MC-02

モバイル属性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 17 年度活動報告書（平成 18 年 5 月 19 日付）及びモバイル IT フォーラムモバイルコマース部会平成 18 年活動報告書（平成 19 年 5 月 8 日付）に記載されていた「モバイルコマースにおける属性証明書プロファイル」を抜粋、誤記訂正及び再編集した文書である。

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。

モバイル属性証明書プロファイル
目次

1　モバイル属性証明書プロファイルの検討方針

認証 WG では、モバイルコマースにおいて電子認証基盤の統一的なインタフェースをサービス提供者に提示することを目的として、平成 15 年度に電子証明書（PKC）の参考プロファイルを規定した。様々なサービスにおいて電子認証基盤を利用するためには、従来の PKC に加えて、属性に基づく認可技術が重要になると考えられる。したがって、属性証明書（AC）についてもモバイル環境での利用を想定した共通プロファイルを提示することが望ましい。上述の背景を考慮し、以下の方針に基づき属性証明書のプロファイルを規定した。

(1) モバイルサービスの特徴であるローカル環境を意識し、リモート環境のみでなく、ローカル環境で利用が想定される属性を整理する。

(2) AC の所有者については、PKC と AC とのライフサイクルの相違を考慮し、PKC への参照に限定せず、他の識別情報（例えば、エンティティ名）との紐付けを可能とする。

(3) モバイル証明書参考プロファイルとの整合性および、汎用的な利用を想定し、公的個人認証サービスで提供される基本 4 情報（氏名、住所、生年月日、性別）を、属性情報と定義し、AC の基本属性に含める。

2　属性情報として取り扱う情報

属性値は年単位以上の継続性を有する長期属性と 1 年より短い期間の継続性を有する短期属性に分類できる。本文書では、属性証明書に記載する長期属性を、「基本属性」、「連絡属性」、「所属属性」、「特徴属性」、「認証属性」、「決済属性」、「第三者証明属性」といった 7 つのカテゴリに分類し、短期属性を「所有属性」、「履歴属性」の 2 つのカテゴリに分類した。

表 1 において、これら 9 つカテゴリの属性値を、実際に属性値として利用するための OID と表現する形式について定義した。今回の OID の付与の考え方としては、新規に追加したいカテゴリ、もしくは属性値が発生した際には、カテゴリであればそのレベル 7 での最後尾の値、属性値であれば当該カテゴリを検索し、そのカテゴリの中でレベル 8 における最後尾の値を割り振る規則とする。

表 1 各属性値に対する OID とその表現形式

レベル								項目名称	属性表記方針
1	2	3	4	5	6	7	8		
0								ITU-T	表現としては、arib-mc-attribute-xxxx とし、xxxx 部に項目名称の英語表記を記述
	2							ITU-T Administration	
		440						Japan ITU Member	
			200028					ARIB	
				68				ARIB 高度無線通信研究委員会モバイルコマース部会	
					1			属性値	
						1		基本属性	
							1	名前(name)	携帯で表記可能な範囲での全角表記（姓名の区切りには全角スペース） 例：属性　太郎
							2	住所(address)	携帯で表記可能な範囲での全角住所表記（番地の区切りは”－”を利用） 例：東京都属性区青坂１－２－３日本青坂ビル１０Ｆ
							3	生年月日(dateOfBirth)	半角西暦表記(yyyymmdd) 例：20050815
							4	性別(gender)	全角表記（男性、女性、不明）
						2		連絡属性	
							1	携帯電話番号 (cellularNumber)	半角数字表記 例：01234XX7890
							2	携帯メールアドレス (cellularMailAddress)	半角英数字記号表記 例：aaXXa@doXXmo.ne.jp
							3	自宅電話番号(phoneNumber)	半角数字表記 例：0344XX5555
							4	自宅 FAX 番号 (facsimileTelephoneNumber)	半角数字表記 例：036XX67777
							5	自宅メールアドレス (mailAddress)	半角英数字記号表記 例：bbXXb@ccc.moXXra.ne.jp
						3		所属属性	
							1	職種(occupation)	携帯で表記可能な範囲での全角表記 例：会社員、公務員、学生、主婦、自営業、パート・アルバイト、その他
							2	所属組織(organizationName)	携帯で表記可能な範囲での全角表記 例：株式会社属性商事法人営業本部、属性大学大学院理工学研究科
							3	所属組織住所 (organizationAddress)	携帯で表記可能な範囲での全角住所表記（番地の区切りは”－”を利用） 例：東京都属性区青坂１－２－３日本青坂ビル１０Ｆ
							4	所属組織電話番号 (organizationNumber)	半角数字表記 例：0344XX5555

