SCIS 2015 The 32nd Symposium on
Cryptography and Information Security
Kokura, Japan, Jan. 20- 23, 2015
The Institute of Electronics,
Information and Communication Engineers

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

Demonstration experiment of usability and effectiveness of Organizational Cryptosystem for protecting personal information in local government activities

才所 敏明* 近藤 健* 庄司 陽彦* 五太子 政史*
Toshiaki Saisho Takeshi Kondo Takahiko Shouji Masahito Gotaishi
沼田 秀穂† 仙石 正和† 辻井 重男*
Hideho Numata Masakazu Sengoku Shigeo Tsujii

あらまし 中央大学・研究開発機構では，組織間での個人情報を含む機密情報の安全な配信・利活用支援をめざし，組織暗号という新たな暗号方式の研究開発を進めている．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考案され，受信組織の事情に応じ臨機応変に受信組織内を暗号化状態のまま逐次転送可能で，受信者（復号者）への安全な機密情報の配信が可能な暗号方式である．現在，実装が完了した楕円エルガマル暗号ベースの組織暗号を利用し，個人情報を取り扱う業務が多い自治体の方々に組織暗号の有用性・有効性をご理解いただくべく，自治体での実証実験を展開中である．本発表では，楕円エルガマル暗号ベースの組織暗号の紹介と共に，長野県大町市役所，同箕輪町役場，新潟県燕市役所にて実施した組織暗号実証実験の内容や結果について，報告する．

キーワード 組織暗号，個人情報保護，マイナンバー，自治体，組織間通信，暗号実装，実証実験

1 組織間通信の特徴

情報送信者と情報利用者が異なる組織に属する通信（組織間通信）では，個人間通信とは異なり，送信者が利用者を特定できない場合が多い．一般に，組織体制，担当者などは，組織変更や人事異動などで変化し，最新の状況を常に情報送信者へ徹底させることは困難である．また組織情報・人事情報の外部への公表を控える場合も多いため，情報送信者が異なる組織内の情報利用者を特定するのは難しい．

そこで，情報送信者（送信代表者）は受信組織内のしかるべき窓口（受信代表者）に送信し，受信組織内の適切な情報利用者への配信は，その受信代表者へ委託する場合が多い．受信代表者は，送信代表者より送信されてきた情報の内容を確認し，適切な部門長（中間管理者）または情報の利用者へ送信し，中間管理者は更に下位の中間管理者または情報の利用者へ送信する．このように，送信代表者から送付された情報は，受信代表者が受け取った後，受信組織内を転々と転送され，適切な情報利用者へ到達することになる．

* 中央大学 研究開発機構 〒112-8551 東京都文京区春日 1-13-27
Research & Development Initiative, Chuo University
1-13-27,Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan

† 事業創造大学院大学 〒950-0916 新潟市中央区米山 3-1-46
Graduate Institute for Entrepreneurial Studies
3-1-46, Yoneyama, Chuo-ku, Niigata-city 950-0916, Japan

組織間通信の特徴は, 情報送信者から情報利用者までの情報配信プロセスに多くの関係者が介在することにある. また, 受信組織内の配信プロセスや情報利用者は, 受信組織側の判断で決定されることにある.

2　組織間通信と組織暗号

組織間通信を利用し機密情報を配信する場合, 個人間通信の場合と同様, 機密情報の保護のために暗号方式の利用が必要となる.

しかし, 組織間通信へ個人間通信向けに利用されている既存の暗号方式をそのまま適用した場合, 送信代表者から受信代表者, 受信代表者から中間管理者, 中間管理者から情報利用者, などの機密情報の送受信ごとに暗号化/復号が必要となる. その結果, 受信組織内の機密情報の利用者以外の関係者（受信代表者, 中間管理者など）の転送処理の過程で, 機密情報が不必要に復号されてしまい, ウイルスや不正アクセスなどの脅威に晒され, 機密情報漏えいのリスクが高まることになる.

