特集2 Part3

これだけは知っておきたいシステムの運用管理

サーバーは構築して終わりというものではありません。24時間365日，安定してサービスを提供し続けることができるよう，日々のメンテナンスが欠かせません。ここでは，Linuxサーバーの運用管理とセキュリティ設定の基本を説明します。

中島 能和

システムの運用管理と一口にいっても，その内容は多岐にわたります。アプリケーションの管理はもちろんのこと，ユーザー管理，CPU（プロセサ）/メモリー/ハードディスクの監視，ログの確認など，ハードウエアとOSとアプリケーションに関する総合力が問われます。一朝一夕には身に付きませんが，ポイントを押さえて基本を学び，そこから対応力を広げていきましょう。

システムの運用と管理

それではユーザー管理から見ていきましょう。Part2で導入した仮想マシンを起動し，そのコンソール（シェル）にコマンドを入力して確認しながら読み進めてください。

ユーザー管理

システムを利用するユーザーが増えるごとに，ユーザー・アカウントを追加する必要が出てきます。ユーザーを追加するにはadduserコマンドを使います。次の例では，koalaユーザーを追加しています。

```
$ sudo adduser koala
```

するとパスワードなどを尋ねられますので，キーボードから入力してください。ここでパスワードは，確認のために2度入力します。

ユーザーのパスワードを後で変更したいときは，passwdコマンドを使います。

```
$ passwd koala
```

新しいパスワードを2度入力すると，パスワードの変更が完了します。

利用しなくなったユーザー・アカウントは，userdelコマンドを使って削除します。

```
$ userdel -r koala
```

これでユーザー・アカウントとユーザーのホーム・ディレクトリが削除されます。ホーム・ディレクトリを残しておきたい場合は，-rオプションを付けないで実行してください。

ちなみに，adduserと同様のコマンドにuseraddもあり，こちらはホーム・ディレクトリが自動生成されないなど，使い勝手が異なります。混乱しないように注意しましょう。

一般ユーザーとrootユーザーのパスワード

一般ユーザーは自分のパスワードのみ変更できますが，rootユーザーはすべてのユーザーのパスワードを変更できます。

また，一般ユーザーがパスワードを変更するときには，「短すぎないか」「辞書に載っているような単純な単語ではないか」「以前のパスワードと似すぎていないか」などがチェックされ，チェックに通らなかった簡単なパスワードは設定できません。

一方，rootユーザーの場合も同様にチェックされますが，たとえ単純すぎて不適切であっても警告だけにとどまるので，簡単なパスワードを設定できてしまいます。権限の大きいrootユーザーだからこそ，きちんとしたパスワードを設定するようにしましょう。

CPUの負荷状況を知る

サーバー・マシンのCPUの負荷状況を知りたいときは，topコマンドを使います。使い方は簡単で，topと入力するだけです。すると，**図1**のような画面が表示されて，「load average」欄にCPUによる実行待ちプロセス数の平均値が表示されます。左から1分，5分，15分間の平均値が示されており，これらの値が大きいほど，CPUの負荷が高いと判断できます。常時数値が大きくてシステムの動作が遅くなりがちなときには，CPUの負荷を減らす手立てを検討することになります。

topコマンドを終了するときは，「q」キーを押します。

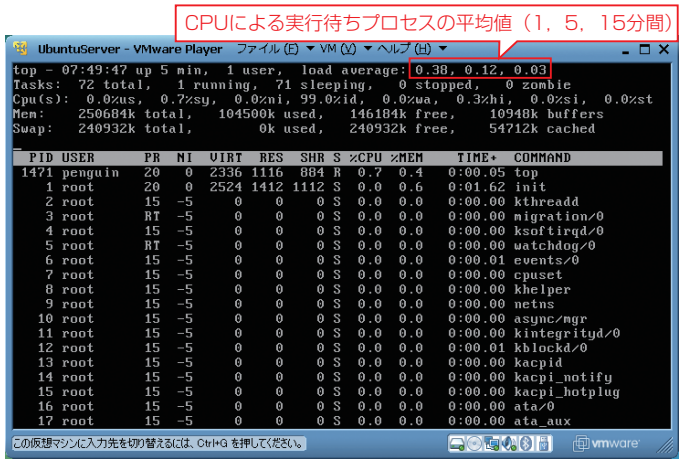

図1●topコマンドの表示例。「load average」欄には，待ち行列で待機してCPUの割り当てを待っているタスクの数，つまり実行可能状態だけれども，他のプロセスをCPUが処理しているために実行できないプロセスの数の平均値が示される

