QC プロファイルの整合的な利用法

宮川　寧夫 †　　松本　泰 †

† 独立行政法人 情報処理推進機構
isec-info@ipa.go.jp

あらまし　欧州においては，EU 指令によって電子署名法に準拠する場合の X.509 証明書として QC（Qualified Certificate）プロファイルが利用されている．近年，欧州各国は QC プロファイルをリモート認証用途にも使う動きが見られるようになってきた．QC プロファイルとは，個人のアイデンティティを，何らかの法的な裏付けのもとに確認されたクレデンシャルを統一的に表現するためのフォーマットであり，IETF においても一般的な規定がなされている．わが国における QC プロファイルの導入可能性について，他の様々な要件との整合性を勘案しながら検討する．

Consistent Usage of Qualified Certificates

Yasuo Miyakawa†　　Yasushi Matsumoto†

†Information-technology Promotion Agency (IPA)
isec-info@ipa.go.jp

Abstract　In Europe, QC (Qualified Certificate) profile has been utilized under the EU Directive on Electronic Signature. Recently, each member countries started to use the QC profile also for remote authentication. QC is used, describing a certificate whose primary purpose is to identify a person with a high level of assurance, where the certificate meets some qualification requirements defined by an applicable legal framework. We discuss here about the possibility of employing this profile in Japanese government PKI certificates, and its consistent usage.

1　電子政府 PKI における X.509 証明書

1.1　欧州において

欧州においては，その電子署名用の X.509 証明書 [1] として，QC プロファイルが採用されている．QC プロファイルとは，個人のアイデンティティを，何らかの法的な裏付けのもとに確認されたクレデンシャルを統一的に表現するためのフォーマットである．EU の域内各国においては電子署名アプリケーションの相互運用可能性が重視されてきたため，共通のフォーマットが要請されていた．EU 域内で適用国の範囲が広がるほど，クレデンシャルが流通するので，フォーマットが共通化されていることは，サービスを向上させる基礎となると共に，国を超えた全体最適化をはかる手段となっている．

2008 年には電子署名法および本人確認についてのアクションプラン [8] が発行された．このアクションプランにおいて，EU 特有の 3 つの形態の電子署名が掲げられており，この内の 2 つで QC プロファイルが利用されている．

また，リモート認証アプリケーションについても QC プロファイルが採用されるようになってきた．アクションプランの中で，リモート認証は，‘eID’ の一環として記述されており，国家間で法的な要件等の調整を要する論点である．

当初の紙に基づく手続き	数
実印	3
印鑑に加えて真正性検証	36
真正性検証を伴わない印鑑	6
印鑑無し	2
計	47

表 1: アンケート調査結果の概要

このような論点は，STORK プロジェクトにおいて調整されるという [10].

1.2 日本において

わが国においては QC プロファイルは，採用されていない．現在，公的な PKI システムにおいては電子署名アプリケーションしか運用されていないが，リモート認証アプリケーションに関する動きもある．

2008 年に内閣官房において電子申請アプリケーションの利用率が低いことを問題視して，他の電子行政サービスのアプリケーションも視野に入れたシステム要件を決める枠組みについての検討が開始された．現在，「電子政府ガイドライン作成検討会」[1] において検討されている．ここでは，各省庁に対するアンケート調査も実施されている．「オンライン利用拡大行動計画」における 71 の重点手続きのうち電子署名を要する 47 の手続きの管轄官庁に対してアンケート調査が実施され，必要に応じて訪問インタビューも行われた [11].

わが国においては，紙の公文書に対して，署名ではなく印鑑を押す慣行があり，実印，認印がある．安易に捺印を電子署名に置き換えてきたことが認識されている．現在に至るまで否認防止用証明書しか発行されていない．また，この検討会においては，「電子署名」のみならず「リモート認証」も併せて考慮してシステム要件が選択できるような枠組みを検討している．ちなみに，リスク分析に基づいてシステム要件が「保証するレベル（LoA）」を選択できる枠組みも検討されている．

また，公的個人認証サービス普及拡大検討会[2] においてもリモート認証用証明書の発行についての検討が行われている．「公的個人認証サービス普及拡大検討会中間取りまとめ (案」[3] としては，「現行証明書を認証用として併用する」案を軸として検討されている．しかし，この案のように電子署名用の証明書とリモート認証用の証明書を混用することには，攻撃の可能性がある [13].