							5	所属組織役職 (organizationTitle)	携帯で表記可能な範囲での 全角表記 例：課長、部長、社長等
							6	所属識別子 （社員番号、会員番号等） (roleIdentification)	半角英数字表記 例：BD73KF82905
							7	サービス提供組織 (serviceProviderName)	携帯で表記可能な範囲での 全角表記 例：ＴＵＴＵＹＡ、ＪＴＡ
							8	サービス提供組織住所 (serviceProviderAddress)	携帯で表記可能な範囲での 全角住所表記（番地の区切りは”－”を利用） 例：東京都属性区青坂１－２－３日本青坂ビル１０Ｆ
							9	サービス提供組織電話番号 (serviceProviderNumber)	半角数字表記 例：0344XX5555
							10	会員役職(role)	携帯で表記可能な範囲での 全角表記 例：シルバー、ゴールド
							11	会員識別子 (memberAccount)	半角英数字表記 例：BD73KF82905
						4		特徴属性	
							1	身長(length)	半角数字表記(0.5 単位の cm) 例：198.5
							2	体重(weight)	半角数字表記(0.5 単位の kg) 例：128.5
							3	スリーサイズ(bwhSize)	半角数字表記(0.5 単位の cm)とし、左から右に BWH、かつ半角カンマ（,）で区切る 例：78.5,55.5,75.5
							4	フットサイズ(footSize)	半角数字表記(0.5 単位の cm) 例：28.5
							5	血液型(bloodtype)	半角英字表記（A、B、AB、O）
							6	既婚・未婚(marriage)	全角表記（既婚、未婚）
							7	子供の有無(children)	全角表記（有、無）
							8	趣味・嗜好(interest)	携帯で表記可能な範囲での 全角表記、複数記載する際には、全角カンマ（,）で区切る 例：映画，読書，テニス
						5		認証属性	
							1	記憶認証情報(password)	半角英数字表記とし、左から右に ID,PW で表記 例：zokusei,rdovipocri
							2	生体認証情報(biometrics)	顔写真情報等 jpg ファイル
						6		決済属性	
							1	クレジットカード番号 (creditCardNumber)	半角表記 例：11112222XXXX4444
							2	クレジットカード有効期限 (creditCardValidity)	半角表記(mmyy) 例：1205
							3	デビッドカード番号 (debitCardNumber)	半角表記（銀行番号＋店番番号＋口座番号） 例：00003331234567

						7		第三者証明属性	
							1	運転免許証 ID (driverLicenseID)	半角表記 例：0123XXXX8901
							2	支払い証明証 (paymentEvidence)	半角表記 例：2,000,000
						8		所有属性	
							1	所有物名称(itemName)	携帯で表記可能な範囲での 全角表記 例：パソコン、キーホルダー
							2	所有物 UID (possessionUniqueIdentifier)	半角英数字表記 例：BD73KF82905
							3	所有物 Type(itemType)	携帯で表記可能な範囲での 全角表記 例：携帯端末、文房具
						9		履歴属性	
							1	GPS 情報(gpsInformation)	半角英数字表記(任意長) ※様々な表現手法があるため、例示なし
							2	ID-Tag 情報 (IDTagInformation)	半角英数字表記 例：BD73KF82905
							3	時刻情報(time)	半角数字 YYYYMMDDHHMMSS.SSSS (24H 表記) 例：20051018103010.3450
							4	利用サービス名称 (serviceName)	携帯で表記可能な範囲での 全角表記 例：ＸＸマート、ＴＳＵＸＸＹＡ
							5	利用サービス UID (serviceUID)	半角英数字表記 例：BD73KF82905

3　モバイルコマースで定義する属性証明書

ここでは、RFC3281 の仕様に基づき、モバイルコマースにおいて利用されるべき属性証明書のフォーマットを定義する。なお、モバイルコマースで選択されるべき表現形式、値については、太字で明記している。

