組織暗号応用機密情報配信システムに関する考察

才所敏明†　　辻井重男‡

†‡中央大学　研究開発機構
〒112-8551　東京都文京区春日 1-13-27
†toshiaki.saisho@advanced-it.co.jp　‡tsujii@tamacc.chuo-u.ac.jp

あらまし　マイナンバーの導入や医療・介護サービス提供体制が改革される中、パーソナルデータや企業秘密などの、組織間での機密情報流通が活発化するのは必至。
中央大学では、組織間で流通する機密情報の漏えいリスク低減を目指し、新たな組織暗号の研究開発を推進中。しかし、実際の運用場面での機密情報漏えいリスク低減には、組織暗号応用機密情報配信システムのマネジメントが重要。
本稿では、組織暗号応用機密情報配信システムの、情報漏えい確率の評価方式、それに基づく異なるシステム構成間での情報漏えいに関する安全性の比較、情報漏えい確率を左右する構成要素の特定とデータ流出要因の検討など、システムセキュリティ面の検討結果について報告する。

Considerations about the confidential information distribution system based on new cryptosystems for social organizations

Toshiaki Saisho†　Shigeo Tsujii‡

Research & Development Initiative, Chuo University, Japan
1-13-27, Kasuga, Bunkyo-ku, Tokyo 112-8551, Japan
†toshiaki.saisho@advanced-it.co.jp　‡tsujii@tamacc.chuo-u.ac.jp

Abstract Circulation of confidential information, such as personal data and trade secrets, between the organizations, such as local government and company, is activating. In Chuo University, new cryptosystems are under R&D, aiming the reduction of leak risk of the confidential information which circulates among organizations. However, management of the confidential information distribution system based on those new cryptosystems is very important for reducing leak risk. This paper describes the consideration results about the evaluation method of leak risk probability of the confidential information distribution system and about the leak risk comparison between different system configurations.

1. はじめに

2003 年に個人情報保護法が成立以来、我が国の自治体、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てきた。が、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きた。一方、我が国では、社会保障・税番号（マイナンバー）の活用開始を間近に控え、また、地域の医療･介護サービス体制の改革がこれから全国で展開される中、自治体、医療機関、介護機関、民間企業での（個人情報を含む）パーソナルデータの相互利活用が進むことが想定される。産業界の事業活動でも、昨今の事業環境の急速な変化に対応すべく、企業間の多様な連携、部分連携が展開される中、企業間での秘密情報の相互提供が活発になり、受け取った企業内での秘密情報の適切な保護と利活用がますます重要になるものと思われる。このように、我が国では、パーソナルデータや企業秘密などの機密情報の、適切な保護を維持しつつも、更に広範な利活用が展開されることになる。

中央大学・研究開発機構では、このように増大する機密情報の利活用ニーズへ対応すべく、機密情報の利活用時の安全性を高めることが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。が、機密情報の利活用時の安全性を高めるには、新たな暗号方式等の暗号技術の採用だけではなく、その他の技術的対策、運用・管理面の対策も不可欠である。中央大学・研究開発機構では、新たな暗号方式「組織暗号」の研究開発と並行し、「組織暗号応用機密情報配信システム」のシステムセキュリティ面の課題、対策についての調査研究を進めている。

本稿は、「組織暗号応用機密情報配信システム」のシステムセキュリティ面の調査研究成果の一端を報告するものである。

2. 組織暗号

ここでは、本稿が対象とする機密情報配信システムの構成に採用した組織暗号の特徴を紹介する。中央大学・研究開発機構では、多変数公開鍵暗号および楕円エルガマル暗号をベースとした組織暗号の研究開発を進めているが、組織暗号のアルゴリズムの詳細については、参考文献[1],[2]を参照願いたい。

組織暗号とは、組織間で機密情報を送受する場合の、受信側組織で受信後、機密情報の復号を必要とせず、暗号化状態のまま、臨機応変に組織内に配信を可能とする、暗号方式である。一般に組織構造はさまざまであるが、複雑な組織構造を構成する部門の管理者（受信側代表者および多数の中間管理者）は、それぞれの管理者の役割・権限の範囲での臨機応変の判断に応じ、適切な下位の管理者へ暗号化状態のまま機密情報を配信でき、機密情報の復号および適切な処理を必要とする担当者へ暗号化状態のまま配信可能な暗号方式である。

