社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2003－ＣＳＥＣ－22　(28)
2003／7／18

モバイルコマースにおけるＰＫＩの現状と課題
－mITF モバイルコマース部会　認証ＷＧの活動状況－

田中 俊昭† 関野 公彦‡ 菊地 仁†‡ 梅澤 克之‡‡

†ＫＤＤＩ研究所（株） 〒359-1132 埼玉県上福岡市大原 2-1-15
‡（株）ＮＴＴドコモ 〒239-8536 横須賀市光の丘 3-5
†‡Ｊ－フォン（株） 〒105-6205 東京都港区愛宕 2-5-1
‡‡（株）日立製作所システム開発研究所 〒244-0817 横浜市戸塚区吉田町 292 番地

E-mail: †toshi@kddilabs. jp, ‡sekino@nttdocomo.co.jp, †‡hitoshi.kikuchi@j-phone.com, ‡‡ume@sdl.hitachi.co.jp

あらまし 携帯端末を用いた決済サービス（モバイルコマース）の普及促進を目的として，利便性・安全性の高いサービスの実現が必要となる．この要求を満たすセキュリティ基盤技術として，公開鍵基盤（ＰＫＩ：Public Key Infrastructure）が一つの有力な候補と考えられており，その利用が期待される．しかしながら，ＰＫＩに基づくモバイルコマースを実現するためには，モバイル特有の利用環境や具体的なサービスを想定し，その課題の明確化・検討を通じて，ＰＫＩ技術の利用可能性を検証する必要がある．従って，本稿では，mITF モバイルコマース部会・認証ＷＧで検討を行っているＰＫＩに基づくモバイルコマースを実現する際の課題および，そられの課題に対する検討状況について報告する．

キーワード PKI，モバイルコマース，認証，ドメイン間認証，電子証明書，属性証明書

Current Topics on PKI Technologies for Mobile Commerce
－Activities on Authentication WG, MC Committee, mITF－

Toshiaki TANAKA† Kimihiko SEKINO‡ Hitoshi KIKUCHI†‡ and Katsuyuki UMEZAWA‡‡

†KDDI R & D Labs. Inc. 2-1-15 Ohara, Kamifukuoka-shi, Saitama, 356-8502 Japan
‡NTT DoCoMo, Inc. 3-5 Hikarino-oka, Yokosuka-shi, Kanagawa, 239-8536 Japan
†‡J-PHONE Co., Ltd. 2-5-1 Atago, Minato-ku, Tokyo, 105-6205 Japan
‡‡Hitachi, Ltd., Systems Development Laboratory, 292, Yoshida-cho, Totsuka-ku, Yokohama-shi, Kanagawa, 244-0817 Japan

E-mail: †toshi@kddilabs. jp, ‡sekino@nttdocomo.co.jp, †‡hitoshi.kikuchi@j-phone.com, ‡‡ume@sdl.hitachi.co.jp

Abstract Aiming at the penetration mobile commerce into mass market, its services are to be secure and usable. Pubic Key Infrastructure (PKI) is considered as one of the promising technology for the provision of such secure mobile services. Therefore, its deployment is highly expected. For the purpose to realize mobile commerce based on PKI, however, it is further necessary to verify its applicability from the viewpoint of mobile environments and real payment models. Accordingly, this paper clarifies and discusses the issues when applying PKI to mobile commerce, those are mainly from the result of the study on Authentication WG, MC Committee of mITF.

Keyword PKI, Mobile Commerce, Authentication, Inter-Domain Authentication, Digital Certificate, Attribute Certificate

1. はじめに

公開鍵基盤（ＰＫＩ）を認証技術として用いた電子政府の実現にともない，これまでのＰＫＩの様々な技術検討が実サービスとして結実し，その技術の可能性が立証されつつある．一方，携帯電話の普及に伴い，モバイルインターネットサービスが普及し，着信メロ

ディの有料配信サービスのような携帯電話を用いた決済サービス（モバイルコマース）が立ち上り始めている．このような背景を踏まえ，より安全で信頼性の高いモバイルコマースの実現と，オープンな標準技術によるモバイルコマースの普及促進を目的として，ＰＫＩ技術のモバイルコマースへの適用が注目されている．

