日本セキュアOSユーザ会
セキュアOS塾 - 02

TOMOYO Linuxで Linuxの動きを見てみよう

2009年2月2日

（株）NTTデータ
沼口大輔
numaguchid@nttdata.co.jp

今日のお話

1. 現状認識
2. TOMOYO Linux のしくみ
3. TOMOYO Linuxを用いた Linuxの動作解析

「権限」とユーザモデル

- オペレーティングシステムには「権限」という考え方があります
- 何故「権限」が必要なのでしょう？
  - 「誰でも何でもできる」では、セキュリティ以前に秩序が保てません＝たとえばWindows 95, 98, Me
  - かといって「誰も何もできない」のでは話になりません＝たとえば電源を落としたコンピュータ
  - そこで「（必要な）権限を持っていれば実行できる」ようにしようというわけです

具体的には

- Windows
  - Administratorは、「全権」を与えられています
    - 何でもインストールできますし、Windowsが起動しなくなるようなこともできてしまいます
- Linux / UNIX
  - 当たり前ですがrootとしてログインしたユーザは「全権」を持ちます
    - Windowsと同じように、起動しなくなるようなことができてしまいます

ゼロデイ攻撃

- WindowsでAdministratorの権限を奪われたり、Linux/UNIXでrootの権限を奪われてしまうとどうしようもありません
  - 権限を奪われてしまう脆弱性はよく見つかります
  - たとえばWindows Updateの月例パッチでも毎月のように出てきます
  - 2008年10月に公開されたServerサービスの脆弱性（MS08-067）、12月に公開されたIEの脆弱性（MS08-078）では、被害についてニュースにもなっていました。
- そうした脆弱性（セキュリティ上の欠陥）を埋めるためにアップデートやパッチを当てるわけですが、当然ながら攻撃する側はそうした対処を待っていてくれません

攻撃されたらどうなる？

- 攻撃者のやりたいことは何でもできます
- ありそうなのは
  - 攻撃できて満足する
    - ここで終わる人はそんなにいない
  - HPの内容を書き換える
    - 別サイトへのリンク
    - 不正プログラム（ウイルス、ボット）をダウンロード
  - コッソリ情報をもらってお金にする

事例

- MS08-067の脆弱性では、多くの被害が出ています。
  - 猛威を振るう「Conficker」ワーム、感染PCは約900万台に - Computerworld.jp
    - http://www.computerworld.jp/topics/vs_2/132329.html
  - 個人に遅れる企業の対策：10月のMS脆弱性問題、企業ばかりに被害多発 - ITmedia エンタープライズ
    - http://www.itmedia.co.jp/enterprise/articles/0812/19/news004.html
- パッチ適用を直ぐにできていないことが、被害拡大の原因

なぜ直ぐにパッチを適用しないか

- 脆弱性が見つかったからといって直ぐにパッチ適用にはなりません(特に商用システム)
- パッチ適用によるサービス停止は避けたい
- デグレードしないか試験しないといけない
  - 試験に時間がかかる
  - 試験環境自体がないので試験ができない
- 被害を最小限にするためにも、事前の対策が必要です

対策

- 基本的な考え方
  - 「権限」を分割する
    - 全権とそれ以外しかなければ、処理をする度に全権を渡すことになります（消しゴムの購入のために社印を渡してそれが悪用されたら？）
  - 「権限」の審査を徹底する
    - 管理者であろうがなかろうが例外扱いしない
    - 事前に定めた「条件」に基づき審査する

「セキュアOS」とは

- 管理者をも「制限」できるOSのことです
- 技術的には
  - 「強制アクセス制御」(Mandatory Access Control)を実装したOSです。
- 標準機能/オプションの違いはあっても主要なOSではだいたい利用できるようになりました
  - LinuxであればSELinux, Smack, AppArmor, TOMOYO Linux

セキュアOSの利点と大変なところ

- 利点
  - ポリシー（良い悪いの定義）が適切に行われていれば
    - 万一不正アクセスを受けた場合でも被害を限定（局所化）することができます
    - ポリシー違反の監視により不正アクセスの検知が可能となります（本来は検知だけでなく守るべきですが）
    - 管理者の誤操作による被害や内部関係者による情報漏洩の可能性を軽減できます（管理者であろうが内部関係者であろうがポリシーで許可されていない操作は失敗します）
- 大変なところ
  - ポリシーを『適切に設定』することが一番難しい

