

2007年度
オープンソースソフトウェア活用基盤整備事業

セキュリティ強化 Linux (SELinux) の
管理運用手法の調査

概要

2008年2月

独立行政法人 情報処理推進機構

- * Red Hat は、米国およびその他の国における Red Hat, Inc. の商標または登録商標です。
- * 「Linux」は Linus Torvalds 氏の米国及びその他の国における登録商標及び商標です。

目次

1. はじめに	4
1.1. 調査の背景	4
1.2. 概要 (Executive Summary)	5
1.3. 本報告書で使われる用語の定義.....	7

1. はじめに

1.1. 調査の背景

現在、様々なセキュリティ事故や、新会社法・金融商品取引法などにより、セキュリティや内部統制への関心は非常に高い。そのような流れの中で、OS 層のセキュリティ技術として、セキュア OS への関心も高まっている。セキュア OS のアクセス制御技術は、アプリケーションの脆弱性に対する攻撃や、侵入攻撃などの被害を最小化することが可能であり、パッチ運用コストの削減や、ログ保護の強化など、様々な効果があるためである。

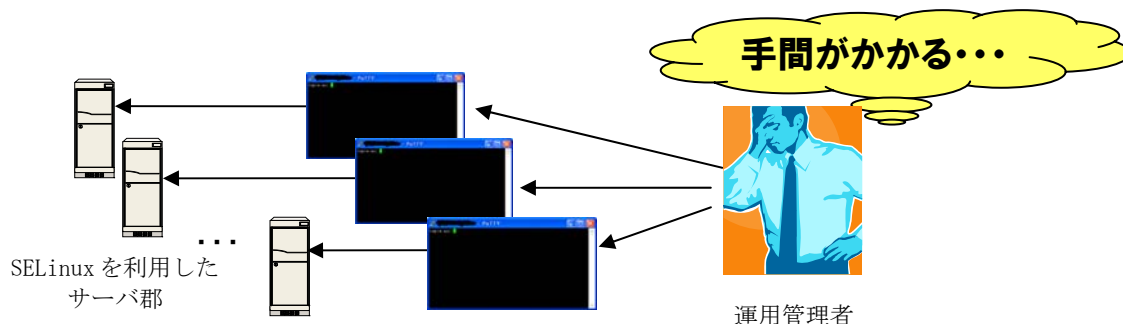
OSS の代表的なセキュア OS である SELinux は、Fedora や CentOS、Red Hat Enterprise Linux などにおいて、デフォルトで利用可能な環境が整っている。また当初は、SELinux の設定が困難であるという問題があったが、外部向けサービスのセキュリティ強化に絞った Targeted Policy が提供されるようになったこと、SELinux Policy Editor に代表される設定ツールが整備されてきたこと、有償の設定サービスが出現したことなどにより、導入フェーズの問題は解決されてきた。

しかしながら、二つの課題がある。一つ目は、SELinux を利用したサーバの運用方法は依然として確立しておらず、SELinux を知らない一般の運用管理者が運用管理できないという課題である。二つ目は、一般的な運用管理製品が SELinux を利用したサーバに対応しておらず、一つ一つのサーバに直接 ssh などログインし、運用管理しなければならないという課題である。このため、導入が出来ても運用できないという問題から、SELinux の利用が進んでいない状況が見て取れる。

【課題 1 : SELinux を知らない一般の運用管理者が運用できない】



【課題 2 : 運用管理製品が SELinux に対応していない】



1.2. 概要(Executive Summary)

本調査では、まず「SELinux を知らない普通の運用管理者が運用できない」という課題に対し、SELinux を利用したサーバの運用方法について調査検討を行った。この中では、SELinux のために従来の運用に追加して行わなければならない事柄や、その方法等を中心として調査検討した。そして、成果物として以下の二つの文書を作成した。

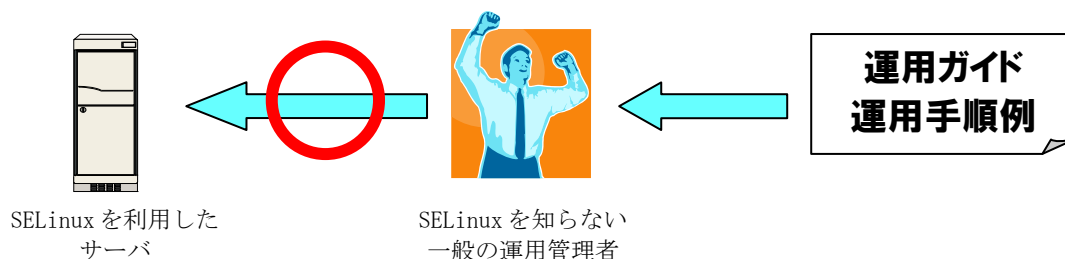
- **SELinux を利用したサーバの運用ガイド**

SELinux を知らない運用管理者に対し、SELinux サーバを運用管理するために必要最低限の SELinux の知識と、運用管理すべき項目やその意味、運用管理する方法を示した文書である。これから SELinux を利用したサーバを運用管理する運用管理者の教育資料等に利用して頂きたい。

- **SELinux を利用したサーバの運用手順例**

「SELinux を利用したサーバの運用ガイド」を元に、実際に構築されたサーバに対する詳細な運用手順をまとめた文書である。運用手順書を作成する際や、実際に運用管理する際に、参考文書として利用して頂きたい。

