組織暗号 利用の手引き

―情報漏洩とマイ・ナンバー導入に備えて―

２０１４年７月

中央大学研究開発機構

辻井重男研究ユニット

本提案の背景

２０１４年７月、世間に大きな衝撃を与えたベネッセ（株）関連企業からの数千万件に上る個人情報漏洩事件は、我々に、これまでの情報セキュリティ対策のあり方に対して、根本的な変革を迫っています。

また、２０１６年度から始まるマイ・ナンバー・システムの導入は、行政基盤や国民の生活基盤として不可欠である反面、個人情報保護について、自治体などが抜本的な対策を立てることの緊急性を高めています。

これまでの情報セキュリティ対策は、どちらかと言うと、ネットワーク防御・境界防御に力点が置かれていました。しかし、最近の情報漏洩の特徴は組織内部の管理者などによる漏洩件数は増大にあります。このことは、米国ＣＥＲＴのレポートなどに明確に現れています。漏洩件数の増大もさることながら、１件当たりの被害金額が大きいことも、内部不正・犯罪の特徴です。いくら外堀を深くしても、あるいは、外壁を高くしても、内部者の裏切りには効果がありません。

「万里の長城、胡を防がず」、明王朝は、内部から崩壊して、清朝に覇権を奪われました。

これからは、境界防御と合わせて、情報システムの本丸、即ち、データベースを暗号化して守ることが決め手となるでしょう。１９９０年代、暗号は、軍事・外交だけでなく、情報社会にも有用なのか、という興味から、世間の関心を集めました。当時、情報セキュリティはそれほど深刻な課題ではなかったこともあり、情報セキュリティ＝暗号　の感がありました。その後、署名・認証や伝送情報の秘匿等への暗号の利用が進むにつれて、新技術の宿命として、世間の関心は薄れてしまいました。

現在、情報システム技術者でも暗号に対する知識が十分でなく、誤った利用により情報システムの脆弱性を招いている場合も少なくありません。

２０１１年頃からの標的型攻撃や内部不正・犯罪の増大に備えて、今後は、データ自体の暗号化と、一旦暗号化された情報の復号（平文に戻すこと）を必要最小限に抑えること、即ち、暗号化状態処理方式が重要なシステムとなります。例えば、クラウドのデータベースに暗号化して預けた機密データに対して統計処理を行う場合、一旦、復号（暗号文を平文に戻うこと）して統計処理し、再

度、暗号化することは、効率性の面からも情報漏洩の面からも好ましくありません。このため、暗号化した状態のまま、加算や乗算を行うことにより統計処理を行う方式の研究が進められています。

本提案も、このような暗号化状態処理の一つであり、今後、急増すると予想される電子化文書の送受信に対応するシステム提案です。送信側組織の担当者が、受信側担当者を判断できる場合は、その担当者に送れば済みますが、そうでない場合や、組織の代表者に送ることが望ましい場合も少なくありません。現在、郵便ベースで、文書を送る場合、受信側代表者（例えば、総務部長）は、封を切り、内容を大まかに判断して、担当者を定め、再び封をして、その担当者に転送しています。

本文では、今後の電子化文書の増大に備えて、暗号化状態のまま、情報漏洩を防ぎつつ、効率的な組織内転送を行うシステムを提案するものです。インターネットを利用できる環境であれば、導入される組織内でのシステム構築・変更は全く必要ありません。全ての処理はクラウドに行わせます。

提案する組織暗号の概要

最近、文書の電子化が進み、自治体や医療・介護ネットワークなどの組織間での機密通信が増大しています。２０１６年度からマイ・ナンバーが導入されれば、組織間の情報通信は益々普及するでしょう。

個人間通信と異なり、組織間通信では、送信情報の正確性に加えて、個人情報保護や企業秘密保護の観点から、機密性確保への要請が高まっています。

組織間通信における機密保護のため、軍事・外交分野では、暗号通信が昔から利用されて来ました。しかし、うっかり（あるいは止むを得ず）平文に戻したために、大事を招いたことは枚挙に暇がありません。１９１７年、第１次世界大戦への米国の参戦は、ドイツから在メキシコ・ドイツ大使館に送る暗号電文が、一旦、アメリカ大使館で平文に戻されたことがきっかけとなりました。

