TOMOYO Linux Q&A

TOMOYO Linux プロジェクト
2009 年 2 月 2 日

概要

TOMOYO Linux について、これまでよく聞かれた質問について、分類ごとに回答をまとめてみました。

1 TOMOYO Linux概要

Q. TOMOYO Linux とはそもそも何ですか?
A. NTT データが開発し、オープンソースとして公開している Linux セキュリティ強化のパッチとユーティリティ、および開発しているプロジェクトの名前です。

Q. ディストリビューションではないのですか?
A. 世の中には多くの Linux ディストリビューションが存在しますが、各ディストリビューションで用いられているカーネル(中核となる部分)は、「メインライン」と呼ばれる Linux の標準ソースコードから作られています。 TOMOYO Linux はカーネルのソースコードに対するパッチで、パッチを適用すれば各ディストリビューションを TOMOYO Linux 対応にすることができます。一種、「拡張機能」でありディストリビューション自体ではありません。

Q. ということは使うためには、自分でパッチをあててカーネルを構築しないといけないのですか?
A. それでは利用者の方が不便なので、 Red Hat, Debian など主要ディストリビューションについて、あらかじめパッチを適用してコンパイル済みのパッケージも配布しています。ダウンロードして、rpm などのコマンドを実行するだけで使えます。

Q. でもやっぱりインストールしないと使えないんですよね?
A. Ubuntu, CentOS, Turbolinux Client 2008 については、 LiveCD(CD から起動してメモリ上で動作する)も提供しています。既存の環境に影響を与えずに経験することができます。

Q. LiveCD 版はどうやって作っているんですか?
A. 元となる LiveCD に含まれているカーネルを TOMOYO Linux 対応のものに取り替えています。それぞれの LiveCD がもともと持っている機能は全部そのまま使えて、その上に TOMOYO Linux 機能も追加されているとお考えください。

Q. どうやって利用するのですか?
A. イメージファイルと手順をプロジェクトの Wiki ページで公開していますのでそちらをご参照ください。簡単に言うと、イメージファイル (ISO)をダウンロードして、 CD-R 等に焼いて利用します。

2 機能

Q. TOMOYO Linux の特徴はなんですか?
A. セキュリティ強化の設定(ポリシー)について、管理者が理解し、編集できる点が最大の利点です。プロジェクトでは、DIY (Do It Yourself)型と説明しています。

Q. 逆に言うと SELinux や他のセキュリティ強化は理解し、編集できないということですか?
A. SELinux は多くの機能を持ち強力ですがあまり使いやすいものではありません。また、「SELinux のポリシーは、 Linux を知り尽くしたセキュリティのプロが書くものであって、一般の利用者は下手にいじらないほうが良い」というスタンスで開発されています。

Q. 何故 TOMOYO Linux だと DIY になるのでしょう?
A. TOMOYO Linux は「パス名ベースのセキュア Linux」と呼ばれています。これはポリシーをパス名（ファイル名やディレクトリ名）を用いて書くことを意味しています。同じパス名ベースとして、Novell の AppArmor がありますが、それ以外は「ラベルベース」と呼ばれます。

Q. 何故 DIY にする必要があるのでしょうか?
A. 同じディストリビューションであっても利用する状況、ユーザによって使い方はさまざまです。TOMOYO Linux のポリシーは、いわばオーダーメイドの服のようなもので、利用者の方が使いたい内容に合わせて作り込むことにより、セキュリティを高めることができます。

Q. セキュリティを高められても作るのが大変では困るのですが...
A. 後述する学習モードを活用すれば大丈夫です。

Q. パス名ベースとラベル名ベースはどちらが優れているのですか?
A. ラベル名ベースは、情報セキュリティの研究の歴史に基づいたものであるのに対して、パス名ベースは AppArmor や TOMOYO Linux が提唱した非常に新しい方式です。一般的な認識としては、「情報フロー制御」の観点からは、ラベル方式のほうが良いと言われていますが、パス名方式について課題、有効性とも未知数の部分があります。プロジェクトでは、将来的にはパス名方式とラベル名方式が協調して動作する方向に向かうと予想しています。

3 ポリシー

Q. ポリシーとは何ですか?
A. セキュリティを強化した Linux では、管理者も例外とせずに不必要な機能の実行を拒否することにより、クラッキング被害などを限定します。必要か不必要かの判断基準となるのが、ポリシーと呼ばれる設定です。

Q. ポリシーは誰が書くのですか?
A. TOMOYO Linux の場合には、管理者が作成します。

Q. どうやって書くのでしょう?
A. TOMOYO Linux は「学習モード」と呼ばれる機能を備えています。これは、操作を行うことによりその操作に必要な機能を記録し、ポリシーとして保存するものです。 TOMOYO Linux のポリシーは可読性が高く、標準的なスキルを持ったシステム管理者であれば誰でも理解し編集できます。