どれを使う？

- SELinux（米National Security Agencyが開発）
  - Linux標準機能に含まれており、Red Hat EL, Fedoraでは有効状態で出荷されています。強力ですがその分難易度も高くなっています（管理GUIが開発されるなど、着実に改善されています）
- Smack（Casey Schauflerが個人で開発）
  - 2008年4月、SELinuxに続きLinux標準機能に追加されました
- AppArmor（Novellが開発）
  - Linux標準には含まれていませんが、Ubuntu, openSUSE, Mandrivaに搭載されています
- TOMOYO Linux(NTTデータが開発)

TOMOYO Linuxはディストリビューションではありません

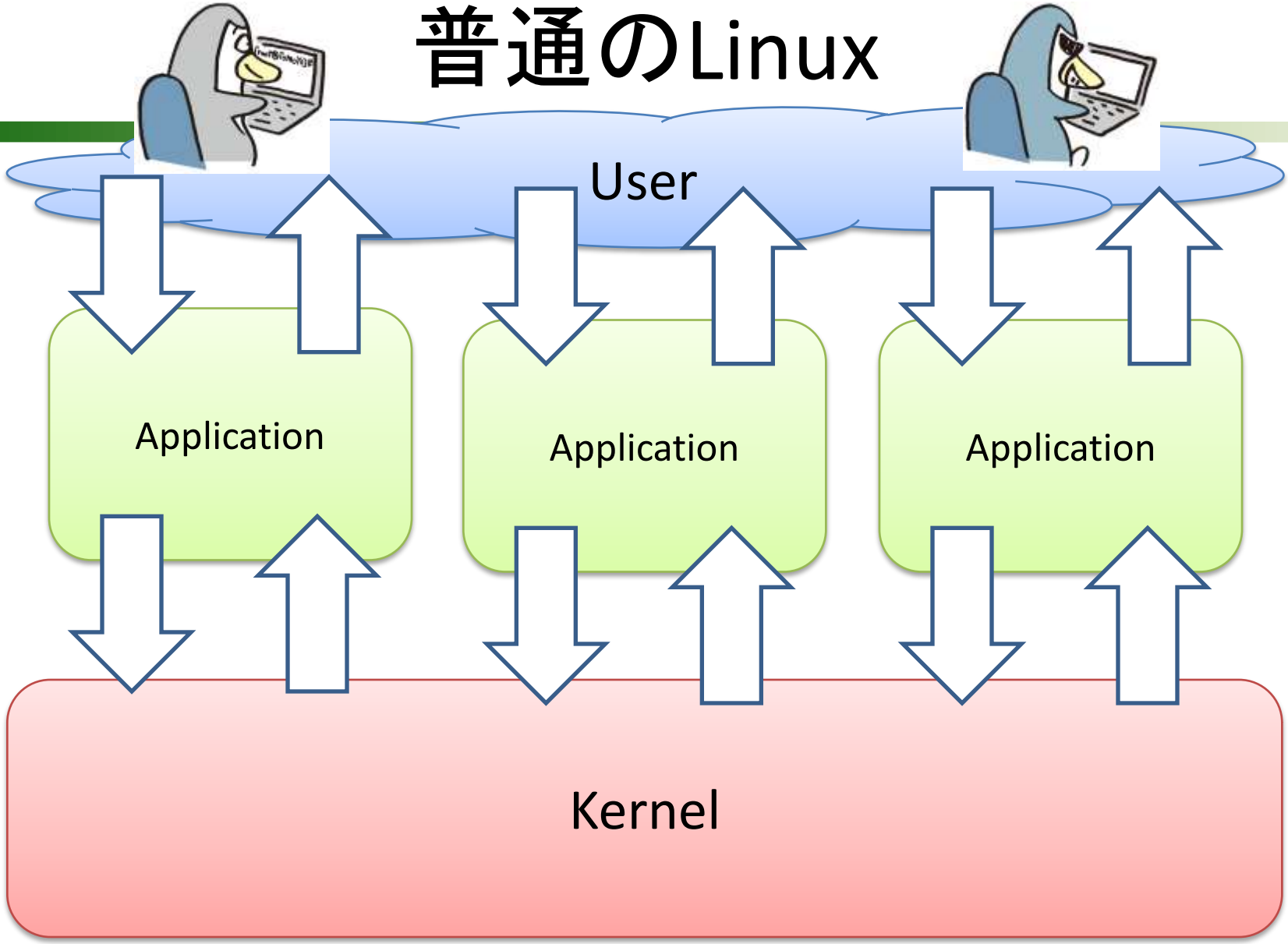
TOMOYO Linuxとは

- 「使いこなせて安全なLinux」を目指してNTTデータが開発しました。
- パス名を基に強制アクセス制御を行います。
- 2つのものから構成されています。
  - カーネル
    - 通常のカーネルに強制アクセス制御を追加したもの
  - ユーティリティ
    - 強制アクセス制御機能を設定、運用するもの

TOMOYO Linuxの導入事例

- Mandriva 2009.0, Turbolinux 11 Server, Turbolinux Client 2008では、標準搭載されています。
  http://www.turbolinux.co.jp/products/server/11s-tomoyolinux.html
- 2008年３月からNPO日本ネットワークセキュリティ協会のサーバで稼働しています。
  http://www.jnsa.org/result/2007/tech/secos/

普通のLinux



TOMOYOの動作

User

Application

Application

Application

TOMOYO Linux

Kernel

OK?
not OK?

TOMOYO Linuxの特徴

- パス名を使ったアクセス制御をしています。
  - ポリシーもパス名を使って定義されています。
- 自動学習機能が標準搭載されています。
  - プログラムを実行させれば、自動でポリシーを作成してくれます。

```
<<< Domain Policy Editor >>>          15 entries

<kernel> /etc/rc.d/init.d/sshd
_   0: allow_execute    /bin/cp
    1: allow_execute    /bin/touch
    2: allow_execute    /sbin/consoletype
    3: allow_execute    /sbin/runlevel
    4: allow_execute    /usr/sbin/sshd
    5: allow_read       /bin/bash
    6: allow_read       /etc/nsswitch.conf
    7: allow_read       /etc/passwd
```

TOMOYO Linuxの使い道

- TOMOYO Linuxに限らず、セキュアOSはポリシーに違反していないか常にOSの動きを監視しています。（セキュリティ対策として）
- セキュリティ対策以外にも、強制アクセス制御機能を使うことができます。
- それはLinuxの動作解析です。
  - デバッグで不必要なファイルの抽出など