メモリーの正しい監視方法

システムのメイン・メモリー（以下，メモリー）の空き容量が不足し始めると，システム全体の動作が遅くなってしまいます。そのような兆候を感じたときには，空きメモリーの容量を確認しましょう。メモリーの状態を調べるには，**図2**のように，freeコマンドを実行します。

この例では，搭載されている物理メモリー（Mem行のtotal欄）が「250684」つまり約250Mバイト，使用中のメモリー（Mem行のused欄）が「240556」（約240Mバイト），空きメモリー（Mem行のfree欄）が「10128」（約10Mバイト）となっています。ただし使用中のメモリーには，ディスク・アクセスのパフォーマンスをよくするためのバッファ・キャッシュも含まれています。使用中のバッファ・キャッシュを除いた空きメモリーは「126144」（真ん中の行のfree欄）ですので，半分近くが空いています。

```
$ free
             total       used       free     shared    buffers     cached
Mem:        250684     240556      10128          0       9960     106056
-/+ buffers/cache:     124540     126144
Swap:       240932        272     240660
```

合計値の126144が空き

図2●freeコマンドの実行例

Linuxは空きメモリーがあると，できる限りバッファ・キャッシュに使います。Linuxを起動してしばらく時間が経過すると，一見メモリー不足に陥っているように見えますが，バッファ・キャッシュを差し引いた数値で判断してください。

また，物理メモリーが本当に不足しているようであれば，仮想メモリー領域であるスワップ領域が使われます。最下行のSwap行のused欄で，スワップ領域がどの程度使われているかを確認してください。

サーバーの稼働中にこうしてメモリーの状態を確認し，常時スワップ領域が多く使われているようなら，慢性的なメモリー不足状態にあると判断できます。こうしたときは，常駐しているソフトウエアを減らす，あるいはメモリーを増設するなどして対処します。

ディスクの空き容量不足を防止しよう

ハードディスク（以下，ディスク）の空き容量が不足し始めると，

ユーザーが新しいファイルを保存できなくなるばかりか，システムが定期的に出力するログ・ファイルを保存できなくなり，システム全体の動作にも支障を来たします。こうしたことがないよう，ディスクの空き容量については常に気を配るようにしましょう。

ディスクの空き容量を調べるには，dfコマンドを実行します（**図3**）。左端の列で「udev」や「none」となっている行は無視して構いません。この例では，ディスク容量の約24%が使われていて，2812040Kバイト（約2.8Gバイト）の空きがあります。-Hオプションを付けると，見やすい単位（MiB，GiBなど）で表示してくれます（**図4**）。

```
$ df
Filesystem     1K-blocks      Used Available Use% Mounted on
/dev/sda1        3889892    880256   2812040  24% /
udev              125340       192    125148   1% /dev
none              125340         0    125340   0% /dev/shm
none              125340        44    125296   1% /var/run
none              125340         0    125340   0% /var/lock
none              125340         0    125340   0% /lib/init/rw
```

図3●dfコマンドの実行例

```
$ df -H
Filesystem     Size   Used  Avail Use% Mounted on
/dev/sda1      4.0G   902M   2.9G  24% /
udev           129M   197k   129M   1% /dev
none           129M     0    129M   0% /dev/shm
none           129M    46k   129M   1% /var/run
none           129M     0    129M   0% /var/lock
none           129M     0    129M   0% /lib/init/rw
```

図4●-Hオプションを使ったdfコマンドの実行例

このようにして，ディスク容量を定期的に確認しながら，空き容量が少なくなってきたときには，不要になったファイルを消したり，ディスクを増設したりして対処しましょう。

サーバー・ソフトはスクリプトで起動/停止

サーバー・ソフトウエアの起動と停止は，/etc/init.dディレクトリ以下に配置されているスクリプトを使って操作します。例えば，SSHサーバーを起動するときは，

```
$ sudo /etc/init.d/ssh start
```

