

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

はじめに

中央大学研究開発機構は、国立研究開発法人情報通信研究機構(NICT)より委託を受け「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—」の研究開発を推進中です。

本研究開発では、新たな暗号技術、秘密分散状態処理、暗号化状態処理など、多くのテーマの研究開発を実施しています。

本報告は、その中で、試実装まで完了した楕円エルガマル暗号ベースの組織暗号の、実用化に向けた活動の報告です。

組織間通信

組織間通信とは

**情報送信者と情報利用者が異なる組織に属する通信
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

情報送信者(送信代表者)は

**受信組織内のしかるべき窓口の方(受信代表者)に送信
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

組織間通信では、

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、

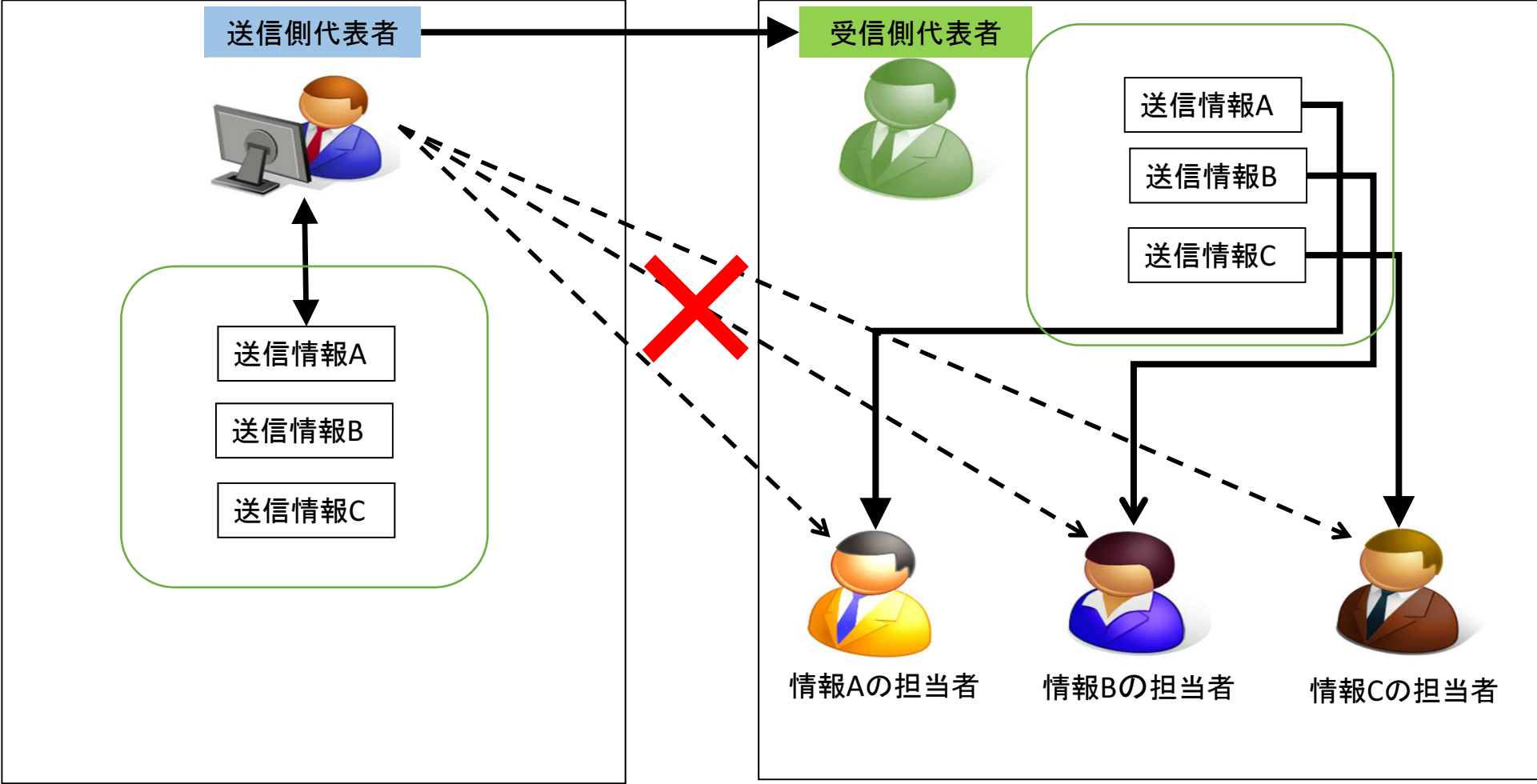
受信組織側の判断で受信組織内を転々と送信され、

適切な情報利用者へ到達する

組織間通信

送信側

受信側



組織暗号

組織間通信を利用し機密情報の配信する場合、
受信組織内を機密情報が転々と転送されることになる

組織暗号は、転送が必要な組織間通信向きの暗号技術
従来の暗号方式では、

受信者向けに暗号化された機密情報を転送する場合
一旦機密情報を復号し、
新たな受信者向けに再度暗号化が必要

組織暗号方式では、

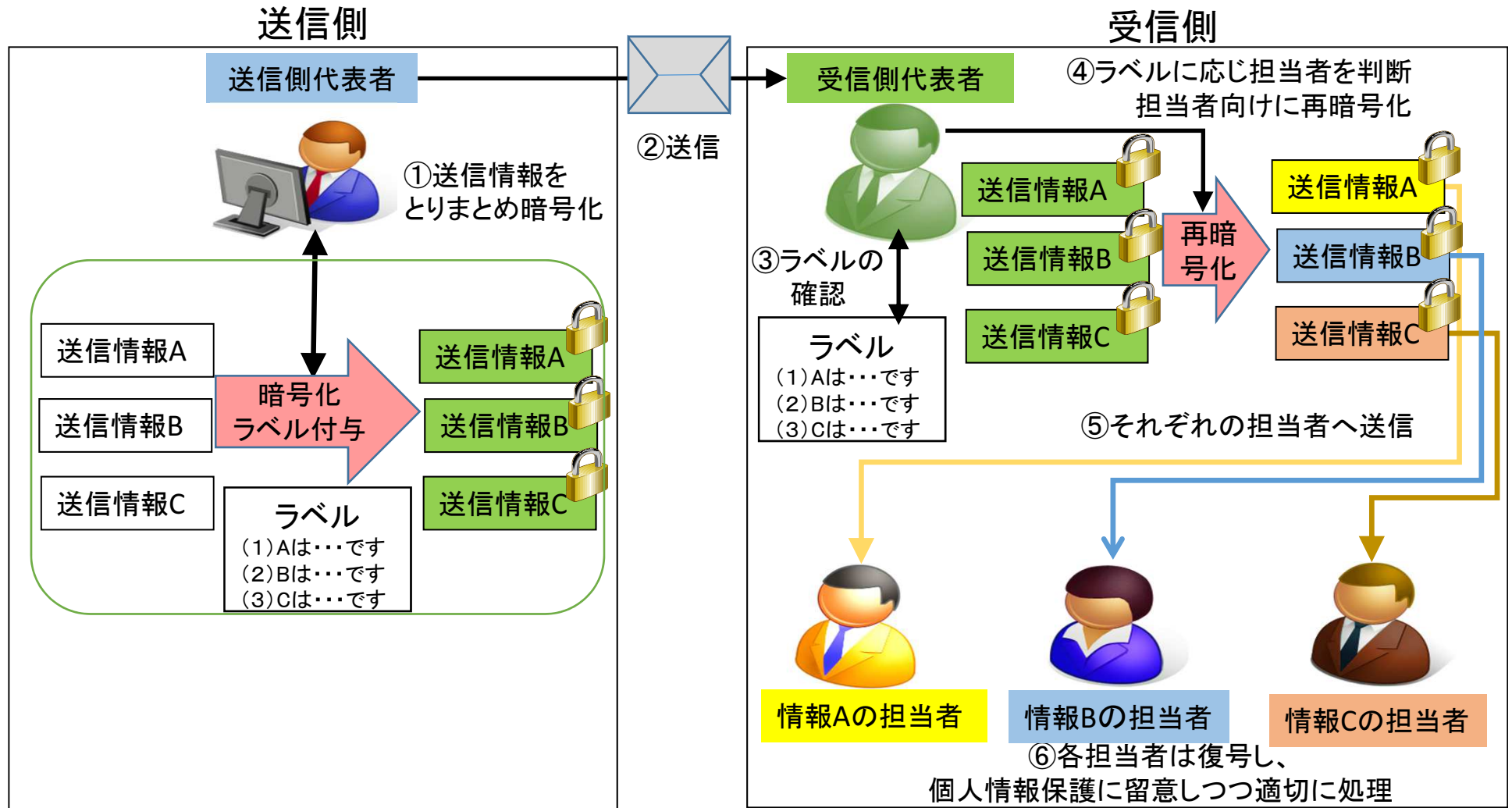
受信者向けに暗号化された機密情報を復号することなく、
その暗号化機密情報を

新たな受信者向けの暗号化機密情報へ変換が可能

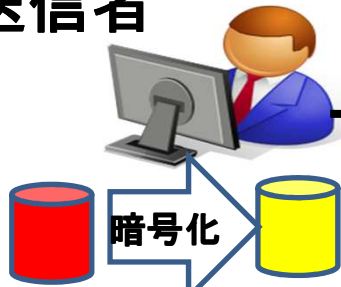
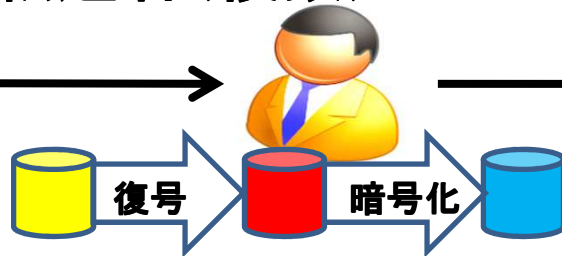

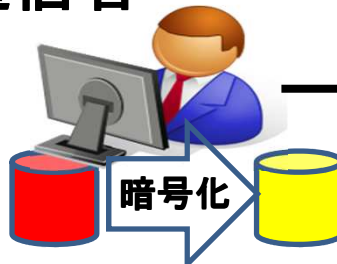


受信組織内を機密情報が転々と転送される場合も

機密情報を暗号化状態のまま最終利用者（復号者）まで転送可能

組織間通信と組織暗号



組織暗号の安全性

従来の暗号方式	送信者 	転送者(複数) 	利用者 
	転送者は機密情報を、一旦復号する(平文に戻す)必要があり、転送者の数に応じ、情報漏えいのリスクが増大		
組織暗号方式	送信者 	転送者(複数) 	利用者 