組織は、その大きさや形態などさまざまですが、一般に、送信者が、受信側組織の担当者を知っている場合には、従来の郵便・電子メールと同様に、直接担当者に送ればよいでしょう。そうでない場合、送信者は、受信側組織の代表者（例えば、自治体や企業などの総務部長や庶務課長、病院の事務局長など）宛てに、暗号化文書を送ることになります。受信側組織の代表者は、一旦、それを復号（平文に戻すこと）して、組織内の誰が担当かを判断し、その担当者に転送することになります。その担当者以外の人が、その文書の内容を知ることは、個人情報保護の点などから、好ましくない場合が多いので、この組織内転送にも機密性が求められます。

多くの場合、受信側代表者は、受信文書全体を見なくても、例えば、ラベルなどのメタデータを見るだけで、誰が担当者か判断できます。

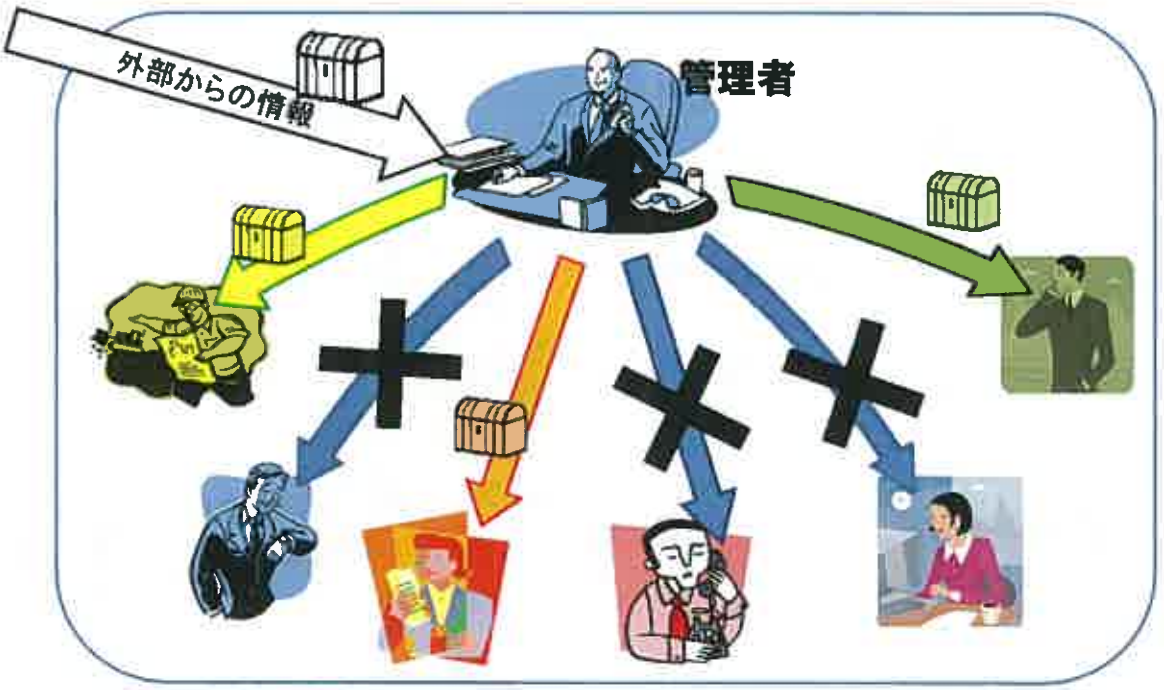


図 1: 外部から送られた機密情報の組織内での分配

以上のような背景の中で、本提案では、情報漏洩の機会と受信側代表者の手間を大幅に減らすような組織暗号を提案することと致します。電子自治体の先導者である井堀幹夫東京大学高齢社会総合研究機構（IOG）特任研究員（元千葉県市川市ＣＩＯ）からは

