Vol.2013-DPS-154 No.51
Vol.2013-CSEC-60 No.51
2013/3/15

# 企業間におけるデータ交換方式の提案

大越冬彦[†1]　　桜井鐘治[†1]

これまで企業間でデータ交換を行う場合にはデータを電子メールに添付して送付するのが一般的であった．しかし電子メールでは送信可能なデータサイズの制限や，誤送信などによる情報漏えいなどの問題があるため，データ交換サービスを用いる場合が増えてきた．データ交換サービスは送信時にデータの暗号化を行い，受信時に復号化を行うことで安全にデータを交換するものである．企業におけるデータ交換サービスでは，上長などの承認者の承認が必要な場合があり，この場合に暗号化データを承認者に閲覧させる方法が課題となっていた．今回データ交換サービスにおいて，暗号化手法に関数型暗号を用いることを検討した．検討の結果，承認者及び受信者に関する条件を暗号化時に指定することにより，承認者によるデータの閲覧が可能となり，データを安全に処理することを可能とした．またデータ暗号化時に社外のデータ交換サービスに受信者の属性を問い合わせることにより，社外の受信者に対してもデータ交換を行うことを可能にした．

# A proposal of the data exchange system between companies

FUYUHIKO OKOSHI[†1]　　SHOJI SAKURAI[†1]

It was common to have attached data to an E-mail and to have transmitted to it when transmitting data between companies. However, it was problems that big data cannot be transmitted by E-mail and that there is a risk of information being leaked by transmission to incorrect address. For this reason, using data exchange service has increased. The data exchange service encrypts data at the time of transmission, and it exchanges data safely by decrypting at the time of reception. In the data exchange service in a company, the approval of an acknowledger may be required at the time of transmission, and it is required for an acknowledger to inspect the encrypted data. We examined using a function type code for the encryption technique in data exchange service this time. As a result of examination, by specifying the attribute about an acknowledger and a recipient at the time of encryption, the inspection of the data by an acknowledger was allowed and it made it possible to process data safely. Moreover, by asking external data exchange service a recipient's attribute at the time of data encryption, data exchange to the external recipient was made possible.

## 1. はじめに

これまで企業間でデータ交換を行う場合には電子メールに添付して送付するのが一般的であったが，送信可能なデータサイズに制限がある，誤送信などに起因する情報漏えいの危険などの問題があり，データ交換サービスを用いる場合が増えてきた．データ交換サービスは送信時にデータの暗号化を行い，受信時に復号化を行うのが一般的である．

一方で企業におけるデータ交換サービスでは，上長などの承認者による送信の承認機能を持つ場合があり，この場合に暗号化データを承認者による閲覧させる方法が課題となっていた．

上記の課題を解決するために企業内のワークフローシステムの暗号化手法に関数型暗号を用いることが提案されている[1]．今回は企業間におけるデータ交換サービスにおいて，セキュリティと利便性を両立させるため，暗号化手法に関数型暗号を用いることを検討した結果について述べる．

今回提案する方式では，データ交換サービスで交換するデータを送信者，（複数の）承認者，（複数の）受信者のみが復号可能な関数型暗号を用いることで，データ交換サービスの承認経路上のセキュリティを確保するとともに，承認経路変更などについても一回の暗号化のみで対抗可能なデータ交換サービスを提供するものである．

本論文では，2.にてデータ交換サービスの概要，3.にてデータ交換サービスの課題，4.にて提案するデータ交換サービスについて述べ，5.にて考察を行い，最後にまとめを行う．

## 2. データ交換サービスの概要

これまで企業間で交換されるデータは，帳票や EDI データなどの定型データが主流であり，それらを前提としたサービスが存在している．

一方，企業活動の電子化に伴い，ワープロ文書や設計図面や画像・映像といったメディアデータを送付したいというニーズが増えてきている．

これまではこのようなデータを交換する場合，電子メールに添付して送信するか，CD や DVD などのメディアにコピーしてから郵送するなどの手法がとられてきた．しかしながら以下のような問題点があった．

- 電子メール添付では送信するデータのサイズに制限があるとともに，宛先間違いによる誤送信などのセキュリティ事故が頻発している．また安全のためにデータを暗号化する場合には添付時に人手で実施しなけ

