CSS2014（札幌）

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

独立行政法人情報通信研究機構（NICT） 高度通信・放送研究開発委託研究
「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―」

背景

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、広範な利活用が今後展開される予定

- ∴社会保障・税番号（マイナンバー）の活用
- ∴地域の医療・介護サービス体制の改革

中央大学・研究開発機構では、
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
独立行政法人情報通信研究機構（NICT）の高度通信・放送研究開発委託研究
「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―」の一環として実施中

本発表の位置づけ

組織暗号の研究開発テーマの一環として実施

機密情報の配信時の安全性 ≠ 新たな暗号方式等の暗号技術の採用
　∵その他の技術的対策、運用・管理面の対策も不可欠

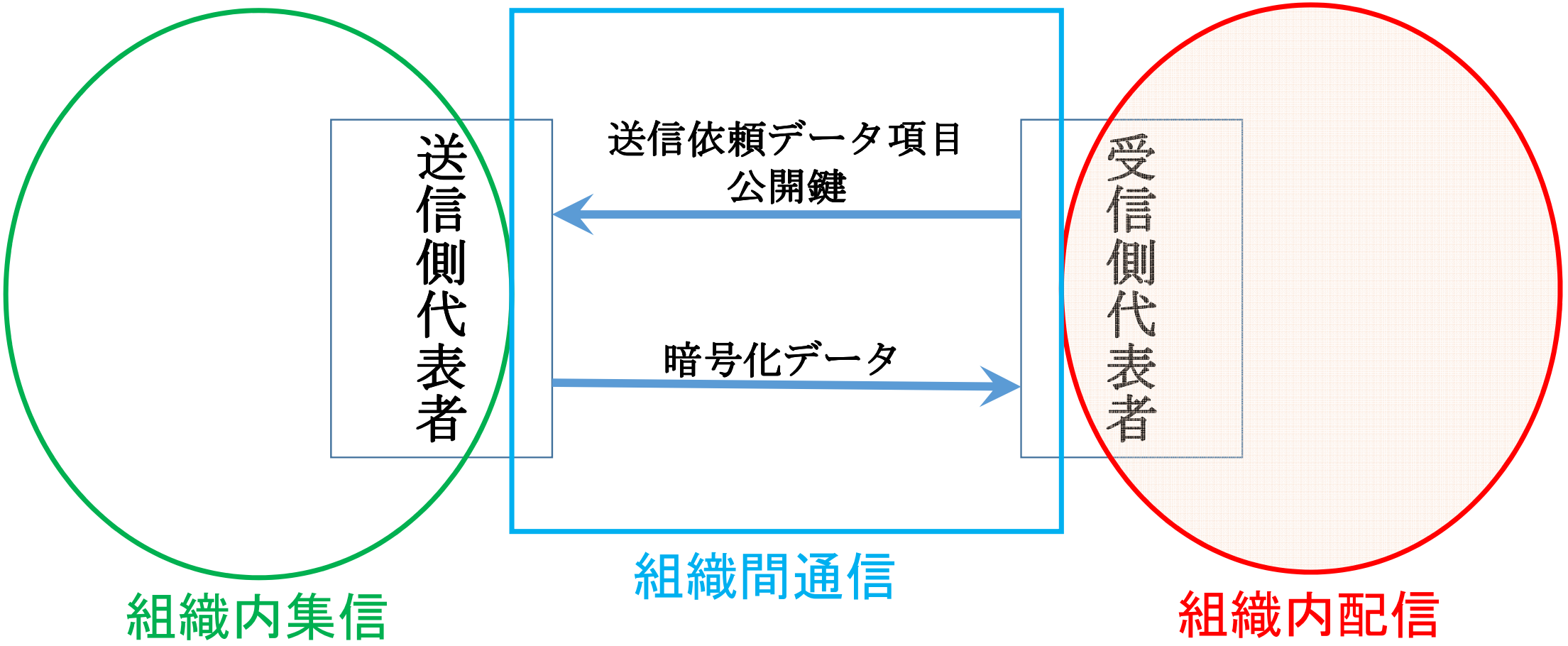
「組織暗号応用機密情報配信システム」の
システムセキュリティ面の課題、対策についての調査研究を実施中
本発表では、この成果の一端を報告
（システム構築・運用に関する留意事項、ガイドラインの提示が目標）

組織暗号の特徴

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、暗号方式であり、

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、
　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
＊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
に活用されることを想定

