研究速報

モバイルサービス向け認証基盤の検討

梅澤　克之[†]　坂崎　尚生[†]
佐藤　一夫[††]　松木　彰[††]
曽我　健二[†††]　片山　透[†††]
清本　晋作[††††]（正員）　田中　俊昭[††††]（正員）

Design of an Authentication Infrastructure for Mobile Services

Katsuyuki UMEZAWA[†], Hisao SAKAZAKI[†], Kazuo SATOU[††], Akira MATSUKI[††], Kenji SOGA[†††], Toru KATAYAMA[†††], *Nonmembers*, Shinsaku KIYOMOTO[††††], and Toshiaki TANAKA[††††], *Members*

[†]（株）日立製作所 システム開発研究所，川崎市
Hitachi, Ltd., Kawasaki-shi, 212–8567 Japan
[††]（株）NTT DoCoMo，東京都
NTT DoCoMo, Inc., Tokyo, 100–6150 Japan
[†††]日本電気株式会社，東京都
NEC Corporation, Tokyo, 108–8557 Japan
[††††]（株）KDDI 研究所，ふじみ野市
KDDI R&D Laboratories, Fujimino-shi, 356–8502 Japan

あらまし　モバイル環境において安心してサービスを提供・享受するために，特定の事業者に依存しない統一的な認証基盤が必要である．本論文では，モバイル ID を含む公開鍵証明書（以降 PKC）とそれに対応づけた属性証明書（AC）のモバイル環境における発行・利用・検証方式に関する提案を行う．

キーワード　公開鍵証明書，属性証明書，有効性確認，VA，CVS

1. まえがき

近年，モバイルキャリヤ網内に閉じたサービスにとどまらず，インターネットを利用したモバイルサービスが増加し，インターネット上の脅威がそのままモバイル環境にも当てはまるようになっている．したがって，安全なユーザ（端末）認証及び安全なサーバ認証が必須である．また，サービスの多様化に伴い，ユーザ自身のみならず，ユーザのもつ属性の認証も必要となっている．本論文では，モバイル ID を含む公開鍵証明書とそれに対応づけた属性証明書のモバイル環境における発行・利用・検証方式に関する提案を行う．

2. 課　題

属性証明書（以降 AC）は公開鍵証明書（以降 PKC）とセットで用いられるが，モバイル環境の場合，機種変更が頻繁に行われる等の理由で，AC に比べ，PKC の寿命の方が短い場合がある．こうしたライフサイクルの違いを吸収した PKC と AC の対応付け方法を検討する必要がある．また，モバイル環境においてはネットワークを経由したリモートサービスのみならず，店頭で実際に携帯電話端末をかざして利用するようなローカルサービスも存在する．したがって，それぞれのサービス形態に適した利用方法を検討する必要がある．更に，PKC 及び AC について統一したフォーマットを規定することで，事業者間での相互利用を可能にするとともにその際の検証処理に要する負荷を軽減する方式を検討しなければならない．本論文では，以上の課題を解決する認証基盤について検討を行う．

3. 認証基盤の提案

本章では，モバイル向け AC プロファイルの規定，PKC と AC の対応付け方法，PKC 及び AC の利用方式，並びに PKC 及び AC の検証方式についての提案を行う．

3.1 モバイルサービス向け AC プロファイルの規定

本節では，モバイルサービス向けの AC のプロファイルについて検討した結果を述べる．プロファイルの検討においては，まず既存及び将来想定されるモバイルサービスについて調査を行った上で，各事業者間で相互利用可能なプロファイルを設計した．具体的には，リモートサービスあるいはローカルサービスを考慮した上で，サービス向上が判断できる属性という観点で，モバイル環境向けの属性を網羅的に抽出した．そして，抽出した属性を各事業者が利用しやすいようにカテゴリー分けを行った上で，AC プロファイルとして規定した．規定した AC プロファイルを付録に示す．なお，PKC については，モバイルサービス向けに規定された mITF プロファイル [4] に従って設計した．

