マルチ認証局環境におけるユーザ管理方式*

1J－5

黒田康嗣†

(株)富士通研究所‡

1　はじめに

近年，インターネット，イントラネットが注目され，ネットワーク環境が急速に発達している．ユーザは，電子メールやWorld Wide Webなどを使って，ネットワーク上でのコミュニケーションや情報収集を行なっている．また，エレクトロニックコマースが注目され，例えば，VISAとMASTERが共同でクレジットカード決裁プロトコルSET(Secure Electoronic Transaction)[1]を開発し，今年中に本格的な実験を開始する予定になっている．このようなネットワーク環境の発達に伴い，ネットワーク上のセキュリティの問題を解決することが重要な課題となっている．ネットワーク上のセキュリティ上の問題は，盗聴，改ざん，なりすましに代表される．解決策はそれぞれ，盗聴は暗号化，改ざんは電子署名，なりすましは認証である．

従来，認証方式として慣用暗号系を用いた方式が用いられていた．この方式は，サービスの管理者がユーザ一人一人にIDとパスワードを与え，パスワードやチケットを元に認証を行なうものである．これは，UNIXのcrypt(3)やMITのKerberos[2]に代表されるが，ネットワーク環境が拡大するに伴い，一局集中型の認証では対応し切れず，分散された環境でどのように認証するかが問題となってきた．この問題を解決する一方法が公開鍵暗号をベースとする認証局[3]を中心とした認証の枠組である．これは，”信頼のおける第三者である認証局”を信頼点として，認証局を分散し，ユーザが認証局から発行される証明書を持つことにより，広域な環境での認証を実現するものである．この認証局を中心とした認証の枠組は，現在欧米を中心として様々な標準化，実験，運用がなされている．

しかし，認証局を中心とした認証基盤の標準化，実験，運用は，枠組として認証局が複数ある環境を規定しているが，ユーザやサーバなどのエンドエンティティの管理についての記述がない．また，その認証対象はあくまでエンドエンティティである．現実問題として，例えば企業間取り引きに代表される組織間のコミュニケーションやこの認証局のユーザは信じるが，あの認証局は信じないなどの要求がある．

本稿では，認証局が複数存在するマルチ認証局環境でのユーザ管理について考察し，ユーザ管理方式の手順を提案する．また，提案方式を実際にプライバシー強化仮想端末PET(Privacy Enhanced Telnet)[4]に応用した例を示す．

*A method of client mamagement in the multiple certification authority environment

†Kuroda Yasutsugu

‡Fujitsu Laboratories Ltd., 1-1, Kamikodanaka 4-Chome, kawasaki Japan, 211

2　認証局の環境

2.1　シングル認証局環境

認証局がネットワーク上に単独で存在する環境をシングル認証局環境と定義する．この環境の場合，ユーザやサーバなどのエンドエンティティは，ただ1つの認証局から証明書を取得し，その認証局を信頼点においてコミュニケーションを行なう．この環境の例として，WIDEプロジェクトが現在行なっているWIDE認証局の実験[5]がある．WIDE認証局は，公証人を用いて証明書発行を簡略化している．

2.2　マルチ認証局環境

認証局がネットワーク上に複数存在する環境をマルチ認証局環境と定義する．インターネットでは，Ineternet Societyが管理するIPRA(Internet Policy Registration Authority)を頂点とする認証局の木を形成し，インターネットなどの広域な環境での認証基盤の実現を目指している．日本では，ICAT[6]がIPRAから証明書を取得し実験を行なっており，実際に複数の認証局が立ち上がっている．また最近では，アメリカのVerisign社が独自に認証局の木を形成し，エレクトリックコマースを対象とした認証局の運用を行なっている．

3　ユーザ管理の考察

マルチ認証局環境では，ユーザが複数の証明書を持つ可能性がある．例えば，現実の世界で，電話をかける時にはテレホンカード，ショッピングする時にはクレジットカードとカードを使い分けるように，プライバシ強化電子メールを利用する時は，IPRAの認証の木に属する認証局から発行された証明書を用い，ショッピングを行なう時は，クレジット会社が運用する認証局からから発行された証明書を用いるというふうに，サービスの種類によって利用する証明書を使い分けることが想像できるからである．一人のユーザに複数証明書が存在する環境で考慮すべき点を以下に示す．

- 複数の認証局の管理
  マルチ認証局環境では，エンドエンティティを管理する場合，認証局も考慮に入れて管理しなければならない．例えば，クレジット決裁するシステムを考えた場合，店によってはVISAは許すが，MASTERは許さない，などのポリシーを反映する必要があるからである．
- 組織単位のユーザ管理
  マルチ認証局環境に限ったことではないが，組織単位の管理を考慮する必要がある．例えば，この組織のユーザはアクセスを許可するが，あの組織のユーザは許可しないというポリシーを反映する必要がある．

