取得(**スキャベンジング** : Scavenging [ゴミ箱をあさる])

アカウントクラックの手法２

- Brute Force Attack (BFA, 総当たり攻撃)
  - 考えられる**全てのパスワード**を片端から試す
  - 解読に要する時間は**字数**に大きく依存
    - 一文字増えるごとに解析に要する時間は飛躍的に長くなる
- Dictionary Attack (DA, 辞書攻撃)
  - ありとあらゆる分野の単語を記録した**クラッキング用辞書**を使う
  - BFA より**極めて効率的**
    - 大文字，小文字，数字を組み合わせてクラックできる
      - 例：o →O(小文字を大文字に)，i → 1(英語を数字に)

クラックされた時の問題：本人編

- 自分のアカウント情報書き換え
  - パスワードが変更されれば**ログイン不可**
- データの盗難・破壊
  - 自分が蓄積した経験は水の泡に…
- 将来にわたっての継続的な不安
  - 盗み見られたデータに基づく恐喝
  - ネットワークへのデータ流出に伴う**半永久的な損害**
    - 一旦流出したら事実上回収は不可能

クラックされた時の問題：他ユーザ編

- 計算機の運用妨害
  - 高負荷処理によるサービス妨害
- 他のアカウントへの被害波及
  - いったんログインできればあとは比較的簡単
  - **ルートクラックされる ≒ 計算機の運用停止**

ルートクラックの恐ろしさ

- 計算機の全情報が自由に操作される
  - 計算機管理者は最高権限者なので計算機の**全情報を閲覧できる・変更できる・消去できる**
- 一度でもルートクラックされると…
  1. クラッカー達の鴨リストに載り, その計算機の情報はすぐに**ネットワークを通じて拡散する**
  2. 容易に暴けるクラック対象として世界中から**集中攻撃を受ける**ようになる
  3. **頻繁に**クラックされるようになる
  4. 計算機の**運用停止**に追い込まれる
     (こうして joho21 は…)

クラックされた時の問題：世界編

- クラッカーによるネットワーク内の他の計算機へ侵入
  - 「自分の手」を汚さずに**「内側」から**クラック
    - インターネットを通じて, さらに大規模なクラックを行うための**踏み台**として悪用
    - クラックした複数の計算機を, **さらなるクラックのための高速計算**に転用
    - 多数の計算機を使っての**大規模なサービス妨害**
- **犯罪等への加担**
  - 時には国際問題にも発展
    - http://map.norsecorp.com/#/
- ネットワークにつながった計算機 = **凶器**になりうる

このような問題を
起こさないためにも
アカウントを持つ人は
良いパスワードをつけて
計算機を守る義務がある

5. 良いパスワードを付ける

良いパスワードとは

- なによりも**頑丈** (破られにくい)
- 他者にとっての**使いにくさ** (予想しにくい)
- 自分にとっての**使いやすさ** (憶えやすい)

頑丈なパスワードとは

- 最低でも **10文字** 以上並べる
  - 今の Debian は最大で 512 文字まで設定できる
- 可能な範囲で異なる文字・数字・記号を使う
  - **大文字**, 小文字, 数字, **記号**
  - ! # $ % & @ … など

他者の使いにくいパスワードとは

- 推定しやすい文字列 を用いない
  - 辞書にある単語
  - 個人情報から推定できる言葉
- 簡単な規則のみで置き換えた文字列を用いない
  - 繰り返し　　(dictionarydictionary)
  - 逆つづり　　(yranoitcid)
  - 小文字→大文字 (YranoItcid)
  - 小文字→数字　(yran01tc1d)

パスワード例

- 悪いパスワード
  - アカウント名と同じパスワード(絶対にやめてください)
  - 単語・固有名詞・個人情報から推定できるもの
    - Flower, hokudai, sapporo, 19900709 …
  - 専門用語
    - Pneumonoultramicroscopicsilicovolcanoconiosis (火山塵肺症)
- 良さそうなパスワード
  - 「おしりを出した子 一等賞」を元につくる
    - oshiri wo dashita ko ittousyou
      -> osrwdstkits -> 0sRw#d$tk&1Ts

もちろんこのパスワードは既に良いパスワードではない

パスワードに関する注意

- 他人がパスワード打鍵している時は, **視線を逸らす**
  - ショルダーハッキングされていると相手に無用な不安を与えないため
- 初期パスワードは迅速にログインした上で変更する
- 情報学 I でも学んだように…
  - パスワードは誰にも教えない
  - パスワードはメモしない (方がいい)
    - やむを得ずメモする場合は

