# 次世代セキュア・データベース
# ～Security-Enhanced PostgreSQL～

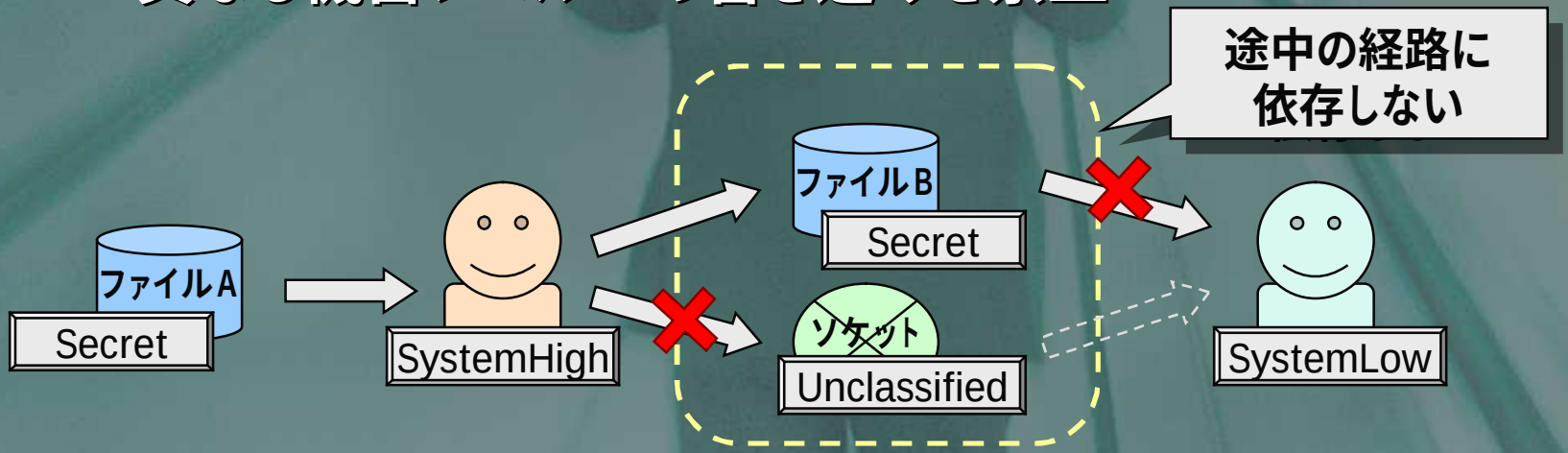
セキュアOSユーザ会／海外浩平 <kaigai@kaigai.gr.jp>

# はじめに

- “情報資産”の保護
  - “情報”には形がない
  - ファイル、データベース、etc... は手段にすぎない
- 脅威
  - 機密情報の漏洩
  - 情報の改ざん
- アクセス制御
  - 一貫性、強制性、柔軟性
  - Bell-La-Padulaモデル

# 情報フロー制御

- BLPモデルの帰結
- “情報”に機密度を示す”セキュリティ属性”を紐付け
  - “ラベル”や”セキュリティコンテキスト”と呼ばれる
- 基本ルール
  - 機密レベル『高』→『低』への読み出しを禁止
  - 異なる機密レベルへの書き込みを禁止



# リファレンスモニタ

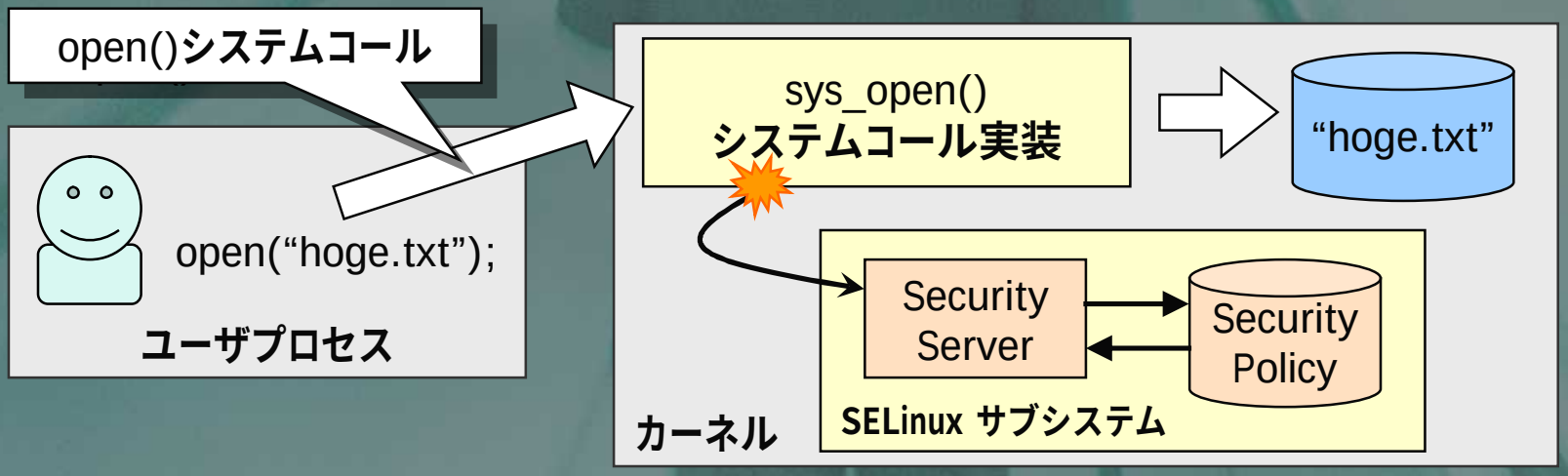
- アクセス制御を行うモジュール
  - システム管理下のリソースに対する、
    アプリケーションのアクセスを、一元的に制御
  - アクセス制御の一貫性を担保

