Vol.2012-DPS-150 No.27
Vol.2012-CSEC-56 No.27
2012/2/29

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

大越冬彦[†]　　桜井鐘治[†]

ワークフローシステムにおいて，セキュリティと利便性を確保するため，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．提案方式では，ワークフローシステムに複数の承認者及び受信者のみが復号可能な関数型暗号を導入する．本提案方式により，ワークフローの経路上のセキュリティを確保するとともに，承認者不在時などの承認経路自動変更など柔軟な対応が可能となる．

Workflow system ensures security and convenience

Fuyuhiko Okoshi[†]　and Shoji Sakurai[†]

We propose a workflow system which uses a functional encryption scheme to ensure both security and convenience. In our proposing method, the functional encryption scheme in the workflow system to allow approvers and recipients to decrypt the encrypted workflow messages with their own keys. Because of the functional encryption scheme, the workflow also enables automated approval re-routing when the approvers are absent.

1. はじめに

2005 年に施行された「e-文書法」により，企業における業務の電子化が進行し，これまで紙書類の配送によって行われてきた業務が，電子データの転送・共有で行われるようになった．また，検印を用いて実施されてきた承認処理についてもワークフローの導入により電子化されつつある．

一方で業務の電子化に伴い，社員による不正情報持ち出し，ウィルスやマルウェア感染，電子メールの誤送信などに起因する情報漏えい事故が後を絶たず，その対策として機密情報の暗号化などの対策が推奨されている [1].

暗号化されたデータをワークフローシステムで取り扱う場合，ワークフローの最終受信者がデータを復号化できるだけでなく，ワークフロー経路上の必要な承認者がデータを復号化して内容を確認できる必要がある．しかしながら従来の暗号化手法は，暗号鍵と復号鍵がペアになっているため，複数人の間で同じ暗号化データを復号化するには問題があった．

今回提案する方式では，ワークフローに添付するデータファイルを送信者，（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，ワークフロー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ワークフォローシステムで提供するものである．

2. ワークフローシステム

2.1 ワークフローシステムの概要

ワークフローシステムは予め業務ごとに定められた社内承認経路に基づいたワークフロー経路にワークフローデータを転送することにより，業務処理を行うものである．これまで専用のパッケージソフトウェアを中心に構成されていたが，近年は WEB サーバをベースとしたシステムが主流となりつつある．この形態の場合，画面操作は WEB ブラウザによって画面操作を行い, 通知や督促などに電子メールを利用するのが一般的である [2].

一例として送信者(担当者)が作成したワークフローデータは承認者(課長)，承認者(部長)，受信者(課長)，受信者（担当）という順序で転送される．承認者はデータの内容を確認し，適切であれば承認を行い，そうでなければ否認を行う．承認されたワークフローデータはワークフロー経路上の次の承認者もしくは受信者に転送され，否認されたワークフローデータを送信者に差し戻す．これを繰り返して最終宛先に指定された受信者にワークフローデータが届き業務が実行される．

[†] 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.2012-DPS-150 No.27
Vol.2012-CSEC-56 No.27
2012/2/29

ワークフローシステムの例を図 1 に示す.

近年では内部統制の観点より，業務の証跡を残すためにワークフローシステムを導入し，データやログを記録する場合もある[3].

