組織暗号の社会的実装に向けて

才所 敏明　近藤 健　庄司 陽彦　五太子 政史　辻井 重男
中央大学研究開発機構

Promoting the Practical Use of Cryptosystems for Organizations in Society

Saisho Toshiaki　Kondo Takeshi　Shouji Takahiko　Gotaishi Masahito　Tsujii Shigeo
Research & Development Initiative, Chuo University

Our cryptosystems for social organizations are new cryptosystems for communications between organizations，because all of the conventional cryptosystems were mainly for communications between individuals. The feature of communications between organizations is that the sender who enciphers the message cannot specify the last receiver who decodes that enciphered message. Using our cryptosystems, the enciphered message can be transmitted to the last receiver within the receiving organization flexibly, without any decoding in distribution process. We are now promoting the practical use of Cryptosystems for Organizations in Japan. We are already carrying out the experiments of Cryptosystems for Organizations at local governments of Omachi-city，Minowa-town, Tsubame-city, Hyogo-prefecture. We're convinced that our Cryptosystems for Organizations are useful for local governments and also useful for medical agencies.

Keywords: Cryptosystems for social organaizations, communications between organaizations, Personal data, ID systems for social security and taxes, regional helathcare network, local Government, Healthcare insitiutes, Feasible field study

1. はじめに

我が国では、2013 年の番号関連四法の成立により、社会保障・税番号（マイナンバー）導入が決まり、現在、政省令等の整備が進められている。2016年より、社会保障分野、税分野、災害対策分野において、マイナンバーの利用が順次開始される予定であり、行政機関や地方自治体などが保有する個人情報の相互利用が促進されることになる。マイナンバーは、行政を効率化し、国民の利便性を高め、公平・公正な社会を実現する、社会基盤として期待されている。

これまで、我が国では2003年に個人情報保護法が成立以来、自治体においても個人情報は慎重が上にも慎重に取り扱われ、慎重過ぎるが故に、個人情報の利活用が進まない弊害も顕在化していたが、番号関連四法の成立、マイナンバーの導入により、国民の生活・生命を守るための個人情報の、適切な保護を維持しつつも、積極的な利活用が求められる新たな時代へ突入することになる。

中央大学・研究開発機構では、このように増大する個人情報の利活用ニーズへ対応すべく、個人情報の利活用時の安全性を高めることが可能な新たな暗号方式「組織暗号」の研究開発を進めている。[1-4)]

2. 組織暗号とは

組織暗号は、個人情報やパーソナルデータあるいは企業秘密などの機密情報の、組織間での安全な相互利用の支援を目指し、研究開発を進めている暗号方式である。従来の暗号方式が、主として個人間通信へ適用されるのに対し、組織暗号は組織間通信への適用を念頭に置き設計されている。

組織間通信と個人間通信の違いは、個人間通信では送信者が受信者を特定し情報を直接送信するが、組織間通信では送信者が受信者を特定できない場合や受信者へ直接送信することが不適切な場合が多いことである。そこで、組織間通信では、送信者は受信組織のしかるべき代表者へ情報を送信し、組織内の適切な中間管理者（下位の中間管理者やデータ利用者を指定し機密情報の配信を担当）やデータ利用者（復号し機密情報の処理・利用を担当）への配信は受信組織代表者へ委ねられることになる。

組織暗号は、送信者から受信組織代表者への機密情報の安全な送信だけでなく、機密情報がデータ利用者へ到達するまでの受信組織代表者および中間管理者による、受信組織内での機密情報の安全な配信を可能とする暗号方式である。従来の個人間通信向けの暗号方式を組織間通信へ適用した場合、機密情報の送信/受信ごとに暗号化/復号を繰り返すことになる。その結果、必ずしも機密情報の内容を確認する必要の無い受信組織代表者や受信組織内の機密情報配信に関わる中間管理者の手元で機密情報が復号され一時的にせよ平文が存在することになり、機密情報の平文がウイルスや不正アクセスなどの様々の脅威に晒され、受信組織内の機密情報配信プロセスでの情報漏えいのリスクが発生することになる。組織暗号は、受信組織代表者および受信組織内の機密情報配信に関わる中間管理者が、自らがデータ利用者になる（機密情報を利用する）必要のない場合は、機密情報を復号することなく、機密情報の内容を示すラベルを確認し、適切なデータ利用者または下位の中間管理者へ機密情報を暗号化状態のまま配信が可能な暗号方式である。組織間通信への組織暗号の適用により、受信組織内での配信プロセスにおける機密情報漏えいリスクを軽減させることが可能である。

