

最新セキュアOS事情 (Linux)

Linuxは、サーバやPC用のOSとしてだけでなく、モバイル情報端末や携帯電話といった機器に採用されるようになり、その用途は拡大傾向にある。そのためLinuxのセキュリティへの関心も高まっている。本稿では、LinuxにおけるセキュアOSの取り組みについて、TOMOYO Linuxのプロジェクトマネージャ原田季栄氏が、その基本的な考え方、セキュリティ強化のための方式の解説を含む現在の状況、さらには今日に至るLinuxセキュリティ強化の歴史までを、わかりやすく解説する。



原田 季栄

(Toshiharu Harada)

[haradats@gmail.com]

TOMOYO Linuxプロジェクト
プロジェクトマネージャ

1985年北海道大学工学部応用物理学科卒。同年NTTに入社し、現在の所属はNTTデータ技術開発本部。MITでのマルチメディアオーサリングシステムの開発、郵政省(当時)地上波デジタル放送実験マルチメディアシステム開発リーダー、BSデジタルデータ放送などの放送関連システムの開発とプロジェクトマネージャを経て、2003年よりOSSの研究開発に取り組む。「使いこなせて安全」なLinuxを目指すTOMOYO Linuxのプロジェクトマネージャ。

●イラスト/五十嵐 晃(五十嵐晃事務所)

はじめに

編集部の方より「Linuxのセキュリティの動向について書いて欲しい」とお話をいただいたとき、内心困ってしまいました。

それはひとつには、私が取り組んでいるLinuxのセキュリティ強化(いわゆるセキュアOS)は、確かに「セキュリティ」という言葉はついていますが、暗号理論などいわゆる「情報セキュリティ」とはやや意味が異なるからです。また、ちょうど今(この原稿は2007年11月に書いています)、この分野において大きな動きがあり、何を書いたとしても雑誌が店頭で並ぶ頃には内容が古くなってしまふこと、最後に、提示された紙数ではとても十分な説明ができない

と考えたからでした。

しかし、携帯電話、デジタルテレビなど組み込み機器におけるLinuxの採用は増加の一方です。今やLinuxのセキュリティは開発関係者や専門家だけの話題ではなく、より広くつづつあるように思います。一般の方々に向けて、Linuxセキュリティ強化の現状をお伝えするのは義務であると思ひ、お引き受けした次第です。Linuxをお使いになっていない方々にもおつきあいいただければ幸いです。

基礎知識(概念編)

■セキュアOSの基本的な考え方

Linux、BSD、Microsoft Windows、あるいはMac OS XなどのOSは汎用

汎用でないOSとしては、最近あまり姿を見なくなった専用ワープロ機や医療、軍事、金融等などの特定の用途に向けて開発されたシステムのOSがあるでしょう。

2つの中間に「組み込み系」と呼ばれる汎用OSを用途に特化させたようなものが存在します。Linuxを含めた汎用OSは基本的な考え方として、「可能な限り多くのことができるように」ということを目指し作られています。それをどう実現するかというと、「パーツを提供し、それを組みあわせてもらう」ということです。おもちゃのレゴを用いて驚くような造形が作成可能であるのと同じ原理です。

レゴのパーツは単純なので説明がなくとも組みあわせられますが、OSの場合

は部品の種類が多く、部品には使い方(インターフェイス、仕様書)が提供されています。部品の構成はレイヤー化されていて、用途に応じて、利用者を選択します。組み合わせられた部品を動かす力は、カーネルと呼ばれるOSの核にあります。

汎用OSの最大の利点は、「同じ部品を使ったものは、自分以外の環境でも利用できる」こと、すなわち流通できるということです。流通することにより、組み上げられたソフトウェアは多くの人々が利用することが可能になり、「発展」「進化」が可能になります。

オープンソースのOSの象徴ともいえるLinuxは誰でも無償でダウンロードできます。改造しても良いし、商用利用も可能です。RPMに代表されるパッケージ管理システムの恩恵により導入や環境設定が困難という課題もほぼ解消しましたし、導入もGUIが標準になりました。

OS自体の機能だけでなく、利用できるソフトウェア(パッケージ)の数も増えており、そのことは基本的には良いことなのですが、これが仇になる場合があります。サーバの乗っ取り、データの改ざん等近年報告されている情報システムの被害は、ソフトウェアの脆弱

権限の分割により「全滅」を避けられる



性(いわゆるバグ)をつかれることにより発生します。

含まれているパッケージが多ければそれだけ「攻撃対象」が広がります。また、乗っ取られた場合にOSのフルの機能がフルに利用できてしまうのではクラッカーの思うつぼです。六畳一間でつましやかな生活をしていれば空き巣が入ってもさしたる被害を受けないでしょうけれども、シーズンオフに郊外のリゾートホテルを借りきって生活してれば、目も行き届きませんし被害を受けるリスクは規模に比例します。