以上の点から，マルチ認証局環境でのアクセスを許すユーザは以下の3種類に分類でき，これらを考慮したユーザ管理をしなければならない．

- ある認証局に属するすべてのユーザ
- ある認証局から証明書を発行された組織のすべてのユーザ
- ある認証局から証明書を発行された組織の特定のユーザ

4 ユーザ管理方式の提案

3章で考察した内容をもとにマルチ認証局環境でのユーザ管理方式を提案する．提案方式を図1に示す．

step 1 証明書情報を読み取ることが出来るか．
yes→next, no→fault

step 2 証明書の電子署名は有効か？
yes→next, no→fault

step 2 証明書の期限は有効か．
yes→next, no→fault

step 3 管理ファイルに認証局名が登録されているか．
yes→goto step 6, no→next

step 4 管理ファイルに組織名が登録されているか．
yes→goto step 6, no→next

step 5 管理ファイルにシリアル番号が登録されてるか．
yes→next, no→fault

step 6 ユーザの電子署名は有効か．
yes→success, no→fault

図 1: ユーザ管理の提案方式

図1で，step 2 の電子署名は，ユーザの名前，公開鍵などの証明書情報に対して認証局の秘密鍵で作った電子署名．管理ファイルは，アクセスを許すユーザを記述したファイル．step 5 のシリアル番号は証明書情報の中の認証局が独自に証明書にふる番号で，ユーザを特定することが出来る．step 6 のユーザの電子署名は，例えばセッション毎に変化する乱数を種にユーザの秘密鍵で作られた電子署名である．

実際の管理では，マルチ認証局環境を考慮した本提案方式の管理の他に，証明書 Version 3 フォーマットの拡張部分やサービスに依存した管理の要素が取り込まれてくる．

5 PET での応用

提案方式の実現例として，PET で応用した例を示す．PET では，ユーザ管理ファイルにアクセスするユーザを記述することで提案方式を実現している．PET のユーザ管理ファイルを図2に示す．

図2のユーザ管理ファイルは，空行をデリミタに認証局を記述する部分，アクセスを許す組織を記述する部分，アクセスを許すユーザをシリアル番号によって記述する部分3つの部分にわかれている．認証局の部分は，セミコロンをデリミタに，第1カラムが認証局番号，第2カラムが認証局直下のすべてのユーザを許すかどうかを+, -で表したもの．第3カラムが認

```
1;-;/c=US/o=Fujitsu/ou=CA
2;+;/c=JP/o=AB Card/ou=CA
3;-;/c=JP/o=Verisign/ou=CA

1;/c=JP/o=Fujitsu/ou=Fujitsu Lab

1; 2688, 3746, ab63, dc87, e2d4, f3ed
3; 2325, 8797, 8403, ab73, 8394, bf94
```

図 2: ユーザ管理ファイル

証局の名前である．組織の部分は，セミコロンをデリミタに，第1カラムが認証局番号，第2カラムが組織名．エンドエンティティの部分は，セミコロンをデリミタに，第1カラムが認証局番号，第2カラムがアクセスを許すユーザのシリアル番号をカンマをデリミタに列挙したものである．

第2行目が，ある認証局に属するすべてのユーザすべてのアクセスを許すことを示した例．第5行目が，ある認証局から証明書を発行された組織のすべてのユーザをのアクセスを許すことを示した例．第7，8行目が，ある認証局から証明書を発行された組織の特定のユーザのアクセスを許すことを示した例となっている．

PET は，このユーザ管理ファイルを参照しながら，図1の提案方式に従ってユーザの管理を行なうことになる．

6 おわりに

本稿では，マルチ認証局環境におけるユーザ管理について考察し，ユーザは複数の証明書を持つことから，ユーザ管理の際には，1. 認証局の管理，2. 組織の管理，を考慮することが重要であることを示した．また，その考察に基づくユーザ管理方式を提案した．最後に，提案方式を PET で応用した例を示した．

本研究を進めるにあたり，WIDE プロジェクト，ICAT 広域認証実用化実験タスクフォースでの議論が大変有効であった．議論に参加して下さった両組織のメンバに感謝致します．

参考文献

[1] MasterCard, VISA, “Secure Electronic Transaction(SET) Specification Book 1,2,3,”, June 17, 1996

[2] Jnifer G. Steiner, Clifford Neuman and Jeffrey I.Schiller. “Kerberos: An Authentication Service for Open Network Systems.,” Proceedings of the USENIX 1988 Winter Conference,

[3] ITU-T Recommendation X.509, “The Directory Authentication Framework,” 1992

[4] 黒田康嗣, “公開鍵証明書を用いたプライバシ強化通信,” SCSI96, 2D,1996

[5] 菊池浩明, 黒田康嗣, “公証人を用いた暗号メール公開鍵証明書発行方式,” 情報処理学会第 48 回全国大会,1,pp.251-252, 1994

[6] 認証実用化実験協議会, “暗号認証技術を利用した鍵管理システムの調査研究,” May, 1996