5A-3

# 組込み機器におけるセキュアＯＳ導入評価

矢野 啓二郎† 上床 克樹† 安井 啓介† 佐久間 毅† 島田 智文†

株式会社 東芝†

## 1 はじめに

近年のデジタル情報家電などの組込み機器では、ネットワーク機能をはじめとして、最新技術へのタイムリーな追従のために、Linux などのオープンソースを利用する例が少なくない。このような組込み機器では、インターネットなどの機器外部と接続するモジュールに脆弱性が存在すると、外部からの攻撃を受け、個人情報の流出などユーザの利益を損なう可能性がある。

いくつかの組込み機器では、ソフトウェアのアップデート機能を提供しているものもあり、製品出荷後に不具合や脆弱性が発見された場合などでも対策を講ずることも可能であるが、PC などのような頻繁なアップデートは困難なことが多く、0-day attack などにも対応できない。

そこで、組込み機器の OS においても、セキュア OS を導入し、外部からの攻撃を受けた場合にも、被害を最小限にする取り組みを行うことが重要な課題となってきた。

そこで我々は、メモリ使用量、CPU 性能等、ハードウェア資源が限られた組込み機器を対象とし、Linux 用のセキュア OS の導入について評価を行った。

## 2 Linux 用セキュア OS

Linux Kernel 2.6 から、LSM(Linux Security Modules)というフレームワークが採用され、Kernel が標準で提供するセキュリティ拡張用のインタフェースが用意されている。我々は、Kernel のバージョンアップが行われた際の追随性を考慮し、LSM を利用したセキュア OS を対象にすることとした。

Linux 用のセキュア OS としてよく知られているものには、SE Linux[1]がある。SE Linux は Linux 2.6 に標準で組み込まれており、サーバ系などでの実施事例も多い。

もう一つは LIDS(Linux Intrusion Detection System)を対象とした。LIDS はオープンコミュニティにより開発が進められている LSM 対応のセキュリティ・モジュールであり、使用方法が比較的容易なことから、近年注目を集め始めている。

LIDS は参考文献[2]から入手可能であり、日本国内でも[4]から情報を得ることが可能である。

## 3.機能比較

組込み機器の OS としてセキュア OS を導入するにあたり、導入要件、セキュリティ機能、そして組込み機器で考慮する必要がある、メモリ使用量、性能への影響について述べる。

セキュア OS の評価項目として Linux コンソーシアムがまとめた参考文献[5]をベースとしたが、対象モデルとしてデジタル情報家電とし、いくつかの評価項目を追加した。また、MIPS アーキテクチャを使用し、Linux 2.6.10 が動作する実機上での評価結果も加えた。

### 3.1 導入要件

デジタル情報家電を開発する上で考慮する必要がある導入要件の比較について、表 1にまとめた。

表 1 導入要件比較

| | SE Linux | LIDS |
|---|---|---|
| Kernel version | 2.6 | 2.4 / 2.6 |
| CPU architecture | 非依存 | 非依存 |
| Filesystem | 拡張属性対応必須 | 非依存 |
| Busybox 拡張 | 必須 | 不要 |
| 専用ライブラリ | 必要 | 不要 |

Busybox[6]とは、Linux 上の基本コマンドを一つにまとめたプログラムであり、Linux を採用した組込み機器でよく利用されている。SE Linux では、ps, ls などいくつかのコマンドにおいて SE Linux の API を使用する。この対応のために Busybox に特別な対応が適用され、Busybox とリンクさせる専用ライブラリも必要となる。Busybox 1.1.0 pre1 から SE Linux 対応が追加されている。

また、組込み機器を対象とした場合、SE Linux では Filesystem において特別な機能が必須となる点が重要なポイントとなる。Linux 2.6.10 において、Kernel がサポートするすべての Filesystem で、この拡張属性対応がなされているわけではない。我々が対象モデルとしているデジタル情報機器では、Filesystem の一つとして cramfs を使用しており、この拡張属性対応が含まれていない。今回の我々の評価では、cramfs に対して拡張属性対応を新たに追加実装して実施した。