攻撃を受けるきっかけとなる「脆弱性」について少し補足しておきます。もっともよく知られている脆弱性は「バッファオーバーフロー」です。これは、外部からプログラムを故意に不正な状態に追い込み、それにより自由に操るという手法です。

バッファオーバーフローを含め、ソフトウェアの脆弱性とは、いわゆる「バグ」です。バグは最終的には人為的な間違いに帰着し、根絶することができません。その事実を受け入れると、プログラムの乗っ取り行為の起こる可能性はゼロにできないことがわかります。

乗っ取られてしまうと、標準の(セ

キュリティを強化されていない)OSでは、クラッカーの思いのままになってしまうため、それをなんとかしようと考えられたのが、セキュアOSです。セキュアOSは、「クラッキングを受けた際にその被害を軽減する」ために考案されたもの、とご理解ください。

■具体的な強化の方法

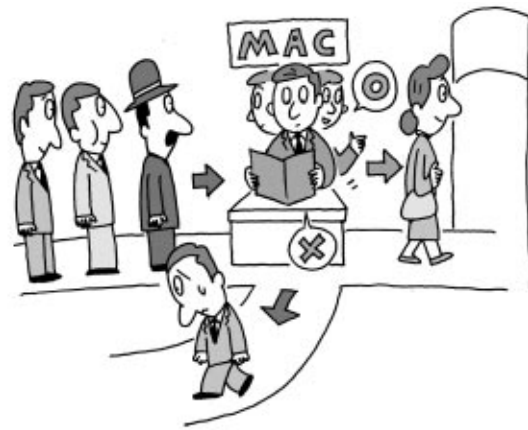
絶対的な定義が存在するわけではないのですが、現在、比較的一般的になっていると思われるのは次の2点です。お読みになっていただければわかりますが、これはLinuxに限った話ではなく、一般的な概念です。

□最少特権(Least Privilege)

いかめしい言葉ですが、意味は簡単で、要するに「権限を集中させずに分割させよう」という考え方です。

例えば、あなたが巨大な工場のオーナーでその管理の委託を考えているとします。監督を一人の人間に委託すると、その人物が悪意を持つと全ての工場が被害に遭う可能性があります。それが、たとえば、衣類、貴重品、書類のように工場の種別により複数の人間に監督を割り当てると全ての工場が同時に被害に

■ ポリシーは例外なく「強制的に」適用される



遭うことはないでしょう。

実は、セキュリティを強化されていないLinuxは実質的に監督が一人の状態です（なので、クラッカーは常にその監督の権限を奪うことを考えます）。

□ アクセス制御の強化 (MAC)

本稿では技術用語は極力用いないようにしていますが、ここだけは覚えておくと良いでしょう。Mandatory Access Control (「強制アクセス制御」) で、よく“MAC”と呼ばれます。名前は専門的ですが、意味的には、

- ・もれや例外なく
 - ・発生するアクセスを
 - ・厳密に判定して
 - ・適切なものだけを実行し、不適切なものを拒否しよう
- ということです。

「厳密に」の部分を読むと、そこに何らかの判断基準、あるいはルールが必要であることがご理解いただけると思います。それが、「ポリシー」と呼ばれるものです。したがって、ポリシーに相当するものを持たないセキュアOSは存在しません。

MACの反対のものとして、DAC (Discretionary Access Control) があ

ります。日本語では「自由裁量のアクセス制御」と呼ばれます。DACでは上記を満たすことができないので、それを補うものとしてMACが考えられたとご理解ください。

ここまですとまとめると、要するにLinuxのセキュリティ強化とは、「権限を分割して、ポリシーという定義により機能の呼び出し（アクセスの制御）を厳密に判断するようにしたもの」ということとなります。機能の名前や実現方法は異なっても上記の考え方はどのセキュアLinuxにも共通です。

■ Linuxセキュリティ強化の状況

■ 2007年11月現在の動向

基本的な概念を理解していただいたところで、本稿を執筆している2007年11月「現在」のLinuxセキュリティ強化の動向について解説することにします。Linuxには多くのバリエーションがありますが、標準となるLinuxはひとつで、それは「標準カーネル」あるいは「メインライン」と呼ばれます。

SELinuxは既にメインラインに含まれていますが、現在メインライン化を提案しているLinuxのセキュリティ強化の

実装は「Smack (Simplified Mandatory Access Control Kernel)」、 「AppArmor」、 「TOMOYO Linux」の3つです。

SELinuxとそれらを整理したものの違いを表1にまとめます。この表は下記URLにある表の2007年11月時点の情報のサブセットです。

(<http://tomoyo.sourceforge.jp/wiki-e/?WhatIs#comparison>)

