

オペレーティングシステム

2023/1/10

海谷 治彦

目次

システムの運用管理

- 1 運用管理
- 2 利用者管理
- 3 構成管理
- 4 障害管理

管理の概要

- OSの運用管理は、当該OSがどのような業務・活動に利用されているかでかなり異なる。
 - 基幹システム: 鉄道, 電力供給, 携帯電話網, 銀行, 株売買...
 - 個人利用: 遊びのPC, 日常生活でのスマホ
- この章で述べられている事は、どちらかといえば、サーバーや基幹システムの管理を意図しており、個人のPC, スマホ等の管理とは剥離している。

運用管理の対象

- 単体のコンピュータでは無い。
 - 今日の業務, 活動は複数の機器, 人間が連携しあうものがほとんどである.
 - 機器: ネットワーク接続機器, ファイルサーバー, プリンタ等
 - 機器に搭載されたOSは周辺の機器, 人間の信頼性を考慮しつつ連携する必要がある.

運用管理者達

- 情報システム部門
 - 例えばビール製造会社でさえ、社内コンピュータシステムを扱う部門がある。(or あった)
 - まあ、外注される可能性も大.
- 管理責任者
 - 管理方針の策定
 - 問題があった場合の責任をとったり・・・
- 運用責任者
 - 実際のオペレータ.
 - 後述の利用者管理, 障害管理等を実際行う.

管理内容の種類

- 利用者管理, 構成管理, 障害管理: 後述
- 稼働管理:
 - 稼働率向上のための情報を集める.
 - 一括処理型のOS運用以外あまり関係ない.
- 性能管理:
 - 今時は応答性能が重要.
- セキュリティ管理: 後述.
- ネットワーク管理:
 - OSの範疇を超えるがネットワークに関する上記の管理.