3. 自治体向け実証実験の内容

組織暗号の応用により自治体業務における個人情報漏えいリスクを軽減できることを、自治体の方々に実感いただき、自治体業務システムでの活用を検討いた

だくことを目的とし、以下の内容の実証実験を企画した。

なお、本実証実験では、楕円エルガマル暗号ベースの組織暗号を使用した。楕円エルガマル暗号および楕円エルガマル暗号ベースの組織暗号方式については、参考文献[5]を参照願いたい。[5)]

1) 組織暗号の概要紹介
2) 個人情報を取り扱う自治体業務の事例調査結果の紹介
3) 実証実験実施自治体の業務における組織暗号適用方式の紹介
4) 組織暗号操作実験システムによる個人情報配信の操作紹介

送信代表者、受信代表者、担当者から構成される組織暗号基本利用モデル（図1）に準じ、実証実験を実施する自治体での個人情報を取り扱う実際の業務を想定し、以下の操作を紹介

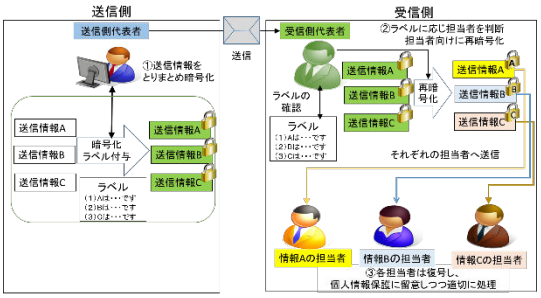

図1 組織暗号基本利用モデル

1) 送信側代表者が送信情報を取りまとめ、受信側代表者だけが復号できるよう暗号化、送信情報の内容がわかるラベルを付与し送信
2) 受信側代表者はラベルの内容を確認し、暗号化されたそれぞれの情報を処理すべき担当者を判断、それぞれの暗号化された情報を担当者だけが復号できるよう再暗号化（鍵の付替え）、ラベルを付与し送信
3) 担当者は暗号化された情報を自分の秘密鍵で復号し、適切に処理
1) 質疑応答

4. 実証実験の実施結果概要

組織暗号実証実験は、2014年度に大町市役所、蓑輪町役場、燕市役所の3カ所で実施、2015年度に入り兵庫県庁で実施した。以下、各自治体で実施した組織暗号操作紹介事例および実証実験への反応などについて報告する。

4.1 大町市役所（2014年10月15日）

組織暗号操作実験事例としては、敬老会招待者リスト作成業務を選定した。住民基本台帳DBをアクセスできるのは市民課であり、敬老会招待者リスト作成を担当する課は直接アクセスできないので、市民課に依頼している。その業務の情報フローを対象に組織暗号を適用した安全な配信例を紹介した。

当日は、大町市役所および北アルプス広域連合の職員の方々、報道関係者の方々、約20名に参加いただいた。参加者からは、組織暗号の、復号せずに鍵の付替えが可能な、再暗号化の機能に、大変驚いた、とのご意見をいただいた。

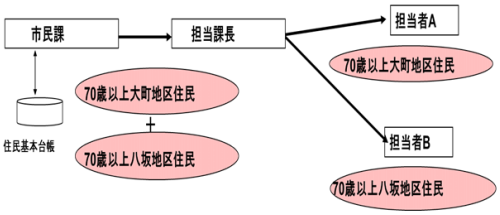

図2 敬老会招待者リスト作成業務・情報フロー

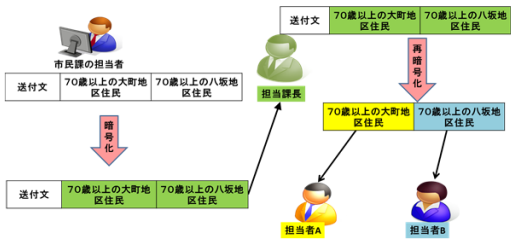

図3 敬老会招待者リストの担当者への安全な配信

なお、本実証実験については、翌日、中日新聞（中信総合版2014年10月16日（木）朝刊の19面）および大糸タイムズ（2014年10月16日（木）の1面）で紹介され、また大町ケーブルテレビで10月22日～28日、1日6回、実証実験の状況が放映・紹介された。

