MC-01

携帯電話加入者証明書プロファイル

平成 22 年 7 月 15 日　　1.0 版

社団法人電波産業会
高度無線通信研究委員会
モバイルコマース部会

本文書は、モバイル IT フォーラムモバイルコマース部会平成 14 年度活動報告書（平成 15 年 5 月 23 日付）に記載されていた「携帯電話加入者証明書」を抜粋及び誤記訂正した文書である。

本文書は、社団法人電波産業会高度無線通信研究委員会モバイルコマース部会の承認を経て、ここに開示するものである。

携帯電話加入者証明書プロファイル
目次

1　序文

1．1　前提

本プロファイルは、当面多くの利用が見込まれる「SSL クライアント認証用証明書」を対象とする。

ディジタル署名は対象としない。

1．2　目的

現在は携帯電話を利用したモバイルコマースの立ち上がり期であり、今後さまざまな業務に携帯電話を利用したサービスが構築されていくことが想定される。

これらのサービスの共通の課題の一つとして、通信先の認証の必要性が挙げられる。その認証方法の一つに電子証明書を利用した方法が考えられるが、携帯電話利用者の認証として携帯電話会社ごとに別々のポリシーで電子証明書が発行された場合、サービス提供者はそれぞれ異なる対応が必要となることが懸念される。

本資料の目的は、携帯電話会社が発行する加入者証明書について共通化が求められる内容をまとめ、システム構築のための参考プロファイルとして公開するものである。

なお、本資料で提示する参考プロファイルは、携帯電話利用者、サービス提供者、携帯電話会社のいずれに対しても、強制力や責務を負わせるものではない。

1．3　共通化の対象項目

本資料では、下記の項目について共通化を行う。

(1) 証明書の位置付け

証明書の所有者あるいは検証者が、発行した携帯電話会社によらず、共通した取り扱いが可能となるよう、証明書の発行対象や利用対象といった「証明書の位置付け」を共通化する。

(2) 証明書の記載事項

証明書の所有者あるいは検証者が、発行した携帯電話会社によらず、共通したシステムで証明書を処理できるよう、証明書の形式や証明対象の表現など「証明書の記載事項」を共通化する。

(3) CRL の記載事項

証明書の検証者が、発行した携帯電話会社によらず、共通したシステムで証明書の失効確認を処理できるよう、CRL(Certificate Revocation List)の形式や更新間隔など「CRL の記載事項」を共通化する。

