技術部データベース系サーバにおけるセキュア OS 環境の試み

平山かほる（工学部・工学研究科技術部計測・情報システムグループ）

はじめに

ネットワークにつながるサーバのセキュリティ対策として、1.セキュリティホールなどによる侵入の阻止、2.ファイアウォールや IDS による侵入検知などの防御、3.侵入された場合の被害を最小にする。といった 3 点が挙げられる。今回、侵入された場合の被害を最小にするため、セキュア OS 環境を使用した。セキュア OS とは文字通りセキュリティを強化した OS をいい、強制アクセス制御（Mandatory Access Control:MAC）機能および最少特権を実現する機能を備えたものである。フリーで代表的なものに SELinux（Security-Enhanced Linux）や LIDS がある。我々が管理しているネットワークサーバでは OS に Turbolinux 10 Server を使用しており、カーネルには、標準で SELinux が組み込まれている。SELinux は、NSA（The National Security Agency －米国家安全保障局）によって開発され、Linux OS レベルで root の特権的権限を無くし、ユーザ/プロセス毎のアクセス制御を実施する。これによって不正侵入を困難にし、クラッキング行為を無力化あるいは影響を最小限にすることができるが、セキュリティポリシーの変更には、それぞれの設定ファイルをどのように読み書きするのかとか、どのようなデバイスやソケットを使用しているのかなどの知識が要求されるため、正しく設定することが困難である。今回は、テスト用サーバにおいて強制アクセス制御をすることなく、セキュリティチェックに違反したところだけをログに書き出すという形で起動し、テストを行っているので報告する。

SELinux とは

1. 動作のしくみ

従来の Linux では、ディレクトリやファイルといったリソースに対するアクセス制限は各ファイルに割り当てられているパーミッション(「オーナー」、「グループ」、「その他のユーザ」に対してそれぞれ「読み込み」、「書き込み」、「実行」の許可を設定）に基づいており、 root は全ての権限があるが、SELinux では root を含む全てのユーザにアクセス制限をかけることが可能である。Linux カーネル内に SELinux モジュールとシ

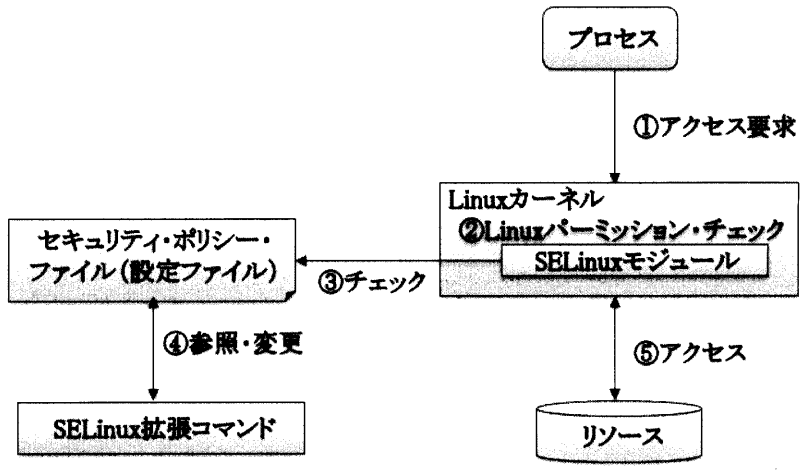

図 1．SELinux の動作のしくみ

ステム内に SELinux 拡張コマンドが追加され、通常のパーミッション・チェックに加えて SELinux 独自のアクセス制御が行われる。動作のしくみを図1に示す。プロセスからアクセス要求があると、Linux カーネルによるパーミッション・チェックが行われ、SELinux モジュールにアクセス要求が渡される。SELinux モジュールはセキュリティ・ポリシー・ファイルを参照し、アクセスが正当であるか否かのチェックを行う。アクセスが正当である場合、プロセスはリソースにアクセスする。

2. 機能

SELinux の主な機能を図2に示す。セキュリティ管理者が定義するセキュリティポリシーによって全てのアクセス制御を行う強制アクセス制御（MAC = Mandatory Access Control)、