	転送者は機密情報を、復号する(平文に戻す)ことなく転送でき、転送プロセスでの情報漏えいのリスクを軽減可能		



は、平文の機密情報



は、暗号化された機密情報

楕円エルガマル暗号

[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

[A のための暗号化]

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

[A による復号]

① $M = M_1' - M_2' * a$

楕円エルガマル暗号ベースの組織暗号

受信者A向けの暗号化データを

受信者B向けの暗号化データへ変換する例

[定義 (追加分のみ)]

Bの秘密鍵：乱数 b

Bの公開鍵： $b*P(=B)$

[AによるBのための再暗号化]

①乱数 r_2 の生成

② $M_2''=r_2*P$

③変換用鍵 X_{AB} の計算 $X_{AB}=a*M_2'-r_2*B$
 $=a*r_1*P-r_2*B=r_1*A-r_2*B$

④ $M_1''=M_1'-X_{AB}=M+A*r_1-r_1*A+r_2*B=M+r_2*B$

$M''=(M_1'', M_2'')$ 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

[Bによる復号]

① $M=M_1''-M_2''*b$

自治体業務と組織暗号

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)導入が決定
(2016年より, 社会保障分野, 税分野, 災害対策分野へ)

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

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ことを期待

自治体向け組織暗号実証実験

目的:

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

自治体の具体的業務を理解し、

組織暗号適用方法を検討する

方法:

自治体の職員の方々に、

直接、現地で、組織暗号の説明を実施する

具体的業務例を自治体に提示いただき、

その業務への組織暗号適用方式を提案、

組織暗号応用により安全性が高まることをご理解いただく

具体的業務例への組織暗号応用システムの

操作デモをご覧いただき、組織暗号応用システムの操作が

簡単であることをご理解いただく

実証実験実施自治体・日程

長野県・大町市(2014年10月15日)

長野県・箕輪町(2014年11月7日)

新潟県・燕市(2014年11月21日)

兵庫県(兵庫県、西宮市、加古川市)

(2015年6月5日)

大分県(大分県、大分市、中津市)

(2015年9月3日)