表には見慣れない言葉が並んでいて抵抗を覚えた方もあるかもしれませんが、前述の概念が頭に入っていれば十分理解できます。この表には、Linuxセキュリティ強化の「エッセンス」が盛り込まれており、これを理解できれば、Linuxのセキュリティ強化を理解したと言っても良い、と思っています。以下、項目ごとに説明します。是非勇気をもって読み進んでください。

□ 方式

Linuxのセキュリティ強化には、ラベル方式、もうひとつはパス名方式という2つの方式があります。これはLinuxのセキュリティ強化の分類を行う際にもっとも重要な項目です。

これら2つが何に関する方式かという

表1 SELinuxと現在メインライン提案中のセキュアOSの概要

	SELinux	Smack	AppArmor	TOMOYO Linux
開発元	NSA	Casey Schaufler	Novell	NTTデータ
方式	ラベル	ラベル	パス名	パス名
メインライン提案状況	取り込み済み	取り込み予定	提案中	提案中
採用ディストリビューション	Red Hat, Hardend Gentoo		SUSE, Ubuntu 7.10	TurboLinux 11 Server
対応カーネルバージョン	2.6 (LSM)	2.6 (LSM)	2.6 (LSM)	2.6 (LSM/独自フック), 2.4
MLS機能	○	○		
MCS機能	○			
RBAC機能	○			
ドメイン定義方法	手動	手動	手動	自動
ポリシー作成方法	配布 (reference policy) + カスタマイズ	自作	配布 (profile) + カスタマイズ	自作
ポリシー生成機能	ログから変換	なし	ログから変換	リアルタイム
MACモード切り替え	システム全体	システム全体	プログラム単位	ドメイン単位

と、「ポリシーの記載」に関するものです。ひらたく言えば、「ポリシーを書くときにパス名（いわゆるファイル名やディレクトリ名など）で記述する」のがパス名方式。「ポリシーをパス名でなくラベルにより記述する」のがラベル方式です。

パス名方式であるAppArmorとTOMOYO Linuxのポリシーを眺めると、いずれも見慣れたパス名表記が含まれています。ところが、SELinuxやSmackのポリシーは、パス名は一部しか登場せず、記号のような名前（SELinuxであれば“_”で終わる）が多数存在しています。これが「ラベル」です。

パス名はもともと存在しており見えますが、ラベルはもともとLinuxには存在していなかったものです。ラベル方式では、存在するファイルやディレクトリなどにラベル名を付与（定義）して、ポリシーではそのラベル名で記述することになります。パス名方式のセキュアOSのポリシーは眺めているとなんとなく何をやろうとしているかわかりませんが、ラベル方式のセキュアOSのポリシーは、暗号のように見えます。当然ながらわかりやすいのは、パス

名方式ですが、パス名方式の問題としてよく指摘されるのは、パス名の偽装に対するリスクです。たとえば、passwordというファイルがあったとして、それを何らかの形で、buzzwordという「別の名前に見える」ようにされると、passwordを保護しておいてもその内容が参照されたり改ざんされたりするということです。パス名方式の場合には、そうした場合を防ぐように設計されていますが、そのリスクはゼロにはできません。

それに対して、ラベル方式では（変えられる可能性がある）パス名ではなく、割り付けられたラベルを用いるので安全というのがラベル方式を推すグループの基本的な主張です。実は、ラベルが正しく維持されるかという点についてはパス名方式と同様の問題が付きまとうのですが、一般的にはラベル方式のほうが主流であり、より安心と考えられているとご理解ください。

□ メインライン提案状況

この項目は、メインラインへの提案状況を示しています。Linuxでは独自に開発した成果をLinux自体に取り込んでもらうための手段としてLKML (Linux

Kernel Mailing List) と呼ばれるメーリングリストを使用しています。オンラインの表では、各セキュアOSの提案内容へのリンクを含めています。投稿されたメッセージとそれに関する議論のスレッドをたどれますので、興味ある方はブラウザから追いかけてみてください。

Smackは2007年6月から約半年の間に実に11回もの提案を投稿しており、これは驚くべき作業量とレスポンスです。最古参のAppArmorは、2006年の4月から5回の投稿を行っていますが、各投稿について恐ろしく長く議論が続いており、このような形になっています。TOMOYO Linuxは、2007年6月がデビューで、これまでに5回投稿をしています。

□ 対応カーネルバージョン

これは対応しているカーネルのバージョンです。Linuxには、2.4と2.6の二つのバージョンがあり、現在の主流である2.6にはLSM (Linux Security Module) と呼ばれる、セキュリティ強化のための仕組み（フレームワーク）が追加されています。

表を見ると、TOMOYO Linux以外は、全て2.6 (LSM) で、version 2.6カーネル