

9章 重要なシステムサービス

9.1 システム時刻の保守

9.1.1 システムクロックの表示と設定

- システムクロック : OSが管理
- ハードウェアクロック : BIOSが管理

コマンド	意味	設定の対象
date	システムクロックの表示・設定	システムクロック
hwclock	ハードウェアクロックの表示・設定	ハードウェアクロック
ntpdate, chronyc	NTPサーバーとシステムクロックの同期	システムクロック

date

```
date [オプション] [日時/+書式]

# 現在のシステムクロックを表示
date
    2023年  6月 20日  火曜日 18:05:29 JST

# システムクロックを1/1 00:00に変更
date 01010000

# 表示形式を変える
date "+%m%d"
    0620
```

```
# バックアップファイル作成時
tar cf /tmp/`date "+%m%d"` .tar /home
```

9.1.2 ハードウェアクロックの設定

hwclock

```
hwclock [オプション]

-r(--show)      :   ハードウェアクロックを表示
-w(--systohc)   :   ハードウェアクロックを、現在のシステムクロックと同期
-s(--hctosys)   :   システムクロックを、現在のハードウェアクロックと同期
```

9.1.3 タイムゾーンの設定

- 共通の時間帯を使う地域をあわらす言葉がタイムゾーン
 - 日本なら
 - UTC(世界標準時)
 - JSTあるいはAsia/Tokyo(日本標準時) : UTCと比べて + 9 時間
- タイムゾーンの設定は以下
 - TZ変数で設定

```
date
2023年  6月 20日  火曜日 18:10:43 JST
export TZ=UTC
date
2023年  6月 20日  火曜日 09:44:28 UTC
```

```
# 画面操作。設定できるタイムゾーンの値を表示(あくまで確認するだけ！)
tzselect
```

- /etc/timezoneを編集(**Debian**)
 - /etc/localtimeが存在する場合、そちらが優先される

```
cat /etc/timezone
Asia/Tokyo
```

- /etc/localtimeの参照先のファイルをtimedatectl コマンドで変更(**Cent OS+Debian**)

```
ls -l /etc/localtime
lrwxrwxrwx. 1 root root 32 11月  3  2022 /etc/localtime ->
../usr/share/zoneinfo/Asia/Tokyo
```

```
#上記を変更するなら
timedatectl [サブコマンド]

status                :   現在の設定を表示(サブコマンド省略時の動作)
set-time 日時          :   日時の設定を変更
set-timezone タイムゾーン :   タイムゾーンの設定を変更
```

```
timedatectl
Warning: Ignoring the TZ variable. Reading the system's time zone
```

setting only.

```
Local time: 火 2023-06-20 18:58:53 JST
Universal time: 火 2023-06-20 09:58:53 UTC
RTC time: 火 2023-06-20 08:08:27
Time zone: Asia/Tokyo (JST, +0900)
NTP enabled: yes
NTP synchronized: no
RTC in local TZ: no
DST active: n/a
```

9.1.4 NTPの利用（??）

- TCP/IPにはNTP(Network Time Protocol)がある
- システムクロックの設定に利用できる
- ntpdateコマンドで、ネットワーク上に配置されているNTPサーバ(ntpd)とシステムクロックを同期して設定可能

```
ntpdate [オプション] サーバー
```

```
-d : デバッグモードで実行
```

- **pool.ntp.org** pool.ntp.orgで、登録されている様々なNTPサーバのいずれかのアドレスを応答
- 自分自身をNTPサーバにする
 - /etc/ntp.conf

```
# 指定したホストに対してアクセス制御設定を行う。
# ホストには「ネットワークアドレス mask サブネットマスク」と指定すれば、ネットワークを対象可
# defaultと指定すると、ほかのrestrictで指定したアドレスに合致しなかった場合の設定になる
restrict [オプション] ホスト/default [値1...]

```

```
ignore : すべての要求を無視
```

```
# 同期先のサーバーを指定
server ホスト
```

```
# 指定したサーバと接続できなかった場合に参照するローカルアドレスとstratum値を指定
fudge ホスト stratum 値
```

- stratumはntpdの階層を表す
 - 1が最上位のサーバー、2、3・・・
 - 下位のサーバーが上位のサーバーに同期をとる
- ntpq
 - ntpdの状態を確認

```
ntpq [オプション] [サーバー]
```

```
-p : 同期の状態を表示。サーバー名の左の記号で状態を表す

* : 現在同期中のサーバー
+ : 同期の候補となっているサーバー
-i : 対話モードできどする (デフォルト)
```

9.1.5 chronyd (? ?)

