Linux サーバセキュリティミニマム

総合情報基盤センター 准教授 布村紀男

仮想化技術やネットワーク基盤の整備によりクラウドシステムが一般化している。そのシステムでは自らサーバを構築することなく、オンデマンドでサーバサービスの提供が受けられる。本学でも総合情報基盤センターが仮想サーバサービスを提供している。本稿では仮想サーバ利用のユーザおよび自らサーバを構築・運用されている学内ユーザに向けて、確認に意味を込めて Linux サーバセキュリティについて考えてみる。

キーワード：Linux，セキュリティ，サーバ，リモート管理

１．はじめに

JPCERT/CC[1]の 2012 年重大ニュースでは
・インターネットにおける抗議活動
・不正アクセス禁止法改正
・遠隔操作ウイルス事件
・タブレット端末の本格普及
・Android アプリ脆弱性による情報窃取
などが取り上げられている。

スマートフォンやタブレット端末などのモバイルデバイスの普及でこれまでの PC とは異なるセキュリティ対策や管理がユーザに要求されるようになってきている。一方、サイバー攻撃によりサーバが不正アクセスを受けた報道なども後を絶たない。また、自サーバが攻撃されるだけなく、脆弱性があるサイトでは他サイトへの攻撃の踏み台に利用される事例も報告されている。対岸の火事とは思わないでサーバ管理者の方々は日頃から注意しておかなければならない。

２．Linux サーバセキュリティ

サーバセキュリティは参考文献[2]に述べられているように大まかには次の 4 項目で整理される。
(1)ネットワークサービス
(2)ユーザ認証
(3)ログ取得
(4)ファイル保護(アクセス権)
具体的には(1)では不要なサービスを起動しない、telnet、r 系コマンド(rsh, rlogin, rcp)使用禁止して SSH を使うなど。 (2)では root ユーザの直接リモートログインは禁止する。適切なパスワードを設定し定期的に変更するなど。(3)ではログイン認証ログ、sudo コマンドの実行記録ログを取得し、一定期間保存するなどである。(4)ではアプリケーションデータは必要の最小限アクセス権に限定するなどがある。上記以外にもセキュリティに関する情報収集し、随時セキュリティパッチの適用もしなければならない。以下ではサーバ運用時に重要なログ監視、リモート管理、iptables によるパケットフィルタリングを取り上げる。

2.1 サーバ運用時のセキュリティ（ログ監視）

サーバから出力されるログはサーバの不正アクセスやその予兆などを知るための重要なファイルなので適切に保存し、定期的にチェックすることが必要である。リスト-1 は SSH で接続を拒否(refused)された際のログの例である。

リスト-1

```
# grep "refused connect" /var/log/secure*
secure: Jan 10 03:28:29 raptor sshd[8522]: refused connect from
secure: Jan  3 05:10:22 raptor sshd[16049]: refused connect from
```

管理者にとって毎日サーバログを見る作業はなかなか大変である。その作業を軽減させるために役立つログ関連ツールの利用を検討する。Linux では代表的なログ関連ツールとして swatch、logwatech や logmon 等がある。ここではセンターの仮想サーバに標準でインストールされている logwatch を扱う。logwatch はレポート形式で出

力するため個々に調べないで把握できる。出力例を図-1 に示す。表-1 に主なオプションを記述する。

```
[root@raptor log]# logwatch --print --range All --archives
 ##################### Logwatch 7.3 (03/24/06) ####################
        Processing Initiated: Mon Jan 21 19:47:44 2013
        Date Range Processed: all
      Detail Level of Output: 0
             Type of Output: unformatted
           Logfiles for Host: raptor.itc.u-toyama.ac.jp
  ##################################################################
 ---------- httpd Begin ----------
 Requests with error response codes
    403 Forbidden
       /: 2 Time(s)
       http://24x7-allrequestsallowed.com/?PHPSES ... 3PTSJTP_A%5CFYS: 1 Time(s)
    404 Not Found
       http://savoringsarah.files.wordpress.com/2010/12/n495.jpg: 1 Time(s)
```

図-1 logwatch の出力例

表-1 logwatch の主なコマンドオプション

機能	オプション指定例
標準出力	--print
特定サービス出力	--print --service http
複数サービス出力	--print --service http --service sshd
ログの詳細度変更	--print --detail 10 --service httpd
期間指定	--range All
ファイル出力	--save logwatch.txt

2.2 リモート管理のセキュリティ

リモート接続(SSH)のアクセス制限は TCP_Wrapper を用いて接続ホストを設定する。/etc/hosts.allow は接続を許可する記述ファイル、/etc/hosts.deny は接続を拒否する記述ファイルである。設定評価は hosts.allow →hosts.deny の順に行われ、最初に一致した時点で評価は終了する。設定ファイル host.allow, hosts.deny の例をリスト-1, 2 に示す。設定後は接続許可したホストからの接続が通るだけではなく、接続を許可しないホストからの接続拒否をしているかも必ずチェックしておくべきである。

リスト-1 hosts.allow の記述例

```
sshd:  .example.jp
sshd:  192.168.0.
sshd:  192.168.1.0/255.255.255.0
sshd:  192.168.2.0/24
```

リスト-2 hosts.deny の記述例

```
ALL: ALL
```

接続ユーザの制限は、SSH サーバの設定ファイル/etc/ssh/sshd_config で設定する。SSH で root のログイン禁止、接続ユーザを wildcat, hornet, tiger に限定する際はリスト-3 のように設定する。

リスト-3 sshd_config の記述例

```
PermitRootLogin  no
AllowUsers    wildcat  hornet  tiger
```

2.3 iptables によるパケットフィルタリング

Linux サーバの Firewall 機能は iptables によるパケットフィルタリングで利用できる[3]。ほとんどの Linux ディストリビューションで、デフォルトで有効になっている。 iptables –L で設定内容を確認できる。Scientific Linux 6.2[4]のデフォルト設定ではリモートアクセス(SSH)を通す設定になっている。仮想サーバのデフォルトに関しては各自確認してください。リスト-4 にパケットフィルタリングの設定例を示す。

リスト-4 iptables 設定例

```
ICMP パケットの受信拒否
# iptables -A INPUT -s 192.168.0.5 -p icmp -j DROP
SSH 接続を拒否する設定
# iptables -A INPUT -s 192.168.0.5 -p tcp --dport 22 -j
DROP
```

高度なセキュリティ設定としてディレクトリとファイルのアクセス権に SELinux[5]が利用できるが、設定は少々複雑なのでここでは省略する。

3. おわりに

Linux サーバセキュリティについて、ありきたりのことを最小限取り上げてみた。セキュリティ対策には終わりはなく、今日は万全であっても、明日には脆弱ということも有りうる。サーバ管理されている方々は、日頃から情報収集を行い、安全にサーバを運用していただきたい。

参考文献

[1] http://www.jpcert.or.jp/

[2]「プロのための Linux システムネットワーク管理技術」中井悦司. 技術評論社(2011).

[3]http://www.atmarkit.co.jp/flinux/index/indexfiles/iptablesindex.html

[4] https://www.scientificlinux.org/

[5]「SELinux システム管理――セキュア OS の基礎と運用」Bill McCarty. O'Reilly(2005).