信用情報と利用ポリシーの管理が可能な相互認証を実現する認証基盤の提案

山崎 重一郎† 荒木 啓二郎††

デジタル証明書を信用するには，デジタル署名の検証だけでは不十分であり，それに定義されている信用情報や利用ポリシーの検証が不可欠である．本稿では，この観点から相互認証の問題を考え，デジタル証明書に対する与信や利用ポリシーの定義主体や範囲が異なるサービス群に対しても統合的に利用できる認証基盤のモデルを提案し，そ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．我々が提案する認証基盤のモデルは，従来の認証局の機能を「証明書発行」「与信」「利用ポリシー定義」の3つに分離し，信用情報や利用ポリシー定義をデジタル証明書から分離して管理することを特徴としている．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．本モデルでは，信用情報や利用ポリシー情報をデジタル証明書の中に埋め込む代わりに「信用できる証明書リポジトリ」というサービスを仮定し，これを介して信用情報を管理することにより認証局や与信機関の領域を越えた相互認証を実現する．試作したシステムにより，1つのデジタル証明書を使って異なる利用ポリシーや信用情報を要求する複数のサービスを利用できることや，与信機関の領域を越えた相互運用性を持つことが確認できた．また運用実験によってこのモデルに基づく認証システムが現実的に運用可能であることが確認できた．

A Certificate Infrastructure Model for Integrated Cross-authentication with Warranty and Use Policy Control

SHIGEICHIRO YAMASAKI† and KEIJIRO ARAKI††

The validity of a digital signature for a digital certificate is insufficient to trust it because verification of warranty and assigned use policy of the digital certificate is indispensable. In this paper, we propose a cross authentication infrastructure that integrates a variety of services that require different use policies and warranties. We describe desiign and implementation of a prototype system for this model. The significant feature of our model is to separate the function of a certificate authority into "issuing authority," "registration authority" and "use policy approval authority". We call this model "the separation of three authority models for digital certification system." We utilize trustable certificate repository for cross authentication. The warranty information is not embedded into a digital certificate in our model. Warranty information of a digital certificate is provided by the certificate repository. Our prototype system can provide an integrated service of servers that requires different use policies and warranties by only one certificate. Our certification system also endure practical use through our experimentation.

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公開鍵暗号に基づくデジタル認証の必要性が広く認識されるようになってきた．特に，認証局（Certification Authority）によって組織的に発行されるX.509[3]デジタル証明書を用いた認証基盤は，SSL（Secure Sockets Layer）[1]やS/MIME[2]などのアプリケーションを中心にして普及しはじめている．

我々は，デジタル認証の基盤は，インターネット上に社会システムや経済システムを構築するうえで不可欠な新しい社会基盤の1つであるという観点から，電子商取引に限定されない統合的な認証基盤の構築を目的として研究を進めている．これまでに，複数の認証ドメインの連携方式[18]や1つのデジタル証明書に複数の利用ポリシーを定義できる認証基盤の提案[19]を行ってきた．

† 財団法人九州システム情報技術研究所
Institute of Systems and Information Technologies/KYUSHU
†† 九州大学大学院システム情報科学研究科
Department of Computer Science and Communication Engineering, Graduate School of Information Science and Electrical Engineering, Kyusyu University

本論文では，これらの研究成果をさらに進めて，デジタル証明書の信用情報や利用ポリシーに関する管理を含めた相互認証が可能な統合的な認証基盤の提案を行う．

現在，実用化されているデジタル認証システムは，主に暗号化電子メールや電子商取引のような単一の利用領域を前提に設計されているものがほとんどである．利用領域を1つに限定すれば認証局とサービスを行う機関が同一になり，デジタル証明書の信用や用途を認証局側で決定できるので運用が単純になるという利点がある．

しかし，このように用途が1つに限定されたデジタル証明書を使用するユーザは，利用するサービスに応じたデジタル証明書を所持し，別のサービスを利用するときには証明書を切り替えて使わなければならないという問題が生ずる．

さらに深刻なのは相互認証の問題である．デジタル証明書の利用ポリシーが1つの用途に限定されてしまうと，ユーザは複数のサービスを連携させて利用することができないという問題が生ずる．

本論文では，従来の認証基盤との互換性を保ちつつ，異なる利用ポリシーや信用情報を要求するサービスを統合的に利用することを可能にする相互認証基盤を提案し，それに基づいて試作したシステムについて報告する．

本論文では，まず2章で我々が提案する認証システムの3権威分立モデルについての説明を行う．この中で，認証局の3つの権威機能を分離する理由とシステムを構成する各要素の説明を行い，このモデルによるデジタル証明書の発行，利用ポリシーの定義方法，信用情報の定義方法について述べる．

3章では，本モデルに基づく相互認証の方法について述べる．ここでは，まず従来の相互認証の方法について簡単に解説し，我々が提案する信頼できる証明書リポジトリを使った相互認証方法と信用情報の管理方法について述べる．

4章では，試作した証明書発行システムと相互認証基盤を利用するアプリケーションシステムの構成について述べる．

最後に5章では，試作したシステムを用いた実験と評価について述べ，本モデルに基づく相互認証による統合的な認証の連携が実現できることと，本モデルに基づく認証基盤が実用的に運用可能であることを示す．

2. 認証システムの3権威分立モデル

まず最初に，我々が提案する認証基盤のモデルの背景と動機を明らかにしたうえで，システム構成と各機能について述べる．

2.1 認証と利用ポリシーの分離

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．

たとえば，ユーザ認証機能を持った銀行のサーバは，ユーザが提示してきたデジタル証明書とその人の口座との対応関係が定義されているときに限り，そのデジタル証明書を使ってその口座の残高照会，引出し，振込みなどの操作を行えるようにする．逆にいえば，利用ポリシーが定義されていなければ，デジタル認証を使用しても実際の応用システムでは何も行うことができない．

しかし，認証と利用ポリシーが一体化されているデジタル証明書は，他の用途には利用できないという問題があるため，大規模な認証基盤では利用ポリシーの管理が問題になる．IETF の PKIX[6] には，X.509 証明書の拡張フィールドにあるポリシーのマッピングやポリシー伝播に対する制約条件などを使って，認証局間でのポリシーを管理する試みがなされている．しかし，これは同一のポリシーの伝播範囲を規定する方法であり，複数の利用ポリシーを統合的に利用する方法ではない．

我々は，このような問題を解決するために，デジタル証明書の中に利用ポリシーを埋め込まずに外付けで管理し，認証システムとは完全に分離されたシステムで管理する方式を考案した．

2.2 認証と与信の分離

我々は「与信」という用語を経済的な信用以外の意味でも使う．たとえば，本人が医師であるというような情報について，国立病院のような権威ある機関がそれが真実であると保証することも「与信」と呼ぶことにする．

我々の研究目的は，社会基盤としての認証システムを提案することである．子供を含めてあらゆる人を公平に認証の対象にできなければならないという観点から，与信と認証は切り離すことが必要であると考えている．また，与信情報にはその人の所属団体の情報なども含むことがあるが，このような情報の寿命は公開

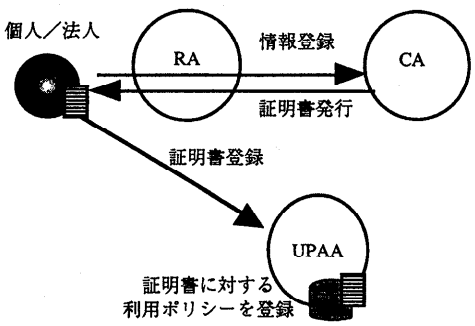


図1 3権威分立モデル
Fig. 1 Separation of Three Authorities Model.