「組織暗号なくして電子行政なし」

と評価して頂いております。

１．　組織暗号とは

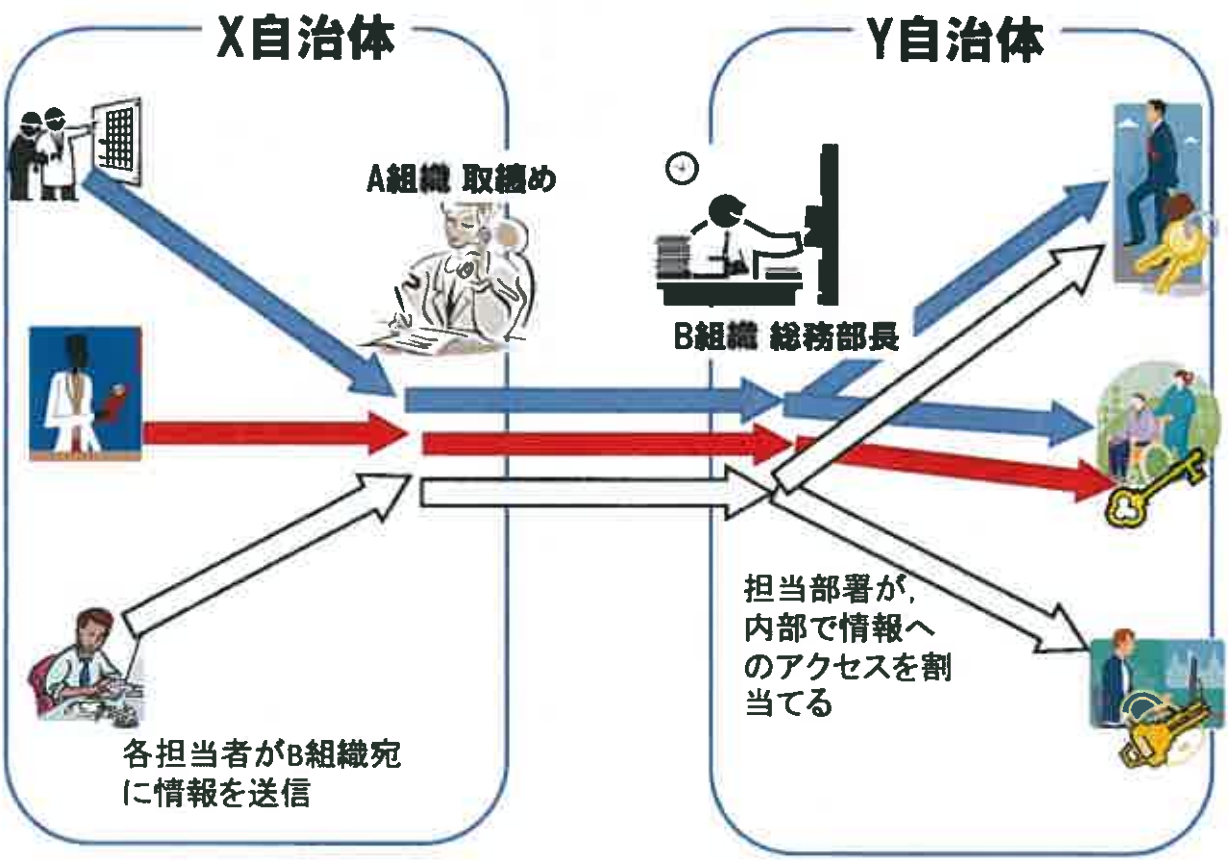


図 2: 組織間通信でのアクセス許可振分けの方式

送信者が送ろうとする機密文書の内容は、１つの場合も、複数の場合もあるでしょうが、ここでは、複数の場合について考えます。例えば、Ｘ自治体からＹ自治体へ

目次

第１章　Ａ氏の医療情報
第２章　Ａ氏の資産情報
第３章　Ｂ氏の医療情報
第４章　Ｂ氏の資産情報

と送る場合について考えて見ます。

Ⅰ　送信側（Ｘ自治体）の処理手順

１） Ｘ自治体では、Ｆ庶務課長が送信者となるものとする。

２） Ｙ自治体では、Ｇ庶務課長が受信代表者となるものとする。

３） Ｘ自治体のＡ氏の医療情報、Ａ氏の資産情報、Ｂ氏の医療情報、Ｂ氏の資産情報の各々の担当者は、それぞれの個人情報を暗号化し、Ｆ庶務課長に伝送する。

４） Ｆ庶務課長は、目次を次のように作成し、その暗号文を作成する。
第１章　Ａ氏の医療情報、　第２章　Ａ氏の資産情報、
第３章　Ｂ氏の医療情報、　第４章Ｂ氏の資産情報

５） Ｆ庶務課長は、目次、及び、第１、２，３，４章（いずれも暗号化されている）を取り纏めて、Ｇ庶務課長に送信します。

Ⅱ　受信側（Ｙ自治体）の処理手順

１） Ｇ庶務課長は、目次のみを復号し、（平文に戻し）、第１章から第４章をいずれも暗号文のまま、各々の担当者に伝送します。

（第１章　Ａ氏の医療情報　と　第２章　Ａ氏の資産情報の担当者が同一人の場合、あるいは、第１章　Ａ氏の医療情報　と　第３章　Ｂ氏の医療情報の担当者が同一人であることもあり得る）

