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

才所 敏明*　　近藤 健*　　庄司 陽彦*　　五太子政史*

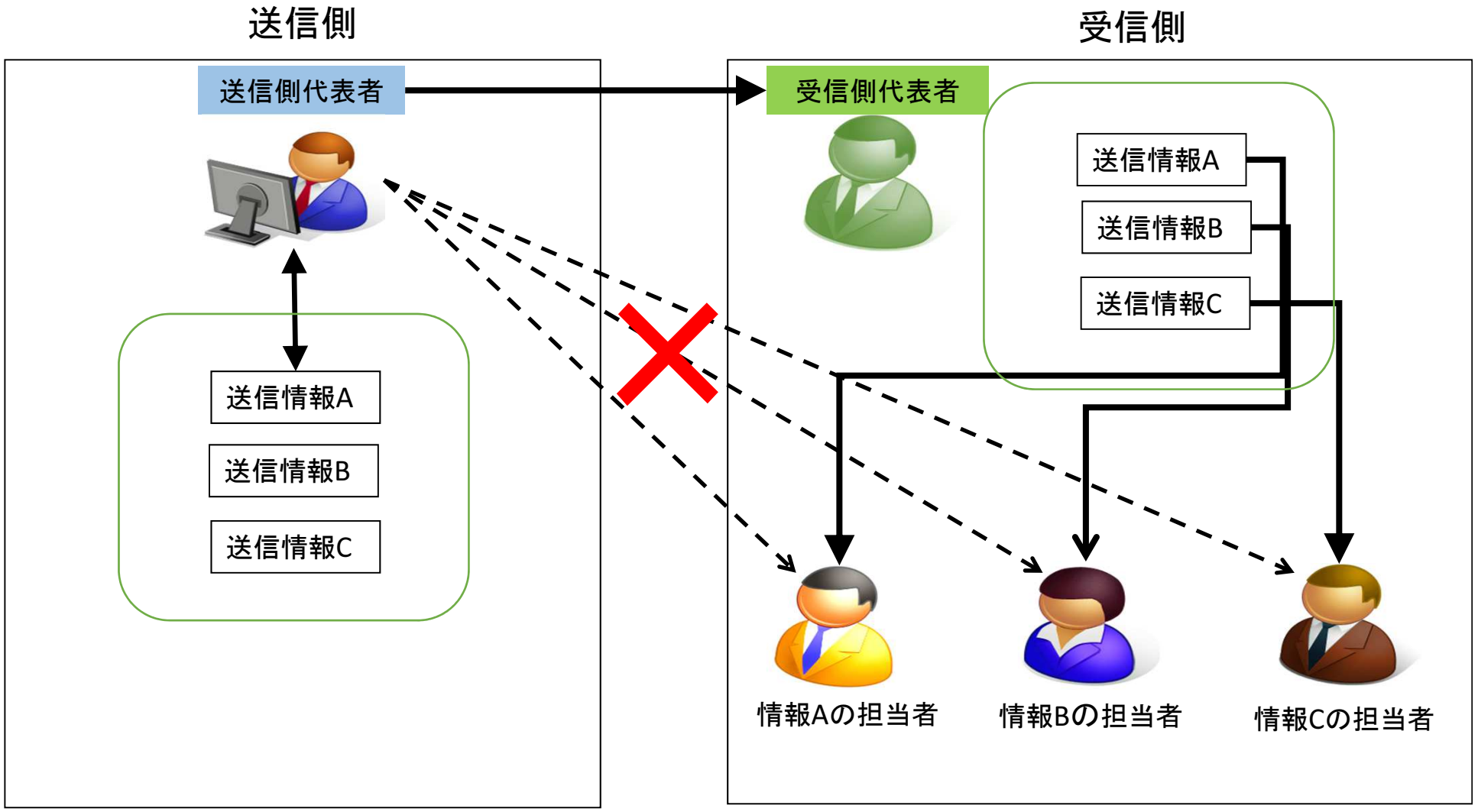
沼田 秀穂†　　仙石 正和†　　辻井 重男*

＊中央大学　研究開発機構　　†事業創造大学院大学

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
送信側代表者
受信側代表者
送信情報A
送信情報B
送信情報C
送信情報A
送信情報B
送信情報C
情報Aの担当者
情報Bの担当者
情報Cの担当者