      パスワードとわかるようなメモをしない
  - 同じパスワードを使いまわさない

前編まとめ 1

- Linux とは
  - OS のひとつ
  - フリーソフトウェア（オープンソース）
  - 基本的に無保証
- マルチユーザシステム
  - 複数人が同時に計算機を利用できるよう設計されたシステム
- アカウントとログイン
  - アカウント : 計算機を使用する権利または, その利用者
  - ログイン　: アカウント情報で認証し, コマンド等を利用できる状態にすること

前編まとめ２

- アカウントクラックの問題
  - アカウントクラック：アカウント名＋パスワードを盗む行為
  - クラックされたら, 自分に限らず他人(世界中)に被害が及ぶ
  - 問題を防ぐため, アカウントをしっかり管理することが重要
  - クラック手法: Social Attack ， BFA，DA
- 良いパスワード
  - クラックを防ぐ方法の一つは, よいパスワードをつけること
  - 長い文字数, 多くの文字種を用いる(頑丈)
  - 辞書に載ってる単語や個人情報を使わない(予想されにくい)
  - 憶えやすい

  - 良いパスワードをつけることは計算機利用者の義務

実技 : Linux をいじり倒す準備を整える

まずはアカウントを作ろう

- アカウント作成
  - アカウント名
  - 良いパスワード
- ログイン・ログアウト

目次

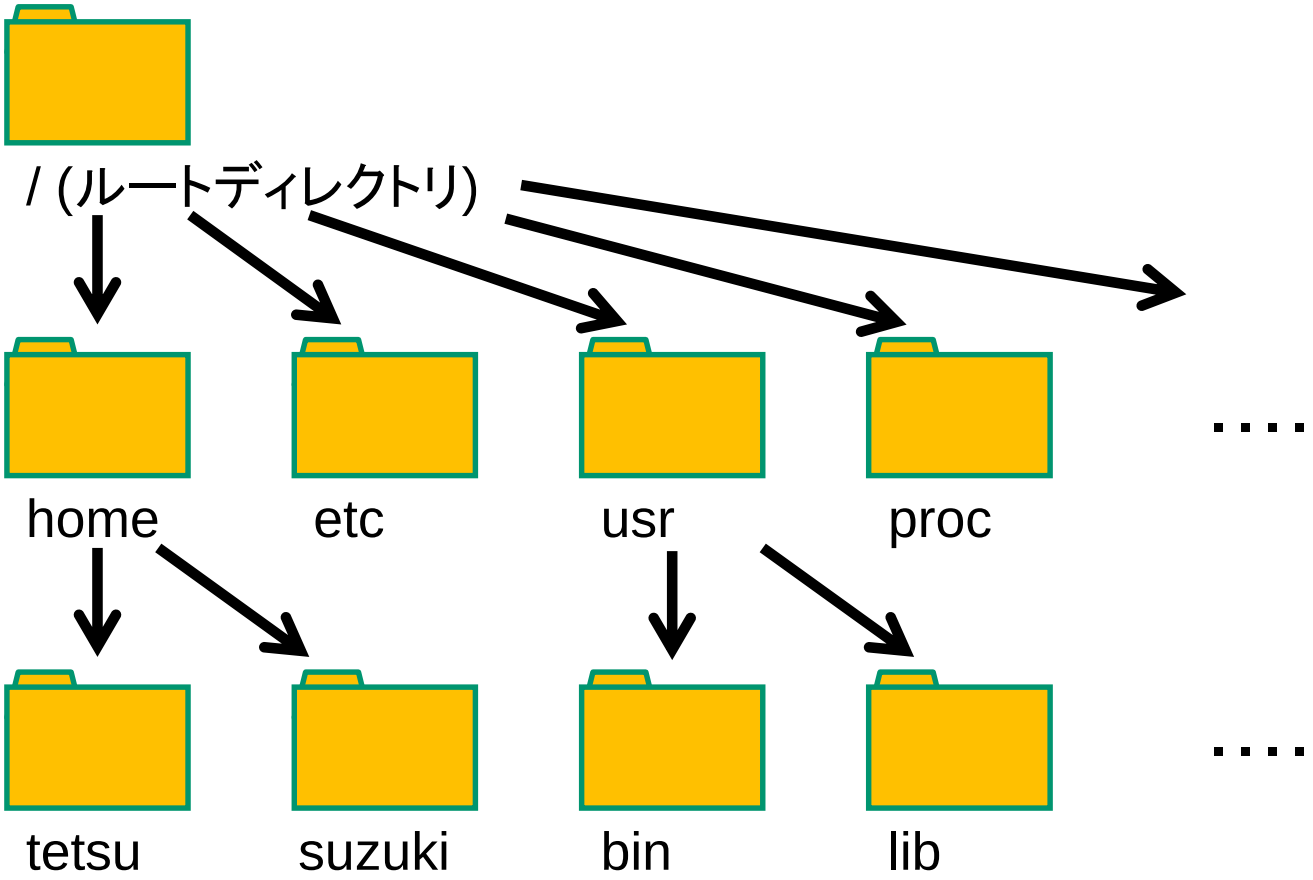
6. Linux のデータ管理

Linux のデータ管理

- 全てファイルとして扱われる
  - アプリケーションソフトウェア, 周辺機器さえもファイル
    - マウス, キーボード, ハードディスク…
- ファイルはディレクトリにより階層的に管理される
  - ディレクトリ とはファイルを格納するためのファイル
    - Windows で言えばフォルダ
  - ディレクトリの中にディレクトリを格納することも可能

