自治体における組織暗号実証実験報告

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
〒112-8551 東京都文京区春日 1-13-27
†toshiaki.saisho@advanced-it.co.jp ‡tsujii@tamacc.chuo-u.ac.jp

あらまし 組織暗号は、個人間通信に適用される従来の暗号方式と異なり、暗号化をする送信者が復号する受信者を特定できないことが多い組織間通信への適用を念頭に置き、受信組織の事情に応じ臨機応変に組織内を暗号化状態のまま転送可能で、復号者への安全な情報配信が可能な暗号方式である。
組織間・組織内で個人情報を取り扱う業務が多い自治体にて、このような特徴を有する組織暗号の有用性・有効性をご理解いただくべく、楕円エルガマル暗号ベースの組織暗号を利用した実証実験を精力的に展開中である。
本発表では、組織暗号の紹介と共に、大町市役所、箕輪町役場、燕市役所、兵庫県庁等、各自治体で実施した実証実験の内容や結果について、報告する。

The reports on Demonstration Experiments of Organizational Cryptosystem at Local Governments in Japan

Toshiaki Saisho† Takeshi Kondo Takahiko Shouji Masahito Gotaishi Shigeo Tsujii‡

Research & Development Initiative, Chuo University
1-13-27, Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan
†toshiaki.saisho@advanced-it.co.jp ‡tsujii@tamacc.chuo-u.ac.jp

Abstract Organizational Cryptosystem, which we are proposing, is a new cryptosystem of which receivers can directly re-encrypt the ciphertext for them into the one decryptable for other people without decrypting. So, encrypted personal data can be transferred safely within organizations to the last receiver who should decrypt it. We are putting many Demonstration Experiments of Organizational Cryptosystem into effect at Local Governments so that members of Local Governments can understand the effectiveness of our Organizational Cryptosystem.
In this report, we explain our Organizational Cryptosystem, contents of Demonstration Experiments of Organizational Cryptosystem, and responses of members of Local Governments.

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．

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．

組織暗号は, 組織間通信における受信組織内情報配信プロセスの特徴である受信組織代表者や中間管理者の臨機応変の情報配信を可能としつつも, 送信者が提供する機密情報のより安全な配信を可能とする暗号方式である．従来の暗号方式が，送信者が受信者を特定する送信側主導の暗号方式であることに対し，組織暗号方式は，受信側主導の暗号方式と言える．

3　組織暗号の構成

組織暗号方式は，多変数公開鍵暗号，楕円 ElGamal 暗号など，いくつかの公開鍵暗号ベースに構成可能であるが, 本章では実証実験に使用した楕円 ElGamal 暗号ベースの組織暗号方式について紹介する．

まず 3.1 にて楕円 ElGamal 暗号を説明し，次に 3.2 にて楕円 ElGamal 暗号の機能を利用した再暗号化（鍵の付替え）方式を説明する．この再暗号化方式によって，受信した人のみが復号できるよう（その受信者の公開鍵で）暗号化された機密情報を，その受信者が復号することなく新たな受信者のみが復号できる（新たな受信者の公開鍵で）暗号化された機密情報へ変換することができ, 組織暗号方式の特徴である, 機密情報の暗号化状態のままの組織内配信，を実現している．

3.1 楕円 ElGamal 暗号

ElGamal 暗号は離散対数計算の困難性，即ち有限体上のベキ乗は容易に計算できるがその逆演算は困難であることを利用した公開鍵暗号である．同様に，楕円曲線上の点が生成する Jacobi 群において乗算は容易に計算できるがその逆演算である除算は困難であることを利用したものが楕円曲線暗号の一種である楕円 ElGamal 暗号である．以下，楕円 ElGamal 暗号の暗号化, 復号手順を説明する．

公開設定：E/F_q: 楕円曲線,
$E(F_q)$: 素位数巡回群,
P: ベースポイント

秘密鍵：乱数 a

公開鍵：A $(=a*P)$

暗号化：

1. 乱数 r を生成する．
2. 平文メッセージ M に乱数と公開鍵の積を加えて暗号文 C_{A1} を得る．
   $C_{A1}=M+ r*A$
3. 乱数にベースポイント P を掛けて C_{A2} $(=r*P)$ を得る．
4. C_A ＝ $(C_{A1},\ C_{A2})$ を，平文 M に対する暗号文として，復号者に送る．