†1 三菱電機株式会社 情報技術総合研究所
Information Technology R & D Center, Mitsubishi Electric Corporation

Vol.2013-DPS-154 No.51
Vol.2013-CSEC-60 No.51
2013/3/15

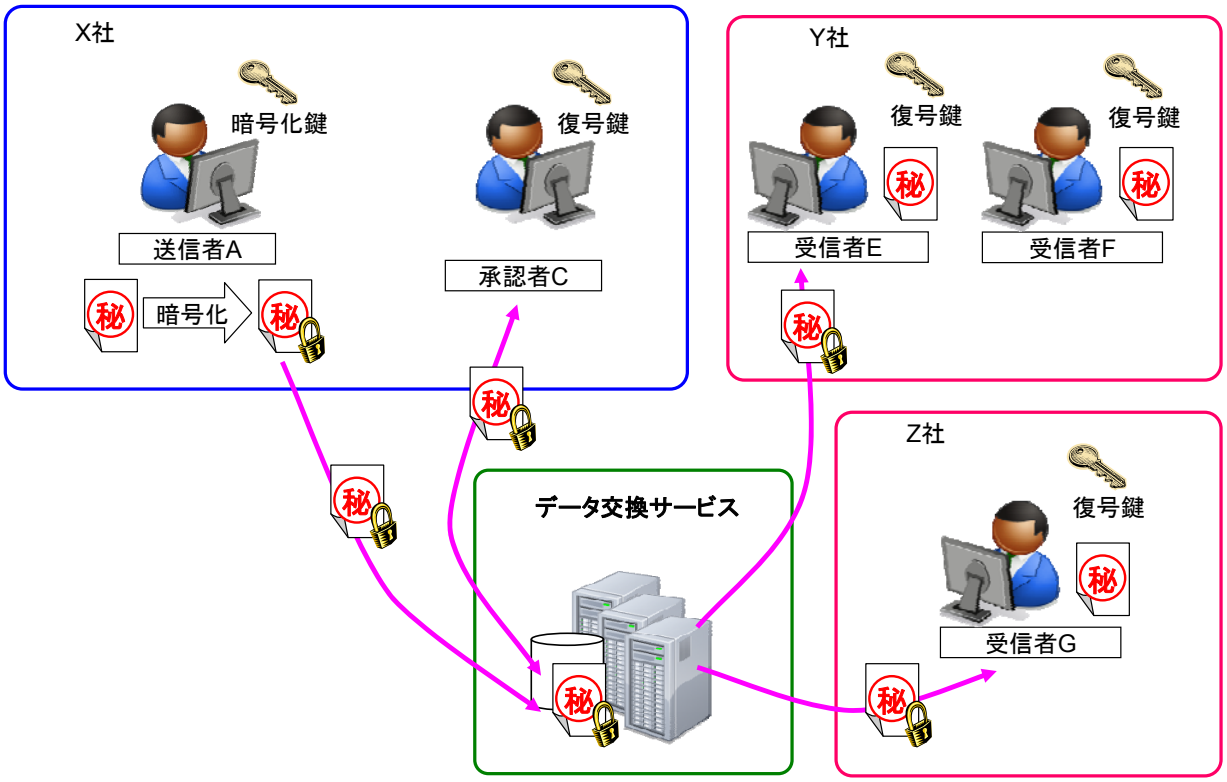


図 1 データ交換サービスの例

ればならず，不注意により平文のまま重要なデータを送信してしまう可能性がある．

- 郵送などの場合は到達まで時間がかかるとともに，物流経費がかかる．特に国外とデータを交換する場合にはこの傾向が顕著である．

これらの問題点を解決するのがデータ交換サービスである．データ交換サービスは，受信者が WEB ブラウザもしくは専用のアプリケーションを介してデータをネットワーク上のサーバやクラウドにアップロードし，宛先の受信者がそのデータをダウンロードするものであり，通信路の暗号化や蓄積データの暗号化により，安全性を高めている．

データ交換システムの中には，データ送信時に上長の承認を必要なワークフロー機能を有しているものもあり，企業などでの利用が始まっている．データ交換サービスの例を図 1 に示す．