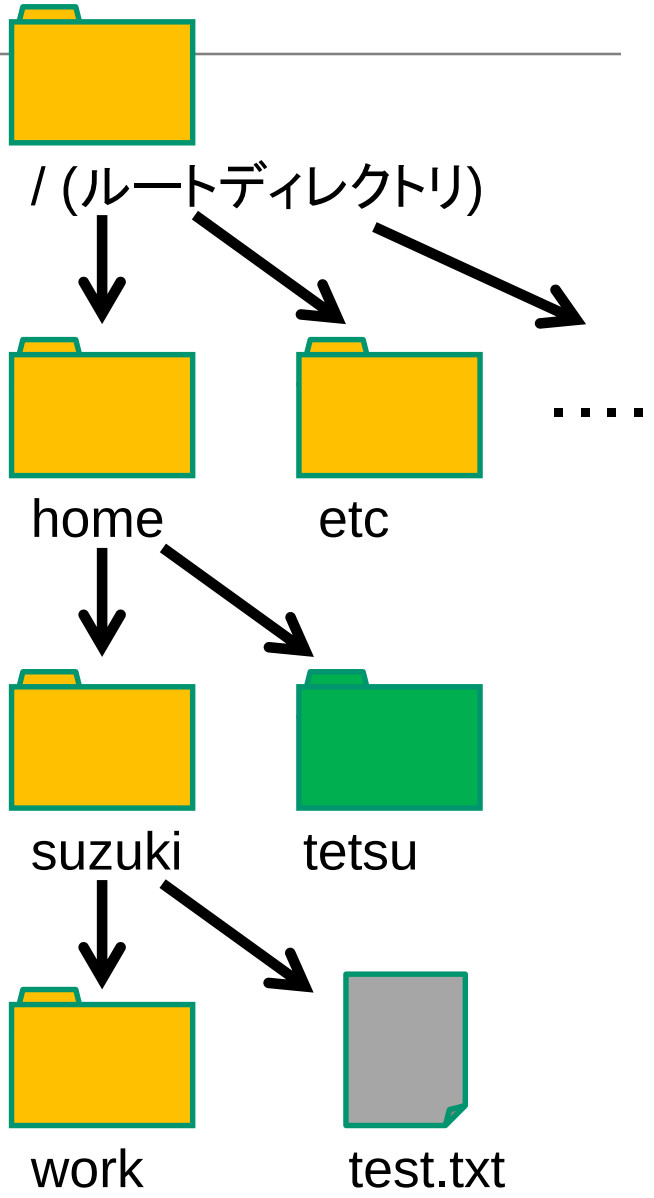
Linux のディレクトリ階層構造

- ルートディレクトリ「 / 」を起点とするツリー構造



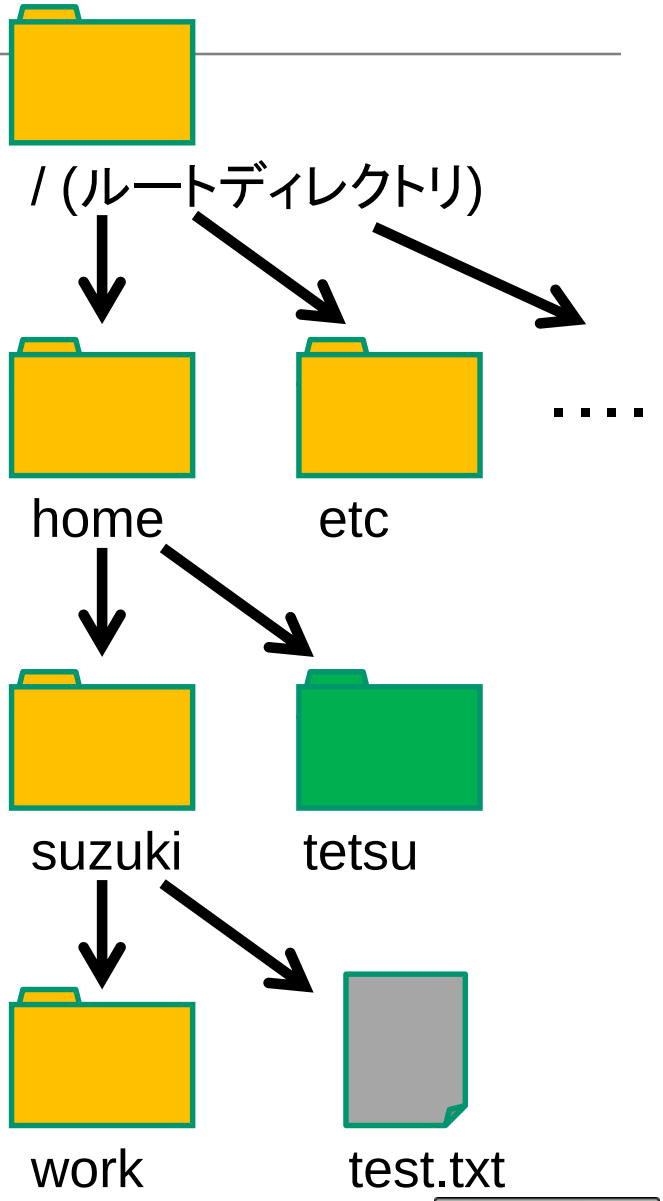
ディレクトリの呼び方

- **ホームディレクトリ**
  - 各ユーザ用ディレクトリ
  - home ディレクトリの直下に存在
  - 「～」 (チルダ)で表す
- **カレントディレクトリ**
  - 現在いるディレクトリ
  - 「 . 」 (ドット)で表す
- **親ディレクトリ**
  - 一段上のディレクトリ
  - 「 .. 」 (ドットドット)で表す
- **子ディレクトリ**
  - 一段下のディレクトリ



ファイルの指定方法

- パス
  - 目的のファイルにたどり着くための道順(path)
- 絶対パスを用いた指定
  - ルートディレクトリ「 / 」を起点
    - /home/tanaka/test.txt
    - /home/tanaka/work
- 相対パスを用いた指定
  - カレントディレクトリ「 . 」を起点
    - ../tanaka/test.txt
    - ../tanaka/work
- 「~ 」を用いた指定
  - 自分のホームディレクトリを起点
    - ~/text.txt
    - ~/work
  - 指定ユーザのホームディレクトリを起点
    - ~tanaka/test.txt
    - ~tanaka/work



ディレクトリに関するコマンド

- **cd**
  - ディレクトリを移動する
- **pwd**
  - 現在のディレクトリの場所を絶対パスで表示
- **ls**
  - ディレクトリの中身や情報を表示
- **tree**
  - ファイル・ディレクトリをツリー形式で表示
- **mkdir, rmdir**
  - ディレクトリを作成・削除
- **rm**
  - ファイル・ディレクトリを削除