### 3.2 セキュリティ機能

表 2にセキュリティ機能に関する比較表を示す。

ここでは、攻撃を受ける可能性があるプロセスをサンドボックス化し、被害を最小限度に抑えることが可能であるかどうか、という観点で特に注意すべきと考えられる項目について下記で述べる。

#### ーアクセス制御の粒度

SE Linux はセキュリティ制御の対象となるクラス（ファイル・ディレクトリやプロセスなど）が 52 種類と非常に豊富であり、それぞれのクラスに応じ、のべ 210 種類のアクセスベクタを用いて、きめ細かなアクセス制限をかけることが可能である。

一方、LIDS ではファイル・ディレクトリなどに対して READONLY/APPEND/WRITE/DENY の 4 種類のアクセス制限を行える。プロセスに対しては、Linux が標準で提供する POSIX ケーパビリティの 28 種類に、LIDS 固有の 3 種類が追加される。

#### ーリンクに対するアクセス制限

LIDS は Linux Kernel の VFS 層でセキュリティ制御を行っており、各ファイルの inode 番号毎にセキュリティ設定を管理している。リンクは正規化されてリンク先の inode 番号を取得してセキュリティ設定を行うため、リンク自身にはセキュリティ設定を行うことが出来ない。

組込み機器においては、Busybox を使用することが多い。Busybox は提供するコマンドをシンボリックリンクで実現するため注意が必要となるが、攻撃を受ける可能性があるプロセスに対して、Busybox で提供するすべてのコマンドの利用を制限すれば問題ない。

Evaluation of Secure OS for Embedded Devices
† Embedded System Platform Development Department,
CORE TECHNOLOGY CENTER, TOSHIBA CORPORATION

**ースペシャル・ファイルに対するアクセス制限**

LIDS では POSIX ケーパビリティと組み合わせてブロックデバイス・ファイルの制限を実施する、または/dev 以下をアクセス不許可にすることは可能だが、cramfs の場合には個々のスペシャル・ファイル毎にアクセス制限を行うことが不可能である。これは、cramfs がスペシャル・ファイルの inode に同じ inode 番号を割り振ってしまうからである。

ディレクトリを分割する等により対策が可能ではあるので、システムとしての構成によっては特に問題とはならない。

**ープロセス間通信に対するアクセス制限**

組込み機器では、複数のアプリケーションが連携することによって機器としての一つの機能を提供する形態をとることが多く、その連携のためにプロセス間通信を利用するのが一般的である。

SE Linux では、システムコール毎に細かくアクセス制限をかけることが可能である。

LIDS では、共有メモリのロックに対する制限や、IPC の権限チェックを行うようにすることは可能であるが、システムコール毎、パイプに制限することは出来ない。

SE Linux ではシグナルに対しても細かくアクセスを制御可能だが、LIDS では KILL などの特別なシグナルのみが対象となる。

攻撃から保護したいプロセスが利用するプロセス間通信やシグナルが問題にならないかの検討が必要である。

**ーカーネル・ログに対するアクセス制限**

LIDS ではカーネル・ログに対する読み込みを制限することが出来ない。

組込み機器においては、カーネル・ログは不必要であることが多く、カーネル・ログの出力を抑制することで対策することは可能である。

**ープロセス毎のアクセス制限**

LIDS でもプロセス名別にアクセス制限を設定することは可能であるが、リンクに対するアクセス制限を実施することが出来ないため、△とした。

また、LIDS では、/proc 以下をアクセス出来ないようにすることで、悪意のあるプログラムからプロセス情報を見えなくすることは可能だが、PID を直接指定したシステムコールを制限出来ない。