組織暗号は, 組織間通信の特徴である受信組織内での機密情報の転々とした配信プロセスにおいても, 都度の復号を必要とせず, 利用者まで機密情報を暗号化状態のまま配信を可能とする暗号方式である.

組織暗号では, 暗号化された機密情報の受信者が, 復号せずにその機密情報を必要とする転送先を決定できるように, 暗号化された機密情報の内容を示すラベルを付与している. 受信者は機密情報を自ら利用する必要があるかどうかを判断, 機密情報の利用（復号）が不要な場合にはラベルの内容により転送先を決定し, 受信者向けに暗号化されている機密情報を転送先の新たな受信者だけが復号できるように暗号化された機密情報へ変換し, 転送することができる.

特定の人向けに暗号化された機密情報を, 復号すること無く, 他の人向けに暗号化された機密情報へ変換できることが組織暗号の特徴的機能であり, この機能により, 組織間通信の特徴である受信組織内での転々とした転送においても機密情報は暗号化状態のまま転送でき, 配信プロセスでの情報漏えいのリスクを大幅に軽減できる.

（文献[1], [2], [3]）

3　楕円エルガマル暗号ベースの組織暗号

中央大学研究開発機構では, 複数の組織暗号方式を開発中であるが, 自治体での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.

本章では, 楕円エルガマル暗号ベースの組織暗号の利用により, 特定の受信者の秘密鍵のみで復号できるように暗号化された機密情報を, 新たな受信者である転送先の中間管理者あるいは情報利用者の秘密鍵のみで復号できるように暗号化された機密情報へ変換（再暗号化, 鍵の付替え）することが可能であることを示す.

まず, 楕円エルガマル暗号の暗号化・復号のアルゴリズムを以下に示す. 平文の機密情報 M は受信者 A 向けに暗号化され, 受信者 A の秘密鍵 a にて復号できることを示している.

［定義］

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

A の秘密鍵：乱数 a

A の公開鍵 : 秘密鍵とベースポイントの積 $aP(=A)$

平文機密情報：M

［暗号化］

① 乱数 r_1 の生成

② $M_1'=M+A*r_1$

③ $M_2'=r_1*P$

$M'=(M_1',\ M_2')$が平文機密情報 M に対する

A のみが復号できるように暗号化された機密情報

［復号］

① $M= M_1'-M_2'*a$

次に，A のみが復号できるように暗号化された機密情報 $M'=(M_1',\ M_2')$を，復号せずに再暗号化（鍵の付替え）し，B のみが復号できるように暗号化された機密情報 $M''=(M_1'',\ M_2'')$へ変換できること，その M''が B の秘密鍵により復号できることを示す.

［定義（追加分のみ）］

B の秘密鍵：乱数 b

B の公開鍵：$b*P(=B)$

［再暗号化］

① 乱数 r_2 の生成

② $M_2''=r_2*P$

③ 変換用鍵 X_{AB} の計算　$X_{AB}=a*M_2'-r_{2*}B$

④　$M_1"=M_1'-X_{AB}$

$M"=(M_1",\ M_2")$が平文機密情報 M に対する

B のみが復号できるように暗号化された機密情報

［復号］

①　$M=M_1"-M_2"*b$

このように，楕円エルガマル暗号ベースの組織暗号では，受信者 A の秘密鍵で復号できるように暗号化された機密情報が，変換用鍵 X_{AB} の利用により，受信者 B の秘密鍵で復号できるように暗号化された機密情報へ変換（鍵の付替え，再暗号化）が可能である．このような再暗号化（鍵の付替え）の機能により，機密情報の暗号化状態での転送が可能となる．

（文献[4]，[5]）

4　自治体業務と組織暗号

自治体業務には個人情報を活用した住民へのサービス業務が多い．しかし多くの自治体では，個人情報の利活用の制限や不便さの課題は認識されつつも，これまでは個人情報の保護を最優先せざるを得ない状況であった．

一方，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．個人情報の保護ために利活用を制限されてきた自治体業務においても，個人情報の保護に留意しつつも，個人情報の利活用が求められる時代となるものと考えられる．