詳しくは実習編で！！

7. パーミッション

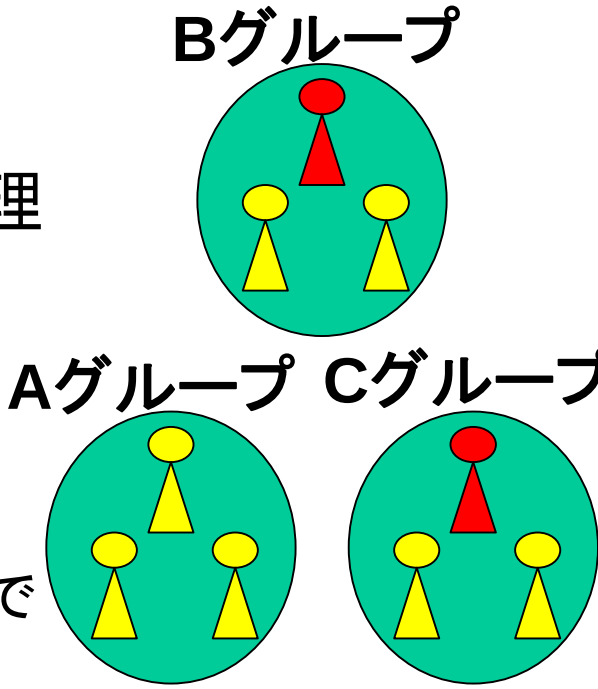
パーミッションとは

- ファイル・ディレクトリの**利用権限**
  - すべてのファイル・ディレクトリに設定されている
  - ファイル・ディレクトリに対して，「誰に」，「何を」許可するか指定する
    - 「誰に」
      - 所有者 (User), 所有グループ (Group), それ以外 (Other)
    - 「何を」
      - 読み取り (Read), 書き込み (Write), 実行 (eXecute)

マルチユーザシステムを運用する上で
パーミッションは必要

ユーザとグループ

- ユーザ
  - コンピュータの利用者
  - ユーザ ID (UID) とアカウント名で管理
    - UID: 特定のユーザを識別する番号
- グループ
  - 複数のユーザをまとめたもの
    - 特定の目的のユーザの集まりとして管理できる
      - ファイルを共有したりできる
  - グループ ID (GID) とグループ名で管理
    - GID: 特定のグループを識別する番号



パーミッションはなぜ必要か？

利用権限を必要に応じて付与することにより，

安全性・利便性が増す

マルチユーザシステムにおける重要な仕組みの一つ

- プライバシーの保持
  - 他者に見られたくないファイルの保護
    - メール, 未発表の研究データ, 個人的な写真など…
- 情報の共有
  - グループ間でのファイルのやり取り
- 重要ファイルの保護
  - /etc/shadow 等のシステムファイル (実技編発展参照)

後編まとめ

- Linuxのデータ管理
  - すべてファイルとして扱われる
  - ファイルはディレクトリにより，階層的に管理される
- パーミッション
  - ファイル・ディレクトリの利用権限
    - 計算機における情報共有/秘匿のための仕組み
  - User, Group, Others に分けて管理
  - マルチユーザシステムを安全・便利に運用する上で必要

実技：ファイル / ディレクトリ操作をしよう

- 簡単なコマンドの実行
- ディレクトリ階層構造の理解
  - ディレクトリの移動
  - カレントディレクトリの把握
  - ファイルの指定 (絶対パス, 相対パス)
- パーミッションの設定

参考文献(1)

- 情報学I授業テキスト編集グループ, 2017
  情報学Ｉテキスト 2017, 学術図書出版社
- 日本ネットワークセキュリティ協会教育部会, 2009
  情報セキュリティプロフェッショナル教科書, アスキー・メディアワークス
- 林晴比古, 2004, 改訂 新 Linux/Unix 入門, ソフトバンククリエイティブ
- 橋本英勝, 2010, 基礎からのLinux 改訂版, ソフトバンククリエイティブ
- 池田博昌, 2007, 通信ネットワーク事典 第５版, 秀和システム
- 大滝みや子, 2013, 情報処理教科書 基本情報技術者 スピードアンサー 338, 翔泳社

参考文献(2)

- GNU オペレーティング・システム, Free Software Foundation, Inc., 2015, https://www.gnu.org/philosophy/free-sw.ja.html
- Wikipedia – Linux, Unix, Intel 80386, GNU, 386BSD http://ja.wikipedia.org/wiki
- OSの歴史（UNIX系）

  http://www.kogures.com/hitoshi/history/soft-os-unix/
- The Choice of a GNU Generation/An Interview With Linus Torvalds http://gondwanaland.com/meta/history/interview.html
- Why did Linus Torvalds invent Linux? http://wiki.answers.com/Q/Why_did_Linus_Torvalds_invent_Linux?#slide=1

参考文献(3)