組織暗号応用機密情報配信システム



組織内機密情報配信システム

組織内機密情報配信システムとしての最適なシステム構成の特定は困難

∵組織の規模や構造は多様

∵独立したシステムとしての実装は非現実的で、

多様な既存システムとの連携による実装とならざるを得ない

組織の状況や制約条件下の、

適切なシステム構成の選定

安全性を高める対策の選定

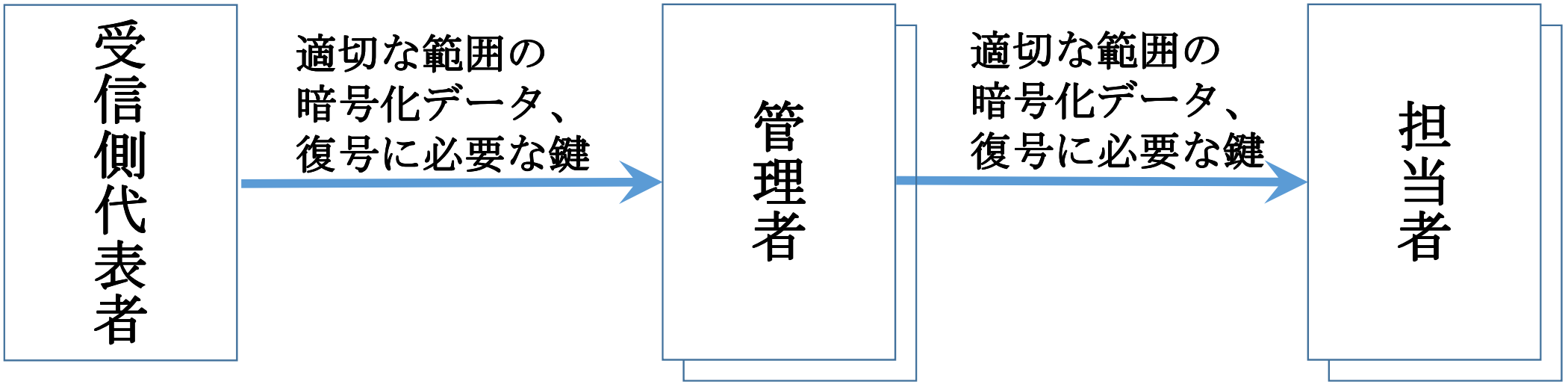
のための方法論を検討

組織内機密情報配信システムとして
安全性の高いシステム構成の選定のために

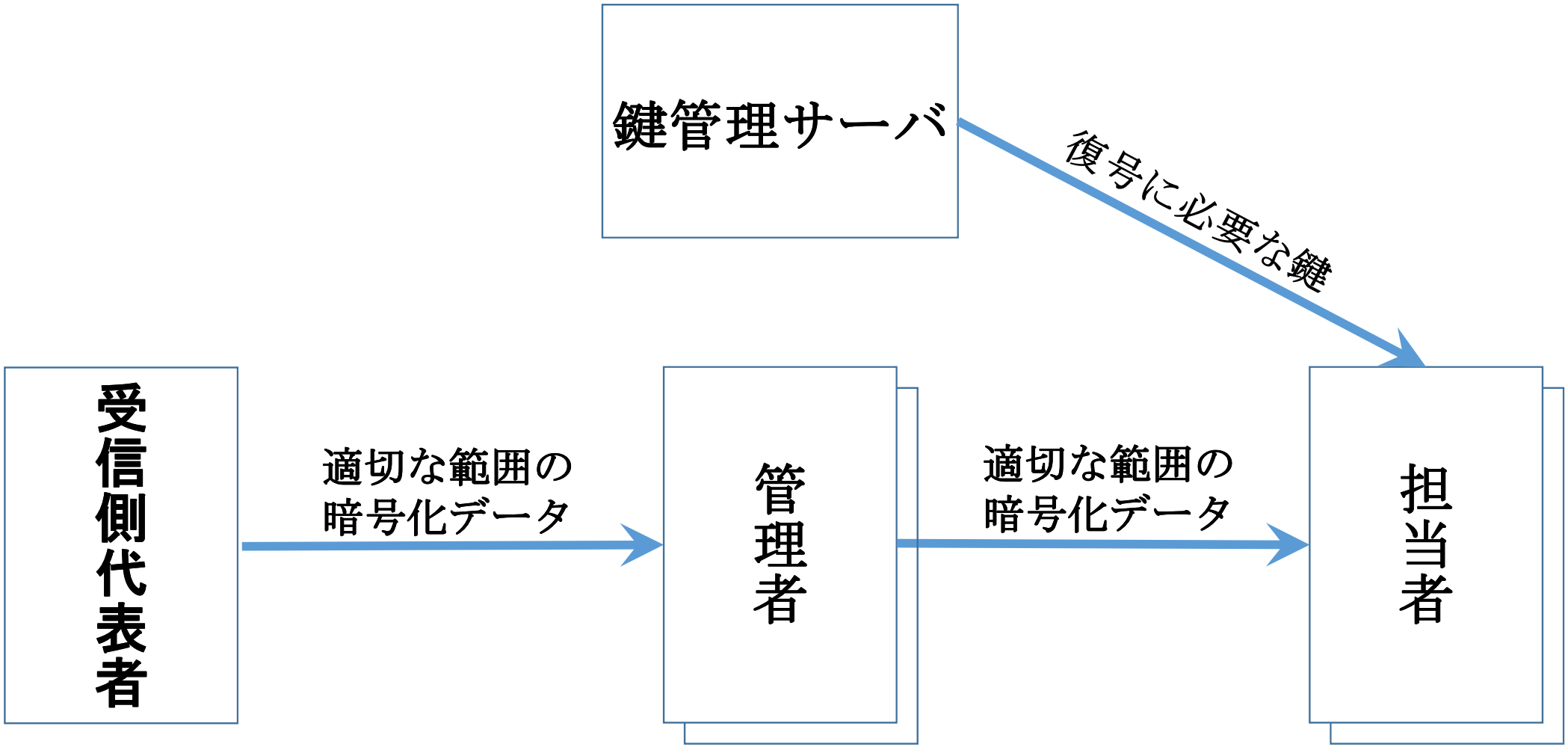
（１）基本的なシステム構成例の安全性の推定