２）　各担当者は、個人情報保護に留意しつつ、適切に処理します。

以上の手順を図３に示します。

(注) システム技術者向けの暗号方式を含めた具体的なシステム構成の説明については、「組織暗号の実装手順書」を参照してください。

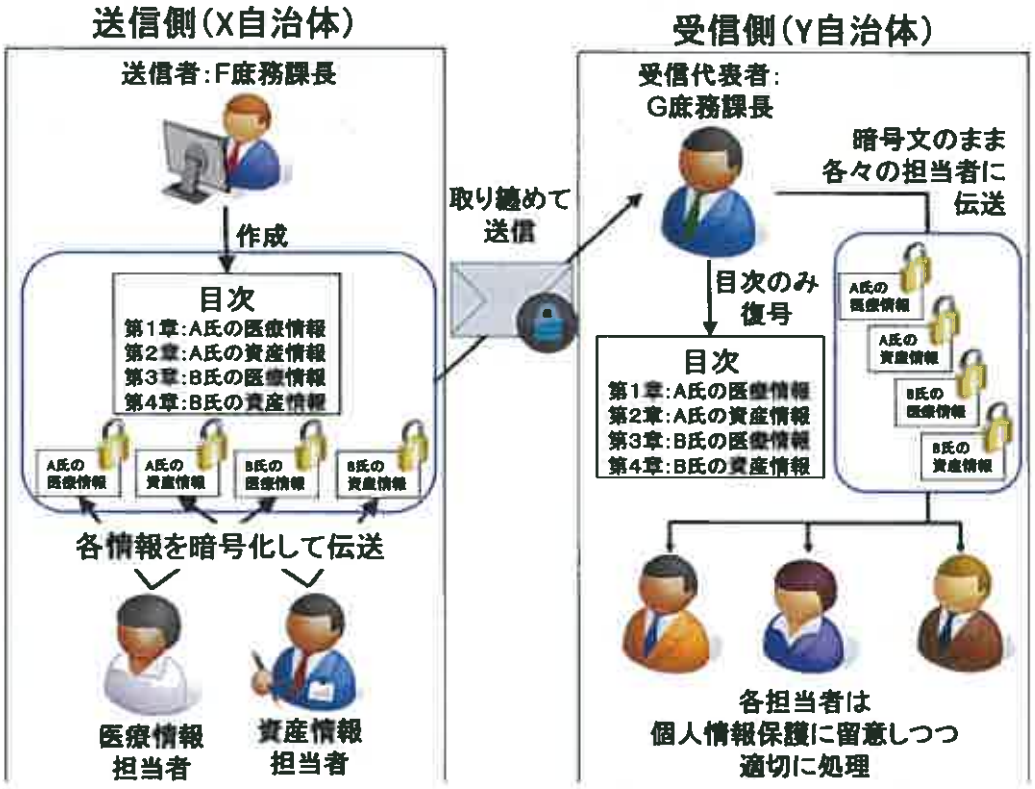
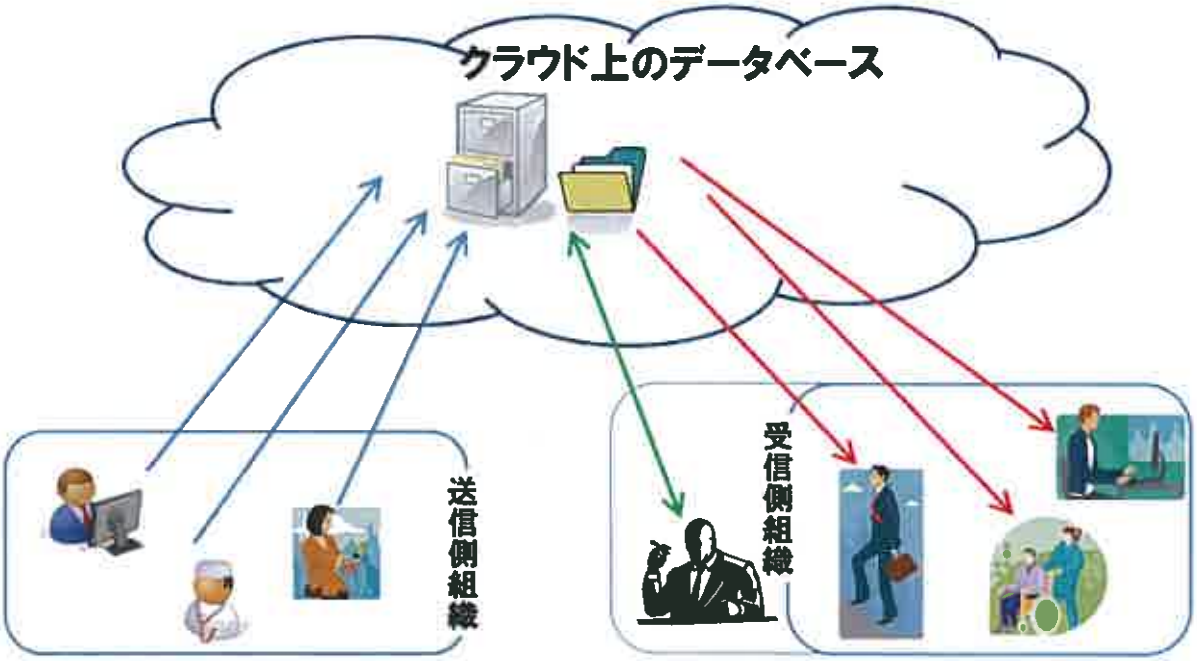