**ーユーザ毎のアクセス制限**

SE Linux には RBAC(Role Based Access Control)が用意されているが、LIDS ではユーザ毎の管理は出来ない。

同様の機能が必要な場合には、LIDS では通常のユーザ毎の DAC(任意アクセス制御)と組み合わせて使用する必要がある。

表 2 セキュリティ機能比較

| | SE Linux | LIDS |
|---|---|---|
| アクセス制御の粒度 | 52 種類のオブジェクトクラスに対し、のべ 210 種類のアクセスベクタを設定可能 | ファイル/ディレクトリに対して 4 種類、プロセスに対して 31 種類のアクセス制御可能 |
| ファイル・ディレクトリのアクセス制限 | ○ | ○ |
| リンクに対するアクセス制限 | ○ | × |
| スペシャル・ファイルに対するアクセス制限 | ○ | △ |
| パイプに対するアクセス制限 | ○ | △ |
| プロセス間通信に対するアクセス制限 | ○ | △ |
| カーネル・ログに対するアクセス制限 | ○ | △ |
| カーネルモジュールのロード・アンロード制限 | ○ | ○ |
| プロセス毎のアクセス制限 | ○ | △ |
| ユーザ毎のアクセス制限 | ○ | × |

### 3.3 メモリ使用量および起動時間

当社製 CPU である TX49 用に Linux Kernel のバイナリを作成し、テキスト、データ、bss の変化量を測定した結果を表 3に示す。また、セキュア OS を導入しない場合と比較した起動時間の差を表 4に示す。

表 3 Linux Kernel サイズの差

| | テキスト | データ | bss | 合計 |
|---|---|---|---|---|
| SE Linux | +102,064 | +8,212 | +4,096 | +114,372 |
| LIDS | +42,384 | +12,312 | +1,785,856 | +1,840,552 |

単位：bytes

LIDS は bss が非常に大きく、メモリ使用量に大きな影響を与える。ただし、実際にメモリ使用量を比較する際には、セキュリティ設定ファイル、ライブラリなどの考慮も必須となるため、システム構成によって総合的に判断する必要がある。

表 4 起動時間の差

| | Phase 1 | Phase 2 |
|---|---|---|
| SE Linux | 87 msec | 605 msec |
| LIDS | 32 msec | 67 msec |

起動時間は、Linux Kernel 自体が起動する時間の差を Phase1 とし、セキュリティ設定の読み込み、設定変更などに要する時間を Phase2 とした。

起動時間は、セキュリティ設定内容によって大きく変動するため、SE Linux/LIDS とも、ほぼ同等のセキュリティ設定を作成し計測した。

## 4 まとめ

本論文では、デジタル情報家電などの組込み機器において、SE Linux / LIDS の導入要件、セキュリティ機能について比較を行い、デジタル情報家電用の評価ボード上で両セキュリティ・モジュールを動作させ、メモリ使用量／起動時間の差について測定した。

SE Linux は機能が非常に豊富であり、機能面では十分である。SE Linux で必須となる既存の実行環境に対する新規対応を実現可能であるか、それによる実行性能への影響が許容できるかが、重要なポイントになると考えられる。また、起動時間に与える影響が、LIDS と比較して大きい点も注意が必要である。

一方で LIDS は、既存の Linux 機能の延長上でセキュリティを強化することを基本として開発していると思われ、導入は比較的容易に行える。機能面で不足がないかどうかが鍵となる。

組込み機器にセキュア OS を導入する際には、対象モデルを明確にし、何をどこから守りたいのか、という点について十分に検討して、性能面も十分に考慮の上で最適なセキュリティ・モジュールを選択する必要がある。

## 参考文献

[1] http://www.nsa.gov/selinux/
[2] http://www.lids.org/
[3] http://www.selinux.gr.jp/
[4] http://www.selinux.gr.jp/LIDS-JP/index.html
[5] http://www.linuxcons.gr.jp/pdf/sec04_output.pdf
[6] http://www.busybox.net/