楕円エルガマル暗号ベースの組織暗号（以下，単に組織暗号と略記）は，個人情報のより安全な取扱いを可能とする新たな暗号方式である．組織暗号の利用により，個人情報が自治体内の業務関係者間，あるいは外部の協力組織の関係者間を転々と配信される場合でも，配信プロセスでの個人情報の復号を必要とせず，個人情報の漏えいリスクを大きく軽減でき，また配信プロセスを構成する機器・ネットワークの運用管理面の対策や関係者に対する情報セキュリティ教育や注意義務の徹底などの人的対策の負担の軽減も期待される．

自治体業務における個人情報の利活用がますます拡大するのは必至と思われる．組織暗号は，個人情報の保護に留意しつつ利活用が求められる自治体業務の中で，幅広く活用いただけるものと考えている．

（文献[6]）

5　大町市役所での実証実験

自治体業務での組織暗号の有用性・有効性を自治体の方々に実感いただくべく，組織暗号の説明や自治体業務への適用例の紹介，デモシステムによる操作体験などから構成される組織暗号実証実験を，自治体の現場で実施中である．

本章では，最初の組織暗号実証実験に協力いただいた，長野県の大町市役所での実証実験の内容・結果を報告する．なお，大町市は，池田町，松川村，白馬村，小谷村を含む 5 市町村にて広域行政を担う北アルプス広域連合を構成，広域連合の行政サービスのための情報システムは大町市役所にある情報センターにて運用・管理されている．

5.1　実証実験概要

実証実験は，2014 年 10 月 15 日の 13 時半～15 時，大町市役所のパソコン教室を借用し実施した．

実施内容は，以下の通り．

① 挨拶（大町市役所および中央大学）

② 組織暗号に関する説明
組織暗号開発の背景，組織暗号の特徴，組織間通信における組織暗号の有用性・有効性などを説明．

③ 組織暗号を活用可能な自治体の業務例紹介
組織暗号が活用可能な個人情報を取り扱う自治体の業務例の他，大町市役所で想定される業務例を紹介（詳しくは 5.2 を参照）．

④ 大町市役所の想定業務への組織暗号適用案紹介
③で示した大町市役所の想定業務例に対し，組織暗号の具体的な適用案を紹介．個人情報の送信者から個人情報を直接処理する担当者まで，暗号化された状態で配信できることを説明．詳しくは5.2 を参照．

⑤ 組織暗号応用システムの操作実験

パブリッククラウドサービス AWS 上に構築された操作実験環境を，借用した大町市役所のパソコンから大町市役所のネットワーク経由アクセス，簡単な組織暗号応用個人情報配信システムの操作実験を実施した．なお，操作は市役所の方々に担当いただき，組織暗号応用個人情報配信システムの操作を体験していただいた．詳しくは 5.3 を参照．

⑥ 質疑応答

5.2 個人情報利用業務例と組織暗号適用案

大町市役所より例示いただいた以下の三つの想定業務に対し，具体的な組織暗号適用案（②のみ以下に図示）を提示，組織暗号がさまざまの業務へ適用可能である事を説明した．

① 市役所の代表メールアドレス管理者は，地方公共団体情報システム機構から個人情報あるいは機密情報を含むメールを受信した後，代表メールアドレス管理者は内容を確認の上，市役所内の各業務担当課長へ送信，更に業務担当課長が内容を確認の上，実務担当者へ転送する．

② 住基システム管理部門が大町市の 70 歳以上の住民の個人情報を地区ごとにまとめ，イベントを担当する業務担当部門の課長へ送信，課長は地区ごとの担当者へ担当する地区の個人情報のみを転送する．

