Linuxによるセキュリティ入門（5）

―― 続・ログの管理（logcheckとsSMTPの導入）――

西 村 竜 一

Ⅰ．はじめに

この文章を書いているのは2003年８月の終わりです。今年の夏はBlasterと呼ばれるWindows2000やXPをターゲットとする新種のウィルスが世界的に大流行しました。私が所属する大学では全学的なファイアウォールが設置されており，インターネットから学内LANへの通信を確立することはできません。しかし，Blasterは学内LANに潜入し，私の研究室内でも多数の感染が発見されました。だれかのノートPCが学外で感染し，それを学内に持ち込んだのが侵入の原因のようです。ここまではファイアウォールを過信し，Windows Updateを怠っていた人が悪いのですが，新しく購入したノートPCを起動して真っ先にWindows Updateでアップデートしている最中にBlasterに感染させてしまった，なんていう報告もあります。これからはネットワークに繋ぐ前に（CDなどを用いた）アップデートが必要なんですね。油断もすきもあったもんじゃない怖い時代になってしまったものだと残念です。みなさんのところは大丈夫だったでしょうか？

さて，今回はログの管理の続編です。前回ではログの基本的な設定として，`syslog`の設定を解説しました。また，いくつかログの実例を見ていただきました。みなさん，日々ログの確認はしていますか？とはいっても，毎日ログをこまめにチェックすることは大変な作業です。そこで，今回はログをチェックして異常をメールで管理者に知らせてくれるログ監視ツールを導入しましょう。

Ⅱ．sSMTPのインストール

メールを利用するということは，みなさんのDebianシステムでメールを扱えるようにする必要があります。LinuxなどUNIX系システムの場合，メールを扱えるようにするということは，多くの場合メールサーバプログラム（専門用語を使うとMTA; Message Transfer Agentsと言います）の導入の話になります。しかし，Mew[1]などの高機能なメールクライアント（こちらはMUA; Mail User Agentと言います）を使う際には，他の計算機で動いているメールサーバプログラムにSMTPやPOP3またはIMAP4などのプロトコルでメール配送を任せてしまうので，自分自身でMTAを動かす必要はありません。ただし，今回のログ管理のようなバッチ処理などでメールを利用する際にはMTAの導入が必要になるケースが多いと思います。これまで余計なサーバプログラ

1　http://www.mew.org/

ムのインストールはしないという方針でこの連載をすすめてきましたので，MTAの導入についてもほとんど触れませんでした。今回，運用上はじめて必要になりましたので，まずMTAをインストールします。

MTAの代表的なプログラムはみなさんご存じのsendmail[2]です。ただしsendmailは設定が複雑なプログラムであるため，最近ではpostfix[3]やqmail[4]などの新しいMTAが使われることが多くなっています。Debianの場合，eximでメールサーバを運用されている方も多いと思います。MTAは運用する際，セキュリティの設定に特に注意しなければいけないプログラムです。メールのリレーの設定を間違えるとSPAMの踏み台になってしまいかねません。導入の際には慎重に作業をすすめるように心がけてください。

さて，今回インストールするMTAは前述のどれでもなくsSMTPというプログラムです。sSMTPはとてもシンプルなMTAプログラムで，配送されてきたメールをメールスプール（ユーザ宛のメールを保存するファイルなどを指す。私書箱に相当）に保存する機能すら持っていません。メールを受信することもできません。ただ，メールをハブ（中心）となる他のメールサーバに送信するだけのMTAです。もちろんsSMTPだけではユーザはメールを受信して読むことはできません（図１）。MTAが正しく動いている他のメールサーバ（メールハブ）が必須になります。

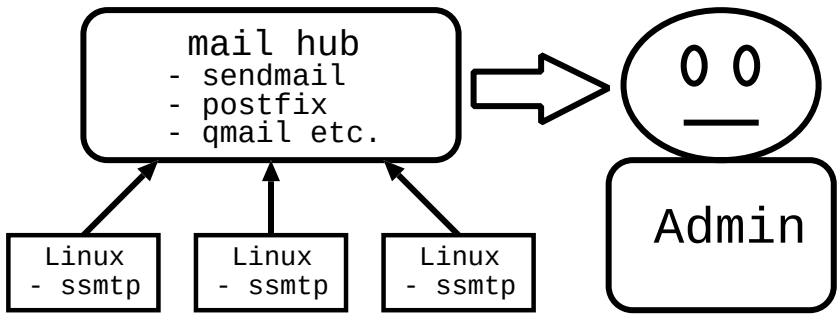


図１　クライアント（Linux）ではMTAとしてsSMTPが動作しています。sSMTPはメールハブにメールを送信するだけであり，ユーザはメールハブ（他のMTAが設定済み）に届いたメールを読むことになります。