3．1　version

version フィールドは、定められた属性証明書フォーマットがどの Version に準拠するかを示す。RFC3281 の仕様としては、Version2 を使用しなければならないため、本文書においても Version2 と定めることを推奨する。

```
AttCertVersion ::= INTEGER { v2(1) }
```

3．2　holder

holder フィールドは、baseCertificateID、entityName、objectDigestInfo といった識別情報を利用して、この属性証明書がだれの所有物であるのか、特にだれの公開鍵証明書に紐付いているのかを示す。本文書では、属性情報自体に有効期限が存在しない場合や、PKC の有効期限もしくは危殆化に伴う失効といった状況に影響されないようなニーズを考慮して、entityName で holder を表現することを推奨する。これにより、属性が公開鍵証明書に紐付くのではなく利用者に紐付く仕様とし、PKC の有効期限に影響を受けないようする。

```
Holder ::= SEQUENCE {
    baseCertificateID      [0] IssuerSerial OPTIONAL,
    entityName             [1] GeneralNames OPTIONAL,
    objectDigestInfo       [2] ObjectDigestInfo OPTIONAL
}
```

本文書では、公開鍵証明書の Subject に記載する DN(distinguished name)を、entityName とすることを推奨する。なお、携帯電話加入者証明書プロファイルにおいて、DN の共通項目として 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)を定め、その他の項目は任意としている。

3．3　issuer

issuer フィールドは、v1Form、v2Form のどちらかの識別情報を利用して、だれが属性証明書を発行しているかを示す。RFC3281 の仕様としては、v2Form を使用しなければならないため、本文書でも v2Form で表現することを推奨する。

```
AttCertIssuer ::= CHOICE {
    v1Form   GeneralNames,
    v2Form   [0] V2Form
```

}

v2Form では、issuerName、baseCertificateID、objectDigestInfo といった識別情報を利用して、誰が発行した属性証明書であるかを示す。RFC3281 の仕様としては、issuerName を使用しなければならないため、本文書においても issuerName で発行者を表現することを推奨する。

```
V2Form ::= SEQUENCE {
    issuerName            GeneralNames  OPTIONAL,
    baseCertificateID     [0] IssuerSerial  OPTIONAL,
    objectDigestInfo      [1] ObjectDigestInfo  OPTIONAL
}
```

３．４　signature

signature フィールドは、どのような署名アルゴリズムで属性証明書へ署名が付与されているのかを示す。RFC3279 の中で、表 2 のように署名アルゴリズムが定義されている。

表 2 署名アルゴリズムのオブジェクト識別子

アルゴリズム	オブジェクト識別子
md2WithRSAEncryption	iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 2
md5WithRSAEncryption	iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 4
sha1WithRSAEncryption	**iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5**
id-dsa-with-sha1	iso(1) member-body(2) us(840) x9-57 (10040) x9cm(4) 3
ecdsa-with-SHA1	iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) 1

公開鍵証明書の署名アルゴリズム、およびアルゴリズムの強度から、本文書では sha1WithRSAEncryption を利用することを推奨とし、その他のアルゴリズムについてはオプションでサポートすることを考える。しかし、暗号アルゴリズム危殆化動向を踏まえたとき、今回選択したアルゴリズムも現時点のものであり、CRYPTOREC 等外部において得られる暗号アルゴリズム評価の動向に基づいて、その都度判断する必要がある。

３．５　serialNumber

serialNumber フィールドは、その属性認証局で唯一の証明書であることを示す。RFC3281 の仕様としては、非常に短い期間であっても、issuer と serial の組み合わせで唯一であることを示さなければならない。この制限を満たすため、大きい整数（4 オクテット以上 20 オクテット未満）として表現される必要があり、本文書とし

ても、4 オクテット以上 20 オクテット未満を推奨する。

```
CertificateSerialNumber  ::=  INTEGER
```

３．６　validityPeriod

validityPeriod フィールドは、属性証明書発行者が利用者と証明対象の属性の紐付きが有効であることを証明できる期間である。長期属性、短期属性の双方の利用が想定されることから、本文書においては推奨する有効期間を規定しない。また、表記についても規定しない。

```
AttCertValidityPeriod  ::= SEQUENCE {
    notBeforeTime  GeneralizedTime,
    notAfterTime   GeneralizedTime
}
```

