マルチメディア通信と分散処理　85－22
（１９９７．　１１．　６）

モバイルエージェントによる電子発注と電子決済の統合モデルの提案

山崎重一郎*、　須賀祐治*、　荒木啓二郎*,**
tonton@k-isit.or.jp,　suga@k-isit.or.jp,　araki@c.csce.kyushu-u.ac.jp
*（財）九州システム情報技術研究所 (ISIT), ** 九州大学

概要

本稿ではインターネット上に分散しているサービスを統合的に利用するためのモデルを提案する。本モデルの検討のために、電子発注サービス群と電子決済サービス群の動的な統合を題材としてとりあげた。この題材では特に次の２点が重要である。(1) 異なる企業の認証システムで、互いに他のサービスの顧客が同一人物であることを判断できなければならない。このために、利用ポリシー（有効な利用方法）が異なるデジタル証明書の交換を可能なデジタル認証の管理方法が必要になる。(2) 顧客から見ると発注と決済は一連の処理と見るのが自然である。この顧客の観点の実現のために、注文書の内容などの顧客が持っているコンテクストをネットワーク上の複数のサーバーにまたがって維持する手段が必要となる。

我々は、異なる利用ポリシーを持つデジタル証明書の交換を可能にするために、認証局の権威機能を認証、発行、利用ポリシー適用の3つに分割する "3権威分立モデル (S3Aモデル)"を提案した。また、ネットワーク上の複数のサーバーを利用している顧客のコンテクストを持ち運ぶために、モバイルエージェント技術を利用した "セキュアな移動するトランザクションのレイヤー(SMTL)"を提案した。

A System Integration Model for Electric Purchase Systems and Electric Payments Systems with A Mobile Agent

Shigeichiro Yamasaki*,　Yuji Suga*,　Keijiro Araki* *
tonton@k-isit.or.jp,　suga@k-isit.or.jp,　araki@c.csce.kyushu-u.ac.jp

* Institute of Systems & Information Technologies/Kyushu (ISIT), * * Kyushu University

abstract

In this paper, we propose a model to integrate distributed services over the internet. To examine our model, we picked up a case that integrates electric purchase systems and electric payment systems as an application of our model. In this case, crucial problems are as follows; (1) To integrate these distributed services, the authentication system of the each service must have an ability to judge the equality of individual users of the various kinds of services. To realize this, our model should have some method to exchange digital certificates that have different use policies. (2) From the point of the view of a customer, a purchase and a payment is one transaction. To realize this, our model should have some method to keep a customer's context of distributed processes among servers of shops and servers of banks.

As the method to exchange digital certificates of different use policies, we propose "Separation of Tree Authority Model (S3A model)" which divides the authority of "Certificate Authority (CA)" to authentication of an individual, issue certificate and application of use policy.

As the method to keep a context of a customer who use distributed services, we propose a "Secure Mobile Transaction Layer (SMTL)" that utilize mobile agent technology.

1. はじめに

近年、安全な電子商取引などを目的として認証局サービスなどが出現し、X.509 デジタル証明書 [1] による公開鍵暗号を使ったデジタル認証 [2] がネットワークインフラの一つとして整備されてようとしている。このようなデジタル認証インフラが整備されると、ネットワーク上の世界に現実と

の確実に結び付きを持った様々な個人や法人が登場することになり、ネットワーク上で安全に社会的な活動や経済的な活動が行えるようになる。

しかし、デジタル認証をベースにしたシステムの構成方法や運用方法にはまだ不明な部分が多い。その一つがネットワーク上に分散したサービスの統合的な利用方法である。例えば、大手のクレジットカード会社が提供する一つのデジタル認証インフラの配下でそのサービス群を連携させることはたやすいが、そのクレジットカード会社の支配領域の外のサービス群との統合的な連携は難しい。

本稿では、このような問題を解決するためにネットワーク上に分散しているサービス群を統合するためのモデルを提案する。モデルの検討と検証のために、電子発注サービス群と電子決済サービス群を統合することを題材に選んだ。もちろん、電子発注サービスを行っている小売店と電子決済を行っている金融機関は異なるデジタル認証のドメインにあることが前提である。

