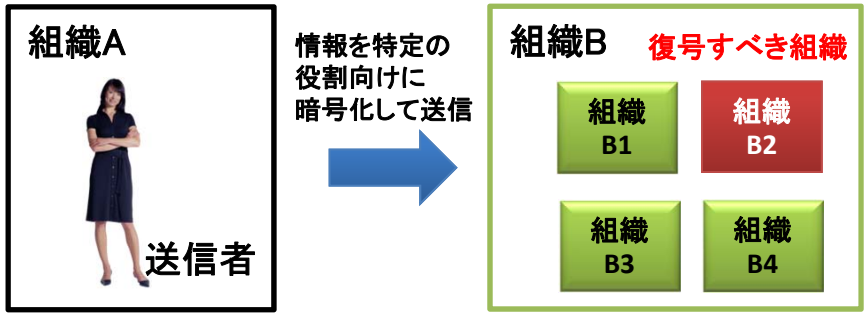
課題172

組織間機密通信のための公開鍵システムの研究開発

企業間の情報流通や、官民連携システムなど、複数の組織をまたがる情報流通のセキュア化を行うために必要な「組織暗号」技術の研究開発と、実際に想定されるシステム規模とユースケースにおける組織暗号の性能面・運用面でのフィージビリティ評価を行う。

背景と解決すべき課題

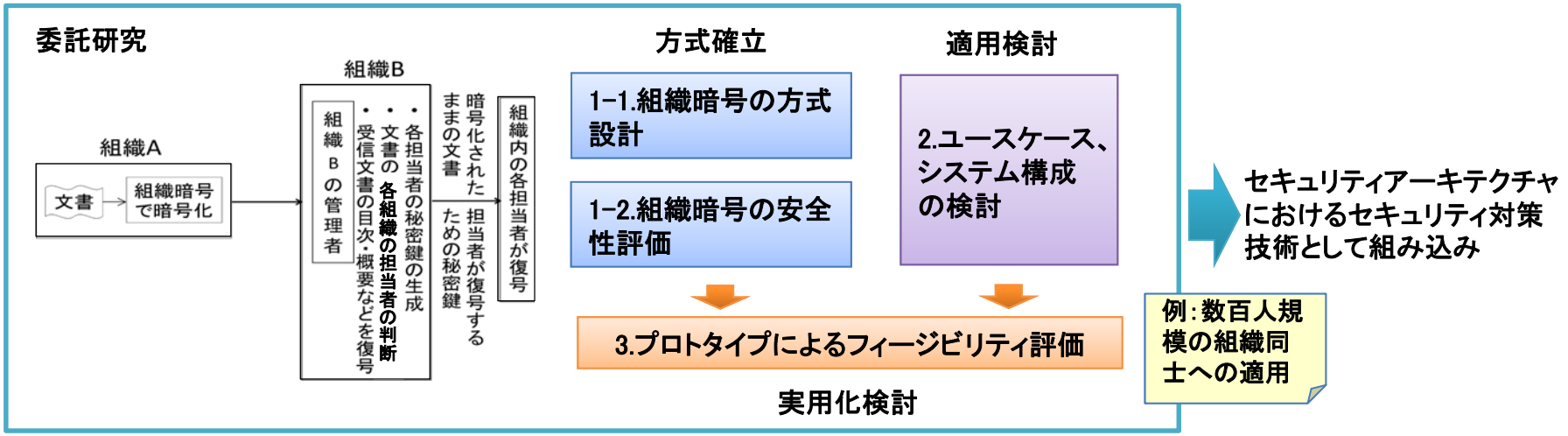
組織間の情報流通において必要とされるアクセス制御について、
単純に既存の暗号技術のみでは運用の要件を満たさない



課題

- 条件に応じたアクセス制御を行う暗号技術として、属性暗号、関数暗号が提案されているが、送信者が受信側の復号者の組織構造を事前に知っている必要がある。
- 受信者側の組織が、セキュリティ管理上の理由で復号できる人を改めて指定したい場合、既存の技術では対応できない

研究開発項目とゴール



研究開発期間： 契約締結日から平成27年度末まで（3年間）　　予算： 平成25年度　55百万円（上限）　　採択件数： 1件