- リファレンスモニタの定義
  - Always invoked
  - Tamperproof
  - Small enough

特権ユーザ (root) に対しても、
例外なく適用！

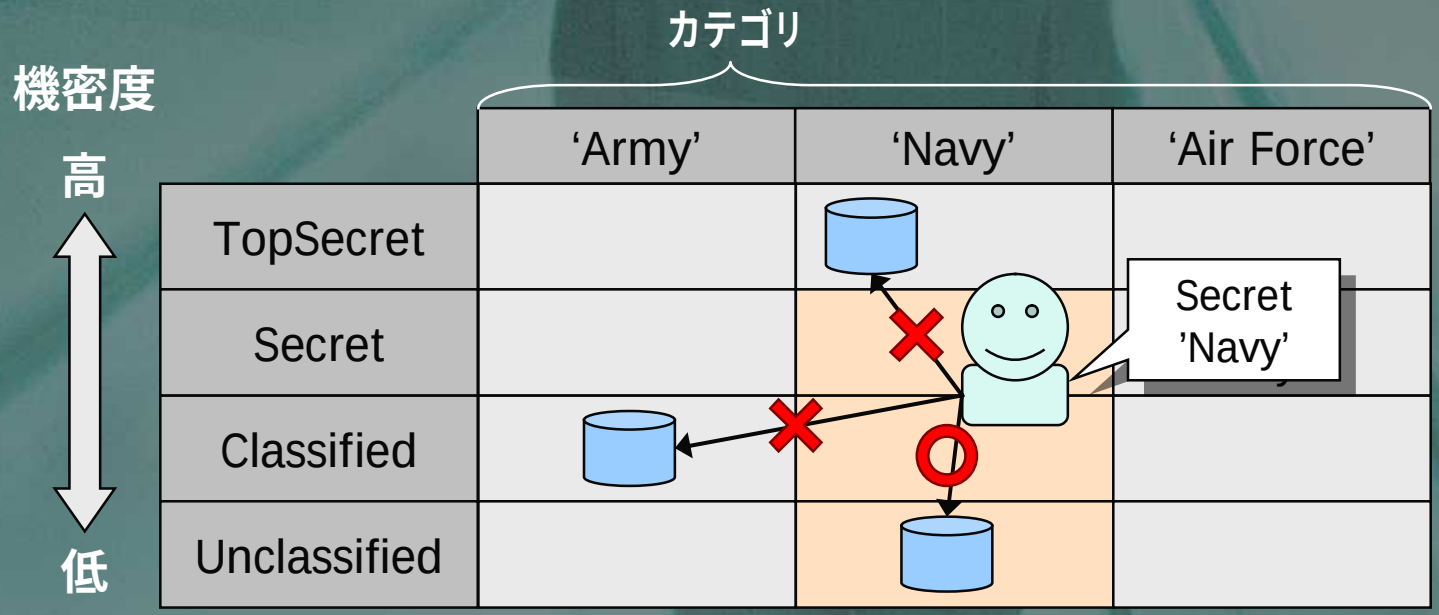
# SELinux

- OSのリファレンスモニタ
  - OS管理下のリソース
    = ファイルシステム、ソケット、IPC、etc...
  - システムコールの実行を許可/禁止
  - セキュリティポリシーによる一元管理