従来の暗号方式は、送信者が受信者を特定し、その受信者のみが復号できるよう暗号化を施すような、主として End To End の暗号通信に使用される。このような暗号方式でも、送受信ごとに暗号化･復号を繰り返し適用すれば、組織内を転々と流通させることが可能である。が、その都度、機密情報が復号されることは、機密情報の漏えいリスクを高めることになり、好ましくない。

組織暗号は、送信者が必ずしも受信側組織の詳細や具体的構成要員を把握できず、送信する機密情報の復号･処理を必要とする担当者を特定できない場合や、あるいは、組織間の機密情報の送受信を担当者間で直接実施することが不適切な場合に、機密情報の配信

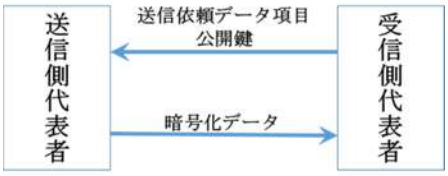
をしかるべき受信側代表者に委託、受信側組織の管理の構造に則りつつ、組織内への機密情報の安全な配信を可能とする、暗号方式である。

3. 組織暗号応用機密情報配信システム

「機密情報配信システム」とは、送信側組織が保有するパーソナルデータや企業秘密などの機密情報の、受信した組織内での安全な配信を目指したシステムであり、「組織暗号応用機密情報配信システム」とは、中央大学・研究開発機構で研究開発を進めている「組織暗号」を応用した「機密情報配信システム」、である。

組織暗号応用機密情報配信システムは、受信側と送信側の組織代表者間の情報交換および受信側組織内の情報配信を担当するシステムから構成されている。

受信側と送信側の組織代表者間の情報のやり取りは以下の通り。送信側代表者が送信を依頼するデータを送信側代表者へ連絡する際に、依頼したデータの暗号化に使用する公開鍵も同時に連絡する。送信側代表者は、依頼されたデータを指定された公開鍵を利用し暗号化を施し、受信側代表者へ送付する。



本稿では、以下、組織暗号応用機密情報配信システムのうち、受信側代表者が暗号化データ受信後の組織内の配信を担当する、組織内機密情報配信システムの安全性の考察結果を報告する。

本節では以下、組織暗号応用機密情報配信システムの典型的な構成例を提示する。

3.1 組織内機密情報配信システム構成（A）

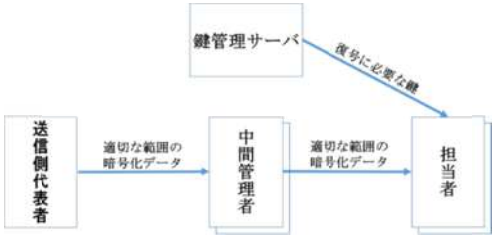
最もシンプルなシステム構成例。組織暗号による暗号化データおよびその復号に必要な鍵情報が一括して転々と組織内を配信される構成。

独立した管理サーバ等は不要で、小規模な組織に適した構成といえる。

3.2 組織内機密情報配信システム構成（B）

暗号化データの復号に必要な鍵情報を集中管理する鍵管理サーバを配置し、暗号化データとその復号に使用される鍵情報の流通ルートを分離した構成。

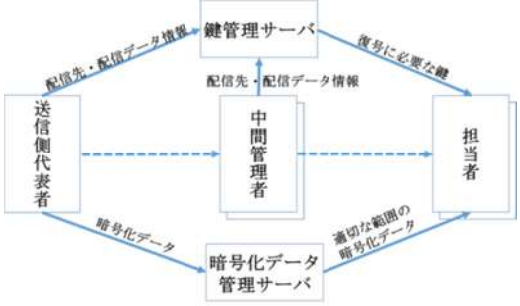
復号が必要な管理者/担当者のみ、鍵管理サーバより必要な鍵情報を入手、暗号化データを復号できる構成である。



