

特集

Linuxの セキュリティ 機能

編集にあたって

杉田由美子 (The Linux Foundation) 須崎有康 ((独)産業技術総合研究所)

Linux はサーバや組込みにおける利用率が高く、一般ユーザには縁がないものという印象があったが、Google Chrome OS や Android の登場により身近なものとなりつつある。PC だけでなくネットブックやスマートフォンなどの資源がネットワークで相互接続され、面識のない世界中の人たちと通信を行う

現状において、マルウェアの侵入や感染を防ぎ、感染した際には迅速な検知と駆除を行うセキュリティ強化は重要な課題である。OS の提供するセキュリティ機能は最も重要な要素の1つであり、Linux においても研究・開発が進んでいる。2010年8月にボストンで開かれた Linux 技術に関する国際会議

LinuxCon においても「Linux Security in 10 Years」の発表が行われ、各種の機能追加の経緯および今後の課題が話された。

この特集では、Linux システムにおけるセキュリティに焦点を当て、脅威の内容、開発されているセキュリティ機能、その特徴と課題を、設計思想や実装方式とともに紹介する。Linux における多様なセキュリティの取り組みを紹介することによって、今後のセキュリティのあり方を議論するきっかけにしたい。さらに、汎用機器の利用者にも、システムの安全度・脅威度を知っていただく一助になればと考えている。

幸い、日本には、Linux の開発コミュニティでセキュリティ機能を検討・開発している主要メンバがいるので、彼らにセキュリティ機能の解説をお願いした。多忙な中で今回の執筆を引き受けていただいたことに、この場を借りて深く感謝申し上げる。なお、数名の執筆者は、9月に東京で行われるLinuxCon Japan において本特集に関連した発表を行う予定であり、本特集が出版される際にはその成果が評価されているものと期待している。

本特集では、6つのテーマでLinuxのセキュリティについて解説する。Linuxの想定する脅威モデルの解説から始まり、Linux 2.6で採用されている個々のセキュリティ機能 (SELinux, TOMOYO Linux, IMA) を掘り下げて、脅威モデルに対するそれぞれの対処法を解説する。また、今後広く普及が進むと考えられる Chrome OS は Linux ベースであるが、ファームウェアと連携した独特なセキュリティ機能を提供しており、この方式の解説を行う。

最初の「OS へのセキュリティ脅威とLinuxの強制アクセス制御」では、Linuxのセキュリティ機能がどのような思想のもとに設計され、どのような脅威に対処するのかを解説している。Linux カーネルのセキュリティがどのような構造になっているか、その構造でできること、できないことを解説している。

具体的なLinuxのセキュリティ機能に関しては、バージョン 2.6 系で実装されている SELinux,

TOMOYO Linux, IMA について取り上げた。

まず「SELinuxのアーキテクチャとアクセス制御モデル」では、SELinuxがどのような思想と実装方式でセキュリティを実現しているかを、分かりやすく説明する。「セキュリティポリシー設定簡易化手法」では、強制アクセス制御方式が生まれた背景に触れ、強制アクセス制御方式が抱えるポリシー設定の対策について紹介する。

「ラベルに基づくセキュリティの限界とその補完」では TOMOYO Linux (名前に基づくセキュリティ) が開発された背景や設計思想を説明する。ラベルに基づくセキュリティ方式を採用した SELinux が開発されていた中で、TOMOYO Linux をなぜ開発したのか、どのような特徴を持つのかについて述べる。

「高信頼を実現するLinuxの新しい機能」では、Linuxのバージョン 2.6.30 (2009年6月公開) から導入された、IMA (Integrity Measurement Architecture) について解説する。背景にある考え方は Trusted Computing であり、セキュリティチップと連動して高信頼システムを構築する。ここではLinuxでどのように実装しているかを、使い方を交えて紹介する。

「Google Chrome OSの構成から見るセキュリティ対策」では、Google社がネットブック向けに開発している Chrome OS のセキュリティ対策について解説する。Chrome OS はソースコードが公開されており、現在も開発中である。Web ブラウザを動作させるという用途に対して行われている5種類のセキュリティ対策について紹介する。

利用者や社会に大きな被害を及ぼすマルウェアが後を絶たず、セキュリティには「これで大丈夫」と言えることはない。今回の特集が、より強固なセキュリティ対応を実現するために、機能間連携や新たな発想の機能などを議論するきっかけになれば幸いである。

(平成 22 年 8 月 9 日)