TOMOYO Linux を体験しよう

2.1. TOMOYO Linux について

ポイント！ ――――――――――――――――――――――――――――――――――――

TOMOYO Linux は誰でも使えるセキュア OS を目指して開発された国産のセキュア OS です。

――

SELinux はもともと軍事、政府向けに開発されていること、特に CC 認証を取得することを目的としていることもあり、使い勝手の面ではあまりよくありませんでした。そこで、「誰でもつかえるセキュア OS」をコンセプトの元に、NTT データ株式会社が国産のセキュア OS として、TOMOYO Linux を開発しました。
大きな特徴としては、ポリシー自動学習機能を搭載しており、セキュア OS の課題であるセキュリティポリシー定義の行程を大幅に省略できることが期待されています。

最近では Linux カーネルのメインラインに提案するため、LSM にも対応したヴァージョンもリリースされています。TOMOYO Linux には以下のようなヴァージョンがあります。最新のヴァージョンは 1.5.1 です。
＊　2007 年 10 月現在

表 1　TOMOYO Linux のヴァージョンについて

ヴァージョン	説明
1.x	カーネルパッチ 最新機能を搭載　カーネル 2.6、2.4 の両方に対応
2.x	LSM モジュール メインラインにマージするために LSM に対応 一部の機能が搭載されていないので注意

参考

TOMOYO Linux の開発背景や歴史、その他の詳細については以下のサイトで確認することができます。
http://tomoyo.sourceforge.jp/

2.2. TOMOYO Linux のインストール

TOMOYO Linux をインストールするには、以下のパッケージを追加します。（CentOS5 の場合）

表 2　TOMOYO Linux のパッケージ

パッケージ名	説明
kernel-2.6.18-8.1.14.el5_tomoyo_1.5.1	TOMOYOLinux 用カーネル
ccs-tools-1.5.1-1.CentOS5	TOMOYOLinux 用ツール

以前の TOMOYO Linux ではカーネルコンパイルなどの作業が必要でしたが、最新のヴァージョンでは、主要なディストリビューションごとのパッケージが用意されていますので、たいへん簡単に導入することができます。

参考

TOMOYO Linux のパッケージは以下のサイトからダウンロードすることができます。

http://sourceforge.jp/projects/tomoyo/

参考

カーネルパッチ形式の TOMOYO Linux は SELinux が有効な状態でも共存させることも可能ですが、慣れないうちは無効にしておいたほうがよいでしょう。

2.2.1. TOMOYO Linux の初期設定

TOMOYO Linux カーネルをインストールしたら、/boot/grub/grub.conf に TOMOYO Linux カーネルを起動するためのメニューが以下のように追加されます。

```
# more /boot/grub/grub.conf

title CentOS (2.6.18-8.1.14.el5_tomoyo_1.5.1)
        root (hd0,0)
        kernel /vmlinuz-2.6.18-8.1.14.el5_tomoyo_1.5.1
            ro root=/dev/VolGroup00/LogVol00 rhgb quiet
        initrd /initrd-2.6.18-8.1.14.el5_tomoyo_1.5.1.img
```

次に、TOMOYO Linux を動作させるために必要な設定ファイルを作成する以下の初期設定スクリプトを実行します。

■ 書式

```
init_policy.sh --file-only-profile
```

```
# /usr/lib/ccs/init_policy.sh --file-only-profile
```

