平成27年度研究開発成果概要図 （目標・成果と今後の成果展開）

採択番号：17201

1. 研究課題・実施機関・研究開発期間・研究開発予算

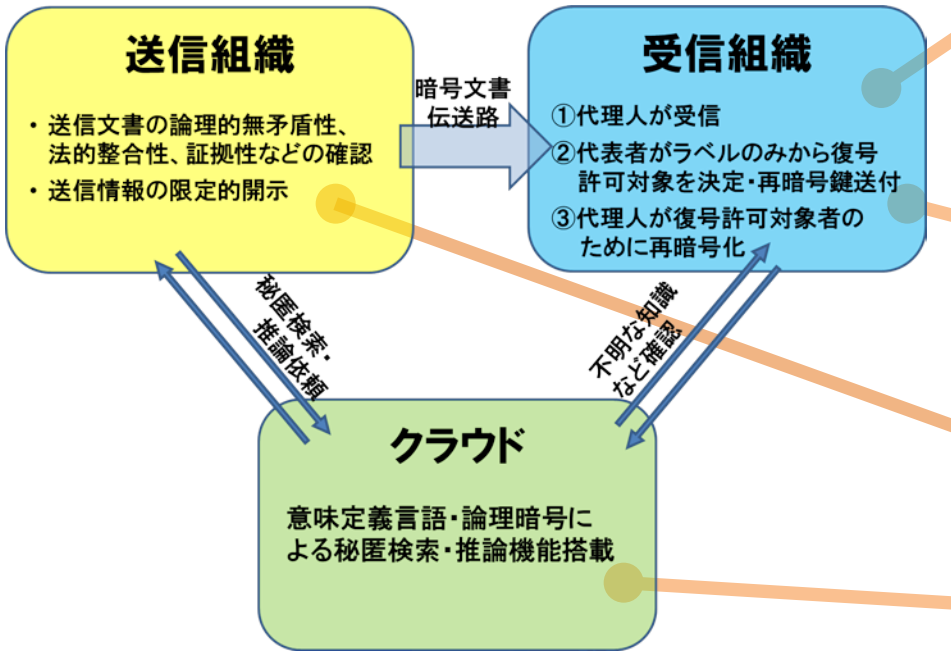
◆課題名　　：組織間機密通信のための公開鍵システムの研究開発
◆副題　　：クラウド環境における機密情報・パーソナルデータの保護と利用の両立に向けて
◆実施機関　　：中央大学
◆研究開発期間：平成25年8月～平成28年3月
◆研究開発予算：48,598,000　円

2. 研究開発の目標

◆「組織通信」の概念を提案し、組織間機密通信のための安全性・性能共に実用に耐えうる暗号方式「組織暗号」を開発する。また、それを実際に組織のネットワークで動作させ、クラウド時代の組織通信のあるべき姿を提案する。
◆「組織暗号」による機密情報（個人情報・医療情報）保護を自治体・医療機関へ提案し、「組織暗号」の社会的実装のための土台を築く。

3. 研究開発の成果

①組織間機密通信の構成・要件と研究開発成果概要



● **多変数公開鍵暗号に基づく組織暗号**
組織構造に対応した鍵構造を持つ暗号方式
IoTネットワークに適したな軽量・高速な暗号方式
耐量子コンピュータ暗号としての安全性を持つ暗号方式

● **楕円曲線暗号に基づく組織暗号**
暗号文の暗号化されたままの鍵の付替えが可能な暗号方式
鍵の付替え処理を2つのエンティティで分担処理する暗号方式
（暗号化情報の制御・証跡確保が可能、特許出願済み）

● **組織暗号の社会的実装を目指した啓蒙・周知**
11カ所の自治体、6カ所の医療・介護機関を訪問し組織暗号紹介
5か所の自治体、1か所医療機関にて組織暗号の実証実験実施