## 3. データ交換サービスの課題

データ交換サービスでは利用者の事前登録や通信路の暗号化，データの暗号化などをサービス機能として保有するために，電子メールによるデータ添付などに比較すれば格段に安全である．またワークフロー機能を有する場合には不注意による誤ったデータ送信を承認者が否認することにより，情報漏洩を防止できる．しかしながら以下の部分にてセキュリティ上の課題が存在する．

### 3.1 パスワード伝達の問題

安全にデータを交換するためには，End-End での暗号化が有効であるが，このためには復号化のためのパスワードを送信者と受信者で共有する必要がある．このため，多くの場合，送信者が自分で受信者にパスワード情報をメールで送信するか，サービス側で自動的にデータ受信通知とは別のメールにてパスワードを通知する場合が多い．

しかしこの場合には，悪意ある者によって受信者のメールアカウント自体が乗っ取られていた場合や，PC 内部のメールソフトウェアのフォルダデータが流出した場合には，データ配信通知メールとパスワード通知メールが同時に漏洩し，悪意のある者によってデータをダウンロード，復号されてしまう．

これらを防ぐためには，パスワードを電話や FAX など別メディアで伝える必要があるが，これは利便性の面が劣るとともに，時差のある海外との間のデータ交換では実用的でない．

### 3.2 データ暗号化における課題

データ交換システムにおいて，ワークフロー機能を有するものでは，承認者は送信者が添付したデータの内容を確認する必要があるため，

Vol.2013-DPS-154 No.51
Vol.2013-CSEC-60 No.51
2013/3/15

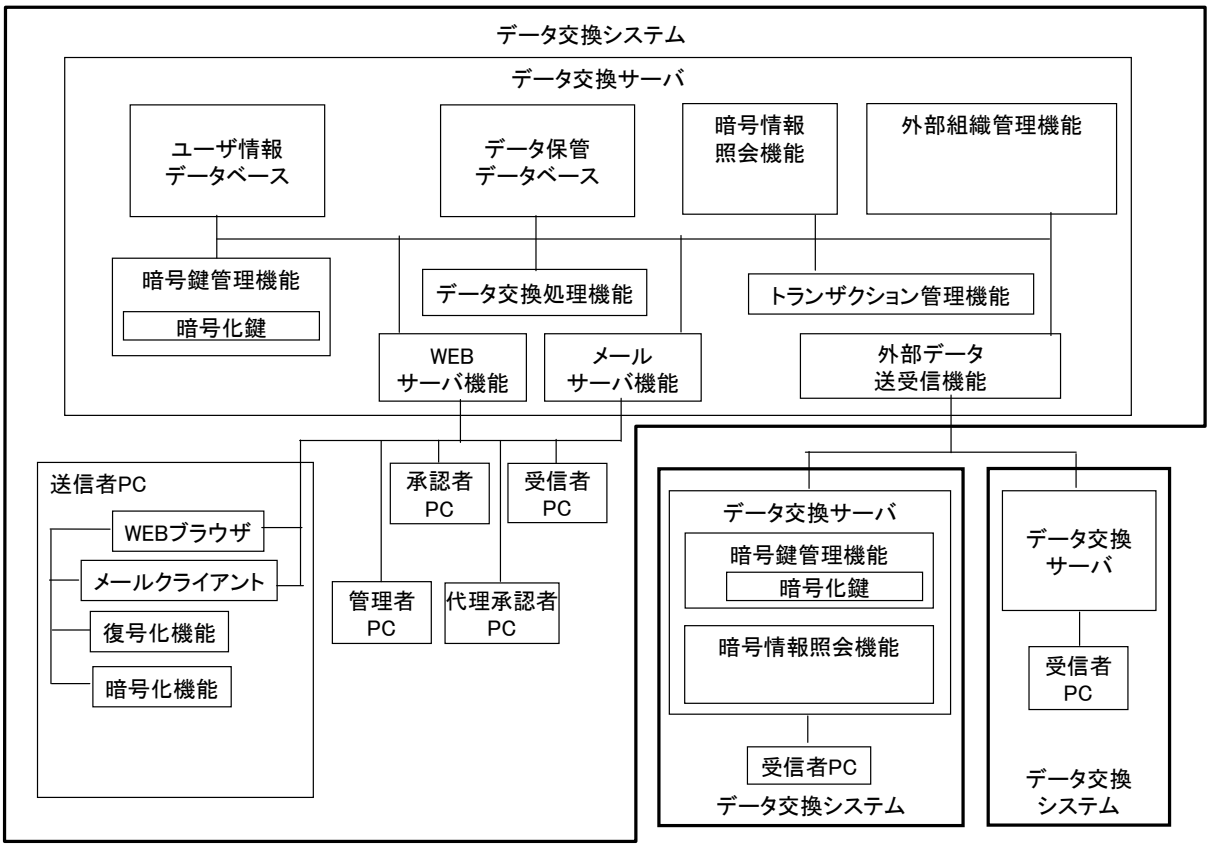


図 2 システム構成

- 送信者がデータを送信する時に暗号化を実施し，送信者，承認者，受信者が複号鍵を共有する場合．データ送信時からデータは暗号化されるが，共通鍵を 3 者以上で共有する必要があり，セキュリティ上の問題となる．