3.3 組織内機密情報配信システム構成（C）

組織暗号により暗号化されたデータおよびその復号のための鍵情報のそれぞれを独立したサーバで管理する構成。

復号が必要な管理者/担当者のみ、鍵管理サーバ、暗号化データサーバより、必要な暗号化データおよび鍵情報を入手、復号できる構成である。



4. 機密情報漏えい確率の推定式

本稿では、組織内機密情報配信システムの安全性を、機密情報漏えいリスクの低さ（機密情報漏えい確率の小ささ）と定義し、前節で示したシステム構成例の機密情報漏えい確率の推定を試みる。なお、推定にあたっての前提は以下の通り。

＊機密情報の一部の漏えいも、機密情報の漏えいと定義

＊機密情報の暗号化データおよびその復号のためのデータの両方の流出も、機密情報の漏えいと定義

＊機密情報漏えい確率とは、各組織内機密情報配信システムに対し定義され、機密情報またはその一部の平文データの流出、または、機密情報またはその一部の暗号化データおよび復号のためのデータの両方の流出、が発生する確率と定義

＊データ流出確率とは、システムを構成する各構成要素（管理者、担当者が使用するクライアント、鍵管理、暗号化データ管理に使用されるサーバ、情報の送受に使用される通信路など）に対し定義され、各種データが不正に流出する確率と定義

＊組織内機密情報配信システムの範囲は、暗号化データおよび復号のためのデータが担当者クライアントへ配信されるまで、と定義（平文データの処理が必要な担当者クライアントは範囲外）

また、組織内の機密情報配信システムを構成するクライアント/サーバ、通信路からのデータ漏えい確率を以下の通り表記するものとする。

X：受信側代表者クライアントからのデータ流出確率

Y_i：i 番目の管理者クライアントからのデータ流出確率

K：鍵管理サーバからのデータ流出確率

W：暗号化データ管理サーバからのデータ流出確率

x_i：受信側代表者クライアントと管理者クライアント間の i 番目の通信路からのデータ流出確率

x_w：受信側代表者クライアントと暗号化データ管理サーバ間の通信路からのデータ流出確率

y_j：管理者クライアントと担当者クライアント間の j 番目の通信路からのデータ流出確率

k_j：鍵管理サーバと担当者クライアント間の j 番目の通信路からのデータ流出確率

w_j：暗号化データ管理サーバと担当者クライアント間の j 番目の通信路からのデータ流出確率

上記定義の表記を利用すれば、前節に示した構成例（A）の機密情報漏えい確率 S は厳密には以下の式で表現できる。

$$S = 1-(1-X)*(1-\Sigma Y_i)*(1-\Sigma x_i)*(1-\Sigma y_j)$$

が、本式の右辺の主要項は $X+\Sigma Y_i+\Sigma x_i+\Sigma y_j$ であり、構成例（A）の機密情報漏えい確率 S は以下の式で推定できる。

（A）：$S_A = X+\Sigma Y_i+\Sigma x_i+\Sigma y_j$

同様に、構成例（B）、（C）のシステムからの機密情報漏えい確率 S は、それぞれ以下の式で推定できる。

（B）：$S_B = (X+\Sigma Y_i+\Sigma x_i+\Sigma y_j) * (K+\Sigma k_j)$

（C）：$S_C = (X+W+x_w+\Sigma w_j) * (K+\Sigma k_j)$

さて、この機密情報漏えい確率の推定式の比較により、システム構成間の情報漏えいに対する安全性の比較を試みる。

4.1　システム構成（A）、（B）の比較

異なるシステム構成（A）、（B）の機密情

報漏えい確率の差は以下の通り。

$S_A - S_B = (X+\Sigma Y_i+\Sigma x_i+\Sigma y_j) * (1-(K+\Sigma k_j))$

ここで、各単項はデータ流出確率であり、すべて正であるから

$(X+\Sigma Y_i+\Sigma x_i+\Sigma y_j) > 0$

ということで、システム構成（A)、(B）間の安全性面の優劣は

$(1-(K+\Sigma k_j))$

の符合（正負）の如何による。つまり、鍵管理サーバおよび鍵管理サーバと担当者間の通信路のデータ流出確率如何により優劣が左右されることを示している。

さて、理論的な裏付けがあるわけではないが、多くの組織で現実に運用されているシステムの状況から判断すると、鍵管理サーバは一般に技術対策・管理対策もしっかり取られていることが多いので