推定方法の提案

（２）異なるシステム構成例間の安全性の比較
推定方法の妥当性の確認

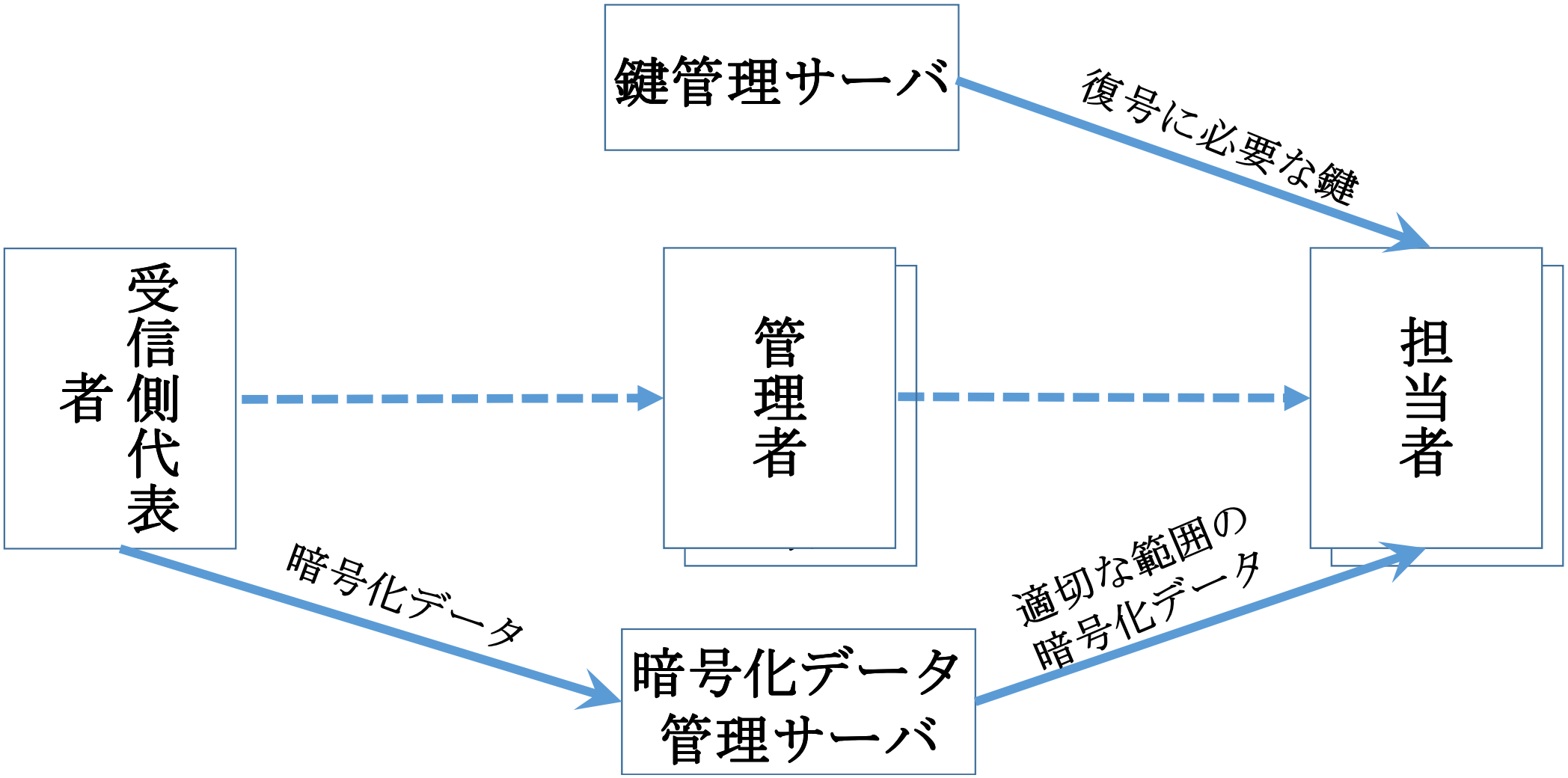
組織内機密情報配信システム構成（A）



組織内機密情報配信システム構成（B）



組織内機密情報配信システム構成（C）



組織内機密情報配信システムの安全性

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

基本的なシステム構成例の機密情報漏えい確率の推定

機密情報漏えい確率推定の前提

＊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）

