

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？



その答えが
次世代セキュア・データベース
SE-PostgreSQL

- 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
- 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
- 監査ログ強化

The terminal window shows the following commands and output:

```
[kaigai@masu ~]$ id -Z
system_u:system_r:unconfined_t
[kaigai@masu ~]$ psql -q
kaigai=# SELECT seppgsql_getcon();
seppgsql_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:seppgsql_table_t:s0:c0 tclass=db_tuple
NOTICE: SELinux: denied [ select ] scontext=system_u:system_r:unconfined_t tcon
text=user_u:object_r:seppgsql_table_t:s0:c0 tclass=db_tuple
security_context | id | name | price | alcohol
-----
system_u:object_r:seppgsql_table_t | 1 | coke
system_u:object_r:s
system_u:object_r:s
system_u:object_r:s
(4 rows)
```

The diagram illustrates information flow control. A person icon at the top represents the user. Below them are two database icons: 'SE-PostgreSQL' on the left and 'Filesystem' on the right. A central box labeled 'SELinux' has arrows pointing to both databases. A person icon at the bottom represents the OS. A box labeled 'OSと共通のセキュリティ属性' points to the SELinux box. A box labeled '機密レベル: 高' (High Confidentiality) is connected to the SE-PostgreSQL database, and a box labeled '機密レベル: 低' (Low Confidentiality) is connected to the Filesystem. Red 'X' marks indicate that information flow is blocked from the high confidentiality level to the low confidentiality level.

- 【情報源】
- Web: <http://code.google.com/p/seppgsql/>
 - ML: seppgsql@kaigai.gr.jp