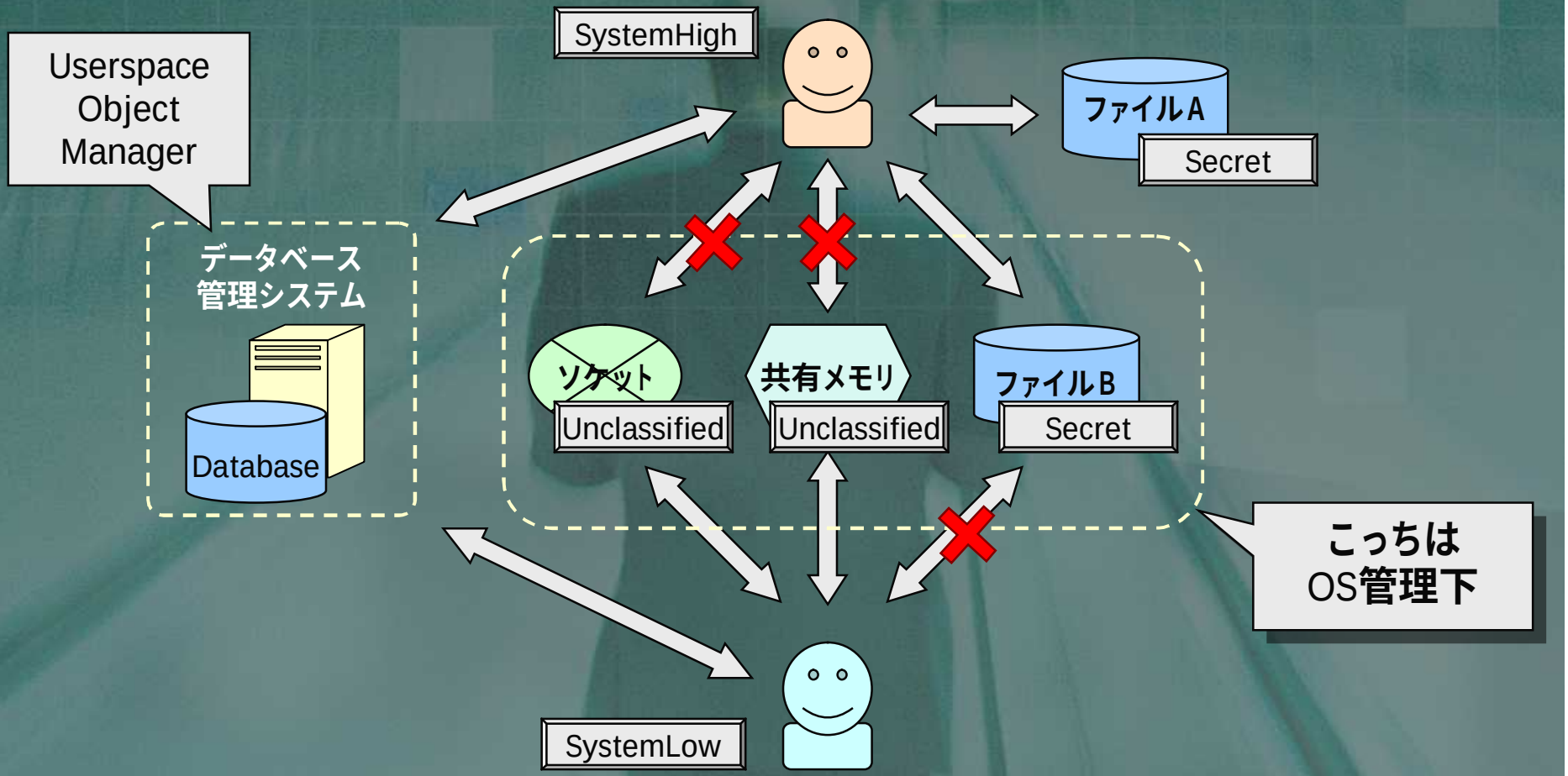


# SELinuxのアクセス制御

- TE (Type Enforcement)
- RBAC (Role Based Access Control)
- MLS (Multi Level Security), MCS (Multi Category Security)