ＰＫＩは，その技術標準の核となる X.509[2] が ITU-T/JTC1 で，また，様々な拡張検討が IETF の PKIX-WG で検討されており，現在，ドラフトも含めて膨大な技術仕様ができあがっている．これまで，この技術仕様について机上調査あるいは，各種ベンダー製品の相互接続実験に基づいた検討を行うなどの試みがあるが，モバイルコマースという一つのサービスに着目し，その適用性について検討を行った例はなく，ＰＫＩに基づくモバイルコマースの実現性について，課題とその解決法を明確にすることが，モバイルコマースをさらに発展させ，かつ，ＰＫＩ技術の利用促進に大きく寄与すると考えられる．

これらの点を考慮し，非営利団体であるモバイルＩＴフォーラムＭＣ部会の認証ＷＧでは，平成１３年度から，上記に述べたＰＫＩのモバイルコマースへの適用を目的とした技術検討を進めている．本稿では，モバイルコマース部会・認証ＷＧでの１４年度の検討結果であるＰＫＩ技術の現状，ＰＫＩをモバイルコマースへ適用する際の課題とその検討状況について報告する．

2. モバイルＩＴフォーラムＭＣ部会

モバイルＩＴフォーラムは，第４世代移動通信システムやモバイルコマース等の新世代モバイルの早期実現を図るため，新世代モバイルに関する研究開発及び標準化の調査研究，関係機関との連絡調整，情報の収集を目的とした非営利団体であり，その中でも，モバイルコマース部会（MC 部会）は，インターネットにおける標準技術をベースとして携帯電話，モバイル網を対象に，モバイルコマースを実現するためのビジネスおよび技術の側面からの検討を行う作業部会である．ＭＣ部会の構成を図１に示す．ここで，推進専門委員会では，利用者の視点に重点をおいてビジネスモデルの検討を，技術専門委員会では，リファレンスモデルの策定，セキュリティ等の要件の定義づけ，インターフェース仕様の体系化を行っている．技術専門委員会はさらに，リファレンスモデル（RM）ＷＧ，決済ＷＧ，認証ＷＧから構成され，特に認証ＷＧでは，上記に述べたＰＫＩのモバイルコマースへの適用を目的とした認証技術の検討がなされている．認証 WG では，これまで，利用者が遠隔に存在するサービス提供者からサービスをうける”リモート環境”での認証方式を中心に検討を進めている．

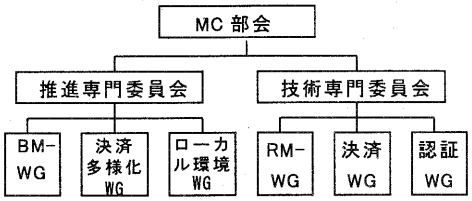

図１　MC 部会の組織構成図（H. １４年度）

3. モバイルコマースのＰＫＩ利用における課題

ＰＫＩ技術は，様々な観点から検討がなされているが，その利用面においても，検討すべき点が多々ある．さらに，モバイル環境では，有線系のサービスと比較して考慮すべき制約もある．認証ＷＧでは，これらの課題を抽出するとともに，ＰＫＩ技術仕様に基づき検討を行っている．本節では，まず，モバイルコマースでのＰＫＩ利用を想定した際に検討すべき課題についてまとめる．

・モバイルコマースの信頼モデル

モバイルコマースは，利用者に加えて，コンテンツ提供者・サービス提供者（CP/SP），決済機関，モバイルオペレータ（通信事業者）など様々なエンティティが連携し実現される．モバイルコマースは，オンラインクレジット，デビット，プリペイド，チケットなどその利用形態は多岐にわたっており，それぞれの利用形態によって，認証の対象（すなわち到達点）や認証者が異なる．従って，各エンティティを電子証明書に基づき認証する際には，誰が何の目的で認証するのかという前提を明確にしておくことが最も重要である．さらに，これらのエンティティは，どのような信頼ドメインを形成するのか，また，マルチドメイン環境の場合，ドメイン間認証とはどうあるべきなどか等の検討を行う必要がある．

・モバイルコマースにおけるインターフェース共通化

モバイルコマース普及促進のためには，その基盤技術に関わる各種インターフェースを可能な限り共通化し，モバイルコマースをオープンかつ，コスト効率の高いサービスとする必要がある．

