SCIS 2005 The 2005 Symposium on Cryptography and Information Security
Maiko Kobe, Japan, Jan.25-28, 2005
The Institute of Electronics, Information and Communication Engineers

ファイルアクセスパーミッションの統合手法とそのトレードオフに関する考察

On the Security of Integration of File Access Permissions and Its Tradeoff

田端 利宏 * 櫻井 幸一 *
Toshihiro TABATA Kouichi SAKURAI

あらまし SELinux は強力なアクセス制御を実装しているものの，アクセス制御設定ポリシが複雑であるため，正しい設定を行うには管理者に十分な知識と労力が要求される．このため，SELinux の設定補助ツールの一つである SELinux Policy Editor が開発された．このツールは，設定補助の一環として，SELinux の複雑なアクセス制御ポリシの設定項目を一部統合し，設定を簡易化している．しかし，SELinux Policy Editor による設定項目の統合によって，SELinux の安全性が損なわれる可能性がある．本論文では，セキュリティ上の問題を解決した統合パーミッションを提案する．また，OS におけるパーミッション粒度とセキュリティ，及び設定工数のトレードオフについて述べる．

キーワード オペレーティングシステム，安全性，パーミッション統合，SELinux

1 はじめに

計算機ネットワークの普及に伴い，ネットワークに接続された計算機がクラッカーによる侵入攻撃を受けたり，ウイルスに感染する危険性が増大してきている．これらの攻撃による計算機内のデータの漏洩，改竄，そして破壊といった被害を最小限に抑えるには，システムの根幹をなすオペレーティングシステム（OS）レベルでのセキュリティの向上が求められている [1]．このため，米国家安全保障局（NSA）が Linux をベースに開発しているセキュア OS である Security-Enhanced Linux（SELinux）[2] に注目が集まっている．SELinux は，任意アクセス制御（Discretionary Access Control, DAC）に加えて，強制アクセス制御（Mandatory Access Control, MAC）を採用することでセキュリティの向上を図っている．また，セキュリティ機能向上の代償として，SELinux は Linux に比べて複雑なアクセス制御設定を必要とするため，誤設定の可能性も高い．そこで，設定に関する問題を解決するため，SELinux のアクセス制御設定を簡易化し，設定に要する労力を軽減する目的で設定補助ツール SELinux Policy Editor が開発された [3] [4]．このツールは，設定の簡易化の一環として，アクセス制御設定の項目を一部統合しているという特徴を持つ．

我々は，Web サーバソフトウェアである Apache の利用に必要なファイルアクセス制御設定を例に取り，SELinux Policy Editor による設定項目の統合がシステムのセキュリティに与える問題を指摘した [5]．ファイルアクセスのパーミッションが 4 種類に統合されることにより，ファイルの改ざんやファイル名の漏洩の可能性が生じる．そこで，本論文では SELinux Policy Editor におけるセキュリティ上の問題を解決する統合パーミッションを提案する．また，パーミッションの粒度とセキュリティ，及び設定工数のトレードオフについて述べる．

2 Security Enhanced Linux (SELinux)

SELinux のアクセス制御機構は，元となる Linux のアクセス制御機構の外側に，強制アクセス制御 (MAC), Type Enforcement，Role Based Access Control(RBAC) 機能を持つアクセス制御機構を追加することで実現されている．つまり，両方の機構からアクセス許可を得て，はじめてアクセスを行うことができる．これらの機能を利用することで，最小特権を実現できる．これにより，攻撃者にプログラムを乗っ取られたとしても，攻撃の影響範囲を限定できる．

ファイルのパーミッションは，表 1 に示すように 17 種類存在する [6]．また，ディレクトリのパーミッションは，表 1 と表 2 に示されるものがある [6]．4 章の説明で関係するディレクトリアクセスの search パーミッションと