３．７　attributes

attributes フィールドは、証明されている属性情報を示す。

```
Attributes ::= SEQUENCE OF Attribute

Attribute ::= SEQUENCE {
  type      AttributeType,
  values    SET OF AttributeValue
}

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY DEFINED BY AttributeType
```

このとき、attributes は、その構成要素の attribute で表現されることとなるが、その表現として、type といったオブジェクト識別子、values といった属性値の集合から構成される。実際には検討の結果作成した属性値と OID の対応表の値を格納することになる。

また利用目的別にて属性の種類を利用するならば、以下のような Attributes フィールドの表現が可能と考える。

```
AttributeType ::= { 各 OID }

AttributeValue ::= IetfAttrSyntax
```

```
IetfAttrSyntax ::= SEQUENCE {
    policyAuthority [0] GeneralNames    OPTIONAL,
    values          SEQUENCE OF CHOICE {
            octets    OCTET STRING,
            oid       OBJECT IDENTIFIER,
            string    UTF8String
          }
}
```

各属性値は、属性単位で OID を定めると共に IetfAttributeSyntax で表現することとし、その属性を同列で格納することとする。具体的には、属性証明書の attributes フィールドに含まれている type と values に対し、type は OID、values は IetfAttributeSyntax で格納される属性値となる。このような OID と IetfAttributeSyntax を用いて表現した例（氏名、所属組織、血液型の三つを含んだ attributes の表現）を以下に示す。

```
0.2.440.200028.68.1.1.1:   ←氏名の OID
SEQUENCE[C] = 1 elements
  SEQUENCE[C] = 1 elements   ←属性値(IetfAttributeSyntax で表記)
    UTF8String = "属性 太郎"

0.2.440.200028.68.1.3.2:    ←所属組織の OID
SEQUENCE[C] = 1 elements
  SEQUENCE[C] = 1 elements          ←属性値
    UTF8String = "株式会社属性認証"

0.2.440.200028.68.1.4.5:    ←血液型の OID
SEQUENCE[C] = 1 elements
  SEQUENCE[C] = 1 elements   ←属性値
    UTF8String = "A"
```

※：上記例においては、policyAuthority を省略している。

上述した仕様を定めた経緯について下記へ示す。

- 日本語表記を考慮した際には、role や group 等といった規定格納形式にも格納可能であるが、「日本語の属性値」を前提にした国内利用を考慮した際には、日本語を利用していることが明確になるように独自 OID を定めると共に、IetfAttributeSyntax で表記することが望ましいと考えた。

- role や group 等といった規定格納形式に納まらない属性値も考慮していることから、独自仕様との混在になることにより利便性が損なわれることを危惧し、すべてを IetfAttributeSyntax で表現することとした。
- IetfAttributeSyntax で表現することにより、属性値の大半は UTF8String で表現される（場合によっては、OCTET STRING、OBJECT IDENTIFIER を利用する）。
- IetfAttributeSyntax が標準仕様であることから、市販の暗号ライブラリによる処理が可能となる場合もある。

以上のことを踏まえて、本文書では、モバイルコマースで利用する属性証明書の属性値の表現として IetfAttributeSyntax を推奨する。

３．８　issuerUniqueIdentifier

issuerUniqueIdentifier フィールドは、発行者を一意に識別する。属性証明書発行者の公開鍵証明書で利用されていないならば、設定してはならないフィールドであり、本文書では規定しない。

```
UniqueIdentifier  ::=  BIT STRING
```

３．９　extensions

extensions フィールドは、属性認証局の運用に関する補足情報を示す。本文書では、属性証明書の有効性検証に利用される拡張情報のみに着目し、表 3 のように Authority Key Identifier、Authority Information Access、CRL Distribution Points の三つを定める。