・携帯電話，モバイル網の制約

現行の携帯電話はパソコンと比較して，計算能力や，メモリ量に，また，モバイル網は有線網と比較して通信速度の面で制約がある．これらの使用環境を考慮し，ＰＫＩ技術を利用しなければならない．

3.1. オンラインクレジット決済モデル

本節では，有望な決済方式の中の一つであるオンラインクレジット決済モデルを例にとり，前述の決済WGで規定した以下の３つのモデルを対象として，PKI利用に対する先の課題について検討する．

データ入力型モデル：本モデルは，利用者，利用者が使用する携帯端末，オペレータネットワーク，オペレータネットワークがインターネットと接続するためのオペレータゲートウェイ，CP/SPなどの加盟店，加盟店が接続されるインターネット，決済ゲートウェイ，決済機関でCP/SPなどの加盟店を扱うアクワイアラ，利用者がカード契約するイシュア，および，決済機関専用の決済ネットワークから構成される（図２参照）．ここで，本モデルでは，利用者がカード情報と取引情報を携帯端末に直接入力することにより，そのデータがCP/SPを介して決済機関に送信され決済処理が行われるモデルで，現行すでにサービスが存在する．

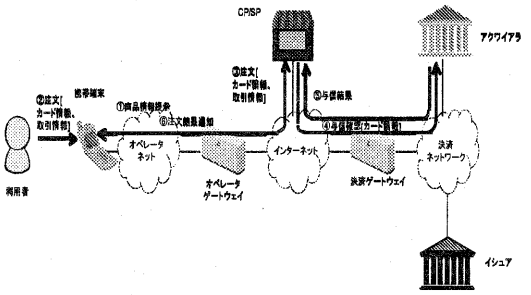

図２ データ入力型モデル

端末格納型モデル：本モデルは，データ入力型モデルの構成に加えて，携帯端末に外部からの不正なアクセスに対して耐タンパー性を有するセキュアエレメントが具備された構成をなし，セキュアエレメント内に利用者情報や，カード情報を安全に管理し，決済時には，そのセキュアエレメントの保管された利用者情報やカード情報がネットワークを介して，CP/SPや決済機関に提示するモデルである．

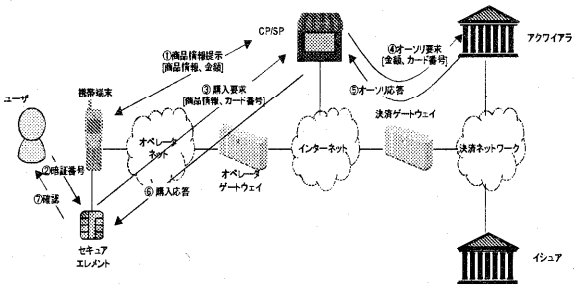

図３ 端末格納型モデル

サーバ管理型モデル：本モデルは，データ入力型モデルの構成に加えて，インターネット上に，利用者情報やカード情報を管理するウォレットサーバが存在する形態であり，携帯端末からの購入要求を上記ウォレットサーバが受け取り，利用者になりかわり，その利用者のカード情報や，利用者情報をCP/SPに提示するモデルである．

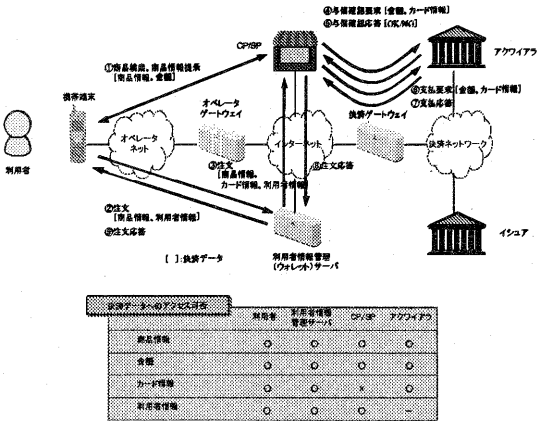

図４ サーバ管理型モデル

3.2. モバイルコマースにおける認証

認証WGでは上記3.1にて整理したオンラインクレジット決済モデルについて，現実のモバイルコマースサービスやシステムにPKIを適用する前提でモバイルコマース固有の認証要件の洗い出しを行った．

