公開鍵証明書の日本語対応における一考察

4T－9

高村 昌興　橋川 善之　土屋 茂樹　中村 逸一
{takamura, hashii, tsu, naka}@rd.nttdata.co.jp
株式会社 NTT データ

1.はじめに

現在、公開鍵証明書を利用したセキュア通信（公開鍵インフラ：PKI）[1, 2]が、web、メール等インターネットを利用したアプリケーションにおいて利用されている。特に、電子決済システムで見られるように、課金情報やプライバシー情報を扱うためには、情報をセキュアに扱える公開鍵インフラが必須と言える。

このとき、公開鍵証明書は、証明書発行者が持っている利用者情報に基づいて発行されることになるが、その利用形態を考えたとき、公開鍵証明書を鍵の証明書としてだけではなく、身分証明書として利用する場合もある。そのため、このようなシステムにおいては、日本語でかつ外字も扱える証明書を必要としている。

本報告においては、日本語を必要としている公開鍵証明書に対して、我々が検討を行った観点とその検討結果に従って実装した例を紹介する。

2.日本語対応公開鍵証明書の問題点

我々は、数多くの PKI システムを構築するにあたり、様々な検討を行った。その結果として、公開鍵証明書の利用方法は、従来の暗号通信やアクセス制御に加え、以下の必要性を把握した。

・証明書の内容を、日本語で記載したい。
・外字を扱いたい。
・システム個別情報を扱いたい。
・公開鍵証明書を、身分証明書と同等に扱いたい。
・日本語で証明書検索を行いたい。

これらを X.509 Certificate Ver.3 [2] に適用することを考えたとき、多大な改造を行う必要があり、場合によっては、規格外になりうる。また、身分証明書相当に扱えるように個人情報を公開鍵証明書へ取り入れることは、証明書が公開される情報であることを考えたとき、プライバシーの問題にも発展すると考える。

しかし、身分証明書相当の公開鍵証明書は、SET 等オープンなシステムにおける公開鍵証明書の利用でない限り、プライバシーの問題は回避できると考える。そのため、今回の必要性で見られるような特殊な証明書の利用は、運用方法によって意味のある仕組みと考える。

3.公開鍵証明書における規格

IETF(Internet Engineering Task Force)においては、ドラフト段階ではあるが、これまで X.509 Certificate Ver.3 といった証明書フォーマットが提案されている。各ソフトメーカは、これとは別の ITU-T [3] に準拠した実装を行っており、記載方法として PrintableString を利用している場合が多い。しかし、我々は、このドラフトに従うことで、先行して日本語対応することを考える。

我々は、表 1 で示される文字コードに関する扱いに従って検討を行うが、ドラフトの仕組みとしては、英語圏以外にも対応できる仕組みを持っている。

表 1. X.509 Certificate で扱う文字コード

PrintableString	大文字／小文字の英字、数字、句読点、空白より構成
TeletexString	ISO2375 への登録番号、87、102、103、106、107 の文字集合と空白より構成
BMPString	基本多言語面(BMP : Basic Multilingual Plane) の 約 36,000 文字より構成
UTF8String	Unicode で非 ASCII 領域(80h~FFh)のみをエンコードした文字セットで構成
UniversalString	日本語, 中国語などの漢字圏を含めた世界的に共通なコード体系の文字セットで構成

A Case Study of X.509 Certificate Handling Japanese Characters
Masaoki Takamura, Yoshiyuki Hashikawa, Shigeki Tsuchiya, Itsukazu Nakamura
NTTDATA CORPORATION

4.利用形態を踏まえた日本語対応証明書の検討

公開鍵証明書の項目において、日本語で属性を記載できる箇所としては、表2で示す項目を考える。考え方としては、X.509 Certificateの中の利用者、及び発行者の属性が入る箇所に観点を置き、かつ住所、会社所属等の一般的な個人情報以外の情報も入る可能性を持つ属性である。その際に、日本語対応を行ったときの長所、短所を合せて示す。