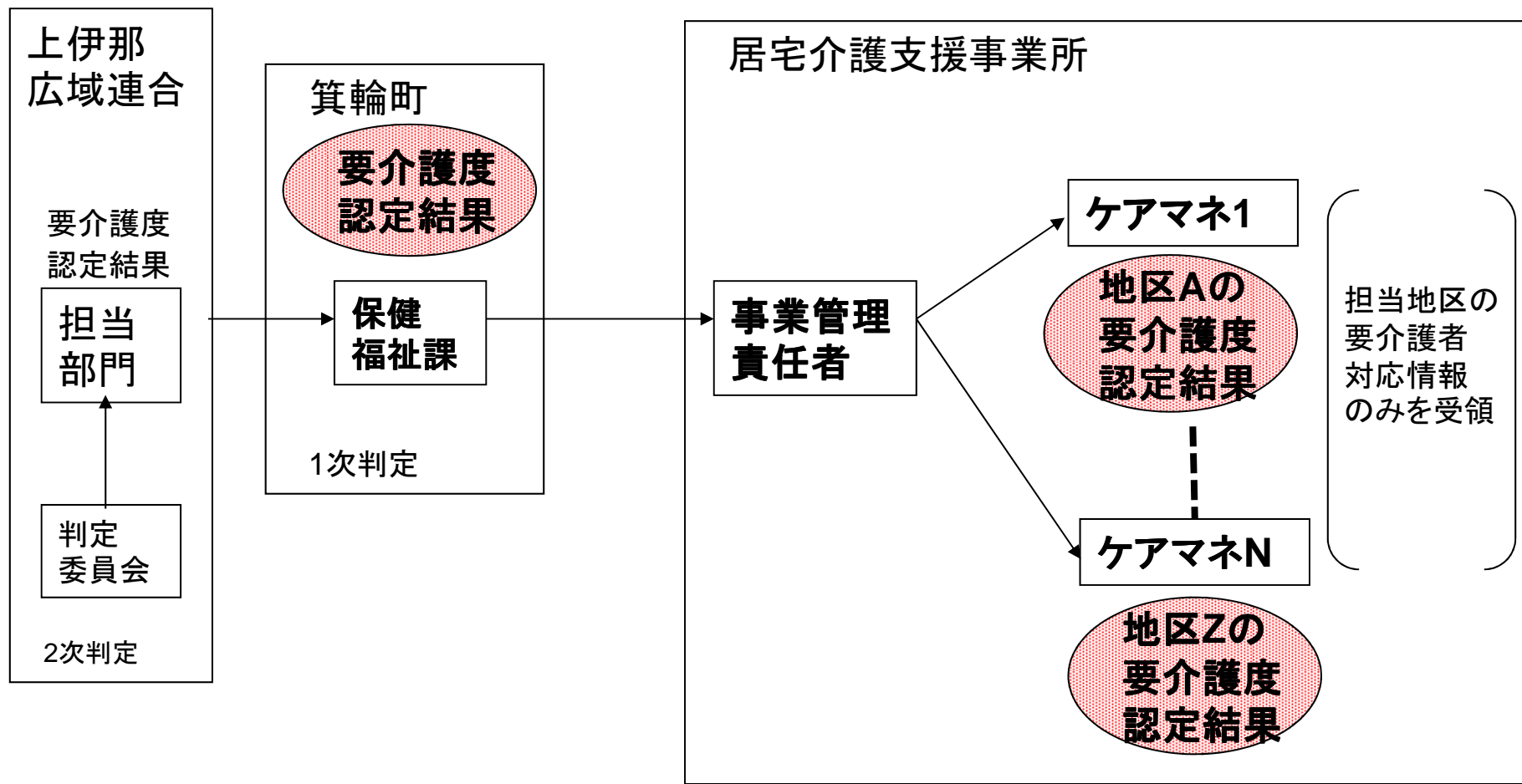
組織暗号実証実験式次第(2015年9月3日)

司会 才所敏明 中央大学 研究開発機構 専任研究員

- 10:00～ 挨拶
大場善次郎 ハイパーネットワーク社会研究所 理事長・所長
辻井重男 中央大学 研究開発機構 機構教授
- 10:10～ 講演「情報通信・セキュリティ概念の高度化とその具体的方策」
辻井重男
- 10:50～ 組織暗号 ー自治体での活用可能な業務例ー
近藤健 NPO法人中央コリドー情報通信研究所 理事
中央大学 研究開発機構 客員研究員
- 11:05～ 組織暗号 ー大分県内自治体想定業務への適用案
および操作実験の構成・内容紹介ー
才所敏明
- 11:25～ 組織暗号 ー実験システム動作説明ー
庄司陽彦 YDKコミュニケーションズ
中央大学 研究開発機構 客員研究員
- 11:45～ 質疑応答

(12:00 終了予定)