- デジタル用語辞典 – マルチユーザシステム
  http://yougo.ascii.jp/caltar/マルチユーザーシステム
- 過去のINEX 資料 (各年度第2, 3回 講義のもの)

  http://www.ep.sci.hokudai.ac.jp/~inex/index-list.html
- UNIX COURSE, MISTY-NET UNIX Cours, 2003,
  http://cmd.misty.ne.jp/basic/04.html

付録

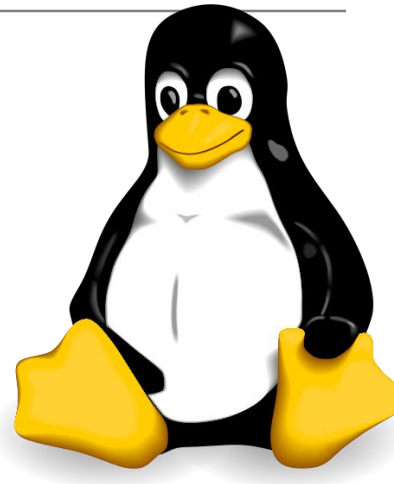
Linux の興隆

- Linux はフリーソフトウェア（オープンソース）として公開される
  - GNU で Unix の機能の一部を表現
    - GNU: Unix互換のソフトウェア環境を全てフリーソフトウェアで実装することを目標とする組織，及びそのソフトウェア
  - 結果，GNU思想に賛同する人々から Linux への注目が集まった
    - 当時，GNU 内で OS の開発はしていなかった
  - 個人から組織（大学・研究所等）の順で急速に普及・発展した

GNUのロゴマーク
Aurelio A. Heckert,
http://www.gnu.org/graphics/heckert_gn
.html

Linux の特徴

- フリーソフトウェア
  - オープンソース
    - ソースコードが開示されている
- システムを自分好みにカスタマイズ可能
- 様々なハードウェア上で実装可能
- ソフトウェアの脆弱性には, ユーザ間で対応
- ウェブ上のフリーのマニュアルも充実などなど…



Linux公式マスコット：タックス
http://commons.wikimedia.o
rg/wiki/Image:Tux.svg

ただし，基本的に無保証！！

Linux ディストリビューション

- Linux カーネル (OSの中核，第3回) に各種アプリケーションを加えたもの
- 例
  - Debian系
    - Debian GNU/Linux (https://www.debian.org/index.ja.html)
    - Ubuntu (http://www.ubuntulinux.jp/)
  - Red Hat 系
    - Fedora (https://getfedora.org/ja/)
    - CentOS (https://www.centos.org/)

INEX で利用する Debian GNU/Linux の特徴

- フリーソフトウェア（自由）+ 無料
  - ソースコードが公開されている
  - 一企業ではなく有志が開発

  教育的意義が高い / 卒業後も利用できる
- 堅牢なパッケージ管理システム
  - 安心の三段階審査（stable, testing, unstable）

  （Linux ディストリビューションの中で多段階審査を最初に導入）
- サーバの構築・管理に便利
  - 必要最小限のシステム構成にすることが比較的容易
    - セキュリティを高める上で重要

  地球惑星科学分野におけるサーバにも利用されている

付録：Linux 内でのユーザ情報管理

- 3 つのファイルに分けて管理されている
- /etc/passwd
  - アカウントの基本情報
    - 閲覧制限なし
- /etc/shadow
  - アカウントの暗号化済みパスワード情報
    - root のみ閲覧可
- /etc/group
  - グループの基本情報
    - 閲覧制限なし

付録：ドットファイル(隠しファイル)

- ドットファイルの例
  - .bashrc, .bash_profile, .emacs　など
- ユーザの環境設定用ファイル
  - 「．」で始まるファイル
  - 各ユーザのホームディレクトリ以下に存在
  - ls (ファイル一覧表示コマンド) と打っただけでは表示されない (ls –a と打つべし)
  - 日本語環境の設定など
  - 削除したり書き換えする際には慎重に！!
  - 実習編でも紹介

付録：「 / 」以下のディレクトリの役割(一部)

- /home
  - 各ユーザのホームディレクトリを格納
- /usr
  - 各種プログラムやカーネルソースを格納
- /etc：
  - システム管理用の各種設定ファイルを格納
- /proc：
  - カーネルの動作情報を示す，特殊なファイルを格納

その他にもたくさんあります
詳しくは実習編の発展のページで