を実行します。「start」の代わりに「stop」なら停止，「restart」なら再起動を行います。「reload」で設定ファイルの再読込を行えるサーバー・ソフトウエアもあります。設定ファイルを変更したときは，サーバー・ソフトウエアの再起動か設定ファイルの再読込が必要です。

ログの確認

Linuxのログ（利用履歴）は，/var/logディレクトリ以下に，テキスト形式のファイルで保存されています。テキス

表1●主なログ・ファイル

ログ・ファイル名	説明
auth.log	認証関連のログ
mail.log	メール関連のログ
daemon.log	デーモン（サーバー・プログラム）のログ
syslog	システム・ログ（認証を除く）
messages	システム・ログ（認証，メール，cron，デーモンを除く）
dmesg	システム起動時のカーネル・ログ
kern.log	カーネルが出力するログ
user.log	ユーザー・プログラムが出力するログ
mysql.log	MySQLサーバーのログ
mysql.err	MySQLサーバーのエラー・ログ
apache2/access.log	Apacheのアクセス・ログ
apache2/error.log	Apacheのエラー・ログ

ト・ファイルなので，catコマンドやlessコマンドなどで閲覧できます*1。主なログ・ファイルは**表1**の通りです。

主要なログ・ファイルは，logrotateという仕組みにより，1週間単位で切り分けられます。例えば，messagesファイルであれば，「messages.1」「messages.2」というようにバックアップされていきます。ファイル名末尾の数字が大きいものほど，古いログファイルです。

logrotateのデフォルト（初期設定）ではバックアップ・ファイルは四つしか保存されない，という点に注意しましょう。つまり，5週間以上経過したログ・ファイルは削除されてしまいます。これを変更するには，/etc/logrotate.confファイルを編集します。「rotate 52」とすると，52週間，すなわちほぼ1年にわたってログ・ファイルのバックアップが保存されます（**図5**）。

Windowsからのリモート接続

手元のパソコン上で動いている仮想マシンであればシェルからコマンドを直接入力できますが，実際にはLinuxサーバーが近くにあるとは限りません。一般には，パソコンからネットワーク経由でログイン（リモート接続）して運用管理をすることになります。

リモート接続ではTelnetが有名ですが，平文（プレーン・テキスト）で通信するため，盗聴に対して無防備です。

そこで，Telnetに代わってSSH（Secure SHell）を利用します。SSHでは通信経路が暗号化されますし，多くのディストリビューションではSSHサーバーがデフォルトで動作しています。Windows側にSSHクライアントを導入すれば，簡単にアクセスしてLinuxサーバーを操作できます。

Windows用のSSHクライアントには，TeraTermやPoderosaなどのフリーソフトがあります。ここではTeraTermを使うことにしましょう。TeraTermは，Webサイト「http://sourceforge.jp/projects/ttssh2/」からダウンロードできます。2009年11月中旬時点での最新版は「teraterm-4.64.exe」です。ダウンロードしたファイルをダブルクリックするとインストーラが起動しますので，指示に従ってインストールしてください。

TeraTermのインストールが完了したら，リモート接続してみましょう。その前に先に紹介した「sudo /etc/init.d/ssh start」を仮想マシン上で実行してSSHサーバーを起動しておきます。

TeraTermを起動すると，**図6**のようなウィンドウが表示されます。

IPアドレスは，Ubuntu上でifconfigコマンドを実行して

```
# keep 4 weeks worth of backlogs
rotate 4          ← この数字を変更する
```