図4 中日新聞（左）および大糸タイムズ（右）の記事

4.2 箕輪町役場（2014年11月7日）

組織暗号操作実験事例としては、箕輪町役場から居

宅介護事業所への要介護度認定結果の通知業務を選定し、その業務の情報フローを対象に組織暗号を適用した安全な配信例を紹介した。

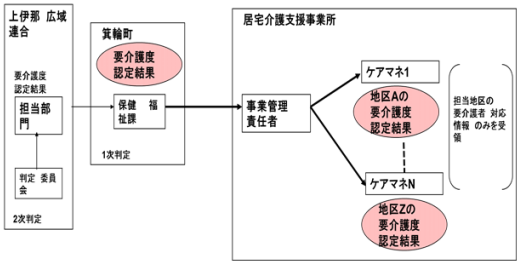

図5 要介護認定結果通知業務・情報フロー

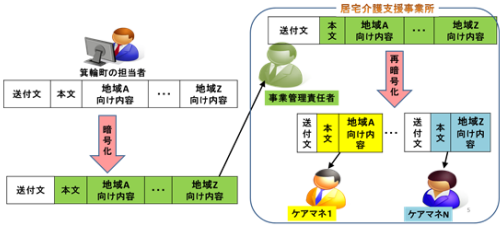

図6 要介護認定結果のケアマネへの安全な配信

当日は、箕輪町役場の方々、報道関係者など、約20名の参加者であった。自治体の様々の業務を担当されている部門の方々に参加いただいたこともあり、質疑応答は活発に行われ、個人情報の取り扱いや組織暗号の可能性への関心の高さがうかがえた。

なお、本実証実験については、翌日、みのわ新聞（2014年11月8日の1面）で紹介された。


みのわ新聞

町で「組織暗号」実証実験

技術の実用化に向け協力

箕輪町は7日、中央大学研究開発機構ユニットから依頼を受けて実験に協力、各課情報化推進員の職員が参加し、パソコン5台を使って情報のやり取りをした。

福祉課役が個人情報を暗号化、福祉施設事業者役が再度暗号化を施し、ケアマネジャー役が平文化する一連のセキュリティーの流れを確認した。モデル実験に対し、箕輪町で採用したケースを踏まえ「町の外部団体との連絡時には便利だけでなく保管する時も暗号化できるのか」などの意見が出た。ユニット担当者は「参考にして自治体での実用展開を目指したい」とした。

これまでに情報漏えいなどの問題は町内では発生してない、同技術を採用する予定は現在ないという。担当の町総務企画課は「マイナンバー制度の導入が見込まれている。これまで以上に厳しい管理を求めていきたい」としている。

図7 みのわ新聞の記事

4.3 燕市役所（2014年11月21日）

組織暗号操作実験事例としては、後期高齢者医療広域連合から燕市役所への後期高齢者医療通知業務を選定し、その業務の情報フローを対象に組織暗号を適用した場合の安全な配信例を紹介した。

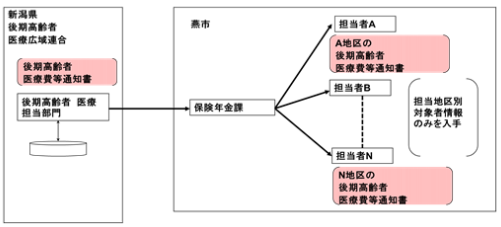

図8 後期高齢者医療通知業務・情報フロー

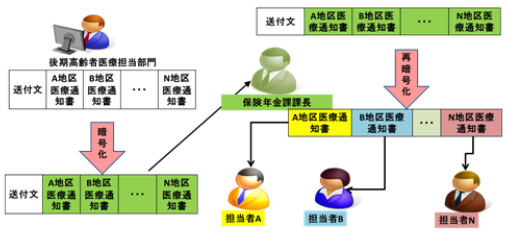

図9 医療通知書の担当者への安全な配信

当日は、燕市役所、新潟県庁、本実証実験に協力い

ただいた事業創造大学院大学の方々や報道関係者など、総勢約20名の参加者であった。自治体関係者からは、個人情報を保護しつつも利活用を更に推進する必要があるとの認識や、暗号技術により個人情報のより安全な取り扱いが可能になることへの期待などが表明され、また質疑応答では、組織暗号の運時の鍵管理問題への質問など、組織暗号への関心の高さがうかがえた。

なお、本実証実験については11月28日、電波タイムズ(2014年11月28日の1面)で紹介された。


燕市役所で「組織暗号実証実験式」
中央コリドー情報通信研究所など

図10 電波タイムズの記事

4.4 兵庫県庁(2015年6月5日)

組織暗号操作実験事例としては、納税滞納者一斉催告業務を選定し、その業務の情報フローを対象に組織暗号を適用した場合の安全な配信例を紹介したが、ここでは、災害時の避難行動支援者のための要支援者情報フローを対象にした組織暗号適用方式を示しておく。