鍵の寿命と比較すると頻繁に変わるという性質を持っている．

医療情報処理学会では，医師の頻繁な異動に対応するために認証システムを認証のレベルと信用情報のレベルの2階層で管理し，デジタル証明書の中の公開鍵は変更せずに信用情報のみを頻繁に変更する方法を提案している[22]．我々は，デジタル証明書の中には与信情報を埋め込まず，外付けで管理するという方針をとった．

2.3 3権威分立モデルの構成

我々のモデルでは，認証局の証明書発行に関する機能を，証明書発行局（CA: Certification Authority），登録機関（RA: Registration Authority），利用ポリシー定義機関（UPAA: Use Policy Approval Authority）の3つに分ける．このモデルを「認証システムの3権威分立モデル（Separation of Three Authorities Model）」と呼ぶことにする．**図1** に本モデルの概念図を示す．

我々のモデルは，IETF の PKIX のモデル[6]との整合性を持っており，既存の X.509 証明書に基づく他の認証基盤との互換性を保っている．

以下，このモデルの各要素について説明する．

2.3.1 CA：証明書発行局

3権威分立モデルでは，CA は純粋にデジタル証明書リクエスト形式（RSA Laboratories 社の PKCS#10 形式[10]を想定）へ自分の秘密鍵を用いてデジタル署名を行いデジタル証明書の発行を行う機能のみを受け持つ．

この CA が担う責任は，主に秘密鍵の管理と技術的なセキュリティの確保に限定される．また，本モデルにおける CA は，証明書リポジトリへの証明書登録の権限を持つ特権的な機関であり，その CA が発行したデジタル証明書を証明書リポジトリを使って公開する権利と責務を持つ．

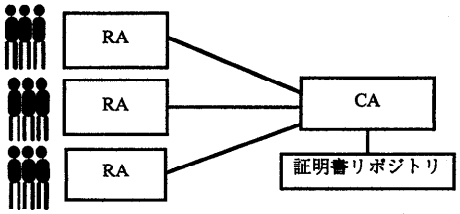


図2 RA と CA の関係
Fig. 2 RA and CA.

一般的に，高いセキュリティシステムを確保するには，高いコストの施設や設備が必要となる．従来の用途ごとに独立した CA では，要求されるセキュリティレベルに応じた CA が運営されているが，3権威分立モデルでは1つの証明書が様々なレベルの証明書として使用されるので，このモデルでの CA は非常に高いレベルの安全性が要求される．しかし，この CA は多くの RA から共有されて利用されるので，コストは分散されることになる．

2.3.2 RA：登録機関

RA は，実際に本人確認を行い，証明書を本人に渡す窓口になる機関である．また，秘密鍵の漏洩など証明書に事故が発生した場合も RA がその通知や対処における窓口になる．

システム的には，**図2** に示すように，1つの CA に対して複数の RA が対応しているというのが典型的な構成形態となるが，RA が CA を選択してもよい．RA は証明書を発行するという機能のみを CA に求めるわけであり，実質的には RA が証明書を発行しているといってよい．したがって，発行された証明書に関する責任は基本的に RA にあることになる．このような意味で，RA は，実は与信機関としても機能することになる．

与信機関としての RA は，発行済みの証明書に対して，信用情報のみを定義することもできる．我々のモデルでは，信用情報は，証明書リポジトリと呼ばれる公共的な情報サービスを通じて安全に登録され公開される．

2.3.3 UPAA：利用ポリシー定義機関

UPAA は，各サービスが運営するサービスであり，ユーザの証明書に対してそのサービスに対する一定の利用権限つまり利用ポリシーを定義するものである．

たとえば，ある銀行がオンラインバンキングサービスを行っていれば，その銀行が UPAA になる．自分のデジタル証明書にそのオンラインバンキングサービスの利用資格を登録したいユーザは，自分のデジタル証明書を持ってその銀行に行き，そのサービスへの利

用ポリシーを登録してもらう．いったん利用ポリシーが登録されれば，そのデジタル証明書は，キャッシュカードとして機能するようになり，オンラインバンキングのサーバにおいて口座の振込みなどの操作が許可される．

信用情報の登録と利用ポリシーの登録は似ているが，区別が必要である．RAで登録される信用情報は，証明書自身が一般的な外部のサービスに対して持つ信頼度を意味するが，UPAAで登録される利用ポリシーは，そのサービスに限定されたサービスの利用権限である．

ポリシーを定義するためにいくつかの専門用語を導入する．

ロール：アプリケーションシステムにおけるユーザの「役割」を表す．たとえば，商店システムには，「顧客」や「店員」のようなロールがある．不特定の人に「顧客」のロールを与えると，事故が起きる可能性が高いので，特定の「与信情報」を持った人だけにロールを与えるというのが，商店システムにおける「ポリシー」になる．ロールは，サービスシステムにおけるユーザの権限を意味し，読み，書きのようなメソッドごとに定義された権限の集合体に付けられた名前である．

与信情報：「信頼できる証明書リポジトリ」を使って公開されるユーザの信用に関する情報である．「カード会社のメンバ」とか「医師」などが与信情報の例である．ロールが個々のサービスに依存して変わるものであるのに対して，与信情報は広域的な属性情報なので「広域的なロール」と呼ぶこともある．

ルール：クライアントのエンティティが特定の与信情報を持つときにどのようなロールが与えられるべきであるかという規則である．UPAAにおけるユーザの利用ポリシーの定義は，このルールで記述される．

2.3.4 証明書リポジトリ

証明書リポジトリは，CAが発行したデジタル証明書を公開する公的なサービスである．X.500ディレクトリーシステム[5]に基づいたサービスを想定している．証明書リポジトリは，相手のデジタル証明書を入手したいときに利用される．

証明書リポジトリは，我々の相互認証方式の中核的な役割を持つことになる．信用情報の公開も証明書リポジトリを介して行われる．このため，各サービスのサーバは，デジタル証明書の信用状態を確認するためにつねに証明書リポジトリの情報を参照することを想定している．

もう1つ重要なのは，証明書リポジトリへの登録を通じてデジタル証明書の名前空間の管理が行われることである．デジタル証明書には，X.500ディレクトリーの標準に従ったDN（Distinguished Name）と呼ばれる構造を持った一意名が付けられる．

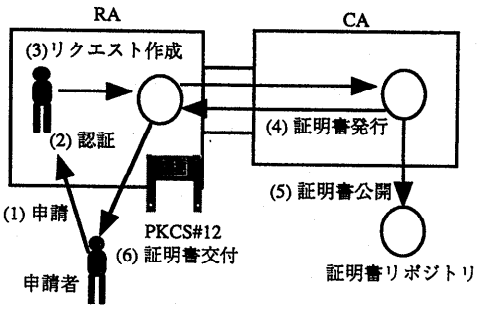


図3 デジタル証明書の発行
Fig. 3 Issuance of a certificate.