Q. 学習漏れがあったらどうするですか?
A. 学習機能はポリシー策定の際の参考素材を提供するものとお考えください。学習した結果はその内容を確認した上で実際の保護を開始します。

4 情報

Q. 導入事例はあるのでしょうか?
A. お客様ご都合により名称は書けませんが、国内規模のシステムのファイアウォールサーバに導入され、稼働中です。その内容について、 2006 年 5 月に講演を行っており、講演資料は公開しています。その内容は内閣官房情報セキュリティセンターの調査報告の資料の中にも含まれています。また、平成 19 年度下期に実証実験として、 NPO 日本ネットワークセキュリティ協会の Web サーバに導入し、現在も稼働中です。その内容について、報告書が公開されています。

Q. TOMOYO Linux を導入した場合の性能への影響は?
A. 計測結果について Wiki で公開していますが、数パーセント程度です（ SELinux もほぼ同程度）。

Q. 「メインライン化」とは何ですか?

A. あらゆる Linux ディストリビューションは、 www.kernel.org で公開されている Linux 標準カーネルソースをもとにしています。 TOMOYO Linux の機能をその標準カーネルに追加する作業をメインライン化と呼んでいます。

Q. 具体的には何をするのですか?
A. 明文化された手順や規約はありませんが、メーリングリストにパッチを投げて提案し、議論します。メインラインはその内容によりメンテナーと呼ばれる管理者が決まっており、該当するメンテナーが承認することにより標準ソースコードに取り込まれます。

Q. メインライン化の見込みは?
A. TOMOYO Linux の名前は、世界のセキュリティ関連 Linux 開発者に知られており、「候補」として認識されています。今年度末達成に向けて活動しています。

Q. メインライン化されていない状態で利用しても問題ないのでしょうか?
A. プログラム(パッチ)の内容については、これまでの提案から得られた指摘を反映してきており実用的な意味での問題はありません。

Q. 商用製品からの移行する場合に、機能面で問題(不足)はないのでしょうか?
A. TOMOYO Linux は、通常のサーバの運用については必要十分な機能を有していますが、実際に利用(評価)いただきご確認いただきたいと思います。

Q. その他、TOMOYO Linux として主張したい点はありますか?
A. TOMOYO Linux は「実際に管理、運用できる」という点において他を寄せ付けないレベルに到達しています。簡単な使い方ならその日のうちに習得できます。

5 情報源

1. **TOMOYO Linux とは(はてなキーワード)**
   http://d.hatena.ne.jp/keyword/TOMOYO%20Linux
   TOMOYO Linux の最新情報を公開しているインフォメーションセンターです。主なイベントは時系列で記入されており、イベントで使用した資料へのリンクもあります。また TOMOYO Linux が含まれたブログ(はてなダイアリー)を探すのにも便利です。

2. **TOMOYO Linux LiveCD**
   http://tomoyo.sourceforge.jp/wiki/?TomoyoLive
   PC にインストールしなくても、CD から起動するだけで既存の環境を壊すことなく簡単に TOMOYO 使用できます。そこで TOMOYO Linux を手軽に使っていただくために、Ubuntu と CentOS 版の LiveCD を公開しています。TOMOYO Linux LiveCD のダウンロードへのリンク、使い方が掲載されています。

3. **TOMOYO Linux の世界**
   http://tomoyo.sourceforge.jp/wiki/?WorldOfTomoyoLinux
   技術評論社の Software Design 誌にて、2007 年 1 月号から 12 回にわたって連載された TOMOYO Linux の紹介記事です。TOMOYO Linux に関する詳細な解説がされています。

4. **JNSA セキュア OS 導入結果の報告書**
   http://www.jnsa.org/result/2007/tech/secos/
   2007 年に日本ネットワークセキュリティ協会(JNSA)にて、TOMOYO Linux を用いたサーバの導入について、「セキュア OS の導入に関する課題の試行結果報告書」として報告書が公開されています。

5. **TOMOYO Linux プロジェクトホームページ**
   http://tomoyo.sourceforge.jp/ (日本語)
   http://elinux.org/TomoyoLinux (英語)
   TOMOYO Linux の情報へのリファレンスがあります。TOMOYO Linux についてもっと情報がほしい場

合は、こちらを探して見てください。

6. メーリングリスト

http://lists.sourceforge.jp/mailman/listinfo/tomoyo-users
http://lists.sourceforge.jp/mailman/listinfo/tomoyo-users-en
http://lists.sourceforge.jp/mailman/listinfo/tomoyo-dev
TOMOYO Linux の利用者向け（日本語版と英語版）と開発者向けがあります。どなたでも登録が可能です。またアーカイブも一般公開していますので、過去のやり取りもチェックすることができます。
TOMOYO Linux についてわからないことや、やってみたいことがあれば、メーリングリストへ投稿してください。