図 3: 組織暗号

これらのシステム操作イメージを図 4 に示す．送受信といっても，例えば自治体 A と B の両方からアクセスできるクラウドシステムの上にデータを上げるという形で運用することになっており，各担当者及びマネージャは基本的にはブラウザや Excel のような通常の Office アプリケーションなどの操作のみで実行できます．



- 送信者は文書を暗号化してサーバーにアップロード
- 受信側管理者はサーバー上で設定を操作する
- アクセス許可設定に従って，受信者は情報をサーバーから受け取る

図 4: 組織間通信でのアクセス許可操作イメージ

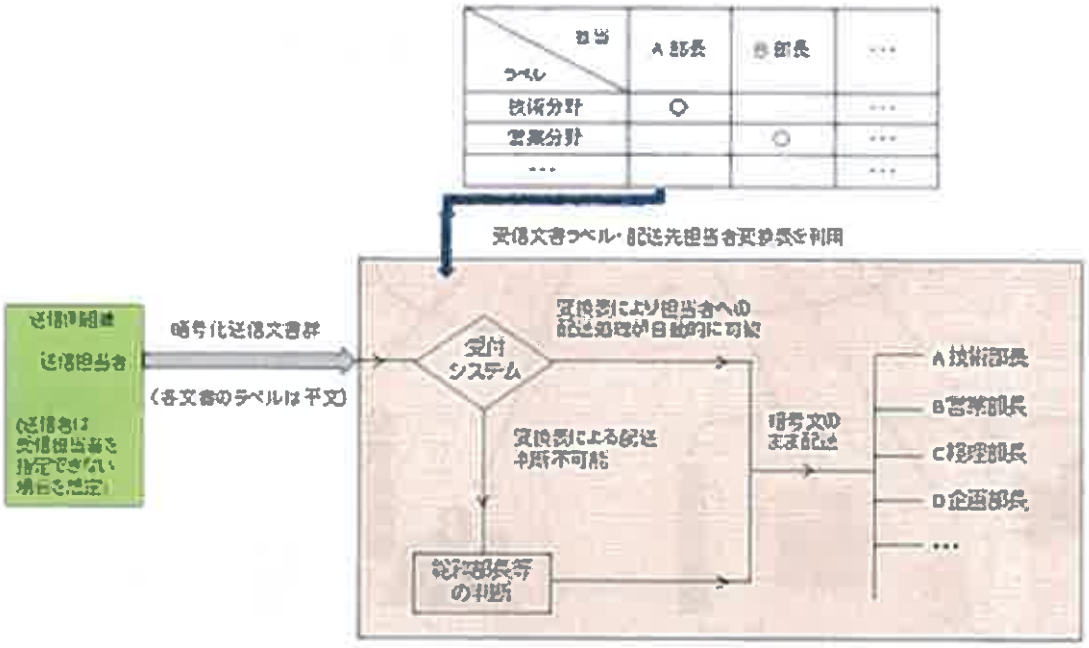


図5　組織暗号(暗号化受信文書を暗号文のまま適切な担当者に配送するシステム)
―文書宛暗号文と担当者宛暗号文に楕円エルガマル暗号を利用して変換する方式―

組織暗号を使用することによる具体的メリットの例

① 個人データ等保護すべきデータを見ることができる人数を必要最小限に限定することができるため、データ漏洩の機会を減少できます.
業務データも担当分しか見ることができません。

