SCIS 2016 2016 Symposium on
Cryptography and Information Security
Kumamoto, Japan, Jan. 19- 22, 2016
The Institute of Electronics,
Information and Communication Engineers

自治体・医療機関における組織暗号の実証実験,
Demonstration Experiments of Organizational Cryptosystems in Local governments and Medical Organizations

才所 敏明* 近藤 健* 庄司 陽彦*
Toshiaki Saisho Takeshi Kondo Takahiko Shouji
五太子 政史* 辻井 重男*
Masahito Gotaishi Shigeo Tsujii

あらまし 中央大学研究開発機構では，組織間での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，暗号化をする送信者が他の組織に属する受信者（復号者）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開発中の暗号方式である．また，研究開発と並行し，組織暗号の有用性・有効性を社会に幅広く認知いただき活用を検討いただくためのプロモーション活動を展開中である．本稿では，楕円エルガマル暗号ベースの組織暗号，組織暗号を応用した機密情報配信システムの構成例を紹介すると共に，個人情報を取り扱う業務が多い自治体および医療機関への紹介活動や実証実験の展開状況およびその結果について報告する．

キーワード 組織暗号，組織間通信，個人情報保護，マイナンバー，自治体，地域包括ケア体制，医療・介護機関，暗号実装，実証実験

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，本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る．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，組織間通信が活発化することになる．

また，我が国では 2014 年の医療介護総合確保推進法の成立により医療・介護サービスの提供体制の改革が決まり，現在，地域における医療・介護の総合的な確保を図る動きが各地で活発化しつつある．このような医療・介護の総合的なサービス体制においては，医療・介護サービスに関わる様々の専門組織の間での患者の個人情報の相互利用が促進されることになり，組織間通信が活発化することになる．

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，医療・介護機関，企業等の各組織では，個人情報は慎重が上にも慎重に取り扱われ，慎重すぎるが故に，個人情報の利活用が進まない弊害も顕在化していたが，番号関連四法や医療介護総合確保推進法の成立により，国民の生活・生命を守るため，個人情報の組織の枠を超えた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，このような組織間での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．

現在，多変数公開鍵暗号に基づく組織暗号と楕円エルガマル暗号に基づく組織暗号の研究開発を推進しているが，本稿では楕円エルガマル暗号ベースの組織暗号にて展開している社会的実装に向けた活動を中心に報告する．

2　楕円エルガマル暗号ベースの組織暗号

組織間通信を利用し個人情報等の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技術の利用が求められる．

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介在者（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，転送の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．

以下，楕円エルガマル暗号ベースの組織暗号による，送信者によるメンバＡのための暗号化，メンバＡによるメンバＢのための再暗号化（転送のための鍵の付替え），メンバＢによる復号，の方法を示す．

［定義］

平文機密情報：$\boldsymbol{M}$（Ａを経由しＢへ転送）

公開設定：E/F_q: 楕円曲線，$E(F_q)$: 素位数巡回群，

$\boldsymbol{P}$: 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 $a*\boldsymbol{P}(=\boldsymbol{A})$

Ｂの秘密鍵：乱数 b

Ｂの公開鍵：$b*\boldsymbol{P}(=\boldsymbol{B})$

［送信者によるメンバＡのための暗号化］

①　乱数 r_1 の生成

②　$\boldsymbol{M}_1'=\boldsymbol{M}+r_1*\boldsymbol{A}$

③　$\boldsymbol{M}_2'=r_1*\boldsymbol{P}$

$\boldsymbol{M}'=(\boldsymbol{M}_1',\ \boldsymbol{M}_2')$が平文機密情報 $\boldsymbol{M}$ 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

［メンバＡによるメンバＢのための再暗号化］

①　乱数 r_2 の生成

②　$\boldsymbol{M}_2''=r_2*\boldsymbol{P}$

③　変換用鍵 $\boldsymbol{X}_{AB}$ の計算　$\boldsymbol{X}_{AB}=a*\boldsymbol{M}_2'-r_2*\boldsymbol{B}$

④　$\boldsymbol{M}_1''=\boldsymbol{M}_1'-\boldsymbol{X}_{AB}$

$\boldsymbol{M}''=(\boldsymbol{M}_1'',\ \boldsymbol{M}_2'')$が平文機密情報 $\boldsymbol{M}$ 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