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

配信中の機密情報保護のための暗号技術

　　従来の暗号方式では、

　　　　送信者が受信者（復号者）を特定し暗号化

　　　　受信者が暗号化機密情報を転送する場合

　　　　　一旦復号し、新たな受信者向けに暗号化が必要

　　組織暗号方式では、受信者が復号することなく、

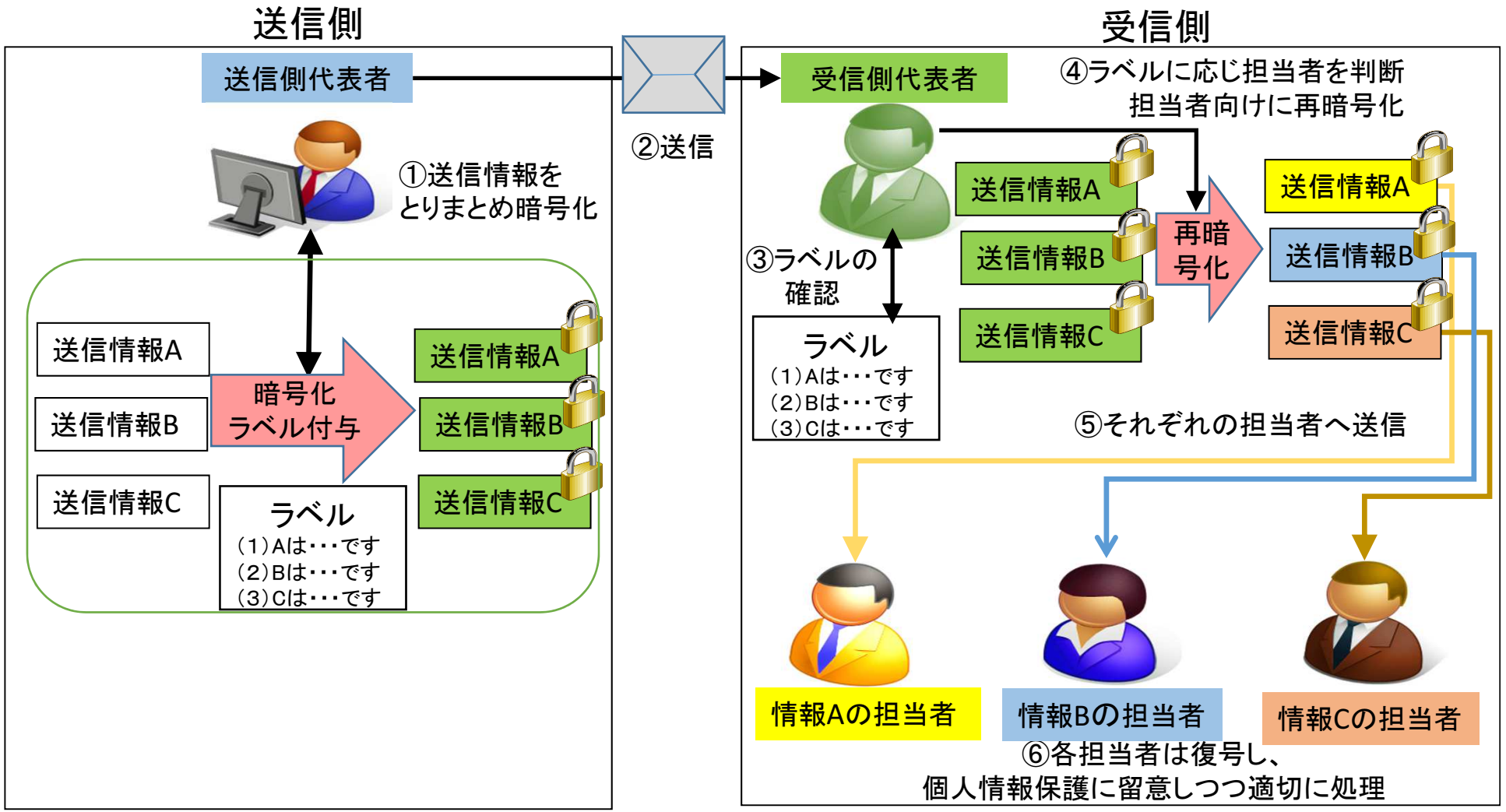
　　　　　新たな受信者向けの暗号化が可能

　　　　受信組織内を機密情報が転々と転送される場合も

　　　　　転送者は、都度復号することなく、

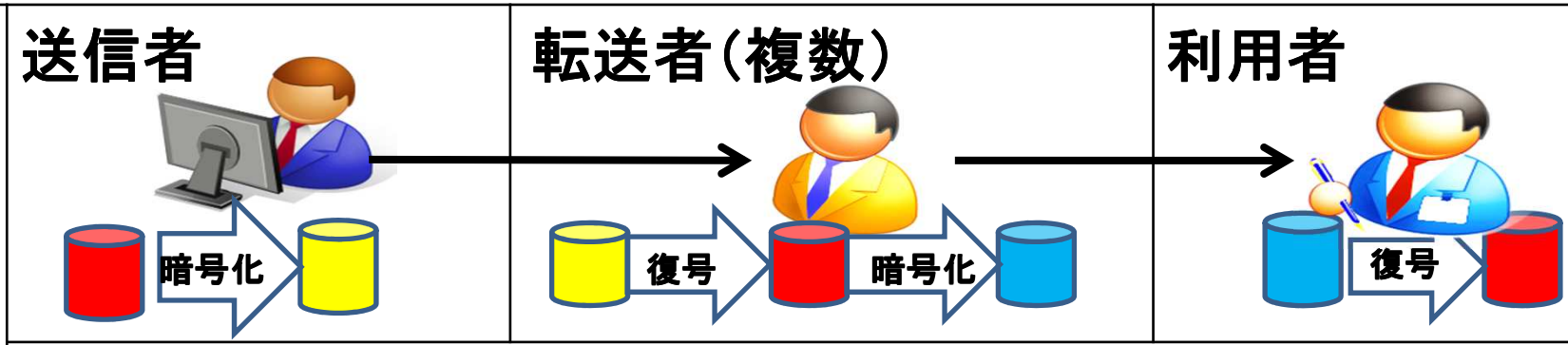
　　　　　機密情報を暗号化状態のまま転送可能

組織間通信と組織暗号


送信側
送信側代表者
①送信情報を
とりまとめ暗号化
送信情報A
送信情報B
送信情報C
暗号化
ラベル付与
送信情報A
送信情報B
送信情報C
ラベル
（1）Aは・・・です
（2）Bは・・・です
（3）Cは・・・です
②送信
受信側
受信側代表者
④ラベルに応じ担当者を判断
担当者向けに再暗号化
③ラベルの
確認
ラベル
（1）Aは・・・です
（2）Bは・・・です
（3）Cは・・・です
送信情報A
送信情報B
送信情報C
再暗
号化
送信情報A
送信情報B
送信情報C
⑤それぞれの担当者へ送信
情報Aの担当者
情報Bの担当者
情報Cの担当者
⑥各担当者は復号し、
個人情報保護に留意しつつ適切に処理

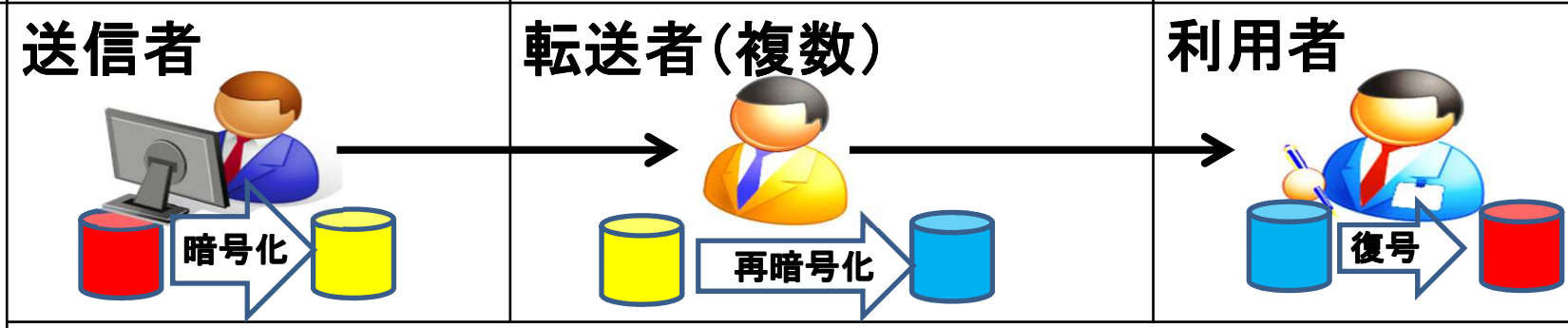
組織暗号の安全性

従来の暗号方式



転送者は機密情報を、**一旦復号する（平文に戻す）必要**が有り、
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