機密情報漏えい確率推定式内記号の説明

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

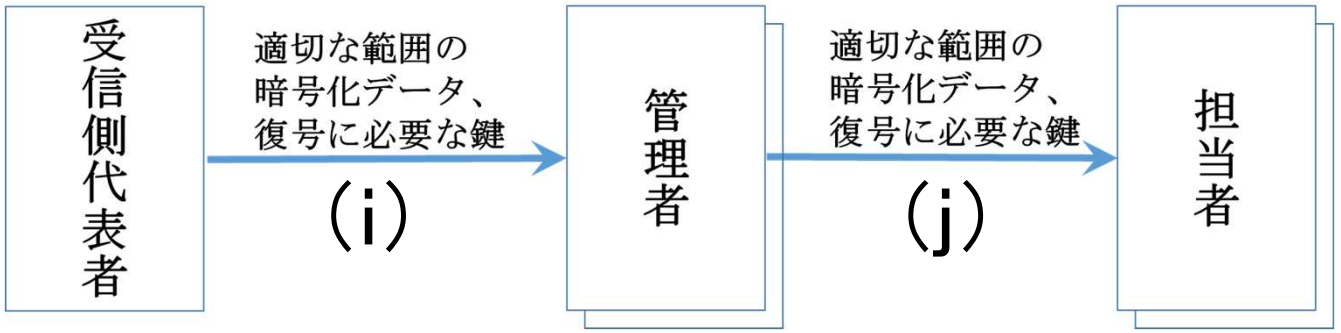
k_j：鍵管理サーバと担当者クライアント間のj番目の通信路からのデータ流出確率

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

なお、データ流出確率とは、機密情報の配信ごとに、その構成要素から情報漏えいに繋がるデータの流出が発生する確率とし、基本的な情報セキュリティ対策を実施している構成要素からのデータ流出確率は、1より十分小さい、と考えられる