# OS管理下にないリソース

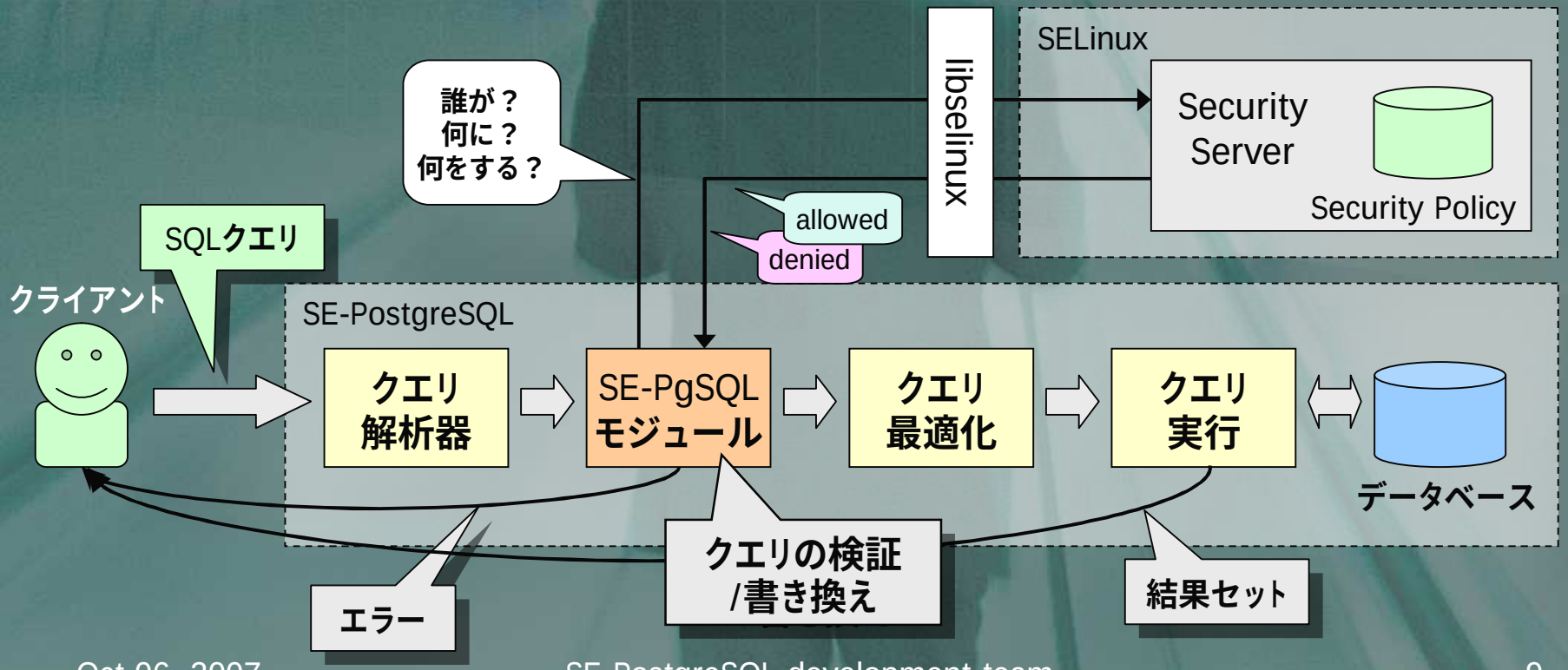


# SE-PostgreSQL

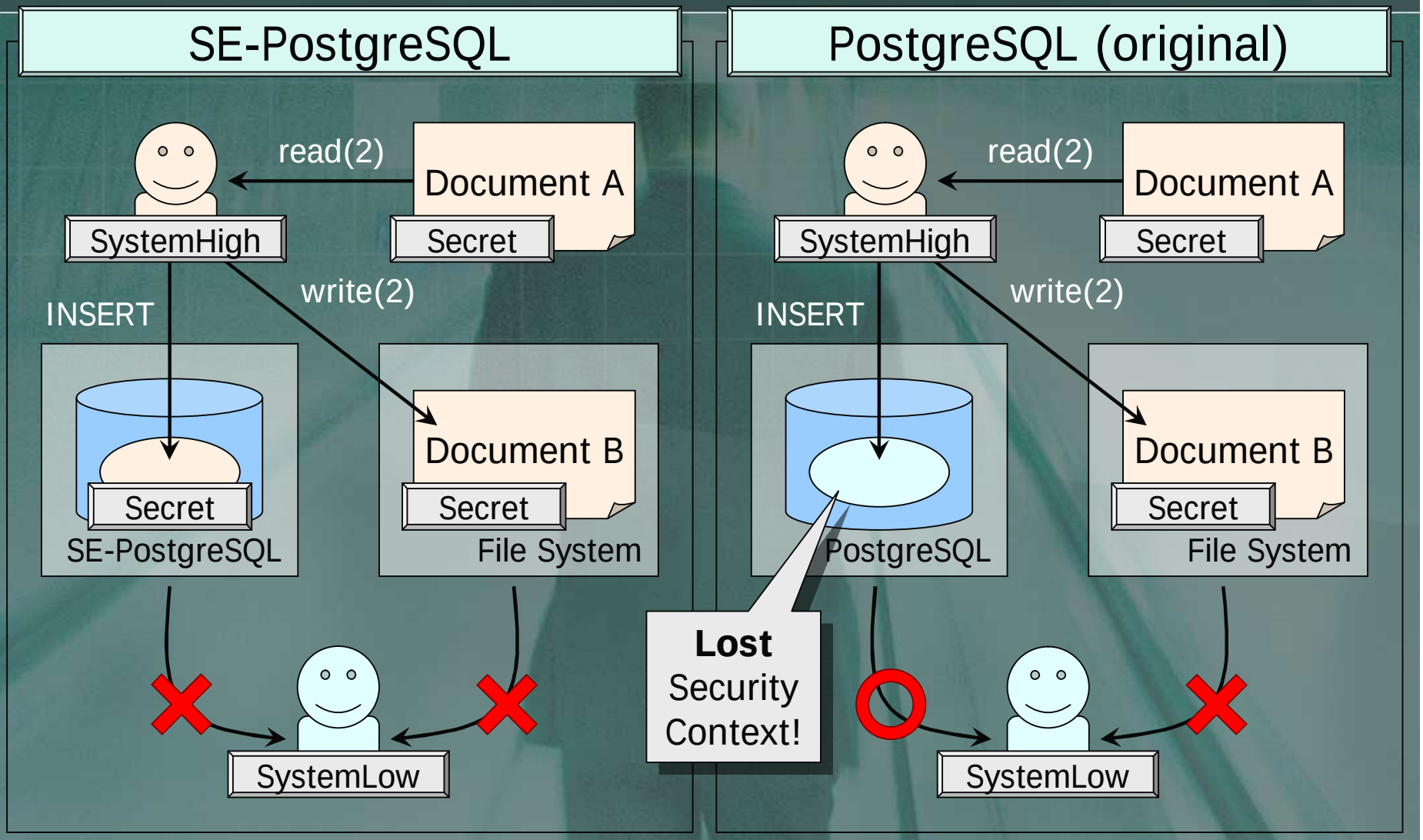
- OSとデータベースのアクセス制御を一元化
  - SELinuxのセキュリティポリシーを利用
  - SELinuxのラベル情報を利用
  - Security ServerとしてのSELinux
- 細粒度のアクセス制御
  - 行レベル／列レベルでの制御
- 強制アクセス制御
  - Super User にも例外なく適用