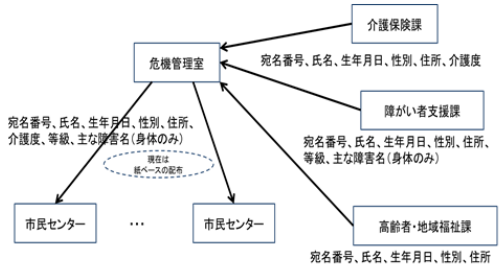

図11 避難行動要支援者情報配布業務・情報フロー

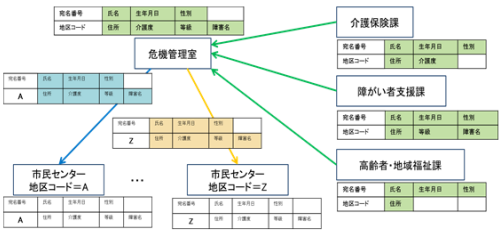

図12 避難行動要支援者情報の安全な配布

当日は、兵庫県電子自治体推進協議会会員である兵庫県内自治体の情報システム担当部門の方々など、総勢約30名の参加者であった。質疑応答では、組織暗号の運用時の鍵管理の問題や組織暗号利用上の課題への質問など、組織暗号への関心の高さがうかがえた。

5. 医療機関向け紹介活動状況。

2015年7月より、医療機関における組織暗号の活用可能性を把握するため、以下の医療機関・組織の協力を得、組織暗号の説明と各機関・組織における個人情報の管理・共有方法についての情報収集を開始した。

①信州メディカルネット
②しまね医療情報ネットワーク
③京都医療センター
④富士吉田医師会検査センター

今後、上記医療機関・組織と議論を深めると同時に、更に多くの機関・組織との意見交換を実施、各地で構築される地域包括ケア体制における個人情報の利活用と保護の両立面の課題把握と、組織暗号の活用の可能性を検討する予定である。

6. おわりに

組織暗号の実証実験を通じ、組織暗号への期待とその実務への適用時の課題が把握できた。それを踏まえ、我々研究開発部隊としては以下の活動に注力する予定である。

(1)実証実験等の紹介活動の継続

多くの組織で、組織暗号の個人情報保護に対する有効性・有用性を実感していただくことが重要

(2)組織暗号実装支援環境整備への注力

組織暗号の活用/組込みが容易に行えるよう、モジュール/組込みパッケージ/SIサービス提供事業者の確保が重要

(3)組織暗号利用の関係省庁へのご説明

自治体、医療・介護、金融機関・民間企業等での組織暗号活用に対する関係省庁のご理解・ご支援が大変重要

(4)多様な個人情報保護ニーズへの対応

個人情報の収集・共有・利用環境は多様であり、組織暗号により個人情報保護が実現できる組織間・組織内の配信は、そのごく一部。社会のニーズを的確に把握しつつ、暗号化状態処理、秘密分散状態処理等の更なる研究開発の企画・推進が必要

7. 謝辞

本研究は、国立研究開発法人情報通信研究機構（NICT）における高度通信・放送研究開発委託研究課題「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―」の下に行ったものである。

組織暗号の実証実験にあたっては、大町市役所、箕輪町役場、燕市役所、事業創造大学院大学、兵庫県庁、加古川市役所、西宮市役所の各自治体・大学に協力いただいた。

関係各位に感謝する。

参考文献

[1] 辻井重男,山口浩,只木孝太郎,五太子政史,藤田亮. 受信側主導による組織暗号の構想 － 階層型組織用多変数公開鍵,及びフラット型組織用楕円暗号 －. 信学技報告, ISEC2013-40, SITE2013-35, ICSS2013-45, EMM2013-42(2013-07), July2013.

[2] 辻井重男,山口浩,才所敏明, 五太子政史,只木孝太郎,藤田亮. 受信側主導による組織暗号の構想 － 第2報 －. Proc. SCIS2014, 3E1-1, January 2014.

[3] 才所敏明,辻井重男. 組織暗号応用機密情報配信システムに関する考察. CSS2014.

[4] 才所敏明,近藤健,庄司陽彦,五太子政史,辻井重男. 組織暗号の実証実験－自治体における個人情報保護に向けて. SCIS2015.

[5] 才所敏明,近藤健,庄司陽彦,五太子政史,辻井重男. 組織暗号の構成と社会的実装－個人情報の安全な利活用を目指して－. 情報処理学会論文誌56巻9月号.