情報処理学会論文誌 Vol.56 No.9 1868–1876 (Sep. 2015)

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

才所 敏明[1,a)] 近藤 健[1] 庄司 陽彦[1] 五太子 政史[1] 辻井 重男[1]

受付日 2014年11月26日, 採録日 2015年6月5日

概要：本論文では，中央大学・研究開発機構で研究開発を進めている組織暗号について，暗号方式，実装状況，および普及・啓蒙のために展開中の実証実験について報告する．組織暗号は，主に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た暗号方式であり，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転送でき，復号者への安全な機密情報の配信が可能である．わが国では，マイナンバーの導入や医療・介護サービスの提供体制の改革が決まり，国民の生活・生命を守るため，組織の枠を超えた個人情報の利活用が求められる時代に入りつつある．組織暗号は，組織の枠を超えた個人情報の利活用と保護の両立を目指し，研究開発および実用化を推進している暗号方式である．本論文では，受信組織における人事的役割分担と楕円エルガマル暗号方式の 2 つの項を対応させた点が特徴である方式を提案し，それにより暗号文の受信代表者が復号せずにその暗号情報の担当者だけが復号できる暗号文へ変換（再暗号化）できることを示し，次に PC 上で実装した組織暗号が実用上問題のない処理性能であることを，最後に，NPO 法人中央コリドー情報通信研究所などと協力して実施した，長野県大町市役所，同箕輪町役場，新潟県燕市役所での，わが国初となる実証実験の内容・結果を報告する．

キーワード：組織暗号，組織間通信，個人情報，マイナンバー，自治体，実証実験

New Cryptosystems for Social Organizations and Practical Use of It in Society —Promoting the Personal Data Utilization Securely

Toshiaki Saisho[1,a)] Takeshi Kondo[1] Takahiko Shouji[1]
Masahito Gotaishi[1] Shigeo Tsujii[1]

Received: November 26, 2014, Accepted: June 5, 2015

Abstract: 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. Firstly, we propose the system of our cryptosystems that utilize the correspondence between organizational allotment of roles within the receiving organization and the features of Elliptical ElGamal cryptosystem that is composed by 2 factors, and show that our re-encryption process (changing of key for decoding the cryptogram) can be carried out so that only newly specified receiver can decode the new cryptogram, without any decoding in the re-encryption process. Secondly, we report the performance data of our software implementation on the PC and show that it is good performance satisfactory for practical use. Lastly, we report the results of the first operational experiments in Japan that carried out in local government of Omachi city, Minowa town and Tsubame city.

Keywords: organizational-cryptosystem, Elliptical-ElGamal, inter-organizational-communication, information-protection, field-experiment

[1] 中央大学研究開発機構
Research & Development Initiative, Chuo University, Bunkyo, Tokyo 112–8551, Japan
[a)] toshiaki.saisho@advanced-it.co.jp

1. はじめに

わが国では，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，政省令など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 [1]．また，医療・介護の総合的なサービス体制においては，患者・利用者の視点に立ってサービスが提供され，医療・介護サービスに関わる様々の専門組織や専門家の間での患者・利用者の個人情報の相互利用が促進されるものと期待されている [2]．

中央大学・研究開発機構では，このような個人情報の利活用が求められる時代に対応すべく，個人情報の保護に配慮しつつ組織間での個人情報の利活用を推進可能な，新たな暗号方式「組織暗号」の研究開発を進めている．

ここで，組織暗号という用語について説明しておく．組織間の通信においては，個人情報や医療情報などの機密情報を真に必要なものに限定して送信する方式 [3] や，属性暗号・関数暗号，秘匿検索，暗号化状態処理，再暗号化など，多様な暗号方式が必要となる．我々は，組織間通信に必要な暗号方式を総称して，暗号開発者の視点ではなく，暗号利用者の社会的視点から，組織暗号と呼んでいる [4], [5]．なお，本論文で報告する組織暗号は，再暗号化方式である．

