マルチメディア通信と分散処理 86－8
グループウェア 26－8
（1998. 1. 29）

認証、証明書発行、利用ポリシー適用の "3権威分立モデル"に基づくデジタル認証システムについて

山崎重一郎*、須賀祐治*、村上美幸**、荒木啓二郎*,**

*(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、1つのデジタル証明書に複数の利用ポリシーを定義可能にすることを目的としたデジタル認証システムのモデルを提案し、このモデルに基づいて試作したシステムについて報告する。現在の一般的な認証システムでは、デジタル証明書の利用ポリシーは認証局が定義しており、異なる利用ポリシーを持つサービスを利用するには別のデジタル証明書が必要となる。本稿で提案する認証モデルでは、認証局の機能を「認証」「証明書発行」「証明書の利用ポリシー定義」の3つに分離することにより、証明書の利用ポリシーを証明書から分離して運用することを可能にした。これにより1つのデジタル証明書に複数の利用ポリシーを定義することが可能になった。我々はこのモデルを認証システムの3権威分立モデルと呼んでいる。試作したシステムでは、本モデルの特性を活かして1つの証明書による複数の認証ドメイン間の連携やデジタル証明書の廃棄後の再発行におけるサービスの一貫性の維持などが実現できた。

A Digital Certification System Model that Enables to Assign Multiple Use Policy to a Digital Certificate

Shigeichiro YAMASAKI*,Yuji SUGA*,Miyuki MURAKAMI** ,Keijiro ARAKI**

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

abstract

We propose a practical design model for digital certification system that enables to assign multiple use policy to one digital certificate.

In an ordinary digital certificate system, a user must get another digital certificate when the user wants to use another secure service that requires another use policy for the client's certificate, because a use policies of a digital certificate are supplied by the issuer of the certificate and its information is embedded into the digital certificate data itself. The special feature of our model is to separate the function of a certification authority into registration authority, certificate issuer and use policy assignment authority of a certificate. We call our model "Separation of three authorities of certificate."

In our certification system, the function of a digital certificate is restricted to the certification of a person itself. Subjects of policy assignment of a certificate are individual component of our system. This method makes it possible to assign multiple use policies to one certificate of a person.

1. はじめに

インターネットの社会への浸透とともに、セキュリティの確保やプライバシー保護などのためにデジタル認証の必要性が高まっている。本稿では、デジタル認証システムを構築し運用するためのモデルを提案し、それに基づいて試作したプロトタイプシステムについて報告する。

公開鍵暗号に基づくデジタル認証の必要性は広く認識されるようになってきた。SSLやS/MIMEなどX.509 デジタル証明書[1]を利用できるアプリケーションも増えてきた。しかし、デジタル認証をどのように実現し運用すればよいのかという点に関しては不明なところが多い。そのような問題の一つがデジタル証明書の利用ポリシーの管理の問題である。これまで、デジタル認証は主に暗号化電子メールや電子商取引のような単一のドメインでの利用を前提に検討されてきたため、複数の利用ドメインにまたがる利用ポリシーを持つデジタル証明書の発行や管理方法はこれまでまだ十分に検討されているとは言えない。しかし、近年、インターネットの用途は医療、教育、行政サービスなど多くの領域に関わるようになり、このような多様なドメインが関連するプライバシー保護やセキュリティの問題は重要になってきている。

本稿では、このような複数のアプリケーションドメインにまたがるデジタル認証の利用を可能にする方法に関して議論する。

2. デジタル証明書の利用ポリシー

デジタル証明書の本来の機能は本人確認である。デジタル証明書の中の公開鍵と認証局のデジタル署名によって、ネットワーク越しに自分が本人であることを証明する手段を与えることが、デジタル証明書の第1義的な機能である。

しかし、実際にデジタル証明書を使ってネットワーク上のサービスを利用するには、その証明書にそのサービスに対する有効な利用方法や権限が定義されている必要がある。このような有効な利用方法や権限をサービス側から定義したものを「証明書の利用ポリシー」という。

例えば、デジタル認証機能を持った銀行のサーバーは、クライアントが提示してきたデジタル証明書がある口座のキャッシュカードとしての利用権限がそのサービスに定義されているときに限り、証明書を提示してきたクライアントがその口座に対する残高照会、引き出し、振り込みなどの操作を行えるようにするであろう。また、デジタル認証機能を使ったインターネットを利用した企業内決裁システムでは、クライアントが提示したデジタル証明書にその社の部長という権限が定義されているときに限り、そのクライアントに部長決裁という操作を許すであろう。