組織内機密情報配信システム構成（A）の機密情報漏えい確率S_Aの推定式

$$S_A = X + \Sigma Y_i + \Sigma x_i + \Sigma y_j$$



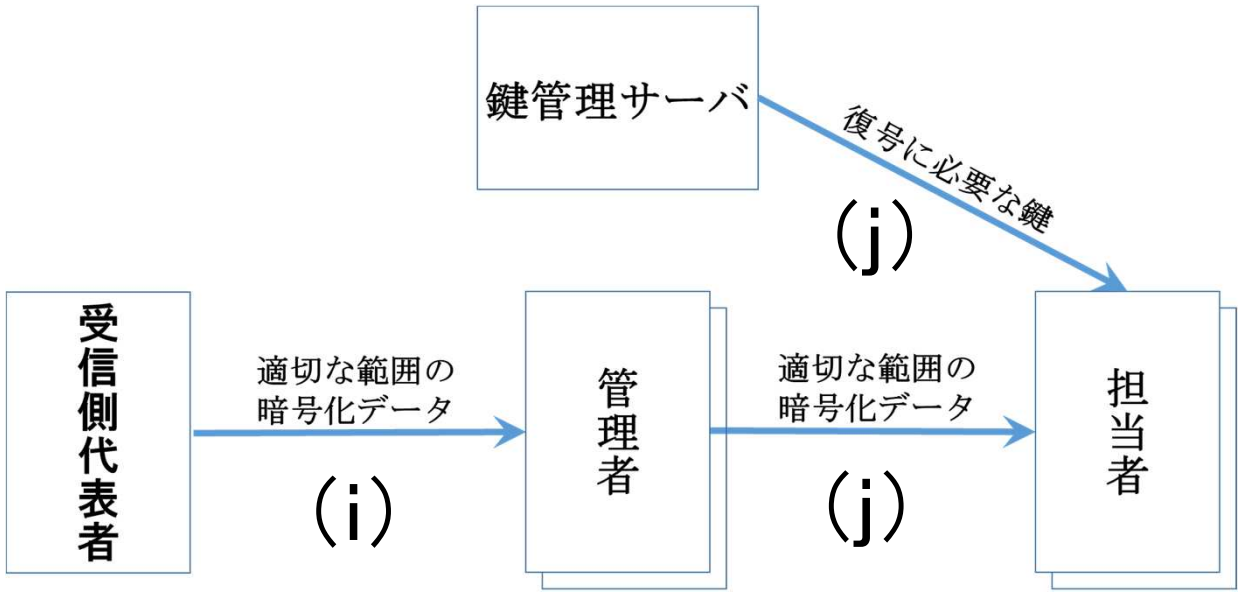
厳密には

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

だが、２次の項を省略し、上記推定式へ

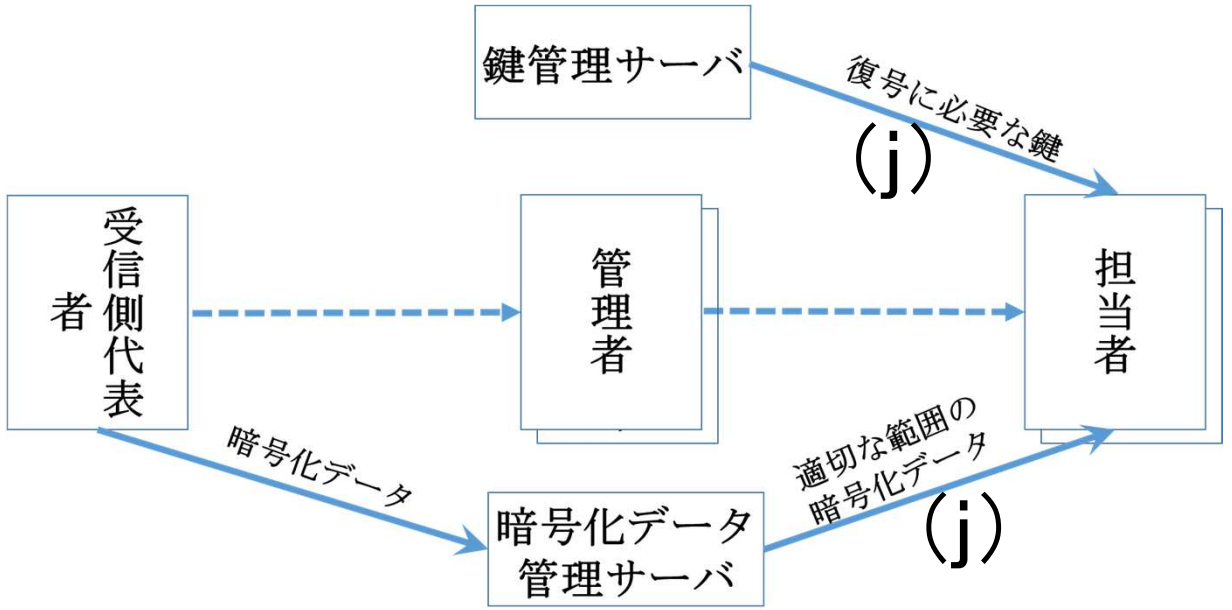
組織内機密情報配信システム構成(B)の機密情報漏えい確率S_Bの推定式

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



組織内機密情報配信システム構成(C)の機密情報漏えい確率S_Cの推定式

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



システム構成（A）、（B）の比較

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

X、Y_i、x_i、y_jは、それぞれデータ流出確率のため　X、Y_i、x_i、y_j ＞ 0

ということで、（X＋ΣY_i＋Σx_i＋Σy_j） ＞ 0

また、 鍵管理サーバおよび鍵管理サーバと担当者間の通信路からのデータ流出確率は、基本的な情報セキュリティ対策が施されている場合は K、Σk_j ＜＜ 1 であり、結果として （1－(K＋Σk_j)） ＞ 0

それぞれ、基本的な情報セキュリティ対策を施したシステム構成（A）、（B）間の安全性の比較結果は $S_A - S_B$ ＞ 0 となり、

システム（B）の方が一般には安全である、と言える。

システム構成（B）、（C）の比較

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

K、k_jは、データ流出確率であり正であるから、$(K + \Sigma k_j) > 0$

ということで、$S_B - S_C$ の大小は$(\Sigma Y_i + \Sigma x_i + \Sigma y_j) - (W + x_w + \Sigma w_j)$の正負に依存する。

通信路からのデータ流出確率は、基本的な情報セキュリティ対策が施されている場合は十分小さいと想定でき、x_i、y_j、x_w、w_j ＜＜ 1 であり、$(\Sigma Y_i + \Sigma x_i + \Sigma y_j) - (W + x_w + \Sigma w_j)$の正負は $\Sigma Y_i - W$ の値に左右されるが、個人管理の分散されたクライアントからのデータ流出確率の方が、しっかり管理されることが想定される暗号化データ管理サーバからのデータ流出確率より大きいと想定されるので、$\Sigma Y_i - W > 0$