復号：

1. 暗号文のうち C_{A1} から C_{A2} と秘密鍵 a の積を減ずることによって平文 M が得られる：

$$M= C_{A1}- C_{A2}*a\ (=M+r*A- r*P*a)$$

3.2 再暗号化(鍵の付替え)方式とその安全性

上記のような楕円 ElGamal 暗号の機能を利用して，メンバ A の公開鍵で暗号化された暗号文を一度も平文に戻すことなくメンバ B の公開鍵で暗号化した暗号文に変換すること（再暗号化）ができる．

まず, A のみで鍵の付替えを行うシンプルな再暗号化方式の説明を以下に行う．なお, Jacobi 群のプロパティである公開設定は **3.1** 節と共通とし, 更に以下のようにパラメータ設定をする．

秘密鍵：A の秘密鍵 a,
B の秘密鍵 b

公開鍵：A の公開鍵 A $(=a*P)$,
B の公開鍵 B $(=b*P)$

平文メッセージ M は A の公開鍵および送信者の生成した乱数 r_1 によって暗号化されて暗号文 C_A となっている．

$C_A=(C_{A1}, C_{A2})$

$C_{A1}=M+r_1*A, \quad C_{A2}=r_1*P$

A から B への再暗号化手順：

(変換用鍵の生成)

1　新しい乱数 r_2 を生成し，$C_{B2}=r_2*P$ を得る．

2　以下の式によって，再暗号化を行うための変換用鍵 X_{AB} を生成する：

$X_{AB}=a*C_{A2}-r_{2*}B$

(変換用鍵による再暗号化)

3　この X_{AB} を使って，暗号文 C_{A1} を C_{B1} に変換する：

$C_{B1}=C_{A1}-X_{AB}$

$(=M+r_1*a*P-a*r_1*P+r_2*B=M+r_2*B)$

以上の手順により，A の公開鍵で暗号化した暗号文 C_A を B の公開鍵で暗号化した暗号文 C_B へ再暗号化（鍵の付替え）できる．

なお，この手順ではシステム上では平文は一切生成されないため平文が直接漏えいするリスクは無いが，再暗号化に使用する暗号文 C_A と復号に使用する秘密鍵 a の両方を A が保有・使用するため，A は平文を求めることが可能となり，また A のシステムからの暗号文および秘密鍵の両方のデータ漏えいによる復号のリスクが残る．

このような課題を解決する対策については情報処理学会論文誌（参考文献[5]）に詳述しているので参照願いたい．なお，以降に説明する自治体での実証実験では，組織暗号そのものおよびその有用性・有効性をご理解いただくことを主眼としているため，本章で説明したシンプルな手順に基づき操作実験用システムを開発，実証実験にて使用することとした．

4　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．

（1）　組織暗号の概要紹介

組織間通信における機密情報保護のニーズ，それに応える組織暗号の特徴の紹介

（2）　個人情報を取り扱う自治体の業務例調査結果の紹介

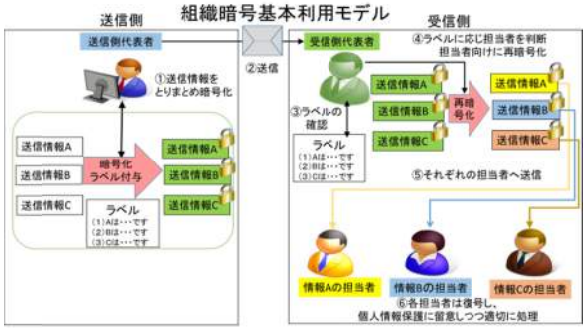
組織暗号の活用が可能と思われる，自治体での個人情報を取り扱う業務の例の紹介

（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

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への組織暗号の具体的な適用方式の提案・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デモ実施

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，以下の内容のデモ実施（操作自体は自治体職員の方々への依頼を想定）