［メンバＢによる復号］

①　$\boldsymbol{M}=\boldsymbol{M}_1''-b*\boldsymbol{M}_2''$

3　組織暗号を応用した機密情報配信システム

3.1　多様な組織構造への対応

暗号化された機密情報を受け取る受信組織では，受信組織の組織構造に応じた段階的な配信（転送）により受信者（復号者）へ暗号化された機密情報が到達することになる．一般に組織構造は，大きく階層型，フラット型，ネットワーク型に分類することができるが，図１に示すように，いずれの組織構造に対しても，楕円エルガマル暗号ベースの組織暗号は適用可能である．

というのも，前章で示したように，楕円エルガマル暗号ベースの組織暗号では，組織構造の如何に関わらず，転送者が転送先の公開鍵を保有していれば再暗号化（鍵の付替え）が可能なためである．また，いずれの組織構造に対しても再暗号化の繰返し適用により，多段の安全な転送が可能である．

楕円エルガマル暗号ベースの組織暗号応用機密情報配信システムは，基本的にはどのような組織構造に対しても構成可能である．

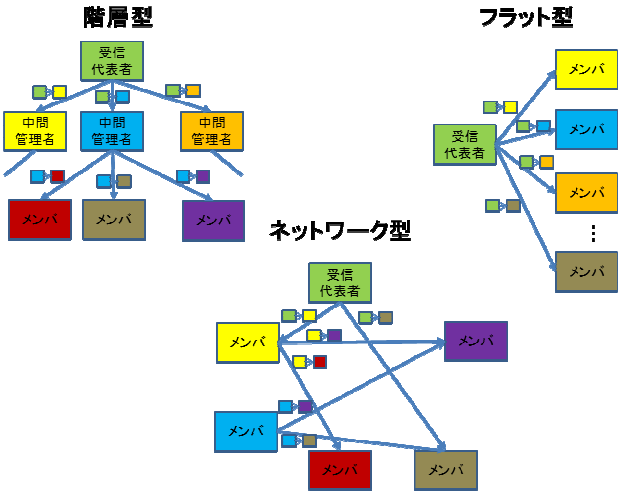


図１．多様な組織構造への組織暗号（再暗号化）適用例

3.2　転送者操作の検証・監査

送信組織の送信者，受信組織の転送者（受信代表者），利用者の三つのエンティティからなる，楕円エルガマル

暗号ベースの組織暗号による機密情報配信システムの基本構成と各エンティティの処理内容を図２に示している．

本構成では，送信者と利用者の間に介在する転送者は単独の判断で転送を実行でき，転送者の誤操作/不正を検知/抑止することは難しい．

また，転送者が使用するシステムは再暗号化（鍵の付替え）のために暗号化データおよび復号鍵の両方を保有するため，転送者のシステムのウイルス感染や不正アクセスによる情報漏えいのリスクが存在する．

本システム構成は，転送者が適切なセキュリティ対策，適切な操作を行うという信頼の元，転送者へ転送・復号に関する権限を委譲するシステム構成である．

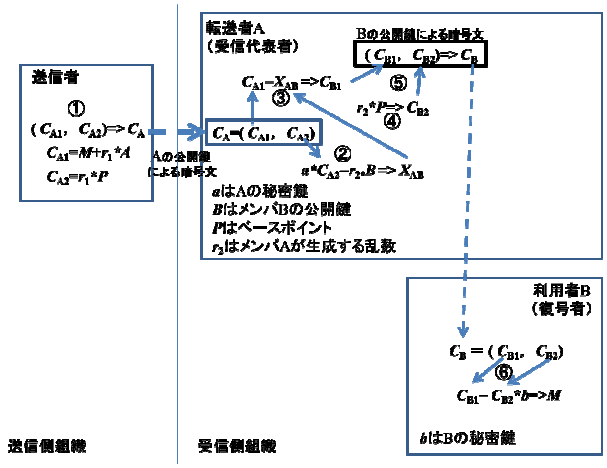


図２．転送者システム内での再暗号化

一方，図３は楕円エルガマル暗号の特徴である暗号化データが２項から構成されていることを利用し，転送・復号操作の検証・監査を可能とする新たなエンティティ（管理サーバ）を導入した構成である．

本構成では，転送者の判断に基づく転送の実行には管理者の協力が必要であり，転送者の操作の確認やログ収集が容易で，転送者の誤操作/不正を検知/抑止することも容易な構成である．