表2. 日本語対応箇所

項目	検討課題	
Issuer Name（発行者名）、Subject Name（所有者名）	長所	①市販暗号ライブラリで、属性の操作可能 ②LDAP [4]との連携が可能
	短所	①ASN.1で定義され ている属性に限定 ②規定外の情報は、オブジェクト識別子取得対応が必要
Subject Alternative Name（所有者別名）、Issuer Alternative Name（発行者別名）	長所	①市販暗号ライブラリで、属性の操作可能
	短所	①ASN.1で定義されている属性に限定 ②規定外の情報は、オブジェクト識別子取得対応が必要
Subject Directory Attribute（所有者ディレクトリ属性）	長所	①所有者の任意の属性が格納可能（画像も可能）
	短所	①市販暗号ライブラリのサポート不足 ②ASN.1で定義され ている属性に限定 ③規定外の情報は、オブジェクト識別子取得対応が必要
Private Internet Extension（個別拡張）	長所	①システム単位で必要な情報を格納可能
	短所	①市販暗号ライブラリのサポート不足 ②オブジェクト識別子取得対応が必須

5.公開鍵証明書の実現

5.1.実装結果

本実装では、証明書のコードとして、UniversalStringをサポートすることとし、かつ発行者、及び利用者名の項目を日本語に対応することとした。証明書の利用方法を考えたとき、発行者名、利用者名が日本語表記されていることは、日本語で証明書検索できるため、利用者の利便性向上にも繋がると考えた。

上記実装によって、2節で挙げた検討課題は、外字対応以外の項目について対応可能である。

5.2.実装に伴った問題点

発行者名、所有者名の利用方法を考えたとき、それぞれの属性を単に提示するだけでなく、公開鍵証明書を取得するための階層構造も考慮する必要がある。例えば、図1の例を考えたとき、従来の検索では、社員名までで証明書が取得可能であったのに対し、本方式では、社員番号まで入力する必要がある。

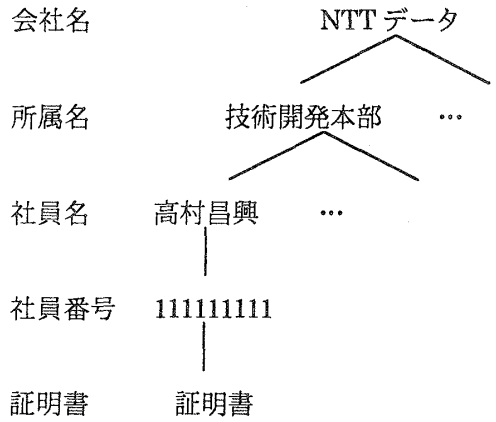

図1.階層構造の例

そのため、情報検索と言う観点を取り入れたとき、全ての個人情報を発行者名、所有者名に収めることは、情報検索に不向きな場合も考えられる。

6.まとめ

本報告では、身分証明書相当の公開鍵証明書を実装するために、発行者名、及び利用者名部分を日本語に対応することについて述べた。その結果、目的に伴って生じるいくつかの検討項目も抽出された。

しかし、今回の実装方式は、数多くある実装の一つであり、検討した範囲でも4節で示したような様々な実装がある。今後は、それぞれの長所、短所について更なる検討、及び新規実装方法を検討し、最適な証明書の日本語対応を実現することである。

また、今回は外字の対応を見送ったが、日本語を扱う限り、対応が必ず必要となる課題である。例えば、運用において氏名や法人名と言った情報を正式名称で扱う際は、外字が必須である。今後は、そのような外字の取り扱いについて実現することである。

Reference

[1] http://csrc.nist.gov/pki/documents/welcome.html
[2] http://www.ietf.org/rfc/rfc2459.txt
[3] http://www.iso.ch
[4] http://www.ietf.org/rfc/rfc2587.txt