# SE-PostgreSQLアーキテクチャ

- DBオブジェクトに”ラベル”を紐付け
- SQLクエリの実行可否をSELinuxに問い合わせ



# 情報フロー制御


SE-PostgreSQL
PostgreSQL (original)
read(2)
Document A
Secret
SystemHigh
write(2)
INSERT
Secret
SE-PostgreSQL
Document B
Secret
File System
SystemLow
Lost
Security
Context!

# SE-PostgreSQLのアクセス制御

SQLクエリ

```
SELECT id, name, price FROM drink
    WHERE alcohol=true;
```

SE-PostgreSQL
**モジュール**

**SQLクエリの検査**

- ✓ **権限のないテーブル/カラムetcのアクセスを即エラーに**

**SQLクエリの書換え**

- ✓ **WHERE句に条件を追加、権限の無いタプルを結果セットから除去**

drinkテーブル

| id | name | price | alcohol |
|---|---|---|---|
| 1 | ‘coke’ | 110 | |
| 2 | ‘tea’ | 120 | |
| 3 | ‘juice’ | 150 | |
| 4 | ‘water’ | 120 | |
| 5 | ‘wine’ | 340 | |
| 6 | ‘beer’ | 240 | |

drinkテーブル

| id | name | price | alcohol |
|---|---|---|---|
| 1 | ‘coke’ | 110 | false |
| 2 | ‘tea’ | 120 | false |
| 3 | ‘juice’ | 150 | false |
| 4 | ‘water’ | 120 | false |
| 5 | ‘wine’ | 340 | true |
| 6 | ‘beer’ | 240 | true |

# Case Study (1)

```
SELECT id, name, price * 1.05 FROM drink WHERE id in (3,4);
```

- idカラム ... db_column:{select use} 権限
- nameカラム ... db_column:{select} 権限
- priceカラム ... db_column:{select} 権限
- drinkテーブル ... db_table:{select use} 権限

- numeric関数 ... db_proceduer:{execute} 権限
- numeric_mul関数 ... db_procedure:{execute} 権限

- 各タプルに対して ... db_tuple:{select use} 権限

# SQLクエリの書き換え

- 行レベルアクセス制御の課題
  - 実際にSQLクエリを実行するまで、
    どのタプルにアクセスするのか予想できない
- 解決策
  - SQLクエリ実行時に、タプルへのアクセス権を評価
  - SQLクエリのWHERE句を書き換えて条件を追加
- 例
  - SELECT * FROM drink WHERE alcohol = true;
  - SELECT * FROM drink WHERE alcohol = true
    AND sepgsql_tuple_perms(...);