$K << 1$

また、機密データの送受信の際には一般的に通信データの暗号化対策が取られることが多く、通信路からのデータ流出確率を十分低く抑えることができるので、

$k_j << 1$

以上の理由から、

$(1-(K+\Sigma k_j)) > 0$

ということが推定でき、

$S_A - S_B = (X+\Sigma Y_i+\Sigma x_i+\Sigma y_j) * (1-(K+\Sigma k_j)) > 0$

となり、(A）は（B）より、機密情報漏えい確率は大きい、つまり、いくつかの条件付きではあるが、一般的には（B）の方がより安全な構成と言える。

4.2　システム構成（B)、(C）の比較

同様に、異なるシステム構成（A)、(B）の機密情報漏えい確率の差は以下の通り。

$S_B - S_C = ((\Sigma Y_i+\Sigma x_i+\Sigma y_j) - (W+x_w+\Sigma w_j)) * (K+\Sigma k_j)$

ここで、各単項は確率であり正であるから、

$(K+\Sigma k_j) > 0$

ということで、システム構成（A)、(B）間の安全性面の優劣は

$(\Sigma Y_i+\Sigma x_i+\Sigma y_j) - (W+x_w+\Sigma w_j)$

の正負の如何による。

さて、理論的な裏付けがあるわけではないが、多くの組織で現実に運用されているシステムの状況から判断すると、個人が管理する管理者クライアントに比べ、暗号化データ管理サーバの方が一般には技術対策・管理対策もしっかり行われるので

$W < \Sigma Y_i$

また、暗号化データ管理サーバと担当者クライアント間の通信路は、管理者クライアントと担当者クライアント間の通信路に比べ、一般にはしっかりとした技術対策が施され高い安全性が期待されるので

$\Sigma w_j < \Sigma y_j$

また、受信側代表者クライアントと暗号化データ管理サーバ間の通信路は、受信側代表者クライアントと管理者クライアント間の通信路に比べ、一般にしっかりとした技術対策が施され高い安全性が期待されるので

$x_w < \Sigma x_i$　であるから

$((\Sigma Y_i+\Sigma x_i+\Sigma y_j) - (W+x_w+\Sigma w_j)) > 0$

ということが推定でき

$S_B - S_C = ((\Sigma Y_i+\Sigma x_i+\Sigma y_j) - (W+x_w+\Sigma w_j)) * (K+\Sigma k_j) > 0$

となり、(B）は（C）より、機密情報漏えい確率は大きい、つまり、いくつかの条件付きではあるが、(C）の方が一般的にはより安全な構成と言える。

4.3　機密情報漏えい確率推定式の一般化

今回提案した、構成要素からのデータ流出確率ベースの機密情報漏えい確率の推定方

式は、必ずしも組織暗号応用機密情報配信システムに特化したものではない。以下のように一般化した情報漏えい確率推定式は、様々のシステムの情報漏えいに対する安全性評価の指標として活用可能である。

S（システムからの情報漏えい確率）　＝
1－
（漏えい防止対象の情報の全部または一部あるいは漏えい防止対象の情報の全部またはその一部を生成できるデータを保有する構成要素について、各構成要素からデータが流出しない確率の積）
＊
（複数の構成要素からの流出データによって漏えい防止対象の情報の全部またはその一部を生成できる構成要素の組合せについて、各組合せからデータが流出しない確率の積）

5. 機密情報漏えい確率を左右する構成要素の特定

本節では、機密情報漏えい確率の推定式から、システム構成（A）、（B）、（C）それぞれの機密情報漏えい確率を左右する構成要素の特定を試みる。

システム構成（A）の機密情報漏えい確率の推定式は、以下のとおりである。

（A）：$S_A = X+\Sigma Y_i+\Sigma x_i+\Sigma y_j$

システム構成（A）は、クライアントと通信路から構成されており、この2種の構成要素からのデータ流出確率を如何に抑えるか、がシステム構成（A）の機密情報漏えいに対する安全性を高めるポイントになる。

構成要素の一つである通信路からのデータ流出確率は、適切な暗号化対策により、十分小さく抑えることが可能である。

一方、もう一つの構成要素である多くの管理者が利用する多数のクライアントは、一般にはオフイスに分散配置されており、管理もまたそれぞれの管理者に任されている場合が多く、様々の脅威に晒されており、データ流出確率が高いことが想定される。