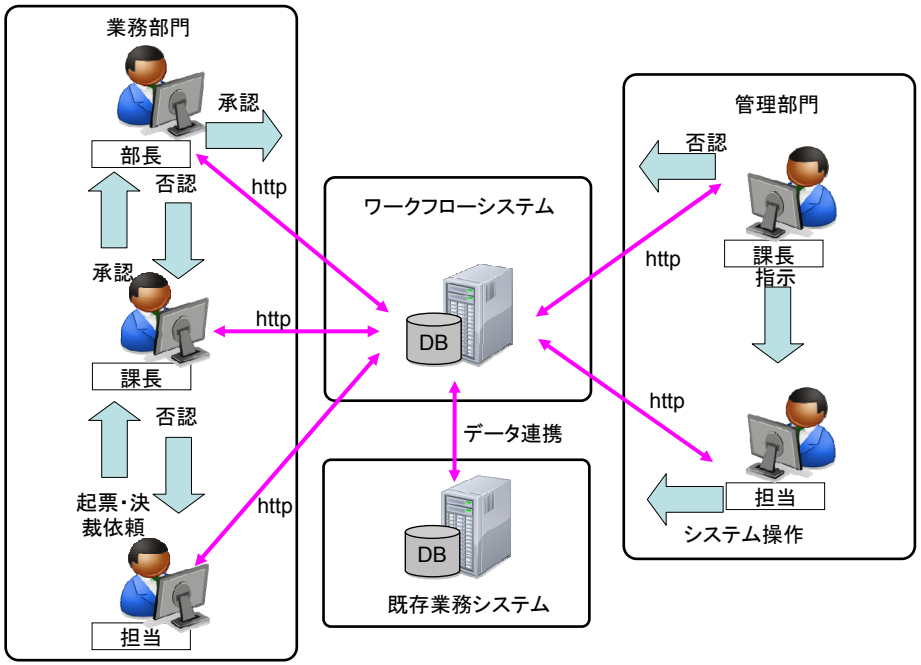

図 1　ワークフローシステムの例

3. ワークフローシステムの課題

企業の業務においては，文書処理ソフトウェアや表計算ソフトウェアを用いており，これらソフトウェアのデータファイル利用を前提に業務が構成されている場合も多い．このためワークフローシステムの導入時に，これらのデータファイルをワークフローデータに添付してワークフローを構成する場合がある．

ワークフローシステムは利用者登録，受信者登録が前提となっているためデータファイルを添付する場合には，電子メールによるデータファイルの添付や共有ファイルサーバによるデータファイルの共有などよりもセキュリティ上有利であると考えられる．しかし以下の場合，暗号化を実施したほうがよりセキュリティが向上する．

- 閲覧者を限定すべき機密度の高い企業機密を含んだ情報や個人情報などを含んだデータファイルを扱う場合
- システムの一部もしくは全てをストレージやクラウド等の社外サービスで構成する場合

暗号化を行うことで，システムに対して特権を有した社員や，サービス提供会社の不備による情報漏えいを予防できる．しかしながら暗号化を行う場合次の課題がある．

3.1 データファイル暗号化における課題

送信するデータファイルを暗号化する場合，暗号化には共通鍵を用いる場合と，公開鍵を用いる場合が考えられる．承認者は送信者が添付したデータファイルの内容を確認する必要があるため，暗号化を行うタイミングには，送信者がワークフローを送信する時に実施する場合と，最終承認者が承認を行う時に実施する場合があり，以下の 4 つのパターンが考えられる．

(1) 共通鍵で送信時暗号化

送信者は予め，承認者，受信者間で共通鍵を取り決めておき別途連絡しておく．その共通鍵でデータファイルの暗号化を行い，ワークフローデータに添付して送信する．承認者は連絡された共通鍵でデータファイルを復号化し，ワークフロー承認の可否の判断する．ワークフロー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．

(2) 共通鍵で最終承認時暗号化

最終的な承認者と受信者間で共通鍵を取り決めておく．送信者は暗号化を行わずデータファイルを添付して送信する．最終的な承認者が承認を行う時点でデータを暗号化する．最終承認者が多数の受信者の鍵を管理する必要があり，現実的には利便性が損なわれる．また送信者がワークフロー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ファイルが保存される点で，セキュリティ上問題がある．

(3) 公開鍵で送信時暗号化

公開鍵暗号を用いる場合は，3 者以上で秘密鍵を共有することが困難であるため，送信者は全承認者と全受信者に対して個別の公開鍵を用いて暗号化データを作成する必要があり，処理負荷が高くなる．この場合，別途共通鍵暗号にてデータファイルを暗号化しておきその共通鍵を個々の公開鍵で暗号化することで処理負荷を下げることができるが，暗号化データに複数の鍵データを添付する必要がある．