それぞれ、基本的な情報セキュリティ対策を施したシステム構成（B）、（C）間の安全性の比較結果は $S_B - S_C > 0$ となり、

システム（C）の方が一般には安全である、と言える。

機密情報漏えい確率推定式の一般化

S(システムからの情報漏えい確率) ＝ １－
（漏えい防止対象情報の全部またはその一部保有する、あるいは
漏えい防止対象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）

＝＞この機密情報漏えい確率推定式を利用により、
より安全なシステム構成の選定が可能

（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く、
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）

機密情報漏えい確率を左右する構成要素の選定（安全性を高める対策の選定のために）

システム構成（A）

機密情報漏えい確率の推定式　$S_A = X + \Sigma Y_i + \Sigma x_i + \Sigma y_j$

構成要素：クライアントと通信路

クライアントからのデータ流出確率：X、Y_i

通信路からのデータ流出確率：x_i、y_j

通信路からのデータ流出確率は、

適切な技術（暗号化）対策により、十分小さく抑えることが可能

クライアントは一般に分散配置、分散管理の場合が多く、

データ流出確率が高い

ことから　X、Y_i　＞＞　x_i、y_j　であると推定できる

➔ クライアントが、機密情報漏えい確率を左右する主要な構成要素

システム構成（B）

機密情報漏えい確率の推定式　$S_B = (X + \Sigma Y_i + \Sigma x_i + \Sigma y_j) * (K + \Sigma k_j)$

構成要素：クライアント、サーバと通信路

クライアントからのデータ流出確率：X、Y_i

サーバからのデータ流出確率：K

通信路からのデータ流出確率：x_i、y_j、k_j

$(X + \Sigma Y_i + \Sigma x_i + \Sigma y_j)$の項は、システム構成（A）と同一

➔クライアントが機密情報漏えい確率を左右する主要な構成要素と言えるが、$(K + \Sigma k_j)$の効果により、クライアントの機密情報漏えい発生確率への影響を、鍵管理サーバからのデータ流出確率により下げることができる

➔　専門家の管理下で運用される鍵管理サーバからのデータ流出確率を下げることにより、機密情報漏えい発生確率へのクライアントの影響を低く抑えることが可能

システム構成（C）

機密情報漏えい確率の推定式　$S_C = (X + W + x_w + \Sigma w_j) * (K + \Sigma k_j)$

構成要素：クライアント、サーバと通信路

クライアントからのデータ流出確率：X

サーバからのデータ流出確率：K、W

通信路からのデータ流出確率：x_w、w_j、k_j

機密情報漏えい確率を左右する主要構成要素は

鍵管理サーバ、暗号化データ管理サーバ、受信側代表者のクライアント

本システムの特徴は、一般にオフィス内に分散配置される多数のクライアント、多数の利用者が使用するクライアントの影響を排除していること

➔　機密情報漏えい確率を、限られた構成要素、専門家の管理下にある、あるいは意識の高いと想定される受信側代表者の管理下にある構成要素で制御可能なシステム構成

機密情報漏えい確率を左右する
主要な構成要素の選定

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

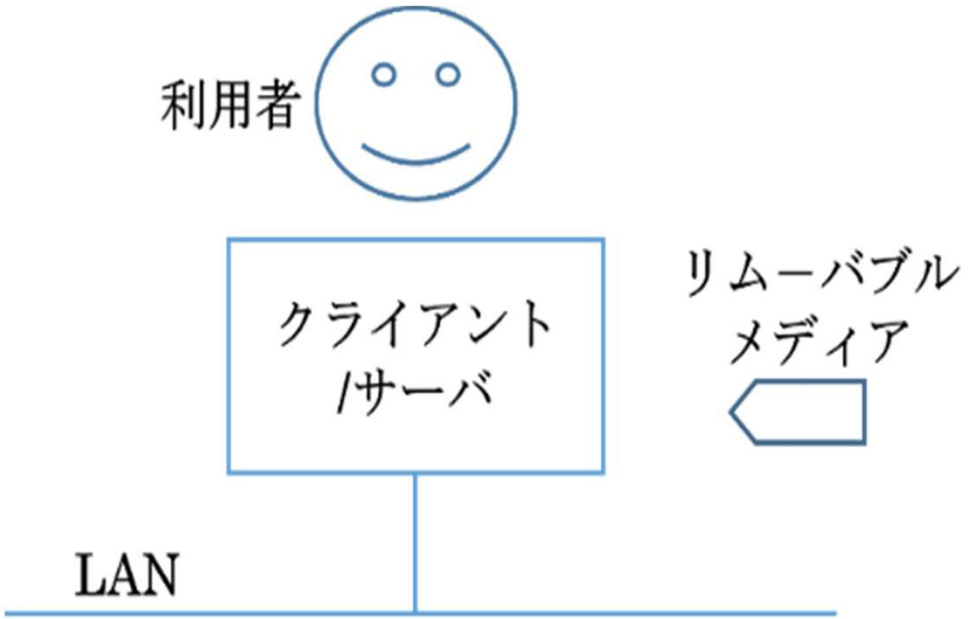
＝＞機密情報漏えい確率推定式を利用し、
機密情報漏えい確率を左右する主要な構成要素の選定が可能

