Linux VPS で実現する堅牢サーバ［ファイアウォール管理編］

第2回 Linux VPSでファイアウォール【基礎編】

今回から2回に分けて，ラピッドサイトのVPSサービス「RV-7」シリーズ上でのファイアウォール構築／管理について解説します．まずは，iptablesの基礎について紹介します．

テキスト＝日吉 龍 HIYOSHI Ryu

Linux VPSでのファイアウォールの構築

VPSの概要は前回（本誌**2007**年**9**月号），すでに解説しましたが，一言で言うならば“共有サーバ上に構築された，それぞれが**root**を持つことができる仮想的な**OS**環境”ということになります．これを聞くと，次に“それではネットワークはどのようになっているのだろう？”という疑問を持つ方がいるかもしれませんが，結論から言えば普通の**Linux**マシンと何ら変わるところはありません．

NICが仮想化されており，それに伴う細かい差異はあるものの，ネットワークを利用するアプリケーションから見れば，**VPS**環境であることを意識する必要はまったくありません．

本稿では，**iptables**を利用したファイアウォール構築の基礎を紹介しますが，内容はラピッドサイトの「**RV-7**」シリーズの**VPS**環境を利用して評価／検証した内容に基づいております．**RV-7**シリーズ特有の要素もありますので，注意してください．

iptablesとは

iptablesとは，それが動作しているホストに入出力されるパケットをどのように処理するかを司るソフトウェアです．複数のネットワークの境目に設置されている**Linux**サーバで**iptables**を利用すれば，**Linux**サーバをルータとして機能させることもできますし，複雑な**NAT**処理を行うこともできます．

本稿で想定する**VPS**環境である**RV-7**シリーズは**Web**などの各種サーバであるため，ルーティング機能や**NAT**機能は必要ありません．必要とされるのは，とくにパケットの受領時にパケットを取捨選択する機能で，その機能を利用してファイアウォールを実現します．

iptablesの概念モデル

すでに述べたとおり，**iptables**の処理対象は，ホストに入出力されるパケットになります．**iptables**では，“テーブル”と“チェイン”という**2**つの概念を組み合わせて，パケットの処理を行っています．

“テーブル”は事前定義済みで，**iptables**を利用する目的に応じたテーブルを選択して利用することになります．**filter**，**nat**，**mangle**の**3**テーブルが定義されており，ファイアウォールとして利用する場合は，**filter**テーブルを利用することになります．

“チェイン”は，具体的にパケットの処遇を決める“ルール”の集合体で，基本的に定義済みのチェインを利用することになります[注1]．また，チェインごとにパケットを処理する過程のどのタイミングで適用されるかが決まっています（図**1**）．“**ROUTING**判断”というボックスは，**iptables**が内部的に行う固定の処理で，ユーザ側では制御できないので気にする必要はありません．

注1：自分でチェインを定義することもできるが，そこまでやらなければならないような状況は，ほとんどないだろう．

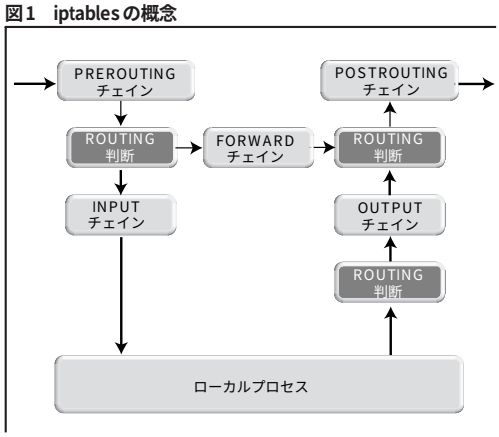
利用できるチェインはテーブルごとに決まっています．テーブルの役割とそれぞれのテーブルが利用できるチェインを表1に，それぞれのチェインの意味を表2にまとめましたので，参考にしてください．

iptablesの操作

ここまでの解説で，どのようなパケットに，どのタイミングでどのチェインが適用されるかのイメージが掴めたと思います．あとは，それぞれのチェインが適用されるタイミングでiptablesに行わせたい挙動を，“ルール”として記述するだけです．

iptablesはルーティングやNAT変換を行うことも可能であるため，膨大なオプションが用意されています．ファイアウォールとして動作させる場合に関係するのはその一部ですが，それらを解説するだけでも，かなりの誌面を費やすことになるため，ここでは実際に設定を行う手順に沿って，必要最低限の解説のみを行うこととします[注2]．