また，暗号化データと復号鍵は異なるエンティティ，転送者と管理サーバが分散保管するので，両エンティティが使用するシステムの両方がウイルス感染や不正アクセスに遭わない限り情報は漏えいしない．

なお，図２，図３に示した両構成の安全性の詳細に関しては情報処理学会論文誌を参照願いたい．（文献[6]）

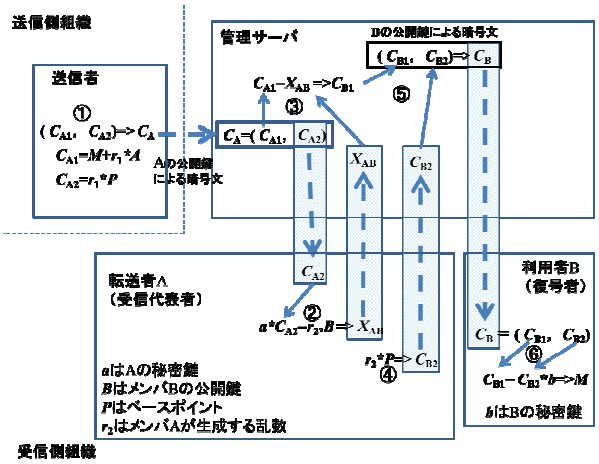


図３．管理者・転送者の両システム連携による再暗号化

3.3 組織暗号の適切かつ有効な実装のための実践規範（ガイドライン）

一般に、組織暗号応用機密情報配信システムは、組み込まれる既存のシステム環境に応じ大きく変化するものであり、安全な実装のための留意事項は個々に異なるが、実際にシステムを実装する際の検討に資するため、図３のシステム構成を対象に組織暗号応用機密情報配信システムのリスクを分析し安全に実装するための実践規範の整理を試みた。

検討にあたっては、暗号化・再暗号化（暗号化データの第１項の変換）・復号はソフトによる実装、楕円暗号系を規定するパラメータ群・秘密鍵の管理および乱数生成・変換鍵の算出にはICカード（耐タンパーなデバイス）内での実装を前提とした。

リスク分析結果を表１に示している。本表では、a～dの４種の機密情報の漏えいパターンがあり、英字に続く数字は盗聴・改変の同時発生時に機密情報の漏えいが発生する組合せを示している。

表１のリスク分析結果を参考に作成した、組織暗号の適切かつ有効な実装のための実践規範（ガイドライン）を表２に示している。

表１．リスク分析結果

①	送信者システム	盗聴	改変	破壊
	暗号化ソフト/パラメータ	-	a2	妨害
	生成した乱数	a2	a2	妨害
	転送者の公開鍵	-	a2	妨害
	転送者向け暗号化データ	a1,b1	妨害	妨害
	平文データ	漏洩	妨害	妨害
②	送信者システムと管理サーバ間の通信路	盗聴	改変	破壊
	転送者向け暗号化データ	a1,b1	妨害	妨害
③	管理サーバ	盗聴	改変	破壊
	暗号化データ変換ソフト	-	c2	妨害
	変換鍵	-	c2	妨害
	転送者向け暗号化データ	a1,b1	妨害	妨害
	利用者向け暗号化データ(第2項)	-	妨害	妨害
	利用者向け暗号化データ	c1,d1	妨害	妨害
④	管理サーバと転送者システム間の通信路	盗聴	改変	破壊
	転送者向け暗号化データ(第2項)	-	妨害	妨害
	変換鍵	-	c2	妨害
	利用者向け暗号化データ(第2項)	-	妨害	妨害
⑤	転送者システム	盗聴	改変	破壊
	変換鍵生成ソフト/パラメータ	-	c2	妨害
	利用者の公開鍵	-	c2	妨害
	転送者の秘密鍵	b1	妨害	妨害
	生成した乱数	c2	c2	妨害
	算出した変換鍵	-	妨害	妨害
	転送者向け暗号化データ(第2項)	-	妨害	妨害
	利用者向け暗号化データ(第2項)	-	妨害	妨害
⑥	管理サーバと利用者システム間の通信路	盗聴	改変	破壊
	利用者向け暗号化データ	c1,d1	妨害	妨害
⑦	利用者システム	盗聴	改変	破壊
	組織暗号ソフト/パラメータ	-	妨害	妨害
	利用者の秘密鍵	d2	妨害	妨害
	利用者向け暗号化データ	c1,d1	妨害	妨害
	平文データ	漏洩	妨害	妨害