このように、デジタル認証を利用した実際の応用システムでは、単に証明書を提示するだけではほとんど何も行えない。サーバーを管理する組織や団体から、そのデジタル証明書の利用ポリシーが定義されていなければ、その本人にのみ許された固有の処理が行えないからである。そして、本人だけに限定された処理が不要ならば、わざわざデジタル認証システムを使う必要はないので、デジタル証明書の利用ポリシーの管理方法は、デジタル認証システムにとって本質的に重要な要素になっている。

3. 現在の利用ポリシーの定義方法と問題点

現在の一般的な認証システムでは、証明書の利用ポリシーは証明書の発行元である認証局が定義しているのが普通である。例えば、クレジットカード会社がデジタル証明書の発行元であれば、発行された証明書は、その会社のクレジットカードとしての利用ポリシーが与えられることになる。そして、そのような利用ポリシーに関する情報はデジタル証明書のフォーマット自体の中に埋め込まれてしまうこともある。また、PEM[2]などで規定しているように、デジタル証明書の発行元の認証局の階層構造や相互認証関係に基づいて利用ポリシーが定義されることもある。

このため利用ポリシーの異なるサービスを利用するためには、改めてそのサービス専用の証明書を入手することが必要となる。また、利用ポリシーが異なるサービスを利用したければ、サービスに応じて証明書を切り替えて使用しなければならない。

複数のデジタル証明書を切り替えて利用するという方法には操作が煩雑であるという問題と共に、一般ユーザーが多くの秘密情報を管理しなければならないという問題も持っている。また、もう一つの大きな問題は、デジタル証明書の利用範囲が一つのドメインの内部に限定されてしまい、その外部との連携ができないということである。医療システムと決済システムの連携など、同一人物がドメインを越えてサービスを受けようとすると、この問題が現れてくる。デジタル証明書がそれぞれのサービスで別のものを使った場合、異なる組織や団体が運営するサーバーの間で、その二つの証明書が同一人物のものであることを確認する手段がない。しかし両者のサーバー間で連携的な処理を行おうとするときには、同一人物であることを確認する手段がどうしても必要である。

このようなドメイン間での連携処理を実現する一つの方法は、1つのデジタル証明書に複数の利用ポリシーを定義することである。そうすれば、複数のサーバー間で同一人物の判断は簡単にできる。また、利用者にとっても使いやすく秘密の管理もシンプルになる。

4. デジタル認証システムのモデル

問題を整理するために、デジタル認証システムのモデル化を行い、問題を解決するためのモデルを提

案する。

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。認証局とは、個人や法人が確かに実在し、固有の権限を持っていることを認定する権威機能である。我々は、認証局をこの権威機能の持ち方によってモデル化し分類する。

4.1 認証局の権威集中モデル

認証局の実現方法として最も基本になるのが、認証局が本人確認や証明書の発行などのデジタル証明書の発行や管理などについて全て責任を持つモデルである。我々は、このような方式を「認証局の権威集中モデル」と呼ぶことにする。

認証局の権威集中モデルは、PEMの認証局階層などで考えれてきたモデルである。このモデルでは、デジタル証明書の利用ポリシーは、PCAと呼ばれる認証局によって定義され、これが実際の証明書発行元となる下位の認証局に継承されることによって規定される。異なる認証局から発行されたデジタル証明書の相互運用は、認証局の階層構造に基づくポリシーの継承とデジタル証明書自体に埋め込まれている認証検証経路情報などによって定義される。したがって、このモデルでは基本的に利用ポリシーの異なるデジタル証明書の相互運用は定義されていない。もちろんこのモデルを元にPCAを越える証明書の相互運用を行う方法も考えられるが、実現手段は非常に複雑になるであろう。また中継する認証局を欺く攻撃への対処方法など現実的な運用方法についても不明な点が多い。

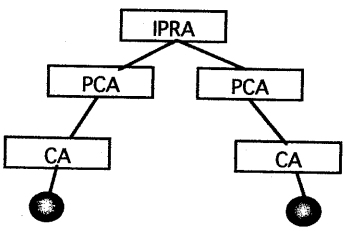


図1. PEMの認証局階層モデル

4.2 認証局の2権威分立モデル

現在、実際に商用目的などで利用されているデジタル証明書の発行は、認証局の機能を、認証登録機関(Registration Authority (RA)) と証明書発行機関(Certificattion Authority (CA)) の二つの権威機能に分割されたモデルで実現されているものがほとんどである。