2 QC プロファイル仕様

2.1 QC Profile の概要

‘Qualified Certificate’ という用語は，IETF においては，高い保証レベルによって個人を識別する「適格証明書」を指すために使われている [5].

一般に，紙の法定文書について一定の様式が指定されているように，X.509 証明書 [1] についても一定のフォーマットを規定する必要がある．さらに，ディジタル証明書の項目のいくつかについては，システムによって自動処理できるようにする必要性が加わる．

一般型としての X.509 証明書 [1] のインターネット上におけるプロファイル仕様が RFC 5280[3] であり，その中で自然人をサブジェクトとする証明書のプロファイルとして QC プロファイル [5] が制定されている．一般的な X.509 証明書プロファイルは，裁量の幅がある柔軟な構造をもっている．それゆえ，証明書発行者に自由にさせると，多様な構成をもつ証明書が発行され続けてしまうことになる．アプリケーションを相互運用可能かつ高機能に開発できるための基礎として，共通フォーマットは意義をもつ．

QC プロファイルの各フィールドについて，一般的なプロファイルが規定している以外にも，いくつかの項目について標準化することが不可欠

[1] http://www.kantei.go.jp/jp/singi/it2/guide/index.html

[2] http://www.soumu.go.jp/main_sosiki/kenkyu/kojin_kakudai/index.html

[3] http://www.soumu.go.jp/main_sosiki/kenkyu/kojin_kakudai/16935.html

であった．現行の QC プロファイルに固有な項目は，法的な規定への対応を示すための参照項目と,「自然人の ID を表現する諸項目」についての 2 つであると言える．

ちなみに，QC は特定の法律に基づいて発行されるが，当該 QC を 「適格証明書」と見なすべきか否かを決定する手続き等については，QC 仕様の範囲外とされている [5].

2.2 QC プロファイルの経緯

欧州の電子署名法 [9] に準拠する事項も表現できるフォーマットとして意図され，IETF と ETSI において標準化されてきた．IETF における初版（前版）RFC 3039 を策定するためのインターネットドラフトが 1998 年 10 月に投稿され，2001 年 1 月に発行された [4]．ETSI におけるプロファイルの初版（v1.1.1）は，2000 年 12 月に発行されたことになっているが，これは既に RFC 3039[4] を参照しているので，両者は，ほぼ同時に発行されたといってよい．

IETF の改訂版の RFC が 2004 年 3 月に RFC 3739[5] として発行された後にも，同年 6 月に ETSI は固有要件を加えてプロファイルを更新した [7].

このように QC プロファイル仕様については欧州の ETSI が主導しつつ，IETF においても，より国際的な標準化活動が行われてきた．

2.3 QC の否認防止用途以外の利用可能性

かつて，QC プロファイル仕様において，旧版の RFC 3039[4] には「否認防止用」と書かれた部分があった．

> Within this standard the term ”Qualified Certificate” is used more generally, describing the format for a certificate whose primary purpose is identifying a person with high level of assurance in public non-repudiation services.

しかし，現行の RFC 3739[5] の QC プロファイルを利用する条件は，ディジタル署名の否認防止，すなわち電子署名法における利用に限定されていない．

> Some editorial clarifications have been made to introductory sections to clarify that this profile is generally applicable to a broad type of certificates,

したがって，このプロファイルは他の用途においても，採用することができる．他の用途として，適格なユーザをネットワーク越しにリモート認証する状況に用いるリモート認証用があり，近年，欧州において利用されるようになってきたことは上述のとおりである．

2.4 QC プロファイルを採用する利点

QC プロファイルを利用できるような，何らかの法的な裏付けのもとで本人確認が行われる場合，QC プロファイルを利用べきと考える．

相互運用可能性の確保の観点からは「統一的な処理」ができる共通フォーマットが，一般的な X.509 証明書よりも具体的なレベルで存在していることが望ましい．また，国際的な標準化活動の成果を活用れば，範を示し易い．

日本においては，QC プロファイルは採用されておらず，独自に変則的なプロファイルが定められいるものがある.「名前や属性情報の格納法」において後述する．

3 QC プロファイルの適用可能性

QC プロファイルを導入し適用するする際には，鍵用途拡張のビットのセット法，QC 宣言の書き方，名前や属性続税情報の格納法等の論点がある．

3.1 鍵用途拡張のビットのセット法

鍵用途（Key Usage）のセット法については RFC 5280[3] 中に明記されていない．そこで，

電子署名用およびリモート認証用を指定する設定を行う際の留意点を整理する．

X.509 証明書において，拡張領域に鍵用途拡張を指定する．鍵用途拡張には，9 種類が挙げられており，対応するビットを立てることによって指定する．: digitalSignature, nonRepudiation, keyEncipherment, dataEncipherment, keyAgreement, keyCertSign, cRLSign, encipherOnly および decipherOnly.

