組織暗号
—情報漏洩とマイ・ナンバー導入に備えて—

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　会長

組織暗号とは

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を想定し、

組織間での個人情報の安全な利活用を支援する暗号方式として、

総務省所管の独立行政法人・情報通信研究機構（NICT）の委託を受け、
研究開発を推進している暗号方式

暗号技術の必要性

個人情報漏えい事件の多発 ・・・　ベネッセ事件など

従来の情報セキュリティ対策は境界防御中心
情報セキュリティ対策に完全なものは無い・・・多重の対策が必要
境界防御と合わせて、守るべきデータの暗号化が重要

マイナンバー・システムの導入

自治体における個人情報保護対策の緊急性
境界防御と合わせて、暗号技術による個人情報保護対策が重要

暗号化状態処理と組織暗号

暗号化状態処理方式とは
暗号化された情報の復号（平文に戻すこと）せずに必要な処理を行うこと
2011年頃からの標的型攻撃や内部不正・犯罪の増大により、
暗号化された情報の復号を必要最小限に抑えることが重要に
しかし、暗号化状態処理方式は研究途上、実用化は未だ先

組織暗号は暗号化状態処理の一種
組織暗号は個人情報などを暗号化状態で配信（転送）可能とする暗号方式
暗号化された情報の配信過程での復号を必要最小限に抑えることが可能

組織間通信への従来の暗号方式適用時の課題

組織間通信の特徴

一般に、送信先の組織体制、担当者の状況を正確には把握できない

組織間通信へ従来の暗号方式を適用する場合の手順例

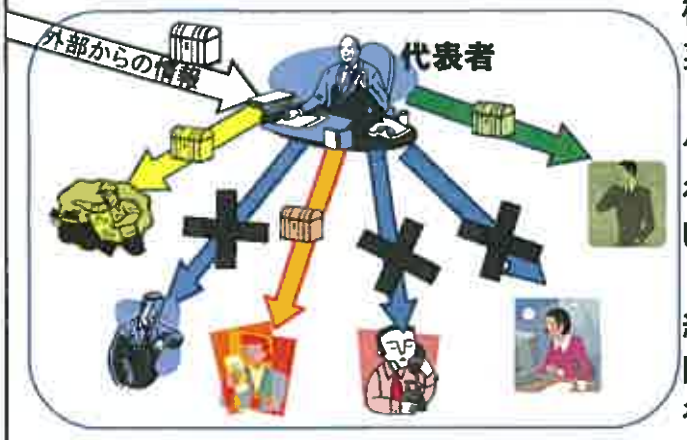
(1)送信者は、受信側組織の代表者(例えば、自治体や企業などの総務部長や庶務課長、病院の事務局長など)宛てに、暗号化文書を送る

(2)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、組織内の然るべき下位の管理者を判断、その管理者へ、再度暗号化し、転送する

