平成２５年度研究開発成果概要書

課題名　　：組織間機密通信のための公開鍵システムの研究開発
採択番号　：17201
副題　　：クラウド環境における機密情報・パーソナルデータの保護と利用の両立に向けて

(１)研究開発の目的

組織の機密情報やパーソナルデータの活用と保護の両立を図ること

(２)研究開発期間

平成２５年度から平成２７年度（３年間）

(３)委託先

中央大学研究開発機構

(４)研究開発予算（契約額）

総額　　156 百万円（平成 25 年度　　55 百万円）
※百万円未満切り上げ

(５)研究開発課題と担当

A-1　組織間機密通信のための暗号方式の開発
A-1-1　基本方式の確立
A-1-1-1　階層型組織への多変数公開鍵暗号方式の確立
A-1-1-2　フラット型組織のための楕円エルガマル暗号及び楕円クラマー・シュープ暗号方式の確立
A-1-1-3　隣接・関連技術との連携・役割分担の確立
A-1-1-4　社会的背景の考察と利用環境高度化への対応
A-2　組織間機密通信におけるユースケース、システム構成の検討
A-3　プロトタイプによるフィージビリティ評価
A-3-1　評価対象：暗号方式
A-3-2　評価対象：システムフィージビリティ
A-3-3　評価対象：社会的利用フィージビリティ

以上，全て中央大学研究開発機構が担当

(６)これまで得られた研究開発成果

		（累計）件	（当該年度）件
特許出願	国内出願	0	0
	外国出願	0	0
外部発表	研究論文	0	0
	その他研究発表	8	8
	プレスリリース	6	6
	展示会	0	0
	標準化提案	0	0

(7)具体的な成果実施内容と成果

A-1　組織間機密通信のための暗号方式の開発

A-1-1　基本方式の確立

A-1-1-1　階層型組織への多変数公開鍵暗号方式の確立

具体的暗号方式を検討し，プロトタイプによるフィージビリティ評価(A-3-1)を行うべく，システム仕様・暗号機能仕様を作製した.

A-1-1-2　フラット型組織のための楕円エルガマル暗号及び楕円クラマー・シュープ暗号方式の確立

具体的暗号方式を検討し，プロトタイプによるフィージビリティ評価(A-3-1)を行うべく，システム仕様・暗号機能仕様を作製した.

A-1-1-3　隣接・関連技術との連携・役割分担の確立

上記 A-1-1-1，A-1-1-2 のシステム仕様を作成するに当たり，隣接・関連技術(例：代理人再暗号化方式等)を適用する選択肢を与える形にしている.

A-1-1-4　社会的背景の考察と利用環境高度化への対応

地方自治体や介護組織，在宅医療や医療と介護の連携の実際について調査を行った.

また，組織通信におけるセキュリティ要件を考察し，そこから情報セキュリティ三要素の一つである「完全性」(Integrity)の概念を拡張した、文書の正確性、論理的矛盾性、法的整合性を保護するシステムの概念の提案を行った。

A-2　組織間機密通信におけるユースケース、システム構成の検討

A-3-1 及び A-3-3 などの実施において，実際に利用を行う組織の活動や組織事情などを考慮して暗号方式構成やシステム仕様を作製した.

A-3　プロトタイプによるフィージビリティ評価

A-3-1　評価対象：暗号方式

階層型組織用組織暗号(多変数公開鍵方式利用)：

(一財)マルチメディア振興センターと中央大学の通信に，多変数公開鍵暗号を用いた「階層型組織用組織暗号」を実際に使用し，十分実用に足るだけの性能が実現されることを確認した.

フラット型組織用組織暗号(楕円曲線 ElGamal 方式利用)：

(一財)放送セキュリティセンターへの「プライバシーマーク取得に関する相談」及び「個人情報保護に関する相談」に相談内容を，割り当てられた専門家のみに対して開示するためのセキュリティシステムとして，楕円曲線暗号を用いた「フラット型組織用組織暗号」を実際に使用し，十分実用に足るだけの性能とセキュリティ水準が実現されることを確認．現場からは，「全体的に導入したい」という希望を得ており，更にバージョンアップしたシステムを提供する予定.

A-3-2　評価対象：システムフィージビリティ

上記 A-3-1「プロトタイプによるフィージビリティ評価」の中ではシステム構成も具体的に計画している.

A-3-3　評価対象：社会的利用フィージビリティ

SI ベンダーの請負った総務省の事業で構築する「在宅医療・介護分野における情報連携基盤」の中に，医療組織と介護組織，または介護組織間の通信などの組織間通信に組織暗号によるアクセス制御を提供することが決定している.