（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選定に有効）

機密情報漏えい確率を左右する主要な構成要素からの主要なデータ流出対策の検討に向けて

以下、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。

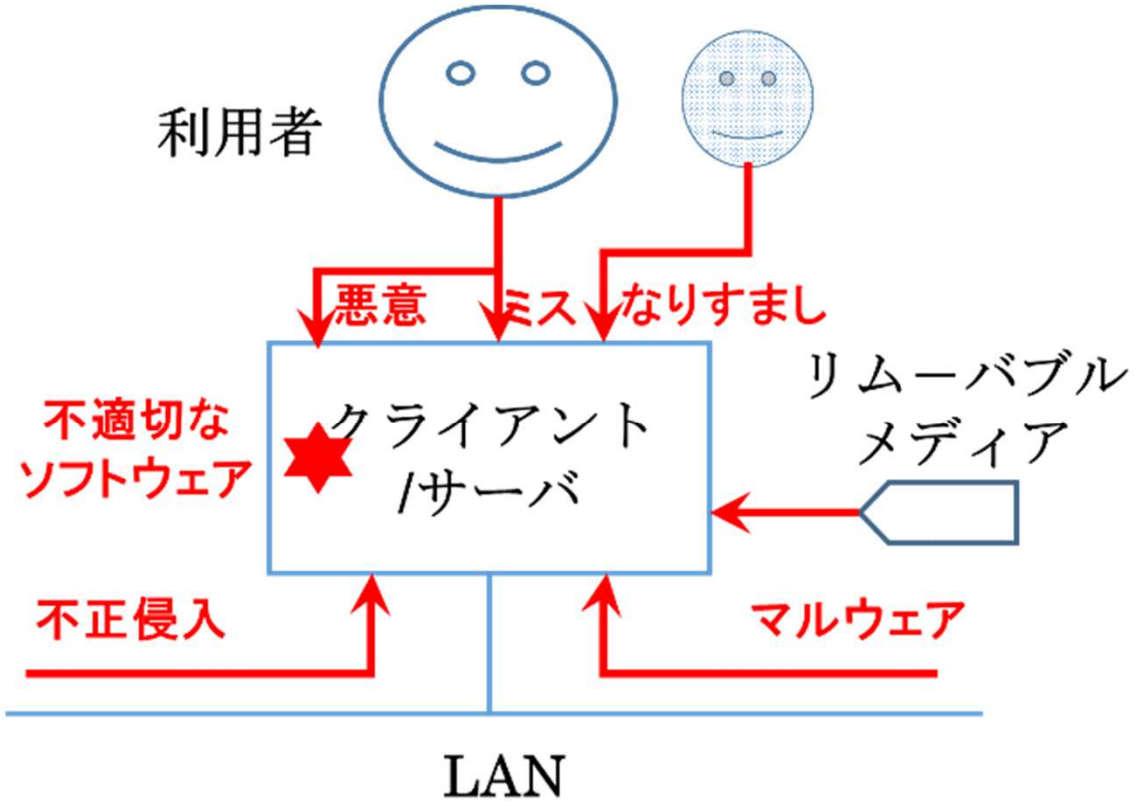
クライアント/サーバに対する操作/侵入は、特殊な構成の場合を除き、キーボード、ネットワーク、メディア経由で行われるものと想定される。



クライアント/サーバからの主要なデータ流出要因

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は右図の通り。

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

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}

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。

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。

要因発生確率によるデータ流出確率の推定

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。

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

（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）

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。

まとめ

中央大学・研究開発機構では、

①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

②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

を実施している。

本発表では、マネジメントの側面の調査研究の一環として、

①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

情報漏えい確率推定式の考案

②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

③その推定式に基づき、情報漏えい確率を左右する構成要素の選定

などの考察結果を報告した。

今後の主な課題

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。

①今回の考察の延長として、適切なセキュリティ対策の選定方法に関する検討

②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

③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

組織暗号の実証実験、開始！

目的：自治体業務での組織暗号の有用性、
個人情報保護に対する有効性を
自治体の方々にご理解いただくこと

方法：自治体の想定業務への組織暗号適用方式の提示と
その方式を念頭に置いたモデルシステムの
自治体職員の方々による操作実験

大町市役所での組織暗号実証実験
（2014年10月15日）

参加者：

自治体関係者　８名　（大町市役所、北アルプス広域連合）
報道関係者　　６名　（中日新聞、大糸タイムズ、
テレビ信州、大町市有線放送）

結果：

個人情報の配信途中で一切復号を必要としないこと、
そのことが個人情報漏えいに大きな効果があること
をご理解いただけた


組織番号とは

放課後

入り口に掲げた看板の除幕をする小口市長(左)や児童ら＝塩尻市の塩尻東小学校北校舎で

の除幕をした小口利幸市長は、開館式典で、「児童館、児童クラブは小学校内にあるのが一番使いやすい。この施設を利用して多くの子どもが育ち、市の未来を担う人になってほしい」と期待した。