デジタル認証のドメインが異なる電子発注サービスと電子決済サービスの処理を統合しようとすると次の2点が問題となる。

(1) 注文と決済の処理を安全に連携させるには、顧客、小売店、金融機関の3者がそれぞれ相互認証できなければならない。そしてそのためには小売業から見た顧客と金融機関から見た顧客が同一人物であることを判断できる必要がある。

これを実現するにはデジタル認証の利用ポリシーを越えた交換手段が必要となる。現在のデジタル認証インフラでは、利用ポリシーの定義機関が階層構造の頂点になっているので、このようなデジタル証明書の交換は極めて難しく、新しいデジタル証明書の管理方法が必要となる。

(2) 顧客から見ると発注と決済は一連の処理と見るのが自然である。これを実現するには、注文書のような電子発注サーバーでの顧客の処理結果のコンテクストを、ネットワーク上の別の場所にある決済サーバーまで維持する手段が必要となる。

我々は、(1) の異なる利用ポリシーを持つデジタル証明書の交換を可能にするために、認証局の機能を認証、発行、ポリシー付与の3つの権威に分割する「認証局の3権威分立モデル (Separation of Three Authority model)" 略称 "S3Aモデル" を提案する。このモデルに基づくデジタル証明書は利用ポリシーの情報が分離されているので、デジタル証明書の本来の機能である本人確認の機能だけを代表しており、利用ポリシーに依存しない認証が可能である。

また、(2) の顧客が持っているコンテクストを複数のサーバーにまたがって保持する方法として、モバイルエージェント技術を利用した "セキュアな移動するトランザクションのレイヤ (Secure Mobile Transaction Layer)" 略称 "SMTL" を提案し、これによって電子注文と電子決済サービスの統合が可能になることを示す。

本稿の構成は、まず、「2.デジタル証明書の利用ポリシーの問題」で、デジタル証明書の利用ポリシーの説明とその問題について述べる。「3.デジタル証明書の管理モデル」で、現在行われているデジタル証明書の管理方法と我々が提案するS3A モデルによるデジタル証明書の管理方法について述べる。「4.顧客のコンテクスト維持の問題」で、WWWを用いたセッションで顧客の注文内容などのコンテクストを管理する方法と問題点について述べる。「5.モバイルエージェントを利用した統合モデル」で、提案したS3A モデルとモバイルエージェントを使ったSMTL によって、顧客、小売店、銀行の3者相互認証と顧客のコンテクストの維持が可能であることを示す。「6.おわりに」で、今後の実証実験の計画などについて述べる。

2. デジタル証明書の利用ポリシーの問題

まず「利用ポリシー」という用語について説明する。

銀行で、運転免許証を認証の根拠にして個人の口座を開設することはできる。しかし、運転免許証による本人確認だけではその口座のお金を引き出すことはできない。銀行口座に対する操作のためにはその銀行が発行した自分のキャッシュカードや通帳が必要である。このような本人認証と利用者確認の違いはレンタルビデオショップの顧客カードの作成と利用でも同様である。

デジタル証明書の本来の機能は、自分が本人であることを証明することである。しかし、デジタル証明書を実際に電子商取引などに利用するためには、それにキャッシュカードとしての意味付けやレンタルビデオショップの顧客としての意味付けなどが必要になってくる。このようなデジタル証明書に対する意味付けや有効な用途のことを「利用ポリシー」と呼ぶ。

デジタル証明書の利用ポリシーはその利用機関から与えられていなければならない。したがって、その運用管理方法によってはちょうどレンタルビデオショップのカードと銀行のキャッシュカードには相互に融通性がないように、個人が全く利用ポリシーの異なるデジタル証明書を複数枚持ち、利用の場面ごとに切り替えて使用する必要がでてくる。これは、一人のユーザーが複数の異業種のサービスを統合的に利用しようとすると問題

になってくる。その典型例が、電子商取引における注文と決済の連携である。

3. デジタル証明書の管理モデル

3.1 S2Aモデル

デジタル証明書は、認証局から認証された個人や法人に対して発行される。

しかし、現在のデジタル証明書の発行はこの認証局の機能を、認証登録機関(Registration Authority (RA)) と証明書発行機関(Certificate Authority (CA)) の二つの権威に分割されたモデルで実現されている。RAは、実際に個人や法人の認証とポリシーの適用を行う機関である。CA は、デジタル証明書の発行という技術的な処理を行う機関であり、鍵管理などのセキュリティ技術や施設や装置などの安全性を保証する機関である。CA は認証局そのものを指す用語でもあるので、注意が必要である。

