マルチメディア通信と分散処理　101－9
コンピュータセキュリティ　12－9
（2001．2．20）

柔軟な権限委譲機能を備えたワークフローシステムの開発

湯浅 貴寛*　若山 公威*　村瀬 晋二**　鈴木 春洋**　岩田 彰*

* 名古屋工業大学　電気情報工学科
** 株式会社 シーティアイ SI事業部

ビジネス形態は複雑化し、複数の組織が一時的に連携し、一つの企業体統合として活動する機会が増えている。これらの組織間の円滑な業務連携を実現するための方法としてインターワークフローの構築が注目されている。しかし、そのためには、連携する組織がすべてインターワークフローに対応したワークフローシステムを持っていなければならない。だが、ワークフローシステムの導入経費は高額であり、小規模な組織などでは必要だからといって簡単に導入できる物ではない。そこで、本稿では、単一のワークフローシステム上での複数組織の連携を可能とするため、柔軟な権限委譲機能を備え、組織のプライバシ問題に配慮したワークフローシステムを提案し、実装を行った。

Development of Workflow System providing Flexible Delegation

Takahiro YUASA*　Kimitake WAKAYAMA*　Shinji MURASE**
Shunyo SUZUKI**　Akira IWATA*

* Nagoya Institute of Technology
** CTI Co., Ltd.

The business form has become more complex, it is often that act as one enterprise integration and several organizations cooperate temporarily. Actually the building of Interworkflow is in evidence as a method for achievement of smooth business cooperation between these organizations. However, a specific workflow system is needed in order to make the organizations cooperate each other. Even if there is necessity, it is not a easy thing for a small-scale organization to introduce the workflow system because a large amount of money is required. Therefore, in this paper, to enable cooperation of plural organizations on single workflow system, we propose and implement a workflow system which provides flexible delegation and protects the privacy of the organization.

1. はじめに

オフィスにおける業務は多種多様であるが、それらの大半が人や部門間で書類などを受け渡すことで成り立っている。しかし、このプロセスを人手によって行うと、ケアレス・ミスによる伝達の遅れや紛失などが発生する。そこで、仕事のプロセスをコンピュータ上で定義し、実行・制御することによって、業務の流れを管理・自動化し、これらの問題を解消するのがワークフローシステムの目的である。そして、近年、業務の処理時間短縮、精度の向上、管理の効率改善のため、ワークフローシステムを導入する組織が増えている。

一方、近年、ビジネス形態は複雑化し、単一の組織内で業務プロセスが完了せず、複数の組織が一時的に連携し、一つの企業体統合として活動する機会が増えている。これらの組織間のスムーズでシームレスな連携を実現するための方法としてインターワークフローの構築が上げられる[1][2]。元来、ワークフローシステムは単一組織内での運用を想定していたが、これらのシステム同士を組織の枠を越え相互に接続し、連携させたものがインターワークフローである。しかし、インターワークフローを実現するためには、連携する組織がすべてインターワークフローに対応したワークフローシステムを持っていなければならない。だが、ワークフローシステムの導入経費は高額であり、小規模な組織などでは必要だからといって簡単に導入できる物ではない。そこで、代表の組織、もしくは第三者がワークフローシステムを運用し、そのシステム上で複数の組織が連携する、といった形態が考えられる。

ところで、このように組織が連携する場合、業務プロセスがこの連携関係の中だけで完結するとは限らない。各組織は独立性をもって活動する[3]。組織の独立性とは、組織はその内部の物事については他の組織による干渉の埒外にあり、その組織のポリシーに則り単独で決定することのできる権利を有しているということである。つまり、この場合、各組織はワークフローの担当部分については独立して定義できるよう配慮されねばならない。例えば、ある組織が担当部分の業務について、その一部分をこの連携関係に加わっていない他の組織に委託するかどうか、言い換えれば、組織の業務を遂行する権利を他の組織に委譲するかどうかという判断は、その組織に委ねられている。現行のワークフローシステムではこのような業務の委託が起こる場合、その委託先の組織を新たにシステムに登録しなければならない。

また、作業の担当者が不在となる場合には、その代理人が作業を行うということがある。現行のシステムでは、ユーザーが指定のフォームに入力することで代理人と代理作業の期間を指定できるといった方式をとっており、この場合にユーザーが選択できる代理人はそのシステムに登録されている人物に限られる。しかし、単一組織内でのワークフローと違い、このような状況では組織内の誰もがシステムに登録されているとは限らない。

そこで本研究では単一ワークフローシステム上で複数組織が連携する場合において、組織間の業務委託や、担当者不在時の代理作業などの際に必要となる権限の委譲をSPKI証明書により柔軟に行えるシステムを提案し、実装を行った。