RA とは、実際に窓口などで個人や法人の認証を行う機関であり、本人を認証し証明書を交付するという権威機能を担う。また証明書発行機関としての（狭義の）CA は、デジタル証明書の発行を実際に行う機関であり、鍵管理などのセキュリティ技術や施設や装置などの技術的な安全性を保証する機能を担う。多数の個人に実際にデジタル証明書を発行するには、窓口が地理的にいたるところにある必要があり、また実際の本人確認業務などの事務処理を遂行する能力も必要である。一方、デジタル証明書の発行には、システムセキュリティーやネットワークセキュリティなどを確保する知識や経験が要求されるので、このような分業体制は合理的である。このモデルの典型例は、クレジットカード会社がRAとなり、認証サービス会社がCAとなるものである。

我々は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)" と呼ぶことにする。

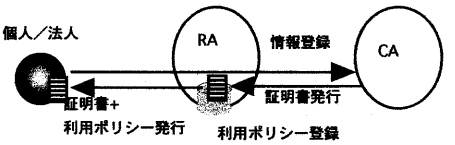


図2. 2権威分立モデルによるデジタル証明書の発行

このモデルで発行されたデジタル証明書は、認証を行ったRAが証明書に関する全ての責任主体になるために、RAが証明書の中に利用ポリシーを埋め込む。CA間の階層構造や相互認証はほとんど意味を持たないので、このようなCAは自己署名になっているものがほとんどである。

このモデルを前提にしたシステムでは、利用ポリシーの異なるサービスには、そのサービスに利用ポリシーに対応する別のRA によって発行された別の証明書が必要となる。

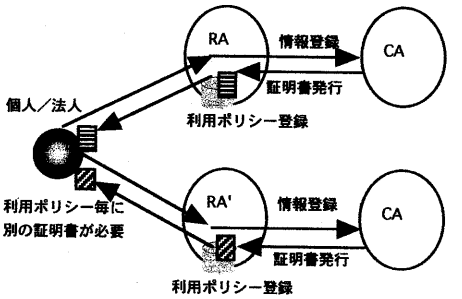


図3.2 権威分立モデルでの複数の利用ポリシーの登録

また、このモデルでは、公開鍵そのものは変わらない場合でも、役職、住所、勤務先など利用ポリシーに関わる情報の変更のためにデジタル証明書を再発行する必要性が生じる。

4.3 認証局の3権威分立モデル

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、認証局の権威機能を認証登録機関(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)"と呼ぶことにする。

3権威分立モデルでは、RAとCAは純粋に認証だけを行い、利用ポリシーには関わらない。具体的に言うと、このモデルにおけるデジタル証明書には利用ポリシーは与えられず、純粋に認証の機能のみを担う。利用ポリシーに関する権威機能は、全てPAAが受け持ち、PAAが登録やその後の管理を引き受ける。

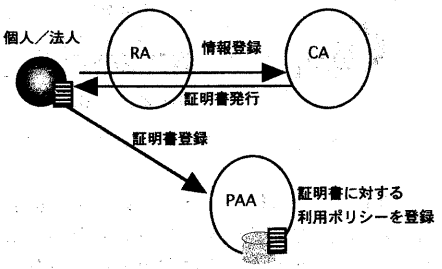


図4. 3権威分立モデルによるデジタル証明書の発行

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。

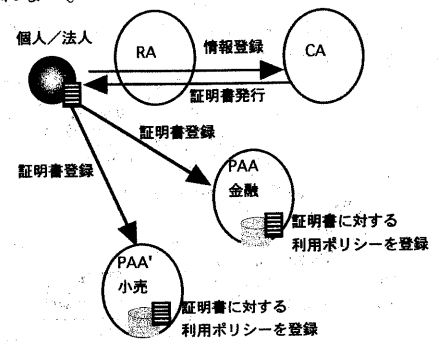


図5. 3権威分立モデルでの複数の利用ポリシーの登録

3権威分立モデルでは、デジタル証明書の利用ポリシーはPAAで分散されて管理されるために、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。したがって異なる利用ポリシーのサービスを利用する場合でも複数枚のデジタル証明書を持つ必要がない。

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。また、3権威分立モデルのRAやCAは既存の2権威分立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。

5. 試作したデジタル認証システム

我々は3権威分立モデルに基づいて認証システムを試作し、複数のサービスを統合的に利用できることを確認した。ディレクトリーサービスと連携してデジタル証明書やCRLを管理していること、DNを使ってデジタル証明書の再発行を行うことによって一貫性を保証していること、デジタル証明書の利用ポリシーをカードのメタファーを使って視覚化しているなどの特徴を備えている。

5.1 RAとCAによる証明書発行

試作したまず、RAとCAの部分について説明する。我々のシステムでは、認証の窓口はRAである。ここでは、RAとCAが1対1の例で説明するが、一般的にはRAとCAは多対1の関係になる。