3.2.1. データ入力型モデル

本モデルは携帯端末とアクワイアラの間にCP/SPが仲介し，信頼を委譲する構成をなしている．従って認証要件は，携帯端末とCP/SP間，およびCP/SPとアクワイアラ間に分離される．

＜携帯端末とCP/SP間＞
- CP/SPによる携帯端末認証
- 携帯端末によるCP/SP認証と真正性確認

＜CP/SPとアクワイアラ間＞
- アクワイアラによるCP/SP認証と真正性確認
- CP/SPによるアクワイアラ認証と真正性確認

この認証要件に基づきPKIで必要となる証明書は下記のようになる．

- 携帯端末のクライアント証明書
- 携帯端末の署名用証明書

・CP/SP のサーバ証明書
・CP/SP の署名用証明書
・アクワイアラの署名用証明書

商用 SSL サーバ証明書を使用する現状のモバイルコマースサービスでは，すでに CP/SP の認証ドメインが存在するが，データ入力型モデルではこれに加え携帯端末の認証ドメイン，アクワイアラドメインが必要となる．なお，このモデルではオペレータドメインと CP/SP ドメインのセキュリティポリシーがともにモバイルコマースを実施する事業主体間で許容する認証レベルであれば，オペレータドメインと CP/SP ドメインを一体化することも可能となる．

この場合ビジネスモデルに関連が深い認証ポリシーの統一化の実現性が課題となるであろう．

3.2.2. サーバ管理型モデル

本モデルはウォレットサーバ（ウォレット）が利用者と CP/SP の間の認証及び利用者と決済機関の間の認証を仲介する．この場合の認証要件は携帯端末とウォレット間の認証と，ウォレット～CP/SP～決済機関の間の認証に分解できる．

＜携帯端末とウォレット間＞
・携帯端末による CP/SP 認証と真正性確認
・携帯端末によるウォレット認証と真正性確認
・ウォレットによる携帯端末認証
・ウォレットによる携帯端末認証と真正性確認

＜ウォレット，CP/SP，決済機関＞
・ウォレットによる CP/SP 認証と真正性確認
・ウォレットによるイシュア認証
・CP/SP によるウォレット認証と真正性確認
・イシュアによるウォレット認証
・イシュアによる CP/SP の真正性確認

これらを実現するには，PKI において下記が必要となる．

・携帯端末のクライアント証明書
・携帯端末の署名用証明書
・ウォレットのサーバ証明書
・ウォレットの署名用証明書
・CP/SP のサーバ証明書
・CP/SP の署名用証明書
・決済機関の署名用証明書

このモデルでは，SET の例に見られるようにウォレットと CP/SP，ウォレットと決済機関間の真性性確認において二重署名や暗号化が必要となる．

また，認証ドメインとしてオペレータ，ウォレット，CP/SP，決済機関の 4 ドメインが存在するが，ドメイン間認証のためのポリシーマッピングにおいて各ドメインの認証ポリシーの整合をとっていくことが必要となる．

3.2.3. 端末格納型モデル

端末格納型モデルでは，セキュアエレメントを用いるユーザと決済機関の間を CP/SP が仲介する形態となっているが，ユーザと決済機関でのエンドトゥエンドの認証を実現するため電子署名を用いることを前提としている．また，ユーザと CP/SP 間においても事後のデータの検証が可能となるよう電子署名によるデータ検証を前提とした．この場合の認証要件は以下のように単純化される．

・ユーザによる CP/SP の認証と真正性確認
・ユーザによる決済機関の真正性検証
・CP/SP によるユーザの認証と真正性確認
・決済機関によるユーザの認証
・決済機関による決済データの真正性確認

これらを実現するために必要となる電子証明書は下記のようになる．

・ユーザのクライアント証明書
・ユーザの署名用証明書
・CP/SP のサーバ証明書
・CP/SP の署名用証明書
・決済機関のサーバ証明書
・決済機関の署名用証明書

なお，上記ドメイン間認証を整理するうえで，セキュアエレメントの発行主体がポイントとなる．この想定としては下記が考えられる．

1. オペレータがセキュアエレメントを発行
2. 決済機関がセキュアエレメントを発行
3. CP/SP がセキュアエレメントを発行

この場合，商品購入内容などの確認を携帯電話利用者と CP/SP 間で行うことから，オペレータドメインと CP/SP ドメインのドメイン間認証が必須となる．

また，決済そのものはセキュアエレメントが決済機関に対し行うものであるため，セキュアエレメントがオペレータドメインに属する場合のみオペレータドメインと決済機関ドメインのドメイン間認証が必要となり，それ以外の場合においては CP/SP ドメインと決済