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

組織暗号

組織暗号は，

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―」の活動の一環として、

中央大学研究開発機構が研究開発を進めている暗号方式。

楕円エルガマル暗号

受信者A向けの暗号化と受信者Aによる復号の例

［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$M= M_1'-M_2'*a$

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：$b*P(=B)$

［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$M=M_1''-M_2''*b$

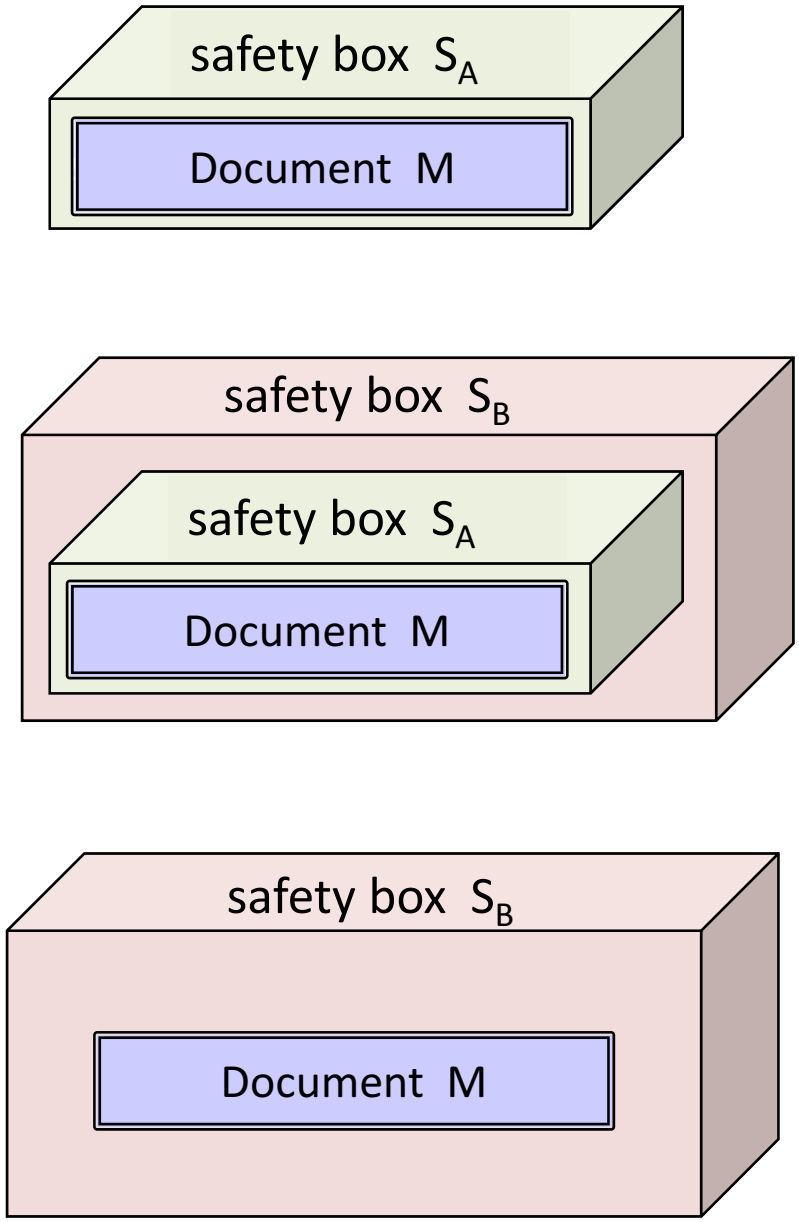
1) 文書Mを金庫S_Aに入れる

2) 文書Mの入った金庫S_Aを金庫S_Bに入れる

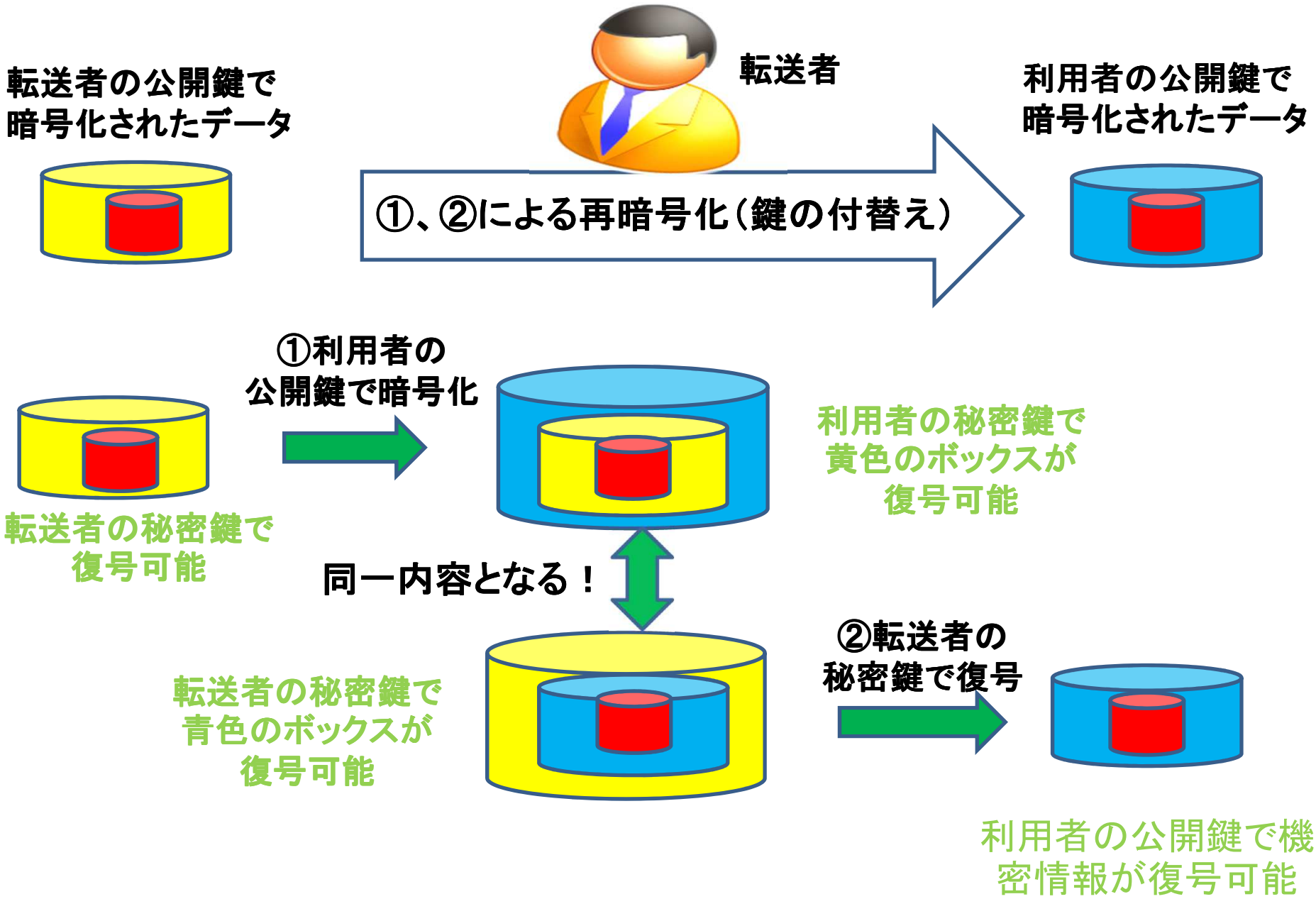
3) 金庫S_Bを開けずに、金庫S_Aを抜き去ることが出来る

これは、マジックか当然か？

楕円暗号だから可能
RSA暗号では不可能



転送者における再暗号化（鍵の付替え）のイメージ



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:

