SELinux による PostgreSQL アクセス制御強化
～The Development of SE-PostgreSQL～

1. 背景

セキュリティ技術の目的は、守るべき生命や資産をその脅威から保護することである。情報システムにおいては、そのシステムが管理する”情報資産”を漏えいや改ざんといった脅威から保護する必要があり、適切な権限を持ったユーザのみに情報の開示や編集を許可するアクセス制御技術は、最も重要なセキュリティ技術の一つである。

“情報資産”はそれ自身が形を持つものではなく、ファイルシステム上にファイルとして保持されるもの、データベース上にレコードとして保持されるものなど、様々な形態で管理されている。

アクセス制御を行う際に重要なのが、それが網羅的であり、かつ一貫性のある事である。しかし、既存のアクセス制御の仕組みは、異なるサブシステム間で全く独立に作用し、それらの間で一貫性を担保することは困難である。例えば、ファイルシステム上のアクセス制御である伝統的 UNIX パーミッションと、データベース上のアクセス制御である GRANT/REVOKE による ACL は、一般に何の関係もない。

したがって、”情報資産”に対して網羅的かつ一貫性のあるアクセス制御を適用するには、これら従来型のアクセス制御とは独立に、システム全体を見通したアクセス制御を行う事が求められることは言うまでもない。

情報セキュリティ研究の歴史は、このような課題に対する示唆を我々に与えてくれる。TCSEC でも言及されているリファレンスモニタは、ソフトウェアの実装とは独立に、アクセス制御の意思決定を行うというアイデアである。

ファイルの読み書きなど、OS の関与する操作に対するリファレンスモニタとしては、SELinux という優れた、そして広く利用されている実装が存在する。SELinux では、全てのプロセス及びオブジェクトにセキュリティ属性が付与され、これをセキュリティポリシーに照会することでアクセス制御を行う。

データベース管理システムにおいても同様に、テーブルやタプル等のデータベースオブジェクトにセキュリティ属性を関連付け、クエリの実行時にはこれを SELinux に照会することで、OS とデータベースのアクセス制御を一元化することが可能になる。これは同時に、 ”情報資産”に対して網羅的かつ一貫性のあるアクセス制御を適用することとなり、情報フロー制御の枠組みにデータベース管理システムが組み込む事を可能にするものである。

2. 目的

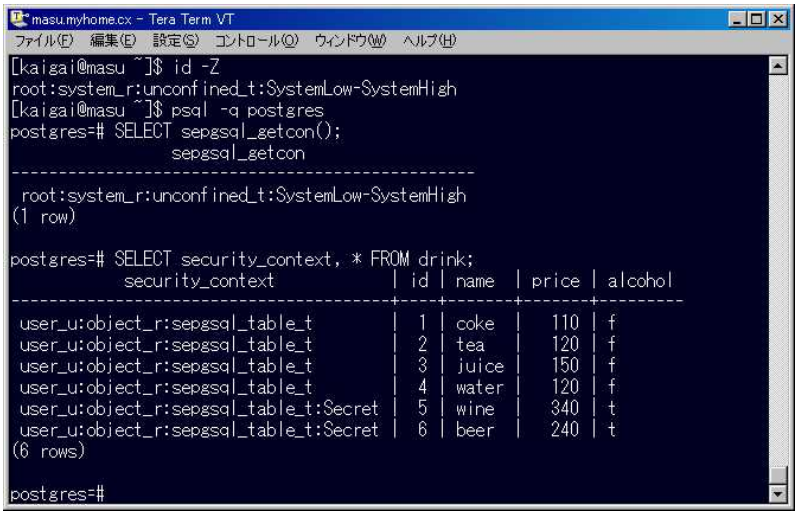
本プロジェクトの目的は、データベースアクセス制御のリファレンスモニタとして SELinux を利用する、PostgreSQL のセキュリティ機能拡張である SE-PostgreSQL の開発とドキュメントの作成、およびこれら開発成果を OSS コミュニティに受け入れさせる事である。

3. 開発の内容

本プロジェクトで開発した SE-PostgreSQL は、SELinux をリファレンスモニタとして利用してデータベースに対するアクセス制御を行う。したがって、下記の各機能を実装することが必要となる。

3－1. データベースオブジェクトにセキュリティ属性を関連付ける機能

PostgreSQL では、全てのテーブルにシステム列と呼ばれる特殊なカラムが存在し、ユーザが各タプルのメタ情報を SQL クエリによって参照するための手段を提供している。SE-PostgreSQL では、各タプルのセキュリティ属性を格納･参照するためにシステム列を拡張している。(security_context 列)



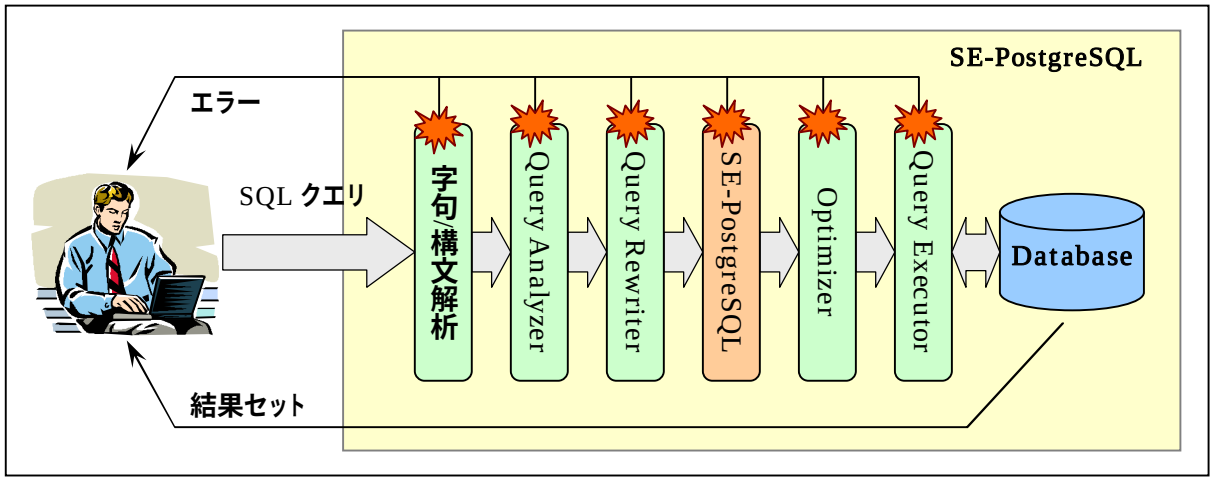
テーブルやカラムなどタプル以外のデータベースオブジェクトは、PostgreSQL ではシステムカタログと呼ばれる特殊なテーブルのタプルとして表現されており、同じ方法でセキュリティ属性を関連付けている。