機関ドメインのドメイン間認証が必要となる．

いずれにおいても各エンティティの認証ポリシーの整合性を取る必要があるため，3.3.1で後述するドメイン間認証技術を適用する際には，必要となるドメイン間のポリシーの整合性がとりやすいよう各ドメインの運用を取り決める必要がある．

3.3. モバイルコマースにおけるＰＫＩ信頼モデル

3.3.1. ドメイン間認証技術の分類

上記3.2で例示したオンラインクレジット決済モデルにおいて複数のドメインが存在する場合，ドメイン間認証（Inter-Domain Authentication）が必要となる．PKIを用いたドメイン間認証方式としては下記3方式が挙げられる．

- 相互認証（Cross Certification）方式[1]

認証局間で相互証明書を発行する方式

- 第三者方式[1]

両認証局が信頼のおける第三者機関を設定し，各ドメインのエンドエンティティ間において認証を行う際，この第三者機関へ検証を依頼することにより相手エンティティの認証を確立する方式

- 独立方式

証明書の検証者が複数の信頼する認証ドメインの認証局証明書を保有する方式

各方式のドメイン間認証における基本要件，技術要件，運用要件への対応を表1にまとめる．

表1 PKIを利用したドメイン間認証の方式比較

分類	要件	相互認証方式	第三者方式	独立方式
基本要件	ポリシーの合意形成	ドメイン間認証する両ドメインが合意の上，相互証明書を発行	ドメイン間認証する両ドメインが合意の上，TTPに対し相互認証を登録	検証者が認証局証明書取得時に独自に判断
	ドメイン間認証の考え方	検証者が属するドメインの認証局のみを信頼	検証者が属するドメインの認証局，及びTTPを信頼	信頼する全てのドメインの認証局を信頼
技術要件	ポリシー通知（制御）技術	証明書拡張の確認による	TTPにおいて制御	無し
	パス構築，検証	相互証明書を取得，自ドメイン認証局へパス構築	TTPへパス構築を依頼	無し
	大規模ドメイン間認証	メッシュ形接続，またはブリッジCA利用	TTP間の連携	認証者の判断
運用要件	新規ドメイン間認証先ドメインの追加	認証局管理者により，相互証明書を発行	認証局管理者がTTPへ登録	認証者が新ドメイン認証局証明書を取得
	新規ドメイン間認証先ドメインの無効化（通知）	認証局管理者が相互証明書を失効	認証局管理者がTTPへ無効であることを登録	認証者が認証局証明書を削除

3.3.2. ドメイン間認証技術の適用

上記技術の分類に基づき認証WGではオンラインクレジット決済モデルごとにPKI信頼モデル（ドメインモデル）の洗い出しを行った．

一般的なモバイル以外でのPKIにおいてはその技術要件の容易さから独立方式での実装が多いと考えられる．しかしながらモバイル環境で，かつクレジット決済モデルによっては技術要件，運用要件に応じて他の方式を用いるほうが望ましいケースも考えられる．