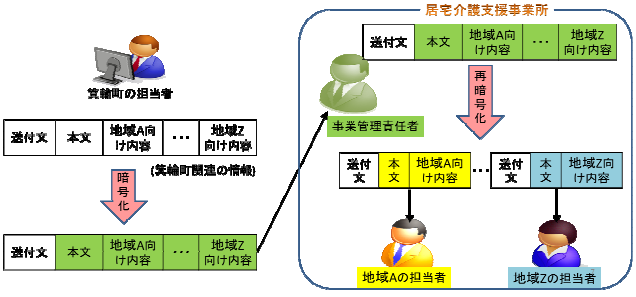

図 1．想定業務②への組織暗号適用案

③ 長野県国民健康保険団体連合会（国保連）の担当者より個人情報を含む外字字形提供依頼及び外字同定作業確認依頼が北アルプス広域連合の担当者へ届き，広域連合の担当者は依頼内容を確認し，該当市町村の担当者へ転送する．

5.3 実験環境/実験シナリオ

組織暗号を応用した個人情報配信システムの操作を体験いただくのに必要な機能は，暗号化，再暗号化，復号の三つである．これらの機能の操作を体験できる図 2 の組織暗号基本利用モデルを定義し，実験環境を構築した．

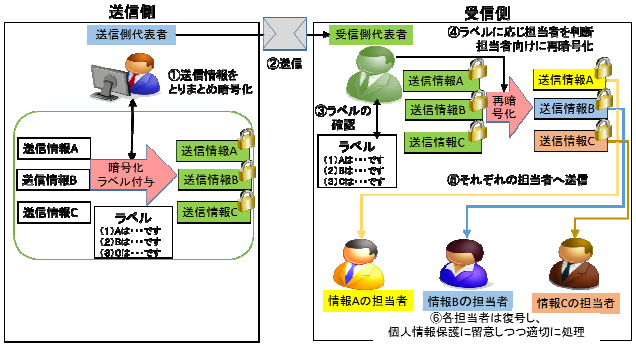

図 2．組織暗号基本利用モデル

なお，市役所内のサーバや PC 上に操作実験環境を構築することは，市役所の業務サービスへの影響やセキュリティポリシーの関係で困難であったため，パブリッククラウドサービス AWS 上に実験環境を構築，借用した PC からブラウザ経由実験環境をアクセスする形で操作実験を行った．

実験シナリオは，想定業務②をベースに，住基システム管理部門が大町市の 70 歳以上の住民の個人情報を 3 カ所の地区ごとにまとめ，イベントを担当する業務担当部門の課長へ送信，課長は地区ごとの担当者へ担当する地区の個人情報のみを転送する，というシナリオで実験を行った．

5.4 実施状況・結果

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．

6 箕輪町役場での実証実験

2 度目の実証実験は，同じく長野県の箕輪町役場の協力を得，実施した．なお，箕輪町は，伊那市，駒ケ根市，

辰野町，箕輪町，飯島長，南箕輪町，中川村，宮田村の 2 市 6 町村による上伊那広域連合を構成，箕輪町役場は伊那市の共同利用センターを行政サービスに使用している．

6.1　実証実験概要

実証実験は，2014 年 11 月 7 日の 13 時～14 時半，箕輪町役場の会議室を借用し実施した．

実施内容は，以下の通り．

① 挨拶（箕輪町役場および中央大学）

② 組織暗号に関する説明（5.1②に同じ）

③ 組織暗号を活用可能な自治体の業務例紹介
組織暗号が活用可能な個人情報を取り扱う自治体の業務例の紹介，および箕輪町役場での想定業務例の紹介（詳しくは 6.2 を参照）．

④ 箕輪町役場の想定業務への組織暗号適用案紹介
③で紹介した箕輪町役場の想定業務例に対し，組織暗号の具体的な適用案を紹介．個人情報の送信者から個人情報を直接処理する担当者まで，暗号化された状態で配信できることを説明．詳しくは 6.2 を参照．

⑤ 組織暗号応用システムの操作実験
パブリッククラウドサービス AWS 上に構築された操作実験環境を，持ち込んだパソコンから箕輪町役場のネットワーク経由アクセス，簡単な組織暗号応用個人情報配信システムの操作実験を実施した．なお，箕輪町役場の方々に操作をお願いした．詳しくは 6.3 を参照．