3.2 PKC と AC の対応付け手法

AC は PKC と対応づけて利用される．しかし，属性は，短期間で変化する属性から永続的な属性まで多種多様であり，PKC の有効期間と AC の有効期間は必ずしも一致しない．そのため，利用者の利便性を考慮した場合，PKC が更新されても AC の更新処理が行わなくてもよいような設計が必要である．現在，通信事業者が使用している mITF プロファイル [4] 準拠の PKC は過去の発行枚数を把握する等の理由により，PKC の Subject フィールド内に，カウンタとしての役割をもつ “Title” の値が「T = n」という形式で記述されている．そこで，AC の holder フィールドを entityName で表現し，その場合に PKC の Subject フィールドの Title を省略して記述することにより PKC と AC を紐づけることとした．なお，AC や PKC の検索の際

には，PKC の DN から Title 部分を削除して検索を実施することで，AC については Title の値に影響されずに取得でき，PKC については，サーバ側が Title の値が一番大きい最新の PKC を返すようにすることで，取得できる．また，AC の検証の際にも，PKC と AC の DN から「T = n」を削除することで，PKC と AC の紐付けが可能となる．

3.3 モバイルサービスを想定した PKC 及び AC の利用方式

PKC に紐づいた AC の利用形態として，AC を携帯電話端末の内部に保持し，利用時には携帯電話端末から AC を提示する Push 型と，AC は携帯電話端末の外部（例えば AA のリポジトリ）に保管し，CP/SP がリポジトリから取得する Pull 型が考えられる．Push 型と Pull 型のシステム概要を図 1 に示す．Push 型では，【1】，[2]，[3]，【4】，【7】，【8】，Pull 型では，【1】，(2)，(3)，【4】，(5)，(6)，【7】，【8】の処理を行った後，携帯電話端末は AC を利用したサービスを受けることができる．

Pull 型モデルの場合には，Push 型に比べて，リポジトリからの AC の取得（図 1 の (5) (6) の処理）を含むため，その際には表 1 に示したセキュリティ機能が必要である．

3.4 PKC 及び AC の検証方式

PKC 及び AC の検証方式として，検証処理負荷の低減を目的として，検証サーバを導入した．以下，図 1 の検証サーバ（VA，AVA）について記述する．PKC 検証サーバ [2], [3] を拡張し，モバイル環境に適した PKC 及び AC の検証サーバ（VA，AVA）の開発を行った．AC を検証する場合，通信事業者は CRL（Certificate Revocation List）や ACRL（Attribute CRL）を公開する必要がある．しかし，通信事業者の CRL や ACRL を無条件に公開すると解約者の絶対数や増加率などの積極的には公開したくない情報も公開することになってしまうため，CRL や ACRL を適切に取り扱う必要がある．本研究では，証明書検証サーバへ他の通信事業者が発行した AC の検証が要求された場合，適切な AC 検証サーバへ検証要求を転送し検証結果のみを受け，それを検証要求者に返信することで CRL や ACRL を公開しない方式を実現した．

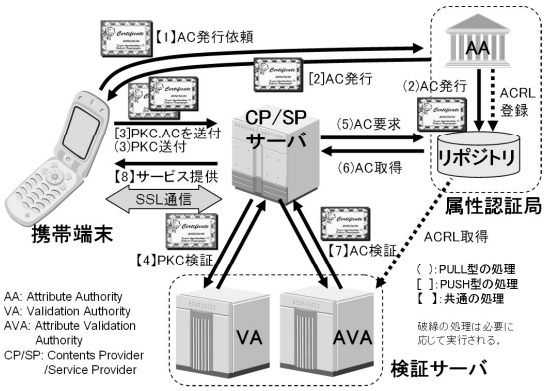

図 1 AC 利用モデルの概要
Fig. 1 Outline of an AC use model.

提案方式の PKC 及び AC の検証時間の性能測定結果を表 2 に「提案方式」として示す．具体的には，証明書検証サーバが検証要求を受け取り，PKC と AC の二つの証明書の検証処理が終了するまでの時間を計測した．更に，比較のために検証サーバを用いず携帯電話端末が自ら検証を行う場合の性能測定結果を表 2 に「携帯電話方式」として示す．この結果は，携帯電話端末として CDMA 1x WIN 規格の BREW 端末を用いたときの計測値である．なお，表 2 の数値は 100

表 1 リポジトリに要求されるセキュリティ機能
Table 1 Security functions for AC repository.