この中で，digitalSignature ビットと nonRepudiation ビットの用法は紛らわしく，長年，議論されてきたが，未だに，これらの使い分けについての明確な指針は無い．セキュリティの観点から悪用されないようにしつつ [13]，実装者が誤らないように統一的な指針を示すことが期待される．

リモート認証において利用されるデジタル署名が文書への永続的署名とされてしまうリスク [13] を考慮して，digitalSignature ビットは，自動処理される処理（典型例：リモート認証）にのみセットしたい．他方，人間の意志によって署名者が行う永続的な（将来検証される）処理（典型例：デジタル署名）については nonRepudiation ビットをセットすべきということになる．

リモート認証には digitalSignature ビットのみを立てた証明書を使い，電子文書に人間が行う署名には nonRepudiation ビットのみを立てた証明書を使うようにすれば，悪用されることは無く，実装を誤りにくい．

3.1.1 否認防止用証明書

否認防止用証明書，すなわち電子署名用の証明書では，nonRepudiation ビットがセットされる．RFC 5280[3] 中の該当部分の記述を抜粋する．

> The nonRepudiation bit is asserted when the subject public key is used to verify digital signatures, other than signatures on certificates (bit 5) and CRLs (bit 6), used to provide a non-repudiation service that protects against the signing entity falsely denying some action. In the case of later conflict, a reliable third party may determine the authenticity of the signed data. (Note that recent editions of X.509 have renamed the nonRepudiation bit to contentCommitment.)

そもそも，digitalSignature と nonRepudiation の用語は，紛らわしく，誤解を生み易い．実際，それらは世界中で異なるように使われている．

欧州においては nonRepudiation ビットのみを立てている．RFC 3039[4] においても，nonRepudiation ビットのみを立てることを規定していた．

一方，米国においては nonRepudiation ビットのみならず digitalSignature ビットも立てるのが慣行となっている．日本の電子政府 PKI システムは，2000 年に，この米国式を採用してしまった．現在に至るまで，このような否認防止用証明書しか発行されていないが，nonRepudiation ビットのみをセットするように．改めることは可能であろう．

3.1.2 リモート認証用証明書

リモート認証用の証明書では，一般に，digitalSignature ビットがセットされる．QC プロファイルを採用する場合も同様となる．RFC 5280[3] 中の該当部分の記述を抜粋する．

> The digitalSignature bit is asserted when the subject public key is used for verifying digital signatures, other than signatures on certificates (bit 5) and CRLs (bit 6), such as those used in an entity authentication service, a data origin authentication service, and/or an integrity service.

リモート認証用の証明書では，表 3 のように拡張鍵用途（ExtendedkeyUsage）の表現力も使うようにする．

	nonRepudiation bit	digitalSignature bit
Europe	Yes	-
US	Yes	Yes

表 2: Key usage bit setting

	電子署名	リモート認証
Key Usage	nonRepudiation	digitalSignature
ExtendedkeyUsage	-	ClientAuth

表 3: digitalSignature bit setting

3.2 QC 宣言の書き方

RFC 3739[5] によれば，ある証明書が何らかの法的な裏付けのもとに確認された QC であることを示す書き方には 2 つの方法がある．

- As information defined by a certificate policy included in the certificate policies extension, and
- As a statement included in the Qualified Certificates Statements extension.

