SELinuxで組み込み機器のセキュリティを高める

中村 雄一

Linuxのセキュリティを高める手法の一つとしてSELinuxがある．前編で，SELinuxはLinuxカーネルのパーミッション・チェック機能を拡張し，ファイルやポート番号ごとに細かくアクセス制御を行えることを解説した．今回は組み込み機器でSELinuxを使う方法について，実例を元に紹介する．（編集部）

前編（2008年6月号，pp.128-135）では，SELinuxの仕組みと構成要素について解説しました．今回は，実際に組み込み機器向けマイコン・ボードにSELinuxを移植し，動作させてみます．マイコン・ボードとしては，シリコンリナックス（http://www.si-linux.co.jp/）のCAT760を対象にします（**写真1**）．CAT760はEthernetポートを備えるため，小型のサーバとしても使えます．しかし，サーバをインターネットに接続して使う場合は，当然セキュリティに配慮しなければなりません．今回は，CAT760でhttpサーバを立ち上げ，SELinuxでhttpサーバを最小限の権限で動作させてみます．

なお，今回の例はCAT760ですが，手順の大部分はほかの機器にも共通です．違いは，開発機からターゲット機へのファイル転送方式程度です．また，開発機のディストリビューションは，CentOS 5を前提として話を進めます．

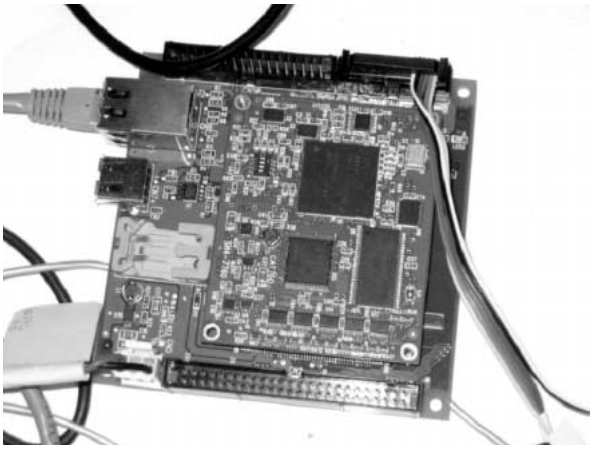

写真1　SELinuxを移植するターゲット・ボード
（シリコンリナックス製CAT760）
200MHz動作のSH7760（SH-4），64Mバイトの RAM，16Mバイトのフラッシュ ROM，Ethernet（100Base-TX）インターフェースを搭載する．

1　一般的な移植手順

組み込みシステムにSELinuxを移植するための一般的な手順は，以下の四つのステップです．

1）SELinuxに関係するプログラムをクロス・コンパイルする
2）最小限のセキュリティ・ポリシ（以下，ポリシと略記）を作成する
3）1）で作成したプログラムと2）で作成したポリシを基に，ターゲット上に最低限SELinuxが動作するシステムを構築する
4）システムに適したポリシを開発する

本稿では，この順番に従ってCAT760ボードにSELinuxを移植してみます．

2　SELinux関連プログラムのクロス・コンパイル

● ソース・ファイルの入手

組み込み機器にSELinuxを導入するためには，SELinuxに対応したカーネルおよびユーザ・ランドのソース・ファイルを入手して，クロス・コンパイルする必要があります．最低限必要なものとして，Linuxカーネル本体，ライブラリlibselinux，コマンドBusyBoxがあります．Linuxカーネルには，SELinuxのアクセス制御エンジンが組み込まれています．libselinuxには，SELinuxの管理操作を行うためのAPIが格納されています．SELinuxに関連する管理コマンドも必要ですが，BusyBoxに取り込まれているものを使い，サイズを小さくします．

表1に示すように，これらのソフトウェアはバージョン

KEYWORD ―― SELinux，組み込みLinux，アクセス制御，Type Enforcement，SELinux Policy Editor

表1
SELinuxを導入するために必要なソフトウェアのバージョンによる違い

ソフトウェア	バージョン	組み込み対応状況
Linuxカーネル	2.6.0以降	SELinuxサポート ext2，ext3でxattrサポート
	2.6.18以降	jffs2のxattrサポート
	2.6.24以降	SELinuxのメモリ消費量を約200Kバイト削減 SELinuxによるread/writeシステム・コールのオーバヘッドを1/10に削減 SELinuxによるセキュリティ・チェックの最悪実行時間を1/3に削減
libselinux	2.0.35以降	libsepolの分離によりファイル・サイズを約300Kバイト削減
libsepol[注]	−	特になし
BusyBox	1.5.0以降	SELinux関連コマンドの取り込み開始
	1.9.0以降	必要最小限のSELinux関連コマンドの取り込み完了

注：実機には入れないが，libselinuxとBusyBoxのコンパイルに必要．

表2
SELinuxを導入するために必要なソフトウェアと入手場所

ソフトウェア	バージョン	ソース・コードの入手先
Linuxカーネル	2.6.24	ターゲット機器の製造元．CAT760の場合は，http://sourceforge.jp/projects/selpe/files/よりダウンロード可能
libselinux	2.0.35	NSAのWebサイト http://www.nsa.gov/selinux/code/download-trunk.cfm
libsepol	2.0.11	
BusyBox	1.9.1	BusyBoxプロジェクトのWebサイト http://www.busybox.net/

によって組み込み機器対応が異なります．カーネルについては，バージョン2.6.0がSELinuxを最低限サポートしています．けれども，jffs2上でシステムを構築するには，2.6.18以降が必要です．2.6.24以降はチューニングが施されており，より組み込みに適しています．libselinuxは，バージョン2.0.35以降がお奨めです．それ以前ではlibsepolが必要ですが，300Kバイトほど容量が増えます．BusyBoxについては，1.9.0以降であれば，必要なコマンド類がほとんどそろっています．

今回は移植のために，**表2**のようなバージョンのソース・ファイルをダウンロードします．なお，これらのファイルは，http://sourceforge.jp/projects/selpe/files/の「CAT 760 SELinux用各種ソース・ファイル」からもダウンロード可能です．

ダウンロードしたら，作業ディレクトリにそれぞれ展開しておきます．

また，CAT760ボードで作業する場合，確実に本記事の例を試すためには，ルート・ファイル・システムを，筆者がSELinuxの動作を確認したものと入れ替えることをお奨めします．ルート・ファイル・システムのイメージは，http://sourceforge.jp/projects/selpe/files/よりダウンロードします．ファイル名はrootfs_selinuxtest.binです．なお，こちらのルート・ファイル・システムには，後述するBusyBoxとlibselinuxが既に移植済みです．イメージをFATでフォーマットしたCompactFlashカードに保存します．ボードにCompact Flashカードを差し込み，CAT760のブート・ローダより以下のコマンドを入力します．

```
>> admin
<パスワード入力（初期設定はsilinux）>
#> cp cf0:rootfs_selinuxtest.bin rom:
rootfs
```

● カーネルのコンパイル

さて，カーネル，libselinux，libsepol，BusyBoxを順番にクロス・コンパイルしていきます．まずは，カーネルです．コンパイル方法は通常のクロス・コンパイルと同じです．

筆者の環境では，次のコマンドでカーネルのコンパイル・オプションを設定します．

```
$ make menuconfig ARCH=sh
```

表3のようなSELinuxに関係するオプションをONにします．

クロス・コンパイルを行います．筆者の環境では，クロス・コンパイラの実行ファイル名は「sh4-linux-gnu-gcc」です．

```
$ make CROSS_COMPILE=sh4-linux-gnu-
$ make CROSS_COMPILE=sh4-linux-gnu-
```