- 送信者がデータを平文で送信し，承認者が承認後にシステムが暗号化を実施する場合．送信者がデータを送信してから最終承認者が承認するまでストレージ上に暗号化されていないデータが保存される点で，セキュリティ上問題がある．

## 4. 提案するデータ交換サービス

企業間におけるデータ交換サービスにおいて，セキュリティと利便性を両立させるために，暗号化方式として関数型暗号を用いたデータ交換サービスを考える．

関数型暗号は，暗号化と復号化の鍵それぞれがあるパラメータによって定まっていることが特徴である．例えば，暗号化するときにあるＸというパラメータを持った暗号化鍵を使い，その暗号文を復号化するときにはあるＹというパラメータを持った復号鍵で復号化する．そして，このＸとＹがある論理関係を満たすときにのみ正しく復号化ができるという特徴がある[2][3].

このパラメータには AND，OR，NOT を任意に組み合わせた論理式が指定可能であり，本方式ではデータ交換サービスが管理している所属情報を論理式に割り当てることにより，承認経路のみの承認者および受信者が復号可能なデータの暗号化を行う．

表 1 データ交換サービス構成

| 名称 | 機能 |
|---|---|
| データ交換処理機能 | データ交換処理を実行 |
| 暗号鍵管理機能 | 暗号鍵生成及び管理 |
| トランザクション管理機能 | データ交換システム間の通信を同期 |
| 暗号情報照会機能 | 社外のユーザ情報を照会 |
| 外部組織管理機能 | 他のデータ交換システムと接続する際のネットワークアドレス情報を管理 |
| 外部データ送受信機能 | 他のデータ交換システムと通信 |
| ＷＥＢサーバ機能 | クライアント PC に対して画面 I/F を提供 |
| メールサーバ機能 | クライアント PC に対して通知メールを受信 |
| ユーザ情報データベース | ユーザ情報の記録及び管理 |
| データ保管データベース | データの記憶及び管理 |