表2.　組織暗号の適切かつ有効な実装のための実践規範

組織暗号の適切かつ有効な実装のための実践規範(ガイドライン)
① 暗号化ソフトの正当性(非改竄性)を使用の都度確認できることが望ましい
暗号系を規定するパラメータは、ICカード内に発行者の署名付きで保管することが望ましい
乱数の生成・利用は、ICカード内に制限することが望ましい
送信先である転送者の公開鍵は、ICカード内で公開鍵証明書により正当性を確認できることが望ましい
ICカード内で計算された攪乱項は、デバイスの署名により正当性を確認できることが望ましい
② 転送者向け暗号化データの送信時には、通信路の暗号化が望ましい
③ 暗号化データ変換ソフトの正当性(非改竄性)を使用の都度確認できることが望ましい
転送者より受信する利用者向け暗号化データ(第2項)および変換鍵は、転送者の署名により、正当性を確認できることが望ましい
④ 転送者システムからの変換鍵の送信時には、通信路の暗号化が望ましい
⑤ 暗号系を規定するパラメータは、ICカード内に発行者の署名付きで保管することが望ましい
管理サーバより受信する転送者向け暗号化データの第2項は、管理サーバの署名等で正当性を確認できることが望ましい
乱数の生成・利用は、ICカード内に制限することが望ましい
送信先である利用者の公開鍵は、ICカード内で公開鍵証明書により正当性を確認できることが望ましい
乱数及び利用者の公開鍵を使用した新たな攪乱項の算出は、ICカード内で実施するのが望ましい
ICカード内で計算された攪乱項は、デバイスの署名により正当性を確認できることが望ましい
⑥ 利用者向け暗号化データの送信時には、通信路の暗号化が望ましい
⑦ 復号ソフトの正当性(非改竄性)は、使用の都度確認できることが望ましい
暗号系を規定するパラメータは、ICカード内に発行者の署名付きで保管することが望ましい
管理サーバより受信する暗号化データは、管理サーバの署名により正当性を確認できることが望ましい
ICカード内で計算された復号に使用する攪乱項は、デバイスの署名により正当性を確認できることが望ましい

4　自治体向け組織暗号紹介・実証実験活動

中央大学研究開発機構では，組織暗号の研究開発と同時に，組織暗号の有用性・有効性を広く社会に理解いただくための活動をも重視，まずはマイナンバー導入により更に個人情報の取扱いが増加することが想定される自治体で組織暗号を理解いただくことを目的とし，2014 年より自治体向けに組織暗号の紹介や実証実験活動に着手した.

これまで,組織暗号の実証実験を実施した自治体は以下の通りである.

2014 年 10 月 15 日：長野県・大町市

2014 年 11 月 7 日：長野県・箕輪町

2014 年 11 月 21 日：新潟県・燕市

2015 年 6 月 5 日：兵庫県(兵庫県，西宮市，加古川市)

2015 年 9 月 3 日：大分県(大分県，大分市，中津市)

また，組織暗号の紹介や個人情報取扱い状況・業務の把握のために訪問した自治体は以下の通りである.

2015 年 8 月 5 日：京都府

2015 年 9 月 15 日：京都市

本章では以下,自治体で実施した組織暗号の実証実験の内容・結果について報告する.

4.1　実証実験のプログラム構成・目的

実証実験は，自治体の方々に自治体業務における組織暗号の有用性・有効性を理解いただくことなどを目的として，以下の内容で実施した.

①　挨拶

現地の自治体の幹部の方に，個人情報の利活用と保護に関する考えを，表明していただくのが目的.

②　組織間通信，組織暗号に関する講演

自治体業務における個人情報保護の重要性，暗号技術の必要性・有効性，組織暗号の新規性・有用性・有効性などを理解いただくのが目的.

③　組織暗号が活用可能な自治体業務の紹介

多くの自治体が抱える業務で，組織暗号の有効活用が可能な業務例の紹介．自治体業務全般での組織暗号の有用性・有効性を理解いただくのが目的.