(1) 個人がRAに証明書を申請する。(2)RAの管理者はその個人が本人であることを対面と文書で認証する。(3)秘密鍵を公開鍵を生成する。公開鍵と登録情報からPKCS#10形式のリクエストファイルを作成し、CAに改ざん不能な通信路で送る。(4)CAは認証局の秘密鍵を使って署名し、X.509形式のデジタル証明書を作成する。(5)デジタル証明書をRAに送り返すとともに、CAと連携したディレクトリーサーバーに証明書を登録し、公開する。(6)RAでは、秘密鍵と完成したデジタル証明書、および認証局のデジタル証明書やディレクトリーサーバーのデジタル証明書をPKCS#12形式にまとめてフロッピーに入れて本人に手渡しで交付する。

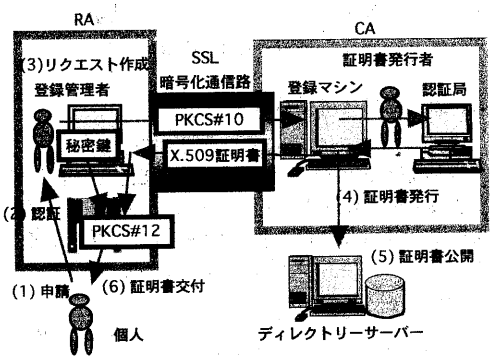


図6. RAとCAによる証明書発行処理

この証明書発行の過程で、秘密鍵やパスワードな

どは一切通信路を流れないので、暗号化通信路の目的は改ざんや再送の防止とRAの認証である。

5.2 PAAによる利用ポリシーの登録

証明書を得た個人や法人は、次にPAAつまり、サービスに関する権威機構にたいして自分の証明書に一定の権限を与えるよう申請する。

我々の証明書管理はディレクトリーサービスを前提にしており、個人や法人の名前は、ディレクトリーサービスに使われるDN(Distinguished Name)を使っている。PAAへの登録もこのDNに基づいて行われる。

例えば、自分のデジタル証明書に銀行のキャッシュカードとしての利用ポリシーを与えたい場合、銀行PAAに行き、自分の証明書のDNと自分の口座の対応を登録してもらう。また、小売店に自分のデジタル証明書をメンバーズカードとして登録したければ小売店に行き、やはりそのDNと配達先などの情報の登録を行う。学生証としての登録や病院の診察券としての登録なども同様である。

このようにして、1枚のデジタル証明書のDNに対して複数の利用ポリシーが登録されることがわかる。

5.3 他の認証ドメインとの連携

次に、複数の認証ドメインでの連携が可能であることを示す。例としては、小売店と銀行の決済の連携を使う。

クレジットカードに基づいた電子商取引の決済は、店舗、顧客、金融機関の全てが共通のクレジットカード会社が管理する同一ドメインで行われているが、我々の例は、小売店と金融機関の間には仲立ちをするような機関はなく、独立した関係である。

(1)ユーザーは、ショップに対して自分のデジタル証明書をメンバーズカードとして登録しておき、登録顧客としてショップのサービスを受け、注文書を作成する。(2)注文書の情報をクッキーなどの形でコンテクストとして維持した状態で、決済機関のサーバーにアクセスする。ユーザーはこれに先だって、自分のデジタル証明書をキャッシュカードとして登録しておく。このため、このサービスに入るとき、ユーザーのデジタル証明書はその金融機関のキャッシュカードとしての利用ポリシーが与えれる。ユーザーはこの利用ポリシーを使い、注文書に基づいて振り込み指示を行う。(3)ユーザーはショップに戻り、振り込み指示を行った旨通知する。(4)今度は、ショップが金融機関にアクセスして振り込みを確認する。このとき、ショップは自分のデジタル証明書をその金融機関の通帳として使う。以上により、完全な3者の相互認証の元に注文と決済の連携が行われたことが確認できた。

この方式の特徴は、通信路をクレジットカード番号やパスワードなどの危険な情報が一切流れないことである。PAAへの登録のときに、そのような危険な情報はオフラインで伝えてあり、実際の認証のときにはデジタル証明書を提示するだけでサーバー側が本人確認できるからである。このように、本方式が安全で軽量な決済システムに応用できることが示すことができた。