Vol.2013-DPS-154 No.51
Vol.2013-CSEC-60 No.51
2013/3/15

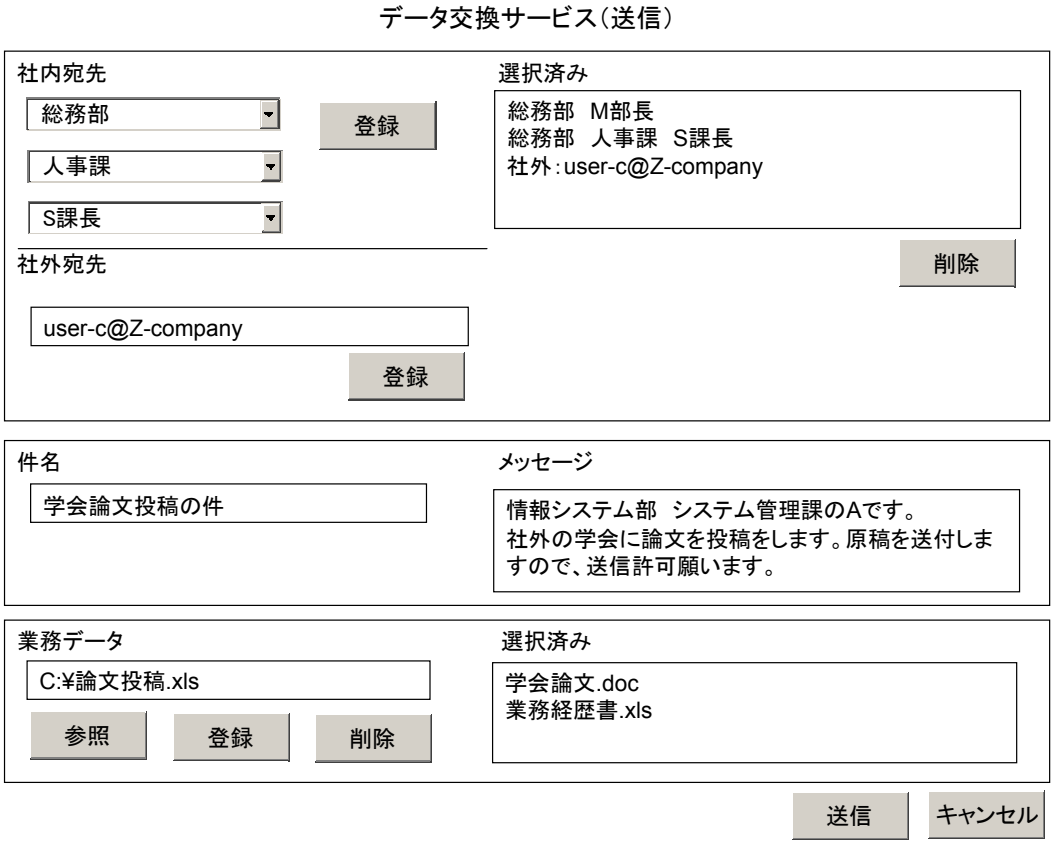


図 3 データ交換サービス画面例

### 4.1 システム構成

提案方式のデータ交換サービスのシステム構成図を図 2 に示す．

データ交換サービスは企業ごとに設置されたデータ交換システムから構成する．データ交換システムは，データ交換サーバ，ユーザ PC（送信者，承認者，代理承認者，受信者，管理者）から構成される．各ユーザ PC は WEB ブラウザ，メールクライアント，暗号化および復号化を行うモジュールから構成している．データ交換サーバは，データ交換処理機能，暗号鍵管理機能，トランザクション管理機能，暗号情報照会機能，外部組織管理機能，外部データ送受信機能を有する．データベースはユーザ情報データベース，データ保管データベースである．これらの機能及びデータベースを表 1 に示す．

### 4.2 動作

本データ交換サービスの動作は以下の通りである．

(1) **ユーザ登録**

個々のデータ交換システムのシステム管理者は管理者 PC を用いて自社のデータ交換サービスのユーザ（送信者，承認者，代理承認者，受信者）をユーザ情報データベースに登録するとともに，暗号鍵管理サーバを用いて各ユーザの復号鍵を生成し，ユーザが使用する PC に記憶させておく．また社外のデータ交換システムの情報を登録しておく．

(2) **送信処理**

送信者は送信者 PC から WEB サーバ経由でデータ交換サービスにアクセスして，データを登録する．送信者 PC は送信者が入力したデータをデータ交換サービスに送信する．このときに PC 内の暗号化/複合化機能にてデータを暗号化する．受信者が社外の場合には暗号化に用いる鍵と属性情報を該当する受信者が所属するデータ交換システムから得る．送信したデータはデータ保管データベースに保存される．この時の画面例を図 3 に示す．

(3) **承認者選択**

データ交換処理機能は，承認者の在席状況を確認する．承認者が在席している場合，データ交換処理機能はその承認者にメールサーバ経由でデータ交換処理依頼メールを送信する．承認者がデータ交換システムに対して不在登録を行っている場合，データ交換処理機能は，予め定めてある優先順位に従って代理承認者を選択し，データ交換処理機能はその代理承認者にデータ交換処理依頼メールを送信する．

(4) **承認処理**

承認者もしくは代理承認者は，自己の PC を用いて，データ交換システムから送信者が送信したデータをダウンロードする．ダウンロードされたデータは承認者もしくは代理承認者 PC の暗号化/復号化モジュールにより復号化される．承認者もしくは代理承認者はデータの内容を確認して，適正であればデータ交換の承認を行い，適正でなければ，否

