SELinuxで組み込み機器のセキュリティを高める

中村 雄一

組み込み機器がインターネットに接続されるようになり，さまざまな攻撃にさらされることになった．SELinuxは，Linuxのアクセス権限機能を拡張し，ファイルやポート番号ごとに細かくアクセス制御を行うことができる．前編の今回は，SELinuxの概要と組み込み機器への適用の取り組みについて解説する．（編集部）

1　SELinuxはなぜ必要か？

SELinux（Security-Enhanced Linux）とは，LinuxのセキュリティをOSレベルで強化したものです．SELinuxは（Red HatやDebianのような）ディストリビューションの名前ではなく，Linuxカーネル中の一機能の名称です．Linuxカーネル本体の持つアクセス制御機能を強化し，攻撃の被害を最小限に封じ込めることができます．米国のNSA（National Security Agency，http://www.nsa.gov/selinux/）を中心に開発・公開され，Linuxカーネル2.6本体に取り込まれています．SELinuxは，これまで，サーバ分野で広く用いられてきました．最近では，組み込み分野にも適用する動きが高まっています．

なぜ，組み込み分野にSELinuxが必要となってきたのでしょうか？　その理由として，インターネットに接続される組み込みLinux機器が増え，ネットワークを通じた攻撃にさらされるようになってきたことが挙げられます．薄型テレビやDVDレコーダ，ブロードバンド・ルータ，セットトップ・ボックスなど，インターネット接続機能を持つ組み込み機器へのLinuxの採用が増加しています．一方，インターネットにつながると，悪意のある攻撃者やコンピュータ・ウイルスによる不正侵入にもさらされてしまいます．実際に組み込み機器でも不正侵入が発生しています．三つの例を紹介しましょう．

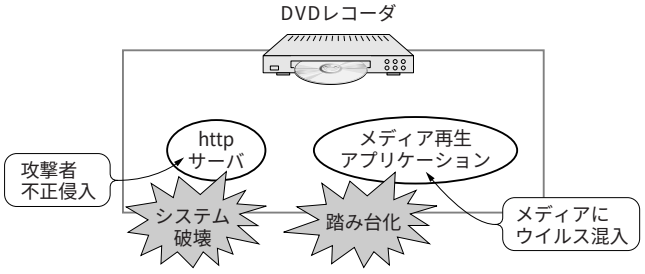

図1　DVDレコーダにセキュリティ・ホールがあった場合の被害

1）不用意に保守ポートを空けていたためログインされた

ブロードバンド・ルータで多くみられる事例です．プロバイダが遠隔から機器を保守したいがために，telnetのポートが空いており，「ユーザー名 root，パスワード admin」のような容易に推測できる認証情報で，ログインできてしまったりします．

2）ウィルスをダウンロードし，実行してしまった

携帯電話で多くみられる攻撃です．インターネットからプログラムをダウンロードし，不用意に実行したらそれがウィルスだったということがあります．

3）バッファ・オーバフロー攻撃

携帯電話やプリンタ，Webカメラなどの機器で報告されている，最も典型的な攻撃です．攻撃者やウィルスが不正に長い入力を送ることで，配列をあふれさせ，スタック上の関数の戻りアドレスを破壊し，任意の命令を実行させる攻撃です．配列にデータを読み込む際のデータ長のチェック・ミスや，メモリ管理周りのバグが原因です．

このように，システム設定の不具合や操作ミス，アプリケーションのバグのようなセキュリティ・ホールがあると，攻撃者やウィルスにつけこまれてしまいます．例えばDVDレコーダの場合，**図1**のようなセキュリティ上の懸念があります．Webで録画できる機能を実現するために，Webサーバが動作していますが，バグがあるとバッファ・オーバフロー攻撃により攻撃者が不正侵入できます．さらに，インターネットから動画メディアをダウンロードしたとします．もしそこにウイルスが混入していたら，動画メディア再生アプリケーションがウイルスを実行してしまいます．一度不正侵入やウイルス実行を許すと，システム・ファイ

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

ルを破壊されて機器が使えなくなったり，ほかのマシンを攻撃するための踏み台として利用されたりします．ユーザにとっても被害が生じると同時に，メーカも修理のために回収が必要になるなど，対応に追われることになります．