自治体職員の方々へ、直接、組織暗号の説明を実施

自治体の現地で、組織暗号応用システムのデモを実施

組織暗号のデモでは、自治体職員の方々に操作を依頼

具体的業務例を自治体に提示いただき、

組織暗号適用方式を提案、

適用が容易であることをご理解いただく

実施場所: 長野県大町市役所、長野県上伊那郡箕輪町役場

新潟県燕市役所

大町市役所での実証実験

２０１４年１０月１５日

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。

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。

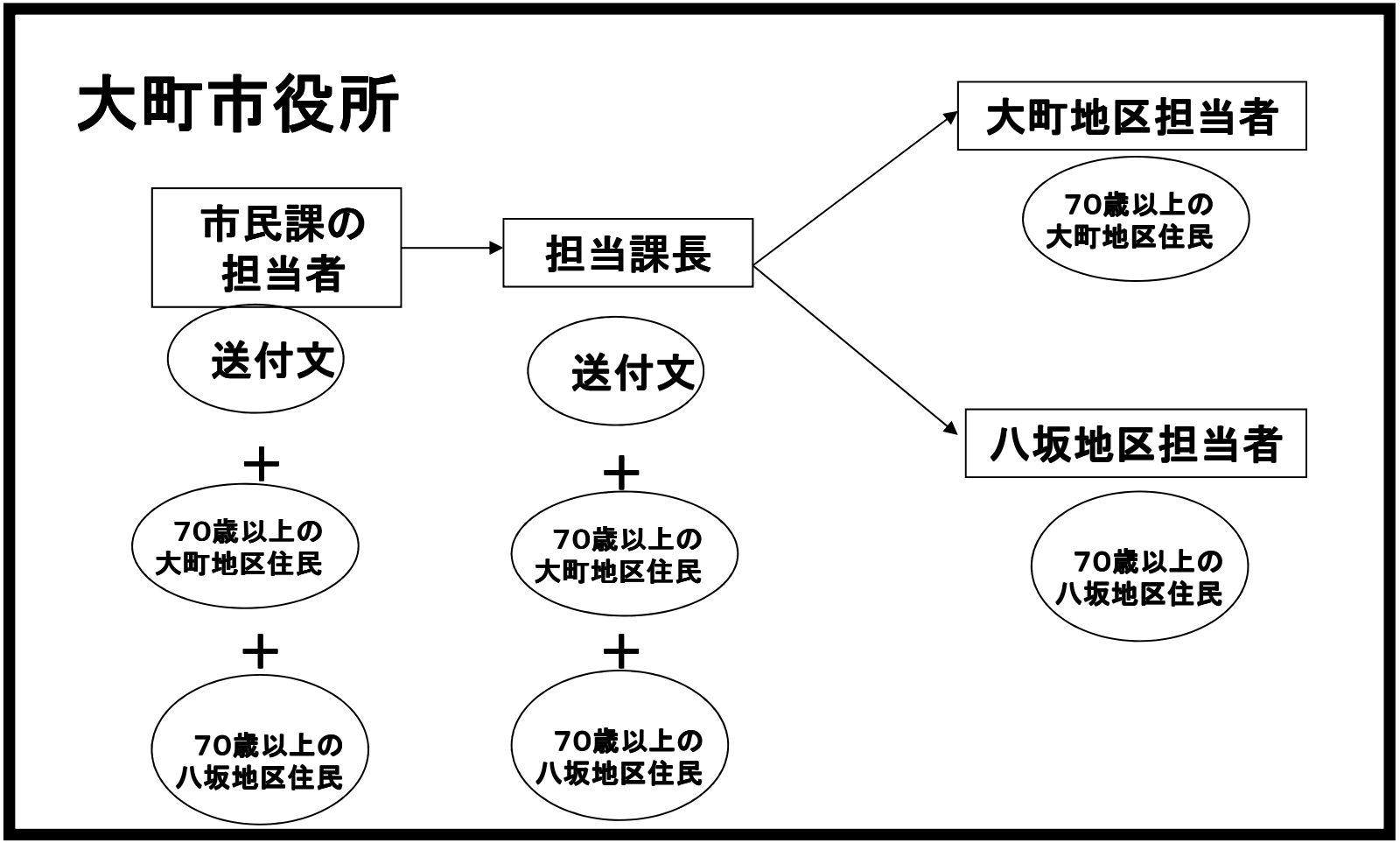
⑤組織暗号応用システムの操作実験

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、
大町市役所のパソコンから市役所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。
操作は市役所の方々に担当いただいた。