要介護認定結果通知業務



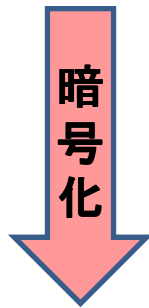
地区を担当する居宅介護支援事業所の ケアマネへの要介護認定結果の安全な通知

居宅介護支援事業所

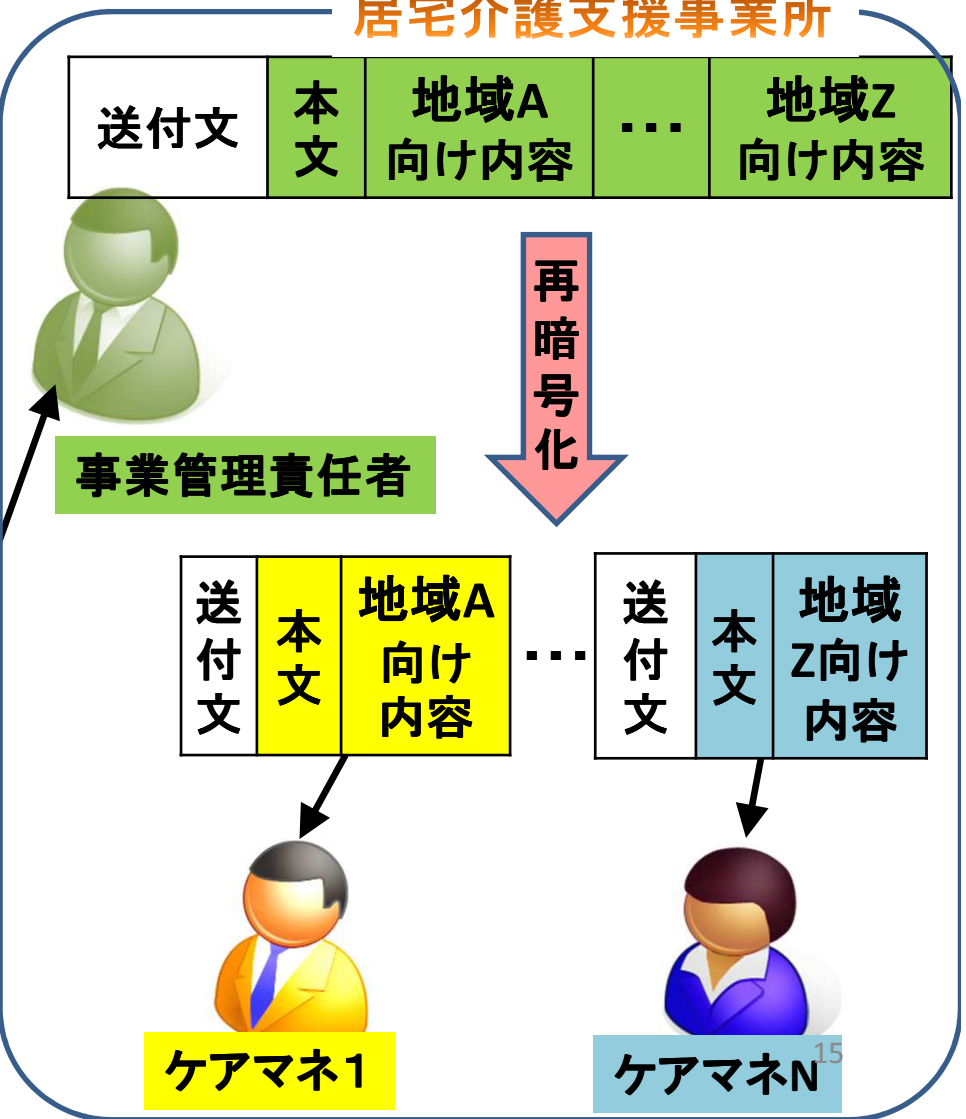


箕輪町の担当者

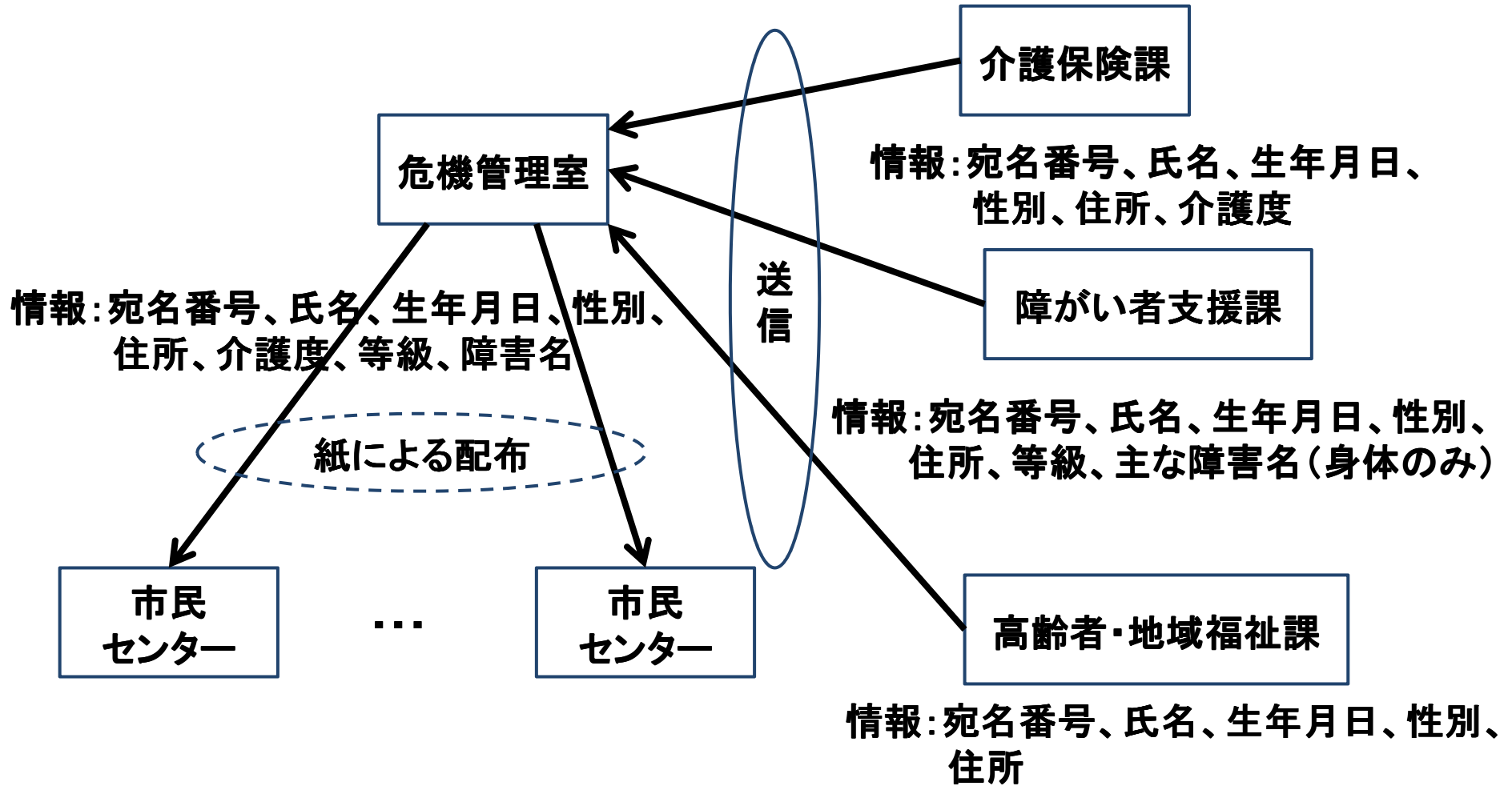
送付文	本文	地域A 向け内容	...	地域Z 向け内容
-----	----	-------------	-----	-------------



送付文	本文	地域A 向け内容	...	地域Z 向け内容
-----	----	-------------	-----	-------------



避難行動要支援者情報配布業務





組織番号とは
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、
行政機関が相互にデータを共有する個人情報の
利便性向上が目的とされています。
税務関係の個人情報は、国税庁が実施する番号方式として、
社会保障分野の個人情報は、社会保障番号(マイナンバー)の発行を受け、
行政機関が共有している番号方式

大町ケーブルテレビ
2014年10月22日～28日
1日6回放映(1分8秒)