2. SPKI

SPKI (Simple Public Key Infrastructure) は公開鍵インフラストラクチャの一つであり、現在はIETF (Internet Engineering Task Force) のSPKI作業部会によって標準化活動が行われている[4][5]。

公開鍵インフラストラクチャとして最も認知されているのはX.509ベースのPKIであり、これは公開鍵証明書としてX.509証明書を用いる。X.509証明書は本人情報（所属組

織、識別名、名前等）と公開鍵との対応を保証するID証明書である。

SPKIにおいて用いられるSPKI証明書は、公開鍵と、その公開鍵に対応した秘密鍵を所有するエンティティの属性、もしくは権限との対応を保証する権限証明書である。SPKIにおいて証明書は <I, S, D, A, V> の5-TupleをS式を用いて記述し、署名される。各項目は

- I (Issuer)：証明書の発行者の公開鍵もしくは公開鍵の安全なハッシュ
- S (Subject)：権限を与えられる主体であり、一般に公開鍵、又は公開鍵の安全なハッシュ
- D (Delegation)：権限委譲の可否を表すブール値
- A (Authorization)：証明書の発行者が主体に対して保証する権限
- V (Validity)：この証明書が有効である時間枠

を示す。また、権限の委譲が行われる際には、権限を有する主体が証明書の発行者となり、被委譲者の権限を保証することが必要である。このためSPKIでは固定のCAを設けず、エンティティ間で比較的容易に権限証明書の発行が可能となっている。権限委譲が繰り返されることで、権限を保証するために必要な証明書の数は増えて行く。その証明書の連なりを証明書チェインと呼ぶ。そして、チェインに属する証明書に以下の規則を繰り返し適用することによって最終的な権限が抽出される。

$$<I_1, S_1, D_1, A_1, V_1> + <I_2, S_2, D_2, A_2, V_2>$$
$$= <I_1, S_2, D_2, AIntersect(A_1, A_2), VIntercect(V_1, V_2)>$$

ただし、$S_1 = I_2$, $D_1 = TRUE$ であり

$AIntersect(A_1, A_2)$ ： A_1 と A_2 の表す権限の共通部分

$VIntercect(V_1, V_2)$ ： V_1 と V_2 の表す時間枠の共通部分

とする。

この処理を縮約と呼ぶ。

3. 提案方式

我々の提案するシステムでは、作業担当者の指定や、業務の委託、代理人の指定などは全てユーザー間のSPKI証明書のやり取りで行う。SPKI証明書の発行には、その証明書を発行される主体の公開鍵が必要となるが、発行者はあらかじめ主体の公開鍵を安全な方法で取得しているものとする。

本章では、このシステム上でのワークフロー定義と業務遂行の手順を述べる。

ワークフロー定義

まずはじめに、ワークフローを定義するため、各組織のプロセス定義担当者が集まり、それぞれに割り当てられる部分プロセスを相互接続する部分のみをシステム上で定義する。この時、各組織の担当者はワークフローサーバ（ワークフローシステムというサービスをユーザーに提供するエンティティ）から、このワークフロー定義において、組織内のワークフロープロセスを定義する権限を保証した証明書を発行される（図1：①）。その後、各担当者はそれぞれ独立して自分が所属する組織内のワークフロープロセスを定義する。このようにトップダウンでワークフローを定義することで、各組織の独立性を尊重しながら、矛盾無くフローの経路を設定できる。同様な提言は文献**[1]**, **[2]**においてもなされている。ただし、文献**[1]**, **[2]**では異なる種類の分散したワークフローシステムの連携を想定しているが、本方式は単一のワークフローシステム上での複数組織の連携を想定している。

プロセス定義の際には、定義担当者がワークフロー上の各作業を行う権限の名前を随意に決定し、それを用いて経路を設定する。これはワークフローサーバが提供するプロセス定義ツールを使用して行う（サーバへのアクセスの際には証明書の提示が必要）。また、作業を行う担当者は、その権限を記した証明書を発行することで任命する（図1：②）。この