しかし，機能がシンプルな分，扱いが簡単であり，またプログラムはセキュリティホールが生まれにくい実装になっています。受信機能がないのでSPAMの原因になることもありません。最終的にメールを受け取るメールハブには，みなさんが普段使っているメールサーバを利用することもできますし，今回の目的（メールの送信）には必要な機能は備わっています。前述したメジャーなすべての機能が備わったMTAの導入解説は書籍や関連Webページを参考にしてもらうとして，今回はこのsSMTPを導入しましょう。

sSMTPのDebianパッケージは`ssmtp`です。いつものように`apt-get`を用いてインストールし

2　http://www.sendmail.org/
3　http://www.postfix-jp.info/
4　http://www.jp.qmail.org/

ます。

```
% sudo apt-get install ssmtp
```

ダウンロードが完了すると設定に移ります。以下では実際の画面を見ながら解説をすすめます。なお，掲載するスクリーンショットはお使いのDebianの設定（debconf）により異なる場合がありますが，内容は同じです。また，設定項目が少ないこともありますが，これもdebconfの設定によるものです。設定項目をすべて表示したい場合や後から設定を変更する時は，

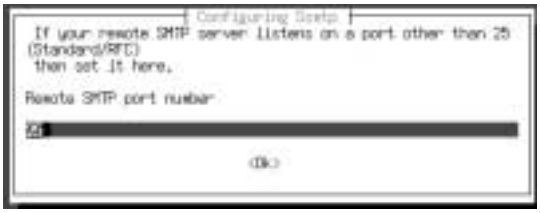
```
% sudo dpkg-reconfigure -plow ssmtp
```

とすることで再設定することができます。それでは順に見ていきましょう。

1．sSMTPの設定ファイルを直接編集するのではなく，debconfのみで設定する場合はYesと答えます。普通はYesで構いませんが，設定をエディタ等で編集する必要がある人はNoと答えてください。

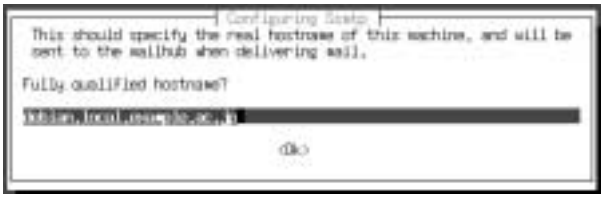
2．rootなどのシステム用アカウント宛のメールを転送するユーザを指定します。あなたのメールアドレスを入力してください。

3．sSMTPからメールを受け取るメールハブのホスト名を入力します。あなたが普段使っているメールサーバを使うことが多いと思います。

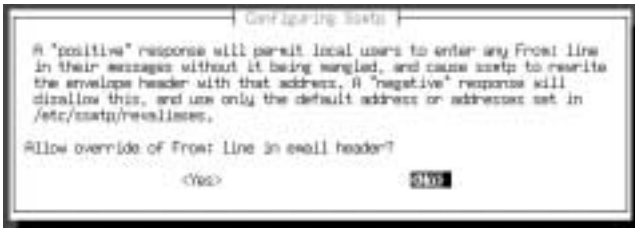


4．メールハブでMTAが動いているポート番号を指定します。SMTPは25番を使うので，デフォルトのまま25と入力してください。

5．From:フィールドに使用するドメイン名を指定します。実際にメールが届くドメインを使うのが原則ですが，ここではsSMTPが動いているホストのホスト名（FQDN）を入力してください。



6．もう一度，sSMTPが動いているホストのホスト名（FQDN）を入力します。



7．sSMTPがすでに存在するFrom:フィールドの書き換えを行うかどうかの設定です。これをNoにするとsSMTPはメールのFrom:フィールドを上記５．で設定したドメインに強制的に書き換えます。どちらにするのが良いかは状況により異なりますが，私はYesに設定しました。

設定が完了したらmailコマンドでメールが送信できるかを確認してみましょう。Debianではmailコマンドはmailxパッケージに含まれています。前回紹介したlogrotateパッケージをいれるとmailxパッケージはいっしょにインストールされています。

root宛にメールを送ってみます。Subject:と本文は適当に入力します。また，本文の終わりにはピリオド（“．”）を入力してください。Cc:は空欄のままで構いません。

```
% mail root
Subject: Test
This is a test.
.
Cc:
```