(4) 公開鍵で最終承認時暗号化

送信者がワークフロー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

Vol.2012-DPS-150 No.27
Vol.2012-CSEC-56 No.27
2012/2/29

に平文データが保存される点で，セキュリティ上問題がある．
これらを図 2 に示す．いずれの場合でも，セキュリティと利便性を両立させることは難しいと考える．

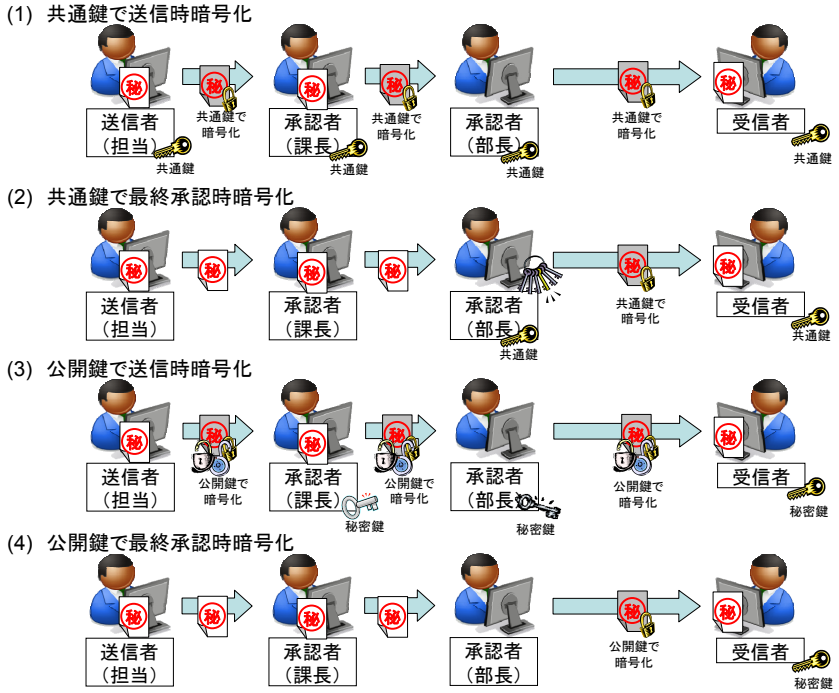

図 2　データファイル暗号化のパターン

3.2 代理承認時の課題

ワークフローシステムにおいては，送信者(例えば第 1 課所属員)が発行したワークフローの承認は原則として承認者(例えば第 1 課長)が実施するが，承認者不在時などの理由でワークフロー処理が滞留する場合がある．この対策として，同等の権限を持つ近傍の上長（例えば第 2 課長)が承認を行う場合が想定される．

その際に送信者によるデータファイルの暗号化が行われていた場合，代理承認者に共通鍵情報を伝達するか，代理承認者の公開鍵を用いてデータファイルを暗号したデータを追加して添付し直す必要がある．

4. 提案方式

データファイル暗号化を行うワークフローシステムにおいて，セキュリティと利便性を両立させるワークフローシステムを実現するために，暗号化手法として関数型暗号を用いたワークフローシステムを提案する．

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[4][5].

このパラメータには AND，OR，NOT，閾値ゲートを任意に組み合わせた論理式が指定可能であり，本提案方式ではワークフロー内部で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，承認経路のみに承認者および受信者が復号可能なデータファイルの暗号化を行う．

4.1 システム構成

本提案方式のワークフローのシステム構成図を図 3 に示す．

システムはワークフローシステムを構成するサーバ群及び，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される．ワークフローシステムを構成するサーバ群は暗号鍵管理サーバ，ユーザ情報データベースサーバ，ワークフローデータベースサーバ，ＷＥＢサーバ，メールサーバ，ワークフロー処理サーバから構成される．これらのサーバの機能を表 1 に示す．

表 1　ワークフローシステム構成サーバの機能

名称	機能
ワークフロー処理サーバ	ワークフロー処理を実行
ユーザ情報データベースサーバ	ユーザ情報の記録及び管理
ワークフローデータベースサーバ	ワークフローデータの記憶及び管理
WEBサーバ	各 PC に対して画面 I/F を提供
メールサーバ	各 PC に対して通知メールを受信
暗号鍵管理サーバ	暗号鍵生成及び管理