図1　iptablesの概念



現状の確認

先に紹介したとおり，今回利用したVPS環境は他者の手により構築された環境なので，まず現在の設定を確認します．実行結果を図2に示します．

-t（--table）は，表示対象とするテーブルを指定するオプションで，ファイアウォールとして利用する場合はfilterテーブルを指定することになります．-L（--list）オプションが，現在の設定内容をリストとして表示するというオプションです．最後の-n（--numeric）は，IPアドレスやポート番号を数字として表示するように指定するオプションです．

RV-7のVPS環境では，デフォルトでは何のルールも設定されていないため，何も表示されません．すべてのチェインに“policy ACCEPT”とありますが，これは任意のパケットがチェインの中のいずれのルールにも合致しなかった場合に適用される処置を示しています．この場合は“ACCEPT”，つまり受け取ることに

図2　iptables環境の確認

```
# iptables -t filter -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

表1　テーブルの役割と使用できるチェイン

テーブル名	使用可能なチェイン					役割
	INPUT	OUTPUT	FORWARD	PREROUTING	POSTROUTING	
filter	○	○	○			デフォルトのテーブル．パケットのフィルタを行う際に利用する
nat		○		○	○	NAT変換を行う際に利用するテーブル．アドレスの書き換えを行うルールが使用可能
mangle	○	○	○	○	○	特殊なパケット変換に利用するテーブル．たとえば，TOS（Type Of Serivce）フィールドを換えれば，QoSを実現することが可能

表2　チェインの意味

チェイン名	適用対象／タイミング
INPUT	iptablesが動作しているマシン自体がパケットを受け取った際に適用される
OUTPUT	iptablesが動作しているマシンがパケットを生成した際に適用される
FORWARD	iptablesが動作しているマシンをパケットが経由する際に適用される
PREROUTING	iptablesが動作しているマシンがパケットを受け取った直後に適用される
POSTROUTING	iptablesが動作しているマシンがパケットを送り出す直前に適用される

注2：その膨大なオプションについては，manを参照していただきたい．Webで検索すれば，全文の日本語訳もあるが，日本語でもすべてを把握するのに一苦労するほどのボリュームがある．

なります．

この状態では，いずれのチェインにもルールが**1**つも設定されておらず，チェインのデフォルトの処置が“**ACCEPT**”になっているため，受領するパケットについても送出するパケットについても，一切フィルタリングは行われないということになります．

チェインへのルールの追加

それでは，実際にチェインへのルールの追加を行ってみましょう．ここでは，**RV-7**の**VPS**環境でデフォルトでオープンしているポートのうち，使用頻度が非常に低いと思われる**pop3s**が利用する**995**番ポートを閉じるルールを記述してみます．

これから解説する一連の作業を図**3**にまとめてありますので，そちらを参照しながら読み進めてください．

iptablesのルール設定状態と，作業対象ポートの状態を確認してから，実際のルール追加作業に入ります．**-t**で**filter**テーブルを指定するのは同じですが，続いてルールを追加するオプションである**-A**（**--append**）が，そして追加先のチェインとして**INPUT**チェインが指定されています．それ以降が

図3　チェインへのルールの追加

```
■作業前の状態を確認する．何もルールは設定されていない
# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

■NMAPで995番ポートの状態を確認
# nmap localhost -p 995

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2007-08-19 11:14 JST
Interesting ports on test-gihyo1.rsjp.net (127.0.0.1):
PORT    STATE SERVICE
995/tcp open  pop3s          ←995番ポートはオープンしている