⑥ 質疑応答

6.2　個人情報利用業務例と組織暗号適用案

箕輪町役場より例示いただいた以下の三つの想定業務に対し，具体的な組織暗号適用案（③のみ以下に図示）を提示，組織暗号がさまざまの業務へ適用可能である事を説明した．

① 上伊那広域連合あるいは地方税滞納整理機構から税滞納者の滞納情報を町役場の税務課課長が入手，その滞納情報を滞納者の居住地域に応じ担当者へ転送する．

② 長野県後期高齢者医療広域連合等から後期高齢者医療通知書が町役場の国保医療係へ送付され，医療国保係の責任者は医療通知対象者の居住地に応じ，担当者へ転送する．

③ 上伊那広域連合の担当部門から要介護度認定の結果を入手した町役場の保健福祉の担当者は，該当する居宅介護支援事業所へ認定結果を送付，更に事業所の管理責任者は地区ごとのケアマネージャへ転送する．

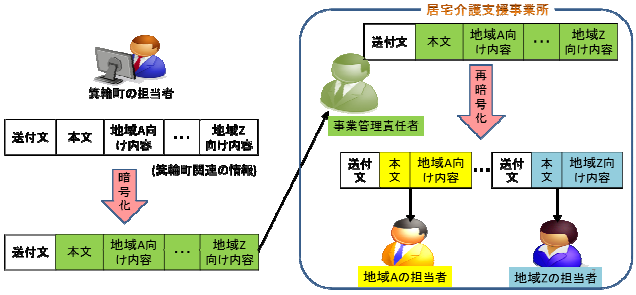

図 3．想定業務③への組織暗号適用案

6.3　実験環境/実験シナリオ

大町市役所の場合と同様，AWS 上に構築した実験環境を利用した．

箕輪町役場では，実験に使用するパソコン 5 台の借用が困難であったため，パソコン 5 台を持ち込み箕輪町役場のネットワークへ接続，AWS 上に構築された実験環境をアクセスする形で操作実験を行った．

持ち込んだパソコンの箕輪町役場のネットワーク接続の際は，町役場のセキュリティポリシーに則り，町役場の担当の方にウイルスチェックなどのパソコンの検査をお願いし，またパソコンの持ち出し時には，ハードディスクを完全消去し，情報持ち出しの無いことを確認いただいた．

操作実験は，想定業務③をベースに，要介護度認定の結果を入手した箕輪町役場の保健福祉の担当者が，特定の居宅介護支援事業所へ認定結果を送付，居宅介護支援事業所の管理責任者が A，B，C の地区ごとに担当が分かれているケアマネージャへ該当する認定結果のみを転送する，というシナリオで実施した．

6.4　実施状況・結果

当日は，箕輪町役場，上伊那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，組織暗号そのものや町役場側の現在の業務実態との関係，あるいは商品化や今後のサポートな

ど質問を多く受けた．多くの方々が，個人情報の取り扱いにあらためてリスクを実感され，組織暗号の自治体での活用可能性を感じられたようであった．

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．

7　燕市役所での実証実験

3度目の実証実験は，新潟県の燕市役所にて実施した．本実証実験は，燕市役所はもちろん，事業創造大学院大学およびNPO法人新潟情報通信研究所のご協力を得，実現した．

7.1　実証実験概要

実証実験は，2014年11月21日の13時～15時，燕市役所の会議室を借用し実施した．

実施内容は，以下の通り．

① 挨拶（燕市役所，中央大学，事業創造大学院大学）
② 暗号の技術・歴史の紹介および組織暗号に関する説明
③ 組織暗号の自治体で活用可能な業務例紹介
④ 組織暗号が活用可能な燕市役所の想定業務紹介
組織暗号が活用可能な個人情報を取り扱う燕市役所の想定業務の紹介（詳しくは7.2を参照）．
⑤ 燕市役所の想定業務への組織暗号適用案紹介
④で示した燕市役所の想定業務に対し，組織暗号の具体的な適用案を紹介．個人情報の送信者から個人情報を直接処理する担当者まで，暗号化された状態で配信できることを説明．詳しくは7.2を参照．
⑥ 組織暗号応用システムの操作実験
パブリッククラウドサービスAWS上に構築された操作実験環境を，借用した燕市役所のパソコンから燕市役所のネットワーク経由アクセス，簡単な組織暗号応用個人情報配信システムの操作実験を実施した．なお，操作は市役所の方々にお願いした．詳しくは7.3を参照．
⑦ 質疑応答