メールは無事にあなた（設定した転送先アドレス）に届いたでしょうか？

メールが届かなかった時は，まず設定時の入力ミスがないかどうかを確認します。つぎに，sSMTP関係のログは/var/log/mail.logに出力されますので確認しましょう。Relay access

deniedといった感じのログが出力されている場合は，３．で指定したメールハブにおいてsSMTPから送られてきたメールを転送するように設定されていないのが原因です（SPAM防止のためこれは正しい動作なのですが)。メールハブのMTAで転送許可の設定に変更するか，２．で指定したメールアドレスを最終的に受け取るメールサーバをメールハブに設定すると良いでしょう（ただし，この場合，sSMTPから２．で指定したメールアドレス以外にメールは送信できません)。また，メールハブ上のMTAの設定にもよりますが，５．で指定したホスト名がメールハブからDNSで参照（正引き）できないとメールが配送されない場合があります。

Ⅲ．logcheckのインストール

さて，やっとここからが本題です。ログ監視ツールの導入を行います。Debianではいくつかのログ監視ツールがパッケージで提供されていますが，今回はその中からlogcheckをインストールすることにします。

```
% sudo apt-get install logcheck
```

依存の関係で，`logtail`や`logcheck-database`などのパッケージも同時にインストールされるはずです。

それでは順に設定を見ていきます。まず２つ説明が表示されますが，これは中身を読んでOKを選んでください。最初の説明はlogcheckの設定ファイルの構成について解説されています。つぎはセキュリティレベルに関する説明です。logcheckではworkstation，server，paranoidの３個のセキュリティレベルが用意されています。workstationは，WebやFTP，Mailなどのサービスを一切提供しないワークステーションとして利用する際に選択します。serverは，サービスを提供するサーバとして計算機を運用する際のセキュリティレベルです。paranoidは計算機をファイアウォールやその他の用途で利用する場合のものです。

OKを選び表示される図２の設定項目で，セキュリティレベルを選択します。今回，ここではserverを選ぶことにします（みなさんは各自で適切なものを選んでください)。

続いての設定項目は，ログを送付するメールアドレスの入力です（図３)。デフォルトのまま

図２　セキュリティレベルの選択

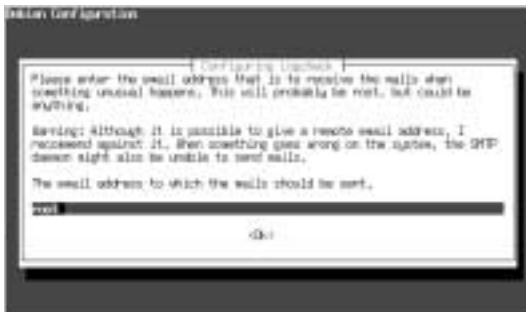


図３　ログ送信先アドレスの指定

root宛に送付すれば良いでしょう。前述のsSMTPの設定のとおりroot宛のメールはsSMTPによって指定されたアドレスに転送されます。

最後の設定項目は，logcheckの設定ファイルの一つである`logcheck.logfiles`の自動生成に関してです。このファイルはlogcheckが監視するログのリストを記述したものです。Yesを選択すると，`/etc/syslog.conf`からログファイルをピックアップします。syslogが出力するログ以外も監視するときは，`/etc/logcheck/logcheck.logfiles`にログのファイル名を追加すれば良いので，ここはYesを選択して自動生成します（図４）。

図４　logcheck.logfilesの自動生成

以上でlogcheckのインストールはとりあえずできました。設定を変更するときは，

```
% sudo dpkg-reconfigure -plow logcheck-database logcheck
```

と実行してください。logcheckは，Debianパッケージの`logcheck`と`logcheck-database`の２つで構成されているので，両方のパッケージの設定を変更する必要があります。

logcheckはcronから定期的に呼び出されます。その時間は`/etc/cron.d/logcheck`に書かれています。catなどを用いて中身を見てみると以下のようになっているはずです。

```
@reboot     root  test -x /usr/sbin/logcheck && nice -n10 /usr/sbin/logcheck
2 * * * *   root  test -x /usr/sbin/logcheck && nice -n10 /usr/sbin/logcheck
```

この例では，システムのリブート時と毎時２分にlogcheckが実行されるのがわかります。

ということで，しばらく待っていると

```
Subject: debian 2003/09/01 17:02 system check
```

といった感じのSubjectが付いたメールが送られてくると思います。ここで“ debian ”はホストネームであなたが計算機につけた名前です。続いてログをチェックした日付と時間です。