上記二つの文書により、SELinux を知らない一般の運用管理者でも、SELinux を利用したサーバを運用管理できるようになる。



次に、「運用管理製品が SELinux を利用したサーバに対応していない」という課題に対し、運用管理製品が、SELinux を利用したサーバに対応するために必要な機能を調査検討した。そして、成果物として、以下の文書とプロトタイプを作成した。

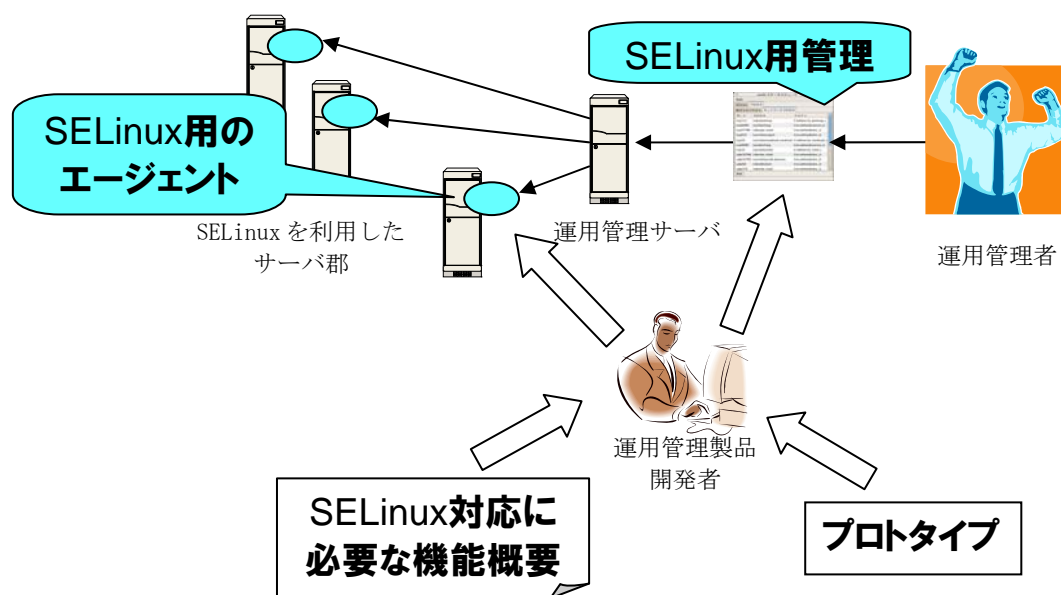
- **運用管理製品における SELinux 対応に必要な機能の概要**

運用管理製品が SELinux を利用するサーバに対応するために、追加すべき必要な機能の概要を示した文書である。既存の運用管理製品を SELinux 対応するための拡張をする、もしくは SELinux に対応した運用管理製品を開発する際に、主に概要設計段階で参考にして頂きたい。

- **運用管理製品における SELinux 対応に必要な機能のプロトタイプ**

「運用管理製品における SELinux 対応に必要な機能の概要」の中で、SELinux の動作状態の監視と、SELinux のログの監視機能を、OpenDRIM をベースに開発したプロトタイプである。成果物は、ソースを含むプロトタイプと関連ドキュメントで構成される。既存の運用管理製品を SELinux 対応するための拡張をする、もしくは SELinux に対応した新規の運用管理製品を開発する際に、主に詳細設計及び実装段階で、ソースや関連ドキュメントを参考にして頂きたい。

上記のプロトタイプおよび関連ドキュメントは、運用管理製品が SELinux 対応する際のサンプルとなり、SELinux 対応へのハードルを下げる。これにより、運用管理製品の SELinux 対応が進めば、運用管理者の負担を軽減することができる。



以上より、SELinux の導入が出来ても運用できないという問題を解決することができ、SELinux の利用を促進することができる。

1.3. 本報告書で使われる用語の定義

用語	意味
Apache	Apache HTTP Server の略。 Apache ソフトウェア財団の Apache HTTP サーバプロジェクトで開発が行われている Web サーバソフトウェア。
BIND	Berkeley Internet Name Domain の略。 カリフォルニア大学バークリー校で開発された DNS サーバソフトウェア。
CGI	Common Gateway Interface の略。 Web サーバが、Web ブラウザからの要求に応じて、プログラムを起動するための仕組み。
DMZ	DeMilitarized Zone の略。 社内ネットワークと社外のインターネットの間に置かれるセグメント。外部向けの Web サーバ、Mail サーバ、DNS サーバなどを配置する。
DNS	Domain Name System の略。 インターネット上のホスト名と IP アドレスの対応を解決するシステム。
Domain	SELinux において、サブジェクト（プロセス）に付与するラベル。
MTA	メールサーバ上で動作し、ユーザが送信したメールの配送、メールサーバにアカウントを持つユーザへのメールの受信および保管を行うソフトウェア
OS	Operating System の略。 コンピュータを制御する基本ソフト。
OpenDRIM	Open Distributed Resource Information の略。 北東アジア OSS 推進フォーラム WG1 OpenDRIM プロジェクトにおいて、日中韓で共同開発されているリソース管理ツール。
Postfix	IBM 社ワトソン研究所の Wietse Zwietsje Venema 氏が開発した電子メールサーバソフトウェア (MTA)
SELinux	Security-Enhanced Linux の略。 NSA（米国国家安全保障局）が作成したセキュア OS モジュール。
Type	SELinux において、オブジェクト（ファイルやディレクトリなどのリソース）に付与するラベル。
ssh	Secure Shell の略。 暗号化した、ネットワーク経由でほかのコンピュータを操作するためのプロトコル。