2.4 3権威分立モデルによる証明書の発行

本モデルに基づいたデジタル証明書の発行は，次のような手順で行われる．この時の処理の流れを図3に示す．

(1) 申請者がRAに証明書を申請する．
(2) RAの管理者はその申請者が本人であることを対面と文書で認証する．
(3) RAで申請者の秘密鍵と公開鍵を生成する．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，改竄に対して安全な通信路を介してCAに送る．
(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申請者本人に手渡しで交付する．

このモデルによるデジタル証明書発行の特徴は，CAとRAの機能を完全に分離しているところである．また，CAとRAの間には，秘密鍵やパスワードのようなセキュリティに関わる情報はいっさい流さずに処理を行えるという特徴も持っている．これらの特徴により，CAとRAをまったく別の組織によって運営することが可能になっている．

2.5 UPAAによる利用ポリシーの登録

デジタル証明書を得た個人や法人は，利用したいサービスのUPAAに自分のデジタル証明書に一定の

権限を登録してもらう．

UPAAへの登録もDNをキーにして行われる．たとえば，ユーザが自分のデジタル証明書を使って銀行口座から他の口座への振込み操作ができるようにしたい場合，銀行UPAAに行き，ユーザのデジタル証明書のDNと関連づけて口座からの振込み操作が可能な「口座の持ち主」というロールが与えられているという利用ポリシーを登録してもらう．

2.6 RAによる信用情報の登録

RAは与信機関としての機能を持っている．RAによって保証を受けたい個人は，RAの窓口に自分のデジタル証明書を持ち込んで信用情報の登録を依頼する．

RAは，所定の審査を行い，保証の資格があると判断すると，証明書リポジトリに信用情報を登録する．たとえば，医師が国立病院RAに自分が医師であることを保証してしてもらう場合，証明書リポジトリのその医師のエントリーに，「医師であることを国立病院RAが保証する」という保証情報が登録される．

このような信用情報の登録を行うために，証明書リポジトリの各エンティティのエントリーに信用情報を登録するためのフィールドを設けている．このフィールドには，信用情報を複数登録できるようにしている．これにより，1つのデジタル証明書に手形の裏書きのように複数の信用情報を定義したり，デジタル証明書自体を廃棄することなく，その信用情報のみを廃棄するということも可能にしている．

安全性のために証明書リポジトリへの直接的な更新権限を持っているのはCAだけなので，RAは，CAを仲介にして間接的にこの証明書リポジトリに信用情報を登録したり更新したりする権限を持っている．

2.7 信用情報の内容と与信コスト

デジタル証明書の運用や管理にはシステムが想定する安全性のレベルがあり，より高い安全性のレベルを実現するにはよりコストがかかる．1枚のデジタル証明書を複数の用途に利用できるようにするためには，用途ごとのコストとバランスがとれた安全性を設定できる必要がある．

本人確認の意味での「認証」の安全性は，公開鍵の鍵長と，CAの秘密鍵の保護に帰着する．我々のモデルでは，CAは多数のRAから共有される「公共財」として行政機関や中立的な非営利団体などが装備するということを想定しており，施設や設備なども，かなり高度な安全レベルを持つことを仮定している．一方で，信用維持のための審査や与信者への継続的なモニターなどのRAの運営コストは，RAがどのようなレベルの「与信」を行うかによって変わってくる．

「信頼できる証明書リポジトリ」にRAによって定義されて公開される信用情報の中身は，次の3つ組およびその有効期限と現在の有効性の状態である．

- RAのシンボル：RAの一般に知られている名前．トレードマークなどもこれに入る．
- RAの保証情報のURL：RAが「与信」した対象のエンティティが，もし第三者の信用を破る事故を起こした場合にRAが支払うペナルティと，それが成立する条件などRAが担保する信用レベルの情報．
- RAの運営ポリシーのURL：RAが対象者を与信するための条件，審査項目，与信者の事後モニター，与信の取消しを行う場合の条件，情報公開やプライバシー情報の管理の方針などRAの運営方法に関する情報．

URLでリンクされている情報は，RA自身のエントリーに存在する．各サービス側のサーバは，クライアントへの権限を割り当てるときに，「信頼できる証明書リポジトリ」のRAの信用情報を参照して，信用度を判断する．したがって，RAが与信したエンティティに対して保証する信用度は，この信用情報が鍵をにぎることになる．

RAがより高度な与信を行おうとすると，RAの与信に関するコストは高くなるのが一般的である．また逆に，認証にコストをあまりかけたくないRAは「信頼できるリポジトリ」には「低レベル保証」という与信情報を付けざるをえない．なぜなら，もしそのRAが与信したエンティティが事故が起きた場合には，そこで公開している保証条件に基づいてペナルティを支払う義務が生じるからである．このようにして，本モデルでも，信用情報一体型の証明書システムと同様に，認証コストとバランスした与信レベルの設定が可能になる．

2.8 与信情報の有効期限の定義

信用情報が一体化した証明書では，用途ごとに異なる証明書なので個別に有効期限が設定できる．我々の証明書を共通化したモデルでも，用途ごとに有効期限が設定されることを示す．

複数のRAに与信してもらうと「信頼できる証明書リポジトリ」の個人のエントリーには複数の信用情報が定義されることになる．そして，前節で触れたようにそれぞれの信用情報の中にはその有効期限が定義されている．これを参照することによって，1つの証明書に複数の有効期限が定義されたことになる．

表1 第三者機関による相互認証
Table 1 Cross certificate by third sector.

タイプ	実現方法	代表例
リポジトリ型	リポジトリに証明書を登録	XCert, ICAP
中継ハブ型	中継者による証明書の交換	NetDox
プロトコル型	認証機関どうしで通信	Commerce Net, SET

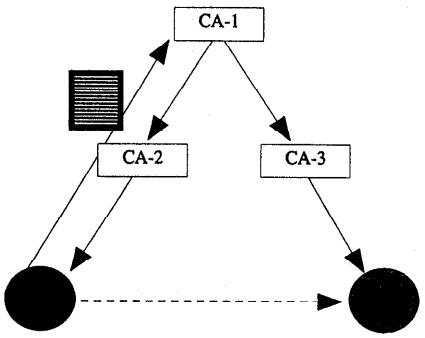


図4 認証局の階層構造による相互認証
Fig. 4 Hierarchical model of cross certificate.

