工学部技術部 平成12年度技術講習会

「Linuxを用いたインターネットサーバの構築」
－ PCの組み立てからサーバの運用まで －

第4回 「システム管理」

技術部ネットワークグループ
伊藤 篤

構成

1. システム管理とは？
2. サーバをとりまく環境
3. システム管理者の業務

1. システム管理とは？

サーバの環境を快適で
安定な状態に維持する。

要素
- ハードウェア
- ソフトウェア
- ネットワーク
- ユーザ
- サーバ運営

2. システム管理面からみたサーバをとりまく環境

ネットワーク:インターネット
セキュリティ

ハードウェア:PC
動作状況、構成変更、故障
ソフトウェア:OS、アプリケーション
動作状況、設定、バグ、
バックアップ

ユーザ:一般ユーザ、スーパーユーザ
ユーザ管理、対応
サーバ運営:
運営方針、規則、役割分担、
非常時対応

2. システム管理面からみたサーバをとりまく環境
サーバ用の機器とOS

- サーバ機
  - ワークステーション
  - PC
- OS

名称	開発または、販売
AIX	IBM社
IRIX	Silicon Graphixs社
Netware	Novell社
Solaris	Sun Microsystemus社
HP-UX	Hewlett Packard社
BSD	UCB
Linux	Linus Torvals氏
Windows NT	Microsft社

3. システム管理者の業務

サーバ環境を快適で安定な状態に維持するために
- システムの監視
- セキュリティー
- バックアップとリストア
- 障害時の対応
- ソフトウェア管理
- ユーザ管理
- サーバ運営

システム管理者の業務
1. システムの監視

a. プロセス (*ps*、*vmstat*、*top*)

b. ハードウェア (*df*、*du*、*hwclock*)

c. ネットワーク (*lsmod*、*ifconfig*、*netstat*、*ping*、*nslookup*、*traceroute*)

d. ログ 検証、ローテーション
(*lastlog*、*last*、*w*、*utmp*、*wtmp*、*syslog*、*logrotate*、*cron*)

e. その他 (*date*、*ntp*、*uname*)

カーネル(kernel)とは？

プログラムの動作に必要な *基本的機能* を提供する。
カーネルバージョン 2.2.15 (TurboLinux Server 日本語版 6.1)
実体は、/boot/vmlinuz → vmlinuz-2.2.15-8

カーネルが担う基本的な機能

◆ プロセス管理	マルチタスク
◆ プロセス間通信	複数のプロセスが協調して働く
◆ メモリ管理	プロセスへのメモリ割り当て、開放、仮想記憶
◆ デバイスドライバ	全てのデバイスを制御
◆ ファイルシステムサポート	ハード・ソフト異種間を対応、中継
◆ ネットワーク	TCP/IP, 各種サービス

システム管理者の業務
1. システムの監視

a. プロセス (*ps*、*vmstat*、*top*)

b. ハードウェア (*df*、*du*、*hwclock*)

c. ネットワーク
(*lsmod*、*ifconfig*、*netstat*、*ping*、*nslookup*、*traceroute*)

d. ログ 検証、ローテーション
(*last*、*lastlog*、*w*、*syslog*、*logcheck*、*logrotate*、*cron*)

e. その他 (*date*、*ntp*、*uname*)

システム管理者の業務
1. システムの監視 ● プロセス

■ *ps aux* プロセス表示 : サーバ(マルチタスク)で行っている個々の仕事
prosess status a :全プロセス、u :ユーザ情報、x :端末外含む

USER : プロセスユーザ名	PID : プロセスID
%CPU : CPU使用率	%MEM : メモリ使用率
SIZE : 仮想イメージの大きさ	RSS : 使用中の物理メモリー量
TTY : 制御端末名 ?= デーモン	
STAT : プロセスのステータス	
（R = 実行可能 S = 停止 T = 停止またはトレース中 Z = ゾンビ・プロセス	
N = ナイス値が正 D = 割り込み不可の停止 W = スワップ・アウトしたプロセス ）	
START : 開始時刻	TIME :ユーザとシステムの合計 cpu 時間
COMMAND : プロセスのコマンド名と引数	

システム管理者の業務
1. システムの監視 ● プロセス

■ *vmstat 3 3* プロセス、メモリー、仮想記憶、CPUの使用・負荷率の状態表示
Virtual Memory status 3秒間隔で3回チェック

procs	プロセス数	r : 実行可能、b:ブロック、w:スワップアウト
memory	メモリー状態	swpd :スワップ、free :未使用、buff :I/Oバッファ、cache:ディスクキャッシュ
swap	スワップ領域への毎秒転送量(Kbyte)	si :スワップイン、so: 〃アウト
io	ブロックデバイス	bi :毎秒の書き込み回数、bo : 〃読み込み回数
system	システム	in :毎秒の割り込み回数、cs :毎秒のコンテキスト切り換え回数
cpu	CPU状態	us : ユーザ、sy : システム、id : アイドル