事例：民生委員への個人データ配布
担当地区のみのデータ配布へ限定

中野区の例 (別紙参照)
中野区地域支えあい推進室→民生委員・児童委員(266 人)・主任児童委員(25 人)
(福祉必要可能性のある人員の住所、氏名、年齢、性別等)
(高齢者 世帯構成、介護度等)
(障害者 世帯構成、障害等級、部位、種別等)
(妊産婦 重要時、養育困難者)
(低所得者 生活保護世帯)

これらの情報は、地縁団体、警察署、消防署等にも提供されています。

② 個人データの漏洩の恐れのために、従来紙ベース又は電子媒体で一定の場所で引き渡していたものを通信で遠隔配布可能となり、事務の効率化が図れます。
事例 自治体業務の外部業務委託に伴うデータ受け渡し
(1) 沖縄県 奨学金返還案内に係るコールセンター業務委託
滞納状態にある奨学生への返還案内により滞納解消を目指します。
(H26/7/15～H27/3/31)
a. 対象者データの提供
対象者データは、電子媒体を用い、発注者が受注者の事業所に持ち込み、受注者に直接引き渡す。
b. 電話結果の入力および報告書の引き渡し
受注者は、電話結果について発注者の事業所に持ち込み、発注者に直接引き渡す。
(2) 茨城県後期高齢者医療広域連合
平成 26 年度茨城県後期高齢者医療広域連合医療通知書作成業務委託

茨城県後期高齢者医療広域連合が提供するデータから医療通知書を作成印刷、専用封筒に封入封緘したものを指定場所に納品(約 100 万通).

データの受け渡し：

(電子)媒体等の引渡しは広域連合事務所内で行うこととし、配送等を行う場合はセキュリティを強化した方法で紛失、盗難等を防止すること。

③ 通信回線における盗聴を防止できる。

通信回線を使用することにより、情報の紛失、盗難等を防止できます。

④ 情報送信側に受信側組織構成・人員等を知らせる必要がない(知られない).

また、担当者の配置を自由に変更できる等、組織運営に柔軟性を持たせられます。

⑤ 業務担当者の PC 機器等専用化して、その機器でのみ復号可能で、USB 等の外部メモリへの接続はシステム的にできないようしたうえ、万一ベネッセのように外部機器指定漏れ等で接続ができても暗号化された形でしかダウンロードができないようにして、故意・過失の情報漏れを防ぐことができます。