Vol.2012-DPS-150 No.27
Vol.2012-CSEC-56 No.27
2012/2/29

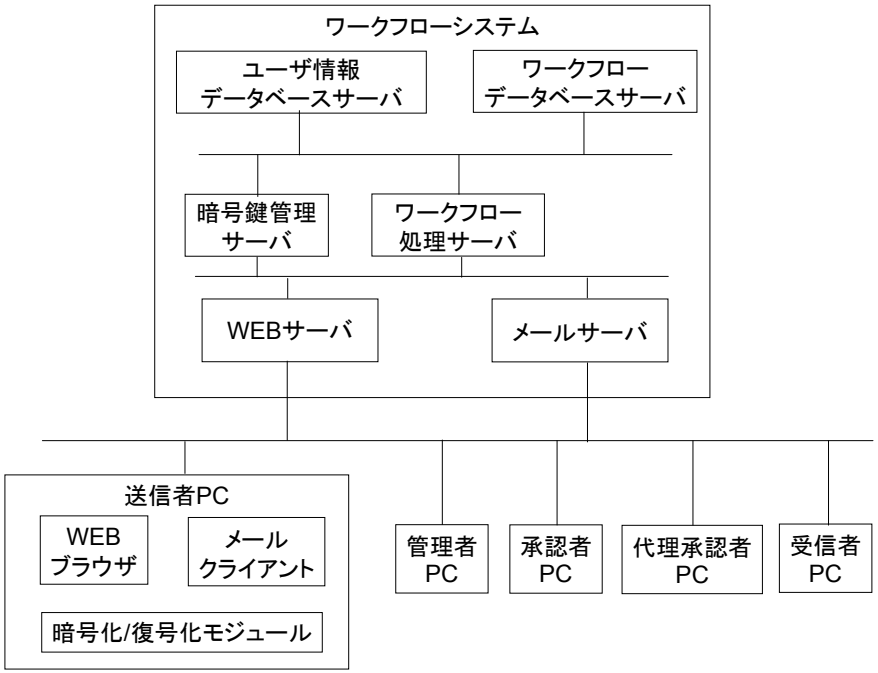

図 3　システム構成図

4.2 動作

本ワークフローの動作は以下の通りである．

(1) ユーザ登録

システム管理者は管理者 PC を用いてワークフローシステムのユーザ（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．

(2) 送信処理

送信者は送信者 PC から WEB サーバ経由でワークフローシステムにアクセスして，ワークフローを作成する．送信者 PC は送信者が入力したワークフローデータとデータファイルをワークフローシステムに送信する．このときに PC 内の暗号化/復号化モジュールにてデータファイルを暗号化する．送信したデータはワークフローデータベースに保存される．この時の画面例を図 4 に示す．