⑥質疑応答

想定業務：敬老会招待リスト作成作業

個人情報を含むデータを
担当課長経由で担当者へ送信



個人情報を含むデータを
担当課長経由で担当者へ送信

市民課の担当者

送付文	70歳以上の大町地区住民	70歳以上の八坂地区住民

暗号化

送付文	70歳以上の大町地区住民	70歳以上の八坂地区住民

担当課長

送付文	70歳以上の大町地区住民	70歳以上の八坂地区住民

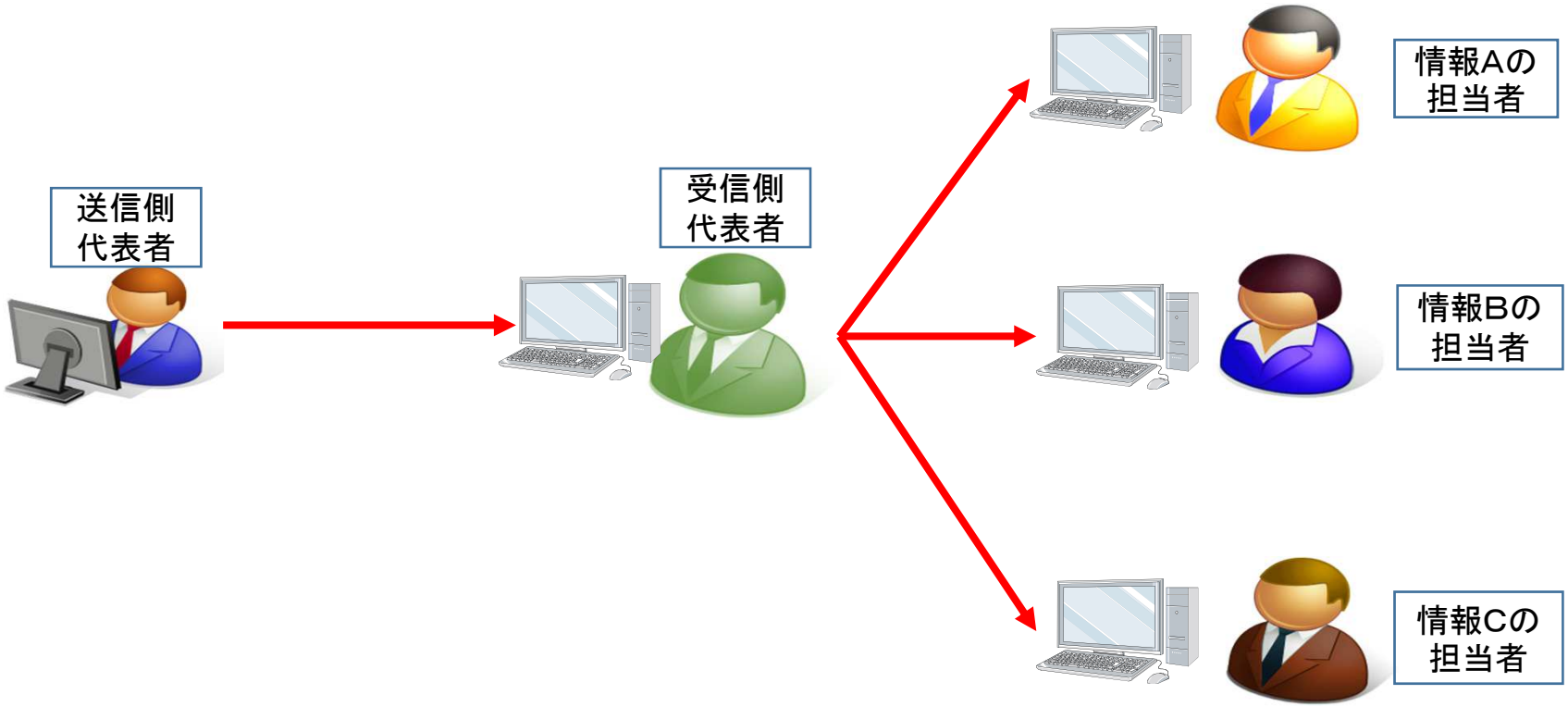
再暗号化

70歳以上の大町地区住民	70歳以上の八坂地区住民

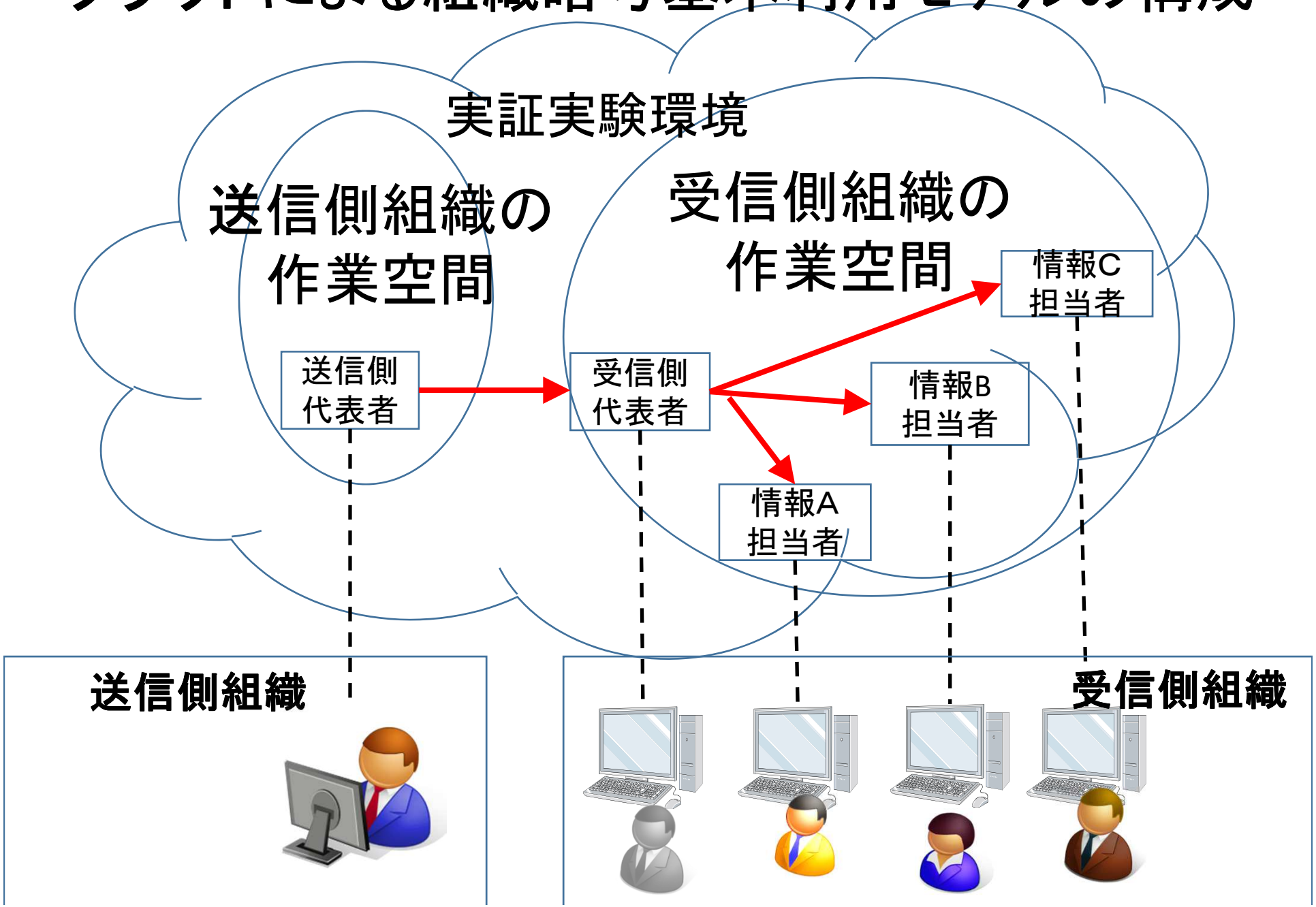
大町地区担当者

八坂地区担当者

PCによる組織暗号基本利用モデルの構成



クラウドによる組織暗号基本利用モデルの構成



実施状況・結果

参加者：約20名

大町市役所の職員の方々

北アルプス広域連合の職員の方々，

報道関係者の方々

中日新聞、大糸タイムズ、大町ケーブルテレビ

質疑・コメント：

鍵長は？　（192ビット）

担当外の暗号化データの復号は？

復号せずに鍵の付替えが可能な，

組織暗号再暗号化の機能に，大変驚いた，とのご意見

大町ケーブルテレビ
10月22日～28日
1日6回放映（1分8秒）

中日新聞　2014年10月16日

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十五日、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。自治体が外部から暗号化されて受け取った情報を役所内の部署へネットを通じて届ける際にも暗号化されたまま送ることができ、情報漏えいを防止することができるという。

この日は、研究の中心になっている中央大・研究開発機構の辻井重男教授らが技術の内容を説明。市職員が、住民基本台帳のデータ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

個人情報がネット上でやり取りされる例が増えることも予想され、辻井教授は「さまざまな場面で情報が漏えいするすきを減らしていくことに役立つ」と話していた。

（吉田幸雄）

大糸タイムズ　2014年10月16日

個人情報保護に「組織暗号」

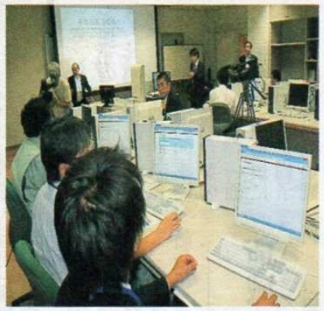
大町市　導入向け県内初実証実験

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を保護する技術について、実際に業務に即した作業を試した＝写真。

行政の業務ではさまざまな個人情報を共有する必要がある。これまでの暗号化技術では、業務担当者が必要な情報を取り寄せる際に途中で暗号化を解く（平文化）必要があり、誤った人に情報が伝わるなど配信途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」データを用い、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、配信途中の情報漏えいを防ぐことができる。税滞納の督促や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、北アルプス広域連合、中央コリドー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が取り入れる「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構の辻井重男教授は「中を開かずに、封筒の宛先を変える技術。プライバシーと効率化の間で賛否両論あるが、行政の効率化は年金の確実な支給など生存権に関わる問題」と述べた。

