平成19年度トップエスイー修了制作

安全要求分析とセキュリティパターンを利用したセキュアな社内システム設計

(株) 東芝 セミコンダクター社　　宮田 尚志　　takashi.miyata@toshiba.co.jp

開発における問題点

部署内での情報管理を Web +DB システムで実現する場合、情報集約により機密情報になり、適切なセキュリティ管理が必要(Need to Know等)となる。このようなシステムを開発する場合、セキュリティ上の攻撃とそれに対する対策を系統立てて分析・設計する必要があるが、**セキュリティに関するノウハウは専門性が高く、安全なシステムの構築は困難。**

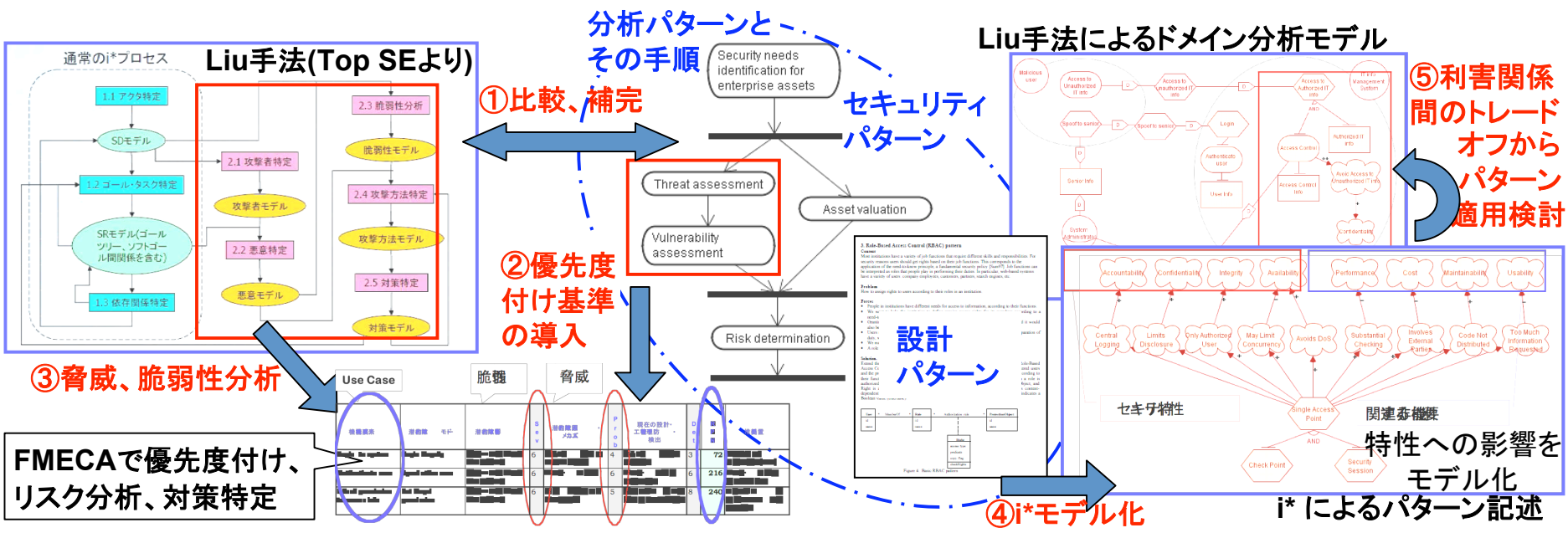
手法・ツールの適用による解決

ステークホルダ間の利害関係を分析した結果からシステム要求を分析する i* 手法を拡張した安全要求分析手法 ***Liu 手法***に対して、

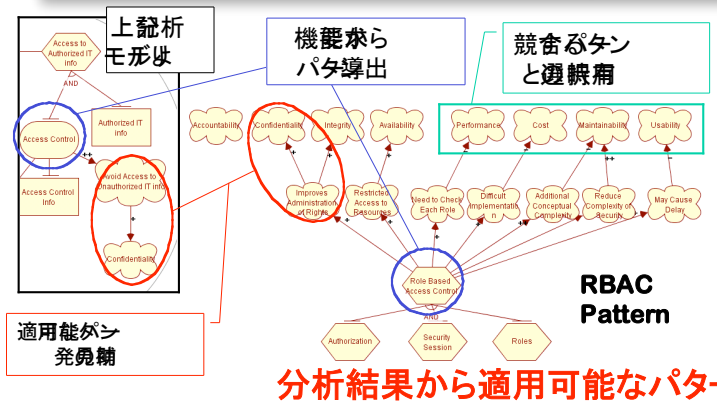
- リスクに対する(半)定量的評価手法 ***FMECA***
- M. Achumacher らの ***セキュリティパターン***
- Weissら の***i*でのパターン記述(非機能要件 考慮)***

を併用することで、**分析・設計間でのトレーサビリティを確保してパターンによるノウハウ導入を図る**

Liu手法,FMECA,セキュリティパターンを組合せたアプローチ



本アプローチの評価



分析結果から適用可能なパターンの導出まで非機能要件を含めて分析・設計可能

今後の課題

- Liu手法だけでは***情報資産に関する分析が不足***
- ***テンプレートの違い***によるi*記述が困難な場合の対応
- ***i*でのパターン記述の妥当性確認***
- ***セキュリティ以外の要件との整合性確認***
  (非機能要件に着目すべき)

実際の開発への応用

組込みシステムでのセキュリティパターン

背景: 組込み機器でのセキュリティトラブル増加

- IPA「複数の組込み機器の組み合わせに関するセキュリティ調査研究」(2008/1)

脆弱性の多くは汎用システムと同じではあるが…

- **コスト、パフォーマンス(時間、空間)に大きな制約**
  例: SSLの暗号化をハード or ソフトで実現すべきか
- **組込みシステム特有な問題(特にファームウェア)**
  - ネットワーク以外の接続 (USB, BT, IEEE1394,..)
  - ハードウェアも含めた対策の必要性
    例: コード解析回避のため、実行時メモリ配置・構成

本アプローチで組込みソフトで有効なパターンを明確化

NII 国立情報学研究所 National Institute of Informatics
トップエスイー　～サイエンスによる知的ものづくり教育プログラム～
文部科学省 振興調整費産学融合先端ソフトウェア技術者養成拠点の形成