このモデルの典型例は、SET [3] のようなシステムが採用しているモデルであり、VISAなどのクレジットカード会社がRAとなり、VeriSign のような認証サービス会社がCAとなるものである。このように認証局の権威機能を2つに分割するモデルを"2権威分立モデル(Separation of Two Authorities Model)" 略称 "S2Aモデル" と呼ぶことにする

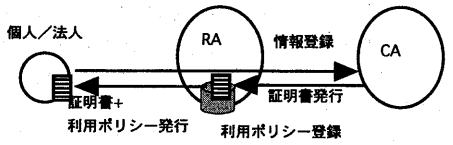

図1. S2Aモデルによるデジタル証明書の発行

このモデルの問題点は、利用ポリシーが異なるごとに異なるデジタル証明書を発行せざるを得ないということである。このために、一人のユーザーは利用ポリシーの違うRAから発行された複数枚のデジタル証明書を持つ必要がある。

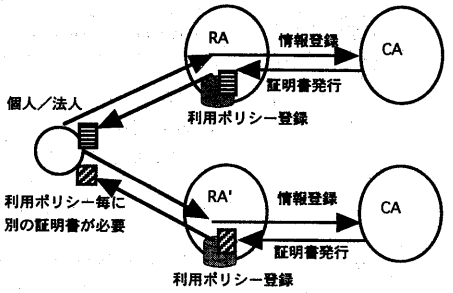

図2.S2A モデルでの複数の利用ポリシーの登録

3.2 S3A モデル

複数の利用ポリシーを持つ個人の同一性を判断できないというS2Aモデルの問題を解決するために、我々は認証局の機能の中からさらに利用ポリシーの登録部分を分離し各利用機関に分散化させるモデルを考えた。

我々のモデルでは、認証登録機関(RA)、証明書発行機関(CA) に加えて、利用ポリシー適用機関(Policy Application Authority (PAA)) の3つに分ける。このモデルを"認証局の3権威分立モデル(Separation of Three Authorities Model)" 略称 "S3Aモデル" と呼ぶことにする。

S3Aモデルが想定している典型的な運営方法は、RA や CA を地方自治体のような中立的な機関やその代行機関が運営するものであろう。PAA は銀行や小売店や旅行会社など、実際に顧客との契約を持つ機関である。

S3AモデルのRA や CA はクレジットカード会社など既存のS2A モデルのものをそのまま利用することも可能であり、その場合1枚のデジタル証明書の利用範囲が拡大するという効果を持つ。

S2AモデルとS3A モデルの最大の違いは、利用ポリシーの管理方法である。S2Aモデルでは利用ポリシーはデジタル証明書の中に埋め込まれる。[4] これに対して、S3Aモデルでは、発行済みの自分のデジタル証明書をPAAに持ち込んでその利用ポリシーを登録してもらう。

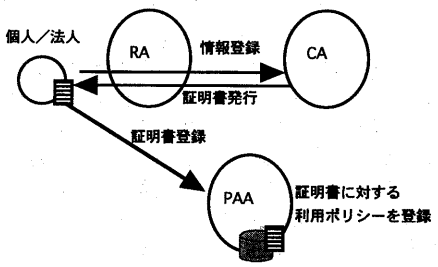

図3. S3Aモデルによるデジタル証明書の発行

利用ポリシーの情報は各PAA のデーターベースに登録されるだけで、デジタル証明書自体には埋め込まれない。自分のデジタル証明書の持ち込みは、SSL などのデジタル証明書の中の公開鍵暗号を使った相互認証のプロトコルを利用すればオンラインでも安全に行うことができる。

S3Aモデルでは、ユーザーは1枚のデジタル証明書に複数の利用ポリシーを登録できるので、複数枚のデジタル証明書を持つ必要がない。その結果、S3Aモデルでの個人のデジタル証明書は、その個人の本人確認という本来の意味だけを担うこ