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

（5） 質疑応答

組織暗号の機能，自治体業務への適用可能性や適用方式などについての質疑

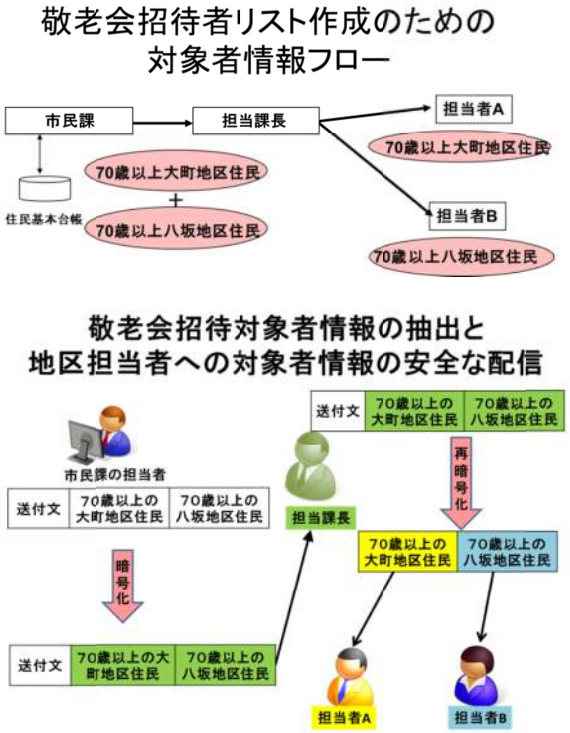
5 実証実験実施状況および自治体側の評価

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実証実験の概要について報告する．

5.1 大町市役所での実証実験

2014 年 10 月 15 日，最初の組織暗号実証実験を長野県の大町市役所にて実施した．

大町市役所内の個人情報の配信が必要となる三つの業務を組織暗号応用想定業務として，個人情報の流れを確認，その安全性を高めるための組織暗号の具体的応用案を提示した．その一例を以下に示す．



その上で，組織暗号操作実験システムを利用し，組織暗号応用機密情報配信システムの主要機能である，個人情報の送信代表者による暗号化送信，受信代表者による再暗号化送信，担当者の復号，などの一連の操作を紹介した．

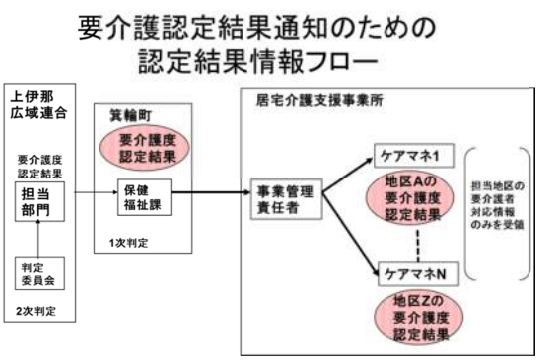
当日は，大町市役所および北アルプス広域連合の職員の方々，報道関係者の方々，約 20 名に参加いただいた．参加者からは，組織暗号の，復号せずに鍵の付替えが可能な，再暗号化の機能に，大変驚いた，とのご意見をいただいた．

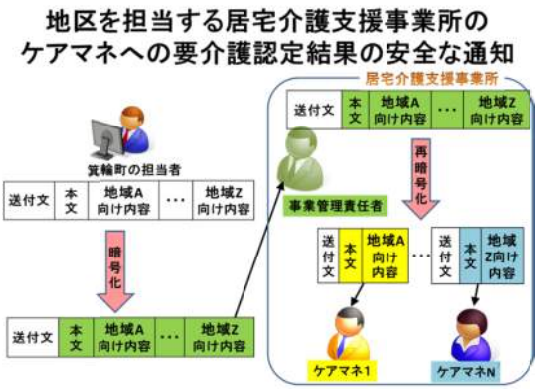
なお，本実証実験については，翌日，中日新聞（中信総合版 2014 年 10 月 16 日（木）朝刊の 19 面）および大糸タイムズ（2014 年 10 月 16 日（木）の **1** 面）で紹介され，また大町ケーブルテレビで 10 月 22 日～28 日，1 日 6 回，実証実験の状況が放映・紹介された．