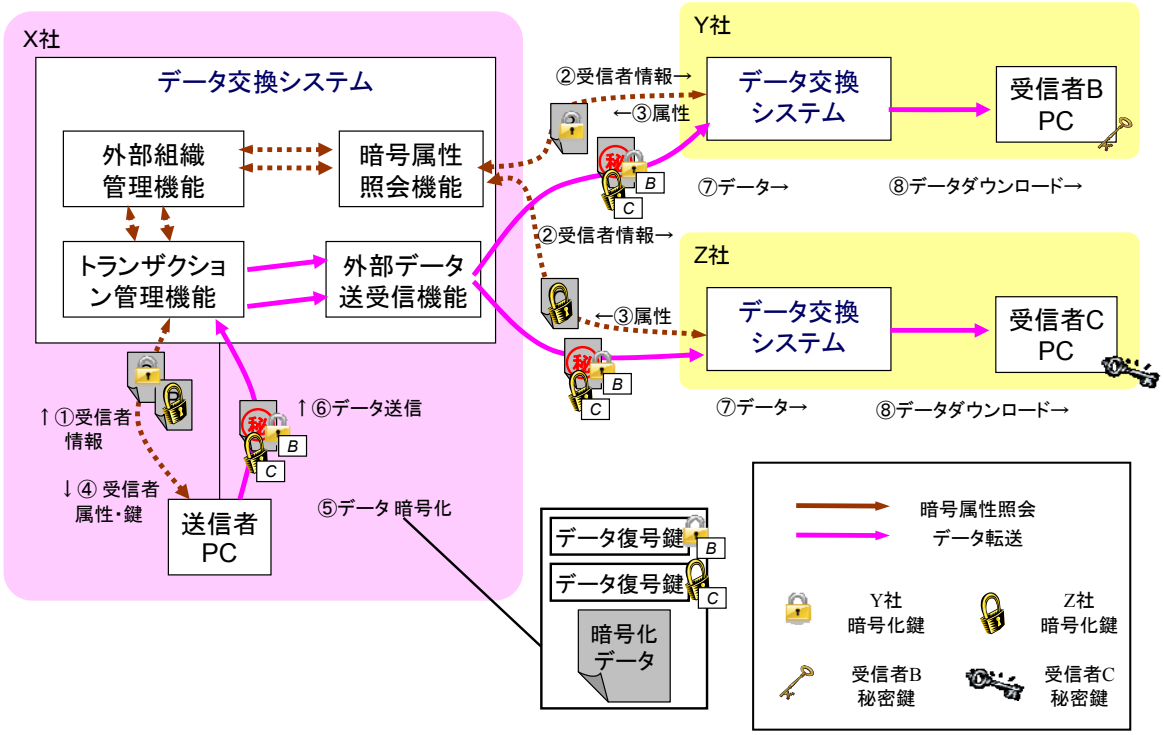


図 4 暗号化手順

認を行う.

(5) **受信通知**

データ交換が承認された場合，データ交換サービスはデータ受信通知メールを受信者に送信する．受信者が社外であった場合には，受信者が所属するデータ交換システムを介してメールを送信する.

(6) **受信処理**

受信者は受信者 PC を利用してデータ交換サービスから送信者が送信したデータをダウンロードする．ダウンロードされたデータは受信者 PC の暗号化/復号化モジュールにより復号化される.

### 4.3 暗号化手順

送信者が社外の受信者宛にデータを送信する場合には，受信者が複号可能な関数型暗号で暗号化する必要がある．暗号化には以下が必要である.

- 相手組織の暗号鍵
- 相手の属性

これらについては送信者のデータ送信時処理において，自社のデータ交換システムの暗号情報照会機能と受信者が所属するデータ交換システムの暗号情報照会機能を介して，相手組織のデータ交換システムに都度照会を行うことにより，取得する．送信者 PC は宛先となる社外の受信者の属性と暗号化鍵を照会するため、データ交換システムに受信者情報を送信する。

① 外部組織管理機能により受信者が所属するデータ交換システムを特定し、暗号属性照会機能により受信者が所属するデータ交換システムに接続し受信者情報を送信する。

② 受信者が所属するデータ交換システムの暗号属性照会機能は受信者情報から、受信者属性を検索して暗号化鍵とともに返す。

③ 送信者 PC は宛先の受信者属性と暗号化鍵を得る。

④ 送信者 PC はデータを暗号化する。この時、宛先の企業が異なる場合には暗号化データを共有できない．このため，データ自体の暗号化は共通鍵を都度生成して，共通鍵で暗号化を行い，この共通鍵自体を各社の暗号鍵で暗号化することにより，暗号化データの増大を避ける.