組織暗号実証実験

2015年9月3日
ハイパーネットワーク社会研究所
中央大学研究開発機構

実証実験参加者

- 参加人数 各回20名～50名程度
- 参加組織
 - 自治体、外郭団体
 - 一般民間企業
 - システム開発ベンダ、コンサル企業
 - 大学・研究開発機関
 - 報道機関

個人情報保護に「組織暗号」

大町市 導入向け県内初実証実験

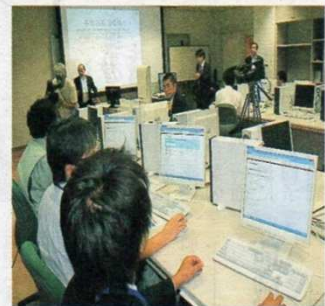
大町市で15日、行政システムの「組織暗号」の導入に向けた実証実験が行われた。行政組織の中で流通する個人情報保護を確保する技術について、実際に業務に即した作業を試した。

写真。

大町市で15日、行政システムの「組織暗号」の導入に向けた実証実験が行われた。行政組織の中で流通する個人情報保護を確保する技術について、実際に業務に即した作業を試した。

(平文化)必要があり、誤った人に情報が伝わるなど配信中に不要な情報が漏れる可能性があった。

組織暗号技術は、特殊な暗号の「鍵」データを扱い、暗号化したまま担当者まで必要な情報のみを渡すことができ、配信中の情報が漏れを防ぐことがで



敬老会のリストづくりなど、さまざまな場合が想定される。実験は大町市、北アールフス広域連合、中央コリド―高速実験プロジェクト推進協議会、中央大学の共同事業。

平成28年に国や地方自治体を取り入れる「マイ・ナンバー（国民ID）」制度導入に向けた実験で、県内初、同協議会長で同大学研究開発機

行政情報を暗号化

漏えい防止 大町で実証実験

自治体が扱う情報の漏えいを防ぐため、情報を暗号化してインターネット上でやり取りする技術の実証実験が15日、大町市総合情報センターであり、市職員らが参加した。

この技術は、中央大・研究開発機構が独立行政法人情報通信研究機構の委託で二〇一三年度から三年間かけて研究を進めている。自治

を使って敬老会の名簿を作成する事例で、暗号化した情報をネットですべて送る体験をした。



暗号化技術で情報を送る実験に参加する市職員ら。大町市総合情報センターで。

(吉田幸雄)



発行所
〒399-4601 箕輪町松島8752-1
みのわ新聞社
編集・発行人 陸 摩 建
電話 代表 79・8484
FAX 79・8485
www.shimin.co.jp
E-mail
minowa@shimin.co.jp
©みのわ新聞社 2014年
定価1ヵ月1,420円
(1部売60円(税込み))
本紙をお届けする販売店
井ノ屋新聞店 ☎79・2368
井ノ屋新聞店 ☎72・7455
Y.C. 箕輪店 ☎79・6663
桑沢新聞店 ☎76・9998
なかむら新聞店 ☎78・8055
中川新聞店 ☎73・5303
高屋新聞店 ☎73・5303
コンビニにもご利用ください

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が研究開発している通信セキュリティ技術の「組織暗号」実証実験を町情報通信センターで行った。自治体の立場で同技術が実装できるのか助言した。

組織内での電子データのやり取りで、情報を暗号化し、転送する際に情報の漏えいを軽減する技術。町は同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の流れを確認した。モデル実

験に對し、箕輪町で採用したケースを話し合った。
「町の外郭団体との連絡時には便利」
「1件ごと暗号化するのは不便では」「伝送だけでなく保管する時に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く、同技術を採用する予定は現在ないという。担当の町経営企画課は「マイナンバー制度の導入が見込まれている。これまで以上に適切な管理を努めていきたい」としている。

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



実験が行われた燕市役所



組織暗号実証実験の様相

中央大学研究開発機構、事業創造大学院大学、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は、11月21日（新潟県燕市役所）で、組織暗号実証実験を開催した。同様の実験は10月に長野県大町市、真狩町で行われ成功を収めた。燕市の実験は、この2市町での経験を踏まえて、地方自治体が多角的に、個人情報を扱う上で重要なものとして、準備は全国に広がっている。

燕市は、情報化社会における、個人情報を扱う上で重要なものとして、準備は全国に広がっている。

燕市は、情報化社会における、個人情報を扱う上で重要なものとして、準備は全国に広がっている。

燕市は、情報化社会における、個人情報を扱う上で重要なものとして、準備は全国に広がっている。

燕市は、情報化社会における、個人情報を扱う上で重要なものとして、準備は全国に広がっている。

燕市は、情報化社会における、個人情報を扱う上で重要なものとして、準備は全国に広がっている。

燕市は、情報化社会における、個人情報を扱う上で重要なものとして、準備は全国に広がっている。

新潟情報通信研究所理事長は「燕市は、情報化社会における、個人情報を扱う上で重要なものとして、準備は全国に広がっている。」と述べた。

燕市は、情報化社会における、個人情報を扱う上で重要なものとして、準備は全国に広がっている。

燕市は、情報化社会における、個人情報を扱う上で重要なものとして、準備は全国に広がっている。

燕市は、情報化社会における、個人情報を扱う上で重要なものとして、準備は全国に広がっている。

燕市は、情報化社会における、個人情報を扱う上で重要なものとして、準備は全国に広がっている。

2014年(平成26年) 第6367号 金曜日
11月28日 発行所 株式会社 電波タイムズ社
〒105-0004 東京都港区新橋5丁目30番1号 電話 (03) 54703601 FAX (03) 54703602
大塚支社/支所/中野 中野 http://www.dempa-times.jp

電波タイムズ

The Dempa Times

大分合同新聞9月4日朝刊5頁

ネット上のやりとり

情報漏えい防げ

組織暗号
実証実験

自治体や企業など団体間でのネット上のやりとりで、情報漏えいの危険性が低いとされる「組織暗号」の実証実験が3日、大分市のホルトホール大分であった。自治体や企業の関係者ら約40人が出席した。

マイナンバー制度の開始を控え、個人情報の保護の重要性が一層増していることから、ハイパーネットワーク社会研究所（大分市）



自治体や企業関係者らが出席

と中央大学研究開発機構（東京都）が主催した。

組織暗号では外部から受信した情報を解読しないまま再暗号化して担当者に送ることがができる。解読後の情報に触れる人を担当者に限定できるため団体内での情報漏えい防止に優れているとされる。