3－2. SQL クエリを解析し、アクセス権を SELinux に照会する機能

SE-PostgreSQL は、PostgreSQL のクエリ処理フローの中にビルトインされており、全ての SQL クエリを検査する。そして、クライアントがアクセスしようとしているデータベースオブジェクトを列挙し、SELinux に対して当該オブジェクトに対する有しているかを検証

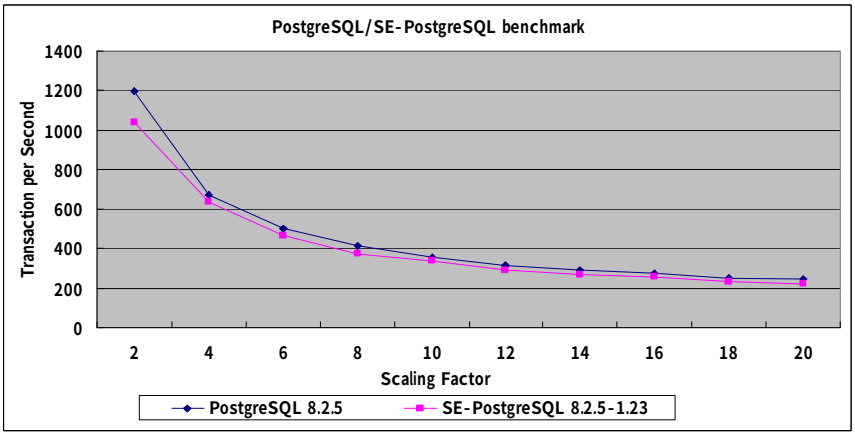
する。

クライアントが必要な権限を有していない場合、SE-PostgreSQL は直ちにトランザクションをアボートし、ユーザにはエラーを返却する。必要に応じて監査ログも生成する。



3－3. SELinux への照会結果をキャッシュする機能

SELinux への照会はカーネル呼び出しであり、比較的重い処理である。SE-PostgreSQL は、過去の SELinux への照会結果をユーザ空間にキャッシュしておく事により、パフォーマンスの劣化を最小限に抑えている。



結果、大規模データベースに対してはネイティブの PostgreSQL とほとんど変わらない性能を出し、小規模データベースに対しても 10%強の性能劣化に留まっている。

3－4. セキュリティ属性付き、データベースのバックアップ／リストア機能

PostgreSQL のバックアップ用ユーティリティである pg_dump および pg_dumpall コマンドに--enable-selinux オプションを追加し、バックアップ時にセキュリティ属性の出力を可能にした。また、本来は Read-Only のシステム列を、security_context 列に限り書き込み可能とすることでセキュリティ属性のリストアを可能とした。

4. 従来の技術との相違

例えば、Oracle 社 Oracle Label Security や IBM 社 DB2 など、従来のデータベース管理システム製品にも、強制アクセス制御や行/列レベルのアクセス制御を可能とするものは存在している。

しかし、SE-PostgreSQL がこれらの製品と根本的に異なるのは、OS のリファレンスモニタを利用することで、システムワイドに網羅性・一貫性のあるアクセス制御を実現できるという点である。従来の製品は、データベース管理システムに閉じたアクセス制御であり、この点で、我々とは拠って立つ哲学が異なる。

5. 期待される効果

SE-PostgreSQL の利用により、”情報資産”の重要な格納手段であるデータベースに対しても SELinux セキュリティポリシーを適用することができる。これにより、データベース管理システムを OS と一体化した情報フロー制御の枠組みに組み込む事が可能になった。

機能面では、これは軍事レベルでのセキュリティ要件に相当するだけの強固なアクセス制御機能であり、従来は国外の商用製品の導入が必要であった場合でも、セキュアな IT インフラ基盤を OSS スタックだけで構築可能になった意義は大きい。

6. 普及の見通し

本プロジェクトにおいて開発を行った SE-PostgreSQL は、2007 年 9 月 3 日に最初の正式バージョンである sepostgresql-8.2.4-1.0 をリリースした。

本パッケージは、既に Fedora Project のリポジトリにもマージされており、次期リリースとなる Fedora 8 からは正式パッケージの一つとして世界中に配布される見込みである。

また、今後 PostgreSQL コミュニティでの議論を通じて、2008 年に予定されている PostgreSQL8.4.0 リリースの公式機能として採用されることを目指すものである。

(情報源)

公式サイト: http://code.google.com/p/sepgsql/

開発者 ML: sepgsql@kaigai.gr.jp

7. 開発者名 (所属)

海外 浩平 (日本電気株式会社 OSSプラットフォーム開発本部所属)