認証WGでは最も技術要件が難しいと考えられる相互認証方式をベースとして検討を行った．

図5にデータ入力モデルに対するドメイン間認証の例を，図6に端末格納型モデルに対するドメイン間認証の例を示す．

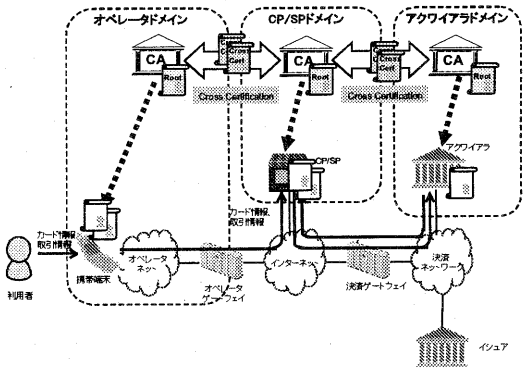

図5　データ入力型モデル

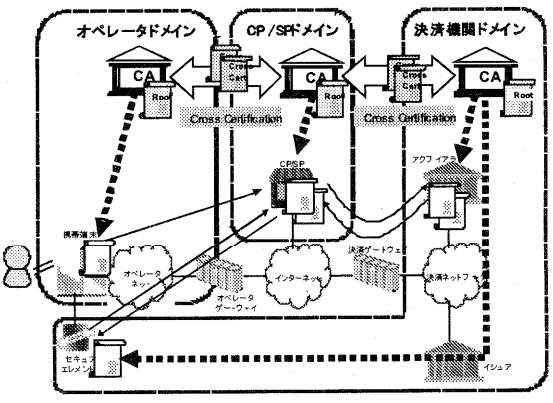

図6　端末格納型モデル

3.4. 共通プロファイル

携帯電話利用者の認証をPKIベースで行う場合，オペレータドメイン内のCAは，利用者に対して公開鍵証明書を発行する必要がある．しかし各社のCAが独自の方針・方法により証明書を発行した場合，サービス提供者は利用者の認証方法をCA毎に変更しなければならなくなる可能性がある．これはサービス提供者のPKI導入に対する阻害要因となり得る．

認証WGではモバイルEC推進の観点から上記問題が生じないようオペレータドメインで利用する公開鍵証明書について共通化が必要な内容をまとめ参考プロファイルとして公開を行った．

本論文では，プロファイルの規定方針，規定対象についての考え方を述べ，またSSLクライアント認証において加入者を示すための方法として規定されたモバイルIDについて紹介する．

3.4.1. 規定方針

本プロファイルは携帯電話利用者，サービス提供者（CP/SP）の双方に広く受け入れられる必要があるという観点から，規定にあたり以下の方針を設定した．

(1)インターネットとの接続性

携帯電話ユーザもサービス提供者から見ればインターネットの一ユーザにすぎない．サービス提供者にとってアクセスの経路によって異なる形式の認証情報が送付されることはシステム開発上望ましくない．従ってプロトコルや形式などはモバイル固有のものを別途規定するのではなく，インターネットで標準的に用いられている形式を取り入れることにした．

(2)最小限の規定

本プロファイルは携帯電話会社やサービス提供者各社の自由なビジネスやシステム構成を阻害しないものでなければならない．また他の標準ドキュメントとの記述の重複は保守上望ましくない．従って，サービス提供者や利用者が証明書を共通的に扱う上で是非必要な項目に限りプロファイル上に規定することとした．

(3)現実性の考慮

プロファイルは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必要がある．特に携帯電話においてはPCのように最新の仕様を実装することが困難な場合がある．本プロファイルの規定においては，現時点で一般に使われている製品のサポート状況を考慮しプロファイルを規定することとした．

3.4.2. 規定対象項目

上記方針に則り，プロファイル規定対象の絞込みを行った結果，主に下記の項目について規定を設けることとした．

(1)証明書の位置づけ

サービス提供者が証明書による認証結果を共通的に取り扱ためには，そもそも証明書は何を証明しているのかといった基本的な「証明書の位置づけ」について共通化が必要である．証明対象の設定に当たっては通信事業者として考慮すべき事項が存在する．これは本プロファイルを規定するにあたり中心となった検討であり次節において詳細を述べる．

(2)証明書の記載事項

各社の発行した証明書を共通したシステムで処理するためには，証明書の形式や証明対象の表現など「証明書の記載事項」に共通化の必要な事項がある．またCRLの形式も共通的な方法を決めておく必要がある．本プロファイルでは，インターネットとの接続性の観点からIETF-RFC2459で定められた標準に準拠することを前提としたが，現実性の考慮の観点からエンコーディングについては特別な規定を行った．

(3)証明書の運用方法

各社の発行した証明書を同様に信頼するためには証明書の運用方法を規定する必要がある．本プロファイルでは，最小限の規定という観点からサービス提供者が信頼を形成するのに必須と考えられる，証明書の更新間隔，失効情報の提供方法，鍵長についての規定を行った．

3.4.3. モバイルID

一般に，公開鍵証明書が証明する対象(subject)としては氏名，電話番号，端末製造番号，契約番号などいろいろな可能性があり，サービス提供者が統一的に扱うためには共通化が必要である．プロファイルの規定に当たっては，証明書発行者がオペレータドメインのCAであることから特に以下の条件を考慮した．