⑤ 送信者 PC は暗号化データを送信する。

⑥ 送信者が所属するデータ交換システムの外部データ送受信機能は受信者が所属するデータ交換システムの外部データ送受信機能に対してデータを送信する。

⑦ 受信者 PC は受信者が所属するデータ交換システムからデータをダウンロードし、受信者の秘密鍵でデータを復号化する。

図 4 にデータ暗号化手順を示す.

Vol.2013-DPS-154 No.51
Vol.2013-CSEC-60 No.51
2013/3/15

### 4.4 関数型暗号による暗号化

関数型暗号では暗号化時の条件式指定に，AND，OR，NOT を任意に組み合わせた論理式が利用可能である. このため，氏名，所属，役職などの各種条件に応じた暗号化が可能となる.

たとえば X 社技術部第 3 課の A が発注仕様書を社外に送付する場合を考える．発注先は販売元 Y 社のシステム部 2 課の所属員，代理店 Z 社の担当 G である．X 社の発注手続きには自己が所属する部の課長以上の役職を持つ者の承認が必要である．また発注仕様書には技術情報が記載されており，社内規則により暗号化が必要となっている．このため暗号化時に復号化可能な属性として以下の条件が必要である.

- 送信者本人であること
- 送信者の所属する部の課長以上であること
- 指定された受信者であること

つまり

| |
|---|
| 氏名＝A OR (所属部＝技術部 AND (役職＝課長)OR(役職＝部長)) OR (組織＝Y AND 所属＝システム部 2 課) OR（組織＝Z　AND 氏名＝G） |

となる．この復号条件においてはたとえば A の同僚である B が暗号化されたデータを手に入れても復号できず，Z 社の受信者でない H も復号できない. 一方で X 社の技術部の課長以上であれば復号可能なため，C 課長が不在の際にも D 課長の代理承認が可能となる．また Y 社ではシステム部 2 課の所属員であれば復号可能なため，担当の不在や多忙による業務の遅延が防止できる．表 2 に関数型暗号による復号可否状況を示す.

表 2 復号可否

| 組織 | X 社 | | | | Y 社 | | Z 社 | |
|---|---|---|---|---|---|---|---|---|
| 所属 | 技術部 3 課 | | | 技術部 2 課 | システム部 2 課 | | 営業部 1 課 | |
| 役職 | － | | 課長 | 課長 | － | | － | |
| 氏名 | A | B | C | D | E | F | G | H |
| 復号 | ○ | × | ○ | ○ | ○ | ○ | ○ | × |

## 5. 考察

本方式の効果と課題について考察する.

本方式はデータ交換サービスの暗号化方式に関数型暗号を利用することで，承認者及び受信者に関する条件を暗号化時に指定することにより，承認者によるデータの閲覧が可能となり，データを安全にデータ交換サービスで処理することを可能とした．またデータ暗号化時に社外のデータ交換サービスに受信者の属性を問い合わせることにより，社外の受信者に対してもデータ交換を行うことを可能にした.

一方で本方式はデータ交換システムと人事管理システムやディレクトリサービスとの連携が必要であり，それらの整備を合わせて実施する必要がある．また各社にデータ交換システムの導入が必要であるため，当面はグループ会社間などでの利用に限定される．システムの構成要素の仮想化により，クラウドサービス化により導入コストを低減させることも検討する必要がある.

## 6. おわりに

本提案方式は，企業間の安全なデータ交換を実現するものである．今後，本提案方式の実装と評価を図っていく.

## 参考文献

1) 大越他,セキュリティと利便性を確保したワークフローシステム，DPS150CSEC56-27,2012
2) 三菱電機 ニュースリリース「クラウド時代の高度なセキュリティー対策を実現する新世代暗号方式を開発」
http://www.mitsubishielectric.co.jp/news/2010/0728.pdf
3) Okamoto and Takashima, Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption, CRYPTO 2010, pp.191-208 (2010)