④　実証実験実施自治体の具体的業務に対する組織暗号適用方式案の紹介

身近な業務に対する組織暗号の適用方式案の紹介.

身近に組織暗号が有効活用できる業務が存在すること，組織暗号の適用方法が容易であることを理解いただくのが目的.

⑤　組織暗号デモ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使用し，④で紹介した業務への組織暗号適用方式案の一つを例題に取り上げ，簡単な組織暗号応用機密情報配信システムの操作実験を，自治体職員の方々に操作を担当いただき実施．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．組織暗号応用機密情報配信システムの具体例をイメージいただくと共に，操作性や性能面で実用上問題無いことを理解いただくのが目的.

⑥　質疑応答

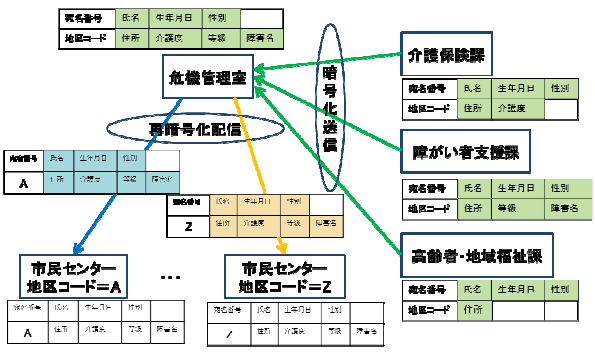
参加者の疑問，質問への回答を実施．参加者の組織暗号および自治体業務での組織暗号の有用性・有効性に関する理解を深めるのが目的.

4.2　自治体の業務例と組織暗号適用案

本節では，今年度、実証実験を実施した２自治体で説明した具体的業務への組織暗号適用案を紹介する．実証実験では，各自治体で 3～4 例を挙げ説明したが，本稿では自治体ごとに 1 例のみを紹介する.

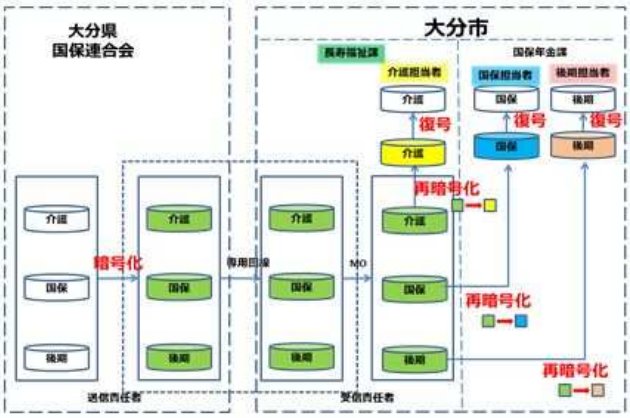
① 加古川市役所の避難行動要支援者情報の安全な配信

介護保険課，障がい者支援課，高齢者・地域福祉課から暗号化された避難行動要支援者情報を入手した危機管理室（緑色）は，個人別に情報を統合し，担当する市民センターへ対象者情報のみ，それぞれの市民センター担当者向けに再暗号化し送信.



② 大分市の公的年金からの特別徴収候補者情報の安全な配信

大分県国保連合会より暗号化された特別徴収候補者情報を入手した長寿福祉課の責任者（緑色）は，介護担当者，国保担当者，後期担当者へ該当する情報のみ，それぞれの担当者向けに再暗号化し送信.



4.3　実証実験の報道状況

実証実験を実施するにあたり，住民の方々にも理解いただくことを目的とし，報道機関向けの文書を作成，配布した．その結果，以下の通り，実証実験に関する報道が行われた.

① 2014 年 10 月 15 日：長野県・大町市

＊中日新聞の中信総合版 2014 年 10 月 16 日朝刊の 19 面に掲載

＊大糸タイムズの 2014 年 10 月 16 日の 1 面に掲載

＊大町ケーブルテレビで 10 月 22 日～28 日の間、毎日 6 回放映

② 2014 年 11 月 7 日：長野県・箕輪町

＊みのわ新聞の 2014 年 11 月 8 日の 1 面に掲載

③ 2014 年 11 月 21 日：新潟県・燕市

＊電波タイムズの 11 月 28 日の紙面に掲載

④ 2015 年 9 月 3 日：大分県(大分県，大分市，中津市)

＊大分合同新聞の 9 月 4 日朝刊の 5 面に掲載

＊大分放送の 9 月 4 日の夕刻のニュースにて放映

4.4　実証実験参加者のコメント/アドバイス

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.