TOMOYOで解析できること

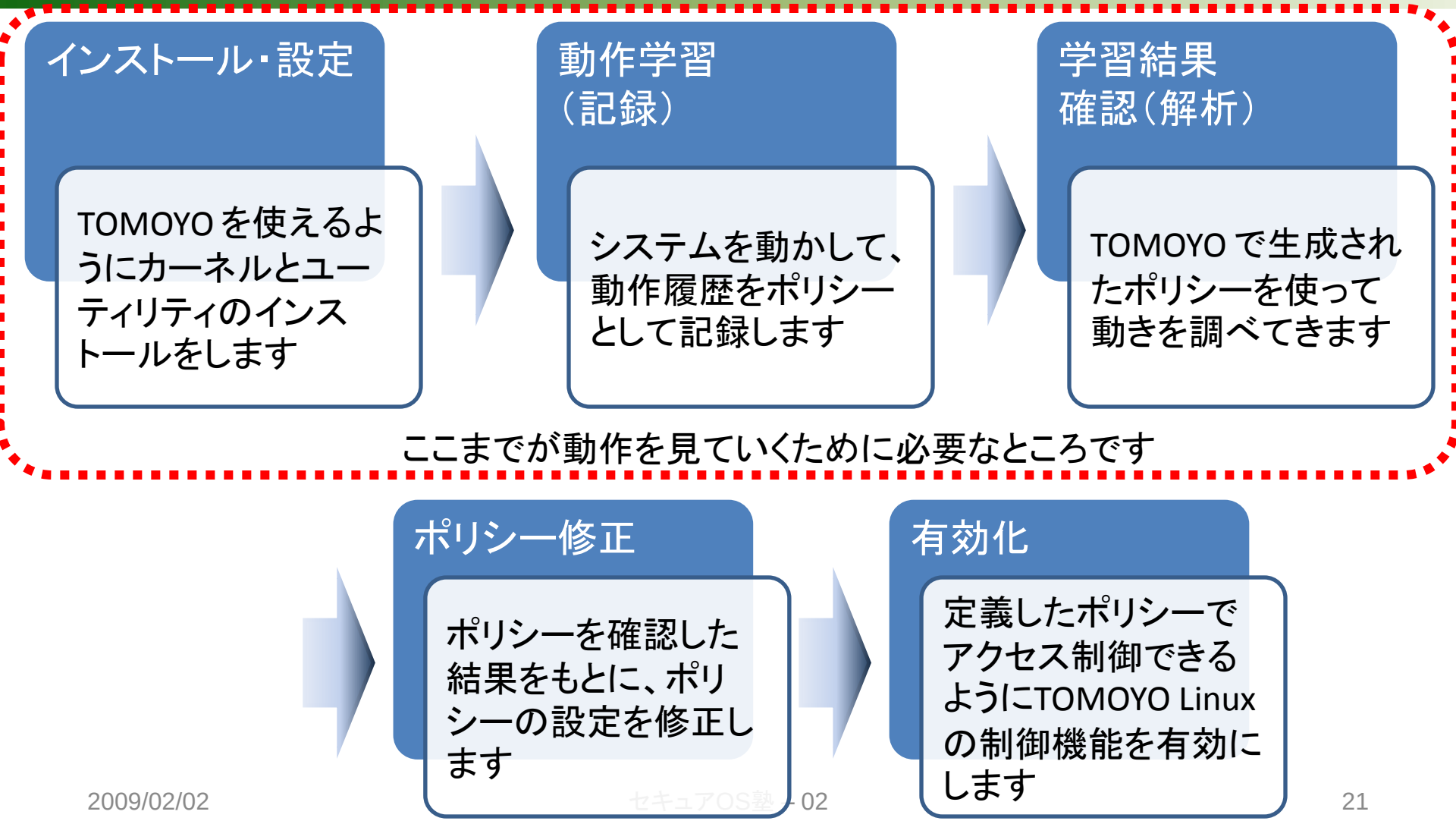
- プロセスの起動履歴
  - プロセスの親プロセス、親の親プロセス、さらにその親、・・・、をさかのぼって記憶しています
- 各プロセスのアクセス履歴
  - 起動履歴ごとにプロセスが、どんなファイルを読み出したのか、実行したのかなどの情報が得られます

動きを見ていこう

- ここからは実際にTOMOYO Linuxを使って、Linuxの動きを見ていきます。

- 動きを見ていくもの
  - Linux起動時の動き
  - GCCの動き

調べる手順



事前準備

- TOMOYO Linuxのインストールに必要なものを準備します
  1. カーネル
     - ディストリビューション毎にバイナリパッケージが公開されています。
     - 対応ディストリビューション
       - Ubuntu、CentOS、Debian、Fedora、SUSE、Vine Linux、Asianux、Red Hat Linux 9、Armadillo-9
  2. ユーティリティ
     - TOMOYO Linuxを制御するためのツール群です。
     - ディストリビューション毎にバイナリパッケージが公開されています。
     - 対応ディストリビューション
       - Ubuntu、CentOS、Debian、Fedora、SUSE、Vine Linux、Asianux、Red Hat Linux 9、Armadillo-9

手順1.「インストール（1/3）」

1. Ubuntu8.04をインストール
2. TOMOYOカーネルのインストール

詳細はhttp://tomoyo.sourceforge.jp/ja/1.6.x/1st-step/ubuntu8.04/を参照

① 3つのパッケージをダウンロードします

- http://osdn.dl.sourceforge.jp/tomoyo/32749/linux-image-2.6.24-23-ccs1.6.6_2.6.24-23.48_i386.deb
- http://osdn.dl.sourceforge.jp/tomoyo/32749/linux-ubuntu-modules-2.6.24-23-ccs1.6.6_2.6.24-23.36_i386.deb
- http://osdn.dl.sourceforge.jp/tomoyo/32749/linux-restricted-modules-2.6.24-23-ccs1.6.6_2.6.24.16-23.56_i386.deb