組織内の情報漏えいを防ぐためには，情報管理における役割分担を明確に定め，1 人の管理者が知りうる情報を可能な限り限定することが必要である．本論文では，受信代表者（たとえば総務部長）とシステム管理者との役割分担を明確化し，その役割分担を，楕円エルガマル暗号文（あるいは Cramer-Shoup 暗号文）の各項に対応させ，代表者は，平文を含む項を受信することなく，暗号文のラベル（平文）のみから復号担当者を定め，自身の秘密鍵を用いて，再暗号化鍵を作成して，システム管理サーバに返し，管理サーバから，担当者へ再暗号化された暗号文を送信する．この場合，システム管理者は，代表者の秘密鍵を持たないので，平文に復号することは不可能である．

上記のように，人事的役割分担と，暗号文の複数の項とを対応させた再暗号化方式はこれまで報告されていない．

本論文では，安全性基準として，既知平文攻撃に対する識別不可能性（IND-CPA），および，選択暗号文攻撃に対する識別不可能性（IND-CCA2）を利用環境（暗号技術以外のアクセス制御技術導入状況など）に応じて使い分けることを前提としている．IND-CPA に対しては，楕円エルガマル暗号を，IND-CCA2 に対しては，Cramer-Shoup 暗号を利用することとする．自治体などにおける実証実験は，実用環境を考慮し，楕円エルガマル暗号方式を用いて行った．

以下，まず組織間通信および組織暗号の特徴を紹介する．次に，現在開発中の楕円エルガマル暗号ベースの組織暗号の，具体的構成例および処理手順を紹介，組織間通信の安全性を高めるための機能が実現されていることを示す．続いて，楕円エルガマル暗号ベースの組織暗号の試験的実装結果を報告，組織暗号が実用上問題ない処理性能で実装可能であることを示す．さらに，先進的自治体で実施したわが国初となる組織暗号の実証実験結果を報告し，自治体業務での個人情報漏えい防止に組織暗号の応用が有効であることを示す．最後に，個人情報の利活用が求められるわが国における組織暗号の広範な活用の可能性および組織暗号の普及のために必要な施策・課題について，報告する．

2. 組織間通信と組織暗号

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を配信）やデータ利用者（復号し機密情報を利用）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，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な脅威に晒され，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な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いえる [6], [7], [8].

なお，研究開発や実用化の試みが数多く展開されている属性暗号，関数暗号も，機密情報を提供する送信者が受信者個人を特定することなく，受信者の属性や条件などを指定することで機密情報の復号を可能とする受信者を柔軟に指定することが可能である．しかし，組織暗号が目指す受信組織内での臨機応変な配信への対応は難しく，従来の暗号方式と同様，送信側主導の暗号方式といえる．

組織暗号は，組織間通信の特徴である，受信側での臨機応変な配信への対応とともに，配信プロセスでの情報漏えいリスクを軽減させるために，機密情報の暗号化状態での再配信を可能とする暗号方式である．

3. 組織暗号方式

組織暗号方式は，多変数公開鍵暗号，楕円エルガマル暗号など，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エルガマル暗号ベースの組織暗号方式について紹介する．

まず 3.1，3.2 節で，IND-CPA 安全性に対応する楕円エルガマル暗号，および，楕円エルガマル暗号の機能を利用した再暗号化（鍵の付替え）方式を説明し，3.3 節で，IND-CCA2 安全性に対応する Cramer-Shoup 暗号の適用について説明する．

本論文では，自治体などのアクセス制御環境などを考慮し，楕円エルガマル暗号の適用について詳説する．

3.1 楕円エルガマル暗号—IND-CPA 対応

エルガマル暗号 [9] は離散対数計算の困難性，すなわ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エルガマル暗号である．以下，楕円エルガマル暗号の暗号化，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：秘密鍵とベースポイントの積 $a*P$ $(=A)$

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．$C_{\mathrm{A1}} = M + r*A$
3 乱数にベースポイント P を掛けて C_{A2} $(= r*P)$ を得る．
4 $C_{\mathrm{A}} = (C_{\mathrm{A1}}, C_{\mathrm{A2}})$ 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：

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

3.2 再暗号化（鍵の付替え）方式とその安全性

上記のような楕円エルガマル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，さら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．

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

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，$C_{\mathrm{B2}} = r_2 * P$ 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：

$$X_{\mathrm{AB}} = a * C_{\mathrm{A2}} - r_2 * B$$

（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：

$$\begin{aligned} C_{\mathrm{B1}} &= C_{\mathrm{A1}} - X_{\mathrm{AB}} \\ &(= M + r_1 * a * P - a * r_1 * P + r_2 * B \\ &\ = M + r_2 * B) \end{aligned}$$