中野区　民生委員への個人情報提供の例を図６に示します。

中野区　民生委員へ個人情報提供の例

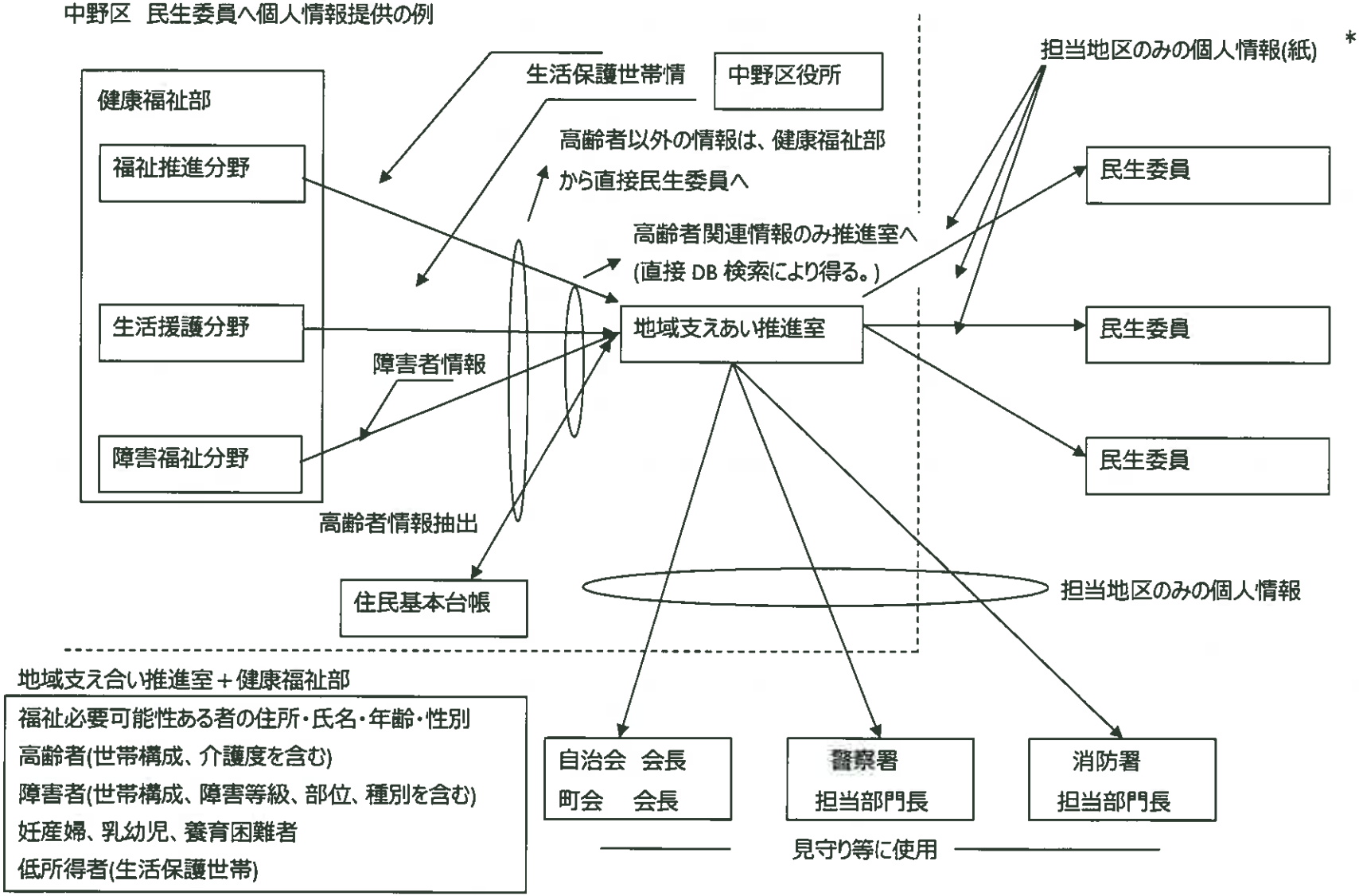


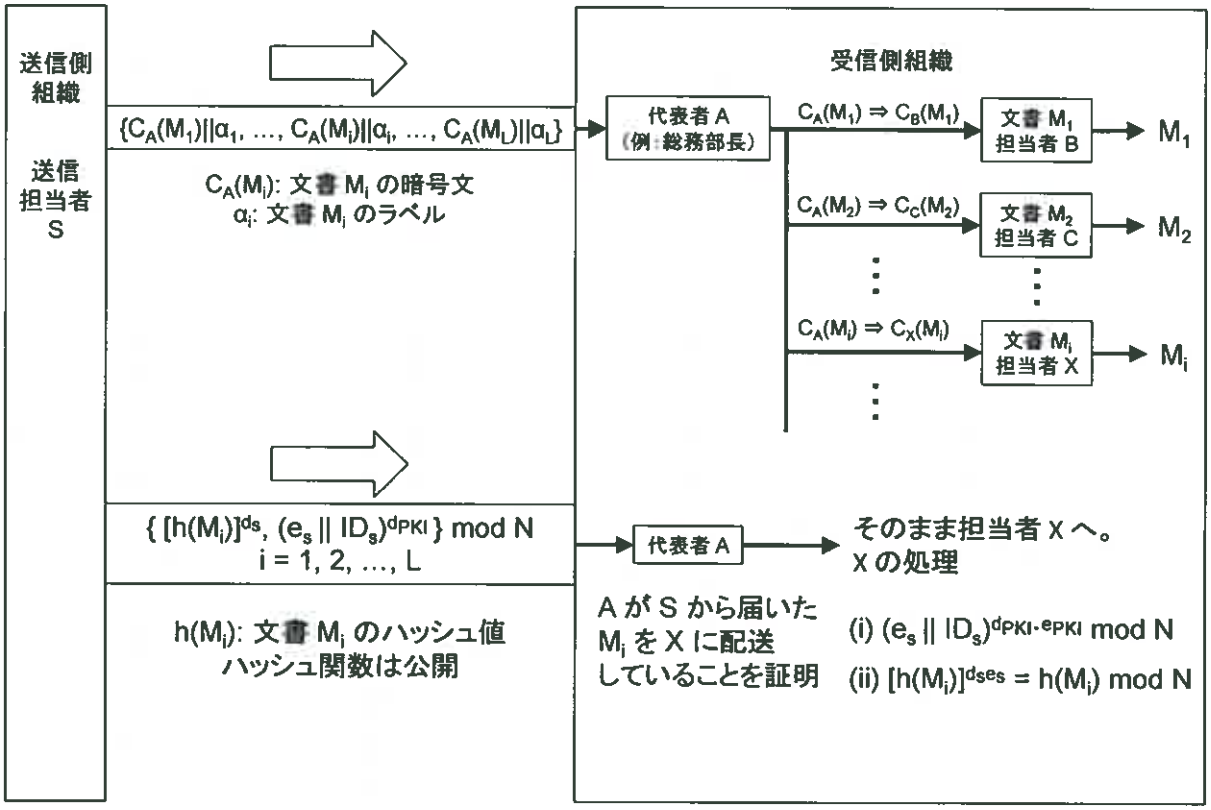
図６　中野区　民生委員へ個人情報提供の例

付録

１．技術的構成

本文で提案したシステムの構成法の一例を附図１に示します。

インターネットを利用できる環境であれば、導入される組織内でのシステム構築・変更は全く必要ありません。全ての処理はクラウドに行わせます。



送信者 S の操作:　　文書 M_i (i = 1, 2, …, L) を A の公開鍵
(楕円エルガマル暗号)で暗号化し、
M_i にラベル α_i(文書名)を平文で付して、A に送信する。

$\{C_A(M_1)||\alpha_1, \ldots, C_A(M_i)||\alpha_i, \ldots, C_A(M_L)||\alpha_L\}$　　Q_A: A の公開鍵
$Q_A = aP$　a: A の秘密鍵
$= \{r_1P, \ldots, r_LP, (M_1 + r_1Q_A)||\alpha_1, \ldots, (M_i + r_iQ_A)||\alpha_i, \ldots, (M_L + r_LQ_A)||\alpha_L\} \bmod p$

受信代表者 A の操作:　　文書 M_i のラベルを見て、担当者 X を定め、
$C_A(M_i)$ を受信側組織の公開鍵で暗号化した後、
A の秘密鍵で復号する。

$[(M_i + r_iQ_A) + r_XQ_A] - a(r_iP) = (M_i + r_XQ_A) \bmod p$

担当者 X に下記の暗号文 $C_X(M_i)$ を送付する。
$C_X(M_i) = [r_XP, M_i + r_XQ_A] \bmod p$

