Linux VPS で実現する堅牢サーバ［ファイアウォール管理編］

第1回 Linux VPSの紹介

今回から3回にわたり，Linux VPS上でのサーバ構築，とくにファイアウォール管理にフォーカスした内容でお届けします．第1回目は，Linux VPSの概要および基本機能について紹介します．

テキスト＝編集部 Software Design

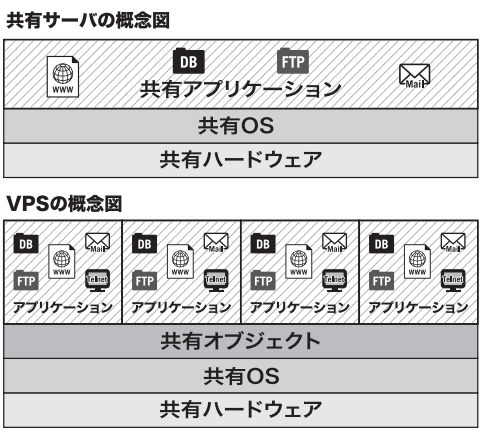
VPSとは？

VPS（**Virtual Private Server**）とは，**1**つのサーバの仮想マシン内に複数の実行環境を設けて，それぞれの環境に仮想の**root**権限が付与される，仮想専用サーバと呼ばれるものです．

一番のメリットは，**1**つのサーバマシン上でほぼ制限なく，リソースを分割できる点です．最近では，レンタルサーバ／ホスティングサービス事業において，**VPS**を利用したものが増えてきました．

第**1**回目の今回は，基本の解説として，レンタルサーバ／ホスティングサービスとしての**VPS**という視点から，メリットや機能について解説します．

図1　共用サーバとVPSの比較



VPSのメリット

具体的には**VPS**にどういったメリットがあるのか，共用サーバ／専用サーバと比較して解説します．

■共用サーバと比較して

共用サーバの場合，**VPS**と同じく**1**台のサーバ上で複数のアプリケーションが実行できます．しかし，**VPS**と一番違うのが，アプリケーションの実行に関して**root**権限が**1**つということです．

そのため，サーバの各種設定変更や複雑な**Web**アプリケーションの実行が行えないだけではなく，複数アプリケーションが動いている場合，思わぬところにセキュリティホールが発生する危険性があります．

その点，**VPS**の場合，仮想の**root**権限を各ユーザ領域ごとに付与できるため，実行環境を複数化でき，それぞれにおいて個別の設定，アプリケーションの実行を行えます．また，**root**権限の乗っ取りのような危険を避けることができます（図**1**）．

■専用サーバと比較して

続いて，専用サーバと比較してみます．

専用サーバの場合，**1**台のサーバすべてを使えるため制限なくサーバ構築／運用が行えます．唯一，ユーザにとって大変なのが，管理／保守です．一般的に専用サーバでは，**root**権限の付与と同時にユーザにすべて管理／保守まで任せます．そのため，**OS**や各種アプリケーションに関して，セキュリティパッチがでた場合は各自で対

応しなければなりません．また，外部からのセキュリティ保守に関しても，ユーザ側で対応する必要があります．

このように，ユーザ側にスキルが求められる点が，専用サーバ利用で注意すべきポイントとなります．

VPSでは，実際の実行サーバは1台で，レンタルサーバ／ホスティングサービスベンダ側で管理／運用を行っています．そのため，OSやベースとなるアプリケーションなど，基本的なソフトウェアの管理はベンダ側に任せることが可能です．

さらに，料金面でも1台分はかからず，共用サーバと同じように複数ユーザでシェアすることが可能です．

VPSの実行環境

続いて，VPSが稼働するプラットフォームについて解説します．

■ FreeBSD上での実行環境

数年前まで，VPSを利用するためにはOSとしてFreeBSDを採用する必要がありました．これは技術進歩の経緯によるもので，元々VPSはIserverという会社が開発し，IntelベースのBSDiのUNIX（BSD/OS）上で稼働していました．その後，1999年にFreeBSDに移行され，2000年にSolarisへ移行という経緯を経ています．

■ Linux上での実行環境

一方，Linux上でのVPSも開発され，現在は実用レベルにまで達しています．とくに，SWsoftが開発したVirtuozzoを利用したものがよく使われています．現在，Virtuozzoのオープンソース版としてOpenVZ（http://openvz.org/，図2）があります．