② dpkg を使ってパッケージをインストールをします

手順1.「インストール（2/3）」

3. ユーティリティのインストール
   ① ユーティリティをダウンロードします
      - http://osdn.dl.sourceforge.jp/tomoyo/32749/ccs-tools_1.6.6-1_i386.deb
   ② dpkg を使ってパッケージをインストールをします
4. 初期設定スクリプトの実行
   – /usr/lib/ccs/init_policy.sh --file-only-profile
   – 設定ファイルがディレクトリ/etc/ccsに作成されます

手順1.「インストール（3/3）」

5. アクセスログ取得設定
   - アクセス拒否ログの保存を行います。
     - cat > cat > /etc/init.d/ccs-auditd << EOF
     - #!/bin/sh
       /usr/lib/ccs/ccs-auditd /dev/null /var/log/tomoyo/reject_log.txt
       EOF
     - chmod +x /etc/init.d/ccs-auditd
     - update-rc.d ccs-auditd start 99 2 3 4 5 .
     - mkdir -p /var/log/tomoyo
6. 設定が完了したらシステムを再起動します

TOMOYOの設定ファイル（1/2）

- TOMOYO Linux には、5つの設定ファイルがあります。

アクセス制御方法の定義

profile.conf

プログラム（ドメイン）単位で、強制アクセス制御のモードを定義します。

ポリシーマネージャの定義

manager.conf

ポリシーの設定変更が行えるプログラムを定義します。

TOMOYOの設定ファイル（2/2）

ポリシー

domain_policy.conf

プログラム単位でのアクセス許可を定義しています。自動学習で設定が追加されます。

system_policy.conf

システム全体に対して適用されるアクセスを定義します。マウントポイントのマウント、アンマウントを設定できます。

例外ポリシー

exception_policy.conf

domain_policyの例外を定義します。パス名のパターン、グループ化、ドメイン遷移を初期化するプログラムなどを設定できます。

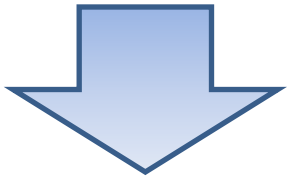
詳細は、http://tomoyo.sourceforge.jp/ja/1.6.x/policy-reference.html を参照

手順2.「設定確認」

- /etc/ccs/profile.confの設定

```
0-COMMENT=-----Disabled Mode-----
0-MAC_FOR_FILE=disabled
0-TOMOYO_VERBOSE=disabled
1-COMMENT=-----Learning Mode-----
1-MAC_FOR_FILE=learning
1-TOMOYO_VERBOSE=disabled
2-COMMENT=-----Permissive Mode-----
2-MAC_FOR_FILE=permissive
2-TOMOYO_VERBOSE=enabled
3-COMMENT=-----Enforcing Mode-----
3-MAC_FOR_FILE=enforcing
3-TOMOYO_VERBOSE=enabled
```

```
1-COMMENT=-----Learning Mode-----
1-MAC_FOR_FILE=learning
1-TOMOYO_VERBOSE=disabled
```



読み下すと

プロファイル1では、ファイルに対するアクセス制御を学習モードにし、コンソールにアクセス拒否メッセージを表示しない。

profile.confの読み方（1/2）

- （プロファイル番号）－（設定項目）＝（制御モード）
  - TOMOYO Linuxを使ったアクセス制御内容を設定します。
  1. プロファイル番号
     - プロファイルを切り替えるための番号です。0～255で設定可能。
  2. 設定項目
     - COMMENT・・・プロファイル区切りに挿入するもの。
     - TOMOYO_VERBOSE・・・アクセス拒否の情報をコンソールに出力するかどうかを設定します。
       - disabled・・・出力なし
       - enabled・・・出力あり
     - MAC_FOR_FILE・・・ファイルに対するアクセス制御
     - 詳しくは、http://tomoyo.sourceforge.jp/ja/1.6.x/policy-reference.html#profile を参照してください。

profile.confの読み方（2/2）

3. 制御モード
   - disabled （無効）モード
     - TOMOYO Linuxの制御は無効となり、普通のLinuxと同じように動作します。
   - learning （学習）モード
     - TOMOYO Linuxは学習モードで動作します。Linuxの動きを記録し、ポリシーを生成します。
   - permissive （確認）モード
     - ポリシーに基づいてLinuxの動きをチェックしますが、ポリシー違反が起きてもログを取得するだけです。
   - enforcing （強制）モード
     - ポリシーに基づいてLinuxの動きをチェックします。ポリシー違反の動作を許可しません。
   - 詳しくは、http://tomoyo.sourceforge.jp/ja/1.6.x/policy-reference.html#profile を参照してください。