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いっさい生成されないため平文が直接漏えいするリスクはないが，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．

そこで，A の公開鍵で暗号化された暗号文 C_{A} の管理および再暗号化を支援する新たなシステム管理者 S を導入し，A および S の一方の独断での復号を不可能とし，かつ

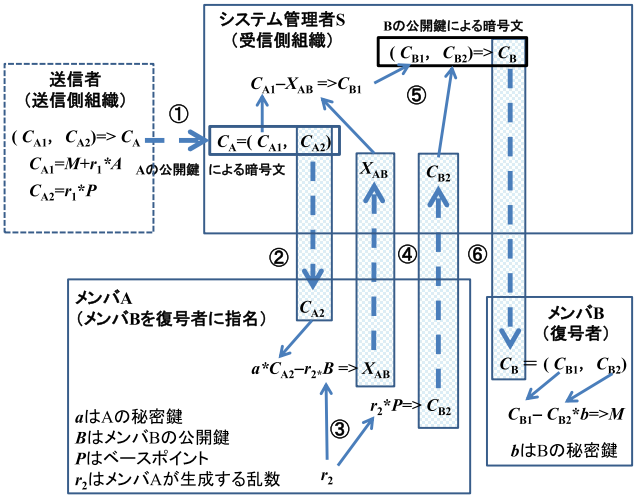

図 1 改良版再暗号化プロセス
Fig. 1 Revised re-encryption process.

A および S の一方のシステムからの情報漏えいによる復号のリスクを回避できる改良した再暗号化方式（図 1）を以下に説明する．

① 送信側組織の送信者は，平文 M を，受信組織の代表者 A の公開鍵で暗号化して送信するが，A はそれを直接受け取らず，システム管理者 S が受け取るように受信システムを構成しておく．S は，送信者から送られてきた A の公開鍵で暗号化された暗号文 $C_{\mathrm{A}} = (C_{\mathrm{A1}}, C_{\mathrm{A2}})$ を受信し，管理する．

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

② S は A に対し，管理する $C_{\mathrm{A}} = (C_{\mathrm{A1}}, C_{\mathrm{A2}})$ のうち，C_{A2} のみを送信する．C_{A2} には平文情報は含まないことに注意．

③ A は，受信した C_{A2}，自ら生成した乱数 r_2，事前に保有している B の公開鍵 B およびベースポイント P，さらに自身の秘密鍵 a を使用し，変換用鍵 X_{AB} および C_{B2} を次の式で生成する．

$$X_{\mathrm{AB}} = a * C_{\mathrm{A2}} - r_2 * B$$
$$C_{\mathrm{B2}} = r_2 * P$$

④ A は，変換用鍵 X_{AB} および C_{B2} を，S へ送信する．

⑤ S は，受信した X_{AB} および C_{B2} を使用し，B の秘密鍵で暗号化された暗号文 C_{B} を生成する．

$$C_{\mathrm{B1}} = C_{\mathrm{A1}} - X_{\mathrm{AB}}$$
$$(= M + r_1 * a * P - a * r_1 * P + r_2 * B$$
$$= M + r_2 * B)$$
$$C_{\mathrm{B}} = (C_{\mathrm{B1}}, C_{\mathrm{B2}})$$

⑥ S は，A の指名に従い，B へ復号に必要な C_{B} を送信する．

以上の手順により，S が管理していた A の公開鍵で暗号化された暗号文 C_{A} は，平文を生成することなく，B の公開鍵で暗号化された暗号文 C_{B} へ，変換されることになる．

S は A の公開鍵で暗号化された暗号文を保有するがそれを復号できる秘密鍵を保有せず，一方，A は秘密鍵を保有するが暗号文は保有しないため，A，S のそれぞれが単独で平文を入手することはできず，また S および A のシステムの一方が不正アクセスやウイルス感染などの攻撃を受けデータ漏えいが発生したとしても，平文が漏えいすることはない．また，暗号文を保有する S とその暗号文を復号できる秘密鍵を保有する A の結託を除けば，他の結託が発生したとしても，平文が漏えいすることはない．本方式は，楕円エルガマル暗号の特徴である「暗号文が 2 項に分かれており，そのうちの 1 つの項には平文の情報が含まれていないこと」を利用した方式である．