とになる。これをサービス側から見ると、サービスの相手が、商品の注文者と料金の決済者のような複数のサービスのドメインでの立場を越えて一貫性を持った同一人物であることを判断する仕組みとして利用できる。

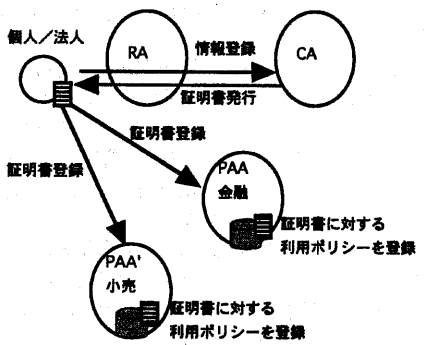

図4. S3A モデルでの複数の利用ポリシーの登録

4. 顧客のコンテクスト維持の問題

商品の発注とその決済は、顧客から見ると一連の処理と見るのが自然である。したがって顧客の視点にあったシステムを作るには、分散環境を統合するトランザクションを実現する必要がある。このためには、まず分散した環境において顧客からの観点でのコンテクストを維持する手段が必要になる。

4.1 同一webサーバーでのコンテクストの維持

まず、一つのサーバーとの処理でコンテクストを維持する既存の手段について概観する。http は、セッションの概念が無いために、ユーザーとサーバーの間のコンテクストを持てないということは良く知られている。しかし、この問題を解決する方法はすでにいろいろ提案されており、オンラインショッピングのショッピングバスケットの実現などでよく利用されている。[5]

hidden form を使う方法は、WWWのクライアントにコンテクストを持たせる方法である。

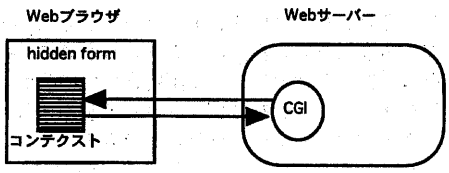

図5. Hidden form を使ったコンテクストの維持

Hidden form を使う方法では、コンテクストの情報は全てクライアントにあるので、サーバーはコンテクストを意識しない。

また、クライアント側でcookie というセッションの識別子の番号を使う方法もしばしば使われている。現実世界でのcookie とは、手荷物預かり所などで渡される番号札のことである。WWW での cookie を使う場合、コンテクストはサーバー側で管理され、クライアントは、自分がコミュニケートしているセッションの識別子となるcookie を毎回サーバーに提示することによってコンテクストを保持しているサーバープロセスを指定することができる。

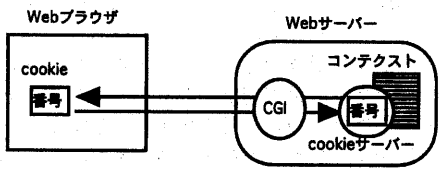

図5. cookie を使ったコンテクストの維持

4.2 複数サーバー間でのコンテクストの維持

次に、複数のサーバーにまたがる処理でのコンテクストの維持方法について実用に即した条件に基づいて考察する。

我々の題材は、電子発注と電子決済なので、ここではサーバー群として小売店サーバーと銀行サーバーを例にとり条件を定める。コンテクストとしては、小売店サーバーと顧客の間で合意された注文書を例にとる。そしてそれまでのトランザクションを継続する形で銀行サーバーに移動して決済処理を行いたい。

まず、Hidden form を使うコンテクスト維持方法を複数サーバーに対して適用する方法について考える。これは図6.に示すように、Webブラウザを介して注文サーバーから決済サーバーにコンテクストが伝播する。

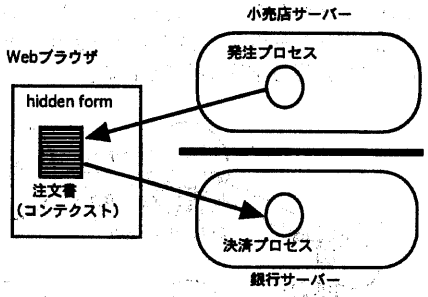

図6. Hidden form を使ったサーバー間のコンテクストの維

この方法は、サーバーのプロセスはコンテクストに関与しておらず、コンテクストの情報は全てクライアント側にあるので、別のサーバーにコン

テクストを渡すのは簡単である。

この方式の問題点は、決済サーバー側で小売店のサーバーが作ったコンテクストを受理しなければならないということである。標準的な注文書の形式やプロトコルの普及が必要となるが、汎用的なものを作るのは困難であろう。もう一つの問題は、3者の相互認証が完全でないことである。小売店サーバーは、顧客を通じて間接的にしか銀行サーバーを認証できない。したがって、小売店の決済に対するリスクが増加する。