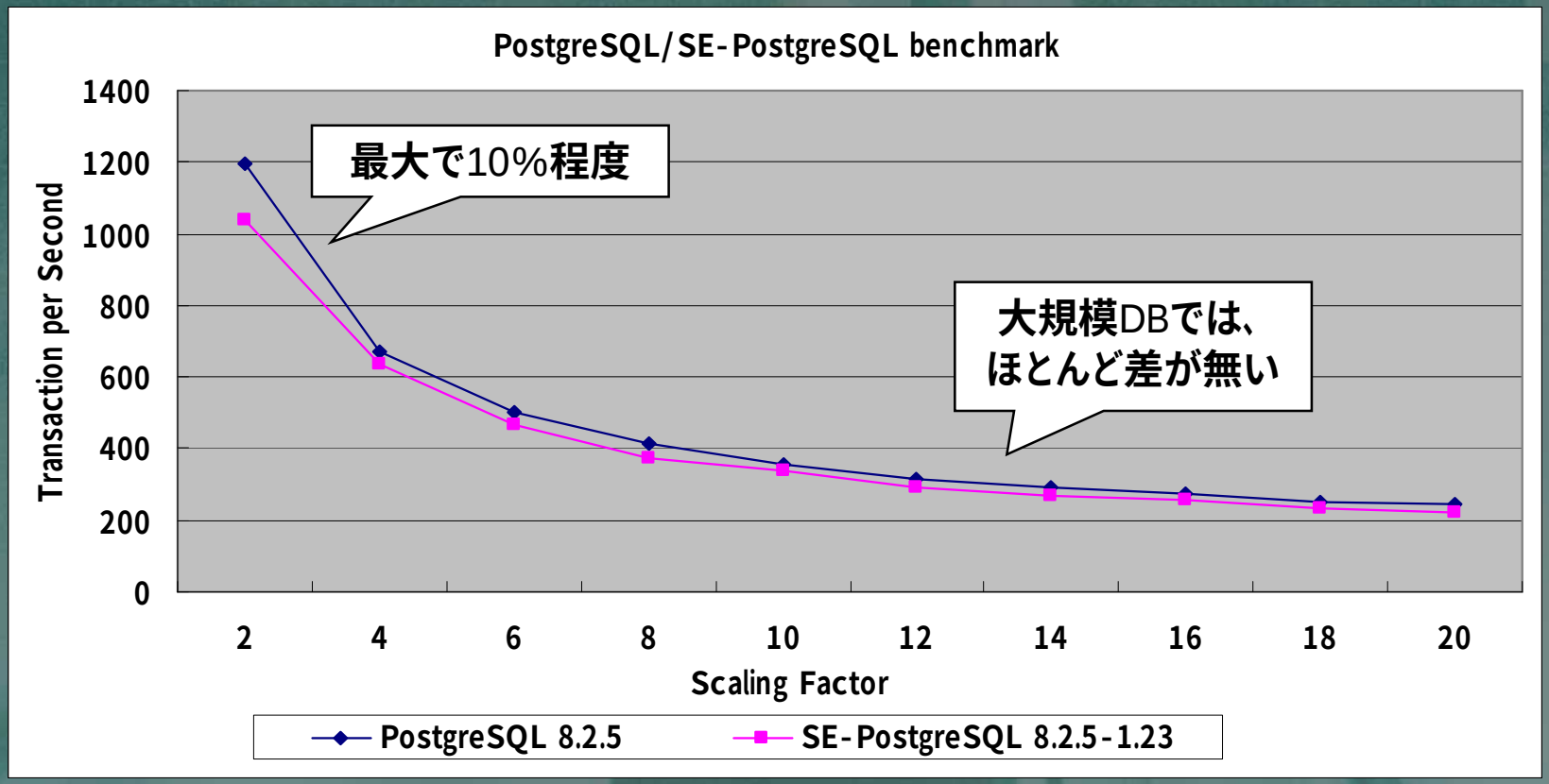
各タプルのアクセス権を
評価するSQL関数

# Case Study (2)

```
UPDATE drink SET name='sake', price = 2 * price WHERE id = 3;
```

- nameカラム ... db_column:{update} 権限
- priceカラム ... db_column:{select update} 権限
- idカラム ... db_column:{use} 権限
- drinkテーブル ... db_table:{select use update} 権限
- int4mul関数 ... db_procedure:{execute} 権限
- int4eq関数 ... db_procedure:{execute} 権限
- 各タプル ... db_tuple:{select use execute} 権限

