Linux VPS で実現する堅牢サーバ［ファイアウォール管理編］

第3回 Linux VPSでファイアウォール【実践編】

今回はいくつかのシーンを想定して，実際にラピッドサイトの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．

テキスト＝日吉 龍 HIYOSHI Ryu

はじめに

前回はiptablesの基本的な考え方と設定方法について解説しましたが，今回は実際のLinux VPS（以下VPS）の利用環境を数パターン想定し，それぞれのパターンに応じたiptablesの設定を解説していきます．

ルール設定時の考え方

iptablesのルールを検討する場合，ゼロから考えると混乱してしまう場合があります．それほど複雑ではないルールを記述する場合であれば，次の3つの部分に分けて考えるとわかりやすいでしょう．

VPSをサーバとして利用するためのルール

当然ではありますが，利用を許可するサービスに応じて許可する通信も変わるので，こちらがiptablesを設定する際の肝になります．目的達成に必要なサービスを見極め，それらに関わる通信を最低限の相手に対して許可するのが理想になります．

また，外部に公開するサービスとは別に，管理者が管理作業を行うためのルートも忘れずに確保しておく必要があります[注1]．

VPSをクライアントとして利用するためのルール

意外と忘れられがちですが，VPSをクライアントとして利用することも少なくありません．たとえば，ソフトウェアをダウンロードするのであれば，外部へのHTTPやFTP，DNSクエリなどを許可する必要があります．

ファイルであれば管理者がサーバに送り込めばいいかもしれませんが，提供するサービスのしくみ上，どうしてもVPSから外部へのアクセスを許可する必要がある場合もあります[注2]．

使用用途にかかわらず，つねに設定する共通ルール

要件が明確であれば，上記2つについては誰が設定してもそれほど大きな差は発生しません．技量の差が出るのはその他の部分で，たとえば前回（本誌2007年10月号）簡単に紹介したset_fwlevelというスクリプトには，ネットワークに詳しい人でも設定が難しいDoS攻撃やポートスキャン対策，重要なイベントのログ取得などが組み込まれています．

これらについては本稿では採り上げることができませんが，Web上にさまざまな情報があるので，余力があったら研究してみると良いでしょう．

注1：RV-7シリーズには，さまざまな管理作業をWeb経由でできるコントロールパネルが用意されているので，こちらとコンソールとを併用することになるだろう．
注2：たとえば，公開するWebサーバにblogを設置するのであれば，トラックバックを送るために外部へのHTTPやDNSクエリを許可する必要があるだろう．

VPSの利用環境

VPSは，実際にどのような環境で利用されるのでしょうか？ 改めて，**VPS**の代表的な特性について考えてみましょう．

- **仮想専用環境ではあるものの，共用環境であることには違いなく，各種リソースなどに論理的な制約が設けられている**
- **root権限があるため，一般の共用サーバよりもはるかに自由度が高い**
- **基本的にホスティングサービスになるので，機器の運用管理は意識する必要がない**

以上から考えると，高い処理能力を必要としないような用途で，インターネット上に低コストでサーバを持ちたい場合に，有力な選択肢になるのではないでしょうか．本稿では，公開されている実ユーザの利用方法などを採り上げ，それぞれでの**iptables**の設定を考えてみることにします．

一般的な外部公開用 Web サーバ

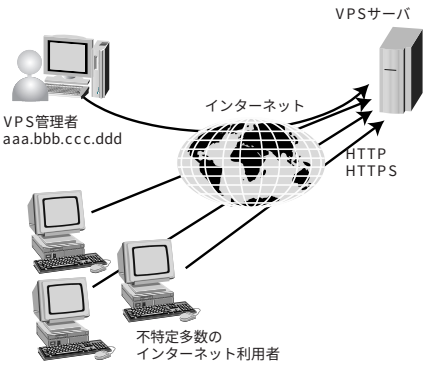
最も基本的な用途が，外部公開用の**Web**サーバとしての利用です．このような用途であれば一般的な共用サーバが第一候補に挙がりますが，メールアドレス数無制限，潤沢なディスク容量，高い自由度などに魅力を感じれば，**VPS**も有力な選択肢になるでしょう．

■設定するルールのポイント

一般的な**Web**サーバとして利用する場合，求められる要件は多くはありません．図**1**のように，管理者からのすべての通信と，不特定多数からの**Web**サーバへの閲覧を最低限許可することになるでしょう[注3]．これだけであれば**iptables**の設定も比較的にシンプルで，リスト**1**のようになります．