* 九州大学大学院システム情報科学研究院，〒 812-8581 福岡市東区箱崎 6-10-1, Faculty of Information Science and Electrical Engineering, Kyushu University, 6-10-1 Hakozaki, Higashi-ku, Fukuoka 812-8581

表 1: SELinux のファイル操作に関連するパーミッション

ファイル操作に関連するパーミッション（17 種類）	read, write, append, poll, ioctl, create, execute, access, getattr, setattr, unlink, link, rename, lock, relabelfrom, relabelto, transition

表 2: SELinux のディレクトリ操作に関連するパーミッション（表 1 以外のもの）

ディレクトリ操作に関連するパーミッション（5 種類）	add_name, remove_name, reparent, search, rmdir

read パーミッションについて説明する．search パーミッションは，ディレクトリアクセス専用のパーミッションである．あるファイルやディレクトリにアクセスするには，そのファイルやディレクトリに対するアクセス権限の他に，そのパス上にあるすべてのディレクトリの search パーミッションが必要になる．また，ディレクトリアクセスにおける read パーミッションは，そのディレクトリ内にどんなファイルやディレクトリが存在するか知るために必要なパーミッションである．

ポリシの設定は，アクセス制御設定ファイルに記述され，設定ファイルの編集権限を持つ利用者しかアクセス制御設定を行えない．また，アクセスは，それが設定ファイル内で定義されている場合にのみ許可され，定義されていないアクセスは一切許可されない．このように，SELinux ではきめ細かなアクセス制御を行うことができる．しかし，きめ細かな設定にはそれだけ労力を要し，誤設定の可能性を増大させる．

3 SELinux Policy Editor

SELinux のアクセス制御設定は，ポリシの管理者が設定ファイルにポリシを記述することで行われる．しかし，このファイルはテキストベースであるため，設定ファイルの内容を把握しづらく，設定漏れや誤設定を引き起こす可能性が高い．設定に不備があれば，SELinux の強力なアクセス制御は十分な効果を得られない．そこで，SELinux の設定を補助するツールである SELinux Policy Editor が開発された．

SELinux Policy Editor の主な機能について説明する．

1. Graphical User Interface（GUI）を通した設定が可能である．これにより，パーミッション付与やドメイン遷移といった現在の設定状況を視覚的に把握することができる．

2. 独自の中間設定言語を採用している．ユーザは GUI を通して，中間言語で記述された中間設定ファイルを編集する．それから SELinux Policy Editor 側で，中間設定ファイルを現在の SELinux のバージョンで有効な設定ファイルに変換する．中間言語は SELinux のバージョンに依存しないので，ユーザは SELinux のバージョン変化を意識する必要がなくなる．

3. 一部のパーミッションを統合している．SELinux Policy Editor では，17 種類のパーミッションのうち 12 種類を 4 種類に統合している．これにより，設定を簡易化している．統合されていない 5 種類のパーミッションは，ラベルを付与する権限などを表わすものである．統合前後のパーミッション間の対応関係を表 3 に示す．r は読み取り（read），w は書き込み（write），x は実行（execute），s は探索（search）を意味する．また，ディレクトリアクセスのパーミッションも同様に 4 種類に統合されている．その対応関係を表 4 に示す．なお，SELinux Policy Editor では統合されたパーミッションの使用を強制される．

表 3: ファイルアクセスパーミッションの統合

統合パーミッション	対応する SELinux のパーミッション
r	read, getattr, ioctl, lock
w	write, setattr, append, create, unlink, link, rename
x	execute
s	getattr

表 4: ディレクトリアクセスパーミッションの統合

統合パーミッション	対応する SELinux のパーミッション
r	read, getattr, ioctl, lock
w	write, setattr, append, create, unlink, link, rename, add_name, remove_name, reparent, rmdir
x	execute
s	getattr, search, read