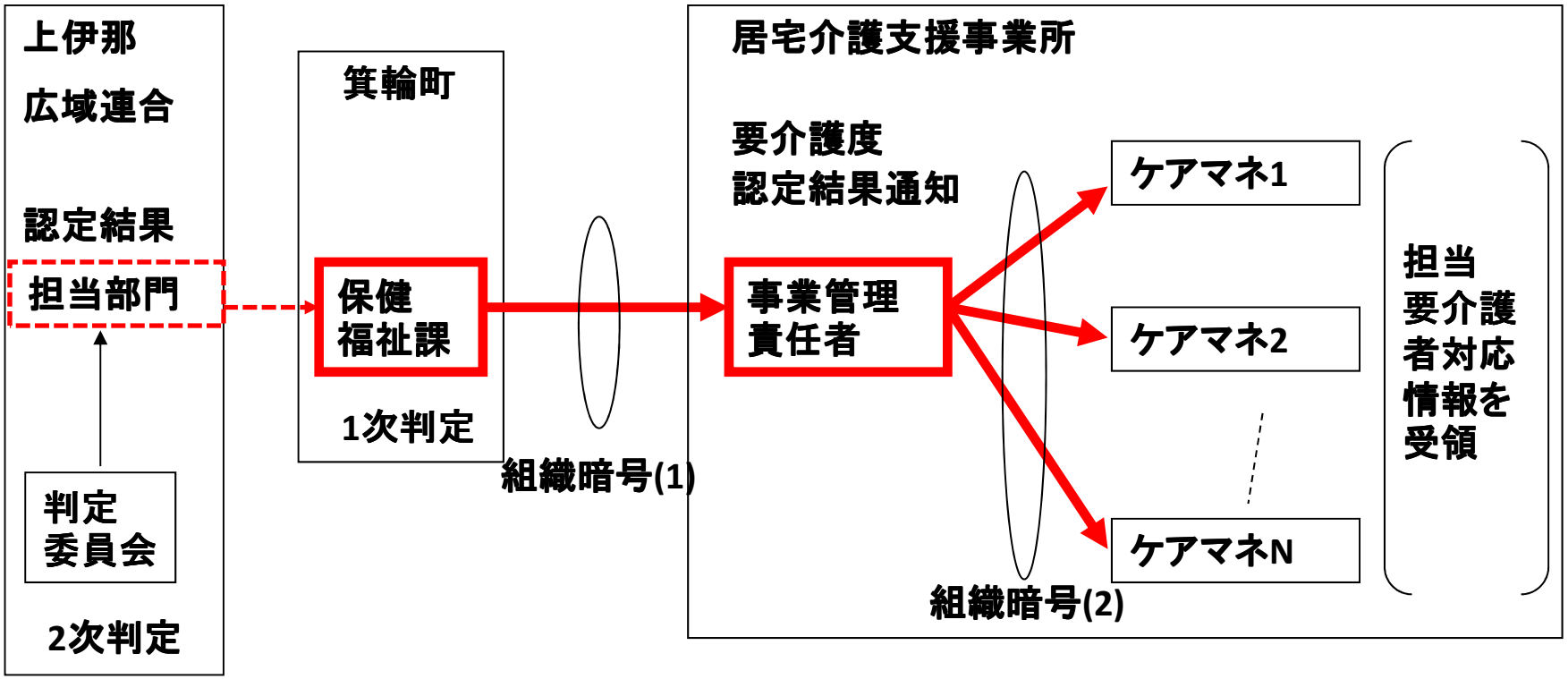
箕輪町役場での実証実験

２０１４年１１月７日

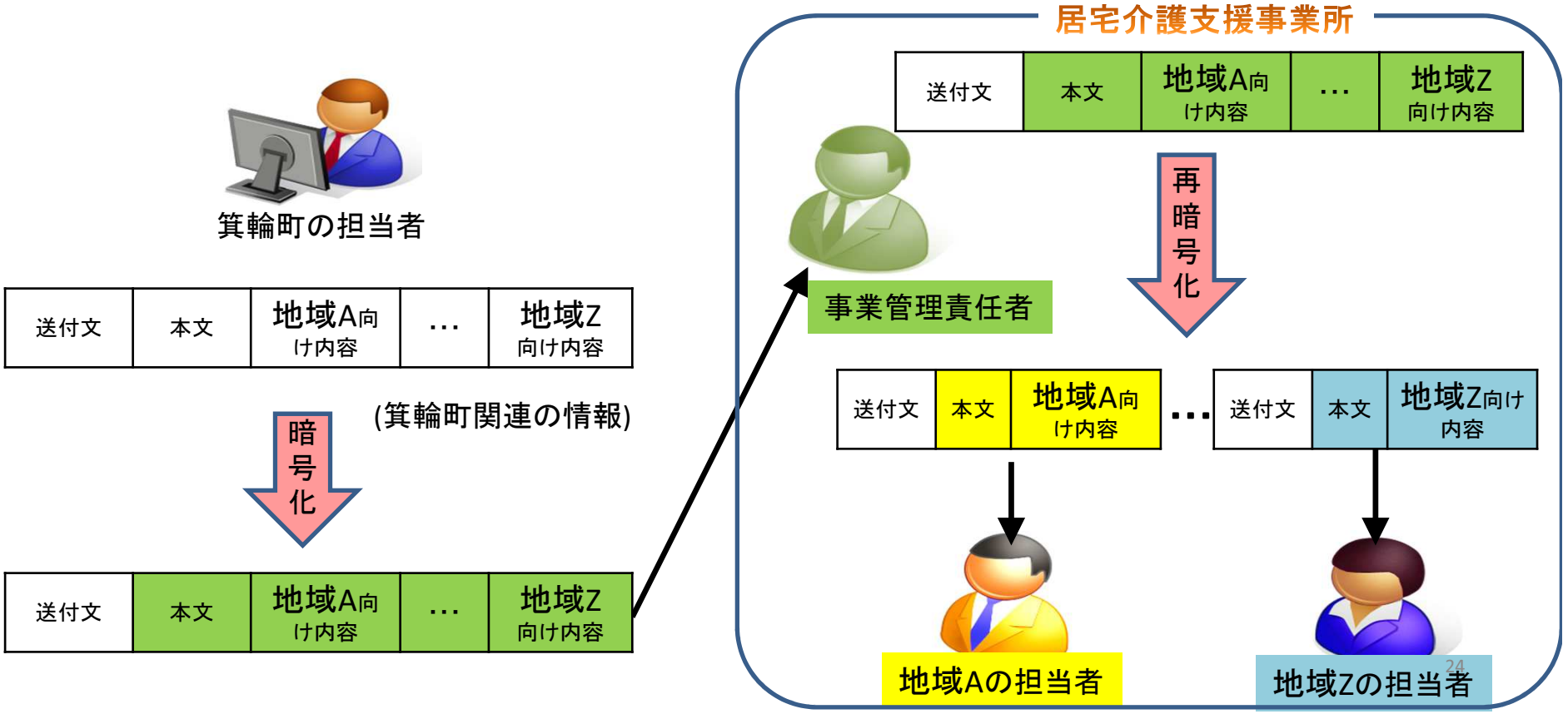
①挨拶（箕輪町役場および中央大学）
②組織暗号に関する説明（大町市役所と同じ内容）
③組織暗号を活用可能な自治体の業務例紹介
　組織暗号が活用可能な個人情報を取り扱う自治体の業務例の紹介、
　　および箕輪町役場での想定業務例の紹介
④箕輪町役場の想定業務への組織暗号適用案紹介
　③で紹介した箕輪町役場の想定業務例に対し、
　組織暗号の具体的な適用案を紹介
　個人情報の送信者から個人情報を直接処理する担当者まで、
　暗号化された状態で配信できることを説明
⑤組織暗号応用システムの操作実験
　パブリッククラウドサービスAWS上に構築された操作実験環境を、
　持込みパソコンから箕輪町役場のネットワーク経由アクセス、
　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
　なお、箕輪町役場の方々に操作を依頼
⑥質疑応答

組織暗号を利用する箕輪町想定業務検討

自治体から外部組織への個人情報受け渡しを伴う業務行う場合
要介護度認定結果通知送付の場合(現在紙ベース)



町の担当者から
居宅介護支援事業所宛に送信



実施状況・結果

参加者：約20名

箕輪町役場の職員の方々
上伊那広域連合の職員の方々，
報道関係者の方々 （みのわ新聞）

質疑・コメント：

メールベースで非常に多く、いちいち再暗号化、転送するのは大変？
実際に使用する場合のサポートなど、商品化は？
小さな組織の役場では、複数の担当者で複数の業務を担当している
個人情報の担当者個人別の分配が現実的か？
現状、他の組織との個人情報のやり取りは少なく、
組織内での個人情報の管理の方が重要だが？
情報漏えい防止のため、専用の閉ざされたネットワークを使用している
それでも、組織暗号は必要か？
転送者が、何のデータかわからない、判断できないこともあるのでは？