担当者 X の操作:　　(i) $C_X(M_i)$ を X の秘密鍵で復号する。
(ii) A が送信者 S からの文書をそのまま送っているかを
確認したい場合には、上図に示すように
公的個人認証方式等を利用する。

附図１　楕円エルガマル暗号による組織暗号の構成

２．本提案方式と属性暗号・関数暗号との関係

本文で提案したシステムは、送信者が、受信側組織の誰に、電子文書を送って良いか分からない場合や、受信側代表者に配送先を一任すべき場合に、即ち、受信側代表者の判断を必要とする場合に、有効なシステムですが、受信側の人間的・システム的な判断を必要としない場合も少なくありません。

例えば、送信者が、受信側組織に属する人の性別、年齢、収入などの属性に応じて、 配送先を決定できる場合には、属性暗号と呼ばれるシステムの導入が有効でしょう。最近、暗号の分野では、属性暗号やそれを数学的に一般化した関数暗号の研究が鋭意進められています。

（尚、送信側では、配送先を決められなくても、受信側代表者が、受信文書のラベルを見て判断することなく、受信文書の配送先担当者を自動的に配送できる場合は、上述のように、本提案に含ませてあります。）

広い意味で、属性暗号も組織暗号だと位置付けることが出来ます。但し、属性暗号・関数暗号は、絶対的に信頼できるセンターが、ペアリングと呼ばれる手法をベースに、送信側、受信側双方の組織を管理し、個々の担当者の秘密鍵や復号ポリシー・鍵ポリシーを発行するシステムであり、Trusted Center に全権を委任している方式です。従って、属性暗号・関数暗号に基づいた組織暗号は、送信側と受信側の双方を含めた組織を広い意味で、一つの組織と見做しているとも解釈できる場合に、適用可能な暗号方式であると考えられます。

将来、実運用では、本提案方式と属性暗号・関数暗号を統合した組織暗号の構成法を検討する必要があると考えられます。