なお，一般に「代理人再暗号化方式」が満たすべき性質 [10] の中で，組織暗号として満たすべきである性質は，非対話性，鍵サイズ不変性，秘密鍵秘匿性，再暗号化鍵偽造不可能性であるが，本論文で紹介した改良した再暗号化方式はすべて満たしている．

3.3 Cramer-Shoup 暗号—IND-CCA2 対応

安全性基準を選択暗号文攻撃に対する識別不可能性（IND-CCA2）とする場合も，楕円エルガマル暗号ベースの場合と同様に，人事的役割分担と Cramer-Shoup 暗号文の 4 つの項を対応させることができる．紙面の都合で，文献 [11] 132 頁の記号を引用して説明する．本文献において暗号文は，C：(a,â,c,d) と表されている．本方式では，サーバは，上記 4 項のうち，c（平文が暗号化された項）を除いて，a,â,d を代表者に渡す．「暗号文が正しく構成されているか」などに関する検証（132 頁の Dec:D1,D2,D3 を参照）は，c を必要とするので，サーバ管理者が行う．プロトコル検証 D4 は，代表者の秘密鍵を必要とするので，代表者がサーバから D3 の結果（v’）を受け取って行う．v’ は，暗号文 c などのハッシュ値であるので，c 自体が代表者 A にわたることはない．上記の検証が終了した後の代表者 A の行為は，楕円エルガマル暗号の場合と同様である．

4. 組織暗号の実装評価

組織暗号方式の早期実用化を目指し，方式の研究開発と並行しソフトウェア実装を鋭意推進中であり，すでに多変数公開鍵暗号を利用した組織暗号および楕円エルガマル暗号を利用した組織暗号の実装は完了している．ここでは，前章で説明した楕円エルガマル暗号を利用した組織暗号，シンプルな鍵の付替え（再暗号化）方式を使用した組織暗号の実装について報告する．

まず 4.1 節で，実装内容，性能評価結果を報告，その結果に基づき，実装した楕円エルガマル暗号方式を利用した

組織暗号の実用性に関する考察を 4.2 節で述べる．

4.1 実装内容および性能評価

楕円エルガマル暗号を利用した組織暗号の実装に使用した開発言語，ライブラリ，楕円曲線パラメータは以下のとおり．

開発言語：Microsoft Visual C# 2008

暗号ライブラリ：The Bouncy Castle Cryptographic C# API（Release 1.7，7th April 2011）

楕円曲線　推奨パラメータ：secp224k1[x2]

今回の実装は，あくまでもアルゴリズムの動作検証のための実装であり，処理性能については考慮していないが，実証実験などに使用可能かどうかの確認のため，性能評価を実施した．性能測定には，以下の仕様の PC を使用した．

OS：Wndows7 Professional（32 bit）

CPU：Intel Core i3-2100 3.1 GHz　メモリ：4 GB

処理性能は，暗号化，再暗号化（鍵の付替え），復号の 3 つの機能に対し，3 種のデータサイズについて測定した．その結果（単位：ms）を**表 1** に示す．

なお，代表的な公開鍵暗号 RSA との比較のため，暗号化，復号の機能について，同一の PC で処理性能を測定した．結果（単位：ms）を**表 2** に示す．

以上の結果から，組織暗号の利用形態，機密情報の送信者とデータ利用者の間に，中間管理者などのデータ転送者の存在を想定した利用モデルを対象に，機密情報配信プロセス全体での暗号化/再暗号化/復号の総処理時間（単位：ms）を試算したのが**表 3** である．なお，RSA 暗号の場合の再暗号化は，いったん受信者の秘密鍵で復号し，その後，送信相手の公開鍵で暗号化，という処理を前提に試算している．

結果として，組織暗号による機密情報配信プロセス全体での暗号化/再暗号化/復号の総処理時間は，RSA 暗号の利用に比べ，大きなサイズのデータについてはそう差はないが，小さなサイズのデータについては 4 倍から 5 倍の総処理時間がかかる，という結果であった．