- ntpdに変わる同期サービスとして**chronyd**が用意されている
 - ntpqと同じくNTPプロトコルを利用したシステムクロックの同期が可能
 - ハードウェアクロックとの同期もサポート
 - 既定ではntpdと同じく123番ポートを利用するがほかのポートを利用することも可能

サービス名	ntpd	chronyd
設定ファイル	/etc/ntp.conf	/etc/chrony.conf
同期確認に利用するコマンド	ntpqコマンド	chronycコマンド
◦ /etc/chrony.conf		

```
•server ホスト [値]
    同期先のサーバーを指定
•allow ネットワークアドレス
    接続を許可するNTPクライアントのネットワークを指定
```

```
# chronydの制御を行う
chronyc [サブコマンド]
```

```
tracking : 同期の状態を表示
sources  : 同期先として利用できるサーバーの一覧を表示
```

9.2 システムのログ

9.2.1 ログ管理サービス

- カーネルや各プロセスがjournaldにメッセージを出力
 - ファシリティとプライオリティを指定
- journald
 - バイナリログを出力
 - 既定では/run/log/journal/以下に出力
 - メモリ上に記録
 - journalctlコマンドで参照

- rsyslogd
 - テキストログを出力
 - /var/log/以下に出力
 - ディスク上に記録
 - /etc/rsyslog.confの内容に基づいて出力先を判断
 - grepコマンドやtailコマンドなどで参照

9.2.2 journaldによるログ管理

journalctl

journalctl [オプション] [条件]

```
-n(--lines) 数値          : 表示するログの件数 (デフォルトで10行)
-u ユニット名          : 表示する対象のユニット
-p プライオリティ値    : 表示するプライオリティ(0:emerg ~ 7:debug)

--since='日時'          : 日時を指定(sinceからuntilまで)
--until='日時'          :
    - 'yyyy-mm-dd hh:mm:ss'
    - 'hh:mm:ss'
    - today, yesterday
    - -1min, -1h, -1days

-f                    : 末尾をリアルタイム表示
-r                    : 逆順に表示
--list-boots          : 管理対象となっているブートIDを表示
-b 数値                : 指定したブートIDのログを表示。0で現在、-1で前回起動中のログを表示
--no-pager            : ページャーを利用せず、標準出力
-l(--full)            : 画面表示可能なすべてのログを表示
-a(--all)              : デフォルトでは表示されない文字も含めて表示
-o(--output)          : ログの出力形式を指定
-k(--dmesg)           : カーネルからのメッセージを表示
```

```
# 引数
_PID=数値      : 指定したPIDのプロセスのログ
パス           : 指定したパスのプログラムが出力したログ
_SYSTEMD_UNIT= : Unit名の指定 (-uと同じ)
```

- ファシリティ

ファシリティ	コード	出力元/意味
kern	0	カーネル
user	1	ユーザーアプリ関連
mail	2	メールシステム
daemon	3	システムのデーモン関連

ファシリティ	コード	出力元/意味
auth	4	認証情報
syslog	5	syslog関連
lpr	6	プリンタ関連
news	7	news関連
uucp	8	uucp関連
cron	9	cron関連
authpriv	10	認証情報
ftp	11	ftp関連
local0~7	16~23	独自に予約

- プライオリティ

ファシリティ	コード	出力元/意味
emerg	0	システムが利用不可な状態
alert	1	緊急に対応が必要
crit	2	致命的な状態
err	3	エラー
warning	4	警告
notice	5	通知
info	6	情報
debug	7	デバッグ情報
none		記録の対象外

- 設定ファイルは`**/etc/systemd/journald.conf`
 - 前回起動中のログを保存したい場合は、`**/var/log/journal/**`を作成する
- `journald`に任意の情報を出力したい場合

```
system-cat [オプション] コマンド構文
```

```
-p プライオリティ    :   プライオリティを指定して出力
```

9.2.3 rsyslogによるログ管理

- `journald`に送られたログメッセージは`rsyslogd`にも送られる

- 出力先情報は、**/etc/rsyslog.conf**
 - セレクタ
 - ファシリティとプライオリティの組み合わせ
 - アクション(出力先)
 - /var/log/messages -> ファイル
 - @192.168.1.100 -> 他ホストにUDPで転送(@@)はTCP
 - 既定の出力先
 - /var/log/messages : 一般ログ
 - /var/log/secure : 認証ログ
 - /var/log/maillog : メールログ
 - /var/log/cron : cronログ
- あるファシリティ、プライオリティが指定されたログメッセージが設定どおりにきろくされているかどうかを確認する

```
# テスト用のメッセージを送信
logger [オプション] メッセージ
```

```
-p ファシリティ . プライオリティ      : 指定されなければ、user.noticeで送信
-i                                     : PIDを記録
-t 名前                                : 指定した名前を出力元として記録
```

9.2.4 ログのローテーション

- /var/logのログファイルはlogrotateによりローテーションされる
- /etc/logrotate.confで管理

9.3 メール配送エージェント(MTA)の基本

9.3.1 MTAの基本

- MTA : メールを転送するSMTPサーバー
 - クライアントからSMTPにより、MTAにメール転送依頼(@example.com)
 - example.comのDNSサーバーにMXレコードを問い合わせ、転送先のメールサーバーを検索
 - SMTPにより、メールサーバへ転送
- Linuxで利用されるMTA
 - postfix
 - exim

9.3.2 メールの参照

- cronジョブなどが失敗したときにメールを送る

```
mail [オプション] [宛先]
```

```
-u ユーザ      :      指定したユーザのメールデータを参照(rootのみ実行可能)
```

-
- /etc/aliases はメールの転送先を設定する
 - postfixが参照するのは/etc/aliases.db
 - /etc/aliasesをいじったら、newaliasesコマンドで更新が必要
 - 一般ユーザがメール転送の設定を行う場合は、ホームディレクトリ内に.forwardファイルを作成。

mailq

- メールキューの内容を表示
- syslog-ng
- rsyslog
- /etc/chrony.conf
- ntp > peers
- ntpqコマンドの項目