SET他の認証システムの構築方法に関する考察

5M－8

吉武 淳　榊原 裕之
三菱電機（株）情報技術総合研究所

1．はじめに

電子商取引など急増しているインターネット上でのデータのやりとりでは、やりとりしている人がその本人であることを確認する技術が重要になっている。このような技術として、証明証を利用した認証システムが広く用いられるようになっているが、その設計手法はまだ確立されているとは言えない。

本稿では、電子商取引プロジェクトJapanNetにおけるSET他の認証システムの設計と運用から、その設計手法について考察する。

2．設計手法の確立の重要性とそのポイント

認証システムの設計は、その証明証が使われるアプリケーションによって、証明証の項目からエンティティの構成、CRLのフローまで変わりうるものである。他のアプリケーション用の認証システムの設計をただ真似るだけでは、運用に不都合が生じたり、性能的な問題が起きたりする可能性がある。

このような問題を起こさず、各アプリケーションに適した認証システムを設計するためのポイントとして、次のような事項が考えられる。

・証明証の内容－証明対象（何を証明するものか）、記載項目、公開／非公開の可否
・証明証とCRLの配布経路
・エンティティの構成法

また、JapanNetのような、複数のアプリケーションを想定した大規模な認証システムを構築する場合、次のような事項もポイントとなるが、これらについては別の機会に述べたい。

- ルートCAの役割
- ポリシーの徹底と柔軟性
- 証明証の項目と柔軟性

The points in design of an authentication sysytem
Jun Yoshitake, Hiroyuki Sakakibara
Information Technology R&D Center, Mitsubishi Electric Corporation

3．JapanNetの認証システム

JapanNetの認証システムの主なものは2つある。クレジット・カードの認証を行うSET (Secure Electronic Transaction) [1]の認証システムと、本人認証を行うJapanNet会員の認証システムである。それぞれのエンティティの構成を図1に示す。

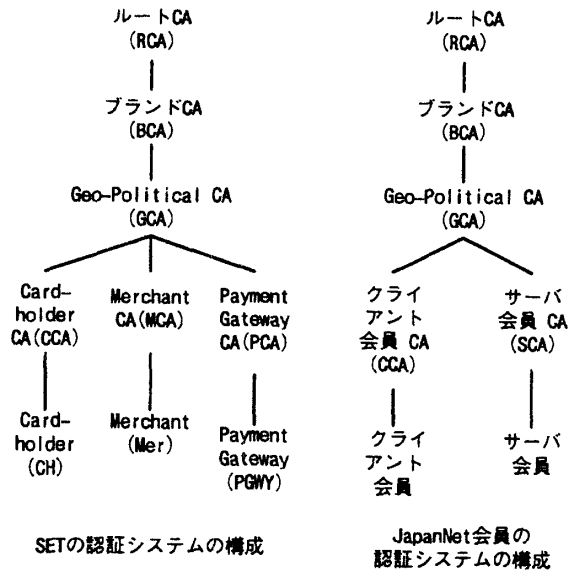

図1 JapanNetの認証システムの構成

以下、この2つの認証システムのそれぞれについて、2節に述べたポイントについて順に考察する。

4．SETの認証システム

(1) 証明証の内容

SETの証明証の証明対象はクレジット・カードである。記載項目は、X.509の標準の項目の他にCertificateTypeなどの独自の拡張項目を設けている。これらの拡張項目は証明証の検証上必要、また

はクレジット・カード決済というアプリケーションとして必要なものと考えられる。

なお、subject はクレジット・カード番号にハッシュ演算他を施したものになっている。また、それに対する余計な攻撃を防ぐため、証明証はディレクトリ・サーバによって配布することはしない仕様になっている。

(2) 証明証と CRL の配布経路

証明証と CRL は相手にメッセージを送る時に同時に送る仕様になっている。 特に CRL は、PGWY に最新のものを集めそこから Mer、CH に配布されるようになっているが、これはすべてのデータが PGWY を通ることによるものと考えられる。

(3) エンティティの構成法

CA の構成法は、クレジット・カード業界のビジネスの構造を反映していると考えられる。すなわち、まず BCA に VISA、MasterCard などの国際ブランドがある。次にその下に GCA がオプションとして用意されているが、これには日本の各カード会社などが相当すると考えられる。そして、その下に、エンド・エンティティに対応するものとして CCA、MCA、PCA がある。そして、エンド・エンティティとして、CH、Mer は現実世界のエンティティを反映したもの、PGWY は決済の処理上必要になったものと考えられる。

5．JapanNet 会員の認証システム

(1) 証明証の内容

証明証の証明対象は JapanNet の会員となった個人または法人である。記載項目は、X.509 の標準の項目の他に Class などの独自の拡張項目を設けている。JapanNet では、オンラインかオフラインかなど証明証を発行する際の本人確認の度合いによってクラスを 3 つに分けており、そのデータなどを証明証に記載しているわけである。

なお、subject は個人または法人を示す識別名になっている。また、証明証はディレクトリ・サーバで公開できるものであるが、現在は特に公開する運用はしていない（このことに特に理由はない）。

(2) 証明証と CRL の配布経路

現在、証明証の使われ方はクライアント会員が、JapanNet のサーバ会員となったショップの Web ページにアクセスする時に、JapanNet のメンバであることを検証する処理に使われるものであるが、その時に相手に証明証と CRL が渡される。しかし、各エンティティでディレクトリ・サーバを参照にいくよう設定されていれば、CRL についてはディレクトリ・サーバに取得にいき、それが相手から受け取った CRL より優先されるようにしている。

これは証明証の用途の 1 つとして電子メールを想定しており、PEM (Privacy Enhanced Mail)などで使用されている CRL の配布法にならったものである。電子メールではどのデータも必ず通るエンティティというものがないため、ディレクトリ・サーバから CRL を配布するようにしたものと考えられる。

(3) エンティティの構成法

CA の構成は SET の階層構造を参考に設計した。また、エンド・エンティティについては、それらが証明証を使用するアプリケーションで担う役割を考えて、クライアント会員とサーバ会員というエンティティを設けた。これについてはアプリケーション中の役割よりも、現実世界を反映した個人会員、法人会員というタイプにした方が運用上わかりやすかったのでは、という考え方もある。

6．おわりに

認証システムの設計方法のポイントをあげ、実際に構築した JapanNet での認証システムでその内容を考察した。今後もこのような積重ねを継続し、よりよい認証システムの設計手法を確立していく。

参考文献

1) Secure Electronic Transaction (SET) Specification, Book 2: Programmer's Guide, Version 1.0 May 31, 1997.