GRACE CENTER FOR GLOBAL RESEARCH IN ADVANCED SOFTWARE SCIENCE AND ENGINEERING

法・規定の同定・洗練とシステム要求の形式化・解析との連動・循環プロセス

Identification and Refinement of Regulations Iteratively Combined with Formalization and Analysis of System Requirements

石川　冬樹　Fuyuki Ishikawa
井上　理穂子　Rihoko Inoue

何が嬉しい？

情報システムの構築や改善において，与えられた法・規定に対応するように詳細な規定やシステム仕様を定めていくにあたり，法律家と開発者が連携して整合性や十分性を高めていくことを支援します

どんな研究？

法・規定および仕様の系統的・段階的な詳細化と分析過程を考え，整合性・十分性双方の観点から法律家・開発者にまたがった洗練プロセスを定義し，それを支援する枠組みを提供します

情報システムと法・規定

情報システムが人間の活動のより大きな基盤を担うにあたり，
遵守しなければならない法律・規定・ガイドラインなどの増加

抽象的・概念的

「個人情報保護法」「SOX法」
センサによる情報収集に関するガイドライン？
ユビキタス環境における物理的な安全性に関するガイドライン？

違反の発生を防ぐ，またはその損害を軽減するよう，

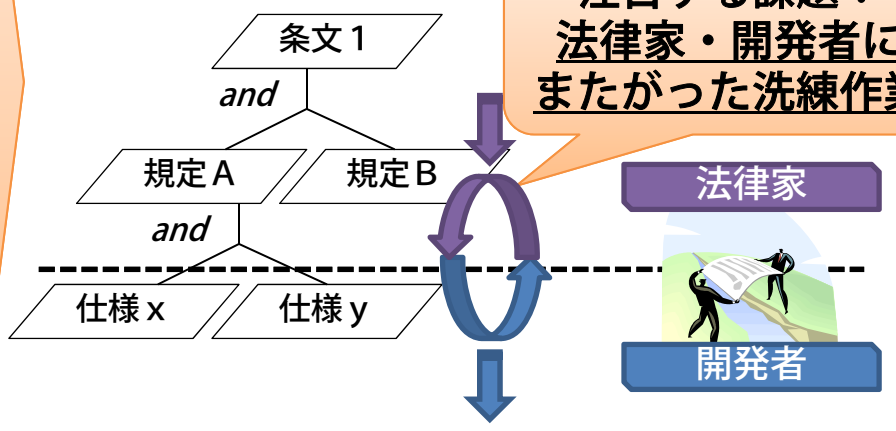
組織やドメインに特化した詳細，具体的な規定
個々のシステムにおける仕様

を整合性・十分性ある形で定める必要がある

既存アプローチ：
ゴール指向要求分析（KAOSなど）

要求を系統的に分析，詳細化し，
具体的な要求（実現手段）を導出，
また変更発生時にトレースし対応

注目する課題：
法律家・開発者にまたがった洗練作業



想定した仕様の検証を通した洗練「規定・仕様の整合性」

規定

「業務上不要な個人情報の操作権利は与えない」
「本業務の各役割において必要な操作とは・・・」
「個人情報を扱う操作は記録」

「ログをとる義務があるがその権限がない」といった不整合を検出，規定・仕様双方で修正

「権利」などのマッピングパターンによる詳細化関係の相互変換

形式仕様

permitted(person, data, write, media)
⇔ role(person, Role1) ∧ …

形式検証フレームワークによる不整合の発見・修正案の検討

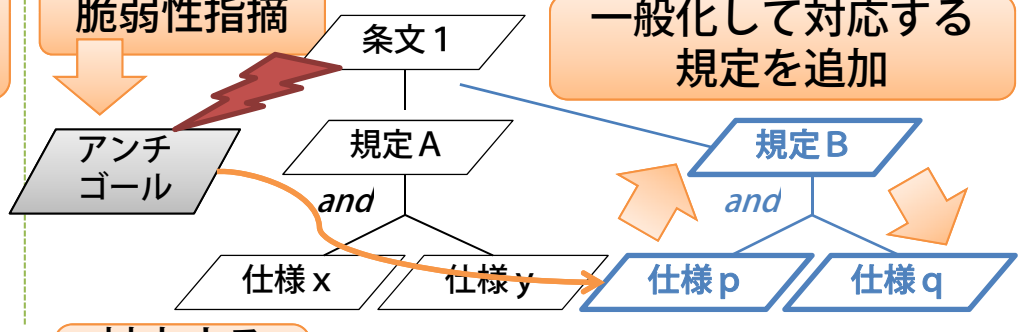
脆弱性（想定漏れ）の分析を通した洗練「規定・仕様の十分性」

判例

「個人情報を売り利益を得る」という行為はしてはならない」という条文に対し，
「メールを送信後消す」という証拠隠滅行為があった

「メールログをとっていない」という脆弱性に対し，解決する仕様を追加．さらに「外部情報送信サービス」に一般化して規定・仕様を再検討

脆弱性指摘



一般化して対応する規定を追加

対応する仕様追加

分析してさらに仕様追加

連絡先：　コンテンツ科学研究系　助教　石川　冬樹
f-ishikawa@nii.ac.jp，03-4212-2584，http://research.nii.ac.jp/~f-ishikawa/

NII