システム管理者の業務
1. システムの監視 ● プロセス

■ *top* 現在実行中のプロセスに関する情報を
リアルタイムに監視する

load average	過去、1分、5分、15分の平均負荷
av	利用可能容量
PRI	プロセス優先度
NI	nice値
SIZE	プロセスサイズ の 合 計

システム管理者の業務
1. システムの監視 b ハードウェア

- *df* ディスク、ドライブの使用サイズ表示
- *du* ディレクトリ内のファイルサイズ表示
- *hwclock* ハードウェアクロックを表示、設定する
  -r :表示、-w :システム時刻を書き込み

システム管理者の業務
1. システムの監視 c ネットワーク

ネットワークの動作確認順 （ 設定変更、トラブル時 ）

- *lsmod* NICのドライバが認識されているか、モジュールを確認する。(/sbin/)
- *ifconfig* ネットワークインタフェースの設定を確認する。(/sbin/)
- *netstat -r n* ルーティングテーブルの設定確認

システム管理者の業務
1. システムの監視 c ネットワーク

- *ping* IPアドレス 他のホストにパケットが届くか？
- *nslookup* ホスト名 他ネームサーバが正しく参照できるか確認する。
- *traceroute* ホスト名 パケットが相手先に到達するまでの経路をトレースする。
  (/usr/sbin/)

システム管理者の業務
1. システムの監視 d ログ

- *last -x* 最近ログインしたユーザの情報表示する。
  x :システム情報を含む
- *lastlog* ユーザ別の最後ログイン情報表示
- *w* 現在ログインしているユーザ名、利用状況を表示する。
  jcpc :全プロセス使用時間、
  pcpu :カレントプロセス使用時間

システム管理者の業務
1. システムの監視 d ログ

- *syslog* システムログを採取、記録するデーモン

syslog 経由で作成されるログファイル

boot.log	起動時のメッセージ
messages	全てのログ(メールを除く)
spooler	news やuucp のログ
secure	認証関連のログ
cron	cron のログ
maillog	sendmail のログ

システム管理者の業務
1. システムの監視 d ログ

- *syslog.conf* syslog の設定ファイル

Facility メッセージソースの分類 (13 分類)

authpriv	認証システム	cron	cronデーモン
kern	カーネル	mail	メール

Priority 優先順位 (8 分類)

emerg	パニック状態	crit	重要な状態
info	情報メッセージ	none	なし

システム管理者の業務
1. システムの監視 d ログ

■ *logcheck* syslogd が生成したログを解析する。

/etc/logcheck/	分類
logcheck.hacking	ハッキング
logcheck.ignore	無視
logcheck.violations	侵入
	" failed "→/var/log/secure
logcheck.violations.ignore	

システム管理者の業務
1. システムの監視 d ログ

■ *logrotate* ログファイルを一定期間でローテートするデーモン
/etc/logrotate.conf 設定ファイル

/etc/logrotate.d/syslog

messages	全てのログ(メールを除く)
secure	認証関連のログ
maillog	sendmail のログ
spooler	news やuucp のログ

システム管理者の業務
1. システムの監視 d ログ

■ *crond* プログラムを定期的に実行するデーモン

Crontab crond の設定ファイル

```
22 4 * * 0 root run-parts /etc/cron.weekly
分 時 日 月 曜日 ユーザ
```

/etc/cron.daily/logrotate

```
#!/bin/sh
/usr/sbin/logrotate /etc/logrotate.conf
```


システム管理者の業務
1. システムの監視 e その他

■ *date* システム時間の設定、表示を行う。
date 月日時間年 例 091916002000：2000年9月19日16時00分

■ *ntp* タイムサーバに時間を問い合わせ設定する。
/etc/cron.daily/ntpdate_exe

```
#!/bin/sh
/usr/bin/ntpdate -s 133.67.1.4
clock -w
```