7.2　個人情報利用業務例と組織暗号適用案

事業創造大学院大学と燕市役所の協議により整理いただき，紹介いただいた以下の三つの想定業務に対し，具体的な組織暗号適用案（③のみ以下に図示）を提示，組織暗号がさまざまの業務へ適用可能である事を説明した．

① 新潟県後期高齢者医療広域連合から後期高齢者医療費等通知書が市役所の保険年金課へ送付され，保険年金課の課長は通知対象者の居住地に応じ，担当者へ転送する．
② 市役所の市民課は転入届等から住民異動情を作成し，国民保険，年金医療関係の情報が含まれていれば，年金保険課へ送信，年金保険課の責任者は国民保険，年金医療関係の情報の存在に応じ，それぞれの担当者へ住民異動情報を転送する．
③ 市役所の社会福祉課は，生活保護に関する申請などを受け付けると，住民異動情報を税務課，および児童福祉サービス対象の住民の場合は児童福祉課へも送信，それぞれの課の責任者は生活保護担当者へ転送する．

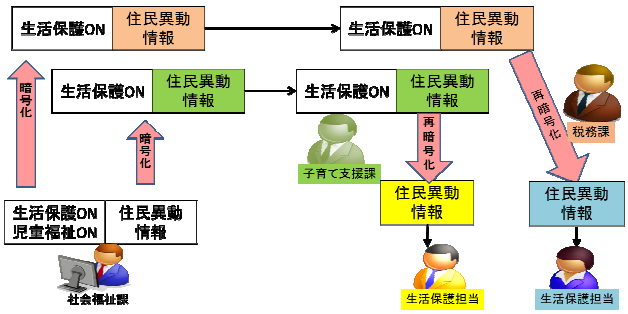

図4．想定業務③への組織暗号適用案

7.3　実験環境/実験シナリオ

大町市役所の場合と同様，AWS上に構築した実験環境を利用した．実験に使用するパソコン5台も借用し，燕市役所のネットワーク経由AWS上の実験環境をアクセスする形で操作実験を行った．

操作実験は，想定業務①をベースに，新潟県後期高齢者医療広域連合から後期高齢者医療費等通知書が燕市役所の保険年金課へ送付され，保険年金課の課長は通知対象者の居住地に応じ，担当者A，B，Cへ転送する，というシナリオで実施した．

7.4　実施状況・結果

当日は，燕市役所，新潟県庁の職員の方々，事業創造大学院大学の方々，報道関係者の方々など，約20名に参加いただいた．

ご挨拶をお願いした市役所幹部の方からは，個人情報の保護に留意しながらも利活用を進める必要があるとの認識を示され，安全な個人情報の利活用を支援する暗号技術への期待も表明された．出席者からは，組織暗号そのものや市役所の現在の業務実態との関係，組織暗号の秘密鍵の管理に関してなど多くの質問を受け，組織暗号への期待を感じられた．

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

8　組織暗号の活用展開に向けて

自治体では，現時点でも多くの業務で個人情報を取り扱われている．住民の個人情報はまさに機密情報であり，自治体ではその取扱いに慎重であるのは当然であるが，その結果，従来からの個人情報の紙ベースの取扱いを情報通信技術による取扱いへ移行することには，慎重な自治体も多いようであった．要因としては，情報機器やネットワーク整備の不十分さ，担当される方々の情報通信インフラの利用に関する習熟性の問題などもあるようだが，情報通信技術への不安・不信も根強いように感じられた．個人情報の情報通信技術を利用した取扱いへの変更は，安全性上のメリットも大きいはずだが，新聞や TV で報道される情報漏えい事件を目の当たりにみると，情報漏えいリスクへの懸念の方が強く，情報通信技術の利用を躊躇されているものと思われる．我々，情報通信技術の研究開発に携わる者としては，情報セキュリティ技術を含めた情報通信技術利用の安全性上のメリットや適切な利用に関する啓蒙活動を通じ，不安・不信を払拭する必要がある．