● **プライバシー保護条件付き情報開示**
機密情報数値を秘密分散によって保護したままで、
その値について大小比較を行うための方式

● **論理学暗号**
管理者が問い合わせの内容を知ることなく、問い合わせ内容に応じたソリューションを提供できる仕組みを実現するための方式

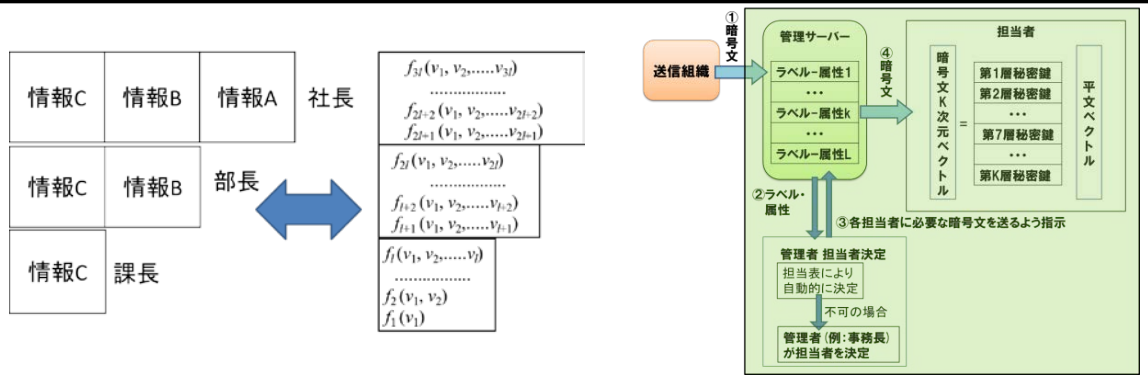
②組織間機密通信のためのセキュリティ技術の研究開発成果

● 多変数公開鍵暗号に基づく組織暗号

組織構造に対応した鍵構造を持つ暗号方式を構築。この方式を論文にまとめ、学会論文誌の査読を受け、採択された。

それと別に、高速でかつデータ効率も高い方式を考案。耐量子コンピュータ暗号としての安全性も持つ方式として国際学会へ投稿した。

センサーやデバイスなどから送られる数値データを集めて送信するような方式に適した高速の暗号。IoTネットワークに適した方式である。

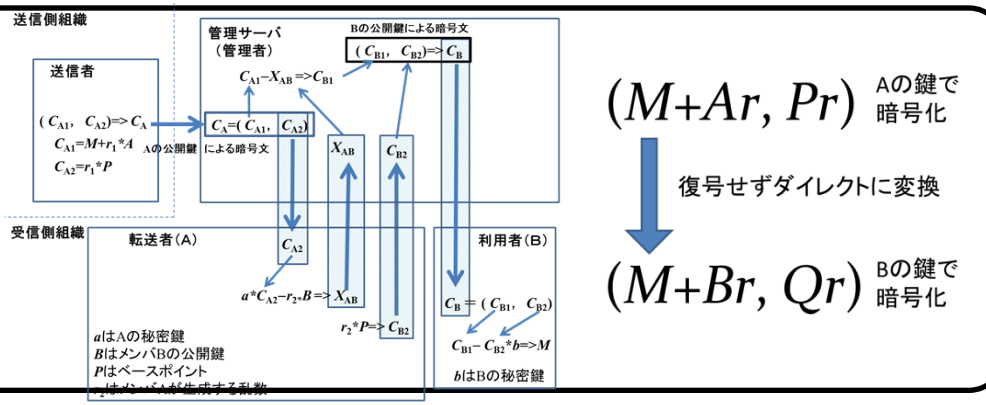


● 楕円曲線暗号に基づく組織暗号

通常の楕円ElGamal暗号の暗号化及び復号とほぼ同じ速度でアクセス許可割り当てのための再暗号化を実行できる。これは類似の方式である関数暗号などよりも遥かに高速である。