■ *uname -a* システム情報を表示する。

システム管理者の業務
サーバ環境を快適で安定な状態に維持するために

1. システムの監視
2. セキュリティー
3. バックアップとリストア
4. 障害時の対応
5. ソフトウェア管理
6. ユーザ管理
7. サーバ運営

システム管理者の業務
2. セキュリティ

a. サーバのセキュリティとインターネットの脅威
b. クラッカーの攻撃例
c. LinuxのセキュリティとTurboLinux Server日本語版 6.1の方針
d. スーパーサーバ inetd
e. アクセス制御 TCP_Wrapper
f. 通信の暗号化 ssh
g. セキュリティ情報の入手
h. wu-ftpdのバグ対処事例
i. 被害時の対応策
j. ファイアーウォール

システム管理者の業務
2. セキュリティ a. サーバのセキュリティとインターネットの脅威

- 何を守るのか　データ、コンピュータリソース
- 何から守るのか　クラッカー、スクリプト・キディ
- セキュリティ対策の基本
  - 入り口を閉じる。
    - 不要なサービスを停止し、ポートを閉じる
  - 常時、監視する。
    - 適切なログの収集、監視。メールでの配信。
  - セキュリティ情報を収集する。
    - 常に最新の情報を入手

システム管理者の業務
2. セキュリティ b. クラッカーの攻撃例

- 侵入　不正にサーバにログインしリソースを使用する。
- 使用不能攻撃　ネットワークトラフィックを増やしサーバを麻痺。
  バッファオーバフロー攻撃　6月のwu-ftpd セキュリティ報告は、printf()関数のバグ
- 踏み台　不正侵入後、他サイトへの侵入や攻撃に利用。
- なりすまし　他人になりすまし、サービスの不正利用をする。
- 偽造、改竄　メールやホームページを書き換える。
- 盗難、盗聴　ファイル、メール、アクセス記録などを盗む
- 攻撃事前調査　ポートスキャンしセキュリティホールを探知する。

システム管理者の業務
2. セキュリティ b. クラッカーの攻撃例

- ウィルス、トロイの木馬　メールや配布プログラムにシステムを破壊したりユーザ情報を盗聴するなどのプログラムを組み込む。
- メール爆弾　大量、大容量のメールを送付する。
- サービス妨害　ホームページ領域の乗っ取り、掲示板へ の不正な書き込みなど
- スパムメール　受信者が希望しないメールを大量に送信する。
- 中継　スパムメールの中継サイトに利用される。

システム管理者の業務
2. セキュリティ b. クラッカーの攻撃例

- DoS 攻撃 (Denial Of Service)
  大量のデータを送りプログラムやリソース不足を起こさせサーバの機能を停止させる
  - 侵入よりも簡単な場合が多い
  - 攻撃者のIPアドレスを偽造することが可能
  - スクリプト・キディが面白がって使うケースが多い
  - 攻撃された側にログが残らないケースが多い
  - 侵入出来なくてもDoSが有効になるサーバが多い

システム管理者の業務
2. セキュリティ c. Linuxのセキュリティと TurboLinux Server 日本語版 6.1の方針

- Linuxのセキュリティ　オープンソース
- TurboLinux Server 日本語版 6.1の方針、初期設定
  - Deny all アプローチ
  - シャドウパスワード
  - ログのローテーション
  - root ログインの制限
  - アップデート

システム管理者の業務
2. セキュリティ d. スーパーサーバ inetd

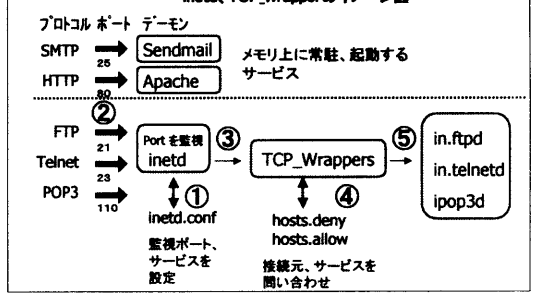
- スーパーサーバとは？
  telnet、ftpなどサーバプログラムを制御し必要に応じて起動するデーモンプログラム。
- 機能と役割
  ① システム・管理の負荷軽減 ② システムの冗長性、堅牢性の向上
- デメリット
  頻繁に接続要求を受けるサービスまたは、起動時の初期化に時間がプログラムはシステムの負荷が高まる。
- スタンドアローンモードでのサービス　sendmail、Apache
- 設定ファイル　inetd.conf
- 起動スクリプト　/etc/rc.d/init.d/inet パラメータ

システム管理者の業務
2. セキュリティ d. スーパーサーバ TCP_Wrapper

- TCP_Wrapper (tcpd)の概要
  inetd がクライアントからの要求を受けた際に起動され、目的のサーバプログラムを起動させるアクセス管理機能を実現する。
- 設定ファイル
  書式 [daemon_list] : [host_list] : (: [command])
  /etc/hosts.allow 許可設定
  /etc/hosts.deny 禁止設定