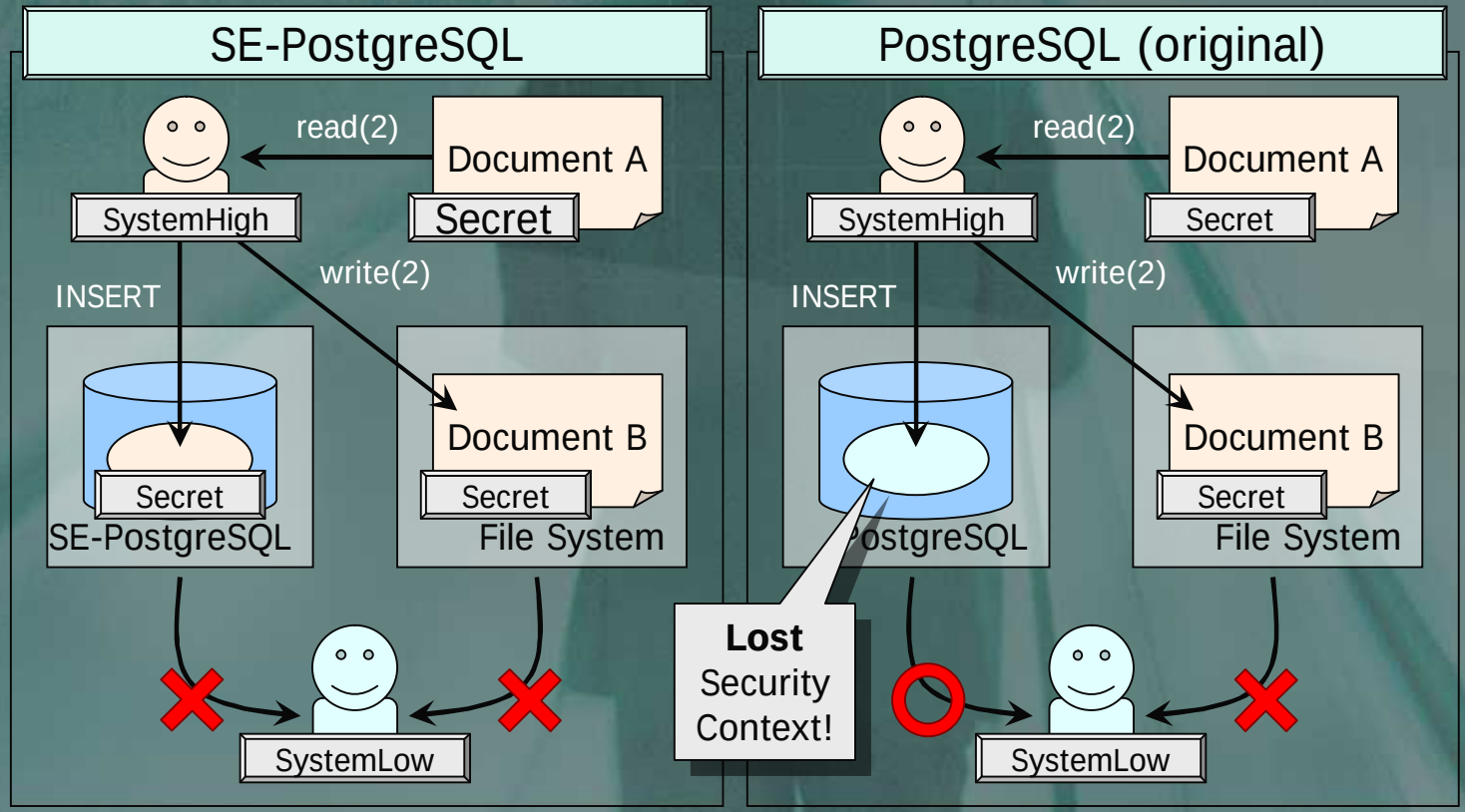
# ベンチマーク（ご参考）




- pgbench -v -c2 -t 64000 を 4回繰り返した平均
- CPU: Core2Duo E6400, Memory: 1GB, HDD: SATA
- shared_bufferを512Mに設定、残りのパラメータはデフォルト値