表 3 Extentions

フィールド名称	利用用途
auditIdentity	規定しない
aCTargeting	規定しない
authorityKeyIdentifier	**AC 署名鍵が複数あった場合にそれを特定するために利用するが、keyIdentifier、authorityCertIssuer、authorityCertSerialNumber といったすべての値を設定する**
authorityInformationAccess	**CA アクセス先の URI を設定する**
cRLDistributionPoints	**CP/SP サーバ（もしくは、検証局）で利用することを想定し、リポジトリの URI を設定する**
noRevocationAvailable	規定しない

３．１０　signatureAlgorithm

signatureAlgorithm フィールドは、どのような署名アルゴリズムで属性証明書へ署名が付与されているのかを示す。RFC3279 の中で、表 x-b に示される署名アルゴリズムが定義されている。

本文書では sha1WithRSAEncryption を利用することを推奨し、その他のアルゴリズムについてはオプションでサポートすることとする。なお、「３．４　signature」と同様に、暗号アルゴリズム評価動向を踏まえてその都度判断する必要がある。

３．１１　signatureValue

属性証明書に対する署名値を示す。署名を付与するのはその属性証明書を発行する属性認証局である。

以上の結果を踏まえて、本文書で推奨する属性証明書の形式として、表 4 のように定める。

表 4 AC プロファイル例

フィールド名称	表記構成	備考
version	v2	
holder	entityName	DN を設定
issuer	c=jp, o=企業名, その他 OU 等は任意	第 2 層までを c=jp, o=企業名とし、第 3 層の ou に AA 名称を入れることを想定
signature	sha1WithRSAEncription	
serialNumber	certificateSerialNumber	
validityPeriod	notBeforeTime notAfterTime	GeneralizedTime 表記、あるいは UTCTime 表記を想定
attributes	type values	type と values の組みが複数格納されることとし、type はオブジェクト識別子、values は IetfAttrSyntax で表現
issuerUnique Identifier	－	規定しない
extensions	authorityKeyIdentifier authorityInformationAccess cRLDistributionPoints	AKI は属性認証局 key のハッシュ値、issuerDN、シリアル番号の三つ、AIA は CA アクセス先の URI、CRLDP は CRL エントリの URI を設定
signatureAlgorithm	sha1WithRSAEncription	
signatureValue	署名値を格納	

４　モバイルコマースで定義する属性証明書失効リスト

ここでは、モバイルコマースにおいて利用されるべき属性証明書失効リストのフォーマットを定義する。なお、モバイルコマースで選択されるべき表現形式、値については、太字で明記している。

４．１　version

version フィールドは、定められた属性証明書失効リストフォーマットがどの Version に準拠するかを示す。本文書においては version2 を推奨する。

```
Version ::= INTEGER { v2(1) }
```

４．２　signature

signature フィールドは、どのような署名アルゴリズムで属性証明書失効リストへ署名が付与されているのかを示す。RFC3279 の中では、表 x-b に示される署名アルゴリズムが定義されている。

本文書では属性証明書と同様に sha1WithRSAEncryption を利用することを推奨し、その他のアルゴリズムについてはオプションでサポートすることとする。なお、暗号アルゴリズム評価動向を踏まえてその都度判断する必要がある。

４．３　issuer

issuer フィールドは、この属性証明書失効リストの発行者名称を示す。発行者名称を表記するフォーマットは Name 型で表される。

```
Name ::= CHOICE {
    RDNSequence }

RDNSequence ::= SEQUENCE OF RelativeDistinguishedName
```

４．４　thisUpdate

属性証明書失効リストが発行された日時を示す。RFC3280 において、2049 年までの日付に対しては UTCTime 表記、2050 年以降の日付に対しては GenralizedTime 表記として符号化されるように規定されているため、本文書においても同様に定める。

```
thisUpdate ::= Time
```

４．５　nextUpdate

属性証明書失効リストが、遅くとも次回に発行される日時を示す。本文書においては、thisUpdate と同じく、2049 年までの日付に対しては UTCTime 標記、2050 年以降の日付に対しては GenralizedTime 表記として符号化されるように定める。

```
nextUpdate ::= Time OPTIONAL
```

４．６　revokedCertificates

失効した属性証明書のリストの一覧を示す。userCertificate、revocationDate の項目にそれぞれ属性証明書のシリアル番号、失効日時が記載される。本文書においては、crlEntryExtention を規定しないが、表 5 に各フィールドで想定される設定内容を示す。