次に，実用性の観点から，大量の機密情報の配信に使用されるハイブリッド暗号方式を適用した場合の，機密情報配信プロセス全体での暗号化/再暗号化/復号の総処理時間（単位：ms）を試算したのが**表 4** である．ハイブリッド暗号方式は「配信したい機密情報の暗号化には共通鍵暗号を使用し，その暗号化に使用した秘密鍵の配信には公開鍵暗号を使用する方式」であるが，今回は共通鍵暗号として AES（鍵長は 128 ビット）を使用するものとし，公開鍵暗号としては組織暗号（楕円エルガマル暗号）または RSA 暗号を使用するものとして試算している．

以上の結果から，ハイブリッド暗号方式を利用した場合，公開鍵暗号として組織暗号を利用した機密情報配信プロセス全体での暗号化/再暗号化/復号の総処理時間は，RSA 暗号を利用した場合に比べ，転送回数にかかわらず，データサイズに応じ 6 倍～13 倍程度長くかかることが分かった．

表 1 組織暗号の主要機能の性能評価
Table 1 Performance data of organizational cryptography.

機能	データサイズ		
	1 k B	10 k B	1MB
暗号化	62	223	17829
鍵の付替え	132	496	40124
復号	50	92	4656

表 2 RSA 暗号の主要機能の性能評価
Table 2 Performance data of RSA cryptography.

機能	データサイズ		
	1 k B	10 k B	1MB
暗号化	0.7	7	757
復号	29	300	30225

表 3 組織内機密情報配信プロセスでの性能比較
Table 3 Performance comparison of secure transfer process within organizations.

転送回数	アルゴリズム	データサイズ		
		1 k B	10 k B	1MB
1	楕円 ElGamal	244.0	811.0	62609.0
	RSA	59.4	614.0	61964.0
2	楕円 ElGamal	376.0	1307.0	102733.0
	RSA	89.1	921.0	92946.0
5	楕円 ElGamal	640.0	2299.0	182981.0
	RSA	178.2	1842.0	185892.0
10	楕円 ElGamal	1432.0	5275.0	423725.0
	RSA	326.7	3377.0	340802.0

表 4 ハイブリッド暗号方式を利用した場合の比較
Table 4 Performance Comparison of secure transfer process within organizations using hybrid encryption.

転送回数	アルゴリズム	データサイズ		
		1 k B	10 k B	1MB
1	楕円 ElGamal	188.02	188.19	205
	RSA	14.42	14.59	31.4
2	楕円 ElGamal	285.02	285.19	302
	RSA	21.62	21.79	38.6
5	楕円 ElGamal	576.02	576.19	593
	RSA	43.22	43.39	60.2
10	楕円 ElGamal	1061.02	1061.19	1078
	RSA	79.22	79.39	96.2

4.2 実用性に関する考察

前節で示した性能測定結果から，アルゴリズムの動作検証のために実装した楕円エルガマル暗号を利用した組織暗号は，RSA 暗号を利用した場合に比べ，かなり処理性能が悪いことが分かった．

しかし，この性能測定結果は，高速化の工夫を施さなかった今回の試験的実装であっても，組織暗号による機密情報配信プロセス全体での暗号化/再暗号化/復号の総処理時間は，1 回の転送の場合の 0.2 ms，10 回の転送がなされたとしても 1 s 程度で，実用上まったく問題にならない総処理時間（性能）であることを示しており，楕円エルガマル暗号を利用した組織暗号の実用性，現実の社会システムへの実装には，性能面ではまったく不安がないものと考えている．

一方，楕円エルガマル暗号を利用した組織暗号では，暗号化データのサイズは平文データのサイズの 2 倍となる．このような，データサイズの倍増が問題となる場合は，ハイブリッド方式により組織暗号を適用すれば回避でき，暗号化データサイズ倍増の問題も，楕円エルガマル暗号を利用した組織暗号の実用化，現実の社会システムへの実装にはまったく支障がないものと考えている．

5. 実証実験

組織暗号の実用的な性能での実装が実現したため，現実の社会システムへの組織暗号実装を実現すべく，組織暗号の有用性・有効性の紹介活動を展開した．まずは，すでに個人情報を取り扱う多くの業務をかかえており，またマイナンバーの利用が軌道に乗るにつれ組織間の個人情報の授受が急増すると思われる自治体を対象とし，組織暗号の適切な応用により個人情報漏えいリスクを軽減できることを実感いただけるよう，実証実験を企画，3 カ所の自治体の協力を得，実施した．