(1) 加入者のプライバシ保護

公開鍵証明書への個人情報を記載にはプライバシ保護の観点から注意が必要である．署名時あるいは公開鍵証明書の通知時にはユーザプロンプトにより利用者に注意を促すことが一般に行われているが，通信事業者としては携帯電話ユーザのリテラシや電話紛失等の事故を考慮し，証明書の記載事項レベルでより厳密にプライバシを考慮する必要がある．

(2) 回線契約業務との整合性

通信事業者は回線契約時に本人認証を行い加入者のデータベースとして管理している．公開鍵証明書を発行する際に別途登録業務を行う代わりに，上記本人認証情報を活用することは自然であろう．

(3) 端末変更の可能性

携帯電話の利用者はある期間が経過すると機種変更を行うことが多い．また機種変更に伴って電話番号を変更することもある．利用者やサービス提供者は，サービスの継続性の観点から，機種変更時等に利用者のアイデンティティ連続性を保証したい場合がある．

以上の考察により認証 WG では

・リアルの世界で利用者個人を特定する情報（実名，電話番号，住所）が隠蔽される．

・機種変更時にも連続性を保証される．

という性質を持つ ID として，加入者契約と一対一に対応し匿名性を持つ ID を定め「モバイル ID」と呼ぶこととした．モバイル ID は上記条件を満たす限りフォーマットは自由である．モバイル ID はオペレータドメイン証明書の Subject の CN として用いられる．

3.5. モバイル環境特有の課題

本節では，モバイル環境特有の課題について述べる．

3.5.1. 証明書有効性確認に関する要件と課題

ここでは、3.3.1 で述べた３つのドメイン間認証方式における証明書有効性確認の要件と課題について述べる．

相互認証方式を用いてドメイン間認証を実現する場合には，回線速度の観点からは，証明書パス検証のために入手が必要な証明書数が増えるという問題点がある．またパス検証のために検査する証明書の数が増えるという処理能力の問題や，複数の相互認証書をモバイル上に記憶しなければならない記憶容量の問題もある．また，モバイル環境ではユーザインタフェースの観点から，パス検証におけるポリシー制御において柔軟性が低いと考えられるため，複雑なポリシー制御が困難である，という課題も存在する．

独立方式を用いてドメイン間認証を実現する場合には，複数のドメインの証明書を検証するために，ドメインの数だけ認証局証明書をモバイルユーザがポリシーを理解した上で，安全に入手する必要があり，これは，ユーザリテラシ，端末の記憶容量等の観点から問題点が多い．

第三者方式を用いてドメイン間認証を実現する場合には，TTP への証明書検証を依頼するために，トランザクションの途中で TTP との通信が発生するために通信遅延が発生する．また処理能力の観点では，証明書の検証プロセスを TTP へ依存できるため他の方式に比べて端末への負荷は少ないといえる．

表２にモバイル環境で PKI を利用したドメイン間認証方式の課題の比較を示す．

表２ モバイル環境での各ドメイン間認証方式の課題

課題	相互認証方式	独立方式	第三者方式
回線速度	証明書パス検証のための相互証明書を取得する必要がある．	ドメインの数だけ信頼する認証局証明書取得のためのトラヒックが発生する．	トランザクションの途中でTTPとの通信が発生する．
処理能力	パス検証のために相手の証明書までのパスを探索しなければならず，検査する証明書の数が増える．また複雑なポリシー制御が困難である	モバイル特有の影響少	モバイル特有の影響少
記憶容量	複数の相互証明書をモバイル上に記憶しなければならない	ドメインの数だけ信頼する認証局証明書をモバイル端末上に記憶しなければならない	モバイル特有の影響少

3.5.2. 個人認証に関する課題

3.4 節で述べたように契約ごとに一意なモバイル ID が記述された証明書により統一的な PKI の枠組みを提供することが可能となる．

PKI は秘密鍵の所有を拠り所とした個人認証であり，端末が移動するモバイル環境では特に，秘密鍵の盗用による他人へのなりすまし対策が必須である．以下のセキュリティが重要である．

- 秘密鍵の秘匿性：秘密鍵が他者へ漏洩しないこと
- 秘密鍵の本人性：秘密鍵が正しい所有者以外に利用できないこと

前者に関しては，セキュアデバイスの使用等が考えられる．また，後者に関しては本人の直接的な属性である生体情報に基づいた本人認証（バイオメトリクス）と連携することで安全性を高められる可能性がある．

図７は PKI の仕組みを強化するためのバイオメトリクス技術活用例である．クライアントで生体情報の照合に成功した場合に限り，秘密鍵が活性化され署名生成ができるという例を示している．

このように適切な個人認証を実現するためには，適切な PKI 技術と適切な本人認証技術の組み合わせが重

要であるということができる.