VPSがクライアントになる通信については，**VPS**→インターネットを無条件で許可するルールを記述した

図1　外部公開用Webサーバとして利用する例



リスト1　ルール設定例（外部公開用Webサーバ）

```
# 1. ループバックインターフェースについては無条件ですべてを許可する
iptables -t filter -A INPUT -i lo -j ACCEPT
iptables -t filter -A OUTPUT -o lo -j ACCEPT

# 2. VPS -> 外部へのすべての通信を許可する
iptables -t filter -A OUTPUT -m state --state NEW,ESTABLISHED -j ACCEPT

# 3. 管理者のIPアドレス -> VPSへのすべての通信を許可する
iptables -t filter -A INPUT -s aaa.bbb.ccc.ddd -m state --state NEW,ESTABLISHED -j ACCEPT

# 4. 外部 -> VPSへのHTTP/HTTPSを許可する
iptables -t filter -A INPUT -p tcp --sport 1024: -m multiport --dports http,https -m state --state NEW,ESTABLISHED -j ACCEPT

# 5. 必要に応じてVPSがクライアントになる通信の戻りパケットを許可する
# iptables -t filter -A INPUT -p tcp -m multiport --sports http,https -m tcp --dport 1024: -m state --state ESTABLISHED -j ACCEPT
# iptables -t filter -A INPUT -p tcp --sport 53 --dport 1024: -m state --state ESTABLISHED,RELATED -j ACCEPT
# iptables -t filter -A INPUT -p udp --sport 53 --dport 1024: -m state --state ESTABLISHED,RELATED -j ACCEPT
# iptables -t filter -A INPUT -s 0.0.0.0/0 -p udp -m udp --sport 123 -j ACCEPT
# iptables -t filter -A INPUT -p tcp -m tcp --sport smtp -m state --state ESTABLISHED -j ACCEPT

# 99. チェインポリシーをDROPにし，明示的に許可されていない通信を拒否する
iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP
```

注3：ここでは，管理者からのアクセスかどうかを接続元IPアドレスで識別できると想定している．

うえで，戻りのパケットを許可するルールを必要に応じて追加する形にしてみました．戻りパケットを許可するルールの例（**HTTP**, **HTTPS**, **DNS**クエリ, **NTP**, **SMTP**）を載せておきますので，参考にしてください．

社内サーバ

ASPサービスが一般的になった今，インターネット上にあるサーバを自社に置かれているサーバと同じ位置付けで利用することは決して珍しくなくなりました．自前でサーバを運用するのに比べると，電源や設置場所の確保，機器購入や構築，運用管理や保守といった，数々の手続きと手間を省くことができるため，メリットは少なくありません．

しかし，インターネット上に社内向けのデリケートな情報を置くことになるため，とくに接続を許可する接続元の設定は，十二分に注意をする必要があります．

■設定するルールのポイント

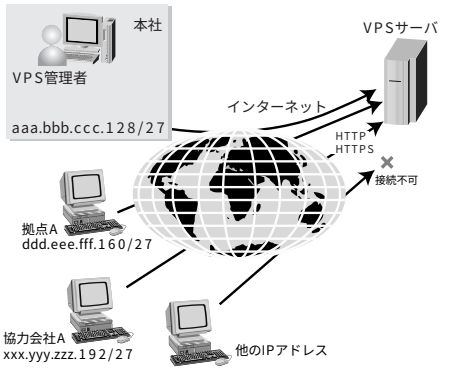
社内サーバとして利用する場合，公開用**Web**サーバよりもさまざまなサービスを提供する可能性が高くなります．提供状況によっては，特定のネットワークアドレスからのアクセスであればサービスを制限せずにアクセスを許可しても良いでしょう[注4]．第三者からのアクセスは一切許可しない一方で，一部のサービスのみへのアクセスを許可する相手がいるのであれば，対応するルールが必要となります（図**2**，リスト**2**）．

盲点になりがちなのが，社内側のファイアウォールの設定です．いくら**VPS**側でアクセスを許可しても，社内から**VPS**に抜けることができなければ意味がありませんので，注意が必要です．

共用ファイルサーバ

開発や運用保守作業を行う際に，社内の別拠点や協力会社，他社の人と大きなサイズのファイルを交換したいという状況は意外とあります．しかし，メールの添付で送ることができるサイズの上限を超えると，一気に手詰まりになってしまうことも少なくありません．そのような要望に応えるストレージサービスもありますが，とくに無料のサービスはセキュリティ面に不安があるため，利用が禁止されている場合もあるでしょう[注5]．