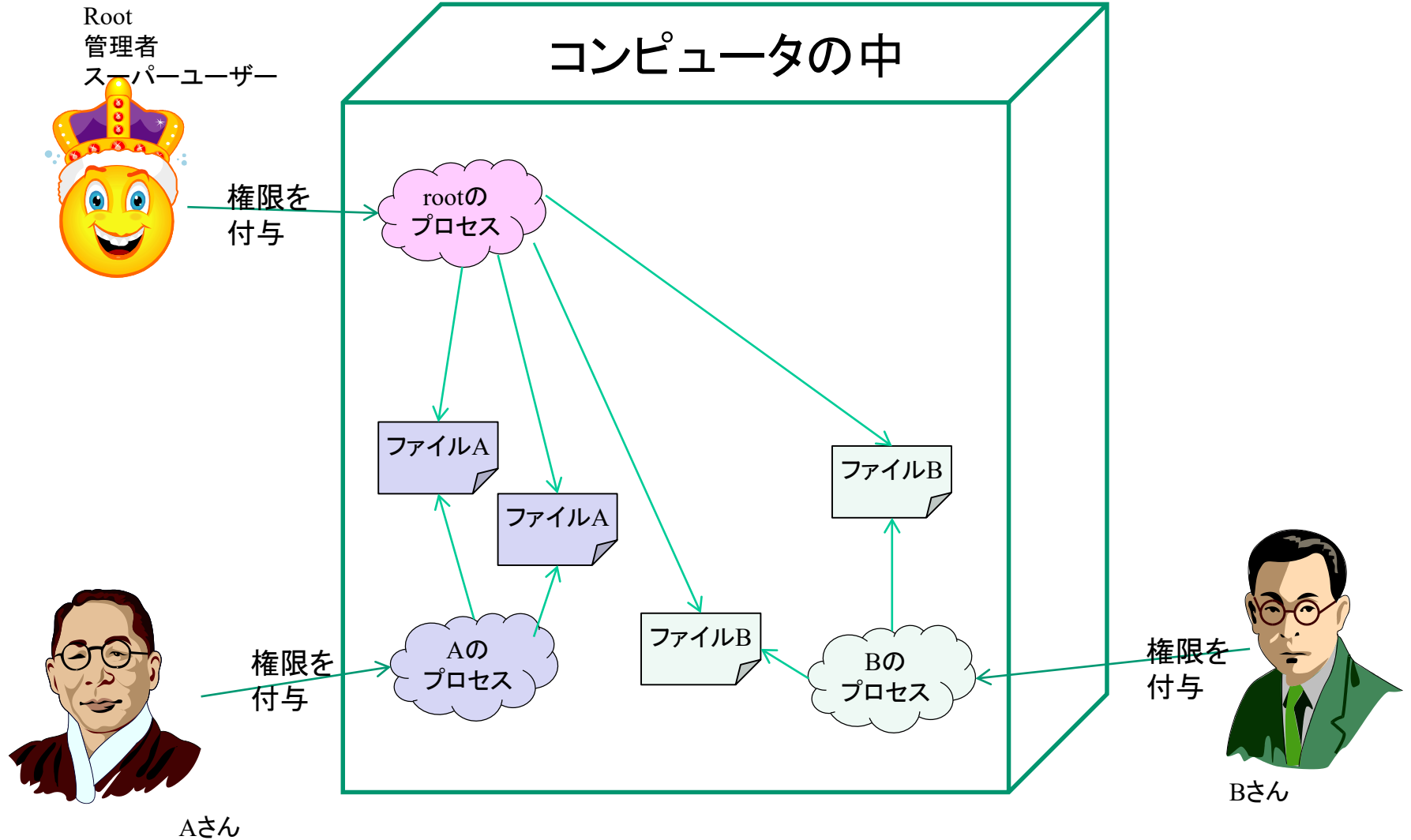
利用者管理

- まず, 大前提として, OSは権限の異なる利用者を想定して作られています.
 - 実際の人間とOSの利用権限を, どのように対応付けるかは次にて.
- 権限には上下関係のレベルがあります.
 - 上は下の権限を含む.
- 権限が付与されるものは以下の二つです.
 - プロセス
 - ファイル (含むデバイスファイル)
- UNIX系OSでは二種類の権限しかありません.
 - 特権ユーザー
 - 一般ユーザー

プロセス・ファイルと権限階層

- OSのプロセスはコンピュータ内で利用者の権限を代行する実体である.
- プロセスに付与された権限に応じて, アクセスできるファイルが異なってくる.
- UNIX/Linuxにおいては,
 - root 特権ユーザー
 - 全てのファイルにアクセス可能. rootのプロセスはカーネルモードで動作する.
 - 一般ユーザー
 - 原則, 自身の所有するファイルにのみアクセスできる.
 - 意図的に全員にアクセス可能となっているファイルはアクセスできる.
 - 一般ユーザー間に上下関係はつけられない.

イメージ



権限階層

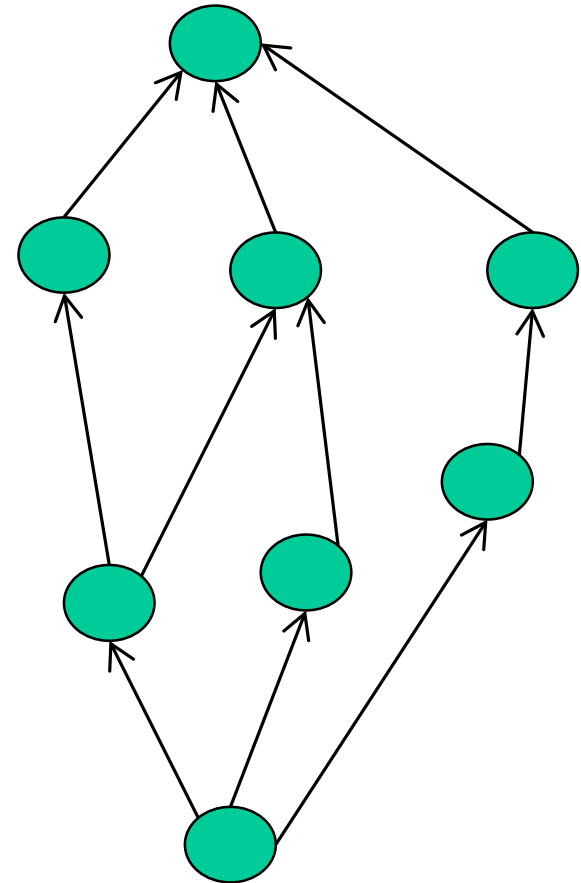
- 権限行使の観点から，以下の用語がつかわれる
 - Subject 権限を行使するアクティブな実体. OSではプロセスのこと.
 - Object 権限を適用される受け身な物. OSではファイル等.
- 本来，Subject, Objectは半順序(後述)の関係があるべき.
 - Subjectについては，例えば，平社員，課長，部長，社長等の階層があったり，
 - Objectに関しては，超極秘ファイル，極秘ファイル，社内閲覧ファイル，公開ファイル等
- UNIX系OSでは，このような階層を二階層に単純化してしまっている.
 - rootとそれ以外の一般ユーザー

半順序と全順序

- 以下の3つの性質を満たす \leq を集合 S 上の半順序 (partial order) と呼ぶ.
 - 任意の要素 $e \in S$ について, $e \leq e$ (反射律)
 - $e \leq f$ かつ $f \leq e$ ならば, $e=f$ (反対象律)
 - $e \leq f$ かつ $f \leq g$ ならば, $e \leq g$ (推移律)
- 加えて以下の性質を満たすと全順序 (total order) と呼ぶ.
 - 任意の要素 $e, f \in S$ について, $e \leq f$ もしくは $f \leq e$ が成り立つ. (完全律)