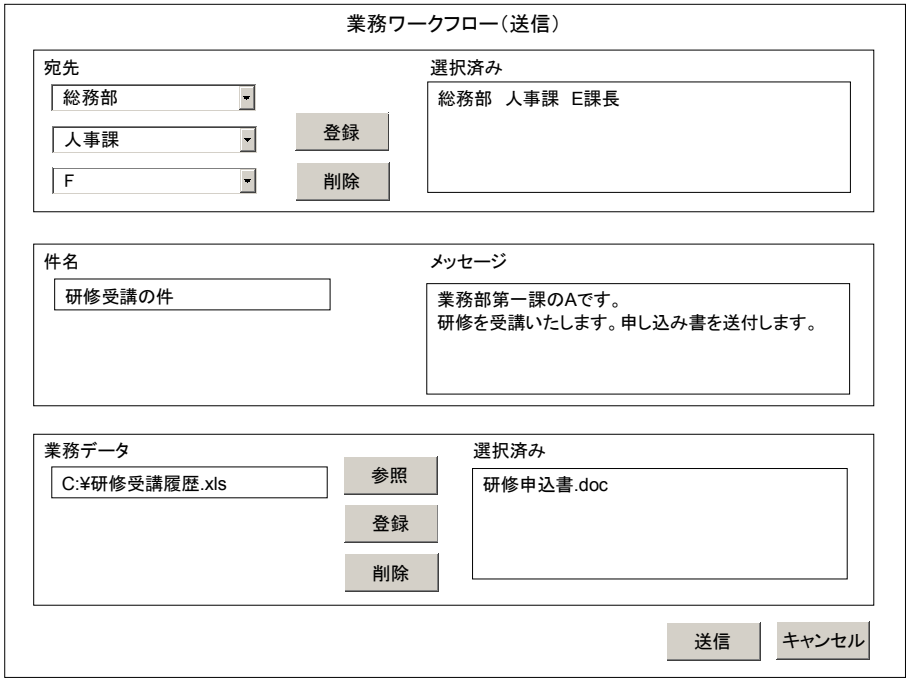

図 4　ワークフロー画面例

(3) 承認者選択

ワークフロー処理サーバは，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，ワークフロー処理サーバはその承認者にメールサーバ経由でワークフロー処理依頼メールを送信する．承認者がワークフローシステムに対して不在登録を行っている場合，ワークフロー処理サーバは，予め定めてある優先順位に従って代理承認者を選択し，ワークフロー処理サーバはその代理承認者にワークフロー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，ワークフローシステムから送信者が送信したデータファイルをダウンロードする．ダウンロードされたデータファイル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ファイルの内容を確認して，適正であればワーク

Vol.2012-DPS-150 No.27
Vol.2012-CSEC-56 No.27
2012/2/29

フローの承認を行い，適正でなければ，否認を行う．

(5) 受信通知

ワークフローが承認された場合，ワークフローシステムはワークフロー受信通知メールを受信者に送信する．

(6) 再送信

ワークフローが否認された場合，ワークフローシステムはワークフロー否認通知メールを送信者に送信する．送信者は，ワークフローおよびデータファイルを修正してワークフローを再送信する．

(7) 受信処理

受信者は受信者 PC を利用してワークフローシステムから送信者が送信したデータファイルをダウンロードする．ダウンロードされたデータファイルは受信者 PC の暗号化/復号化モジュールにより復号化される．受信者はファイルの内容を閲覧して，その内容に基づいて自己の業務を行う．

これらの動作を図 5 に示す．

4.3 関数型暗号による暗号化

送信者がワークフローシステムに送信するデータファイルは，複数の許可されたユーザのみ閲覧すべきファイルである．従来の暗号化手法では，1 つの暗号化鍵に対して，1 つの復号化鍵のみが対応しており，複数のユーザが復号可能なデータを作成することはユーザ間で復号鍵の共有を行うかユーザごとに暗号化を行う必要があった．関数型暗号では暗号化時の条件式指定に，AND，OR，NOT，閾値ゲート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．

たとえば業務部第 1 課の A が研修申し込み処理を行う場合を考える．住所変更業務は管理部人事課の課長 E が管理しており，F が担当している．研修申し込み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．研修申し込みには個人情報を含んだデータファイルをワークフローにて送付する必要があり，社内ルールにて暗号化するルールとなっている．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を指定する．

- 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=業務部 AND 役職≧課長) OR 氏名＝E OR 氏名=F

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ファイルを手に入れても復号することはできない．同様に管理者である管理課の G も復号化できない．表 2 に関数型暗号による復号可否状況を示す．