4 SELinux Policy Editor のセキュリティ上の問題点

我々は，文献 [5] において，SELinux Policy Editor のセキュリティ上の問題点を指摘した．本章では，上記の問題点について簡単に説明する．

4.1 簡易化手法の比較

SELinux Policy Editor によるパーミッション統合が SELinux の設定に及ぼす影響を考えるため，例として

表 5: ファイルに関する統合パーミッションの関係

マクロ	統合パーミッション	余分なパーミッション
x_file_perms	x	—
r_file_perms	r s	—
rx_file_perms	r x	—
ra_file_perms	r w s	setattr, create, link, unlink, rename, write
rw_file_perms	r w s	setattr, create, link, unlink, rename
create_file_perms	r w s	—

表 6: ディレクトリに関する統合パーミッションの関係

マクロ	統合パーミッション	余分なパーミッション
r_dir_perms	r s	—
ra_dir_perms	r w s	setattr, create, link, unlink, rename, reparent, rmdir, remove_name
rw_dir_perms	r w s	setattr, create, link, unlink, rename, reparent, rmdir
create_dir_perms	r w s	—

Apache の example policy と同等の設定を SELinux Policy Editor で行った場合について，安全性を検証した．

SELinux のマクロも，SELinux Policy Editor のパーミッション統合も，利用者の設定項目を減らすことで設定を簡易化する．この 2 つの簡易化手法で設定できるパーミッションの粒度を示すため，ファイルおよびディレクトリに関するマクロと，統合パーミッションの関係を表 5 と表 6 に示す．パーミッションが不足するとプロセスの正常な動作が妨げられるため，マクロが定義するパーミッションを少なくともすべて含むように表現している．表 5 と表 6 から，次のことがわかる．

1. rw_file_perms と rw_dir_perms マクロ（以降，write マクロと呼ぶ）を過不足なく表現できる統合パーミッションの組が存在しない．つまり，SELinux Policy Editor では，write マクロが create_file_perms または create_dir_perms マクロと同一視される．したがって，ファイルへの書き込みを許すとファイル情報の変更も許すことになる．
2. ra_file_perms と ra_dir_perms マクロ（以降，append マクロと呼ぶ）を過不足なく表現できる統合パーミッションの組が存在しない．つまり，SELinux Policy Editor では，append の設定ができない．

マクロはパーミッション単体の設定と併用できるものの，SELinux Plicy Editor の設定では，統合パーミッションのみの使用を強制される．このため，パーミッション単体での設定ができない分だけ，パーミッションの粒度が粗い．

4.2 ポリシへの影響

SELinux は，ファイルやディレクトリだけではなく，プロセスの管理にもパーミッションによる制御を利用しているが，ここではファイルおよびディレクトリのアクセス制御のみを考える．

SELinux Policy Editor による簡易化が Apache の example policy に及ぼす影響は大きく二つある．

1. write マクロや append マクロによる影響
2. ディレクトリの余剰な read パーミッションによる影響
   SELinux Policy Editor の統合パーミッションの一つである“ s ”では，search と read パーミッションが統合されている．Apache の example policy の中には，read パーミッションを与えずに search パーミッションだけを与える記述が存在しているため，SELinux Policy Editor によるポリシ簡易化の影響を受ける．

4.3 考察

攻撃者はすべてのドメインの権限を得ることができるものと仮定し，評価した．

4.3.1 write マクロと append マクロに対する余剰なパーミッションの影響

Apache の example policy では，キャッシュディレクトリおよびログディレクトリに対しては，write 権限が与えられている．キャッシュディレクトリは/var/cache であり，Apache が proxy として用いられる場合には直下に httpd ディレクトリが作成され，そこにキャッシュが蓄えられる．また，/var/cache には一つ上の/var ディレクトリと同じタイプが付与されているので，/var に対しても同じ権限が与えられていることになる．

SELinux Policy Editor による設定の簡易化の結果，rmdir（ディレクトリ削除）などの余分なパーミッションが与えられる．ディレクトリを削除するには，ディレクトリ内のファイルをすべて削除しなければならない．しかし，攻撃者が利用できるドメインは，/var 以下のほとんどのファイルに対してアクセスする権限を持たない．

