



# セキュリティを考慮した システム開発方法論の提案

キヤノン株式会社

中本 泰弘

nakamoto.yasuhiro@canon.co.jp

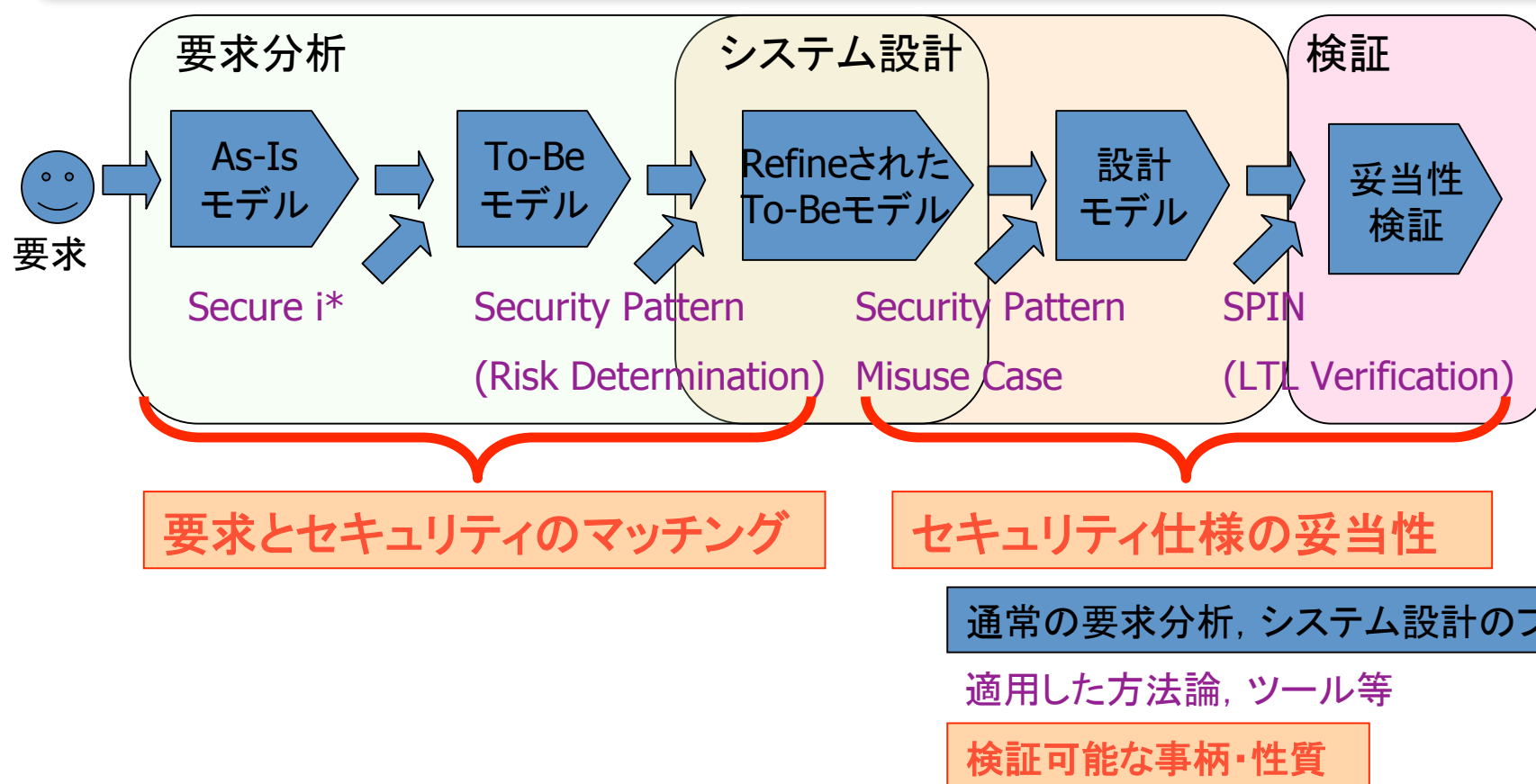
## 開発における問題点

製品・システムのデジタル化, ネットワーク化の拡大によるセキュリティニーズの複雑化に際し, 「ユーザの要求とシステムのセキュリティのマッチング」の確認, 「セキュリティ仕様の妥当性」の検証を可能とする体系的なセキュリティシステム開発方法論を確立する必要がある.

## 連携手法の提案による解決

ユーザのセキュリティの関心事とシステムの対応関係を表す要求分析手法Secure i\*にセキュリティリスクを分析・数値化するSecurity Patternを適用することで, 「ユーザの要求とシステムのセキュリティのマッチング」を確認する. また, 設計モデルにモデル検査ツールSPINを適用することで, 「セキュリティ仕様の妥当性」, つまりセキュリティリスクが発生しないことを確認する.

## 提案するセキュリティシステム開発方法論の全容



## 導入メリット

- 一貫した開発フローにより, 設計モデルの妥当性(セキュリティニーズを満たすこと)の確認が可能.
- 開発初期(要求分析・システム設計)の段階でセキュリティリスクを定量的(リスク分析), 形式的(モデル検査)に検査可能.
- セキュリティ専門家の知識を活用・再利用(Security Pattern)することが可能.