実験は県内の市が県国保連合会から年金データの提供を受けるという想定で実施。立ち会った県情報政策課の担当者は「思ったよりも簡単な操作で扱えた。暗号化されていない情報に触れる人が少ないほど漏えいの危険性が狭まる」と話した。

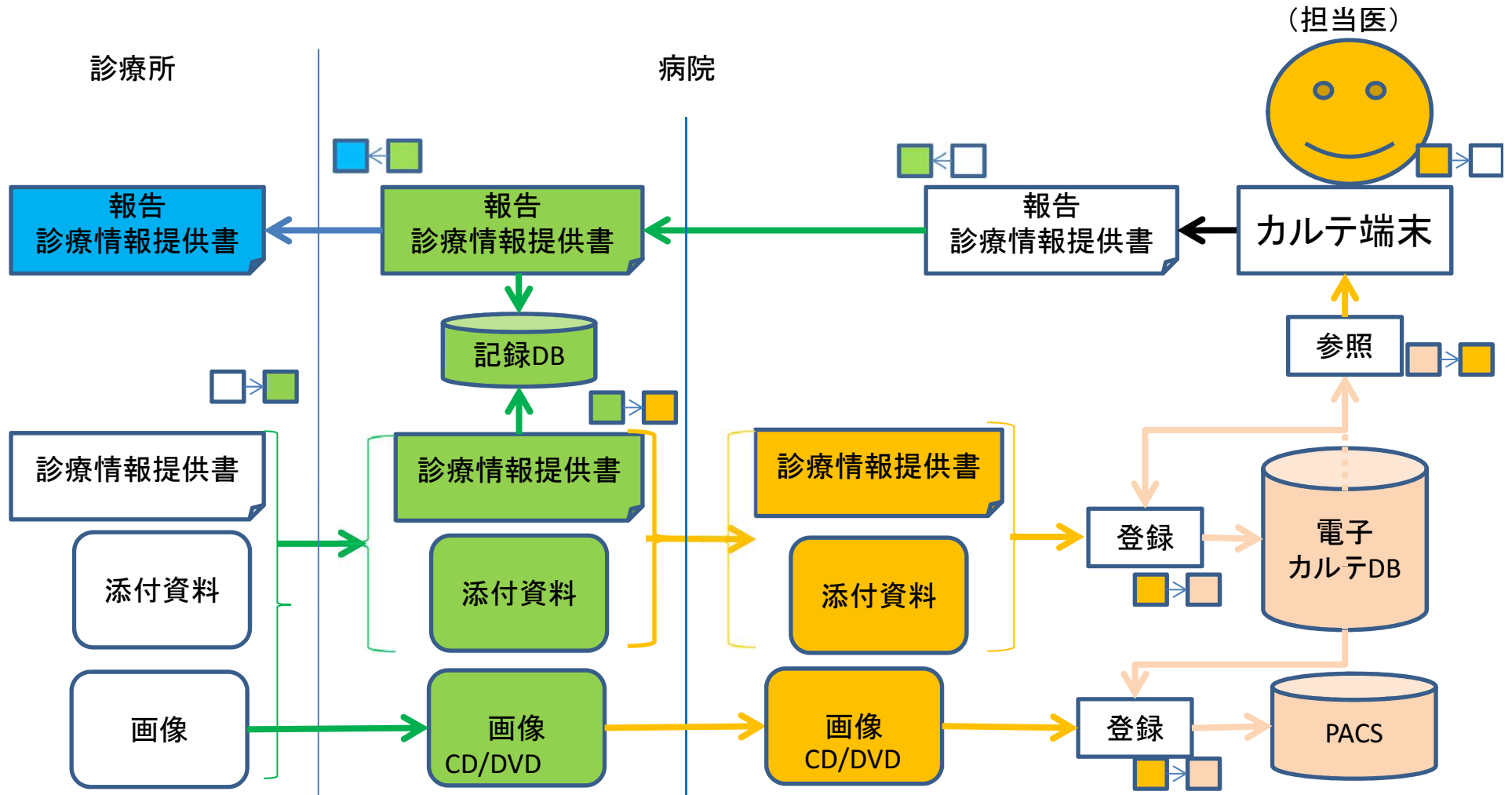
< 実証実験からの知見 > 自治体側の反応・感想

- (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
- (2) 日々取り扱っている個人情報の重要性の再認識
- (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
- (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
- (5) 情報技術への不安、不信 情報漏えい事件の報道など
- (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
- (7) 先進的技術の独自採用は困難