システム構成（A）の機密情報漏えい確率は、多数分散配置されるクライアントからのデータ流出確率に大きく依存する、といえる。

システム構成（B）の機密情報漏えい確率の推定式は、以下のとおりである。

（B）：$S_B = (X+\Sigma Y_i+\Sigma x_i+\Sigma y_j) * (K+\Sigma k_j)$

$(X+\Sigma Y_i+\Sigma x_i+\Sigma y_j)$ は、システム構成（A）と共通であり、この複合項の値は多数分散配置されるクライアントからのデータ流出確率に大きく依存する。が、システム構成（B）では、その複合項に更に

$0 < (K+\Sigma k_j) < 1$

が見込まれる複合項が乗じられており、この複合項の大小がシステム構成（B）の機密情報漏えい確率を大きく左右、つまりシステム構成（B）の安全性は鍵管理サーバおよび鍵管理サーバから担当者へ復号のための情報を配信する通信路のデータ流出確率に大きく依存している、といえる。

なお、鍵管理サーバは、一般に隔離されたスペースに配置され、専門家により管理・運用されるため、データ流出要因対策の徹底も容易となり、データ流出確率を低く抑えることが容易である。

システム構成（C）の機密情報漏えい確率の推定式は、以下のとおりである。

（C）：$S_C = (X+W+x_w+\Sigma w_j) * (K+\Sigma k_j)$

$(K+\Sigma k_j)$ はシステム構成（B）と共通である。システム（B）、（C）間の主たる差異は、システム（B）の機密情報漏えい確率が多数分散配置されるクライアントからのデータ

流出確率に依存しているのに対し、システム（C）の機密情報漏えい確率が暗号化データ管理サーバからのデータ流出確率に依存していることにある。暗号化データ管理サーバは、一般に隔離されたスペースに配置され、専門家により管理・運用されるため、データ流出要因対策の徹底も容易となり、データ流出確率を低く抑えることが容易である。

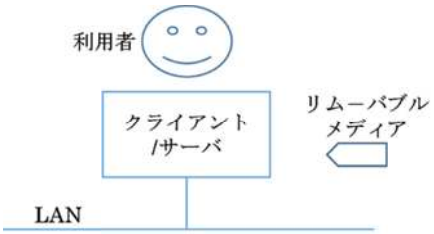
本節では、機密情報漏えい確率の推定式から、システム構成（A）、（B）、（C）それぞれの機密情報漏えい確率を左右する構成要素の特定を実施した。

機密情報漏えい確率を左右する主要な構成要素の特定は、システムの安全性を高めるための効果的な対策の選定の大変重要な一歩である。

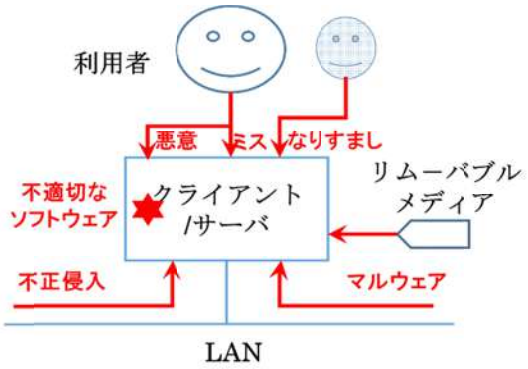
また、今回実施した機密情報漏えい確率推定式を利用した機密情報漏えい確率を左右する主要な構成要素の特定の手法は、組織暗号応用機密情報配信システムに限らず、多くのシステムの情報漏えい確率を左右する主要な構成要素の特定に有効と思われる。

6. 構成要素からのデータ流出対策の検討に向けて

本節では、システム構成例（A）、（B）、（C）の情報漏えい確率を大きく左右する構成要素であるクライアント/サーバからの主要なデータ流出要因の整理を試みる。なお、クライアント/サーバに対する操作/侵入は、特殊な構成の場合を除き、キーボード、ネットワーク、メディア経由で行われるものと想定される（下図）。



それぞれの操作/侵入チャネル経由の主なデータ流出要因を洗い出したのが、下図である。なお、操作/侵入によるデータ流出とは異なるが、機密情報の配信に利用されるソフトウェアの不適切さ（含む、設定の不適切さ）によるデータ流出も想定されるので、要因に加えている。



