X.509 Certificate の実社会アナロジ再考

4G－6

古谷雅年
日立製作所システム開発研究所

1. はじめに

信頼できる第３者機関が発行する X.509 Certificate を利用した情報ネットワーク社会における電子認証の仕組みは、日本では、しばしば実社会における印鑑登録証明制度に類似していると例えられる。これは、電子認証の仕組みが主として公開鍵暗号方式の研究から発展してきた経緯により、Certificate の記載事項の公開鍵を主として取り扱おうとする傾向があるためである。

しかし、両者の性質を比較してみると、似て非なるものがある。本来、X.509 Certificate は、所有者(または、エンドエンティティ)の属性と、公開鍵を結びつけるものであり、これらの主従関係について規定しない。一方、実社会における良く似たもう１つの存在であるパスポートは、所有者の属性を主、顔写真や自署によるサインを従とみなすのが自然なものである。

本稿では、実社会における印鑑登録証明書とパスポートを比較分析することにより、情報ネットワーク社会における X.509 Certificate の意味合いについて再考してみる。

2. パスポートと印鑑登録証明書の比較

表１にパスポートと印鑑登録証明書、及び、X.509 Certificate の特性比較を示す。表を見ればわかるとおり，実社会におけるパスポートと印鑑登録証明書には、有効期間、原本性、利用回数制限、提出と提示、所有者の制限などで特性に違いがある。例えば、パスポートの場合には、取得した後は、有効期間内において、海外旅行時に何度でも利用できる（相手に提示する）のに対し、印鑑登録証明書の場合には、必要な時に取得し、実印を押印した書類とともに相手に提出する。

また、印鑑登録証明書の発行日は、印鑑（正確には印影）を登録した日を意味しているのではなく、利用者からの申請に基づき、登録されていた印影に相違ないことを証明した日であることに注意しなければならない。

両者の特性を比較すると、現行の電子認証の仕組みで利用される X.509 Certificate の意味合いは、よりパスポートに近い。現時点で X.509 Certificate がパスポートの特性に近づけない部分は、属性情報の変更に伴なう柔軟な対応と、「提示（相手に見せて、また自分の手元にもどる)」という概念を、コピーが容易な世界でどう実現するかである。

3.「証」と「証明書」

ここまでの説明においては、あえて X.509 Certificate という表現を用いてきた。ここでその日本語訳について考えてみる。

表２に実社会における書類を２つのカテゴリに分類する。表に示したとおり，保管管理の有無、提示と提出、継続利用と利用時毎という観点で書類を分類すると、日本の慣例では、「～証」と「～証明書」を使い分けている（注：例外もある)。この分類では「～証」系には、「～券」「～手帳」などが入り、「～証明書」系には、「～謄抄本」「～写し」「～書」などが入る。

つまり、これまでの分析からすると、X.509 Certificate は、パスポートの特性に近いので、その日本語訳としては、「公開鍵証明書」ではなく、「～証」と訳すのが適当である。例えば、X.509 Certificate の属性情報が所有者の運転

Analogy Model to X.509 Certificate in Real World
Masatoshi Furuya
Systems Development Laboratory, Hitachi Ltd.

資格であるならば、「電子運転免許証」となる。

4. X.509 Certificate の位置付け

X.509 Certificate の位置付けは、Certificate に示された属性をもつ所有者として、情報ネットワーク社会のサイバーコミュニティに参加するための自己紹介手段である。つまり、コミュニティ上に属性情報を公開することで、他のメンバから認知してもらうためのものである。認知されるかは、コミュニティメンバへ属性開示が十分かどうかによる。

5. 属性を確認するタイミングと作法

実社会のパスポートや運転免許証を考えると、相手が確認するのは、提示された一瞬のみである。コピーをとらない限り、これらの写しを保管しない。X.509 Certificate の利用も相手からの求めに応じて送信し、相手は署名検証の確認が済んだら速やかに破棄するのが作法である。

6. まとめ

X.509 Certificate の実社会のアナロジとしては、印鑑登録証明書よりはパスポートに近く、サイバーコミュニティにおける電子署名時の自己紹介手段の１つであることを示した。

表2 「証」と「証明書」

「証」系	「証明書」系
・所有者が保管管理 ・利用時提示 ・取得後、継続利用	・普段は保持しない ・利用時提出 ・利用毎に取得
パスポート（旅券） 運転免許証、社員証 資格免許証、学生証 健康保険証 クレジットカード キャッシュカード 銀行通帳、 母子手帳、健康手帳 定期券、生命保険証券	印鑑登録証明書 戸籍証明書、 所得証明書 戸籍謄本、戸籍抄本 住民票の写し 健康診断書 領収書、請求書

表1 パスポート、印鑑登録証明書、X.509 Certificate の比較

比較項目	パスポート	印鑑登録証明書	X.509 Certificate
属性記載項目	氏名、性別、生年月日、国籍など	氏名、性別、生年月日、住所	エンドエンティティの属性
結びつけるもの	顔写真、自署サイン	印影	公開鍵
属性情報変更時の対応	追記による属性情報の変更が可能	無関係	失効させて再発行
有効期間の記述	開始日と終了日	発行日のみ	開始日と終了日
有効期間、発行日の意味	開始日と終了日の間で記載事項が有効	印影と属性が一致していることの証明日。 いつまで有効かは利用側の規定による	開始日と終了日の間で記載事項が有効
原本性	所有者へ交付したものが原本。つまり所有者自身が保管管理する。	所有者へ交付したものは原本の写しに相当。所有者が保持するのは申請時から利用時までのごく短い期間である。	電子データなどでどれが原本かはあいまいだが、申請時に本人に交付。所有者自身も保管管理する。
取得時期、利用回数制限	申請時のみに取得し、有効期間内なら何回利用しても良い	必要な時毎に取得し、原則１回のみの利用	申請時のみに取得し、有効期間内なら何回利用しても良い
利用時の相手への提示、提出	利用時、相手に提示	利用時、実印を押印した書類とともに相手に提出	利用時、相手に送信
所有者の制限	原則制限がない	１６歳以上に制限	運用による