(3)受信した管理者も、一旦、それを復号(平文に戻すこと)して、担当者を判断、その担当者へ、再度暗号化し、転送する

従来の暗号方式では、転送の都度、機密情報の復号が必要！

組織内配信の機密性の重要性



機密情報を利用できる人は、
業務上必要な人に限定したい！

代表者も、暗号化された機密情報を
復号しなくても転送できるようにしたい！

組織内でも、異なる担当者には
暗号化された機密情報を
復号できないようにしたい！

暗号化された機密情報を復号せず、しかるべき担当者へ転送でき、
転送された機密情報はその担当者しか復号できないようにしたい！

組織間通信への組織暗号適用時のメリット

（1）組織暗号では、機密情報へラベルを付与

多くの場合、受信側管理者は、受信文書全体を見なくても、
付与されたラベルを見るだけで、誰が担当者か判断できる

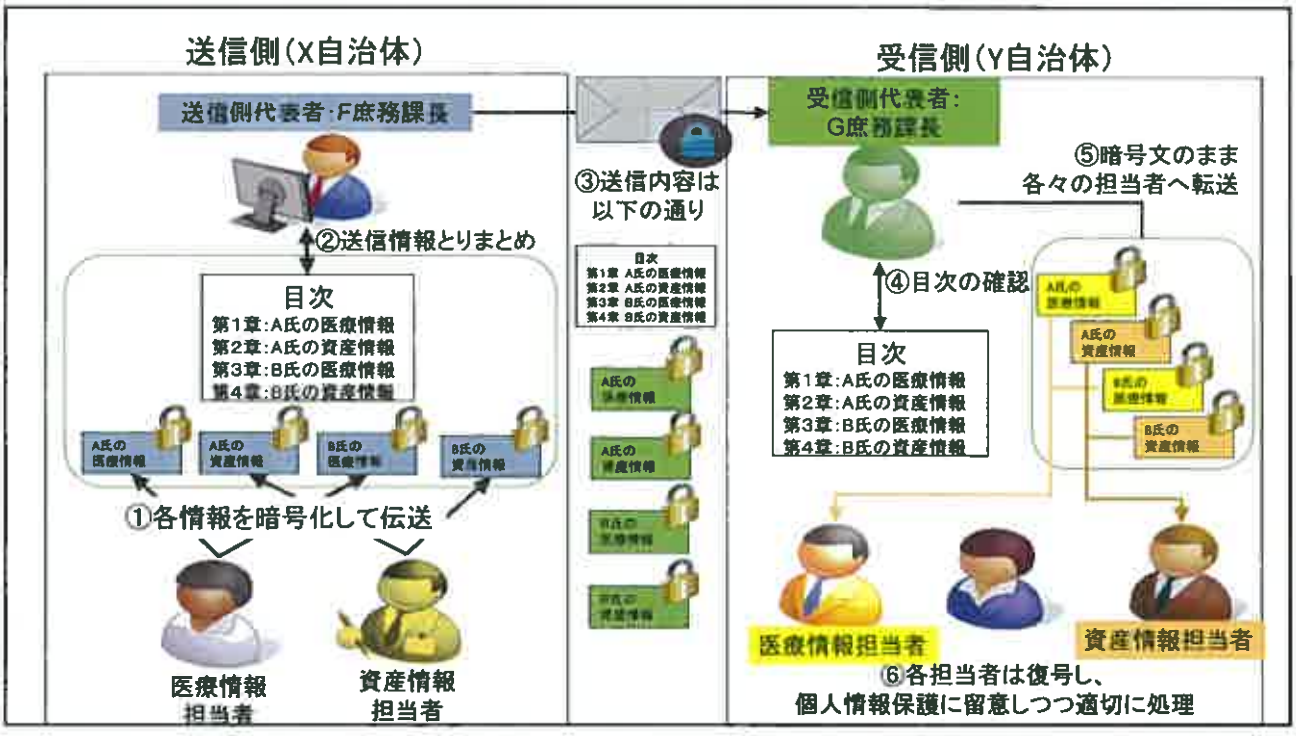
（2）組織暗号では、機密情報を復号せず、再暗号化可能

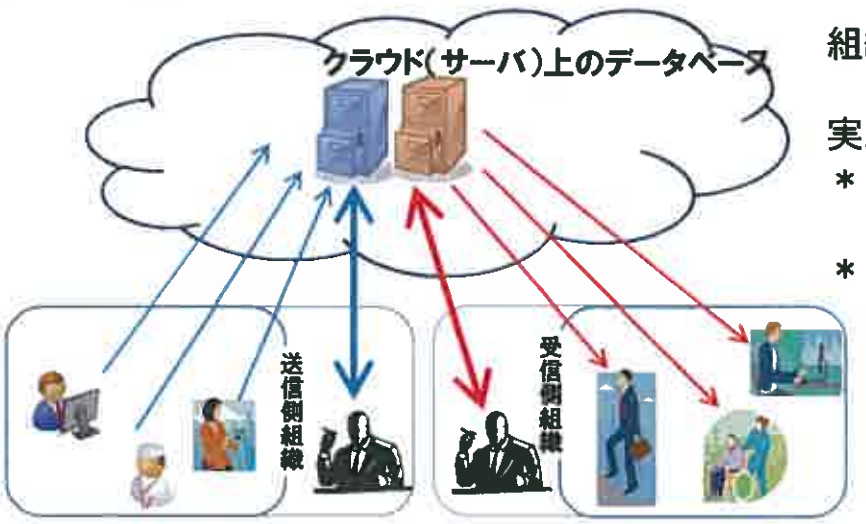
機密情報を暗号化状態で、担当者へ転送可能

「組織暗号なくして電子行政なし」

井堀幹夫

東京大学高齢社会総合研究機構特任研究員（元千葉県市川市CIO）





組織暗号応用システムは

実装方法を工夫すれば、
＊クラウド(サーバ)上
での運用も可能！
＊既存システムへの
影響も少ない！

- **送信者は、文書を送信側代表者向けに暗号化してサーバに登録**
- **送信側代表者は、受信側代表者向けに再暗号化しサーバに登録**
- **受信側管理者は、担当者を決定、その担当者向けに再暗号化しサーバに登録**
- **受信側管理者に指定された担当者は、情報をサーバから入手(復号)**

組織暗号

(1)個人情報等の機密情報の組織間での配信に適した暗号方式

(2)指定された人向けに暗号化された機密情報を、
復号せず他の人向けに再暗号化できる暗号方式
(従来の暗号方式では実現できない機能)

(3)実装方法の工夫により、
既存のシステムに大きな負担をかけることなく、活用可能

(4)組織暗号は、
個人情報の相互利用が増加する地方自治体での活用を念頭に置き、
総務省所管の独立行政法人・情報通信研究機構からの委託により、
研究開発および実用化を推進している暗号方式

(5)組織暗号活用により、より安全な個人情報の利活用を推進願いたい

有難うございました。

ご質問・アドバイスがあれば、よろしくお願いします。