# デモンストレーション

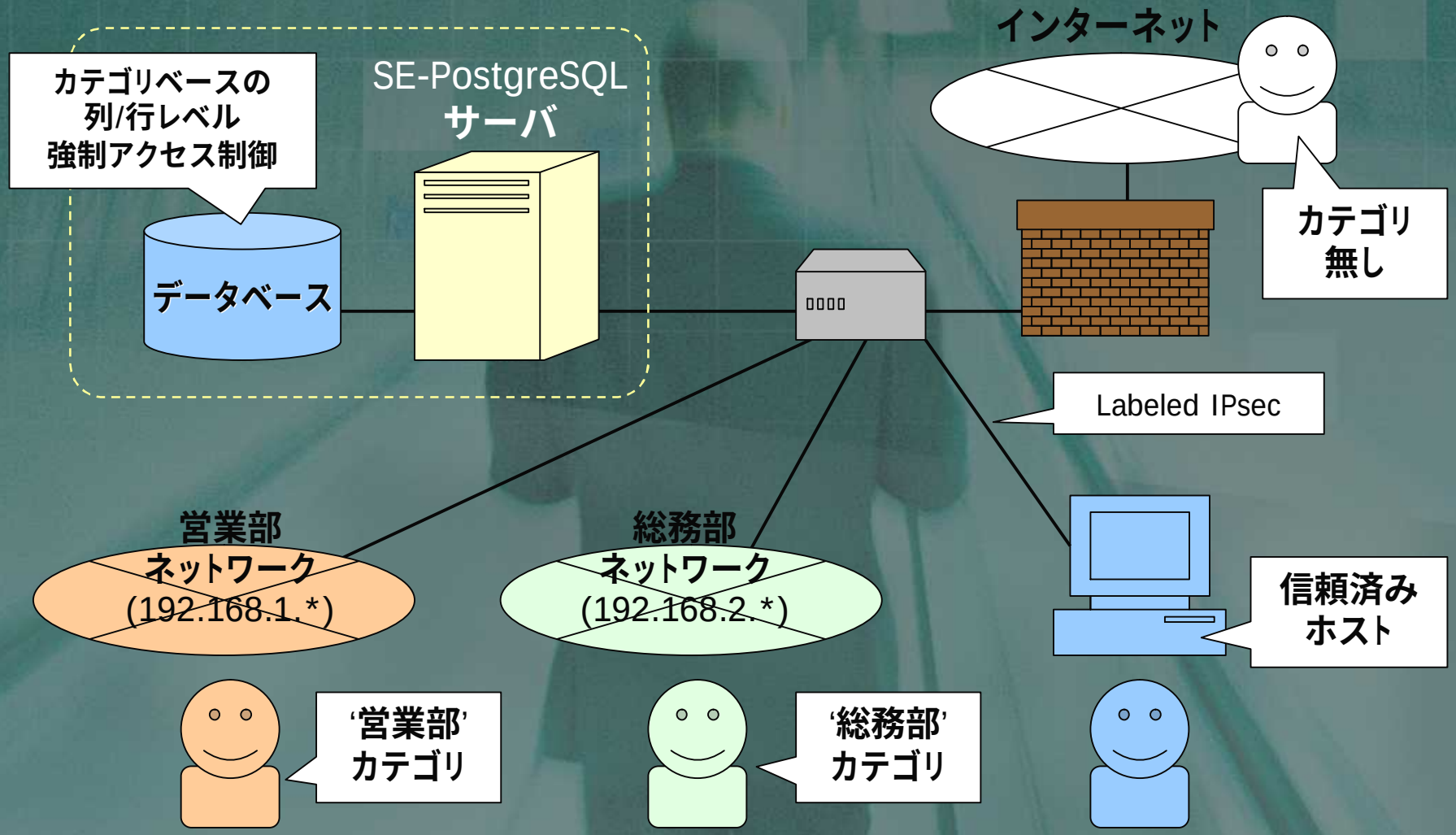
- 行レベルアクセス制御
- OSと一体化した情報フロー制御



# SE-PostgreSQLの運用

- 配布とインストール
  - Fedora7用に RPM パッケージの提供
  - Fedora8以降では、標準リポジトリから
- ドキュメント
  - The SE-PostgreSQL Security Guide(Japanese/English)
- ユーティリティの対応
  - pg_dump, pg_dumpall
  - --enable-selinuxオプションの追加

# SE-PostgreSQL利用イメージ




※ 接続元IPアドレスに基づくコンテキストの割当ては、現在、コミュニティで開発が進められている

# コミュニティとの連携

- SELinuxコミュニティ
  - 設計段階から多くのコメント
  - SE-PostgreSQL対応のための、カーネル機能の強化
  - 標準セキュリティポリシーの対応
- PostgreSQLコミュニティ
  - Trusted Solaris開発者との議論
  - ✓ PGACE(PostgreSQL Access Control Extension)フレームワーク開発
- Fedora Project
  - SE-PostgreSQLのrawhide(開発版)へのマージ

ライトニングトーク(特設会場15:30-16:30)
『知られざるFedora Projectの真実』　(中村雄一)

# 結構、注目されています

- SELinux Symposium 2007/Developer's Summit
- LWN.net での紹介


# 今後の展望

- PostgreSQL 8.3.x 対応
  - ✓ 近々、ベータ版の公開が予定されている
- 新機能の追加
  - pl/pgSQLスクリプト対応
  - Polyinstantiationデータベース対応
  - その他？
- 標準PostgreSQLへのマージ
  - ターゲットは PostgreSQL 8.4.x（2008秋？）
  - ✓ PGACE/SE-PostgreSQLのプッシュ

# 最後に

- SE-PostgreSQL開発のポイント
  - OSS開発者コミュニティとの連携
    - SELinux, PostgreSQL, Fedora Project, ...
  - その分野の専門家の知見をフィードバックできる
  - 関連するパッケージの対応が期待できる
    - Linuxカーネル、selinux-policy、libselinux、...
  - より多くのユーザの利用、より多くのフィードバック
- OSSは”参加することに意義がある”
  - 例えば、ちょっとした『こうだったらいいな』
  - “俺プログラム”を世界の眼でブラッシュアップ！
  - セキュアOSは日本人の活躍が目立っている分野

# 情報源

- SE-PostgreSQL公式サイト
  - http://code.google.com/p/sepgsql/
  - ✓ Subversionリポジトリ、RPMパッケージ、ドキュメント
- メーリングリスト
  - sepgsql@kaigai.gr.jp
- @IT連載記事
  - SE-PostgreSQLによるセキュア・データベース構築
    http://www.atmarkit.co.jp/fsecurity/rensai/sepgsql01/sepgsql01.html
- Fedora Mirrors
  - 各FTPサイトより、rawhide(開発版)向けを配布

# Any Question?

# Thank you!



SE - PostgreSQLの開発は、IPA未踏ソフトウェア創造事業
(2006下期)の支援を受けて行われました。