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。


デモシナリオ

みのわ新聞

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ー技術の「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を暗号化、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ーの流れを確認した。モデル実験に対し、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。

発行所
〒399-4601 箕輪町松島8752-1
みのわ新聞社
編集・発行人 薩摩 建
電話 代表79・8484
FAX 79・8485
www.shimin.co.jp
E-mail minowa@shimin.co.jp

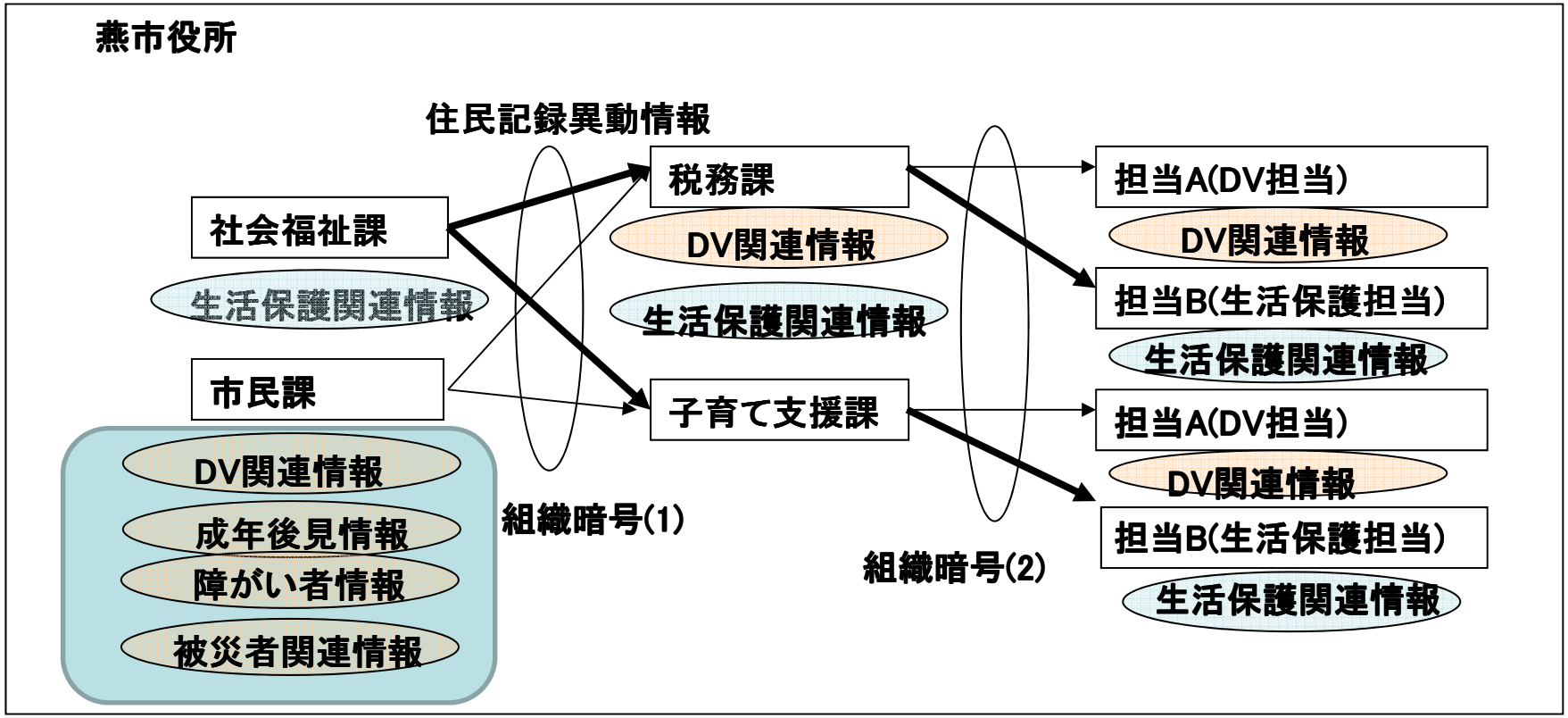
定価1カ月1,420円
1部売り60円 (税込み)
本紙をお届けする販売店
井桁屋新聞店 ☎79・2368
YC箕輪店 ☎72・7455
桑沢新聞店 ☎79・6663
なかむら新聞店 ☎76・9998
中川新聞店 ☎78・8055
萬屋新聞店 ☎73・5303
コンビニもご利用ください