5.2 箕輪町役場での実証実験

2014 年 11 月 7 日，長野県上伊那郡の箕輪町役場で組織暗号実証実験を実施した．なお，箕輪町役場では実証実験に使用する PC の借用が難しかったため，PC を持ち込み，箕輪町役場のネットワークに接続，操作の紹介に使用した．

箕輪町役場内の個人情報の配信が必要となる三つの業務を組織暗号応用想定業務として，個人情報の流れを確認，その安全性を高めるための組織暗号の具体的応用案を説明した．その一例を以下に示す．





その上で, 個人情報の送信代表者による暗号化送信，受信代表者による再暗号化送信，担当者の復号, などの一連の操作を紹介した.

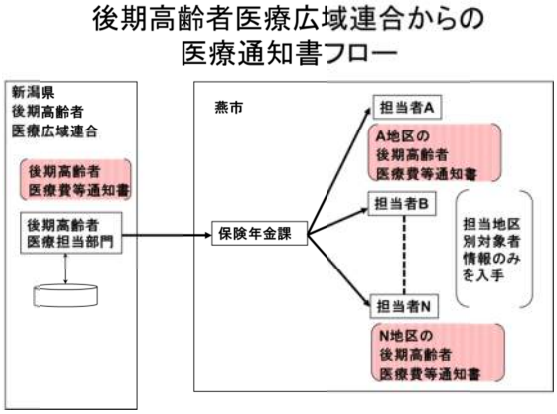
当日は，箕輪町役場の方々，報道関係者など, 約 20 名の参加者であった. 自治体の様々の業務を担当されている部門の方々に参加いただいたこともあり, 質疑応答は活発に行われ, 個人情報の取り扱いや組織暗号の可能性への関心の高さがうかがえた.

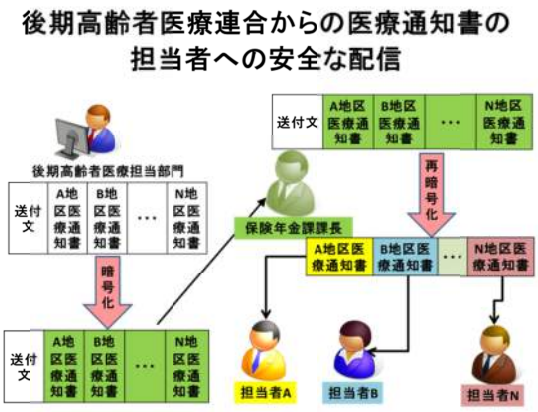
なお，本実証実験については，翌日，みのわ新聞（2014 年 11 月 8 日の 1 面）で紹介された.

5.3　燕市役所での実証実験

2014 年 11 月 21 日，新潟県の燕市役所にて組織暗号実証実験を実施した.

燕市役所における個人情報の配信が必要となる二つの業務を組織暗号応用想定業務として選定, それらの業務における 4 種の個人情報の流れを対象に, その安全性を高めるための組織暗号の具体的応用案を説明した. その一例を以下に示す.





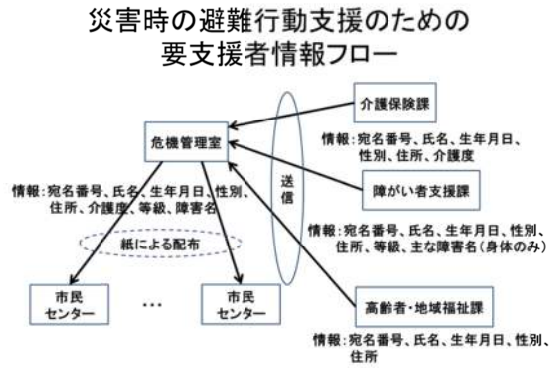
その上で, 個人情報の送信代表者による暗号化送信，受信代表者による再暗号化送信，担当者による復号, などの一連の操作を紹介した.