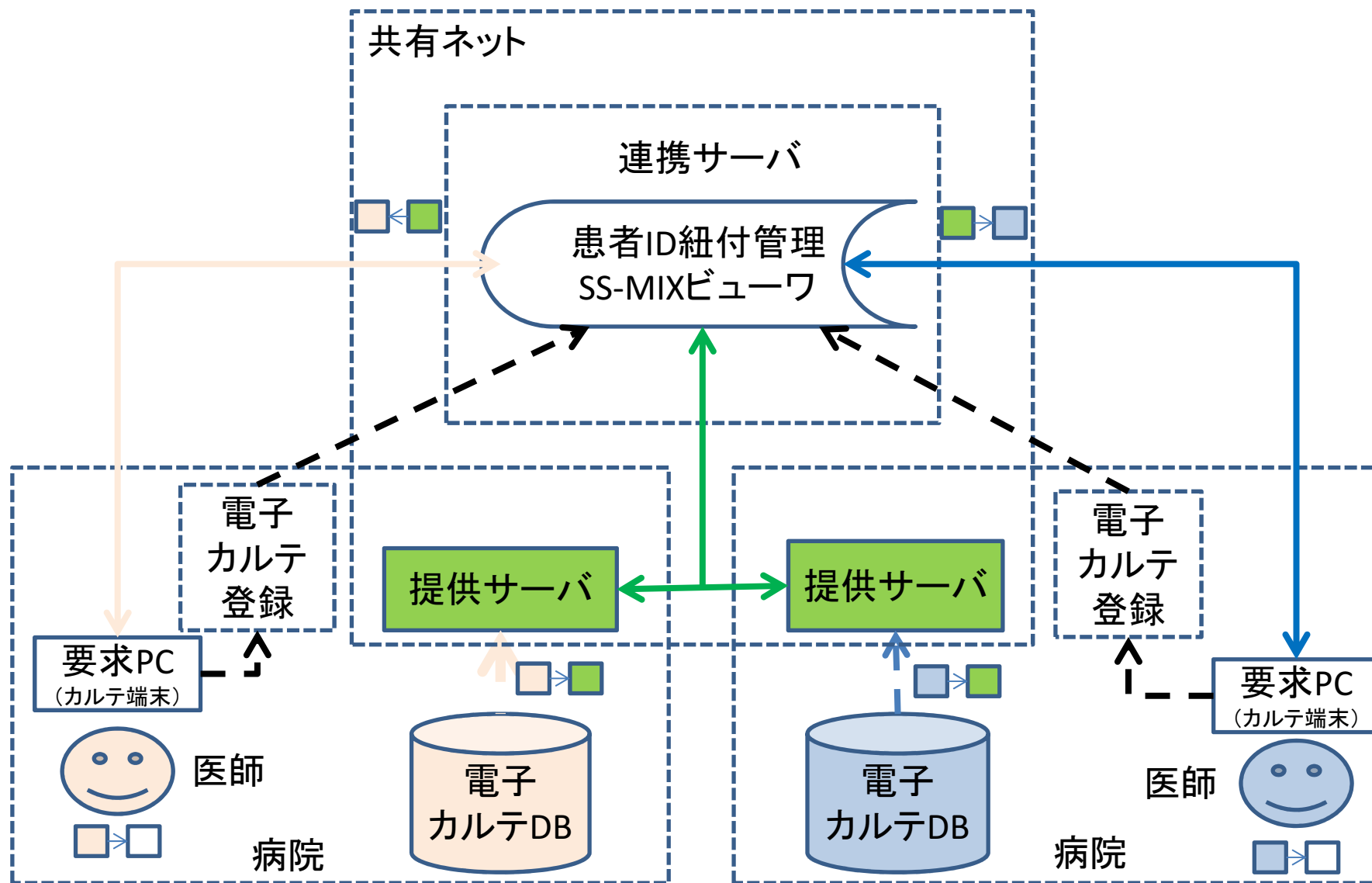
医療機関向け組織暗号紹介活動

- 組織暗号紹介と意見交換のための訪問
 - 長野県・信州メディカルネット(7月15日)
 - 島根県・まめネット
 - (しまね医療情報ネットワーク)(7月23日)
 - 京都府・京都医療センター(8月6日、20日、9月14日)
 - 山梨県・富士吉田医師会(8月21日)
 - 長崎県・あじさいネット
 - (長崎地域医療連携ネットワーク)(9月25日)
- 調査業務例
 - 紹介状(診療情報提供書)の送受業務
 - 電子カルテの相互参照方式

紹介状(診療情報提供書)の安全な送受



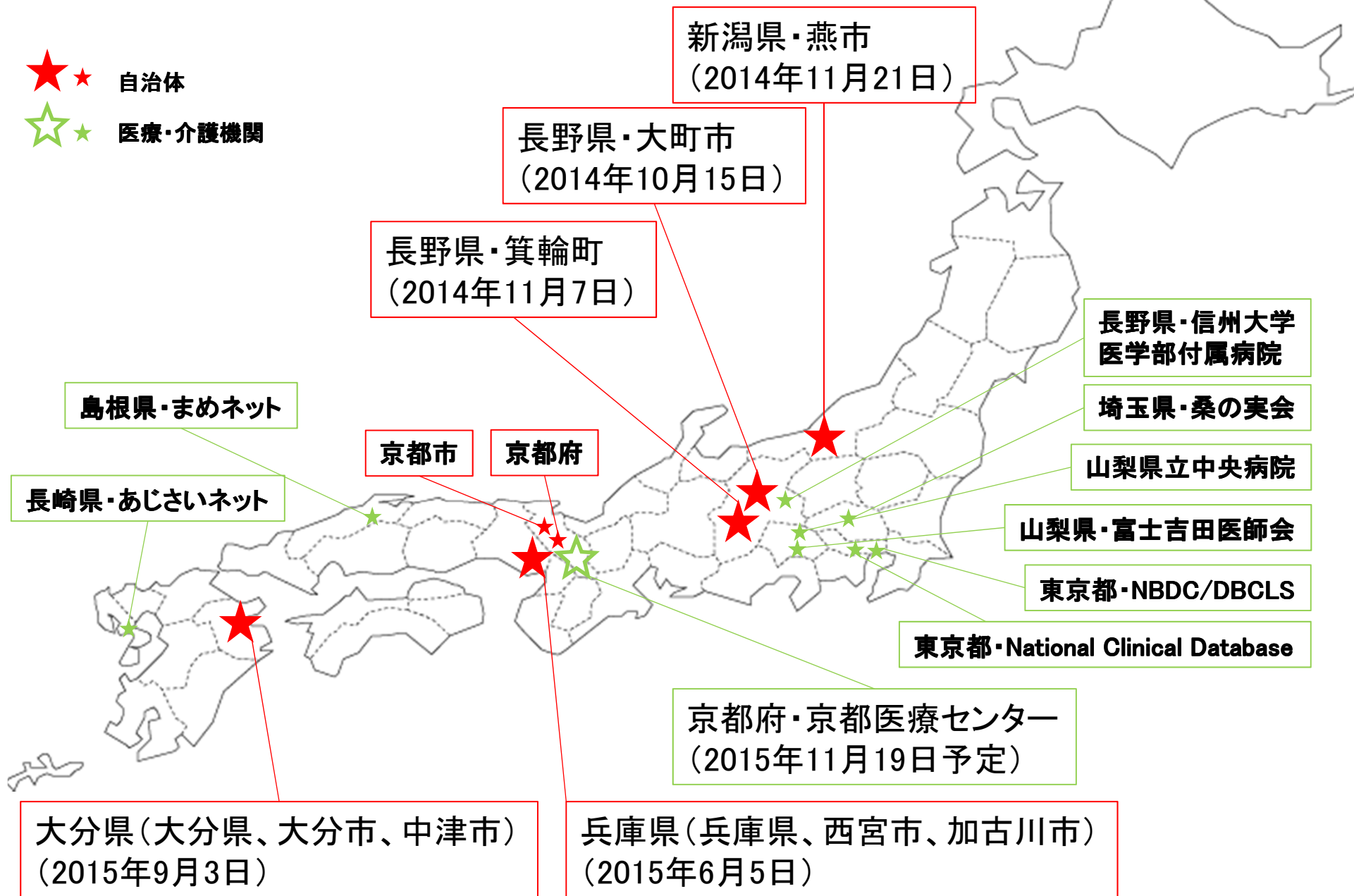
電子カルテの安全な共有



アクセス制御(患者が閲覧できる病院を指定)