したがって，この余分なパーミッションによって可能になるのは，空になった Apache 関連のディレクトリを削除することである．これはログディレクトリに関しても同様である．

CGI スクリプトを格納しているディレクトリや，CGI スクリプトが取り扱う追記専用ファイルおよびディレクトリに対しては，いずれも追記権限が与えられている．SELinux Policy Editor による設定の簡易化の結果，攻撃者は追記専用のファイルやディレクトリを削除できるようになる．ただし，CGI スクリプト本体など，もともと書き込み不可であるファイルを削除することはできない．

4.3.2 余剰な read パーミッションによる影響

/boot ディレクトリ以下には，OS の起動に必要なファイルが格納されている．この/boot に対する設定は，一般的なドメインに共通して行われる．SELinux Policy Editor による設定の簡易化の結果，攻撃者はこのディレクトリ内にあるファイルの一覧を得られるようになる．ただし，ファイルの内容を読み取ることも改竄することもできない．ユーザのホームディレクトリに関しても同様に，それ以下のディレクトリやファイルの一覧を得られるようになる．

以上のことから，SELinux Policy Editor による Apache の example policy の簡易化がシステムのセキュリティに与える影響として考えられるのは，

1. Apache が扱う追記専用ファイルおよびディレクトリの破壊や改竄の可能性
2. ユーザのホームディレクトリなど，一部のディレクトリの構成ファイル名が漏洩する可能性

である．

あるファイルが存在するという情報すら知られてはならないような場合には，search，read パーミッションの統合がシステムのセキュリティを損ないうる．たとえば，どこからもリンクされていない Web ファイルが存在する場合，ディレクトリに対する search パーミッションを得るだけでは，第三者にその Web ファイルの存在を知ることはできない．しかし，パーミッション統合によってディレクトリに対する read パーミッションが余分に付加されると，第三者に対してその Web ファイルの存在を知る権限が与えられることになる．また，破壊や改竄といった攻撃に関しても，乗っ取られたプロセスが追記権限を持っていたファイルが新たに対象になる．

5 統合パーミッションの提案

本章では，セキュリティ上の致命的な問題が生じないという条件を満たした上で，SELinux のアクセス制御設定を簡易化する統合パーミッションについて述べる．

表 7: 提案したファイルアクセスの統合パーミッション

統合パーミッション	対応する SELinux のパーミッション
r	read, getattr, ioctl, lock
a	append
w	write
c	setattr, create, unlink, link, rename
x	execute

5.1 セキュリティに影響を与える権限

設定項目統合により，データの機密性や完全性を損ない，データ漏洩などを引き起こす可能性がある．ここでは，これらのセキュリティ上の問題点を解決する統合パーミッションについて検討する．まず，機密性の観点では，データの読み込みに関して，必要最小限の権限を設定し，データが読み出される経路を必要最小限にする必要がある．また，完全性の観点は，データの生成，削除，書き込み，及び追記に関して，必要最小限の権限を設定できる必要がある．これにより，データの改ざんや破壊の可能性を最小限にする．さらに，ファイルの名前の変更に関しても同様である．

5.2 ファイルに関するパーミッション統合

ファイルの読み込みに関しては，read パーミッションを過不足なく設定できればよい．また，ファイルの生成，削除，書き込み，及び追記に関しては，create，unlink，write，及び append の各パーミッションを過不足なく設定できる必要がある．また，設定の手間を考慮し，ファイルへの生成と削除，及びファイル名の変更の権限は，まとめることとした．

以上のことから，ファイルに関しては，統合パーミッションとして，読み込み (Read)，書き込み (Write)，追記 (Append)，属性変更 (Change)，及び実行 (eXecute) が必要である．提案する統合パーミッションを表 7 に示す．