本稿では，最近主流になってきているLinux VPS上で，ファイアウォールの管理について紹介します．

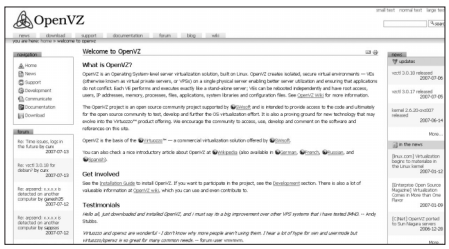
Linuxの汎用性を活かした仮想サーバ

通常のLinuxと同じ扱いが可能

Linux VPSのメリットは，何と言ってもサーバOSとしてデファクトスタンダードの1つとなったLinuxの技術をそのまま活用できる点です．

たとえば，LAMPと呼ばれるWeb＋DBシステムを構築する場合，Linux VPSであれば，自作サーバと同じように，Apache，MySQL，PHP／Perlを活用することができます．その他，Linuxで使われている各種コマンドをそのまま利用可能です．

図2 OpenVZの公式サイト



学習コストを抑えられる

さらにLinuxの場合，各種メディアにより豊富な情報が提供されています．加えて，利用シーンが多いことから，スキルを持った技術者もたくさんいます．これは，裏を返せば管理者の学習コストの軽減につながります．

◆◆◆

前述の専用サーバとの比較でも挙げたように，ホスティングサービスを利用すれば全体的な管理はベンダに任せることができます．このように，ホスティングサービスでのLinux VPSは，非常に高いポテンシャルを持ち，さまざまなシーンでのサーバ構築／運用管理に適しています．まとめると，

- サーバ管理の専任者を配置できない中小企業
- ECなど，通常の情報提供以上のWebサービス／サイト運用をしたい企業／ユーザ
- 複数のドメインによるWebサイト運用をしたい企業／ユーザ

といった方たちにお勧めのサービスです．

本連載では，このLinux VPSホスティングサービスの中でも，ラピッドサイトが提供する「RV-7シリーズ」（http://www.rapidsite.jp/product/vps/rv7/）にフォーカスを当て，解説します．

RV-7シリーズの紹介

まず始めに，RV-7シリーズの特徴について紹介します．

- RV-7シリーズ

http://www.rapidsite.jp/product/vps/

OSにRed Hat Enterprise Linux 4を採用

OSにはRed Hat Enterprise Linux 4（RHEL4）を採用し，独自カスタマイズによる仮想サーバ環境を実現し

図3　RV-7で使用できるコントロールパネル

図4　OpenPNE

表1　プランごとの基本仕様

プラン名	RV-722	RV-723	RV-731	RV-732	RV-733
OS	Red Hat Enterprise Linux（RHEL 4）				
CPU	Intel Xeon 2.8GHz×2（Dual）共有				
メモリ	8Gバイト　共有				
データセンター	米国（34Gbpsバックボーン）		国内（127Gbpsバックボーン）		
ディスク容量（単位バイト）	20G	40G	10G	20G	40G
データ転送量（推奨値）	無課金（200GB／月）	無課金（400GB／月）	無課金（100GB／月）	無課金（200GB／月）	無課金（400GB／月）

ています．

RHELは，多くの企業／組織で使用されているLinuxディストリビューションで，企業ユースとしては非常に豊富な実績を持っています．RV-7では，RHELで使用できるコマンドをそのまま使える他，別途用意されているコントロールパネル（図3）による簡易的な操作での管理も行えます．

ファイアウォール機能で安全な環境を構築

RV-7は，iptablesを利用したファイアウォールの実装／管理を行えます．プランごとに100／200／400ルールを設定でき，規模や目的に応じたサイト運用が可能です．詳しくは，次回，次々回で解説します．

バーチャルホストを利用してIPアドレスの追加が可能

サイトの規模や用途によっては，複数のIPアドレスが必要な場合があります．RV-7では，バーチャルホストを利用してIPアドレスの追加および複数ドメインの管理＋独自認証SSLの実装が可能です．

豊富なアプリケーションを標準で用意

運用という視点で見た場合，最も大きな特徴となるのが標準で用意されている豊富なアプリケーション群です．RV-7では，目的に応じてさまざまなアプリケーションが標準実装されています．たとえば，次のようなアプリケーションが使えます．

