トップエスイー修了制作

モデル検査によるデータベースのアクセスコントロールポリシー違反の検出

NECソリューションイノベータ株式会社　鈴木 祐一郎　suzuki-y@mxv.nes.nec.co.jp

運用における問題点

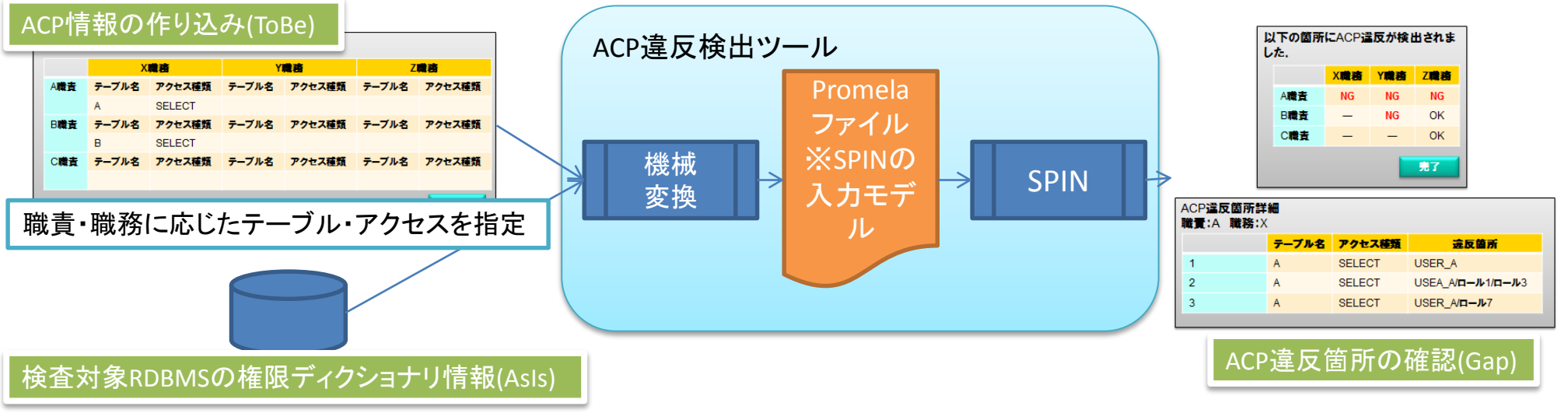
データベース(RDBMS)からの情報漏えいは深刻な問題である．RDBMSからの情報漏えいはアクセス権限が過度に付与されている場合に起こりうるが，稼働から長く経過しているRDBMSでは，
①"あるべきアクセス権限"が規定されていない．
②規定されていても違反箇所の検査は難しい．
という問題がある．

手法・ツールの適用による解決

"あるべきアクセス権限"を現実のセキュリティ要求をベースとして再定義した．さらにユーザのRDBMSアクセスの振る舞いを機械的にモデル変換し，モデル検査ツール"SPIN"を使用し，過度なアクセス権限が付与されている箇所を検査する仕組みを提案し，ケース・スタディをもちいて検証した．

"あるべきアクセス権限"(Access Control Policy)違反の検出

【コンセプト】
ToBeである"あるべきアクセス権限"(Access Control Policy)の情報を与え，AsIsである検査対象RDBMSのアクセス権限設定状況とのGapを分かり易い形で提供する．



ケース・スタディへの適用

【ケース・スタディについて】
検証用のアプリケーションを想定し，それを構成する論理データベース設計を行い，RDBMSに対して実装する．
その上でACP設定より過剰にアクセス権限を付与されたユーザを用意する．
この状態でACP違反検出ツールにて過剰なアクセス権限が付与されていることを妥当な時間で検出できることを評価する．

【ケース・スタディへの適用評価】
- 想定通りの検出結果を得ることを確認した．
- 1件の違反箇所検証の実行時間は0.003秒と非常に短い時間で実行できることを確認した．

まとめと課題

- モデル検査(SPIN)によるACP違反の検出を行うことが出来た．
  - ✓ 検討の中でACPの厳密な定義を行った
  - ✓ 検討した仕組みでACP違反箇所の分かり易い把握をすることが出来るようになった．

【課題】
ケース・スタディより大きな規模のRDBMSに対する検査時間がどのように推移するかが測定できていない．

【今後の展開】
- 最低限必要なアクセス権限付与確認機能の追加
- 複数ユーザの同時検証機能の追加