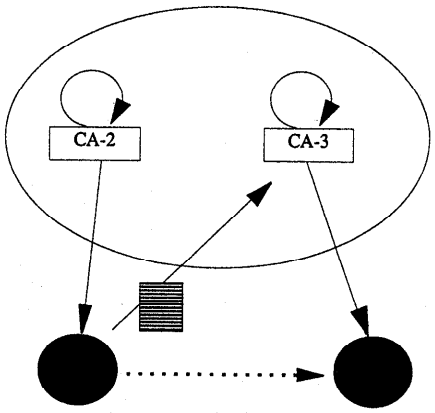


図5 証明書リポジトリによる相互認証
Fig. 5 Repository model of cross certificate.

3. 相互認証

本章では，上述の3権威分立モデルを用いた相互認証について説明する．まず，従来の相互認証モデルについて説明する．

3.1 認証局の階層構造に基づく相互認証

デジタル証明書を発行したCAのデジタル証明書をさらに上位のCAによって署名することによって保証する方法を階層型の認証基盤という．

階層型の認証基盤において，相互に安全にデジタル証明書を入手できる最上位のCAをルートCAと呼ぶ．階層型の認証基盤では，異なるCAから認証を受けている相手のデジタル証明書は，**図4**のように，ルートCAの証明書を元に，連鎖的に署名を検証することによって正当性を確かめることができる．

しかし一方で，1カ所でも認証に関する運用条件に弱いところがあると，そこを含む部分木全体の信頼性が低下するという問題を持っており，認証局全体に対してつねに強い安全性を要求するため，現実的にはあまり普及していない．

3.2 第三者機関に基づく相互認証

署名の検証ではなく，第三者機関によって相互認証を行う方法もいくつか提案されている．その中で，代表的なものは**表1**のように3つのタイプに分けることができる．

この表の中にあるリポジトリ型と中継ハブ型は，いずれも第三者によって相手の認証局の証明書などを入手する手段を得るものなので，実質的には類似した方法であるといえる．

プロトコル型は，認証機関どうしが一定の取り決めをして相互に通信をして認証情報を交換するものである．これはカード会社1の顧客ととカード会社2の店舗が相互運用を行いたい場合に，店舗が顧客から受け取った証明書をカード会社2を経由して第三者機関であるカード会社1に検証依頼をすることによって相互認証を行うものである．

3.3 信頼できる証明書リポジトリによる相互認証

我々の相互認証の方法は，前節のリポジトリ型に分類できるものである．

もし，相手の証明書に署名している認証局の証明書を安全に入手する手段があれば，その証明書を使って直接的に検証できるので，階層的な証明書の管理は不要である．**図5**のように，自分と異なる認証局から認証されているデジタル証明書を検証したいときには，その相手の認証局のデジタル証明書そのものを信頼できる証明書リポジトリから入手すればよいからである．したがって，相互認証の手段をこのモデルにのみに依拠することにすれば，認証局間の階層構造は不要で，各認証局は自分で自分に署名を行う自己署名の証明書だけを持てばよいことになる．

現在のNetscape NavigatorやInernet explorerなどは，Webクライアント自体の中に多数の（階層構造を持たない）認証局の証明書をあらかじめ保持した形で配布されている．現在のこれらWebクライアン

トでは，通信相手の証明書が登録されている認証局リストに入っている認証局から発行されたものであれば信用するという方式で「相互認証」を実現している．このような方式も，我々の観点から見ると「証明書リポジトリによる相互認証」に分類可能である．

3.3.1 証明書リポジトリを信用するための情報

では，どうやって「信頼できる証明書リポジトリ」というものを実現するのかという実現手段が問題になってくる．

我々は「信用できるリポジトリ」はSSL上のLDAPディレクトリーサーバとして実現している．したがって，このディレクトリーサーバ自体のSSL接続のための証明書を安全に配布する手段が必要となる．本モデルでは，RAが各エンティティへ証明書を発行するときに，同時にこのディレクトリーの証明書もエンティティに渡すということによって，確実にディレクトリーサーバの証明書を渡すことができる．

各エンティティは，RAを信用することによって，そのRAから渡されたディレクトリーサーバの証明書を信用し，そのディレクトリーに登録されている認証局の証明書を信用することによって，自分以外のドメインの認証局の証明書を信用する．もし，1つのRAだけでは信用するのに情報が不足であれば，複数のRAからディレクトリーの証明書を受け取ることによって，「信用できるリポジトリ」の信頼度の情報を増やしてゆくことができる．認証局の階層的な署名関係によって「トップダウン」に信頼関係を作る代わりに，このような形で「ボトムアップ」に信頼のための情報を増やしてゆくのが本方式特徴である．

1つの証明書リポジトリの中には，多数の認証局の証明書が格納されるが，それぞれの認証局の証明書の正当性は，リポジトリの信頼度によって決まる．また，このモデルは，地域の証明書リポジトリが，世界中の認証局の証明書をすべて持っているというものではなく，認証基盤を大規模化するためには，多数の証明書リポジトリが相互に連携しあう必要が生じると考えている．しかし，この場合，各エンティティは，自分が直接知っている地域の証明書リポジトリは強く信頼するが，そこから離れていくに従って信頼のための情報が減少するので信頼度も低下してゆくことになると考えられる．

3.3.2 本モデルによる相互認証方式の特徴

証明書リポジトリを利用する相互認証を行っている例として，認証実用化実験協議会（ICAT）が作成したICAP[20]やXcert[14]などがあげられる．

これらのリポジトリ型の相互認証システムでは，証明書リポジトリ自体の信頼性を保証するために，CAを介して証明書リポジトリにアクセスしている．しかし，CAの本来の機能は，デジタル証明書へ署名する機能であり，その秘密鍵は認証基盤の最も重要なセキュリティ要素である．したがって，セキュリティ上の観点から見るとCAへの攻撃の可能性を避けるためにCAはネットワークに接続されるべきでない．

我々の相互認証モデルの特徴は，CAを介さずに直接的に証明書リポジトリ自体をエンドエンティティから見て信頼できるものにした点にある．これはRAがエンドエンティティに証明書を発行するときに，同時に証明書リポジトリのデジタル証明書も安全な手段で渡すという方式によって実現している．また，証明書リポジトリへのアクセスは，LDAP（Lightweight Dirctory Access Protocol）[9]とSSLによる認証付きのセキュアプロトコルを使用している．

以上のような手段で，証明書リポジトリの正当性はCAを利用せずに直接検証されるので，我々のモデルのCAは，ネットワークに直接的には接続はしていない．この特徴により我々のモデルによるCAはより安全であるといえる．

3.3.3 証明書リポジトリのスケーラビリティ

大規模な認証基盤を構築するには，処理能力の面からも運用の面からも証明書リポジトリは集中型システムではなく，スケールアップ可能な分散システムでなければならない．

我々のモデルと同様に証明書リポジトリ機能を持つICAPは，分散リポジトリを統合化するためのhttpに基づくプロトコルを備えており，スケーラブルなシステムになっている．[21]

また，IETFのPKIXのインターネットドラフトでもICAPと同様の分散リポジトリを構築するためのプロトコルが提案されている[7]．

我々のシステムも，LDAPに基づいてスケーラブルな分散リポジトリシステムを構成している．LDAPだけでは偽造されたディレクトリーサービスによる攻撃やデータの改竄を受ける危険性があるので，SSLの上にLDAPをのせることでこの問題を回避している．

3.4 信用情報の相互認証

次に，信用情報に関する相互認証について述べる．

我々が認証局の階層構造による相互認証を採用しないもう1つの理由は，署名の連鎖と違い，与信関係は推移的でないということである．

ここでいう与信関係，つまり，「エンティティaがエンティティbをWという内容で保証する」という関係をW(a,b)と書くとする．この関係が推移的でない

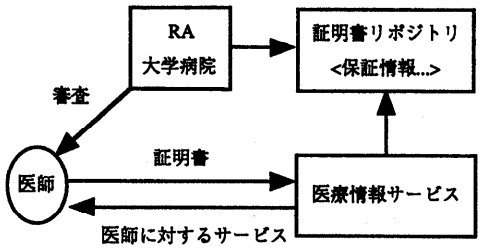


図6 信用に基づくアクセス管理
Fig. 6 Access control by trust.

