

# 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

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 sepgsql_getcon();
sepgsql_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:sepgsql_table_t:s0:c0 tclass=db_tuple
NOTICE: SELinux: denied [ select ] scontext=system_u:system_r:unconfined_t tcon
text=user_u:object_r:sepgsql_table_t:s0:c0 tclass=db_tuple
 security_context | id | name | price | alcohol
-----
system_u:object_r:sepgsql_table_t | 1 | coke
system_u:object_r:sepgsql_table_t | 2 | fanta
system_u:object_r:sepgsql_table_t | 3 | juice
system_u:object_r:sepgsql_table_t | 4 | water
(4 rows)
```

The diagram illustrates information flow control. A central figure represents the OS, with a box labeled "OSと共通のセキュリティ属性" (OS and common security attributes). To the right, a box labeled "機密情報" (Confidential Information) is shown. Below, a box labeled "SE-PostgreSQL" and another labeled "Filesystem" are shown. A box labeled "SELinux" is positioned between them. Arrows indicate the flow of information: from the OS to SE-PostgreSQL, from SE-PostgreSQL to SELinux, from SELinux to Filesystem, and from Filesystem back to the OS. A box labeled "機密レベル: 高" (High Confidentiality Level) is associated with the OS and SELinux, while a box labeled "機密レベル: 低" (Low Confidentiality Level) is associated with the Filesystem. Red 'X' marks are placed over the arrows between SE-PostgreSQL and SELinux, and between SELinux and Filesystem, indicating that SELinux is not enforcing the high confidentiality level for these components. The text "OSと一体化した情報フロー制御 (概念図)" (OS-integrated information flow control (conceptual diagram)) is at the bottom.

### 【情報源】

- Web: <http://code.google.com/p/sepgsql/>
- ML: [sepgsql@kaigai.gr.jp](mailto:sepgsql@kaigai.gr.jp)