1．4　方針

本資料では、下記の方針で共通化を行う。

(1) インターネットとの接続性

- インターネット上のサービス提供者を考慮し、RFC2459 等の標準へ準拠する。なお、WAP2.0 等の関連標準も必要に応じ考慮する。

(2) 最小限の規定

- RFC2459 準拠を基本とした上で、規定の重複を避けるため、特に制約や留意事項がある場合のみ規定する。

(3) 通信事業者としての立場

- 契約者のプライバシを考慮する。
- 契約者の認証内容(認証手続き)を考慮する。

(4) 利便性の考慮

- モバイルコマース等を構築し提供するサービス提供者の利便性を考慮する。
- 証明書を使い、上述のサービスを利用する携帯電話利用者の利便性を考慮する。

(5) 現実性の考慮

- 現状広く利用されている製品のサポート状況を考慮する。

1．5　想定利用モデル

本プロファイルは、SSL クライアント認証で利用されると想定する。

図 1 に、利用モデル例を示す。

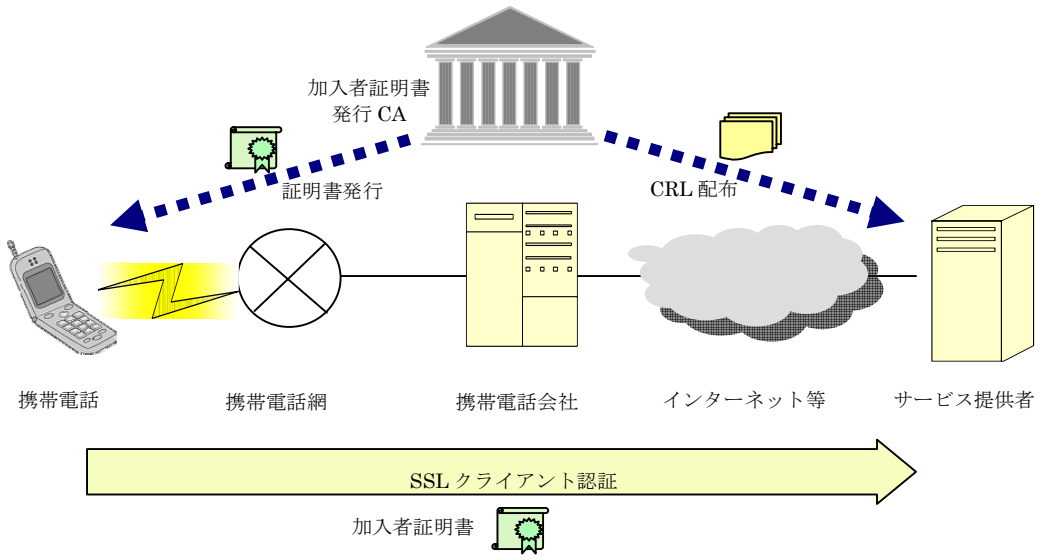

図 1　利用モデル例

２　証明書の位置付けに関するプロファイル

２．１　証明書発行対象

本プロファイルでは、携帯電話契約の「契約」に対して発行することとする。

なお、証明書に記載する発行対象は、契約ごとに一意で、かつ証明対象の特定が困難なモバイル ID で表現する。

２．２　証明書の利用対象

本プロファイルで対象とする証明書は、携帯電話を使用した「SSL クライアント認証」で使用されることとする。

具体的には、以下のプロトコルおよびアルゴリズムへの対応を含むこととする。

利用プロトコル：SSL V3.0

鍵交換アルゴリズム：RSA KeyEncipherment

２．３　秘密鍵（Private Key）

(1) 秘密鍵の保管

証明対象の公開鍵に対応する秘密鍵は、コピーに対する十分な対策を持った媒体に保管する。

(2) 鍵対の強度

証明対象の公開鍵に対応する鍵対の強度は、RSA の鍵長 1024 bits 相当以上とする。

２．４　証明書のライフサイクル

(1) 証明書の有効期間

加入者証明書の有効期間は、安全性や利便性の点から「2 年」を基本する。

(2) 証明書の失効に関する取り扱い

加入者証明書の失効情報は、「CRL」で提供する。

ただし、OCSP 等の他の方法で失効情報の提供を行うことを妨げるものではない。

３　証明書の記載事項に関するプロファイル

３．１　証明書形式

証明書の形式は、X.509 とする。X.509 のバージョンは、拡張情報(Extensions)を使用する場合は V3、使用しない場合は V1 とする。（詳細は「５．関連標準」を参照）

証明書の記載事項に関するプロファイルは RFC2459 に準拠するものとし、記載に際して、特に制約や留意事項がある場合のみ、次節以降に示す。

３．２　証明対象の表現

証明対象は「Subject」に DN(distinguished name)で表現する。

以下の項目は共通仕様とし、他の項目(OU 等)は任意とする。

C = jp
O = (オペレータ社名の英語表記)
CN = (モバイル ID。フォーマットは任意)

なお、証明書の DN の表記は証明書を利用する製品の対応状況を考慮し、PrintableString とする。

３．３　証明書発行者の表現

証明書発行者は「Issuer」に DN(distinguished name)で表現する。

以下の項目は共通仕様とし、他の項目(OU 等)は任意とする。

C = jp
O=(オペレータ社名の英語表記)

なお、証明書の DN の表記は証明書を利用する製品の対応状況を考慮し、PrintableString とする。

３．４　証明書の拡張情報

証明書の拡張情報(Extensions)の利用は任意とする。

４　CRL の記載事項に関するプロファイル

４．１　CRL 形式

CRL の形式は、X.509 とする。X.509 のバージョンは、拡張情報(Extensions)を使用する場合は V2、使用しない場合は V1 とする。（詳細は「５ 関連標準」を参照）

CRL の記載事項に関するプロファイルは RFC2459 に準拠するものとし、記載に際して、特に制約や留意事項がある場合のみ、次節以降に示す。

４．２　CRL の拡張情報

CRL の拡張情報(Extensions)の利用は任意とする。

５　関連標準

５．１　本プロファイルで準拠する標準

- [ITU-T / X.509,1997]
  ISO/IEC 9594-8:1997|ITU-T RECOMMENDATION X.509, INFORMATION TECHNOLOGY. - OPEN SYSTEMS INTERCONNECTION - The Directory: Authentication Framework, ISO/IEC, 1997.

- [IETF / RFC2459]
  RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999.
  http://www.ietf.org/rfc/rfc2459.txt

５．２　本プロファイルに関係する参考標準

- [ITU-T / X.509,2000]
  ISO/IEC 9594-8:2000|ITU-T RECOMMENDATION X.509, INFORMATION TECHNOLOGY. - OPEN SYSTEMS INTERCONNECTION - The Directory: Authentication Framework, ISO/IEC, 2000.

- [IETF / RFC3280]
  RFC 3280, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002.
  http://www.ietf.org/rfc/rfc3280.txt

- [WAP Forum / WAPCert]
  "WAP Certificate and CRL Profiles," WAP-211-WAPCert , WAP Forum.
  http://www1.wapforum.org/tech/documents/WAP-211-WAPCert-20010522-a.pdf

携帯電話加入者証明書プロファイル

MC-01　1.0 版

平成 22 年 7 月　1.0 版第 1 刷発行

発　行　所

社団法人　電　　波　　産　　業　　会
高度無線通信研究委員会モバイルコマース部会
〒100-0013　東京都千代田区霞が関１－４－１
日土地ビル１１階
電　話　03-5510-8594
ＦＡＸ　03-3592-1103