Semi-Honestモデルにおける安全性だけでなく、それより遥かに過酷な条件の、選択暗号文攻撃に対する安全性など、厳密な暗号数理上の安全性も証明した。

この方式について特許を申請。また、この方式の組織暗号システムによって全国の実証実験を行った。

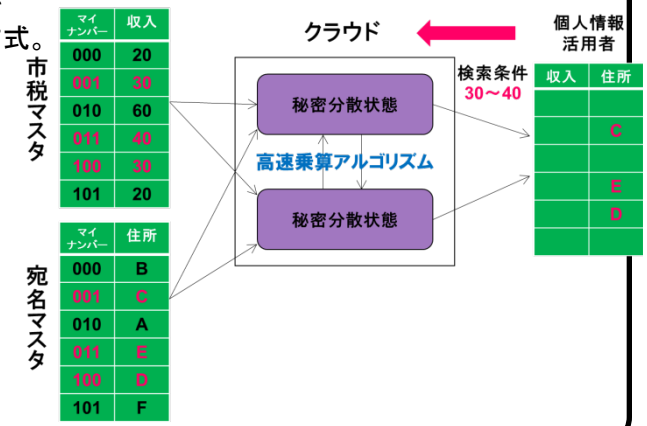


● プライバシー保護条件付き情報開示

数値を保護したままで、それを基準値などとの比較が行える方式。秘密分散を使う。

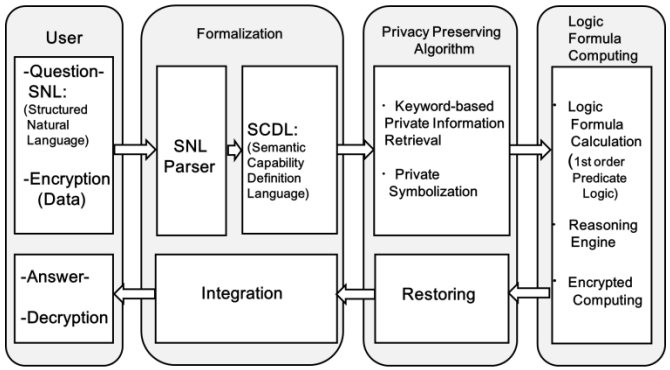
大小比較のアルゴリズムを工夫することによって高速な処理を実現した。

従って、秘密分散されたままでのソートも現実的な時間内で実行可能である。

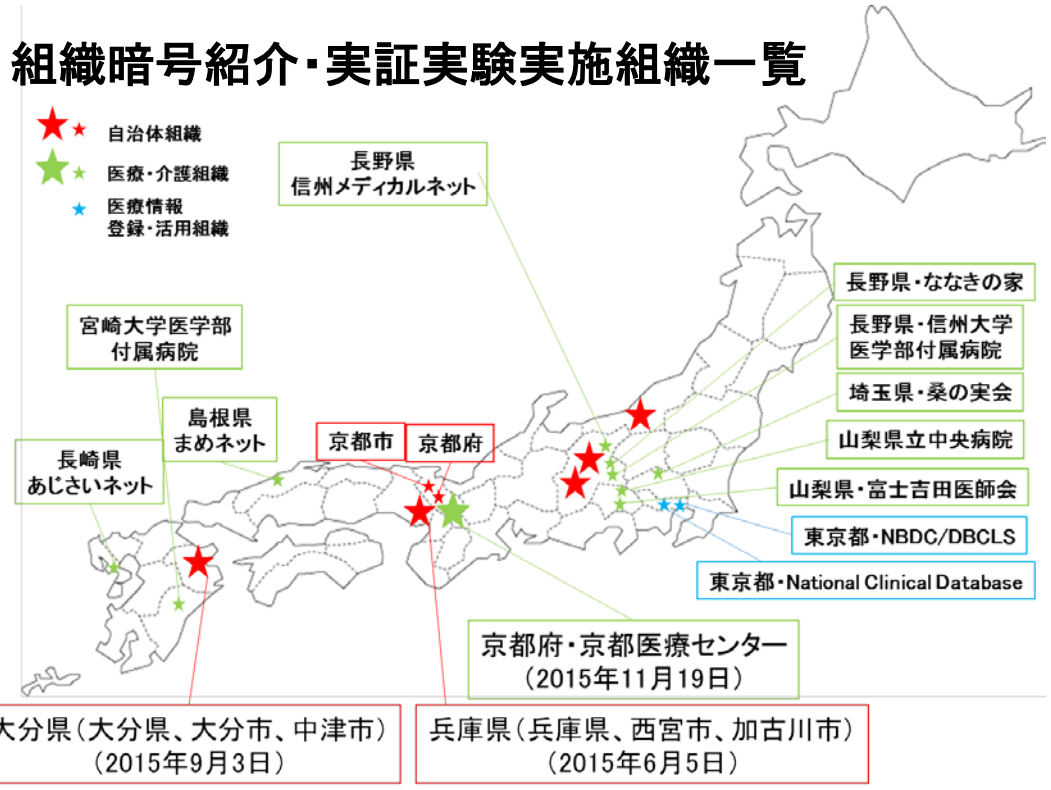


● 論理学暗号

