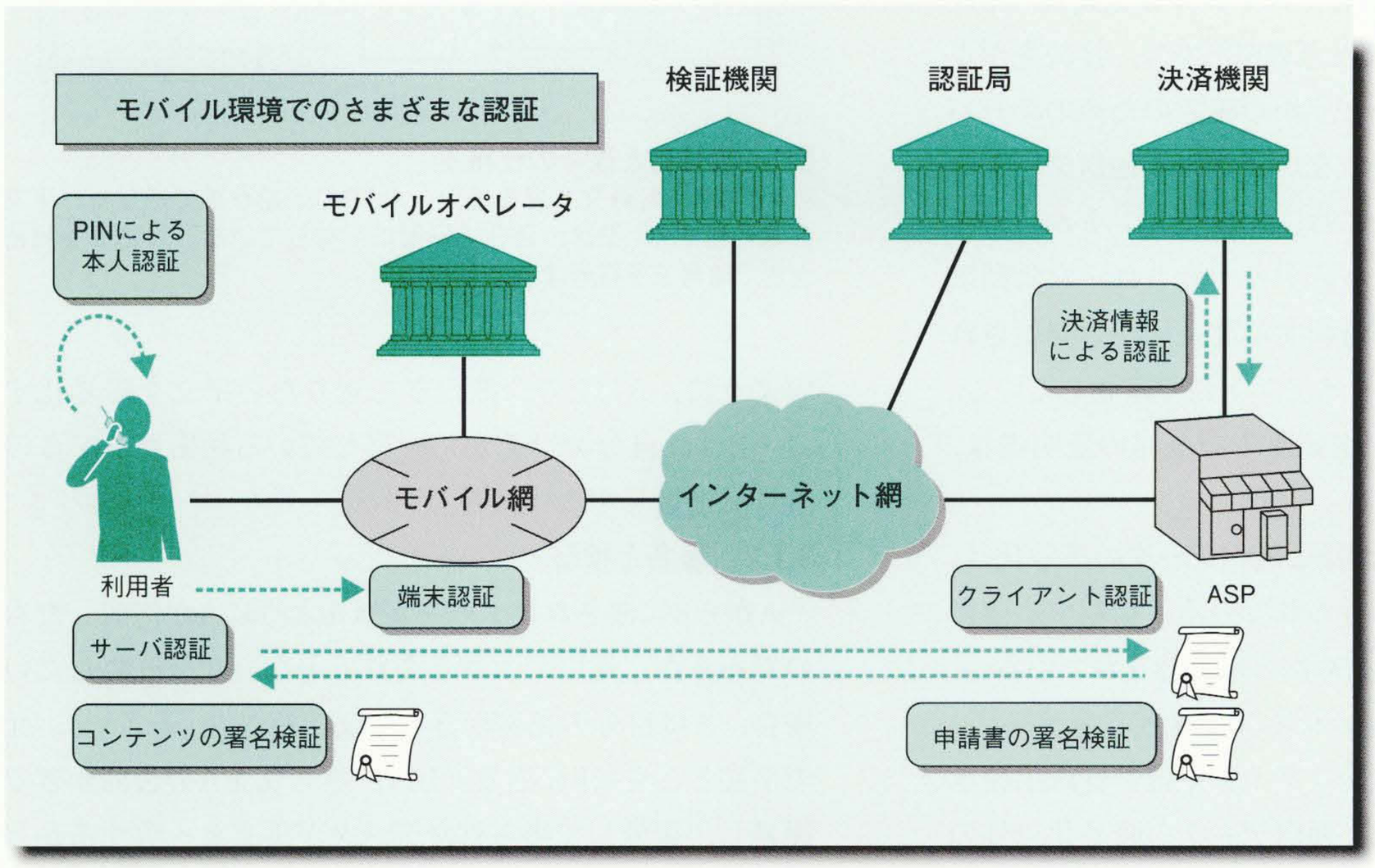
特集　ブロードバンド，モバイルコンピューティングが変えるネットワーク社会

モバイル時代のセキュリティを支える公開かぎ基盤技術と動向

Public key Infrastructure Technologies and Their Trends for Supporting Security Infrastructures in Mobile Environments