図5●設定ファイル/etc/logrotate.confの抜粋

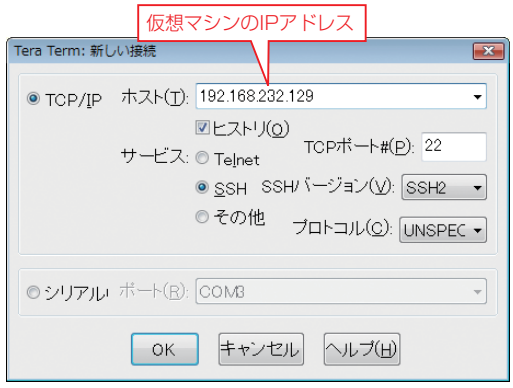

図6●TeraTermの接続先入力ウィンドウ

TeraTermを利用する場合の設定変更

今回使用している仮想マシンでは，Linuxコンソール上での文字化けを避けるため，言語環境を英語に設定しています。TeraTermからのアクセスでは日本語も問題なく表示されるため，TeraTermを利用する場合は，/home/penguin/.bashrcファイルの末尾にある「LANG=C」という行を削除してください。そのうえで1回ログアウトしてからもう一度ログインすると，日本語で表示可能な部分は日本語になるはずです。

*1 ディストリビューションによっては，管理者権限がなければ閲覧できないログ・ファイルもあります。

調べてください。初回接続時は，**図7**のようなセキュリティ警告ウィンドウが表示されますので，「続行」をクリックしてください。

次にユーザー名とパスワードを入力するウィンドウが出てきますので，正しいユーザー名とパスワードを入力するとログインすることができます（**図8**）。

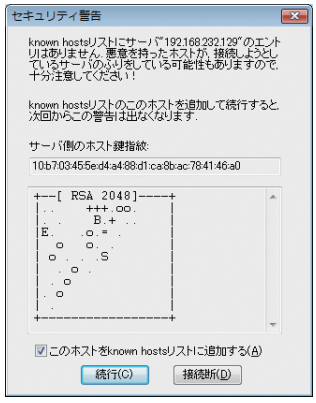

図7●初回接続時に表示されるウィンドウ

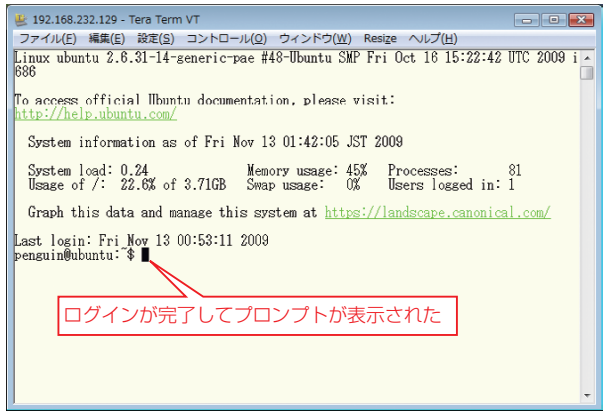

図8●TeraTermでログイン完了

システムのセキュリティ

サーバーを運用する以上，セキュリティ対策は不可欠です。ここで紹介する基本的なセキュリティ対策を実施するだけでも，システムの安全性は格段に向上しますので，ぜひ実行してください。

システムのアップデート

Windowsであれば，月に何度かインターネット経由でWindows Updateが行われ，システムの不具合が修正されて最新版になります。Ubuntuにも同様に，インターネット経由でシステムをアップデートして最新にする仕組みがあります。システムのアップデートは最初に取り組むべきセキュリティ対策の一つです。

Ubuntuでシステムをアップデートするには，次の二つのコマンドを続けて実行します。

```
$ sudo aptitude update
$ sudo aptitude upgrade
```

Windowsとは異なり，LinuxではOSのみならず，パッケージ管理システムを使ってインストールしたソフトウエアもアップデートされます。つまり，Apache HTTP ServerやMySQLなども更新対象です*2。

なお，自動的にシステムのアップデートを行うこともできますが，アップデート内容によってはシステムが再起動されます。そのためサーバーにおいては手動でアップデートした方がよいでしょう。

ファイアウォールの設定

ネットワーク通信を行う際の出入り口となるポート単位でアクセス制御する機能がファイアウォールです。

Linuxカーネルには，「Netfilter」というファイアウォール機能が搭載されており，iptablesコマンドやufwコマンドを使って設定できます。ufwコマンドの方が書式が簡単なので，ここではufwコマンドを使って設定しましょう。