初期設定が完了しましたら、システムを再起動して TOMOYO Linux カーネルでシステムを起動しましょう。

参考

TOMOYO Linux 専用コマンドは/usr/lib/ccs ディレクトリ以下に格納されているので、必要に応じて PATH 変数に追加しておきましょう。

2.3. TOMOYO Linux のセキュリティポリシー作成手順

TOMOYO Linux でセキュリティポリシーを定義するには、自動学習モードを使用し、以下の図のような手順で自動学習モード時に作成したポリシーを適用します。

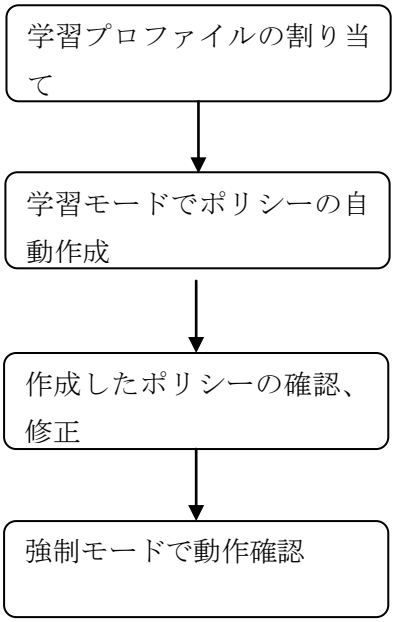

図 1　セキュリティポリシー作成の流れ

参考

TOMOYO Linux の動作モードについては次のページで解説しています。

2.3.1. TOMOYO Linux の動作モード

TOMOYOLinux には SELinux と同様にいくつかの動作モードがあります。
以下の表に動作モードをまとめました。

表 3　TOMOYO Linux の動作モード

モード名	番号	説明
Disabled　（無効モード）	0	TOMOYO Linux は無効の状態
Learning　（学習モード）	1	ポリシー自動学習モード
Permissive （許可モード）	2	強制アクセス制御は無効だがログは出力
Enforcing　（強制モード）	3	強制アクセス制御が有効な状態

番号とは、各モードを提供するためのプロファイル番号になります。

- Disabled
  無効モード。TOMOYO Linux は無効の状態です。
- Learning
  学習モード。セキュリティポリシーを自動的に作成するには、動作を学習させたいプロセスにプロファイル番号 0 を適用します。
- Permissive
  TOMOYO Linux で学習したセキュリティポリシー以外の動作が発生してもアクセス拒否は行いません。しかし、アクセスを拒否したログは出力します。トラブルシューティング時に使用するモードです。
- Enforcing
  TOMOYO Linux の強制アクセス制御機能が有効になります。実際の本番稼働時にはこのモードでなければ、セキュリティ機能を有効化したことになりませんので注意してください。

2.4. 学習モードでポリシーを自動的に作成してみよう

実際に TOMOYOLinux のポリシーを自動的に作成する体験をしてみましょう。
今回は root のログインシェルである bash に対して動作を記録する学習モードを割り当てます。学習モードに変更するためには、以下のコマンドを実行してプロファイルを割り当てます。

■ 書式

```
setprofile  -r  プロファイル番号  割り当てるプロセスのパス
```

root ユーザのログインシェルである bash に対して学習モードのプロファイルを割り当てるには以下のように実行します。

```
# setprofile -r 1 '<kernel> /usr/sbin/sshd /bin/bash'
1 <kernel> /sbin/mingetty /bin/login /bin/bash
1 <kernel> /sbin/mingetty /bin/login /bin/bash /bin/egrep
.....
```

'<kernel> /usr/sbin/sshd /bin/bash'とは
カーネルから起動された/usr/sbin/sshd から起動された/bin/bash に対して学習モード用のプロファイル 1 を割り当てるという意味です。

参考

コンソールログインからのシェルに対してプロファイルを割り当てるなら
'<kernel> /sbin/mingetty /bin/login /bin/bash'
のようになります。

アクセスを許可してもよいファイルにアクセスして自動的にポリシーを学習させます。

```
# tail /etc/passwd
squid:x:23:23::/var/spool/squid:/sbin/nologin
named:x:25:25:Named:/var/named:/sbin/nologin
yuya:x:500:500::/home/yuya:/bin/bash
……

# date
Tue Aug  15 8:15:00 JST 2007

# cal
    August 2007
Su Mo Tu We Th Fr Sa
         1  2  3  4
 5  6  7  8  9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31
```