● Linuxの問題点

Linuxに関する情報は豊富なので，攻撃する側にとっても，攻略しやすいプラットホームと言えます．Linuxを使う場合は，セキュリティに十分気を使う必要があります．しかし，不正侵入が発生した場合，Linuxではその被害が大きくなりがちです[注1]．その原因は，「root権限の存在」と「粗いアクセス制御」です．

1）root権限の存在

Linuxには，任意の操作が許可されるroot権限があります．つまり，攻撃者にroot権限を取られると任意の操作を許してしまいます．組み込み機器では，すべてのアプリケーションをroot権限で動作させていることも多くあります．もし，そのようなアプリケーションにセキュリティ・ホールがあり，攻撃者に乗っ取られると，攻撃者に任意の悪事を働かれてしまいます．

2）粗いアクセス制御

Linuxは，プロセスのユーザIDをベースに，プロセスがアクセスできるファイルを制限できます．しかし，このアクセス制御は，root権限を持ったプロセスには回避されてしまいます（root権限があれば，すべてのファイルにアクセスできる）．悪いことに，root権限に昇格できるようなセキュリティ・ホールがよく見つかっています．その上，アクセス制御をかけられる対象はファイルのみで，ポート番号のようなネットワーク・リソースにはアクセス制御をかけられません．ポートに対するアクセス制御がないと，「攻撃者が組み込み機器を乗っ取り，http通信（80番ポート）を使って，ほかのWebサイトに不正なパケットを送りつける」というように，機器を攻撃の踏み台に使われてしまいます．

● 組み込み機器におけるセキュリティ対策の難しさ

このような不正侵入を防ぐためのセキュリティ対策として，パソコン環境ではファイアウォールを設置する，ウイルス対策ソフトウェアを導入する，定期的なアップデートを適用する，などの対策が行われています．しかし，これらの対策をそのまま組み込み機器の環境に持っていくのは困難です（**図2**）．

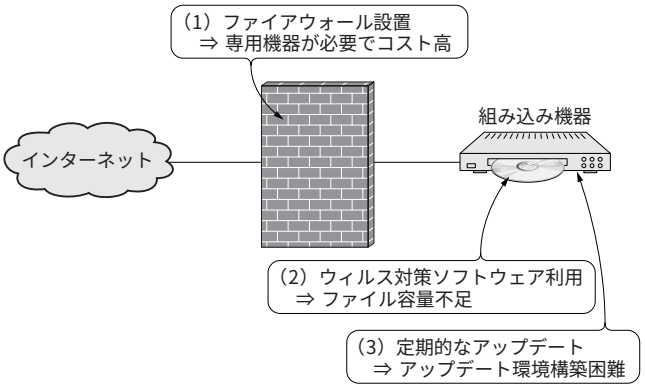

図2　組み込み向けのセキュリティ対策の難しさ

1）専用の機器を置けない

ファイアウォールは，一般的に業務用で高価です．一般家庭にそのような機器を設置するのは，コスト面から難しいでしょう．

2）ファイル・サイズが限られる

ウイルス対策ソフトウェアですが，そもそも組み込み向けのウイルス対策ソフトウェアは，ほとんど存在しません．仮にパソコン向けのものを転用すると考えても，パターン・ファイルの大きさが10Mを超える場合もしばしばです．組み込み機器では，フラッシュROMなどの補助記憶装置の容量が数Mバイト～数十Mバイトしかないことも多く，容量が不足します．

3）アップデート困難

定期的なアップデートを提供する場合，Windowsを搭載するパソコンならばMicrosoft社がアップデートの提供の面倒を見てくれましたが，組み込み機器では，アップデートを継続的かつ漏れなく提供する体制をメーカが整えねばなりません．この体制を整えるのは容易ではありません．

2　SELinuxの特徴

これに対し，組み込み機器に適するセキュリティ対策として注目されているのが，SELinuxです．

● SELinuxのさまざまなアクセス制御機能

SELinuxの基本的な機能は，プロセス単位のアクセス制

注1：Linuxに限らず，ほかの多くのOSでも同様である．