ユーザビリティの観点からは，後者のように QC 宣言中に書く方が分かり易い．前者のように CP（certificate policy）に書く方法もあるが，両方に書けば確実となる．

3.3 名前や属性情報の格納法

公的個人認証基盤（JPKI）[4]は，住民の否認防止用証明書を扱う PKI システムである．ここでは住民基本台帳の 4 情報（氏名，住所，性別および生年月日）を中心に，一般的な名前や属性項目の格納法に関する論点を掲げる．QC プロファイルには，潜在的には ID 番号を格納するという論点があるが，ここでは割愛する．

ローカル言語（例：日本語等）で表記したい名前項目については commonName に UTF8String で書くことになる．今日，現行の RFC 5280[3] にも基づくことになるからである．名前に基づいて自動処理が行われるような要件は想定せずに，表示処理ができれれば十分である．名前について，国際対応の観点からは，併せて英語表記を求めたいところであるが，法定項目とはされていない．

JPKI のエンドエンティティ証明書中のプロファイル [12] においては，独自の名前の格納法を規定している．名前を他の項目と共に日本語表記で subjectAltName 拡張の otherNames に書くこととされており，他の民間認証局が発行する証明書とも異なるプロファイルをもつ．この背景には，いくつかの理由があると推察される．

- 他の法定項目と共にひとかたまりに列挙したかった
- 通常は用いられないローカル文字を表示するための特別な処理を入れたかった

この otherNames 領域は，QC プロファイルには無いので，適切な格納法を検討する必要がある．「サブジェクトディレクトリ属性」を使えば，生年月日および性別の 2 つは，適切に格納できる．

- dateOfBerth
- gender

しかし，住所については，悩ましい．RFC 3039[4] には postalAddress という項目があったが，当時，一般的なプロファイルを規定して

[4] http://www.jpki.go.jp/

いた RFC 3280 [2] と整合性をとるために RFC 3739[5] には無くなってしまった.

欧州においては，一般に，住所は格納されない．別に項目を追加することもできるので，独自に項目を復活させて規定することもできよう.

4 結論および提言

QC プロファイル仕様を要件とすることが適する案件は，わが国の電子政府 PKI においても存在している．民間においても，犯罪収益移転防止法等に基づいて本人確認が求められるサービスがあり，何らかの法的な根拠をもつクレデンシャルの提示に基づいてリモート認証を行うアプリケーションを構築する潜在的な必要性もある.

相互運用可能性の確保の観点は，今後，例えば電子政府のバックオフィス連携を図る際等に重要となる．国際的な仕様に基づくプロファイルを導入することによって，国内において範を示しながら他の民間認証局が発行する証明書との相互運用可能性も確保することができる.

また，自然人のクレデンシャル自体についても，国際化対応をはかる必要もあろう．例えば，英語表記の名前等を統一的に格納すためには法的な検討も必要である.

参考文献

[1] ITU-T Recommendation X.509 (2005) — ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

[2] RFC 3280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” (April 2002) http://www.ietf.org/rfc/rfc3280.txt

[3] RFC 5280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” (May 2008) http://www.ietf.org/rfc/rfc5280.txt

[4] RFC 3039, “Internet X.509 Public Key Infrastructure Qualified Certificates Profile” (January 2001) http://www.ietf.org/rfc/rfc3039.txt

[5] RFC 3739, “Internet X.509 Public Key Infrastructure Qualified Certificates Profile” (March 2004) http://www.ietf.org/rfc/rfc3739.txt

[6] ETSI TS 101 862 V1.1.1, “Qualified Certificate profile” (December 2000)

[7] ETSI TS 101 862 V1.3.2, “Qualified Certificate profile” (June 2004)

[8] “European Action Plan on e-signatures and e-identification” (November 2008) http://ec.europa.eu/idabc/en/document/7768

[9] Directive 1999/93/EC, “Community framework for electronic signatures” http://europa.eu/legislation_summaries/information_society/l24118_en.htm

[10] “D2.2 . Report on Legal Interoperability” (2009) http://www.eid-stork.eu/dmdocuments/D2.2_final._1.pdf

[11] 「セキュリティ分科会の検討状況別紙」，電子政府ガイドライン作成検討会（第 2 回）(2008 年 4 月 20 日) http://www.kantei.go.jp/jp/singi/it2/guide/kaisai_h20/dai2/siryou2-2.pdf

[12] 『公的個人認証サービス プロファイル仕様書』(2004) http://www.lascom.or.jp/jinfo/jpkiapv1/profile.pdf

[13] Y. Miyakawa et al., “Current Status of Japanese Government PKI Systems”, EuroPKI 2008. LNCS, vol.5057, pp.104-117. Springer, Heidelberg (2008)