Ubuntuでは，デフォルトではファイアウォールが無効になっています。ファイアウォールの設定は，

(1) 外部からのアクセスはすべて拒否する
(2) 指定したアクセスのみ許可する

という考え方で行うと，うっかり設定し忘れたポートを経由して攻撃されてしまうのを防げます。このように「すべて拒否しておいたうえで，必要なもののみ許可する」というのがセキュリティ設定の基本です。例えば，サーバー・アプリケ

アップデート方法はディストリビューションによる

システムをアップデートする仕組みは，ディストリビューションによっていくつかの種類があります。そのため，アップデートするときのコマンドがUbuntuとは異なる場合があります。例えば，RedHat系のCentOSやFedoraでは「yum update」コマンドを使ってアップデートします。また，アップデートの仕組みを持たないディストリビューションもあります。

*2 パッケージ管理システムを使わずにインストールしたソフトウエアはアップデートの対象外となります。その場合は個別にアップデート作業が必要です。

ーションにおいても，「すべてを停止したうえで不必要なものは削除し，必要なもののみ動かす」というのが原則です。

それでは，ファイアウォールを設定してみましょう。まずはファイアウォールを有効にします。管理者権限が必要なので，コマンドの前にsudoを付けます。

```
$ sudo ufw enable
```

次にデフォルトのアクセスをすべて拒否します。「deny」は拒否を表します。

```
$ sudo ufw default deny
```

ここから，許可するアクセスを指定していきます。許可するアクセスは，サービス名を指定するか，ポート番号とプロトコルの組み合わせで表現します。今回は，Webサーバーへのアクセスと，外部からのSSH接続を許可することにします。

```
$ sudo ufw allow 80/tcp
$ sudo ufw allow ssh
```

「allow」は「deny」の反対で許可を表します。これで，Webサーバー（80番ポート）へのアクセスとSSHサーバー（22番ポート）へのアクセスが許可されました。設定を確認するには，次のコマンドを実行します。

```
$ sudo ufw status
```

SSHサーバーのセキュリティ

SSHで誰でも接続できる状態にしておくのは，当然のことながら，セキュリティ上好ましいことではありません。システムにログインして作業をする必要のあるユーザーのみ，アクセスを許可しておくのがよいでしょう。それには，SSHサーバーの設定ファイルである/etc/ssh/sshd_configファイルに次の行を追加します*3。

```
AllowUsers penguin
```

このように記述すると，penguinユーザー以外はSSHでログインできなくなります。設定変更を反映させるには，SSHサーバーを再起動する必要があります。前述したように，/etc/init.dディレクトリにあるスクリプトを使って，SSHサーバーを再起動します。

```
$ sudo /etc/init.d/ssh restart
```

*3 設定の変更には管理者権限が必要です。

次のステップへ

ここまで仮想マシンを使って作業してきた皆さんは，Linuxでサーバーを構築する流れを大まかにつかめたのではないでしょうか。さらにスキルを高めるために何をすればよいか，いくつかアドバイスをさせてください。

オンライン・マニュアルを使う

ほとんどのLinux関連のコマンドには，マニュアル（オンライン・マニュアル）が付属しています。マニュアルはmanコマンドで表示します。例えばlsコマンドのマニュアルを見たければ，

```
$ man ls
```

を実行します（**図9**）。マニュアル表示中は，スペース・キーで次ページを表示できます。マニュアルの表示を終了するには「q」キーを押してください。

マニュアルは，日本語化されているものもあれば，英語しかないものもあります。また，コマンドのアップデートにマニュアルが追い付いていないことや，誤記が見られることもある点には注意が必要です。マニュアルをすみずみまで読む必要は全くありませんが，折に触れてマニュアルを読むようにすると，いつの間にかLinuxシステムの知識が身に付いてきます。