梅澤克之　*Katsuyuki Umezawa*　手塚　悟　*Satoru Tezuka*
鍛　忠司　*Tadashi Kaji*　松島　整　*Hitoshi Matsushima*



注：略語説明
PIN（Personal Identification Number）
ASP（Application Service Provider）

モバイル環境でのさまざまな認証例

モバイル環境で電子商取引や電子行政手続きを安全に行うためには，そこに登場するプレーヤーどうしのさまざまな認証が必要である。PKI（公開かぎ基盤）技術は，それらを実現する有望な解決策である。

ネットワークに接続できる携帯電話の普及により，携帯電話を利用するモバイルコマースを含めた電子商取引（EC：Electronic Commerce）全体のビジネスエリアが広がってきた。安心してECを行うためには，取引情報の漏えい防止や取引相手の認証，契約文書の改ざん防止などの機能が不可欠となる。これらの機能を実現する方法の一つに，ECビジネスの根幹を成すセキュリティ基盤であるPKI（公開かぎ基盤）技術の構築がある。

リソース制限が厳しいモバイル端末上にPKIを実施するためには，さまざまな課題がある。例えば，端末そのものの負荷削減のためのアプローチとしてPKIで最重要とされる証明書の正当性を検証しようとする場合，外部の信頼できる第三者である証明書検証機関（VA：Validation Authority）に問い合わせをすることが考えられる。

日立製作所は，この点に着目し，さまざまな認証環境に対応したVAを構築するための，証明書検証サーバ（CVS：Certificate Verification Server）を開発し，提案している。また，2001年6月に総務省の主導で発足したモバイルITフォーラム（mITF）の技術的検討に参加することにより，モバイル時代のセキュリティ基盤構築に貢献していく。

1　はじめに

次世代携帯電話では，現在の携帯電話の単体入力，表示，電波による通信機能に加え，耐タンパ性を備えたICカードの装備が予想される。このような特徴を持つ携帯電話を利用したモバイルコマースに対する要求は大きい。

EC（Electronic Commerce）では，プライバシー情報を含む取引情報の漏えいを防止するため，データ保護の機能は必須である。また，アクションの主体（取引相手）が何者であるかを確認し，成り済ましを防止するユーザー認証機能や，契約内容の改ざんを防止するためのメッセージ認証機能も不可欠である。さらに，取り引きの内容を改ざんまたは消去し，虚偽の内容の履行を強制するような事後否認を防止するための機能も必要である。

ここでは，これらの機能を実現するためのECビジネスの根幹であるセキュリティ基盤のPKI（Public Key Infrastructure：公開かぎ基盤）技術と，それを携帯電話などリソースの制限が厳しいモバイル端末上に実装する際の課題と解決策，および多くの企業や業界の協力が不可欠な，セキュリティ基盤構築のための標準化活動への日立製作所の取り組みについて述べる。

2 モバイル環境のセキュリティの現状

パソコンのウェブブラウザでショッピングサイトのサーバへ接続すると，ブラウザにかぎマークが表示される。このときに使われている通信プロトコルがSSL(Secure Socket Layer)である。このときのSSLでは，接続先が正しい(信頼できる)サーバかどうかの確認のためのサーバ認証と，通信内容を盗聴されないように，通信データの暗号化が行われる。具体的には，クライアントからの接続要求時にサーバからサーバ証明書が渡され，有効期限が切れていないか，自分が信頼する認証局から発行された証明書であるかなどをクライアント側で確認している。その確認に用いる，自分が信頼する認証局の証明書は，ブラウザに組み込まれている。