5.3 ディレクトリに関するパーミッション統合

ディレクトリに関しては，ディレクトリ情報の読み込みと書き込みと，そのディレクトリへのファイルやディレクトリの生成，削除について考える必要がある．

ディレクトリ情報の読み込みに関しては，read と search パーミッションをそれぞれ，過不足なく設定できる必要がある．また，ファイルやディレクトリの追加に関しては append と add_name を，削除に関しては write と remove_name を過不足なく設定できる必要がある．さらに，設定の手間を考慮し，ディレクトリそのものの生成や削除などの権限はまとめて一つのパーミッションとした．

以上のことから，ディレクトリに関しては，読み込み (Read)，書き込み (Write)，追記 (Append)，属性変更

表 8: 提案したディレクトリアクセスの統合パーミッション

統合パーミッション	対応する SELinux のパーミッション
r	read, getattr, ioctl, lock
a	append, add_name
w	write, remove_name
c	setattr, create, unlink, link, rename, reparent, rmdir
x	execute
s	search

表 9: ファイルに関するマクロと提案した統合パーミッションの関係

マクロ	統合パーミッション
x_file_perms	x
r_file_perms	r
rx_file_perms	r x
ra_file_perms	r a
rw_file_perms	r w a
create_file_perms	r w a c x

(Change)，実行 (eXecute)，及び探索 (Search) が必要である．提案する統合パーミッションを表 6 に示す．

5.4 提案した統合パーミッションの考察

以上の統合パーミッションの設計により，Apache のマクロをパーミッションの過不足なく表現することができ，かつディレクトリに対し search パーミッション単独での設定も可能とした．SELinux のマクロと新たに設計した統合パーミッションの関係を表 9 と表 10 に示す．

SELinux Policy Editor の統合パーミッションとの違いとして，

1. Example Policy のマクロを統合パーミッションで過不足なく表現できることと，
2. 各統合パーミッション間で，重複するパーミッションがないこと

がある．提案した統合パーミッションにより，データの機密性や完全性に影響を与えることを回避でき，かつ設定の簡易化を実現できる．また，統合パーミッション間での SELinux のパーミッション重複を避けることで，各統合パーミッションの意味が明確になる．つまり，パーミッションを表現する統合パーミッションの組を一意に決定できる．これにより，設定が把握しやすくなると考えられる．

表 10: ディレクトリに関するマクロと提案した統合パーミッションの関係

マクロ	統合パーミッション
r_dir_perms	r s
ra_dir_perms	r a
rw_dir_perms	r w a
create_dir_perms	r w a c s

表 11: パーミッションの粒度と設定可能な項目の関係

OS	パーミッションの種類	個別に設定可能な項目
SELinux	12	ioctl，読み込み，書き込み，生成，属性閲覧，属性変更，ファイルのロック，追記，消去，リンク，名前の変更，実行
SELinux Policy Editor (proposal)	5	読み込み，書き込み，追記，変更，実行
SELinux Policy Editor	4	読み込み，書き込み，実行，探索
Linux	3	読み込み，書き込み，実行

6 パーミッション粒度と設定工数

パーミッション粒度により，実現できるセキュリティレベルが異なる．5 章で述べたように，機密性と完全性の観点，及び不正アクセス時の被害範囲の限定が重要であると考える．

表 11 に，ファイルアクセスに関するパーミッションの粒度と設定可能な項目の関係を示す．パーミッションが統合されると，個別に設定できない項目が生じる．パーミッションを設計する場合には，個別に設定できるか否かによって，セキュリティにもたらす影響について検討する必要がある．

一方，設定の組み合わせは，パーミッションの種類 (m) に応じて増加する．また，それ以外にも，サブジェクトの種類（n）や設定対象のオブジェクト（l）の種類にも応じて増加する．