手順3.「設定変更と確認」

- /etc/ccs/domain_policy.confの設定内容

<kernel>ドメインに対して、プロファイル番号1を指定し、（profile.confの設定から）学習モードで動作する。アクセス許可は未設定。

domain_policy.confの読み方

1. ドメイン名
   – プログラム起動履歴プログラムのパス
2. use_profile プロファイル番号
   – profile.confで定義したプロファイル番号
3. アクセス許可
   – アクセス許可内容を記述する
   – 詳細は http://tomoyo.sourceforge.jp/ja/1.6.x/policy-reference.html#domain_policy

手順4.「動作学習」

1. Linux起動時の動作
   - 学習モードの設定が終わった段階で、Linuxを再起動し、ログインまでを行います。
2. GCCの動作
   - Hello Worldプログラムをgccでコンパイルします。

- どちらも操作を完了したら、ポリシーエディタ(ccs-editpolicy)で動作を確認します。

手順5.「学習結果の確認」

- 動作を見たいプログラムを実行し、TOMOYO Linuxで記録が完了したら、学習結果を確認していきます。
- 確認をするには、ドメイン遷移情報とドメインポリシー情報を使用します。またログを確認します。
- ドメイン遷移とドメインポリシーの情報を見るために、ポリシーエディタというツールを使用します。

ポリシーエディタ

```
<<< Domain Transition Editor >>>      740 domains

<kernel>
_   0:  1      <kernel>
    1:  1  *       /etc/rc.d/init.d/acpid
    2:  1              /bin/bash
                           /usr/sbin/acpid ( -> 709 )
    3:  1              /bin/touch
    4:  1              /sbin/consoletype
    5:  1  *       /etc/rc.d/init.d/anacron
    6:  1              /bin/nice
    7:  1                  /bin/bash
```

ドメイン遷移画面

ドメインポリシー画面

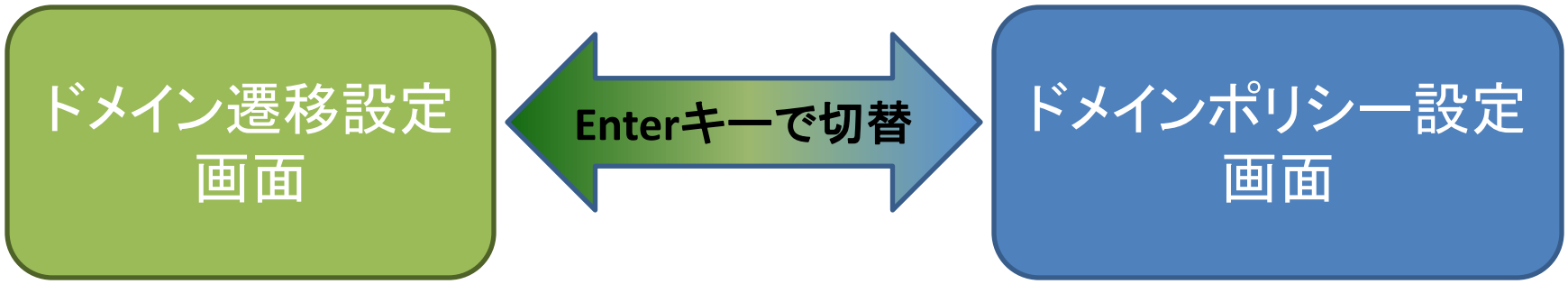
```
<<< Domain Policy Editor >>>      15 entries

<kernel> /etc/rc.d/init.d/sshd
_   0: allow_execute    /bin/cp
    1: allow_execute    /bin/touch
    2: allow_execute    /sbin/consoletype
    3: allow_execute    /sbin/runlevel
    4: allow_execute    /usr/sbin/sshd
    5: allow_read       /bin/bash
    6: allow_read       /etc/nsswitch.conf
    7: allow_read       /etc/passwd
```