システム管理者の業務
2. セキュリティ d, e inetd、TCP_Wrapper

inetd、TCP_Wrapperのイメージ図



システム管理者の業務
2. セキュリティ e. 通信の暗号化 SSH

- SSH (Secure SHell)の概要
  通信の暗号化を行い安全なリモートログインを実現する。
  標準では、IDEA方式で暗号化する。
  - ◆ ホスト認証機能: 公開鍵暗号方式のRSA暗号を用いホスト同士の認証を行う。
  - ◆ ユーザ認証: 接続ユーザの認証にRSA暗号を使用。
- TurboLinux Server 日本語版 6.1では、Open SSHを採用
- Windowsからのリモート接続例
  Tera term Pro 2.3 と ssh 対応アドオンパッケージ ttssh を使用
  接続時のログでRSA Keyが作成されていることを確認。

```
sshd[187]: log: Generating new 768 bit RSA key.
sshd[187]: log: RSA key generation complete.
```


システム管理者の業務
2. セキュリティ f. セキュリティ情報の入手

セキュリティ関連組織

- コンピュータ緊急対応センター JPCERT http://www.jpcert.or.jp/
  コンピュータセキュリティインシデント、セキュリティ対策をシステム運用管理の視点からコーディネーションしている組織。
- 情報処理振興事業協会 IPA http://www.ipa.go.jp/
  ① 不正アクセスの届け出状況をまとめた報告
  ② 緊急性の高いセキュリティーホールに関する告知
- 警視庁 http://www.npa.go.jp/
  「不正アクセス行為の禁止等に関する法律」が施工され
  不正アクセスの被害にあった場合に法的措置が可能になった。

システム管理者の業務
2. セキュリティ g. セキュリティ情報の入手

ディストリビューション、Linux関連のHP

- TurboLinux http://www.turbolinux.co.jp/
- 日本の Linux 情報 http://www.linux.or.jp/

セキュリティ調査

- ネットエージェント http://www.netagent.nd.to/
  「サイトアナライザ」によるセキュリティ診断サービス
- 有限会社長崎ネットワークサービス http://www.nanet.co.jp/
  第三者中継の調査

システム管理者の業務
2. セキュリティ h.wu-ftpdのバグ対処事例

wu-ftpd 2.6.0 以前にリモートから root 権限を詐取できるセキュリティーホールが報告。

wu-ftpd 2.6.1 へのアップデート手順

1. rpm -e wu-ftpd-2.5.0-1 でアンインストール。
2. wu-ftpd-2.6.1.tar.gz 02-Jul-2000 04:13 334kを http://www.ring.gr.jp/archives/net/wu-ftpd/wu-ftpd/ から入手し、/usr/src/ に置く。
3. tar xvzf ./wu-ftpd-2.6.1.tar.gz で展開。
4. cd ./wu-ftpd-2.6.1/
5. ./configure

システム管理者の業務
2. セキュリティ h.wu-ftpdのバグ対処事例

6. make
7. make install
8. /etc/inetd.conf の ftp を有効にする。
9. /etc/rc.d/init.d/inet restart

ftp接続すると、以下のメッセージで接続成功。

```
220 ***.eng.mie-u.ac.jp FTP server (Version wu-2.6.1(1) Tue Jul 18
**:**:** JST 2000) ready.
USER ***
```


システム管理者の業務
2. セキュリティ i. 被害時の対応策

- サービスの停止
- ネットワークから切り離し
- データ、ログの隔離、保存
- 被害状況の把握
- ユーザ、関係機関への通知
  - IPA、JPCERT、警察などへの被害届
- 復旧手段の考慮

システム管理者の業務
2. セキュリティ j. ファイアーウォール

インターネットの脅威から内部のネットワークを守る仕組み

- パケットフィルタリング ファイアウォール
  専用チップまたは、カーネルレベルでルールに従いパケットを
  フィルタリングする。 インターネット層以下で実現。 ipchain など
- プロキシゲートウェイ ファイアウォール
  プロキシサーバでフィルタリングして代理で中継する。
  トランスポート層以上で実現。 delegate など

システム管理者の業務
2. セキュリティ j. ファイアーウォール

TCP／IPの階層モデル

アプリケーション層	DNS,SMTP,Telnet,FTP,NFS
トランスポート層	TCP,UDP
インターネット層	IP,ICMP
ネットワークアクセス層	Ethernet,FDDI,ATM,RS-232C