（設定の組み合わせ）＝ m × n × l

Linux には，サブジェクトの種類はユーザ，グループ，その他の 3 種である．SELinux は，これに加え，RBAC

とドメインという概念が導入されている．ユーザ (u) は role と対応づけられ，role(r) はドメイン (d) と関連つけられる．通常ドメインは利用するプログラムの役割毎に作成されるため，サブジェクトの種類は大幅に増加する．

SELinux には，アクセス対象であるオブジェクト (o) に対して，タイプ (t) が定義される．このタイプに対して，ドメインとのアクセス制御の設定がなされる．したがって，SELinux におけるアクセス設定の組み合わせは，

（設定の組み合わせ）＝ m × (u × r × d) × (t × o)

となる．

また，SELinux では，許可されていないアクセスはすべて拒否されるため，許可するアクセスをすべて設定するだけでよいが，設定が膨大なものになることがわかる．

Linux では，スーパーユーザが存在するため，スーパーユーザの権限を取られるとそのアクセスを制御できない．一方，SELinux では，MAC や RBAC を導入することにより，管理者が許可したアクセスのみ許される．その分だけ，上記で述べたように設定の組み合わせが膨大なものとなりとなり，設定の手間や，設定内容の検証の工数が大きく，計算機の管理者や利用者への負担が大きい．

7 おわりに

本論文では，SELinux の設定を簡易化する SELinux Policy Editor のパーミッション統合方法の問題点を，Web サーバソフトウェアである Apache の Example Policy を例に挙げ，述べた．

SELinux Policy Editor による SELinux アクセス制御設定の簡易化により，追記の概念が欠如し，追記のみ可能であったファイルやディレクトリに対し，データ改竄や削除が可能になることを述べた．また，ディレクトリに search パーミッションに加えて，read パーミッションが与えられる問題を指摘し，これにより本来は得られるべきではないディレクトリやファイルの一覧が取得されることを述べた．この問題は，Web サーバでは，Web 上からリンクされていないファイルに対し，アクセスされる可能性をもたらし，情報漏洩につながる可能性がある．

そこで，本論文では，データの機密性や完全性を満たすために，必要最小限の権限を与えるべきパーミッションを明らかにし，これらのパーミッションを過不足なく与えることのできる統合パーミッションを提案した．提案した統合パーミッションにより，データの機密性や完全性に影響を与えるパーミッションを過不足なく設定でき，かつ設定の簡易化も実現できる．

謝辞 本研究の一部は，財団法人情報科学国際交流財団 SSR 産学戦略的研究フォーラム 海外連携型調査研究「オペレーティングシステムのセキュリティ機能に関する調査研究」，および 21 世紀 COE プログラム「システム情報科学での社会基盤システム形成」の支援を受けている．

参考文献

[1] 総務省，“セキュア OS に関する調査研究会報告書，” URL=http://www.soumu.go.jp/s-news/2004/040428_1.html, 2004

[2] NSA, “Security-Enhanced Linux, ” URL=http://www.nsa.gov/selinux/, 2000 DEC.

[3] 日立ソフトウェアエンジニアリング株式会社，“SELinux Policy Editor, ” URL=http://www.selinux.hitachi-sk.co.jp/tool/selpe/selpe-top.html, 2003.

[4] 中村 雄一，鮫島 吉喜，“Security-Enhanced Linux のアクセス制御ポリシ設定の簡易化，”2003 年 暗号と情報セキュリティシンポジウム (SCIS2003) 予稿集，vol.2，pp.831–836，2003 Jan.

[5] 末安 克也，田端 利宏，櫻井 幸一，“簡易化されたポリシに基づいた SELinux アクセス制御の安全性評価，” コンピュータセキュリティシンポジウム 2003 (CSS2003) 論文集, Vol.2003, No.15, pp.253-258, 2003.

[6] 日立ソフトウェアエンジニアリング株式会社，“オペレーティングシステムのセキュリティ機能拡張の調査，” IPA/ISEC 情報セキュリティ関連の調査・開発に関する公募. URL=http://www.ipa.go.jp/security/fy13/report/secure os/secure os.html