というのは，W(a,b) と W(b,c) から W(a,c) を導くことができないということである．

たとえば，W が「医師であることを保証する」という関係で，a が国立病院，b と c が医師とすると，国立病院 a には，医師であることを保証する与信機関として信用できるが，普通の医師 b には通常はそのような信用能力はない．このため W(b,c) のような保証情報が登録されていたとしても，通常はそれを信用することはできない．したがって，信用できない情報をもとに，W(a,c) という結果を導くことはできない．

我々のモデルでは，信用情報は，証明書リポジトリの中で各エンティティのエントリーに直接定義されるので，この与信関係の非推移の問題は回避されている．

また，信用情報のもう1つの特性として，信用とは本来的に相対的なものであるということがある．たとえば，どんなに有名な機関が与信していても，その信用情報を評価する側の人がその機関を信用しなければ信頼関係は成立しない．

例として，患者のプライバシー保護のために医師のみにアクセス可能な医療情報交換サービスで，しかも，患者が旅行中に急病になったような場合には，医師であることが証明できれば登録されていなくても利用できるというものを考える．このシステムを**図6** に示す．

このサービスは，事前のユーザ登録でデジタル証明書の利用ポリシーを定義するということができない．したがって，アクセスしてきたユーザの信用情報に使って動的に医師としての利用ポリシーを与えるかどうか判断することになる．

このとき，信用情報の信頼度を判断する拠り所は与信機関である．医師であるという信用情報を，無名の病院 RA が保証している場合と，有名な国立病院 RA が保証している場合では，通常は国立病院の方が信頼度が高いであろう．しかし，たまたまその情報の管理者がその無名の病院をよく知っている場合は，その無名の病院の方が信頼度が高くなり，より高度のアクセス権限が与えられるという可能性もある．このように，

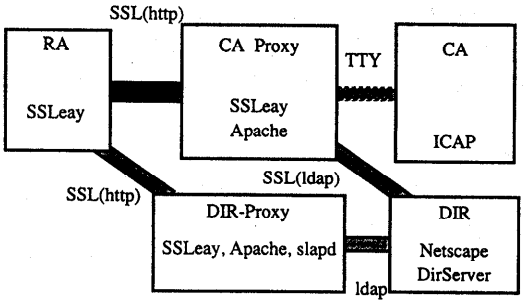


図7 証明書発行システム
Fig. 7 Certificate issue system.

信用情報の信頼度は，認証システム側で設定することは困難であり，最終的な信頼度の判断は各サービス側で行う必要がある．

我々のモデルでは，信用に関する相互認証の基盤は，信頼度そのものを厳密に定義するのではなく，利用する側でそのような判断をするのための情報を得るための信頼できる基盤として構成している．また，我々のモデルでは，1つの証明書のエントリーに複数の信用情報を登録することができるので，信用する側が登録されている信用情報の中で最も適したものを選択することも可能になっている．

4. 試作システム

我々は，認証システムの3権威分立モデルに基づいた証明書発行システムとそれを利用するアプリケーションシステムを試作した．

4.1 証明書発行システム

試作した証明書発行システムは**図7** のようなシステム構成をとっている．

4.1.1 CA

この CA は，証明書の発行という機能だけを受け持つシステムである．

RA からのリクエストがあれば，無差別の証明書を発行してしまうので，人手を介することなく自動運転が可能である．

その反面，セキュリティ技術としては，設備，施設などの面で高度なものを要求している．CA のマシンは，鍵がかかる部屋に設置し，部外者が物理的にアクセスできないように守っている．

CA マシンは秘密鍵をファイルシステムの中に持っているが，これに対するセキュリティ確保のためネットワークに直接つながらないように CA-Proxy を仲介にして接続している．この CA-Proxy 自体も2重のファイアーウォールの中に置いている．CA はネットワークに接続しなくてよいように，CA-Proxy に TTY

による端末としてつながっている．

試作したCAの証明書発行システムの部分は，ICATが作成したICAP[20]の証明書発行機能を使用して実現している．

4.1.2 RA

RAシステムは，多数の実験の協力団体に配布することを想定して設計した．CAは，安全な施設などを要求するので，多数のRAがそのようなCAを共有利用する構成になっている．

RAとCA-Proxyの間は，インターネットを経由して接続されるので，その安全性を確保するために2048ビットのRSA鍵を使用して相互認証付きのSSLを使って通信している．これらの実現にはSSLeayのモジュール群を使用している．また，RAとCA-Proxyは双方ともIPのフィルタリングを行い，相互に特定の相手のパケットしか受け取れないように設定し，偽のRAによる攻撃に対処している．

RAでは，その設置団体のメンバに大量に証明書を発行する機能と，発行済みの証明書に与信を行う機能がある．

証明書発行機能では，各ユーザ用の公開鍵と秘密鍵の対を生成し，PKCS#10形式でCA-Proxyに証明書のリクエストを行い，CAによって署名された証明書を受け取ると，秘密鍵と証明書をPKCS#12形式でパックしパスワードで暗号化することが主な機能である．

また，与信機能では，新たに与信を得たいユーザがネットワーク経由でアクセスしてきたときに，秘密鍵所有検査プロトコルによって，正当な秘密鍵を持つことを確認したユーザにパスワードをSSLを使ったセキュアな通信路で送信する．次に，そのパスワードを持った人が一定の審査に合格した場合，与信情報を「信頼できる証明書リポジトリ」であるディレクトリーサーバにCA-Proxyを経由して登録する．

4.1.3 証明書リポジトリ

証明書リポジトリはSSL上のLDAPによるディレクトリーサーバによって実現している．このディレクトリーサーバへの情報の登録はCA-Proxyのみが権限を持っている．

証明書リポジトリのディレクトリーでは，すべてのエンティティを一意な名前であるX.500に基づくDN（Distinguished Name）管理している．この名前が，システム的にもエンティティの自己同一性の拠り所になっている．証明書の期限切れや廃棄などの後の再発行でも，この名前の同一性によって継続性が維持されている．また，過去のデジタル署名の検証を可能にするために，期限切れの証明書もこのディレクトリーのエントリーの中に，時間軸にそった形で保存されている．