時、サーバから定義担当者へ発行された証明書も一緒に作業担当者へ渡す。

プロセス定義の際、業務の一部を他の組織に委託する場合は、その部分のプロセスを定義する権限を保証した証明書を委託先の組織へ発行する（図１：③）。

また、業務が組織内の部署に分散するような場合には、証明書を発行することで担当部署にフローの定義を任せることも可能である（図１：④, ⑤）。

これらの一連の作業はワークフローを定義するごとに行う。

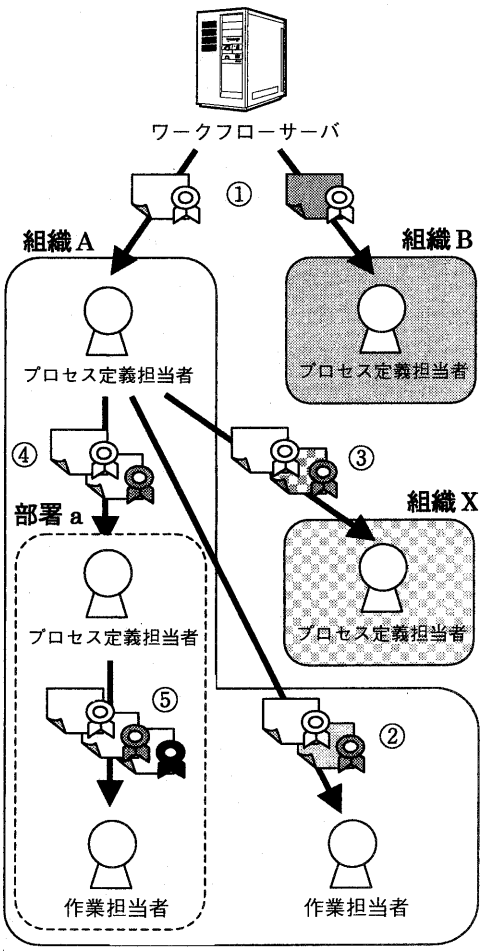

図１　権限証明書の発行

業務の遂行

作業の担当者が業務を遂行するには、まずサーバに対し、プロセスの定義者から渡された全ての証明書を提示する。サーバは提示された証明書を検証し、そこに記載されている権限に対応した作業を行うために必要なリソースへのアクセスを許可する。

以下に具体的な例を上げて説明する。作業担当者Pが組織Aの部署a　に所属しており、ワークフロー定義 W における見積書の作成を担当している場合、P の持つ証明書は Cert1、Cert2、Cert3 である（表１）。P は作業を行う際、まず、この３つの証明書をサーバに提示する。この時サーバはPとの間で、チャレンジ＆レスポンスを行い、K_P に対応する秘密鍵の所有者であることを確認する。次に、サーバはまず自分の公開鍵で Cert1 を検証し、そして、Cert1 に記載されている組織Aのプロセス定義者の公開鍵 K_A で Cert2 を検証し、最後に Cert3 に記載されている部署aのプロセス定義者の公開鍵 K_a で Cert3 を検証する。３つの証明書全てが有効であれば、サーバは縮約により

<K_S, K_P, TRUE, 見積書の作成, V>

を得る。ただし、V は３つの証明書に記載されている時間枠の共通部分であり、また、ワークフロー定義 W に関する権限について以下のことが言えるとする。部署 a のプロセスを定義する権限は見積書の作成権限を、組織Aのプロセスを定義する権限は部署 a のプロセスを定義する権限をそれぞれ包含している。

この縮約の結果から作業担当者Pは「ワークフロー定義 W における見積書を作成する権限」に基づいて、システム上で業務を遂行する。

代理作業

作業の担当者が出張などで不在となる場合は、あらかじめ代理人に業務を遂行する権限を証明書を用いて委譲しておき、作業を代行してもらう。前述の作業担当者Pが代行者D

表1　権限証明書の各フィールドの内容

証明書	Issuer	Subject	Delegation	Authorization
Cert1	サーバの公開鍵 K_S	組織Aのプロセス定義担当者の公開鍵 K_A	TRUE	Wにおける組織Aのプロセス定義
Cert2	K_A	部署aのプロセス定義担当者の公開鍵 K_a	TRUE	Wにおける部署aのプロセス定義
Cert3	K_a	作業担当者Pの公開鍵 K_P	TRUE	Wにおける見積書の作成
Cert4	K_P	作業の代行者Dの公開鍵 K_D	N.A	Wにおける見積書の作成

Validity フィールドには業務の内容に応じた適切な有効期限が記載されているとする

に権限を委譲するならば、証明書の各フィールドは表1の Cert4 のようになる。ただし、Delegation フィールドについては、D がさらに代理作業を依頼することを許可する場合には TRUE が、そうでない場合には FALSE が記載される。

代理人 D が代行作業を行う際は、サーバに Cert1～Cert4 の4つの証明書を提示する。また、この時、代理人 D はワークフローサーバにユーザーとして登録されている必要はない。

証明書の失効

代行作業を依頼した代理人への権限委譲を取り消したい場合は、失効させたい証明書を記載した CRL(証明書破棄リスト)を作成し、サーバに登録する。サーバはワークフローの定義ごとに CRL を管理する。