現代論理学暗号、現代暗号による秘匿検索機能、形式化記述言語（SCDL言語）を用いて、秘匿論理処理及びアルゴリズムや論理の正当性検証を実現する方式を理論研究した。



③組織暗号の社会的実装に向けた啓蒙・周知活動成果



● 組織暗号の実証実験による組織間機密通信の提唱

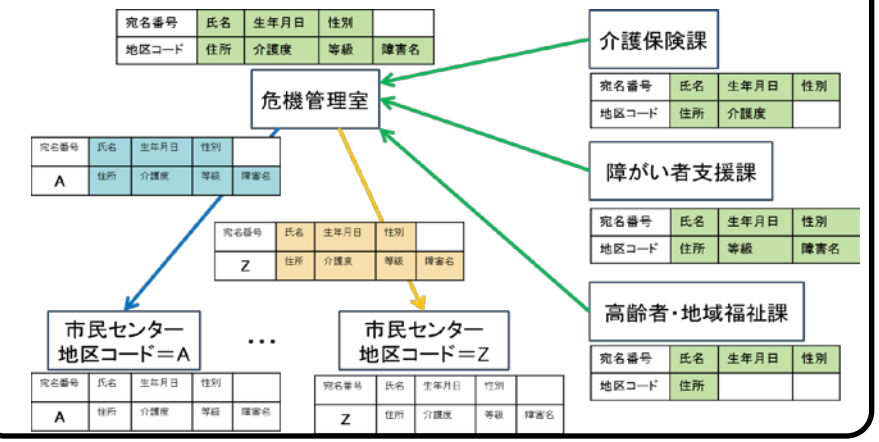
関東及び西日本の主要都市で、11カ所の自治体、6カ所の医療・介護機関を訪問し組織暗号紹介した。また、その中の5か所の自治体、1か所医療機関にて組織暗号の実証実験実施した。

実証実験では、組織暗号をそれぞれの自治体・医療組織の業務（それぞれ3例～4例）を対象に適用方式を検討し説明、訪問先の職員の方々に個人情報・医療情報を取り扱う業務を安全に遂行できることを確認いただき、組織暗号の有効性・有用性を確認できた。