廃棄情報は，通常はCRLで公開するが，我々のシステムではこれに加えて，ディレクトリーのエントリーに現在の証明書の状態を表すデータを含ませ，これによってリアルタイムで廃棄情報をサーバ群に伝えることを可能にしている．

4.2 認証基盤を利用するアプリケーションシステム

本モデルに基づく認証基盤を利用した典型的なアプリケーションステムのプロトタイプを試作した．

このアプリケーションシステムは，クライアントの信用情報に基づいて，サーバの情報へのread権限やwrite権限のようなアクセス権限を変えるものであり，インターネットにおけるプライバシー保護や安全な参加型サービスを目指したものである．

このアプリケーションシステムは，次のような「プレース」と「所有権」モデルによって構成されている．UPAAは，このプレースごとに定義され，ポリシーの定義権限を持っているのは所有者である．

4.2.1 プレース

プレースとは，サービスを提供する場やコンテクストを意味するモデルであり，具体的にはwwwのページである．プレースはそのアプリケーションシステムというシナリオのある世界の舞台にあたるものである．

我々は，UPAAはプレースごとに存在するという設計方針をとっている．したがって，ユーザのロールや権限などは，プレースごとに定義されることになる．

実際のアプリケーションシステムの動作としては，クライアントは，プレースに入るときに一定のロールを要求する．プレースはクライアントの信用情報に基づいてロール割当ての妥当性のチェックが行い，要求したロールが不適切なユーザはプレースへの侵入が拒否される．ロール割当てが許可されたクライアントは，ロールに定義された利用権限でサービスを利用することになる．

4.2.2 所有権

プレースには，所有権の概念があり，プレースの所有者が必ず存在する．UPAAとしてのプレースの定義者は，このプレースの所有者である．所有者のみが，プレースに存在する情報へのパーミッションやそこを訪れるクライアントの利用ポリシーを定義する権限を持つ．所有権の範囲は，プレースに限定され，プレースが他のプレースとハイパーリンクしているような場合でも，リンク先のプレースには独立した所有権があるものとして設計している．

5. 本モデルの妥当性の評価

本章では，で試作したシステムに基づいて，提案したモデルの妥当性の評価を行う．

5.1 モデルの実現性

試作した証明書発行システムとアプリケーションシステムを使って実証実験を行い，モデルの実現性を評価した．

5.1.1 分散RAによる証明書の発行の実現性

まず，CAとRAを分離したモデルの実現性について述べる．

この実証実験では，我々のモデルが，高いセキュリティレベルから，学校の生徒や自社の社員に限定してサービスのみを対象にした低いセキュリティレベルのものまでをを混在させながら，システム全体の安全性を確保できることを検証した．

まず，RAシステムの安全性を確保する手段として，RAの転用による証明書の偽造を防ぐ手段が問題となった．RAシステムには新規登録者のための秘密鍵の生成機能があるので，RAシステムも厳重に管理しなければならないからである．我々は，RAシステムをノートパソコンで運用することを推奨し，証明書の発行に使用するとき以外はネットワークから物理的に切り離したうえで，鍵のかかる金庫やロッカーに保管するという運用方法をとった．

証明書はPKCS#12形式で秘密鍵と証明書が対にして暗号化したデータをフロッピーで配布する方法をとった．この方法は，バッチ的に処理ができるので，大量発行には適していると考えられるからである．

CAと分離されたRAシステムは，福岡オンライン認証実験WGの参加メンバに対してパッケージ化して配布し，実際に10団体でRAが稼働した．一方でCAシステムとCA-Proxyおよび，信頼できる証明書リポジトリは我々が，安全な部屋で管理した．この分散RAを使用して証明書の発行の運用実験を行い，実験期間中に合計70名の証明書を発行した．

現実の運用に近づけるために，審査などに非常に手間のかかる厳重な運用方法をとったにもかかわらず，分散RAシステムの利用により，CAでは，RA用の証明書の発行のための事務手続きとRAシステムのインストールのために3人日の作業工数を要したのみで，その後の証明書発行業務による作業コストはほとんど発生しなかった．また，各RAでも組織内の人間のみの証明書発行のみをすればよいので，円滑に運用を行うことができた．このような窓口の分散による証明書発行方法が，様々なレベルの証明書を大量に安全に発行する実用的な方法の1つであることを確認できた．

我々のモデルは，直接対面認証を基本とするために，非常に高いレベルの認証基盤に適していることは明らかであるが，暗号化電子メールのような用途では，むしろ低いレベルで安いコストで実現できる認証基盤のニーズが高い．学校や企業などには分散型のRAのみを設置し，CA本体の安全性は専門の機関に委託するという我々のモデルは，このような低レベル，低コストの認証基盤にも適していることを以上の実験によって確認することができた．

5.1.2 「信頼できる証明書リポジトリ」の実現性

「信頼できる証明書リポジトリ」は，SSL上のLDAPサーバによるディレクトリーサービスとしてシステムを構築し，実現性の評価を行った．

「信頼できる証明書リポジトリ」の実用的な構成において問題となるのは，スケーラビリティである．我々は地域性に基づいて，「信頼できる証明書リポジトリ」を構成すると，それぞれの地域単位では安全な運用が可能であると考えている．たとえば，これを行政単位とリンクすれば，地方自治体などが「信頼できる証明書リポジトリ」の運営主体になることも考えられる．

「信頼できる証明書リポジトリ」の正当性を検証するには，証明書リポジトリ自体の証明書を正しく入手する必要があるが，これも地域性に基づけば，直接手渡しという手段が可能であり非常に安全で確実は方法で，我々のモデルの認証の最終的な拠り所である「信頼できる証明書リポジトリ」の証明書を配布することができる．

実験では，このような運営方法を想定して，日本のエントリーと福岡のエントリーと東京のエントリーを代表する3つのサーバを稼働させた．

実際に稼働しているRAは，福岡が9団体で，東京が1団体であるが，所在地が福岡のRAから発行された証明書は福岡のサーバに登録され，所在地が東京にあるRAでは東京のサーバに登録される構成とした．発行したユーザのデジタル証明書のDNの名前空間も，この地域主義の考え方で管理した．ディレクトリーサーバ間の連携方法は，LDAPプロトコルの「紹介（refferal）」によって実現している．たとえば，福岡のサーバに東京の証明書の問合せがあった場合には，福岡のサーバは，日本のサーバを「紹介」し，次に日本のサーバが，東京のサーバを「紹介」するという処理を経て東京のサーバにある証明書が返されてくるという形で，スケーラブルな分散リポジトリを実現した．

リポジトリの拡張を行ううえで問題になることは，

名前空間の管理である．我々は地域型という方針で名前空間や証明書リポジトリの管理などを行ったが，地域に限定されなかったり，遠隔地に拠点が分散したりしている団体のRAを地域型で管理するのは不合理な面があり，ディレクトリーサーバの守備範囲の点でも名前空間の管理の点でも拡張が必要であることが分かった．

しかし，地域名に基づく名前空間の管理方法は，所属団体名などを入れずにすむため学校の卒業や退職などの影響を受けないDNを割り当てることが可能なので，証明書の管理には都合が良いことが分かった．