束 半順序の一般的構造

- 半順序がある集合は、木構造になる場合もある。
- しかし、より一般的には、左記のような構造になる。
- 左記の構造は束(Lattice)と呼ばれている。
- 大雑把にいうとループの無いグラフ。
- ちなみに、全順序の集合要素は一直線上に並ぶ。



UNIX系OSでのグループ

- UNIX系OSではユーザーのグループの概念を導入し、同じグループ内でのユーザーがファイル等を共有することを許している。
- 別にグループに対応する実ユーザーがいるわけではないので、前述の権限階層とは異なる。

```
001.CPS
[kaiya@flute03 ~]$ ls -l
合計 90748
-rw-r--r-- 1 kaiya info 1026239 5月 20 16:59 2014 Joho06_pp.pdf
-rw-r--r-- 1 kaiya info 20248 5月 27 17:59 2014 ShowCarpenter4.jar
-rw-r--r-- 2 kaiya info 104 6月 9 17:17 2014 a.c
-rw-r--r-- 1 kaiya info 209038 6月 3 17:04 2014 a.jpg
-rwxr-xr-x 1 kaiya info 6391 6月 9 17:17 2014 a.out*
-rw-r--r-- 1 kaiya info 12368 6月 4 16:06 2014 afo
```

```
[kaiya@flute03 log]$ cd /var/mail
[kaiya@flute03 mail]$ ls -l
合計 352
-rw-rw----. 1 hisys mail 0 3月 19 09:57 2012 hisys
-rw-----. 1 root mail 352989 6月 27 08:00 2014 root
-rw-rw----. 1 rpc mail 0 3月 19 09:39 2012 rpc
-rw----- 1 test02 mail 819 3月 23 09:58 2012 test02
[kaiya@flute03 mail]$
```

課金と制限

- ユーザー情報に基づき,
 - 課金 (いわゆる従量制)
 - CPU, メモリ, ディスクの使用料に基づき金をとる.
 - 資源利用制限
 - ディスクの利用量上限
 - 印刷枚数制限等を行う場合がある.
- クラウドシステムの利用において, 利用資源に応じて課金されるのが普通.
 - 課金を増やせば, 即時に資源を増やせる場合が多い.

構成管理

- ハードウェア
 - 個人利用のOSは可能な限り自動的にデバイスドライバを入れる場合もある.
- ネットワーク
 - ネットワーク構成自体はOSの外の話だが、ネットワーク構成に合うようにネットワークインタフェースを設定する必要がある.
- ファイルシステム
 - これも決める必要がある. 例えば, swapのサイズ等はココで決める.
- プログラム
 - どのプログラムをインストールするか決める.

ログ管理

- どのような統計情報を監視し記録するかも管理項目である.
 - プロセッサ使用率
 - メモリ使用量
 - ディスクのアクセス状況
 - ディスク交換時期等の見積もりに使える.
 - ネットワークトラフィック
 - セキュリティ系の対策材料
 - ソフトウェアの使用状況
 - 不要なソフトの除去
- 役立つ情報を必要なだけ監視すべき.

障害管理

- コンピュータは機械だから壊れる。
 - 場合によっては攻撃等によって.
- いつ壊れそうか監視するのもOSの役目.
- 障害管理に関する三つの指針
 - Prevention 回避する手立てを講じる
 - Detection 障害を検知する, できれば事前に.
 - Reaction 障害から復旧する.
- 最近は以下も重要らしい
 - Forensics 障害の証拠を残す. 主に裁判対応.

Prevention 予防

- ハードウェアの予防交換
 - 毎年新しい部品に変える等.
- OSを含むソフトウェアの更新
 - バグへの対応.
- ファイルシステムの保護
 - 冗長化(RAID) 後述
 - ジャーナリングファイルシステムの導入,
 - バックアップ.

RAIDについて

- Redundant Arrays of Independent Disks
- 複数のハードディスクを束ねて仮想的な一台のディスクに見せる技術.
- 色々レベルがあるが, RAID1 (ミラーリング)が障害予防には有効.
 - 複数の物理ディスクが同じ内容を保持しているので, 一台壊れても平気.
 - ただし, 普通, 書きは遅くなる.
- Linuxでも普通にRAIDは使える.

Detection 検知

- 基本, ログ等の解析から障害を事前に予測する.
- ハード, ソフト等に異常動作の記録が予測のカギ.

Reaction 復旧

- 壊れた部品は交換するしかない. もしくは, ハードウェア全体の交換.
- RAIDの場合, 故障したディスクのみの交換を行い同期をとる.
 - OSを停止せずに交換可能な場合もある.
- バックアップからファイルシステムの内容を復旧する.
 - 昨今でも大規模データセンター等ではテープでのバックアップは現役.



次のスライドへ