表 5　revokedCertificates

フィールド名称		利用用途
userCertificate		**失効対象を示すために属性証明書のシリアル番号を設定する。**
revocationDate		**属性認証局で失効された日付を示す。**
crlEntryExtensions	cRLReason	失効の理由を示すが、CRL において利用状況が異なるので、任意とする。利用する際には、表 x-g に記載したコードが想定される。
	holdInstructionCode	保留状態になったことを示す。
	invalidityDate	失効を要する状態になったことが判明した時間を示す。
	certificateIssuer	間接 CRL に関連付けられた発行者名称である。

表 6　reasonCode

Unspecified	指定なしを示す。
keyCompromise	属性証明書利用者の秘密鍵が漏洩したことを示す。
cACompromise	CA において信頼性が失われる事象が生じたことを示す。
affiliationChanged	**属性証明書の記載内容が変更したことを示す。**
Superseded	属性証明書が破棄されたことを示す。
cessationOfOperation	**属性証明書の必要性がなくなったことを示す。**
certificateHold	属性証明書の利用を一時停止することを示す。
removeFromCRL	一時停止等が解除されたことを示す。
privilegeWithdrawn	**属性証明書の特権が剥奪されたことを示す。**
aACompromise	**AA において信頼性が失われる事象が生じたことを示す。**

４．７　crlExtensions

crlExtensions フィールドは、属性証明書失効リストに関する補足情報を示す。本文書では、属性証明書の有効性検証に利用される拡張情報に着目し、表 7 のように authorityKeyIdentifier と cRLNumber、issuingDistributionPoint を定める。

表 7　crlExtensions

フィールド名称	利用用途
authorityKeyIdentifier	**ACRL 署名鍵が複数あった場合にそれを特定するため、keyIdentifier、authorityCertIssuer、authorityCertSerialNumber といったすべての値を設定する**
issuerAltName	規定しない
cRLNumber	**発行される ACRL に対して、単調増加する連続の番号を設定する**
deltaCRLIndicator	規定しない
issuingDistributionPoint	**ACRL が発行される場所を示すため、distributionPoint、onlyConstrainsAttributeCertificate を設定する。**

４．８　signatureAlgorithm

signatureAlgorithm フィールドは、どのような署名アルゴリズムで属性証明書失効リストへ署名が付与されているのかを示す。RFC3279 の中で、表 x-b に示される署名アルゴリズムが定義されている。

本文書では属性証明書と同様に sha1WithRSAEncryption を利用することを推奨し、その他のアルゴリズムについてはオプションでサポートすることとする。なお、暗号アルゴリズム評価動向を踏まえてその都度判断する必要がある。

４．９　signatureValue

属性証明書失効リストに対する署名値を示す。署名を付与するのはその属性証明書失効リストを発行する属性認証局である。

以上の結果を踏まえて、本文書で推奨する属性証明書失効リストの形式として、表 8 のように定める。

表 8　ACRL プロファイル例

フィールド名称			表記構成	備考
Version			v2	RFC2459 に準拠
Signature			sha1WithRSAEncription	
Issuer			c=jp, o=オペレータ社名、その他 OU 等は任意	PrintableString
thisUpdate			UTCTime 表記／GeneralizedTime 表記	RFC3280 に準拠
nextUpdate			UTCTime 表記／GeneralizedTime 表記	RFC3280 に準拠
revoked Certificates	userCertificate		整数（属性証明書のシリアル番号）	RFC2459 に準拠
	revocationDate		UTCTime 表記／GeneralizedTime 表記	RFC3280 に準拠
	crlEntryExtensions	cRLReason	任意	規定しない
		holdInstructionCode	－	規定しない
		invalidityDate	－	規定しない
		certificateIssuer	－	規定しない
crl Extensions	authorityKeyIdentifier		keyIdentifier を設定	RFC2459 に準拠
	issuerAltName		－	規定しない
	cRLNumber		整数	
	deltaCRLIndicator		－	規定しない
	issuingDistributionPoint		distributionPoint と onlyConstrainsAttributeCertificate を設定	RFC3280 に準拠
signatureAlgorithm			sha1WithRSAEncription	
signatureValue			署名値を格納	

モバイル属性証明書プロファイル

MC-02　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