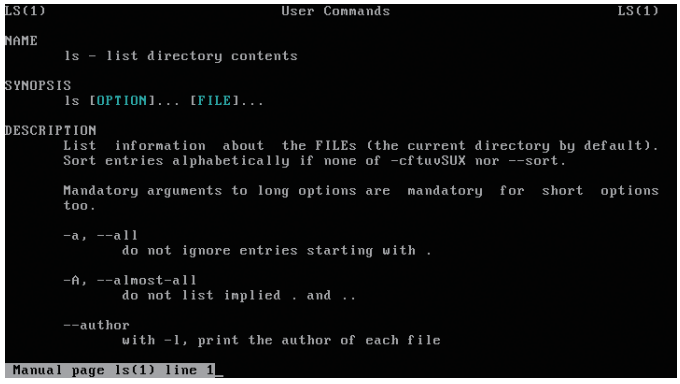

図9●lsコマンドのマニュアルを表示

ドキュメントを活用する

ソフトウエアをインストールすると，多くのケースではドキュメントも一緒にインストールされます。ドキュメントは/usr/share/docディレクトリ以下に，ソフトウエアごとに分けて格納されています。

例えばPHPであれば，/usr/share/doc/php5や/usr/share/doc/php5-commonディレクトリ以下に，READMEやサンプル・ファイルが格納されています。それらの多くはテキスト・ファイルですので，lessコマンドなどを使って閲覧してください。また，ディストリビュータのWebサイトにも多くの技術情報がありますので，それらを読んでみるのも参考になります。

表2●Ubuntu（Debian系）とCentOS（Red Hat系）の違いの例

項目	Ubuntu	CentOS
Apacheのパッケージ名	apache2	httpd
Apacheの設定ファイル	/etc/apache2/apache2.conf	/etc/httpd/conf/httpd.conf
Apacheの再起動	/etc/init.d/apache2 restart	/etc/init.d/httpd restart
SSHサーバーの再起動	/etc/init.d/ssh restart	/etc/init.d/sshd restart
ネットワークの再起動	/etc/init.d/networking restart	/etc/init.d/network restart
パッケージ管理コマンド	aptitude, apt-get	yum
パッケージ形式	debパッケージ	RPMパッケージ

表3●Linuxで使える主なサーバー・ソフトウエア

サーバーの種類	ソフトウエア名
Webサーバー	Apache HTTP Server，nginx，lighttpd
メール・サーバー	Postfix，exim4，sendmail
DNSサーバー	BIND
FTPサーバー	ProFTPD，vsftpd
Windowsファイル・サーバー	Samba
プリント・サーバー	CUPS
SSHサーバー	OpenSSH
LDAPサーバー	OpenLDAP

他のディストリビューションを使ってみる

今回サーバーを構築したUbuntuは，Debian GNU/Linux系のディストリビューションです。もう一つのメジャーなディストリビューションであるRed Hat系では，設定ファイルやパッケージ管理の仕組みなどが異なります（**表2**）。そのため，無償で使えるCentOS*4を使って，今回のサーバーと同様の構築作業をやってみると，Ubuntu固有の部分とLinux全般で一般的な部分が把握でき，応用力が高まるでしょう。

いろいろなサーバーを動かしてみる

Linuxサーバーで利用できる主なサーバー・ソフトウエアを**表3**に示します。必要なもの，あるいは興味のあるものから試してみるとよいでしょう。

なかでも実用性が高いのは，ファイル・サーバーでしょう。Sambaを利用すると，Windows互換のファイル・サーバー（およびプリント・サーバー）を構築することができます。残念ながらActive Directoryへの対応は不完全ですが，一般的なファイル・サーバーとしては十分でしょう。

資格試験を活用してみる

Linuxの資格試験としてスタンダードとなっているのは，カナダに本拠地を持つ非営利組織LPI（Linux Professional Institute）が実施しているLPI認定試験（LPIC）です。レベル1からレベル3が実施されており，レベル1はLinux初級ユーザー，レベル2はサーバー管理者を想定しています。試験範囲は，Linuxユーザーに必要と考えられる技術分野を網羅しているので，LPI認定試験の出題範囲を一通り学習すれば，Linuxの基礎的な素養が身に付くことになります。資格試験は，未知の分野を効率よく学習するツールとしても活用できるのではないでしょうか。

*4 CentOSは，Red Hat Enterprise LinuxからRed Hatの知的所有物（ロゴ・マークなど）を除いて再構成した「クローン（互換）OS」の代表格です。