■blog：Movable Type

blogツールは，シックス・アパートが提供する「Movable Type」が用意されています．標準モデルでは，1ユーザライセンスが使用可能です．

■SNS：OpenPNE

mixiをはじめさまざまなシーンで活用が広がるSNS．RV-7は，オープンソースのSNSツール「OpenPNE」が標準実装されています（図4）．オープンソースのツールのため，目的に応じてさまざまなカスタマイズが可能です．

■Wiki：Pukiwiki

まとめサイト，コラボレーションツールとして期待されているWikiに関しては，PHPベースの「Pukiwiki」が標準で用意されています．そのまま使用可能な他，PHPやDBと連携した高機能Wikiへカスタマイズすることも可能です．

■グループウェア：Aipo

営業や総務といった部署で必要となるグループウェアに関しては，㈱エイムラックが提供するAipoを用意しています（RV-731を除く）．ユーザライセンスは別途有償となります．

◆◆◆

その他，最大40Gバイトまでのディスクスペースの利用，RV-723／RV-733のプランではJavaの実行環境

に対応しています．これにより，Javaによる Webアプリケーションサーバ構築も可能です．

プランごとの基本仕様は表1を参照の他，http://www.rapidsite.jp/product/vps/rv7/plan.html をご覧ください．

Vコマンドによる独自管理

最後にVコマンドについて解説します．Vコマンドは，Linux VPS特有のコマンド群で，アプリケーションの追加，ユーザ管理などを行うためのものです．管理者にある程度のスキルがあり，幅のある管理を行いたい場合は，コントロールパネルだけではなく，これらVコマンドを使った管理を行うと便利です．

おもなコマンドは以下のとおりです．

vadduser

vadduserは，ユーザの設定を行うためのVコマンドです．たとえば，sdmemberというユーザ名でtcshを使う場合，図5のように実行します．

vedituser

vedituserはサーバ内に登録されているユーザ情報を編集するためのコマンドです．図6のように使用します．

これ以外にも，事前に用意してあるアプリケーションソースを展開し，VPSサーバにインストールする「vinstall」や，vinstallでインストールしたアプリケーションを削除する「vuninstall」など，さまざまなVコマンドが用意されています．詳しくはhttp://www.rapidsite.jp/support/manual/rv7/c_179.html などをご覧ください．

次号は

以上，Linux VPSのメリット，そしてホスティングサービスとしてみた場合の例として，ラピッドサイトの「RV-7」シリーズを紹介しました．

次号以降では，もっと具体的な活用ノウハウとして，RV-7シリーズをベースとしたサーバ運用管理，とくにファイアウォールの活用について紹介していきます．SD

RV-7シリーズ
http://www.rapidsite.jp/product/vps/rv7/

問い合わせ先	ラピッドサイト
TEL	03-6415-6226
問い合わせフォーム	https://www.rapidsite.jp/form/contact/info/

図5 vadduserの実行例

```
# vadduser
Enter login: sdmember
Enter password: ********  ←初期パスワード
Enter password (again): ********  ←初期パスワードの確認
Enter full name: Software Design  ←名前
Enter home directory [/home/sdmember]: [ENTER]  ←そのまま ENTER

/bin/sh /bin/bash /sbin/nologin /bin/tcsh
/bin/csh /bin/ksh /usr/bin/ksh /usr/bin/pdksh

Select a shell [/sbin/nologin]: /bin/tcsh  ←tcshを選択
Allow mail? [n]: y  ←メールの許可
Allow ftp? [n]: y  ←FTPの許可
Enter quota (MB): 200  ←ディスク容量を200Mバイトに設定
…
```

図6 vedituser

```
# vedituser
Enter username to edit: sdmember  ←変更したいユーザ名

Now, enter the full name for this account.

Full Name: [Software Design]: Software Design New  ←Software Design Newに名前を変更

Please select the services that this account will be using:

ftp FTP services
mail Email services
shell shell login

Enter the service name (e.g., “ftp”, “mail”, etc.) to toggle that service for
the account. Hit when you are done selecting/deselecting services for
this user.

Select/deselect services [ftp mail shell]: ftp  ←FTPの使用を禁止
Select/deselect services [mail mail]: [ENTER]

Enter filesystem quotas for this user. The quota should be an integer
(no decimal fractions) in megabytes (e.g., 5 = 5 megabytes). Enter 0
for no quota.

Quota (in megabytes) [25]: 300  ←使用可能容量を300Mバイトに増加
Account setup complete.
```