組織暗号紹介実施組織・地域

- ★ ★ 自治体
- ☆ ☆ 医療・介護機関



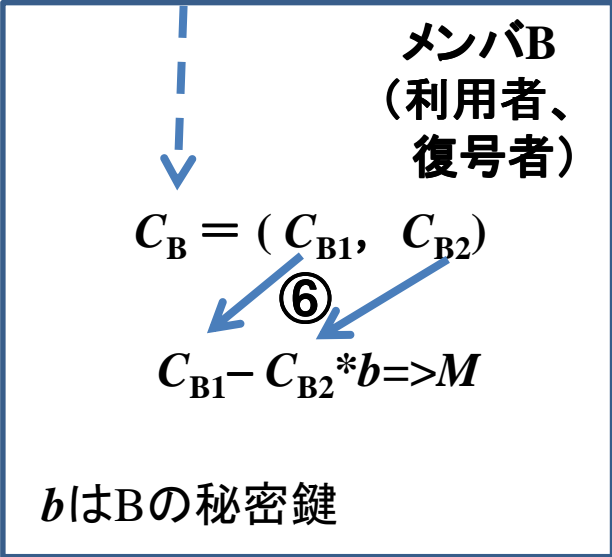
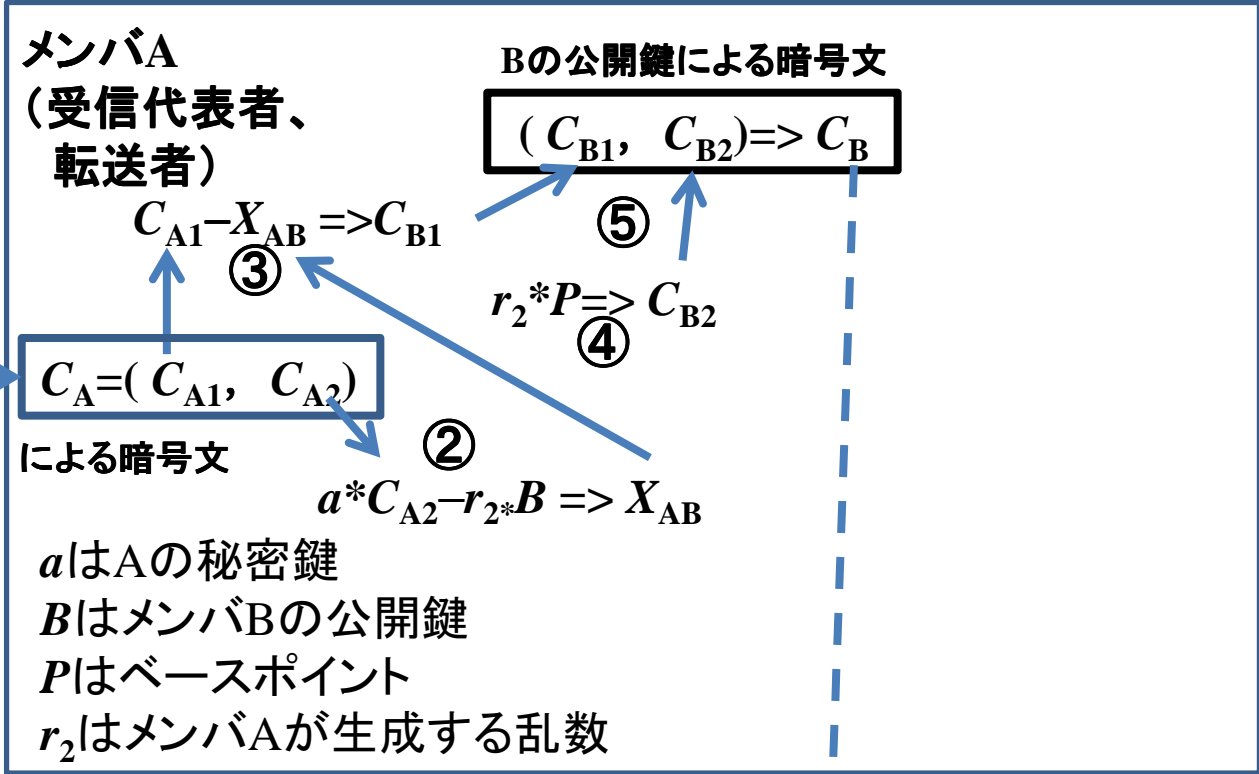
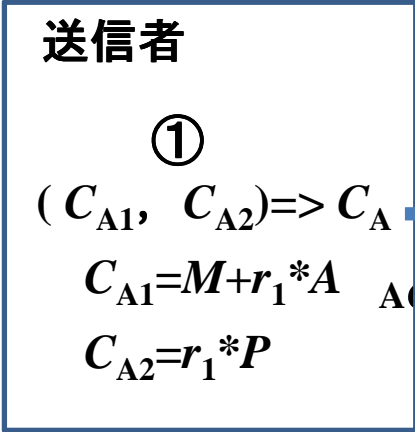
< 実証実験/紹介活動からの知見 > 組織暗号の活用展開に向けて必要なこと

- (1) 自治体・医療機関関係者への精力的な紹介活動の継続
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
- (2) 組織暗号実装支援環境整備への注力
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
- (3) 自治体・医療機関における組織暗号利用の関係省庁への説明
新たな技術、組織暗号活用に対する
関係省庁のご理解・ご支援が必須
- (4) 個人情報を取り扱う多様な場面での保護ニーズへの対応
暗号化状態処理、秘密分散状態処理の研究開発企画・推進

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。関係各位に感謝する。

終



送信側組織

受信側組織

送信側組織

送信者

①
 $(C_{A1}, C_{A2}) \Rightarrow C_A$
 $C_{A1} = M + r_1 * A$
 $C_{A2} = r_1 * P$

Aの公開鍵

管理者S (システム管理者)

Bの公開鍵による暗号文
 $(C_{B1}, C_{B2}) \Rightarrow C_B$

③
 $C_{A1} - X_{AB} \Rightarrow C_{B1}$

⑤

による暗号文

X_{AB}

C_{B2}

メンバA (受信代表者、転送者)

②
 $a * C_{A2} - r_2 * B \Rightarrow X_{AB}$

C_{A2}

④
 $r_2 * P \Rightarrow C_{B2}$

a はAの秘密鍵
 B はメンバBの公開鍵
 P はベースポイント
 r_2 はメンバAが生成する乱数

メンバB (利用者、復号者)

$C_B = (C_{B1}, C_{B2})$

⑥
 $C_{B1} - C_{B2} * b \Rightarrow M$

b はBの秘密鍵

受信側組織