次にcookieを利用するケースについて考察する。図7.に示すように、cookieを使う方法ではコンテクストはサーバー側で管理されるので、発注と決済の連携は小売店サーバーのプロセスが決済サーバーのプロセスをリモートプロシージャコールを使って利用することで実現できる。

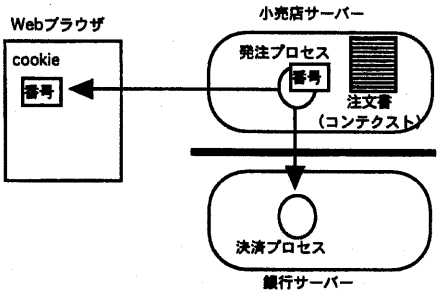

図7. cookieを使ったサーバー間のコンテクストの維持

この方式は、顧客がページの遷移などを意識することなくシームレスに発注と決済が行えるという利点がある。

しかし、このケースでも3者の相互認証が完全でない。顧客と銀行の間の認証は小売店を介した間接的なものになるので、顧客は、自分の口座からの振り込み指示を小売店に委託することになる。これは暗証番号やパスワードなどを小売店に教えることを意味するので現実的でない。

5. モバイルエージェントを利用した統合モデル

我々は、より実用的な分散環境での統合モデルを構築するために、モバイルエージェントを使ったコンテクスト維持方法を提案する。

5.1 モバイルエージェントとは

モバイルエージェントとは、ネットワークを介して移動可能なプロセスのことである。モバイルエージェントを実現している代表的な処理系としてTelescript [6] をあげることができる。kafuka [7] のようにJAVA VMを使ったモバイルエージェントの実装も複数例存在している。モバイルエージェントは、プログラムや実行の環境を別のコンピュータに送り込んで実行させるので、リモートプロシージャコールと対比してリモートプログラミングと呼ばれることもある。[8]

モバイルエージェントは、あるサーバーで実行されていた処理の続きを他のサーバーに移動して継続させることができるので、分散環境でコンテクストを保持する手段として自然である。モバイルエージェントは、実際に移動すること自体よりもむしろこのような分散環境における移動可能なトランザクションを定義するための通信レイヤとみなすことも可能である。我々は、このモバイルエージェントというモデルを用いて、利用ポリシーという複数のドメインに分割されているネットワーク上のサービスを統合するモデルを提案する。これをSecure Mobile Transaction Layer (SMTL) と呼ぶ。

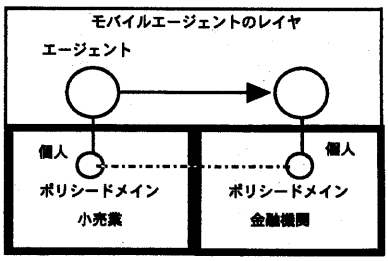

図8. SMTL

5.2 SMTL

注文に先だって、まず顧客と小売店の相互認証が行われる。図9.に示すように、小売店はS3Aモデルに基づき、顧客のデジタル証明書の利用ポリシーを自分のデーターベースで検査し、その小売店の登録顧客であることを確認する。

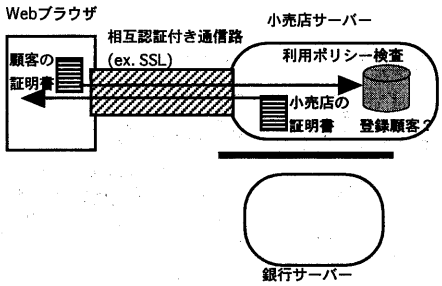

図9. 顧客と小売店の相互認証

小売店サーバーでのコンテクストの管理は、基本的にcookie方式で行なわれる。cookieサーバープロセスはモバイルエージェントとなるプロセスである。小売店と顧客のトランザクションが進行