モバイル環境でのサーバ認証と通信データの暗号化は，一部の携帯電話でもすでに行われている。信頼する認証局の証明書も，携帯電話に初めから組み込まれている。

しかし，今後のモバイルビジネスの発展を考えると，例えば，会員制のサイトへのログインや電子行政手続きなどでは，上記サーバ認証と通信データの暗号化以外のクライアント(利用者を確定する)認証が必要である。携帯電話を用いたインターネットアクセスのユーザー認証は，現在，ID(Identification)・パスワード方式のほか，携帯端末番号などの端末固有番号を送付し，サーバ側で確認する方法などが実用化されている。今後期待されているのは，PKI技術に基づいたクライアント認証技術である。これは，単純なIDや携帯端末番号の代わりに，信頼できる機関から発行された電子証明書により，利用者の認証を行うものである。

3 公開かぎ基盤(PKI)の必要性

3.1 公開かぎ暗号

PKIの基本技術である公開かぎ暗号とは，異なる二つのかぎを1組として使用する方式で，一方のかぎで暗号化したデータは，もう一方のかぎでしか復号できない，さらに，一方のかぎからもう一方のかぎを生成することができないという特徴を持っている。公開かぎ暗号を利用するユーザーは，まず始めに，組になる二つのかぎを作る。一つのかぎは広く一般に開示し，もう一つのかぎは秘密裏に保管する。前者のかぎを「公開かぎ」，後者のかぎを「秘密かぎ」と呼ぶ。

3.1.1 暗号化と復号

AからBにデータを送る際，第三者に内容を知られないように，AはBの公開かぎで送りたい平文を暗号化する。Bは，自分でひそかに所有している秘密かぎでこの暗号文を復号する(**図1**参照)。

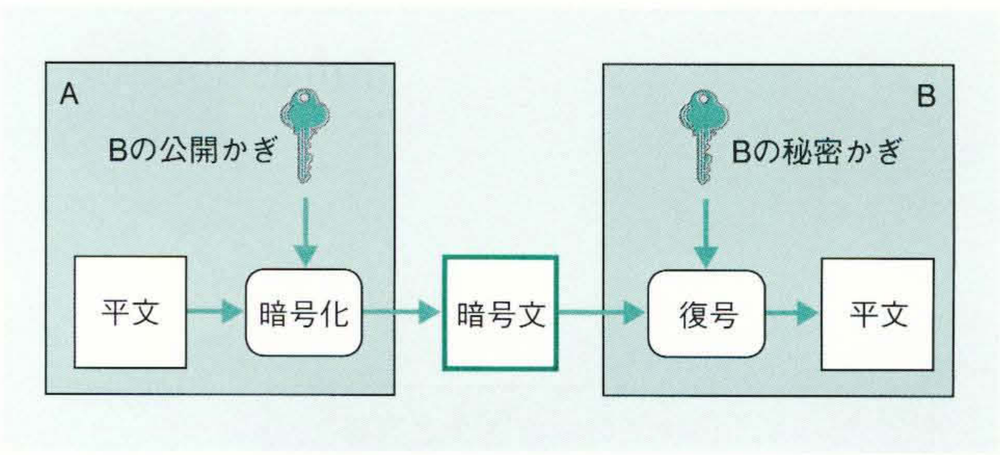


図1 暗号化と復号の仕組み
AからBに暗号文を送る場合，AはBの公開かぎで送りたい平文を暗号化する。Bは，自分で秘密に所有している，対応する秘密かぎで暗号文を復号する。

3.1.2 署名と検証

AからBに渡されたデータがほんとうにAが作成したものであるか，途中で改ざんされていないかを確認したい場合，Aは自分の秘密かぎで平文を暗号化(署名)し，元の平文とともにBに送る。Bは，暗号文をAの公開かぎで復号し，復号して得られたデータが平文と一致するかどうかを確認する(検証)。一致すれば，Aの公開かぎで復号できたのであるから，この暗号文はAの秘密かぎで暗号化されたことになる。Aの秘密かぎはAしか知りえないので，このデータはほんとうにAが署名したということ(ユーザー認証)と，改ざんされていないこと(メッセージ認証)を検証することができる(**図2**参照)。