Nmap finished: 1 IP address (1 host up) scanned in 0.016 seconds

■995番ポート宛てのパケットをDROPするルールをiptablesに追加する
# iptables -t filter -A INPUT -p tcp --dport 995 -j DROP

# 追加したルールが反映されていることを確認
[root@test-gihyo1 ~]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:995

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

■NMAPで995番ポートの状態を確認
# nmap localhost -p 995

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2007-08-19 11:14 JST
Interesting ports on test-gihyo1.rsjp.net (127.0.0.1):
PORT    STATE    SERVICE
995/tcp filtered pop3s  ←ステータスが"open"から"filtered"に変化した

Nmap finished: 1 IP address (1 host up) scanned in 2.024 seconds
```

フィルタしたいパケットにマッチさせるための基準を指定するオプションで，-p（--protocol）でプロトコルとしてTCPを，--dport（--destination-port）で宛先ポート番号として995番を指定しています．最後に，この条件に合致したパケットの処遇が-j（--jump）というオプションで“DROP”と指定されています[注3]．

エラーが出ずに終了すれば，指定したチェインに指定したルールが追加されたことになります．ルールの一覧に今追加したルールが表示されており，外部から見たそのポートの状態が変化していることが確認できます．

ルールの保存

一般的なルータもそうですが，iptablesでは明示的に“ルールの保存”という作業を行わないと，次回起動時に設定した内容が反映されないようになっています．設定したルールの保存は，図4の手順で実施します．

保存したルールは/etc/sysconfig/iptablesに保存され，iptablesが再起動された際に再度読み込まれるようになります[注4]．

iptablesの活用

以上がiptablesをファイアウォールとして利用する際の基本中の基本になります．あとは，さまざまなオプションを駆使して，自分の望むパケットフィルタルールを実現するだけです．

実用レベルで設定を行う場合，注意しなければならない点はいろいろありますが，まずデフォルトのポリシーを“DROP”に設定してから，通過を許可するパケットについてのルールを1つずつ記述するようにしてください．この場合，戻りのパケットについても明示的に許可する必要があるので，忘れないようにしてください．

set_fwlevel

“正直，iptablesを自分で設定するのは面倒くさいなぁ”と思われた方もいるかもしれません．実際，さまざまなサービスが起動しているサーバの状況に合わせて適切なフィルタリングを設定するのは，かなりのネットワークに関する知識があっても容易ではありません．

RV-7シリーズでは，“set_fwlevel”というiptablesの設定スクリプトが用意されており，サーバの利用目的に応じて簡単にiptablesを設定することができるようになっています．具体的な設定内容などはhttp://www.rapidsite.jp/support/manual/rv7/e_1245.htmlに記載されていますが，セキュリティに明るい人でも簡単には設定できない，ポートスキャン対策やDoS対策まで盛り込まれており，iptablesの設定例として非常に勉強になります．

RV-7シリーズを利用するのであれば，一度は有効にしてみてその設定内容を吟味してみることをお勧めいたします．自分でゼロからiptablesを設定する場合であっても，必ず参考になる部分があるはずです．

最後に

今回はかなり駆け足でiptablesの概要を解説しましたが，最終回となる次回では，具体的なLinux VPSサーバの利用シーンに合わせた設定例と，その解説を行う予定です．SD

図4　設定したルールの保存

```
# /etc/rc.d/init.d/iptables save
Saving firewall rules to /etc/sysconfig/iptables:          [  OK  ]
```

注3：パケットの処遇がjumpというオプションで記述される書式になっていることに違和感を感じた方もいるはずだ．ここでjumpという言葉が使用されているのは，“DROP”や“ACCEPT”のような定義済みの処理に加えて，ユーザが定義した別のチェインを引数として指定することもできるためである．
注4：実際にファイルを参照してみればわかるが，iptables専用の書式になっているため，可読性は今一つである．直接編集することもできなくもないが，コマンドを列挙した起動スクリプトファイルを別途用意するほうが，管理しやすいだろう．