本章では，5.1 節で実証実験の目的・内容を紹介し，5.2 節で実証実験のために開発した組織暗号応用機密情報配信実験システムの紹介，その後，5.3 節で長野県大町市役所で行った実証実験，5.4 節で長野県箕輪町役場で行った実証実験，5.5 節で新潟県燕市役所で行った実証実験について報告する．最後に，実証実験についての考察を 5.6 節で述べる．

なお，今回の実証実験に協力をいただいた自治体は，自治体の情報化の支援活動を長年展開し，多くの自治体のキーマンとのチャネルを有する NPO 法人中央コリドー情報通信研究所より推奨していただいた自治体である．

5.1 実証実験の目的・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への組織暗号の実装・組込みの検討に着手いただくことを目的として，実証実験の内容を策定した．

(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) 自治体業務における組織暗号適用案の紹介
　実証実験を実施する自治体での個人情報を取り扱う業務への組織暗号の具体的な適用案の紹介
(4) 機密情報配信実験システムの操作紹介
　送信代表者，受信代表者，担当者から構成される組織暗号応用機密情報配信実験システムを使用した，暗号化/再暗号化（鍵の付替え）/復号の操作の紹介
(5) 質疑応答
　組織暗号の有用性・有効性に関する質疑対応

5.2 組織暗号応用機密情報配信実験システム

組織暗号応用機密情報配信実験システムは，前章で説明した楕円エルガマル暗号を利用した組織暗号の実装成果を利用し作成した．

機密情報配信実験システムの構成としては，組織暗号の主要機能である暗号化/再暗号化/復号が含まれる必要があり，具体的には**図 2** のような構成を目指した．送信側代表者が，機密情報を受信側代表者だけが復号できるよう暗号化し，かつラベルを付加し送信，受信側代表者はラベルを確認し担当者を決定，自分向けに暗号化された機密情報を復号することなく，該当する担当者のみが復号できるよう，暗号化された機密情報を再暗号化（鍵を付替え）し該当する担当者へ送信，そして該当する担当者が暗号化された機密情報を復号，という一連の操作が可能な構成となっている．

しかし，自治体内のネットワークに接続されている PC に，暗号化/再暗号化/復号などの組織暗号利用のためのソフトウェアのインストールは，各自治体のセキュリティポリシ上，許可されない可能性が高いため，機密情報配信実

図 2 実験用配信システム構成
Fig. 2 Information distribution system configuration for the experiment.

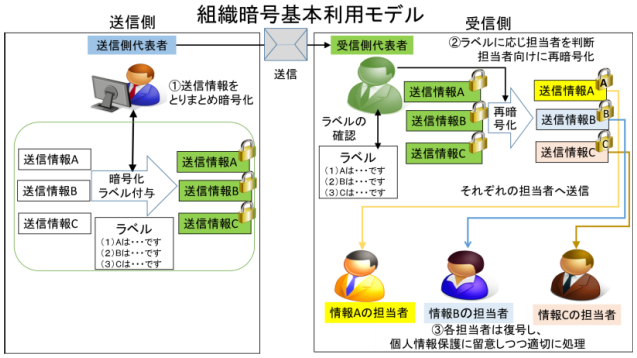

図 3　組織暗号基本利用モデル

Fig. 3　Basic use model of cryptosystems for social organizations.

験システムとしては，図 2 の情報の流れをクラウドサービス AWS（Amazon Web Services）上で実現，各操作者は自治体のネットワークに接続された 5 台の PC からブラウザ経由で操作することとした．

組織暗号操作実験では，組織暗号基本利用モデル（**図 3**）で示した機密情報の流れに沿った操作を，機密情報配信実験システム上で実施した．

① 送信側代表者が送信情報をとりまとめ，受信側代表者だけが復号できるよう暗号化，送信情報の内容が分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．

5.3　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で実施した．実施内容は 5.1 節のとおり．

大町市役所内の個人情報の配信が必要となる 3 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，そのうえで，組織暗号操作実験環境を利用し，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．なお，操作は，大町市役所および北アルプス広域連合の職員の方々にお願いした．北アルプス広域連合とは，大町市，池田町，松川村，白馬村，小谷村の 5 市町村から構成される広域行政を担う組織であり，行政サービスのための情報システムも大町市役所にある情報センターで運用・管理されている．