3.2 公開かぎ証明書

電子商取引では，申し込みがほんとうに本人によってなされたかどうかを確認することが重要である。この確認は，前述の公開かぎ暗号の署名・検証の技術を使えば実現が可能である。しかし，BがAの公開かぎだと思って入手したものが，実はAの名前をかたったCであったとし

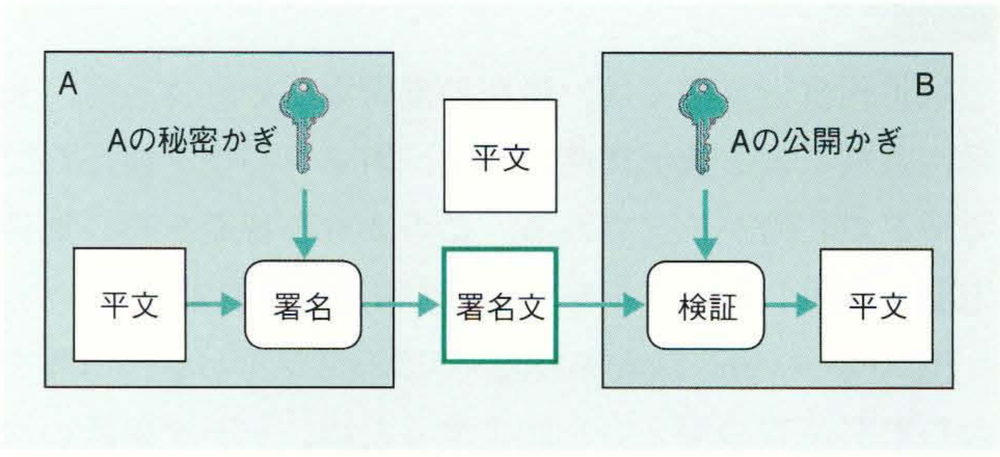


図2 署名と検証の仕組み
Aは自分の秘密かぎで平文を暗号化(署名)し，元の平文とともにBに送る。Bは暗号文をAの公開かぎで復号し，得られたデータが平文と一致するかを確認する(検証)。

ても，BはAからのデータだと思い込んでしまう。したがって，公開かぎ暗号を利用して署名検証を行う場合，本人とその公開かぎの対応関係がきちんと保証されていなければならない。

公開かぎとその所有者を対応づけるものが「公開かぎ証明書」である。公開かぎ証明書は，TTP(Trusted Third Party：信頼できる第三者機関)であるCA(Certification Authority：認証局)から発行される。公開かぎ証明書にはシリアル番号や有効期限，所有者の名前，公開かぎそのものなどが含まれ，さらに，発行元の認証局の署名が付加される。証明書の形式としては，ITU(国際電気通信連合)の勧告"X.509"が広く使われており，モバイルの世界ではメモリの制約のために，内容を簡略化した"WAPCert"がWAP(Wireless Application Protocol)フォーラムで規定されている。

前述の例では，BはAから公開かぎ証明書を入手し，この証明書にある所有者の名前を確認するとともに，証明書に付加されている発行認証局の署名を検証することにより，Cによる成り済ましを防ぐことができる。

なお，発行認証局の署名検証にも発行認証局の公開かぎ証明書が必要であり，それは，さらに上位の認証局から発行される。最上位の認証局を「ルート認証局」と呼ぶ。ルート認証局が複数存在する場合には，それぞれが互いを認証する「相互認証」のモデルもある。

このように，PKIは，公開かぎ暗号技術を使った署名によるユーザー認証や，データの一貫性，否認防止，暗号化による機密性などを実現するための大前提となる基盤である。

4 モバイル環境での課題と解決策

モバイル環境での証明書のライフサイクル管理に関しては，さまざまな課題があげられる(**表1**参照)。

例えば，端末内でかぎを生成するような場合，端末の処理能力が不足となるおそれがある。証明書をオペレータが発行する場合，携帯電話購入時の初期登録の一環として処理することは可能であるが，購入後にオンラインで発行する場合の安全な実行手段が必要とされる。証明書の利用に関しては，複数の証明書を取り扱うための手段が必要とされる。さらに，証明書を携帯電話内で検証する場合は，処理速度や記憶容量に制約の多い携帯端末は適さない。

