http://www.itmedia.co.jp/enterprise/articles/0503/25/news080_3.html

■設定を自動化する audit2allow コマンド

アクセス拒否された内容をすべて手動で設定していく作業は、大変手間が掛かる。そのため、SELinux にはログに出力されたアクセス拒否の内容を、自動的に allow 文に変換してくれる便利なコマンドが用意されている。以下は、audit2allow コマンドを使用して、上記の allow 文の内容を自動で出力している。ほかのログの内容から、write、lock 以外のアクセスベクタも表示されている。

```
# audit2allow -d -l
                :
                :
allow httpd_t httpd_sys_script_exec_t:dir { add_name create remove_name write };
allow httpd_t httpd_sys_script_exec_t:file { create lock setattr unlink write };
                :
                :
```

コマンドオプションとして指定している「-d」、「-l」はそれぞれ、dmesg の内容を出力、設定反映後のログのみを読み込むためのオプションである。

あとは、audit2allow コマンドが自動で出力した allow 文を、「.te」ファイルにコピー＆ペーストすればよい。このコマンドを使うことでログの内容を allow 文に手動で変換する手間を大幅に軽減できる。

■設定の反映

allow 文を設定ファイルに追加しただけでは設定は反映されない。設定を反映するには、make reload コマンドを /etc/selinux/strict/src/policy/ 以下で実行する。このコマンドは、ポリシーをバイナリー形式のファイルに変換するコマンドで、具体的には「.te」ファイルを policy.18 ファイルに変換する。

また、前述の例では「.te」ファイルのみを編集したため、make reload コマンドだけで設定を反映できるが、ファイルのタイプ付けを変更（「.fc」ファイル）した場合、make reload コマンドの実行後に fixfiles relabel コマンドも実行する必要がある。このコマンドは、「.fc」ファイルを file_contexts ファイルに変換するコマンドで、全ファイルのタイプをポリシーの内容で付与し直す。このコマンドは前にも出てきているが、これは、SELinux を無効にするとファイルのタイプ付けが消えてしまうためである。

fixfiles relabel コマンドは全ファイルのタイプをポリシーの内容で付与し直すため、非常に時間がかかる。このため、必要に応じて特定のディレクトリや、特定のファイルのみタイプ付けを行うコマンドを使用するといいだろう。ポリシーファイル関連のコマンドを表 2 にまとめたので参考にしてほしい。