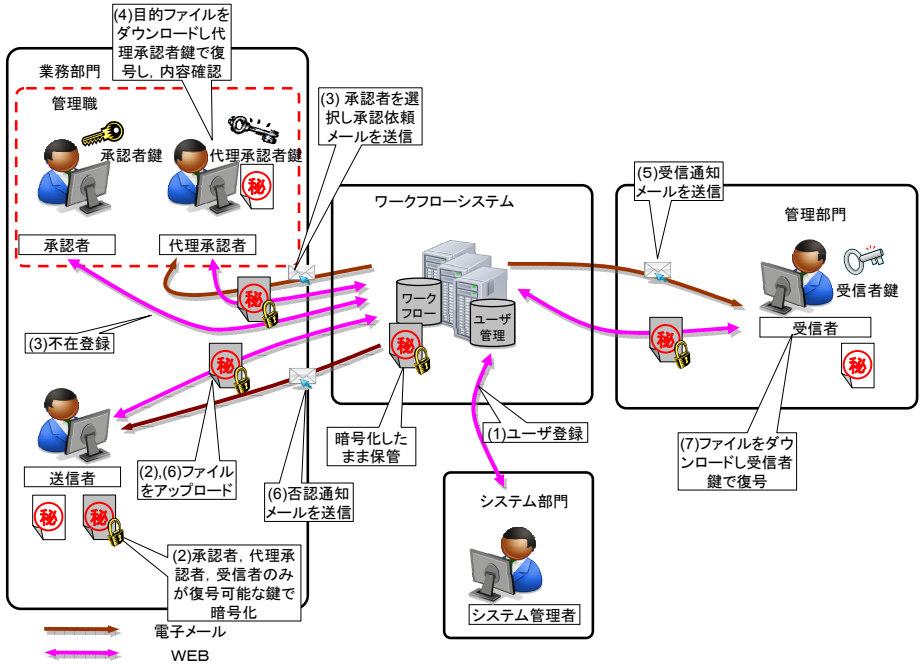

図 5 ワークフロー動作

表 2 復号可否

氏名	A	B	C	D	E	F	G
所属部	業務部				総務部		
所属課	第 1 課			第 2 課	人事課		管理課
役職	―		課長			―	
復号	○	×	○	○	○	○	×
備考	発信者	―	承認者	代理承認者	受信者	受信者	管理者

復号条件として利用

Vol.2012-DPS-150 No.27
Vol.2012-CSEC-56 No.27
2012/2/29

5. 考察

本提案方式の効果と課題について考察する.

本提案方式はワークフローシステムの暗号化手法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,データファイルを暗号化したまま,承認者の承認が可能となり,データファイルを安全にワークフローシステムで処理することを可能とした.暗号化処理は,承認者や宛先が増えても一回のみであり,処理速度が向上する.またデータファイル全てを暗号化するのではなく,通常の共通鍵暗号にてデータファイルを暗号化し,その鍵を関数型暗号にて暗号しても良い.

予め承認者の属性を暗号化時属性に含めておくことで,承認者が不在の場合でも再暗号化なしで代理承認者が復号可能である.この特性を利用して,本提案ではワークフローシステムによる自動的な代理承認者へのワークフロー処理の回送を可能とした.これにより,承認者が不在の場合にワークフローが滞留し,結果として業務遅延の発生を抑止する効果がある.

一方で本提案方式では復号鍵を各ユーザに事前に配布しておく必要があり,この手段の確立が課題である.特に企業の場合,組織変更や人事異動などが頻繁に発生する.復号鍵の管理について,その時点の組織情報を反映しておく必要があるが,一方でワークフローに記録された情報は内部統制の観点より業務の証跡を残す場合がありこの面では過去の組織情報も残しておく必要があることを考慮しなければならない.
本課題を解決するためには,ワークフローシステムのみならず,既存の人事や組織の管理を行うシステムとの連携が欠かせないと考える.なおワークフロー処理サーバと各 PC 間の通信路が安全であれば暗号化,復号化をワークフローシステム側で実施する形式も有効であり,この場合には復号鍵の配布,管理の手間が軽減される.

6. おわりに

今回提案した方式は,企業内のワークフローを対象としたものであるが,企業間の安全なデータファイル転送などにも応用可能と考える.今後,実用化に向けた課題の解決を行い,本提案方式の実現を図っていく.

参考文献

1) IPA「電子メール利用時の危険対策のしおり」,
http://www.ipa.go.jp/security/antivirus/documents/7_mail_v3.pdf
2) 三菱電機 ニュースリリース「汎用ワークフローシステム MELDandy Ver.5 発売のお知らせ」,http://www.mitsubishielectric.co.jp/news-data/2003/pdf/0626.pdf
3) NTT データ イントラマート「ワークフローは intra-mart ワークフロー」
http://www.intra-mart.jp/products/framework/imbiz_wf.html
4) 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
5) Okamoto and Takashima, Fully Secure Functional Encryption with General Relations from the Decisional Linear Assumption, CRYPTO 2010, pp.191-208 (2010)