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．

5.4　箕輪町役場での実証実験

2014 年 11 月 7 日，5.1 節と同一内容で，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 3 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，そのうえで，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．なお，操作は箕輪町役場の職員の方々にお願いした．

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．自治体の様々な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．

5.5　燕市役所での実証実験

2014 年 11 月 21 日，新潟県の燕市役所で組織暗号の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 2 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，そのうえで，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．なお，操作は燕市役所の職員の方々にお願いした．

当日は，燕市役所，新潟県庁，本実証実験にご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．自治体でも個人情報を保護しつつも利活用をさら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．

なお，本実証実験については，電波タイムズ（2014 年 11

月 28 日の 1 面）で紹介された．

5.6 まとめ

実証実験では，個人情報を取り扱う各自治体の具体的業務を例に取り上げ組織暗号の適用方法を説明，送信者から担当者まで，個人情報が安全に配信されることを示した．このような自治体職員の方々の身近な業務での組織暗号の具体的適用方法の説明は，組織暗号の有用性・有効性の理解に大変効果的であった．

また，実証実験では，自治体職員の方々に操作をお願いしたことは，組織暗号応用システムを身近に感じていただき，また操作の容易さや応答性能の実用性を実感いただくのに大変効果的であった．

もちろん，組織暗号が自治体で幅広く使われるための課題も明確になった．

自治体での個人情報を取り扱う業務では，紙ベースで個人情報を配布している場合も多かった．原因は，第 1 に個人情報のネットワーク経由の配信の安全性に対する不安をぬぐいきれず，情報技術の利用にリスクを感じているという方々が多い，さらに個人情報を利用し実際に業務を担当する方々が自治体庁舎外で勤務する場合パソコンを利用できる環境にない，また，個人情報を扱う民生委員，福祉介護関係者などがパソコンを保有していない，パソコンを使いこなせない，などが考えられる．対策としては，組織暗号をはじめとする情報セキュリティ技術の適切な応用とシステム運用時の適切なマネジメントにより，紙ベースの個人情報配信に比べはるかに安全で，しかも効率的であることを，丁寧にかつ精力的に説明を行っていくこと，が必要であることを痛感した．

今回の実証実験では，個人情報の配信プロセスの安全性に的を絞った説明であったが，自治体での個人情報の管理・利用・配信は多様であり，様々な場面での個人情報の保護技術への期待も表明された．今後，組織暗号の様々な場面での応用可能性を検討するとともに，既存の情報セキュリティ技術と組み合わせた総合的な対策の検討・提案，が必要であろう．

また，組織暗号は大学の研究開発の成果であるが，自治体としては実務へ適用する場合のサポートへの期待を表明された自治体もあった．今後，自治体向けに SI サービスを展開されるベンダへの組織暗号組込み支援やワークフローなどの市販パッケージベンダへの組織暗号組込み支援などにも，注力する必要があろう．

6. おわりに

わが国では，個人情報保護法の成立以来，個人情報の漏えい，あるいはそう判断されることを恐れ，個人情報の利活用に慎重になりすぎてきたきらいがある．しかし，番号関連四法の成立（マイナンバーの導入）や医療介護総合確保推進法の成立（医療・介護サービスの提供体制の改革）などから，行政を効率化し国民の利便性を高め，公平・公正な社会の実現や，国民の生活・生命を守るための活動のため，個人情報の利活用が促進されることになる．

もちろん，個人情報の保護をないがしろにすることはできない．中央大学・研究開発機構では，個人情報の保護に配慮しつつ，個人情報の利活用が可能な技術の研究開発を推進しており，今回報告した組織暗号もその 1 つの成果である．

楕円エルガマル暗号を利用した組織暗号の特徴的機能は，受信者の秘密鍵で復号できるよう暗号化された機密情報を，その受信者は別の新たな受信者の秘密鍵だけ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）できること，にある．この機能により，受信者の臨機応変な判断により新たな受信者を選定でき，かつ機密情報を復号することなく再暗号化でき，新たな受信者へ，さらには組織内を転々と最終受信者まで，安全に配信可能となる．組織暗号を，受信側主導の暗号方式と主張するのは，このような特徴にある．

組織暗号のこの特徴的機能を活かすことにより，マイナンバー導入により個人情報の授受や利活用の機会の増大が想定される自治体や，医療・介護サービスの提供体制の改革により同様に個人情報の授受や利活用が求められる医療・介護機関での，個人情報のより安全な配信・利活用が可能となる．