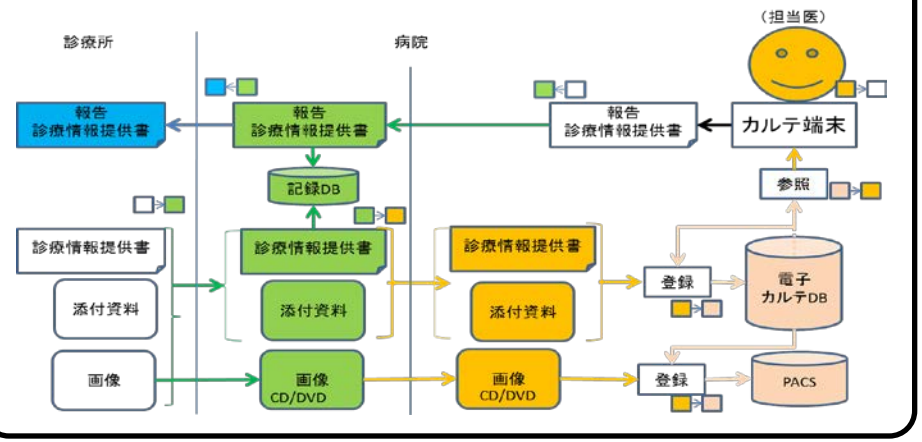
また実証実験では、訪問先の業務を想定した組織暗号適用システムの操作実験を実施、実際の操作を訪問先の職員の方々に行なっていただき、暗号化・鍵の付替え・復号の処理時間が業務に支障をきたさないことを確認いただき、組織暗号の実用性能性を確認した。

マイナンバー制度の運用や地域包括ケア体制の整備の進展に応じ、今後ますます必要となる個人情報・医療情報の利活用と保護の両立に向け、訪問先の職員の方々、別途実施した有識者・専門家との会合（20回程度実施）からは、組織間機密通信を支える組織暗号への強い期待が寄せられた。

● 組織暗号による安全な避難行動要支援者情報配布業務例



● 組織暗号による安全な紹介状（診療情報提供書）送受業務例



4. これまで得られた成果（特許出願や論文発表等）

	国内出願	外国出願	研究論文	その他研究発表	プレスリリース報道	展示会	標準化提案
組織間機密通信のための公開鍵システムの研究開発	1 （1）	0 （0）	4 （2）	94 （37）	18 （3）	0 （0）	0 （0）

※成果数は累計件数、（ ）内は当該年度の件数です。

（1） 組織通信の概念について国内外へ情報発信

組織通信及びそのセキュリティの重要性を説明し、実証実験、ひいては実用化につなげるため、パンフレット「組織暗号　利用の手引き」冊子を作成。自治体、及び医療関係者などへの訪問の際の説明資料とする。また、組織暗号及び関連する情報セキュリティ技術に関する専門的な説明をまとめた学術版パンフレットも同じく作成した。

（2） 情報セキュリティにおける暗号及び日本語(言語論理)処理の位置づけを訴えるフォーラムの実施

中央大学としてMelt-upフォーラムを主宰し、情報セキュリティや電子社会、言語処理などのテーマで実施した：

- 2014年2月14日　「電子立国は、なぜ凋落したか」
- 2014年3月4～5日　「日本の情報通信産業の盛衰から再生へ」
- 2014年4月9日　「日本語処理技術と翻訳などの応用の課題と展望」
- 2014年7月30日　「ビッグデータ時代の産業・法令日本語情報処理の課題」
- 2015年6月15, 17, 19, 20日　「組織間機密通信のための組織暗号の研究開発と社会的利用」
- 2015年10月15日　「NICT委託研究：組織間機密通信のための公開鍵システムの研究開発 ―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―　成果発表会」

5. 研究開発成果の展開・普及等に向けた計画・展望

今後我が国における電子医療・電子行政の進歩のため、利便性、安全性、個人情報保護の面で、格段に優れた性能を有する高度な情報通信システムの構築が求められており、そのようなインフラの一環として、本研究の成果である暗号技術や暗号化状態処理技術の実用化を更に推進するため、企業・自治体・医療機関などとチームを組んで本研究の成果を下記のような方面へ社会実装するプロジェクトを立ち上げたいと考えている。

1. 電子行政ではマイナポータル、電子医療では、ポケットカルテ等のPHR（Personal Health Record）等、個人による自己情報管理が広がる中で、個人―組織―組織―個人（C2B2B2C）というより広い情報通信を念頭においた研究の推進。
2. 上記の個人―組織―組織―個人間通信において、本研究で提案した方式にとどまらず、暗号技術とマネジメントを連携・融合させて機密情報を保護するための総合的研究開発。