

SELinuxによるPostgreSQLアクセス制御強化

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)

SE-PostgreSQLとは？

データベースに対して、OSのセキュリティポリシーに基づいて細粒度・強制アクセス制御を実現する、PostgreSQLのセキュリティ拡張機能です。

背景

- ファイルシステムもデータベースも、“情報資産”を格納する媒体という点では同じ。でも、アクセス制御の方法は別々だよね？
- 同じ“情報資産”のはずなのに、異なるアクセス制御ポリシー、それで本当に大丈夫なの？



リファレンスモニタの強制アクセス制御

列レベル/行レベルアクセス制御

その答えが

次世代セキュア・データベース

監査ログ強化

SE-PostgreSQL

バックアップリストア対応

一元管理されたセキュリティポリシー

システムワイドな情報フロー制御

一貫したユーザ権限の適用

masu.myhome.cx - Tera Term VT

```
[kaigai@masu ~]$ id -Z
system_u:system_r:unconfined_t
[kaigai@masu ~]$ psql -q
kaigai=# SELECT sepqsql_getcon();
sepqsql_getcon
-----
system_u:system_r:unconfined_t
(1 row)

kaigai=# select security_context, * from drink;
NOTICE: SELinux: denied [ select ] scontext=system_u:system_r:unconfined_t tcon
text=user_u:object_r:sepqsql_table_t:s0:c0 tclass=db_tuple
NOTICE: SELinux: denied [ select ] scontext=system_u:system_r:unconfined_t tcon
text=user_u:object_r:sepqsql_table_t:s0:c0 tclass=db_tuple
 security_context | id | name | price | alcohol
-----
system_u:object_r:sepqsql_table_t | 1 | coke
system_u:object_r:s
system_u:object_r:s
system_u:object_r:s
(4 rows)

kaigai=#
```

機密レベル: 高

機密情報

OSと共通のセキュリティ属性

SELinux

SE-PostgreSQL

Filesystem

機密レベル: 低

OSと一体化した情報フロー制御 (概念図)

【情報源】

- Web: <http://code.google.com/p/sepqsql/>
- ML: sepqsql@kaigai.gr.jp