メールの本文を見ると，

```
Active System Attack Alerts
```

や

```
Possible Security Violations
```

```
Unusual System Events
```

に続いてログが添付されています。例えば,

```
Possible Security Violations
=-=-=-=-=-=-=-=-=-=-=
Sep  1 18:27:55 debian PAM_unix[5537]: authentication failure; (uid=0) -> root for ssh service
Sep  1 18:27:58 debian sshd[5537]: Failed password for root from 192.168.24.10 port 48687 ssh2

Unusual System Events
=-=-=-=-=-=-=-=-=-=-=
Sep  1 18:02:04 debian sSMTP[5531]: Sent mail for root@debian.local.example.ac.jp (221 Bye)
```

といった感じになっています。この例には含まれませんが，Active System Attack Alertsがなんらかの攻撃を受けている可能性のある最も危険性の高いログを示します。Possible Security Violationsはセキュリティ上注意が必要なログです。この例ではsshのログインで認証が失敗した際のログが送付されてきています。最後のUnusual System Eventsはこの中では一番レベルが低く，なんらかの異常を示したログです。上記例ではsSMTPがメールを送信した時のログが添付されています。

Ⅳ．logcheckのパターン定義の確認と変更

このようにlogcheckはログをメールで送信してくれますが，すべてのログを送ってくるわけではありません。Unusual System Eventsなど，つまり無視することができない異常なログのみを送られます。ログの中で無視できるものとできないものをどうやって区別するのでしょうか。それを決定しているのが`/etc/logcheck/`ディレクトリ以下の設定ファイルです。いくつかのファイルがありますがその中から具体例を見てみましょう。

まず，前述しましたが`logcheck.logfiles`です。このファイルの中身はチェックの対象とするログファイルのリストです。以下のようになっています。他のファイルもチェックしたい場合はこのファイルにファイル名を追加してください。

```
# these files will be checked by logcheck
/var/log/syslog
/var/log/mail.log
/var/log/daemon.log
/var/log/messages
/var/log/lpr.log
/var/log/auth.log
（以下，略）
```

つぎにlogcheck.ignoreです。このファイルは無視するログのパターンを定義したものになっています。以下はその一部を抜粋したものです。

```
in.qpopper.*: connect from
mail.local
-- MARK --
last message repeated .* times
```

これらパターンを含んだログはメールで送信せず無視します。ちなみにlogcheck.ignoreファイルは，同じディレクトリにあるlogcheck.ignore.serverへのシンボリックリンクです。他にlogcheck.ignore.workstationとlogcheck.ignore.paranoidも用意されており，dpkg-reconfigureでセキュリティレベルを変更した場合は，それらファイルにリンクが張り直される仕組みになっています。

先ほど例に挙げた

```
Sep  1 17:02:04 debian sSMTP[5162]: Sent mail for root@local.example.ac.jp (221 Bye)
```

という行は正常にメールが送られたログなのでlogcheckが無視するよう設定してみます。sSMTPのログのパターンは定義されていないようなので，自分で定義してみましょう。エディタで/etc/logcheck/logcheck.ignoreを編集して以下のパターンを追加するだけです。

```
sSMTP\[.*\]: Sent mail for
```

いかがでしょうか？

/etc/logcheck/ignore.d/ディレクトリ下をファイルをlsで確認すると次頁のようにプログラムごとに無視するパターンの定義ファイルが配置されているのがわかります。

```
% sudo ls /etc/logcheck/ignore.d/
automount  dhcp  imp      isdnutils   postfix  qmail    squid    sysklogd
bind       exim  ipppd    oidentd     ppp      qpopper  ssh      telnetd
cron       imap  isdnlog  portsentry  proftpd  samba    stunnel  uptimed
```

試しに/etc/logcheck/ignore.d/sysklogdの中身を見てみると，

```
% sudo cat /etc/logcheck/ignore.d/sysklogd
syslogd.*: restart\ .
```

syslogdに関する無視するログのパターンが定義されています。このようにDebianパッケージの中にこれらパターンファイルが含まれていれば，ユーザが自前で定義を追加しなくとも適切にログを監視できるようになっています。

なお，logcheck.crackingとcracking.d/は，Active System Attack Alertsに該当する危険性が高いログのパターンの定義ファイルです。同様にlogcheck.violationsとviolations.dは，Possible Security Violationsに該当するパターンの定義です。

logcheckで効率よくログをチェックするには，これらパターンの定義が正しくされている必要があります。残念ながら用意されているパターンは完全なものではないようです。みなさんも送られているメールを参考にパターンの定義を行ってみると良いでしょう。

V．おわりに

本稿ではsSMTPの導入とlogcheckの紹介をしました。今回，MTAをインストールしましたので，次回もメールを有効利用したセキュリティツールを紹介する予定です。

（にしむら　りゅういち：奈良先端科学技術大学院大学情報科学研究科）
（nisimura@linux.or.jp）