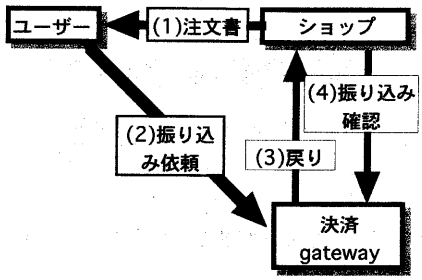
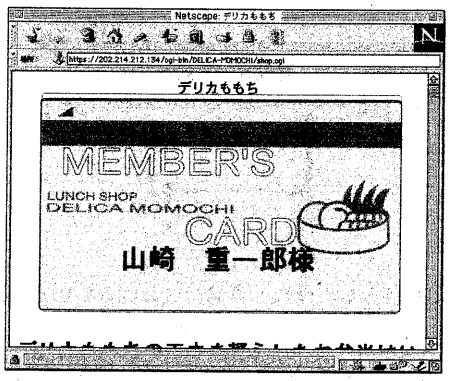


図4. 注文と決済の連携処理の例

5.4 利用ポリシーのカードメタファによる表示

我々の方式では、1枚のデジタル証明書が状況に応じて様々な利用ポリシーが与えられる。これをユーザーにわかりやすく表示するために、カードのメタファを使った。

例えば、銀行サーバーに入るときには、自分のデジタル証明書がキャッシュカードになっているというようなことを表示する。



5.5 ディレクトリーサービスとの連携

我々のCAは、ldapによるディレクトリーサービスと連携させている。証明書の配布やCRLの配布をディレクトリーサービスを使って公開している。

サービスを行っているサーバーも常にディレクトリーの情報を参照しているので、証明書の廃棄など

の情報を即時に得ることができる。

5.6 デジタル証明書の廃棄

証明書の廃棄は、RAによって行う。CAは証明書の廃棄処理を行うとCRLを作成してディレクトリーサーバーを使って公開する。

各サービスのサーバーは、クライアントが提示してきた証明書がCRLに含まれている場合、アクセスを拒絶する。このとき、カードメタファーでは、次のように割れたカードを表示する。

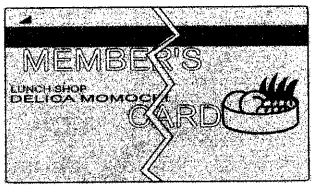


図9　廃棄状態の証明書を意味するカードメタファ

5.7 デジタル証明書の再発行

廃棄されたデジタル証明書の再発行は、発行と同様にRAで実施される。

再発行のときに使われるDNは最初に発行されたときのものと同じものを使う。これは、PAAでの利用ポリシーの登録がDNを基本にしているからである。このため、デジタル証明書が再発行されると、直ちに、その証明書は、廃棄された証明書が持っていた利用ポリシーを全て回復することができる。これも、デジタル証明書とその利用ポリシーを分離して管理する我々の方式の利点の一つである。

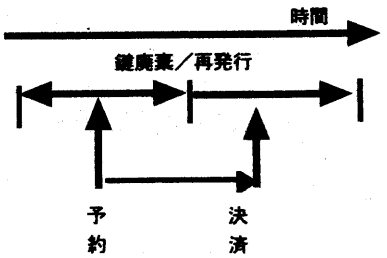


図10 証明書の廃棄と再発行における処理の一貫性

これによって、証明書の廃棄と再発行における処理の一貫性が保持できる。例えば、予約と決済の間に、証明書が事故で廃棄されてしまったような場合でも、新しい証明書の再発行によって利用ポリシーは完全に回復される。予約システムは、廃棄から再発行の期間は受け付けを拒絶するが、新しい証明書が発行されると、DNの一貫性によって連続的に処理を行うことができる。

5.8 地域型の認証システム

3権威分立モデルによる認証は、純粋に本人の実在だけを証明するものである。インターネットの世界における戸籍のようなものと言ってよいだろう。このような認証を行う主体も商用サービスというよりは、地方自治体のような中立な機関が適しているであろう。このような意味で、我々は地域型の認証システムと呼んでいる。

地域型認証システムの特性として重要なのは、公平さである。商用の認証サービスは、有料であるだけでなく、認証の中に与信も含まれているので、子供や低所得者などは認証の対象から外れてしまうであろう。しかし、子供に対しても医療や教育のサービスにおいてプライバシー保護などは必要になってくる。そのような意味で、中立的な認証機関は今後不可欠のものになってくるであろう。このような特性を持つために電子商取引などよりは、教育、医療、行政サービスやその連携に適していると考えられる。

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[7]の一環として、3権威分立モデルに基づいたデジタル認証システムを提案し、試作を行った。まだ、利用ポリシーの定義方法やプライバシーの保護の方法など課題は多い。今後は、試作だけでなく、より実用に即した実験を行いながら、現実に運用可能なデジタル認証のモデルを構築したい。

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] 山崎重一郎他: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 :情報処理学会DPS研究会,Nov, 1997

[7] 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