- デモ
- 手順2から
  やっていきます

ポリシーエディタの使い方

- ポリシーエディタ(ccs-editpolicy)でプログラムの動きを見るときは、ドメイン遷移画面とドメインポリシー画面を切り替えて使います。
- ドメイン遷移画面でドメインを選択して、[Enter]キーを押すとポリシー設定画面に切り替わります。



ドメイン遷移画面の読み方

プロファイル
(動作モード)
0 : 無効
1 : 学習
2 : 確認
3 : 強制
※今回の設定です

```
0:  1     <kernel>
1:  1  *      /etc/rc.d/init.d/acpid    ドメイン
2:  1            /bin/bash
                       /usr/sbin/acpid ( -> 706 )
3:  1            /bin/touch
4:  1            /sbin/consoletype
```

読み下すと…

1. <kernel>から/etc/rc.d/init.d/acpidが実行され、
2. /etc/rc.d/init.d/acpidから/bin/bashが実行され、
3. /bin/bashから/usr/sbin/acpidが実行されている
4. /etc/rc.d/init.d/acpidから/bin/touchが実行されている。
5. /etc/rc.d/init.d/acpidからsbin/consoletypeが実行されている。

ドメインポリシー画面の読み方

ドメイン

アクセス許可リスト

```
<kernel> /etc/rc.d/init.d/acpid
    0: allow_execute     /bin/bash
    1: allow_read        /bin/bash
    2: allow_execute     /bin/touch
    3: allow_read/write /dev/pts/¥$
    4: allow_read/write /dev/tty
    ...
```

読み下すと...

- <kernel>から実行された**/etc/rc.d/init.d/acpid**には、以下のアクセスのみを許可する
  - /bin/bash、/bin/touchの実行
  - /bin/bashの読み込み
  - /dev/pts/¥$、/dev/ttyの読み書き
  - ...

ログファイル

- TOMOYO Linuxのログファイルは、２種類あります。
  1. アクセス拒否ログ（reject_log）
     - ポリシーに未定義の動作をした時に記録される
  2. アクセス許可ログ（grant_log）
     - ポリシーに定義された動作をした時に記録される
- ログファイルの保存設定手順は、インストール手順を参考にしてください。
     - 今回は/var/log/tomoyo/reject_log.txtにあります。

ログの読み方

```
#2009-01-15 15:03:44# profile=1 mode=learning pid=1128 uid=0 gid=0・・・
省略・・・ state[0]=0 state[1]=0 state[2]=0
<kernel> /usr/bin/gnome-terminal /bin/bash /bin/cat
allow_read /etc/ccs/profile.conf
```

禁止された操作（reject_logの場合）

ドメイン(プログラム)

アクセス日時、プロファイル、動作モード、pid、uid、gidなど
プログラム実行時の情報

(推測しながら)
読み下すと…

2009/1/15 15:03:44に学習モードでrootユーザが、gnome-terminalでcatを実行して、/etc/ccs/profile.confを表示した。(一部省略)

さらに

- ファイルアクセス以外も、次のような情報を取得することが可能です。
  1. ネットワークアクセス
     - IPアドレスとポート
  2. 実行時に必要とするケイパビリティ
  3. 実行時に必要とする環境変数
  - 上記の情報を取得するためには、policy.confの内容を変更します。

詳細はhttp://tomoyo.sourceforge.jp/ja/1.6.x/policy-reference.html#profile

TOMOYO Linuxの情報

- 最新の動きは「2ちゃんねる」のTOMOYOのスレッドは、「TOMOYO」で検索すると見つけれます。
  - http://2ch.net
- イベント情報は「はてなキーワード」から確認できます。
  - http://d.hatena.ne.jp/keyword/TOMOYO%20Linux
- 操作方法やソースコードはプロジェクトホームページで公開しています。
  - http://tomoyo.sourceforge.jp/
- メーリングリスト
  - tomoyo-users@lists.sourceforge.jp
  - tomoyo-dev@lists.sourceforge.jp

Q&A

- 質問があればご遠慮なく
- お配りしたQ&Aも参考にしてください
- 今は質問なくても、聞きたくなったら「2ちゃんねる」や「メーリングリスト」へお願いします
- **ぜひTOMOYOを使ってみてください**