ワークアイテムへの署名

サーバは、ユーザーが割り当てられた業務を完了し、次の担当者へ受け渡す際に、処理した仕事（ワークアイテム）への署名を要求する。実際には、ユーザーが次の担当者へ受け渡そうとしているデータのハッシュを計算し、その値にタイムスタンプを付加したものにユーザーの秘密鍵で署名させる。

そして、ワークアイテムのハッシュとタイムスタンプ、及び署名データを保管する。これは、ユーザーがその仕事を処理したことの証拠を残し、責任の所在を明確にするためである。

4. 実装

提案方式で述べたワークフローシステムの実装には、JDK1.2.2、Tomcat3.1、Apache1.3、ワークフローのデータを格納するデータベースに Microsoft Access2000、及び暗号ライブラリ Cryptix3.1.1 を用いた。ワークフローサーバは Web 上での利用を想定し、Servlet と JSP により構築した。ユーザーは Web ブラウザによりワークフローサーバにアクセスするが、システムへのログイン時、及び作業の完了時に秘密鍵へのアクセスが必要となるため、電子署名付きアプレットを用いることでローカル資源へのアクセスを可能とした。この他に、SPKI 証明書の発行及び管理と CRL の作成を行うツール、ワークフローのプロセス定義を行うツールを作成した。

5. 考察

組織のプライバシに関する考察

単一のワークフローシステム上で複数の組織が連携する様な状況では、各組織の内部構造や業務の委託関係などといったプライベートな情報の保護が重要となる。しかし、現行のワークフローシステムではあらかじめ作業人員、及び組織の構造情報（役職やその人物の名前など）をシステムに登録しておき、ワークフローの経路設定などの際にそれを利用している。そのため、例えば、企業体統合の中の一組織Oがそこに所属しない組織Xに業務の一部を委託する場合、X は提携関係のな

いワークフローシステムを管理する組織に、登録のためにプライベートな情報を提示しなければならない。そして、組織OにとってXとの関係は、本来他の組織に知らせる必要のない情報である。

本稿にて提案した方式は、そのような情報をシステムには登録せず、プロセス定義の際には経路上に権限名を配置し、それに対応する担当者はユーザー間での証明書の発行により任命するので、組織のプライバシを保護することができる。

現在、一般的に使用されている証明書はX.509 証明書であり、これは ID 証明書であるが、属性証明書を併用することで権限管理に用いることができる。しかし、X.509 証明書には権限管理に必要とする以上の様々な情報が記載されている。そのため、一つの証明書には組織に関する機密情報が記載されていなくとも、ある組織に関する証明書の集合が例えば組織構造のような情報を露呈してしまうこともありうる。

そのような懸念を考慮した結果、担当者と権限の対応を保証する証明書には SPKI 証明書を用いることとした。

提案システムの適用業務に関する考察

提案システムでは、ワークフロー経路の変更を行う場合、新たな作業担当者を経路に加える際には、証明書を発行しなければならない。そのため、プロセスの操作の過程で手続き規則が修正され，新たに生み出されるアドホックワークフローへの適用には不向きであると考えられる。

提案システムの現状での問題点に関する考察

提案システムではサーバ側にユーザの個人情報を登録しないため、ユーザーが不正な行為を行った場合、その人物を特定するにはログインの際に使用した証明書チェインを辿り、鍵と人物の対応を順に追って行かなくてはならないため、対応の遅れが懸念される。

また、提案システムではワークフロー定義ごとに証明書を発行しなくてはならなため、同時に進行するワークフローが増えるほど、扱う証明書の数が増え、ユーザーの負担が大きくなる。

これらの問題は今後の研究課題である。

6. まとめ

ワークフローの作業担当者の指定や、業務の委託、代理人の指定などをユーザー間のSPKI 証明書のやり取りで行うことで、柔軟な権限委譲機能を備え、組織のプライバシ問題に配慮したワークフローシステムを提案し、実装を行った。今後は考察で上げた問題点を解決する方法の検討を行っていきたい。

参考文献

[1] 森田昌宏，向垣内岳弥，山下武史，速水治夫： インターワークフロー支援：組織間連携ワークフロープロセスの構築と分散型運用管理の支援機構，情報処理学会論文誌、Vol.38，No.11，pp.2298-2308，1997

[2] 速水治夫，勝間田仁，世古将洋，提箸公代，渋谷亮一，石丸知之， 大南正人，岡田謙一：商用ワークフロー管理システムと連動するインターワークフロー支援システム，情報処理学会論文誌、Vol.41， No.10，pp.2708-2717，2000

[3] Veijalainen, J.： Issues in Open EDI, Proc. Systems Integration'92, pp.401-412, 1992.

[4] Carl Ellison： RFC 2692, SPKI Requirements, 1999.

[5] Carl Ellison et al： RFC 2693, SPKI Certificate Theory, 1999.