特に，デジタル証明書の廃棄や期限切れ後の再発行のとき，前のデジタル証明書と同じDNを使うことによって，予約や注文などから決済まで長い時間を要する処理の途中でデジタル証明書が無効になった場合でも，再発行の後，処理を継ぎ目なく継続することが可能なシステムを構成できた．

また，同じくDNが永続的であるため，ディレクトリーのエンティティのエントリーに証明書の状態を表すフィールドを持たせて，CRLを検索することなくLDAPプロトコルによって直接的に廃棄状態を問い合わせることも可能となった．この方法によって，アプリケーションシステムのサーバが，デジタル証明書の廃棄を実時間で認識できるシステムを試作し，実用的に利用できることを確認した．

5.1.3 信用情報と利用ポリシーの分離の実現性

本モデルの目的である，信用情報や利用ポリシーの異なるデジタル証明書の連携処理の例を実際に構築する実験を行い，これらの情報の分離の妥当性を評価した．実験システムは，Apacheによるhttpdに SSLeayによってSSLプロトコルを追加したシステムを利用した．またクライアントはNetscape Navigator 4.03を使用した．

このシステムの典型的な動作は次のようになる．

(1) ユーザは事前に，RAにおいて自分のデジタル証明書に「A社の社員」という与信情報を登録してもらう．この情報は「信頼できる証明書リポジトリ」を介して公開される．

(2) ユーザが旅行社サーバにアクセスすると，UPAAとしての旅行社のポリシーすなわち「ルール」に基づいてクライアントへのロール割当ての妥当性を判断する．この場合，ユーザは「顧客」というロールを要求する．

(3) 「ルール」に（[A社の社員]→[顧客]）というルールが定義されていると，この要求は成功し，ユーザに「顧客」ロールが与えられそれに定義されているメソッドが実行可能になる．

(4) ユーザは，「顧客」ロールに定義されているメソッドを利用して出張のためのチケットの注文書を作成する．

(5) 注文書の情報をHTMLのhidden formなどのコンテクストとして維持した状態で，ユーザは支払いを目的として銀行のサーバにアクセスする．

(6) ユーザが銀行サーバにアクセスすると，UPAAとしての銀行のポリシーすなわち「ルール」に基づいてクライアントへのロール割当ての妥当性を判断する．この場合，ユーザは「口座の持ち主」というロールを要求する．

(7) 「ルール」に（[A社の社員]→[口座の持ち主]）というルールが定義されていると，この要求は成功し，ユーザに「口座の持ち主」ロールが与えられ，それに定義されているメソッドが実行可能になる．

(8) ユーザが銀行サーバで「口座の持ち主」というロールが割り当てられると，自分のデジタル証明書をキャッシュカードとしての利用できるようになる．ユーザはこのサービスを使い，コンテクストにある注文書の情報に基づいて振込み指示を行う．

(9) ユーザは旅行社サーバに戻り，振込み指示を行った旨通知する．

このシステムのポイントは，銀行サーバと旅行社サーバのそれぞれが他の2者の証明書に対する利用ポリシーを定義するルールを持っていて，それに応じて1つしか証明書を持たないユーザに対するサービス内容を変えていることである．

以上のような方法により，提案するモデルの特性である，ドメインの異なるサービス群を連携させて統合的利用できるということが実現できた．

5.2 信用や利用ポリシーの分離モデルと従来モデルの安全性の比較

ここでは，3権威分立モデルモデルと従来の信用情報やポリシー情報が一体化した証明書のモデルとの安全性の比較を行う．

5.2.1 証明書が1枚しかないことによる危険性

用途別に異なるデジタル証明書では，1つの証明書が攻撃を受けてもその被害範囲が限定される．これに対して，我々の1つの証明書ですませる方式は，確かに秘密鍵の漏洩や解読のような事態が生じた場合の被害がその個人の生活の全域に及ぶという意味で深刻で，より被害が大きいといえる．

秘密鍵のトラブルのせいでネットワークを使うあらゆる活動が停止してしまうのは問題である．危険分散の観点からは，1人で複数の証明書を持つのは妥当だと考えられる．

我々のモデルでも，証明書は1枚でなければならないということに制限しているわけではない．事実，我々の実装でも実際に個人が複数の証明書を持つことになる．

本モデルで，1人のエンティティが複数の証明書を持てるようにする方法は次のようになる．我々のモデルで「自己同一性」を保証するのは実は証明書ではなく，「信頼できるリポジトリ」の名前空間における名前の一意性である．証明書の再発行などにおいて以前からの信用情報などが継続されるのは，この機構に基づいている．ここには過去の署名の検証を可能にするために，時間軸にそった構造で過去の証明書もすべて保持されている．また，証明書の期限切れの前に次の証明書が発行されたときには，有効な証明書が複数存在することもある．この延長で，もし複数枚の証明書でリスクの分散ができる場合は，1人の個人のエントリーに複数枚の証明書を組み込み，そのそれぞれに信用情報を対応づけるという構成も可能にしている．しかし，この場合それぞれの証明書に定義された信用情報が異なっているので，一体型の証明書と同様に，ユーザはサーバごとに適切に証明書を使い分ける必要がある．

5.2.2 複数の証明書を持つことによる危険性

「自分はクレジットカードを2枚持っているから1枚くらいなくしても大丈夫だ」というようなことはないように，単純に証明書を多数持てば危険が分散されるというわけではない．

1人のユーザが複数の証明書を持つということは，1人で多数の秘密鍵やそれを守るための多数のパスワードなどを管理する必要があるということを意味する．管理すべき秘密情報が多くなるにつれてどれかが漏洩する危険度が増加するが，一体型の証明書を使用するシステムでは用途ごとに異なる証明書を要求するので，いまの生活で我々が所持している様々なカード類の数と同じくらい多数の秘密鍵，パスワードを管理する必要がでてくるとすると，現実的な安全な運用はかなりの困難が予想される．

我々のモデルを使うと，複数の認証ドメインの証明書を一体化することができるので，管理する秘密情報を減らすことができる．したがって，我々のモデルは危険分散を行いながら，最小の数の秘密情報管理にまとめることができるということがいえる．

5.2.3 用途別の有効期限や失効情報の設定

公開鍵の寿命よりも信用情報の有効期間が短い場合，たとえば，医師は2ヵ月ごとに別の病院に異動することがめずらしくないが，本モデルでは，「信頼できる証明書リポジトリ」にある信用情報の有効期限を短く設定しておくだけで，証明書そのものの再発行を行うことなく有効性を停止することができるという利点がある．

さらに用途ごとの廃棄についても，デジタル証明書そのものが有効期限の前に事故などで失効する可能性があるのと同じように，用途ごとの有効性も期限が切れる前に失効する可能性があり，そのような情報を公開する「信頼できる」場が必要となる．我々の「信頼できる証明書リポジトリ」は，このような信用の失効情報の公開の場としても有効である．「信頼できる証明書リポジトリ」の信用情報の失効などの情報の書き込みの権限は，与信機関であるRAのみが可能であり，RAの署名とタイムスタンプ付きで公開される．