システム管理者の業務
サーバ環境を快適で安定な状態に維持するために

1. システムの監視
2. セキュリティー
3. バックアップとリストア
4. 障害時の対応
5. ソフトウェア管理
6. ユーザ管理
7. サーバ運営

システム管理者の業務
3. バックアップとリストア

再現不可能なデータをどう守り、また障害発生時には、どう復旧するのか。

データ損失の原因

システム構成、実施サービス、データ量、稼動状況に応じて選択

- ハードウェア　テープ装置(DAT、DLT)、MO、ハードディスク、RAID
- ソフトウェア　商用ソフトウェア(TurboLinux8.1:BRU)
  UNIXコマンド dump,restore,tar
  RAID(Redundant Arrays of Independent Disk)
- 運用管理　フル、差分、累積型

RAID(Redundant Arrays of Independent Disk)
データを複数のハードディスクに分散、記録し信頼性、アクセス速度を向上させる。

システム管理者の業務
3. バックアップとリストア

- バックアップ例　　tar と cron による定期、ディレクトリ別バックアップ

  /var/log/ 用　　/etc/cron.log_bkup/var_log_1.exe

  -r--r----- 1 root tech-adm 911360 Sep 11 04:22 * * * _var_log1. 20000911. tg

  バックアップするディレクトリ

  /etc/ 、 /home、 /var/log/、 /var/spool/、 /var/named/ など

- テープによるバックアップ（実施計画中）

  HP SureStore DAT
  外付けテープドライブ
  DAT24eU、DDS－3対応
  24GB

システム管理者の業務
サーバ環境を快適で安定な状態に維持するために

1. システムの監視
2. セキュリティー
3. バックアップとリストア
4. 障害時の対応
5. ソフトウェア管理
6. ユーザ管理
7. サーバ運営

システム管理者の業務
4. 障害時の対応

- 災害復旧プランの作成

  想定される障害について復旧手順をマニュアル化する。

- これまでの事例紹介

  1. FDDIケーブルとコネクタ部分の接合不良。60、engドメインが孤立。
  2. 落雷による停電時に設定の勘違いでSendmailが自動起動しなかった。
  3. 落雷による停電時にUPSの設定ミスで所定の動作をしなかった。

システム管理者の業務
サーバ環境を快適で安定な状態に維持するために

1. システムの監視
2. セキュリティー
3. バックアップとリストア
4. 障害時の対応
5. ソフトウェア管理
6. ユーザ管理
7. サーバ運営

システム管理者の業務
5. ソフトウェア管理

ソフトウェア、カーネルのアップグレード事例
Turbopkg を使用して実施。

1. telinit 1　　シングルユーザモード
2. modprobe loop　　モジュールをチェック
3. turbopkg　　パッケージマネージャ
4. CD-ROMをセットし、u:アップグレードを選択。

システム管理者の業務
サーバ環境を快適で安定な状態に維持するために

1. システムの監視
2. セキュリティー
3. バックアップとリストア
4. 障害時の対応
5. ソフトウェア管理
6. ユーザ管理
7. サーバ運営

システム管理者の業務
6. ユーザ管理

1. ユーザ登録とアカウント構造
   useradd ユーザ名
   フィールド1 2 3 4 5 6
   passwd ファイル ユーザ名:パスワード:ユーザID:ユーザ情報:ホーム:シェル
2. グループの登録、設定ファイル
   grouppadd グループ名
   フィールド1 2 3 4
   group ファイル グループ名:パスワード:グループID:グループユーザ
3. 所有権 ugo とアクセス権 rwx の設定
   chgrp、chmod、chown
4. ネットワークグループWeb編集グループの例

システム管理者の業務
サーバ環境を快適で安定な状態に維持するために

1. システムの監視
2. セキュリティー
3. バックアップとリストア
4. 障害時の対応
5. ソフトウェア管理
6. ユーザ管理
7. サーバ運営

システム管理者の業務
7. サーバ運営

■ 運用体制の構築
以下のことについて規約を定める。

1. ユーザ・グループのアカウント、アクセス権
2. 実施サービス（追加、修正、停止、削除、履歴の記録）
3. バックアップオペレーション
4. 機器（増設、変更、破棄、履歴の記録）
5. ログ監視オペレーション
6. 障害発生時オペレーション
7. 災害復旧訓練とマニュアルの作成
8. ユーザ対応（メンテナンス通知、障害対応）

次回の技術講習会は、

「Linuxを用いたインターネットサーバの構築」
－ PCの組み立てからサーバの運用まで －
第5回 9. 26(tue) WWW、ホームページ
講師 中村勝 さん