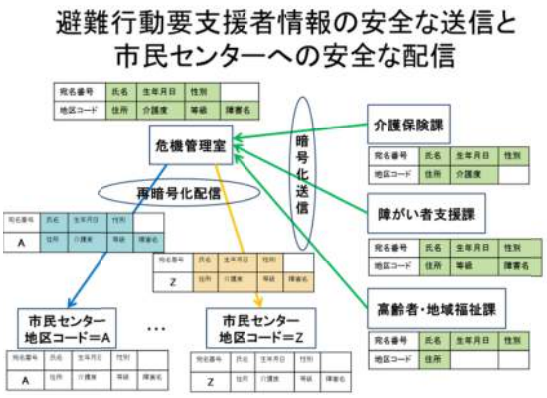
当日は，燕市役所，新潟県庁，本実証実験に協力いただいた事業創造大学院大学の方々や報道関係者など，総勢約 20 名の参加者であった. 自治体関係者からは，個人情報を保護しつつも利活用を更に推進する必要があるとの認識や, 暗号技術により個人情報のより安全な取り扱いが可能になることへの期待などが表明され，また質疑応答では，組織暗号の運用時の鍵管理問題への質問など，組織暗号への関心の高さがうかがえた.

5.4　兵庫県庁での実証実験

2015 年 6 月 5 日，兵庫県庁にて組織暗号実証実験を実施した. 大規模な自治体での最初の組織暗号実証実験であった.

組織暗号実証実験は，兵庫県内全市町（41市町）および，県，兵庫県市長会，兵庫県町村会から構成される兵庫県電子自治体推進協議会向けのイベントとして実施いただくことになり，組織暗号応用想定業務も，県庁，加古川市役所，西宮市役所の業務の中から1件ずつ選定，個人情報の流れを確認，その安全性を高めるための組織暗号の具体的応用案を説明した．その一例を以下に示す．





その上で，個人情報の送信代表者による暗号化送信，受信代表者による再暗号化送信，担当者による復号，などの一連の操作を紹介した．

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．また，実証実験終了後，井戸兵庫県知事と面談，組織暗号が自治体業務における個人情報の安全な利活用を支援する技術であることなど，ご説明した．知事からは，（人的および管理的対策も重要だが）システム的対策（技術的対策）が重要，という認識を示され，情報セキュリティ研究開発部隊としては意を強くすると同時に，適切な技術的対策を提供する責任を痛感した．

6　実証実験の意義・成果

実証実験を通じ，協力頂いた自治体からは，組織暗号そのものや組織暗号の応用に関し，以下のような貴重なご意見・ご感想をいただいた．

(1)組織暗号の再暗号化（復号せず鍵の付替え）機能への驚き

従来の個人間通信向け暗号技術からは想像できない機能であり，組織暗号の可能性を感じていただいた．

(2)日々取り扱っている個人情報の重要性の再認識

組織暗号やその応用に関する感想では無いが，自治体職員の方々に個人情報の保護の重要性を再認識いただいた．

(3)実際に使用する場合のサポートへの期待（モジュールの商品化，市販パッケージへの組込み，SI支援など）

組織暗号の活用を推進いただくには，自治体が容易に取り組める支援環境の整備も重要であることを痛感した．

(4)個人情報の安全な取扱いには，配信プロセスの安全性だけでは不十分

今回の組織暗号の実証実験では，配信プロセスの安全性向上への適用に的を絞ったが，自治体における多様な個人情報取り扱い業務を想定した自治体業務のための安心安全情報処理基盤の必要性を痛感した．

(5)情報技術への不安，不信（情報漏えい事件の報道などより）

情報セキュリティ技術の適切な組込みと確実な運用がなされれば，このような問題が発生しないはずだが，運用・利用者のITセキュリティリテラシーの低さや，運用・利用上の要件にマッチしない技術的対

策などが原因で発生する事故・事件が，情報技術・情報セキュリティ技術そのものへの不信につながっているのは大変残念．事故・事件の原因の本質をご理解いただける説明も必要と感じた．

(6)従来の紙ベースから情報技術利用への変化の責任の重さ

変化はリスクを伴うものだが，情報技術・情報セキュリティ技術利用に対する安心感を醸成する取り組みも必要と感じた．

(7)先進的技術の独自採用は困難

先進的技術を，一自治体で先行し実務へ組み込むことには，躊躇される自治体が多かった．組織暗号を安心して採用いただける環境作りの必要性を感じた．

7　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

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.