中央大学・研究開発機構では，組織暗号の活用により，個人情報の保護に留意しつつも個人情報の積極的な利活用が可能な社会システムの実現を目指し，国民の生活・生命を守るサービスの向上や税負担の軽減化・公平化に貢献するとともに，高齢化先進国，災害多発国であることを生かしたわが国の産業の発展に資する所存である．

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．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] 社会保障・税番号制度（マイナンバー），入手先 ⟨http://www.cas.go.jp/jp/seisaku/bangoseido/⟩.
[2] 地域における医療及び介護の総合的な確保を推進するための関係法律の整備等に関する法律案の概要，入手先 ⟨http://www.mhlw.go.jp/topics/bukyoku/soumu/houritu/dl/186-06.pdf⟩.
[3] 只木孝太郎，土居範久．辻井重男：プライバシー保護条件付き情報開示，電子情報通信学会和文論文誌 A，Vol.J96-A，No.11，pp.735–744 (2013).

[4] 辻井重男：放送・通信の 4 類型と情報セキュリティ概念の高度化—組織通信・組織暗号の普及に向けて，*SCIS2014* (2014).
[5] 辻井重男，吉田正彦，柴崎哲也，小林正幸：放送・通信の 4 類型と情報セキュリティ概念の高度化—第 2 報—組織通信と公共情報コモンズ（L アラート），*SCIS2015* (2015).
[6] 辻井重男，五太子政史：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).
[7] 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，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，Vol.113, No.138 (2013).
[8] 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，*SCIS2014* (2014).
[9] Cilardo, A., Coppolino, L., Mazzocca, N. and Romano, L.: Elliptic curve cryptography engineering, *Proc. IEEE*, Vol.94, No.2, pp.395–406 (2006).
[10] Ateniese, G., Fu, K., Green, M. and Hohenberger, S.: Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage, *Proc. 12th Annual Network and Distributed System Security Symposium*, pp.29–44 (2005).
[11] 日本応用数理学会（監修），森山大輔，西巻　陵，岡本龍明（著）：公開鍵暗号の数理，共立出版 (2011).

才所 敏明 （正会員）

1947 年生．1970 年東京大学工学部計数工学科卒業．同年（株）東芝入社，企業情報活動基盤の企画・構築および情報セキュリティ技術の研究企画・開発に従事，2007 年（株）IT 企画社長，2013 年より中央大学・研究開発機構・研究員．電子情報通信学会，IEEE，ACM 各会員．

近藤 健

1940 年生．1962 年京都大学工学部電気工学科卒業．同年日本電気（株）入社, 電話交換システム開発に従事, 2002 年中央コリドー高速通信実験プロジェクト推進協議会入会．自治体を中心とする ICT 利活用研究に従事，2014 年より中央大学・研究開発機構・研究員．

庄司 陽彦 （正会員）

1979 年生．2001 年工学院大学専門学校卒業．同年（株）ワイ・デー・ケー入社，組込みソフトウェア，セキュリティ技術の開発業務に従事，2010 年情報セキュリティ大学院大学卒業，2014 年より中央大学研究開発機構・研究員．

五太子 政史

1959 年生．1984 年東京大学農学部農芸化学科卒業．2011 年中央大学大学院理工学研究科博士後期課程修了．セキュリティソフトの販売および技術サポートに従事後，中央大学研究開発機構で情報セキュリティ・ネットワークセキュリティの教育，暗号技術の研究に従事．現在，中央大学研究開発機構准教授．

辻井 重男

1933 年生．1958 年東京工業大学工学部電気工学科卒業．同年日本電気（株）入社．山梨大学助教授．東京工業大学教授．中央大学教授を経て，2004 年情報セキュリティ大学院大学長．1998 年一般財団法人マルチメディア振興センター理事長．東京工業大学名誉教授．中央大学研究開発機構教授．工学博士．電子情報通信学会功績賞，NHK 放送文化賞，内閣官房「情報セキュリティの日」功労者表彰，2009 年春瑞宝中綬章，2014 年 C&C 賞等受賞．電子情報通信学会会長，総務省電波監理審議会会長，日本学術会議会員等歴任．日本ペンクラブ会員．