し注文書が完成すると、コンテクストを持ったモバイルエージェントプロセスが銀行サーバーに移動しようとする。この移動の前に、図10.に示すように、S3Aモデルで小売店サーバーと銀行サーバーの相互認証が行われる。

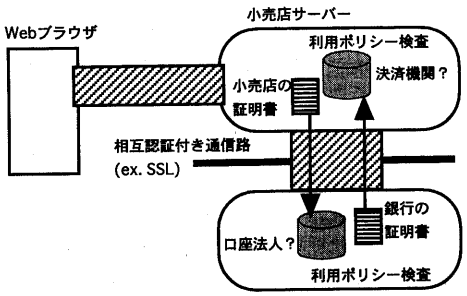

図10. 小売店と銀行の相互認証

この認証においても相互のデジタル証明書の利用ポリシーが検査され、小売店から見て相手が自分が認めている決済機関であることを、また銀行から見て相手が自行に口座を持っている法人であることなどを確認する。

このような相互認証によって確保された安全な通信路を使ってモバイルエージェントが移動する。モバイルエージェントは、潜在的には危険な存在だが、このような完全な相互認証を前提にすると安全に取り扱うことができる。エージェントはcookie などのコンテクストを保持した状態で移動する。

エージェントはcookie や認証情報を持って移動するので、移動した結果、顧客と銀行のサーバーの間にセッションを確保することができる。

図12.に示すように、顧客はこのセッションを通じて銀行サーバーと相互認証を行うことができる。

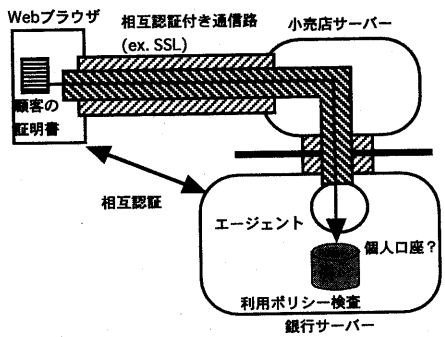

図12.　顧客と銀行の相互認証

顧客はこの相互認証のときも図9.の相互認証と同じデジタル証明書を用いているが、銀行側で検証している利用ポリシーは、その個人がその銀行に口座を持っているかということに切り替わっていることに注意されたい。

以上によって、3者の完全な相互認証が完成する。銀行に送り込まれたモバイルエージェントは、注文書のデーター形式などは知っているので、エージェントからのデーター取り出しプロトコルを標準化しておけば、銀行サーバー側が個々の小売店の注文形式の詳細などを意識する必要がなくなる。このように、モバイルエージェントを利用して、分散環境を統合するためのモデルが構築できることが示された。

6. おわりに

我々は福岡オンライン認証実験プロジェクト[9]の一環として、本稿で述べたS3Aモデルの実用性の評価を目的とした実証実験を計画している。また、本稿で述べたSMTL のプロトタイプを使った分散環境の統合についても実証実験を行う予定である。

参考文献

[1] ITU Rec. X.509 (1993) | ISO/IEC 9594-8: , including Draft Amendment 1: Certificate Extensions (Version 3 certificate).1995

[2] B. Kaliski: RFC1424 IETF Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services: 1993

[3] VISA Card, Master Card: SET Secure Electronic Transaction Specification :http://www.mastercard.com/set/(1997)

[4] R. Housley,et al: Internet Draft Internet Public Key Infrastructure PartI: X.509 Certificate and CRL Profile: 1997

[5] Shishir Gundavaram: CGI programming on the WWW: O'Reilly & Associates, 1995

[6] General Magic (山崎重一郎, 津田宏編訳) : Telescript 言語入門, ASCII 出版局 ISBN4-7561-1656-6 (1996)

[7] 西ヶ谷:Javaにおけるマルチエージェントライブラリの設計: http://www.fujitsu.co.jp/hypertext/free/kafka/jp/paper/,1997

[8] White, J .: Telescript Technology - Mobile Agents: General Magic White Paper #4 (1995)

[9] 山崎重一郎他:福岡オンライン認証実験WG :http://www.k-isit.or.jp/dccf/,1997