5 医療機関向け組織暗号紹介・実証実験活動

組織間通信の活発化が想定され、個人情報である医療情報の利活用と保護の両立が求められるであろう医療機関での組織暗号の有用性・有効性の理解を広めるため，医療機関向けの紹介活動や実証実験も 2015 年より本格化させた.

組織暗号の紹介および医療情報の取扱い状況・業務の把握のために訪問した医療機関は以下の通り.

2014 年 2 月 13 日：埼玉県・桑の実会

2015 年 1 月 29 日：山梨県・山梨県立中央病院

2015 年 2 月 9 日：長野県・ななきの家

2015 年 2 月 9 日：長野県・信州大学医学部付属病院

2015 年 7 月 15 日：長野県・信州メディカルネット

2015 年 7 月 23 日：
島根県・しまね医療情報ネットワーク

2015 年 8 月 3 日：東京都・NBDC/DBCLS

2015 年 8 月 6 日：京都府・京都医療センター

2015 年 8 月 21 日：山梨県・富士吉田医師会

2015 年 9 月 25 日：
東京都・National Clinical Database

2015 年 9 月 25 日：
長崎県・長崎地域医療連携ネットワーク

2015 年 10 月 28 日：
宮崎県・宮崎大学医学部付属病院

5.1 京都医療センターでの実証実験概要

2015 年 11 月 19 日、京都医療センターにて、医療機関としては初めての組織暗号の実証実験行った。本実証実験では、①講演「組織間通信における情報漏洩と組織暗号の実用化」、②組織暗号方式の説明と適用案の紹介、③組織暗号のデモ、を実施した。

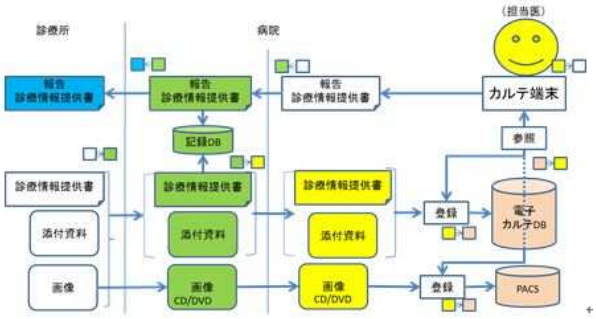
5.2 医療分野の業務例と組織暗号適用案

本節では，実証実験を実施した京都医療センターで説明した具体的業務への組織暗号適用案を 2 例､紹介する．なお，業務例における業務・情報フローは，組織暗号適用方式検討のため簡略化している.

① 紹介状（診療情報提供書）の安全な送受信

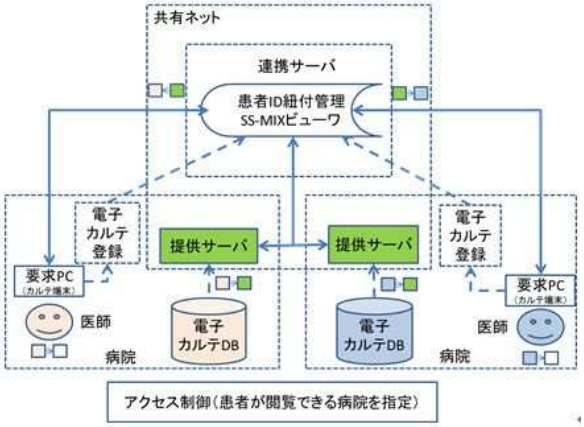
診療所より暗号化された紹介状（診療情報提供書）を入手した病院の窓口責任者（緑色）は，担当医（黄色）へ該当する情報のみ，それぞれの担当医向けに再暗号化し送信．担当医は，内容確認の上，電子カルテ（桃色）へ取り込む.

報告については，担当医より暗号化された返書（診療情報提供書）を入手した病院の窓口責任者（緑色）は，診療所（青色）へ再暗号化し送信.



② 電子カルテの安全な相互参照

連携サーバは，暗号化された提供サーバ上の電子カルテをアクセス，要求元の医師（桃色，青色）向けに再暗号化し表示データを送信.