主要なデータ流出要因とそれに起因する被害の例を次の表に示している。

さて、次の表の要因発生確率 F_{SY}、F_{IN}、F_{MW}、F_{SP}、F_{ER}、F_{ML} とは、対象とするクライアント/サーバが設置されている環境、施されている技術対策・管理対策の条件下でのデータ流出要因の発生確率とする。なお、一般には、サーバにおける要因発生確率は、クライアントにおける要因発生確率より相当程度低いものと想定される。

データ流出要因	起こりうるデータ流出に繋がる被害例	要因の発生確率
システムそのものの不備		
不適切なソフトウェア	乱数生成機能の不具合/設定の不備による弱鍵生成、復号リスクの高い暗号化データの生成 データの暗号化処理の不具合による復号リスクの高い暗号化データの生成など	F_{SY}
システムへの正規ルート（キーボード、ネットワーク）からの不正アクセス		
第3者のなりすまし	利用者になりすましログインし、利用者システム内の暗号化データ、復号のためのデータ等のコピー入手	F_{SP}
利用者のミス	正規の受信者ではない第3者へ、暗号化データ、復号のためのデータ等を送信	F_{ER}
利用者の悪意	業務目的外でシステムを利用し、暗号化データ、復号のためのデータ等のコピー入手	F_{ML}
システムへの非正規ルート（ネットワーク、メディア）からの不正アクセス		
第3者の不正侵入	利用者システム内の暗号化データ、復号のためのデータ等の直接流出	F_{IN}
マルウェア感染	利用者システム内の暗号化データ、復号のためのデータ等の第3者への送信	F_{MW}

上表で定義した要因発生確率 F_{SY}、F_{IN}、

F_{MW}、F_{SP}、F_{ER}、F_{ML}を利用すると、対象とするクライアント/サーバからの現状でのデータ流出確率 P は以下の式で推定できる。

$$P = 1 - (1-F_{SY}) * (1-F_{IN}) * (1-F_{MW}) * (1-F_{SP}) * (1-F_{ER}) * (1-F_{ML})$$

なお、ここでは、流出要因が発生した場合は、常にデータ流出が発生するものと想定している。

対象としたクライアント/サーバからのデータ流出確率 P の値を下げるには、データ流出要因発生確率 F_{SY}、F_{IN}、F_{MW}、F_{SP}、F_{ER}、F_{ML}を下げる何らかの新たな技術的対策・管理的対策が必要となる。その際には、効果的・効率的な対策の選定が求められ、適切な対策を選定する方法が望まれている。適切な対策の選定は、一般に、組織の事情、脅威や脆弱性の状況などさまざまな条件に大きく依存し、難しい課題であるが、何らかの対策選定・評価手法の可能性を今後検討したい。

7. おわりに

中央大学・研究開発機構では、組織間の機密情報の安全な送受信のために、新たな暗号方式「組織暗号」の研究開発を進めている。また、新たな暗号方式の研究開発と並行し、組織暗号応用システムのマネジメントの側面の調査研究も実施している。

本稿では、マネジメントの側面の調査研究の一環として、組織暗号を応用した受信側組織内機密情報システムを対象に、情報漏えいに対するシステムの安全性のレベルを推定できる情報漏えい確率の推定式を考案、その推定式に基づき異なるシステム構成間の安全性の比較、情報漏えい確率を左右する構成要素の特定などの分析結果を報告した。

組織暗号応用機密情報配信システムのマネジメントの側面の調査研究の今後の主な課題は以下の通り。

＊今回の報告の延長として、適切なセキュリティ対策の選定方法に関する検討

＊機密情報の暗号化状態での臨機応変の配信に対応可能な、アクセス制御方式の検討

＊組織暗号応用機密情報配信システムが幅広く利用されるために不可欠な、組織間での情報授受のプロトコル、データ形式の標準化の検討

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。関係各位に感謝する。

参考文献

[1] 辻井重男，山口浩，只木孝太郎，五太子政史，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 －”，信学技報告，ISEC2013-40, SITE2013-35, ICSS2013-45, EMM2013-42(2013-07), July2013.

[2] 辻井重男，山口浩，才所敏明，五太子政史，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 －”，Proc. SCIS2014, 3E1-1, January 2014.