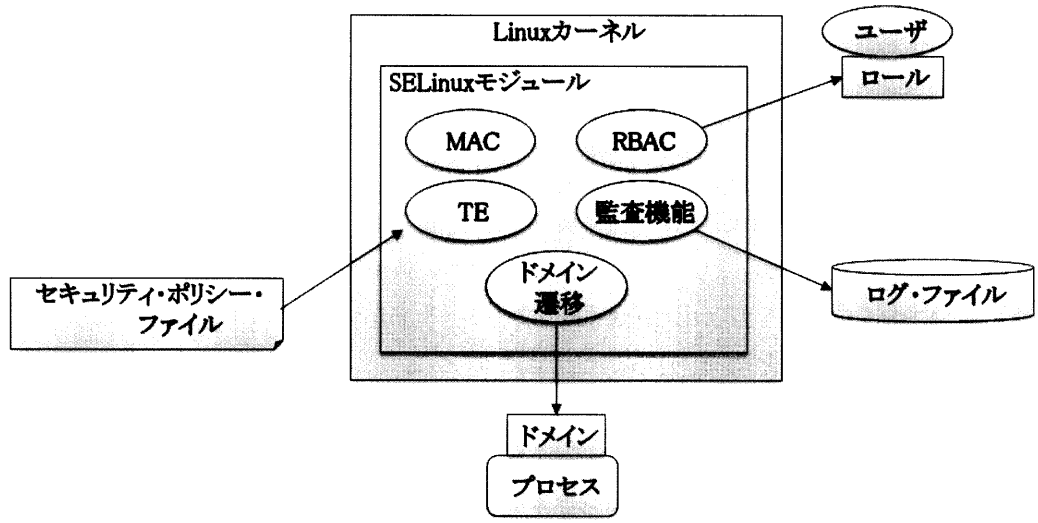

図2．SELinux の主な機能

各プロセスがアクセス可能なリソースの制御を行う TE (Type Enforcement)、各ユーザがアクセス可能なリソースの制御を行う RBAC (Role Based Access Control)、ユーザに最小限の権限を付与するドメイン遷移、リソースへのアクセスが拒否または許可されたときにログが出力される監査機能などがある。また、ユーザにはロール、プロセスにはドメイン、リソースにはタイプというラベルが付与される。このほか SELinux 専用のアプリケーションを開発するためのシステム・コールである SELinux API、伝統的な軍用 OS のアクセス制御機能の MLS、SELinux 同士の安全な通信を行うための機能であるタイプ付き IP 通信などがある。

テスト機における運用

1. 初期設定

技術部データベース系サーバでは、Apache、PostgreSQL、Postfix の機能について SELinux 環境下で動作させたいが、Turbolinux 10 Server のデフォルトでは、代表的なネットワークサービスである BIND、Apache、Postfix の基本的な機能のみの設定となっておりポリシーの設定を行う前段階なので、そのまま使用した。また、SELinux には2つの動作モードがあり、ひとつはセキュリティポリシーの設定で許可されていないアクセスがあった場合にアクセスを拒否してログを出力する enforcing モード、もうひとつはセキュリティポリシーに違反するアクセスであってもアクセスを許可し、ログを出力する

permissive モードである。最初は permissive モードにより起動し、テスト稼動を行い、最終的にはシステムにあわせてポリシーに変更した後、enforcing モードへ移行して実運用を行う。このほか、セキュリティレベルにもほとんどのシステムプログラムに関してアクセス制御を行い、許可されているプログラム以外の動作ができない Strict ポリシーと特定のプログラムだけを SELinux 制御にして、それ以外のプログラムは自由に動作できる Targeted ポリシーの 2 種類がある。実運用で使用するであろう Strict ポリシーを選択した。

図３．出力されたログ

2. 起動

Turbolinux 10 Server では、初期設定において機能が無効である。SELinux カーネルの起動は通常のカーネルにて起動し、root ユーザでコマンド（# fixfiles relabel）を実行する。これによりデフォルトのポリシーファイルに基づき、システムに存在するファイルに対して、タイプが付与される。

次に SELinux カーネルを有効にするために、/boot/grub/grub.conf のカーネルパラメータに selinux=1 を追記後、システムを再起動する。

3. ログの参照

ログの一部を図３に示す。ポリシーファイルの設定により、管理者宛への root メールを配信が拒否されることが読み取れる。現在、運用管理を行う場合の様々な場面を想定しアクセスを行っており、出力されたログによってセキュリティポリシーの設定を行うのであるが、どのアクセス許可が必要であるかないかの選択を行う必要がある。

今後の課題

1. ポリシーファイルの定義

ポリシーファイルの定義を行う場合、①リソースとタイプの関連付けを記述し、②TE の設定（ドメインがアクセス可能なタイプの指定）を行い、③ポリシーファイルへの反映（テキスト形式のポリシーファイルをバイナリファイルへ変換）を行う。そして、④ permissive モードでソフトウェアを動作させ、アクセスが拒否されたリソースをログで確認し、必要であれば許可する設定を追加する。これらの手順を繰り返し最後に⑤enforcing モードに切り替えて動作を確認するということになるが、現段階では④ログにより拒否さ

れたアクセス許可設定を追加するか否かの選択を行っている。今後はその許可設定をどのような方法で行うかを検討する必要がある。というのも、個人レベルにおいて数万行もある設定を手動で行うことは非現実的である。

2. 運用支援ツールの利用

上記のアクセス許可の設定や管理を行う場合、運用支援ツールが利用されている。その代表的なものとしてSELinux Policy Editorがあるが、現時点ではTurboLinuxはサポートされていない。TurboLinuxでは、商用アプリケーションとして提供されているSELinux/Aidを利用することになるので、この利用方法について熟知する必要がある。

まとめ

ネットワークに繋がるサーバのセキュリティを高めるためにテスト用サーバにおいてSELinuxを起動させ、出力ログによるセキュリティポリシー設定の検討を行っている。

参考文献

1)：中村雄一ほか，SELinux徹底ガイド，日経BP出版社，2004