このようなさまざまな課題のうち，証明書の検証に関する一つのソリューションについて以下に述べる。

表1　公開かぎ証明書のライフサイクル管理に関する課題

モバイル環境での証明書のライフサイクル管理に関するさまざまな課題の例を示す。

分　類	課　題
かぎの生成に関する課題	携帯電話内での秘密かぎ作成能力
	第三者によるかぎ生成の安全性
	携帯電話内での秘密かぎの保管の安全性
	公開かぎ証明書の保管の安全性
公開かぎ証明書の申請・発行に関する課題	発効手続きを利用者自身が行ったことの確認
	証明書事前組込み型のかぎや証明書の更新
	証明書と利用者の関連づけ
	オンラインでの発行方式とそのセキュリティの確保
証明書の利用に関する課題	携帯電話が署名者となる場合の負荷
	携帯電話内での証明書検証時の負荷
	検証機関への依頼時のセキュリティの確保
証明書の失効に関する課題	オンラインでの失効時の本人確認方法
	秘密かぎ紛失による証明書失効方法
相互運用性に関する課題	既存システムのモバイル環境への対応
	異なるフォーマットへの証明書での対応

携帯電話で証明書を受け取ったとき，その証明書の有効性確認を外部の信頼できる第三者であるVA(Validation Authority：証明書検証機関)に問い合わせるモデルを**図3**に示す。販売店(ASP：Application Service Provider)から受け取ったデータを検証する場合，まず，ASPの証明書が有効かどうかを証明書検証機関であるVAに問い合わせる。VAはCA(認証局)からのCRL(Certificate Revocation List：証明書失効リスト)を取り寄せたり，ASP側CAに証明書の有効性を問い合わせたりして検証した後，その結果を利用者に返送する。このように，VAを利用することにより，携帯電話でも厳密に証明書失効情報を取り扱うことができるようになる。