図2　社内サーバとして利用する例



リスト2　ルール設定例（社内サーバ）

```
# 1. ループバックインターフェースについては無条件ですべてを許可する
iptables -t filter -A INPUT -i lo -j ACCEPT
iptables -t filter -A OUTPUT -o lo -j ACCEPT

# 2. VPS -> 外部へのすべての通信を許可する
iptables -t filter -A OUTPUT -m state --state NEW,ESTABLISHED -j ACCEPT

# 3. 本社のネットワーク -> VPSへのすべての通信を許可する
iptables -t filter -A INPUT -s aaa.bbb.ccc.128/27 -m state --state NEW,ESTABLISHED -j ACCEPT

# 4. 拠点Aのネットワーク -> VPSへのすべての通信を許可する
iptables -t filter -A INPUT -s ddd.eee.fff.160/27 -m state --state NEW,ESTABLISHED -j ACCEPT

# 5. 協力会社Aのネットワーク -> VPSへのHTTP/HTTPSを許可する
iptables -t filter -A INPUT -s xxx.yyy.zzz.192/27 -p tcp --sport 1024: -m multiport --dports http,https -m state --state NEW,ESTABLISHED -j ACCEPT

# 6. 必要に応じて，VPSがクライアントになる通信の戻りパケットを許可する
【リスト1と同じ】

# 99. チェインポリシーをDROPにし，明示的に許可されていない通信を拒否する
iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP
```

注4：ここでは，管理者が本社のネットワークからアクセスし，接続元IPアドレスでは識別できないと想定している．
注5：ちなみに，筆者の会社では利用が公認されているストレージサービスがあるが，事前申請が必要なので緊急時はどうしようもない．

このような問題の解決方法の**1**つとして，**VPS**をインターネット上の大容量ストレージとして利用するという方法が考えられます．

■設定するルールのポイント

頻繁にファイル交換を行う信頼できる特定少数については，個別のアカウントを作成したうえで**SSH**を許可し，**SFTP**を利用してもらうのが良いでしょう[注6]．しかし，不特定多数を相手にする場合には，個別にアカウントを発行するのは大変ですし，共用アカウントを利用するのはセキュリティ的に問題があります．ここでは，暗号化**ZIP**で圧縮したファイルを**Web**サーバで公開し，**URL**とパスワードをメールで通知するという方式を想定し，そのようなルールを設定してみました（図**3**，リスト**3**）．

VPSでは複数**IP**アドレスや複数ドメインの割り当てを受けることができるため，目的別に**IP**アドレスを割り振り，それぞれの目的に適したルールを**IP**アドレス別に設定するという方法も考えられるでしょう．

リスト3　ルール設定例（共有ファイルサーバ）

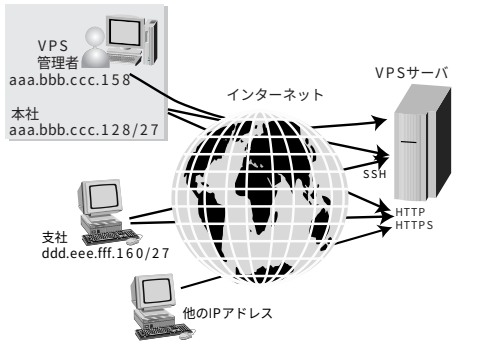
```
# 1. ループバックインターフェースについては無条件ですべてを許可する
iptables -t filter -A INPUT -i lo -j ACCEPT
iptables -t filter -A OUTPUT -o lo -j ACCEPT

# 2. VPS -> 外部へのすべての通信を許可する
iptables -t filter -A OUTPUT -m state --state NEW,ESTABLISHED -j ACCEPT

# 3. 管理者のIPアドレス -> VPSへのすべての通信を許可する
iptables -t filter -A INPUT -s aaa.bbb.ccc.158 -m state --state NEW,ESTABLISHED -j ACCEPT

# 4. 管理者以外のIPからの本社 -> サーバのSSHを許可する
iptables -t filter -A INPUT -s aaa.bbb.ccc.128/27 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

# 5. 支社からのSSHを許可する
iptables -t filter -A INPUT -s ddd.eee.fff.160/27 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

# 6. 不特定多数からのWebサーバへの通信を許可する（HTTP/HTTPS）
iptables -t filter -A INPUT -p tcp --sport 1024: -m multiport --dports http,https -m state --state NEW,ESTABLISHED -j ACCEPT

# 7. 必要に応じて，VPSがクライアントになる通信の戻りパケットを許可する
（リスト1と同じ）

# 99. チェインポリシーをDROPにし，明示的に許可されていない通信を拒否する
iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP
```

おわりに

本稿で解説したルール設定例は，説明上必要とされる必要最小限の例でしかなく，必要十分ではありません．メールサーバとしての設定など，多くの場合に必要とされる設定はまだまだありますし，**Linux**のアカウントの管理と組み合わせてアクセス制御を実現する必要が発生する場合もあるはずです．

manを参照すればわかりますが，**iptables**は非常に奥が深いソフトウェアです．設定する人の腕次第で，非常にきめ細かな管理や運用ができますので，つねに一歩先を目指すように心がけてください．SD

図3　共有ファイルサーバとして利用する例



注6：もちろんFTPを利用するという方法もあるが，セキュリティを考慮してここではSFTPを利用することにしている．また，ここでは複数台の共用端末と1台の管理者用端末が存在し，後者については接続元IPアドレスで特定できると想定している．