一方，個人情報の利活用場面は多様であり，新たな技術対策が望まれる場面も多い．我々，情報通信技術の研究開発に携わる者としては，個人情報の利活用が強く求められる時代の要請に応じ，さまざまの場面での個人情報の安全な利活用を支える新たな技術の研究開発に注力する必要がある．組織暗号は，そのような研究開発の成果の一つであり，個人情報の組織間での安全な通信を支援する新たな技術である．組織暗号の再暗号化機能により，受信代表者および受信組織内の個人情報配信に関わる中間管理者が，自らが個人情報の利用が必要ない場合は，個人情報を復号することなく，個人情報の内容を示すラベルを確認し，適切な個人情報利用者または下位の中間管理者へ個人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個人情報漏えいリスクを軽減させることが可能である．

個人情報の保護と利活用の両立を支援する新たな技術である組織暗号は，個人情報の利活用が活発化することが想定される自治体に向け，まさに紹介活動を開始したところである．今後，紹介活動を更に展開しながら，自治体業務に携わる職員の方々へ，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である．

また，組織暗号が自治体のシステムへ実際に導入されるには，様々の組織暗号応用システム構築に便利な組織暗号実装用モジュールの提供体制，組織暗号応用システム構築へのソフト開発事業者による支援体制，そして組織暗号が組み込まれた自治体向けパッケージの提供体制など，組織暗号実装支援環境の整備が必要である．今後，関係企業・団体の協力を得，実現に向け注力したい．

更には，自治体間あるいは自治体と連携する組織・団体間での組織暗号を利用した個人情報の安全な流通基盤の実現には，多くの自治体や関連組織・団体で共通的に組織暗号を採用いただく必要がある．そのためには，組織暗号の利用を関係省庁にご理解いただくと共に，所管のガイドライン等への折込みなどを通じご支援いただくなど，関係省庁のご協力に期待したい．

組織暗号はまさに実用化に向けた活動が緒に就いたばかりである．今後，個人情報の安全な利活用を支援する要素技術の一つとして，幅広く社会システムで活用されるよう，更なる研究開発と共に，実用化に向けた活動に注力する予定である．

謝辞

本研究は，独立行政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．

また，組織暗号実証実験は，大町市役所，箕輪町役場，燕市役所，中央コリドー高速通信実験プロジェクト推進協議会，NPO 法人中央コリドー情報通信研究所，NPO 法人新潟情報通信研究所の協力を得，実施したものである．
関係各位に感謝する．

参考文献

[1] 辻井重男，　五太子征史: 相補型 STS-MPKC 方式による組織対応型公開鍵暗号の提案，　SCIS2011(2011 年暗号と情報セキュリティシンポジウム).
[2]辻井重男，　山口浩，只木孝太郎，五太子征史，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，電子情報通信学会技術研究報告. EMM，マルチメディア情報ハイディング・エンリッチメント 113(138) (20130711).
[3]辻井重男，　山口浩，　才所敏明，　五太子征史，　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，　SCIS2014(2014 年暗号と情報セキュリティシンポジウム). 著者名，“論文タイトル，” 論文誌名，ページなど
[4] A. Cilardo, L. Coppolino, N. Mazzocca, L. Romano, “Elliptic curve cryptography engineering,” Proceedings of the IEEE 94(2) (2006) 395-406.
[5] 辻井重男編: 暗号理論と楕円曲線，　森北出版株式会社 (2008).
[6] 社会保障・税番号制度（マイナンバー）
http://www.cas.go.jp/jp/seisaku/bangoseido/　.
[7] 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（Computer Security Symposium 2014）.