燕市役所での実証実験

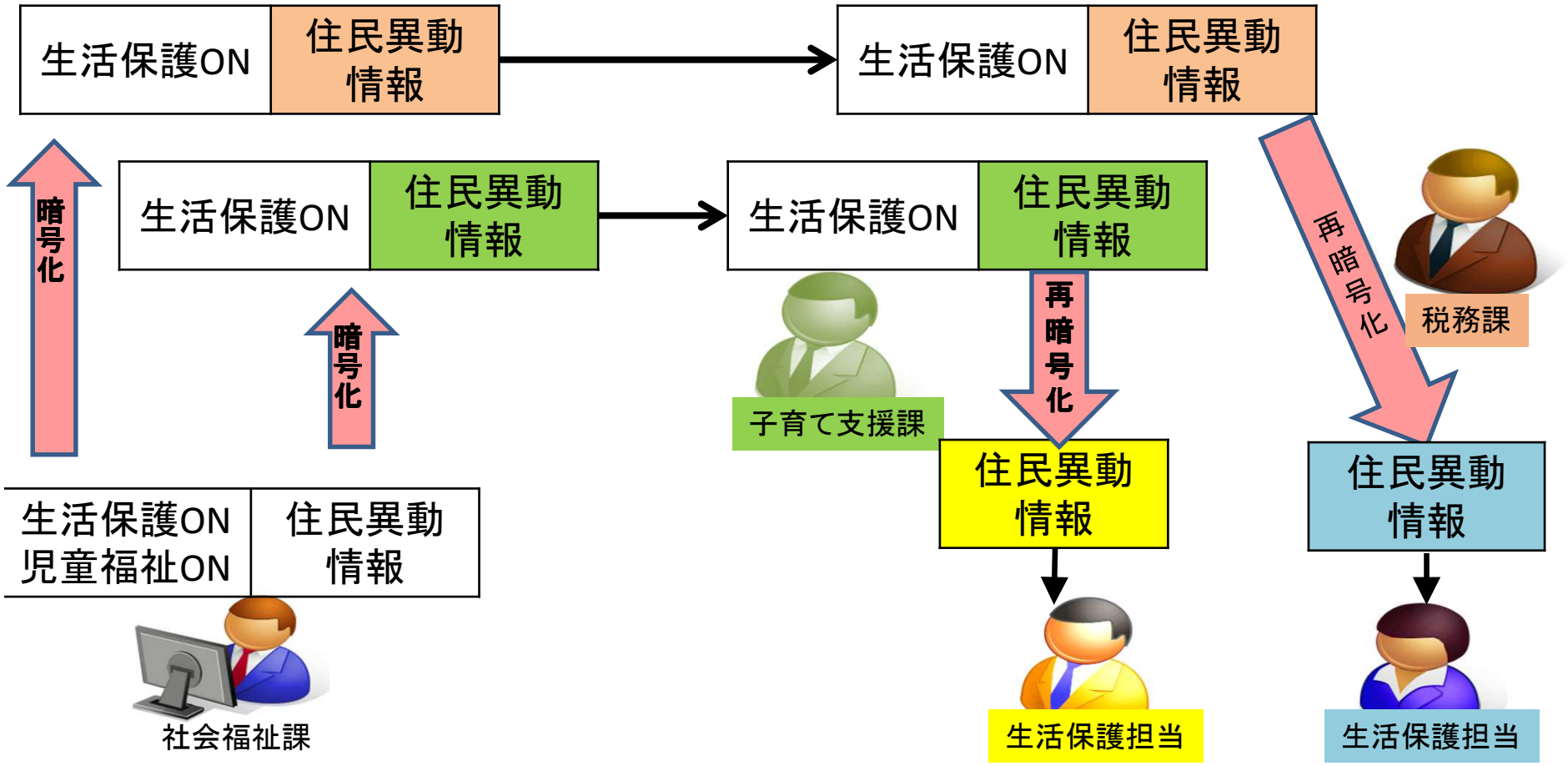
２０１４年１１月２１日

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
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。
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
　なお、操作は市役所の方々に依頼
⑦　質疑応答

住民異動にともなう
国民保険・年金・医療・福祉関連業務



住民異動にともなう
国民保険・年金・医療・福祉関連業務



実施状況・結果

参加者：約２０名

燕市役所の職員の方々
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 （電波タイムズ）

質疑・コメント：

組織暗号における鍵の管理？
組織暗号の商品化は？
現在の市役所の業務実態との関係？
万一、担当者を間違えて再暗号化し、送付した場合は？

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た

昭和25年6月28日第三種郵便物認可
電波タイムズ
The Dempa Times
2014年（平成26年）
11月28日
第6367号
金曜日
月水金曜日発行
（祝日休刊）
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20番1号 電話03(5470)5050 FAX(5470)5051
大阪支社／支局：中部・静岡 http://www.dempa-times.co.jp

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模様

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日に新潟県燕市役所で、組織暗号技術を活用した組織暗号実証実験式を開催した。同様の実験は10月に長野県大町市、箕輪町で行われ成功を収めた。燕市の実証実験はこの2市町での経験を踏まえて行われ、地方自治体などが今後、個人情報を扱う上で重要なものとしている。

挨拶した南波瑞夫燕市副市長は「わが国はユビキタス社会の実現を目指して情報化社会は進んでいるが、実際に情報を使う立場、持っている立場としては、セキュリティ面で個人情報をいかに守っていくか課題であり、行政として個人情報を活用していかなければいけないが、制約もあってリスクもある。ユビキタス社会の実現において、暗号化技術は重要である。燕市は、情報化社会において、職員は全国どこへ行っても携帯内線が使えたり、防災無線の整備、アマチュア無線局を持っていたりと進めている。今回、実証実験に協力することは大変光栄なことである。安心して情報が使える社会に向けて本実験が成果を出せることを期待している」と述べた。

辻井重男中央大学研究開発機構教授、中央コリドー高速実験プロジェクト推進協議会長が挨拶した。

仙石正和事業創造大学院大学学長、NPO法人新潟情報通信研究所理事長は「私どもは新ビジネスの創造などを進めているが、今回、辻井教授からご依頼があって、燕市長さんにお話ししたところ、ご快諾をいただいた。NPO法人新潟情報通信研究所の下坂昇事務局長のご協力もあって、今回実験を行うことになった」と述べた。

中央大学研究開発機構は、平成25年度から3ヵ年計画で、独立行政法人情報通信研究機構（NICT）の委託を受けて、新たな暗号方式「組織暗号」の研究開発を推進している。NPO法人中央コリドー情報通信研究所は、設立以来、ICTによる情報化社会の発展を目的とし、このための大学の研究開発の支援および自治体等の成果の活用による地域の活性化を図る活動を推進。中央大学研究開発推進機構とは過去に電子投票の研究および自治体での応用などで協力してきた。

中央大学研究開発機構、中央コリドー情報通信研究所は、組織暗号がいくつかの自治体でその技術の紹介を行ってきたが、新潟県では、2団体とICT関連技術研究などで連携関係にある事業創造大学院大学、NPO法人新潟情報通信研究所が同様な活動を行っており、今回、協力依頼を行った。

近年、個人情報の保護強化が話題になる中、新潟県内の自治体で組織暗号の実証実験を行うこととなり、燕市の快諾を得たことから、市役所と4団体が連携して行ったもの。同市は、住民の個人情報保護と、個人情報の利活用による住民サービス向上の両立に意欲的に取り組んでいる。

従来型では特定の"鍵"で復号（平文に戻す）できる暗号化情報であるものを、組織暗号は復号することなく、任意の別の鍵で復号できる暗号化情報へ変換（再暗号化）できるもの。つまり、従来方式では、暗号化情報を別の鍵へ切り替えるたびに復号が行われ、個人情報漏えいのリスクが大きくなる。組織暗号は、平文に戻すことなく、暗号化情報を復号できる鍵を切り替えることができ、この暗号方式を組織間の通信に用いることで組織内外での個人情報の配信過程での情報漏えいが防止できる。

実験を行う前に「暗号ー情報セキュリティの技術と歴史ー、組織暗号ー情報漏洩とマイ・ナンバー導入に備えてー」と題して講演を行った辻井氏は同氏が著した「暗号 情報セキュリティの技術と歴史」（講談社学術文庫）の内容を中心に説明した。

続いて「組織暗号ー自治体での活用可能な業務例ー」を近藤健NPO法人中央コリドー情報通信研究所事務局長が説明した。

続いて「組織暗号ー燕市想定業務例ー」を沼田秀穂事業創造大学院大学教学担当副学長が説明した。

続いて「組織暗号ー燕市想定特定業務への適用案および実証実験の構成・内容紹介ー」を才所敏明中央大学研究開発機構研究員が行った。

◇

実証実験に入って、実験システム動作説明を庄司陽彦中央大学研究開発機構研究員が行って、実験は成功した。デモシナリオは「保険年金課の管理者は、後期高齢者への医療通知を行うために、後期高齢者医療広域連合の後期高齢者医療担当部門へ医療通知書の提供を依頼したい。後期高齢者医療担当部門の管理者は、保険年金課の管理者より依頼を受けた、医療通知書の提供を行うが、閲覧する人は最小限にしてもらいたい。保険年金課の担当者は、担当地域の市民への通知業務を行うため、保険年金課の管理者より医療通知書を提供してもらいたい」。例えば、後期高齢者医療担当部門操作では、組織暗号で暗号化を行い、保険年金課の管理者に送る。後期高齢者医療担当部門の管理者は、データを閲覧する担当者を意識せずに暗号化が行えるものだ。また、保険年金課の管理者操作は、組織暗号で鍵の付け替えを行い、各文書を適切な担当者に送るものだ。保険年金課の担当者操作は、組織暗号で復号を行い、適切な担当者のみが復号するものだ。

◇

4団体は今後、実証実験や意見交換を通し、燕市などの自治体業務における個人情報の取り扱いの現状やマイナンバーへの対応に関する動向を把握、組織暗号の適切な利用に関し知見を深め、自治体での組織暗号の実用化に向け活動を展開する計画だ。

＜　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）マイナンバー対応への戸惑い
（８）先進的技術の独自採用は困難

＜　実証実験からの知見　＞
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）自治体向け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）自治体業務における組織暗号利用の関係省庁へのご説明

自治体の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，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.

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.

終