我々のモデルは，用途ごとの信用情報の有効性をきめ細かにしかもCRLの交換のような方法と違いRAでの受付と同時にリアルタイムで公開する手段になっている．

6. まとめ

本論文では，信用や利用ポリシーの制御を含む相互認証を実現する統合的な認証基盤のモデルを提案し実証実験の成果を報告した．

実用的な認証基盤を作るには，デジタル署名の検証可能性だけでは不十分であり，デジタル証明書に対する与信や利用ポリシーの管理方法を含めた認証基盤が必要であるという観点から認証基盤のモデルを検討した．

まず，認証と利用ポリシーの分離や認証と与信の分離によって，信用情報や利用ポリシーの管理が単純化され，デジタル証明書の用途を汎用化できることを示し，認証局の機能から認証，利用ポリシーの定義，与信の3つの機能を分割して分散的に管理を行う「認証システムの3権威分立モデル」を提案した．

さらにこの認証基盤モデルと，LDAPディレクトリーサービスを利用した安全な証明書リポジトリを使った相互認証基盤を提案し，その安全な構成方法や拡張可能性についても提案を行った．我々が提案する証明書リポジトリの特徴は，エンドエンティティへのデジタル証明書の発行のときにディレクトリーサーバのデジタル証明書も一緒に安全な手段で渡すことにより，CAを介さずにエンドエンティティに対して直接

的に信用可能な証明書リポジトリを提供することである．この方式によって，CAをネットワークに接続する必要性をなくし，CAの安全性を高めることができた．

また，利用ポリシーの分散管理法やこの認証基盤を使った信用情報に基づく相互認証の方式についても提案した．

実証実験は，認証基盤システムとアプリケーションシステムを試作し，福岡オンライン認証実験WGに参加している企業や団体を対象に証明書発行実験を行った．実験に使用した分散RAシステムは，電子商取引が可能な水準の強く管理された証明書を大量に発行する現実的な手段として利用可能なことが分かった．

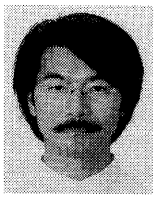
試作システムによるこのモデルの実証実験により，1つのデジタル証明書へ複数の利用ポリシーの定義が可能であることや，異なる利用ドメイン間の連携が実現できることが確認できた．また，試作したシステムは決済システムとしても，安全で実用性の高いシステムであることが分かった．

今後，教育，決済，求人求職，医療などの実用的なプリケーションを題材にした実証実験による実用性の評価を進める．実証実験の中で，この認証基盤のセキュリティ要件やスケーラビリティの検証などを行ってゆく．研究課題としては，プライバシー保護を目的にした信用情報を利用するアクセス制御の方法や相互認証の実現方法などついて取り組んでゆく予定である．

参考文献

1) Freier, A.O.: Netscape Communications, INTERNET-DRAFT: The SSL Protocol Version 3.0 (1996).
2) Dusse, S.: RSA Data Security: RFC2311, IETF, S/MIME Version 2 Message Specification (1998).
3) ISO/IEC 9594-8 – ITU-T X.509, The Directory, Authntication Framework, including Draft Amendment 1, Certificate Extensions, Version 3 certificate (1993).
4) ISO/IEC 9594-6 – ITU-T X.520, The Directory, Selected Attribute Types (1993).
5) ISO/IEC 9594-1 – ITU-T X.500, The Directory, Overview of Concepts, Models, and Services (1993).
6) Housley, R.: Internet Public Key Infrastructure X.509 Certificate and CRL Profile (1998).
7) Reddy, S.: Internet Public Key Infrastructure WEB based Certificate Access Protocol – WebCAP/1.0 (1998).
8) Kaliski, B.: RFC1424, IETF, Privacy Enhancement for Internet Electronic Mail, Part IV, Key Certification and Related Services (1993).
9) Yeong, W., Howes, T. and Kille, S.: RFC1777, IETF, Lightwaight Directory Access Protocol (1995).
10) RSA Laboratories: Public-Key Cryptography Standards, PKCS #10: Certification Request Syntax Standard: ftp://ftp.rsa.com/pub/pkcs/ (1993).
11) RSA Laboratories: Public-Key Cryptography Standards, PKCS #12: Certification Request Syntax Standard: ftp://ftp.rsa.com/pub/pkcs/ (1993).
12) VISA Card, Master Card: *SET Secure Electronic Transaction Specification* (1998).
13) VeriSign: Certification Practice Statement VERSION 1.1, http://www.verisign.co.jp/ (1997).
14) Csinger, A.: White Paper: Cross-Certification, A 50% Solution, http://www.xcert.com/ (1998).
15) 電子商取引実証推進協議会（ECOM）：認証局運用ガイドライン1.0版，http://www.ecom.or.jp/ (1998).
16) 電子商取引実証推進協議会（ECOM）：相互認証ガイドラインアルファ版，http://www.ecom.or.jp/ (1998).
17) Gundavaram, S.: *CGI programming on the WWW*, O'Reilly & Associates (1995).
18) 山崎重一郎，須賀祐治，荒木啓二郎：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，97-DPS-85-22 (1997).
19) 山崎重一郎，須賀祐治，村上美幸，荒木啓二郎：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，情報処理学会DPS研究会，98-DPS-86-8 (1998).
20) 服部浩之，櫻井三子，小林良至，菊池浩明：オンライン証明書発行局パッケージ（ICAP）の実装と評価，SCIS'97-8C (1997).
21) 櫻井三子，服部浩之，小林良至，菊池浩明：証明書発行局間の証明書情報共有機構の設計，SCIS'97-8D (1997).
22) 山本隆一：医療情報のセキュリティ要件の概要と多段階認証システム，SCIS'98-S3 (1998).
23) 山崎重一郎ほか：福岡オンライン認証実験WG，http://www.k-isit.or.jp/dccf/ (1998).

(平成10年 5 月11日受付)
(平成10年11月 9 日採録)



山崎重一郎（正会員）

1957年生．1983年3月東京理科大学理工学部数学科卒業．同年4月富士通（株）入社．1987年4月（株）富士通研究所へ移籍．第5世代コンピュータプロジェクトにおいて並列推論マシンを用いた自然言語解析の研究．次世代文書処理の研究．モバイルエージェントの研究．1996年6月（財）九州システム情報技術研究所へ出向．インターネット上のデジタル認証の研究．

荒木啓二郎（正会員）

1954年生．1976年3月九州大学工学部情報工学科卒業．1978年3月同大学院修士課程修了．同年4月九大学工学部助手．1984年8月同助教授．1993年4月奈良先端技術大学院大学情報科学研究科教授．1996年4月九州大学大学院システム情報科学研究科教授．工学博士．形式的仕様記述，ソフトウェア開発方法論，インターネット，マルチメディア通信等の研究に従事．財団法人九州システム情報技術研究所研究室長兼務，ソフトウェア技術者協会常任幹事，九州地域研究ネットワーク（KARRN）協会事務局長，元博多祇園山笠西流赤手拭等．