5.3 実証実験参加者のコメント/アドバイス

京都医療センターでの実証実験では活発な質疑が行われ、組織暗号そのものや組織暗号の応用、組織暗号のサービス形態に関し，以下のような貴重なご意見をいただいた.

①検査センターと医療機関、病院と調剤薬局の組織間通信に活用できそう。特に、病院から調剤薬局へ送る処方箋については、組織暗号の利用により、厚生労働省が認可しかねている電子処方箋の実現、技術革新の可能性があるのでは。

②紙データの紹介状では、地域連携室の一般事務員が見ることになるが、見て欲しくない情報であり、こういうもの（組織暗号）があってしかるべき。院内処方箋の問題もある。

③医療データを介護事業者へ渡す際も、組織暗号のような機能が望ましい。

④クラウドで組織暗号機能を提供できることは一番のメリットであって、各医療機関で個別に実装するのではコストベネフィットがない。データセンターに置いた組織暗号化機能を各医療機関がクラウドの形で使用できるようにすれば、各機関のコストは利用件数あたりの使用料のみでよいので、簡単かつ速やかに導入できる。

6 組織暗号の実用化に向けての課題

組織暗号の紹介活動や実証実験を通じ，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.

(1)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.

(2)組織暗号利用の関係省庁へのご説明

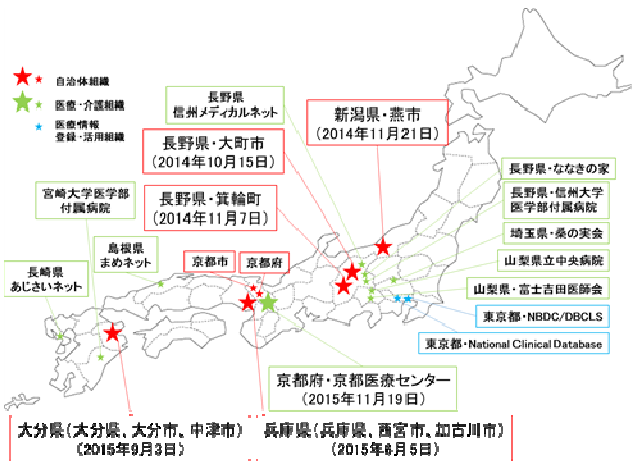
自治体，医療・介護，金融機関・民間企業等での組織暗号活用に対する関係省庁のご理解・ご支援が大変重要.

(3)多様な個人情報保護ニーズへの対応

個人情報の収集・加工・配布・管理・利用環境は多様であり，今回の紹介活動・実証実験の対象とした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，組織暗号を含め暗号化状態処理，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 おわりに

楕円エルガマル暗号ベースの組織暗号を、社会に広く認知いただくと共に、個人情報・医療情報を保護に留意しつつも利活用が求められる自治体や医療・介護組織、その他の多くの企業にて活用を検討いただくため、下図の地域・組織で組織暗号の紹介活動・実証実験を展開してきた。



その結果として、4.4、5.3 に示すように、組織暗号の可能性に期待される多くのご意見をいただいた。一方、6 に示すように、実用化に向けた課題も明確になってきた。

今後は、6 に示した課題の克服に努めつつ、自治体や医療・介護の現場での実業務での組織暗号の有用性・有効性および実用性能性の実証 PJ 等に参画、また組織暗号を含め暗号化状態処理，秘密分散状態処理等の更なる研究開発の機会をとらえ、個人情報・医療情報等の更なる利活用促進とより確実な保護の両立のための技術開発・実用化に貢献すべく活動する予定である。

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，箕輪町，燕市，兵庫県，西宮市，加古川市，大分県，大分市，中津市の各自治体，事業創造大学院大学，ハイパーネットワーク社会研究所の協力を得，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).

[4] 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）.

[5] 才所敏明，近藤健，庄司陽彦，五太子政史，辻井重男: 組織暗号の実証実験－自治体における個人情報保護に向けて， SCIS2015(2015 年暗号と情報セキュリティシンポジウム).

[6] 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.

[7] 才所敏明，近藤健，庄司陽彦，五太子政史，辻井重男: 自治体における組織暗号実証実験報告，CSS2015（Computer Security Symposium 2015）.

[8] 才所敏明，近藤健，庄司陽彦，五太子政史，辻井重男: 組織暗号の社会的実装に向けて，JCMI35（第 35 回医療情報学連合大会）.