機能	説明
不正アクセス防止機能	承認された CP/SP サーバだけが利用できるようにする必要がある．
利用者の承認に基づいて限定された AC 参照（取得）機能	利用者が望まない属性情報までが参照されないようにする必要がある．
属性情報取扱い事業者としての運用の正当性証明機能	アクセスログ，操作ログ等，利用者に対して操作の正当性証明を提供できる必要がある．
AA-CP/SP 間のセキュア通信路	AA，CP/SP 間で相互認証を行うとともに，セション鍵を用いて，通信の暗号化を行う必要がある．

表 2 PKC，AC 検証時間の測定結果
Table 2 Transaction time for PKC and AC verification.

処理内容	処理時間 [ms]	
	提案方式	携帯電話方式
①AA の PKC 取得時間	16	471
②ACRL の取得時間	27	459
③PKC の検証時間	113	1404
④AC 検証時間（上記を含むサーバでの処理時間）	290	-
⑤AC 検証時間（携帯電話端末からの要求時間を含む）	1931	$> 2334^{(*1)}$

(*1): 筆者らは，携帯電話端末に AC 検証処理を実装していないため実測は不可能であるが，本値には①，②，③の処理時間に加えて携帯電話端末内での AC の有効性検証等の処理時間を含むので 2334 [ms] より大となる．

回の計測値の平均値である．

このように，携帯電話端末が自ら AC の検証を行う方式より提案方式の方がより効率的に AC の検証が行えることが分かる．

4. むすび

本論文では，PKC とそれに対応づけた AC のモバイル環境における発行・利用・検証方式に関する提案を行った．具体的にはモバイル向け AC のプロファイルの提案，AC の利用モデルと課題の抽出，AC の検証方式の提案を行った．今後，実環境において実証実験を行い，提案した認証基盤の有用性を検証する予定である．

謝辞 本研究は，独立行政法人情報通信研究機構（NICT）の委託研究「モバイルセキュリティ基盤技術の研究開発」の一環として行われた．

文　献

[1] ITU-T Recommendation X.509 (2000) ISO/IEC 9594-8:2001: Information Technology — Open Systems Interconnection — The Directory: Public-key and Attribute Certificate Framework.

[2] 政府認証基盤相互運用性仕様書，H15/12/17 改定，共通システム専門部会了承．

[3] 藤城孝宏，鍛　忠司，羽根慎吾，熊谷洋子，手塚　悟，“証明書検証サービスの開発，”信学論（D-I），vol.J87-D-I, no.8, pp.833–840, Aug. 2004.

[4] “mITF モバイルコマース部会 平成 14 年度活動報告書，”mITF, 2002.

付　録

モバイル向け AC プロファイル

表 A·1 に AC プロファイルを記述する．

表 A·1　AC プロファイル（属性情報部分の抜粋）
Table A·1　Attribute information in AC profile.

レベル 1	2	3	4	5	6	7	8	項目名称	属性表記方針
0								ITU-T（仮）	表現としては，nict-mobile-attribute-xxxx とし，xxxx 部に項目名称の英語表記を記述
	2							ITU-T Administration（仮）	
		440						Japan ITU Member（仮）	
			200168					独立行政法人 情報通信研究機構（仮）	
				99				○○部門（仮）	
					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：属性口太郎
							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，その他等
							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等
							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，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，等
							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，ゴールド等
							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，テニス等
						5		認証属性	
							1	記憶認証情報（password）	半角数字表記とし，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		所属属性（Owner）	
							1	所有物名称（item name）	携帯で表記可能な範囲での全角表記 例：パソコン，キーホルダー等
							2	所有物 UID（possession unique identifier）	半角英数字表記 例：BD73KF82905
							3	所有物 Type（item type）	携帯で表記可能な範囲での全角表記 例：携帯端末，文房具等
						9		履歴属性（Personal Records）	
							1	GPS 情報（GPS information）	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（ID-Tag information）	半角英数字表記 例：BD73KF82905
							3	時刻情報（time）	半角英数字，YYYYMMDDHHMMSS.SSSS（24 H 表記）例：20051018103010.3450
							4	利用サービス名称（service name）	携帯で表記可能な範囲での全角表記 例：XX マート，TSUXXYA 等
							5	利用サービス UID（service UID）	半角英数字表記 例：BD73KF82905

（平成 18 年 8 月 3 日受付，9 月 29 日再受付）