この時の動作が学習されて TOMOYO Linux のセキュリティポリシーとなり自動的に生成されていきます。

2.5. 強制モードで強制アクセス制御機能を体験してみよう

学習モードで自動的に作成したポリシーを有効化して実際にアクセス制御機能が有効になっていることを確認します。
学習モード用のプロファイルが割り当てられている bash に対して強制モードのプロファイルを割り当てるには以下のように実行します。

```
# setprofile -r 3 '<kernel> /usr/sbin/sshd /bin/bash'
3 <kernel> /usr/sbin/sshd /bin/bash
3 <kernel> /usr/sbin/sshd /bin/bash /bin/egrep
3  <kernel> /usr/sbin/sshd /bin/bash /usr/bin/id
```

強制モード用のプロファイルを割り当てたら、ポリシーに定義されている動作しか実行することができなくなります。そのため、学習モード時に実行した以下のコマンドは実行できます。

```
# date
Tue Aug  15 8:15:30 JST 2007

# tail /etc/passwd
yuya:x:500:500::/home/yuya:/bin/bash
```

しかし、学習モード時に実行しなかったコマンドは実行を許可するセキュリティポリシーが用意されていませんので root ユーザであっても実行することができませんでした。

```
# reboot
-bash: /sbin/reboot: Operation not permitted
# cat /etc/shadow
-bash: /bin/cat: Operation not permitted
```

2.5.1. 自動的に生成したセキュリティポリシーを確認する

ポイント！ ――――――――――――――――――――――――――――――――

学習モードで作成したポリシーは専用のコマンドによって確認、修正を行うことができます。

――――――――――――――――――――――――――――――――――――

学習モードで自動的に生成したポリシーを確認、修正するには editpolicy コマンドで確認することができます。

■ 書式

```
editpolicy
```

たくさんのポリシーが自動的に作成されています。F キーを押すと検索モードになりますので、必要に応じて目的のポリシーを探すことができます。

```
# editpolicy
<<< Domain Transition Editor >>>     706 domains    '?' for help

<kernel>
    0:  0     <kernel>
    1:  0  *      /etc/rc.d/init.d/acpid
    2:  0            /bin/bash
    3:  0               /usr/sbin/acpid
    4:  0            /bin/touch
    ……

    F キーを押したときは検索モードになる
    Search>
```

また、特定のポリシーでエンターキーを押すとより詳細なポリシーを確認することができます。

```
690:  0  *     /usr/sbin/sshd
704:  0              /usr/bin/tail  ←  この行でエンターキー
```

これは、/usr/sbin/sshd から起動された/usr/bin/tail コマンドについてのポリシーです。704 行目でエンターキーを押すと以下のような tail コマンドに対しての詳細なアクセス権を確認することができます。

```
<<< Domain Policy Editor >>>     1 entry   '?' for help

<kernel> /usr/sbin/sshd /bin/bash /usr/bin/tail
    0: 4 /etc/shadow
```

/etc/shadow の隣に表示されている 4 は Linux のパーミッションと同様のアクセス権を表しています。
つまり、カーネルから起動された　/usr/sbin/sshd から起動された/bin/bash から起動された/usr/bin/tail がアクセスした/etc/shadow ファイルには読みとりのアクセス権のみ許可するということが読みとれます。

2.5.2. 修正したセキュリティポリシーを保存する

ポイント！ ――――――――――――――――――――――――――――――――

学習モードで作成したポリシーは保存しないと次回のシステム起動時には無効になってしまうので注意しましょう。

――――――――――――――――――――――――――――――――――――――

editpolicy コマンドでポリシーを修正した場合は、メモリ上のポリシーを修正しているので設定ファイルには保存されていません。修正したポリシーを保存するには savepolicy コマンドを実行します。

■ 書式

```
savepolicy
```

savepolicy コマンドを実行すると、/etc/ccs/domain_policy.conf ファイル内にポリシーが保存されます。システム起動時には、このファイルを読み込んで起動します。

```
# savepolicy
# more /etc/ccs/domain_policy.conf
<kernel> /usr/sbin/sshd
use_profile 0
<kernel> /usr/sbin/sshd /bin/bash
1 /bin/date
1 /bin/more
```