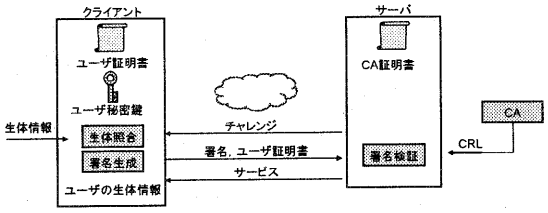

図7　PKIの仕組みを強化するためのバイオメトリクス技術活用例

また，3.4.3節で述べたようにモバイルIDは契約に結びついているIDであるが，プライバシ保護の観点から「証明対象の特定が困難なID」とされている.

このような利用者個人を特定する情報が隠蔽されたモバイルIDが記述された証明書の機能を補完するものとして，属性証明書[4]の利用が考えられる．属性証明書は，公開鍵証明書と類似の構造をしているが，公開鍵の所有者を保証するものではなく，証明書所有者の属性（特権）を保証するものである．属性証明書は，有効期間を比較的短期に設定でき，証明書の失効手続きを省略できるので，3.5.1節で示したようなモバイル端末に不向きな失効確認等が不要になるという利点がある．また，モバイル環境特有の位置情報などを属性として用いることも可能である.

以下に属性証明書を用いた認証技術の一般的なメリット/デメリットを記述する.

＜属性認証のメリット＞

- 属性の追加・変更・抹消にともなう公開鍵証明書の失効の回避が可能
- 本人性を確認する機関と資格を付与する機関の権限を分離することが可能
- 公開鍵証明書に属性を付与した場合に生じる不要な属性情報の伝達を防止可能
- 短い有効期間を持たせることにより，失効プロセスを省略することが可能
- 属性変更にともなう属性証明書検証者側の作業をなくすことが可能
- 1つの公開鍵証明書に複数の属性証明書を割り当てられるため，複数の鍵や当該鍵を活性化するためのパスワード等を管理しなくてすむ
- 公開鍵暗号ベースのセキュリティで，資格や権限の認証を行える
- 公開鍵証明書と違い，属性証明書はオンラインで発行することが可能
- これまで課題とされてきた代理申請を行うための手段の1つとして利用できる

＜属性認証のデメリット＞

- 属性認証局というエンティティが必要となる
- 属性認証局の運用面に課題が残されている
- 属性認証局と属性証明書検証者が同一であるモデルにおいては，ＤＢ等による資格認証方式のほうが実現容易である
- 検証処理が複雑なため，他の方式に比べ検証に時間がかかる
- 属性証明書を取り扱える製品がほとんど存在しない
- 属性証明書を利用できるようにするための基盤整備が必要となる

4. むすび

本稿では，mITF　MC部会　認証WGにおいて，昨年度検討を行ったPKI技術をオンラインクレジット決済に適用した場合のドメインの構成や認証要件，モバイル環境を考慮したクライアント証明書プロファイル，および，PKIをモバイル環境で利用する際の制約や考慮点について考察を行った．これらの机上検討で洗い出された課題や検討結果は，携帯端末やモバイル網など特徴が反映された結果となっているが，本メソドロジーは，PKI技術を他の実サービスに適用する際にも参考になると考える.

今後は，ローカル環境に基づくモバイルコマースに対するPKI技術の適用や，ディジタル署名技術のモバイルコマースへの適用の可能性などについて検討を行う予定である．謝辞：最後に，認証WGの活動を通じて多大なるご協力いただいた認証WG委員の方々に謝意を表する.

文　献

[1] ECOM,“相互認証ガイドライン,” 1998.

[2] IETF,“RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile,” Jan. 1999.

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

[4] IETF, “RFC 3281 An Internet Attribute Certificate Profile for Authorization,” April 2002.