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)

ホースを使って消火作業を体験

大町でフェスタ

消防活動への理解や防災意識の向上を目指した「消防フェスタおおまち」が、大町市の市運動公園であり、家族連れらが防災体験やヒーローショーなどを楽しんだ。

消防服で消火作業を体験する子どもら＝大町市の市運動公園で

四回目を迎えたイベント、会場では市消防団員が来場者を出迎え、体験コーナーで指導したり、消防車両の運転をしたりした。

消防ホースを使って消火作業を体験した白馬村の武田創志君(六つ)は「重かったけど的に当てることができて楽しかった」と満足そうだった。

大北地域のゆるキャラが集ったゲーム大会や、地元の福祉施設も出店した飲食コーナーもあり、家族連れらでにぎわった。(吉田幸雄)

三遠ニュース

豊橋駅前に発信拠点

地元CATVとラジオ局

愛知県豊橋市のケーブルテレビ局「ティーズ」とラジオ局「エフエム豊橋」は共同で、豊橋駅前の複合商業施設「ココラフロント」の1階に、情報発信拠点「ココラスタジオ」を開設した＝写真。番組放送のほか、地元作家の作品を展示したり市民が交流したりするスペースとする。

一部を開放し、ソファや机を置き、ティーズの生放送番組を視聴できるモニターも設置した。自由に飲食でき、待ち合わせにも利用してもらう。

開設に合わせ、新番組も開始。ティーズはまちなかのイベントや地元作家を紹介する番組を、エフエム豊橋は地元のダンサーや歌手をゲストに招いたり若者の流行文化を紹介したりする番組を設けた。

メガソーラーを増設

浜松市、新たに出力500㌔

浜松市は、公有地を民間事業者に貸し出して運営している浜松市西区呉松町のメガソーラー施設「浜松・浜名湖太陽光発電所」を増設した＝写真。

発電所は一般廃棄物埋め立て処分場(静ケ谷最終処分場)の跡地を利用。8.4㌶のうち、西側3.9㌶を中部電力グループのシーテック(名古屋市)、東側2.2㌶を地元中堅ゼネコンの須山建設(浜松市中区)に用地を貸し出し、昨年7月から運営している。

須山建設が運営する東発電所は、増設分1.3㌶(出力は500㌔)と合わせて、計3.5㌶(1500㌔)になる。シーテックの西発電所と合わせると、3490㌔で、発電量は1750世帯の年間電力使用量に相当する。

“おおまぴょん”柄でPR

大町市　CATVが新取材車導入

おおまぴょんの姿が描かれた新車両

市営の大町市ケーブルテレビは15日、新しい取材専用車両を導入した。車体には大町市キャラクター「おおまぴょん」の姿がラッピングされ、市民に親しまれるケーブルテレビスタッフの足として、取材に奔走する。

新車両はスズキの軽自動車ハスラーで、おおまぴょんの色に合わせ、車体の柄は青色のボディと白い屋根。車両の左右とリアドアにおおまぴょんが描かれた。

CATVではこれまで取材専用車はなく、公用車を利用。メンテナンスなど共有しているため、取材に活用できないこともあった。親しまれるCATVとして、より円滑に取材活動を行い、市民の理解とPR効果を得られる車両とした。今後はアルプスマラソンなどの取材時に活躍する姿が見られそうだ。

市情報交通課ケーブルテレビ係の飯島大治係長は「行政として、災害などの情報もより伝えていかなければ。新たな取材車で多くの人に親しんでいただき、加入してもらえるようにしたい」と話した。

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。

組織暗号実証実験の今後

組織暗号実証実験は、研究開発をすすめている組織暗号の実用化に向けた重要な一歩。

今後も、機会をとらえ、組織暗号の有用性・有効性を広くご理解いただくため、実証実験を実施予定。

現在計画中の実証実験は以下の通り。

11月7日　箕輪町役場（長野県）

11月21日　燕市役所（新潟県）

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す。

今回の調査研究の機会をいただいた、独立行政法人情報通信研究機構（NICT）、中央大学・研究開発機構、およびアドバイスをいただいた辻井研究室の方々に感謝いたします。

終