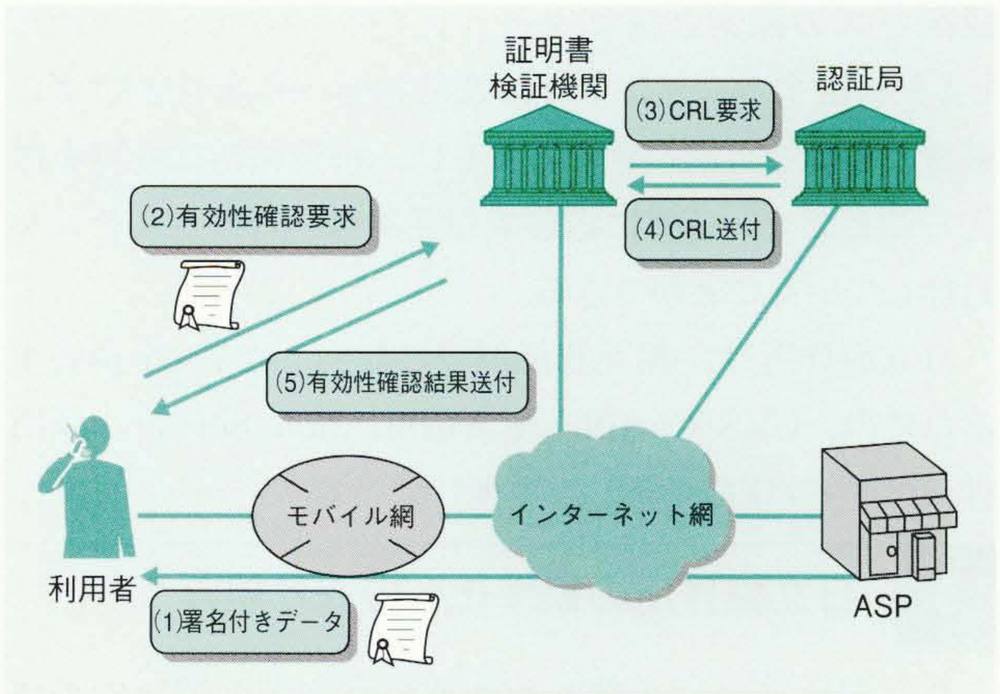


図3　携帯電話の利用者が証明書を検証するシステム例

ASP(販売店)から受け取った電子署名付きデータを，限られたリソースしか持たない携帯電話で利用者が検証する場合には，まず，ASPの証明書が有効かどうかをVA(検証機関)に問い合わせる。VAは，CA(認証局)からCRL(証明書失効リスト)を取り寄せるなどによって証明書の有効性を検証し，検証結果を利用者に返送する。

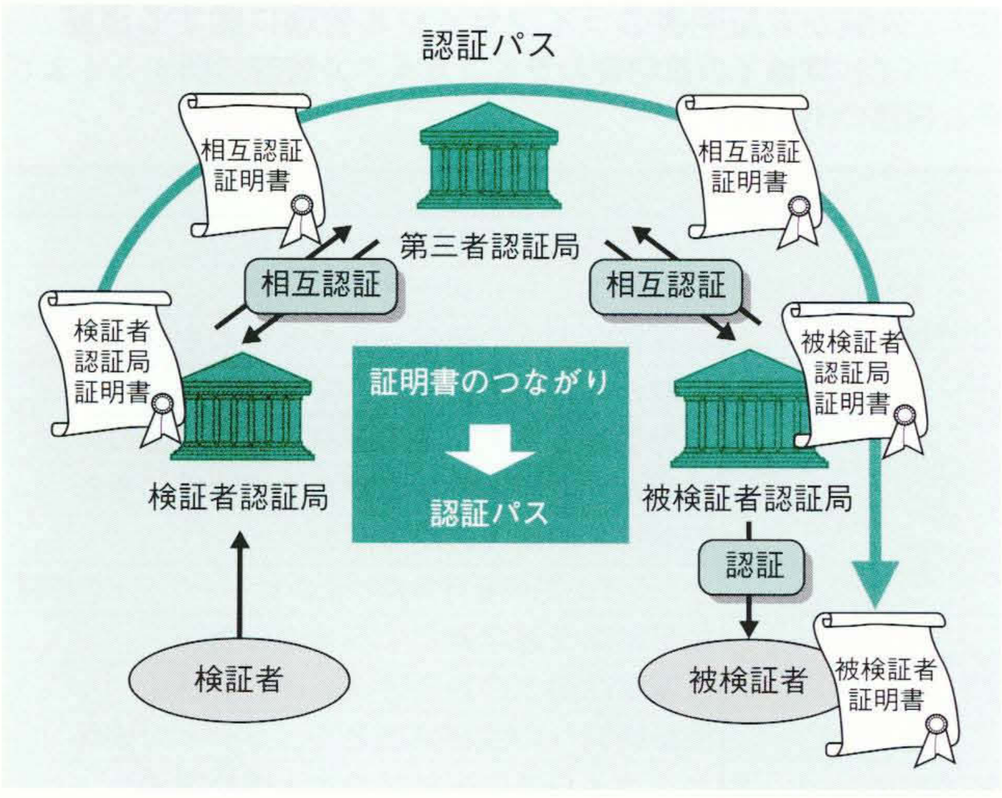


図4 認証パスの構築

検証者と被検証者とで信頼するルート認証局が異なるような状況では，検証者が信頼する認証局から被検証者が信頼する認証局までの相互認証のパスを探索，構築しなければならない。VAはこの機能を持っているので，携帯電話などのモバイル環境でVAを利用することにより，端末に負荷をかけずに厳密な認証が可能になる。

証明書検証にVAを利用することは，さまざまなシステムへの柔軟な対応ができるという点でも優れている。例えば，ルート認証局が異なる二つのシステム間で相互運用を行う場合，二つのシステムに共通のルート認証局を新たに構築するよりも，互いのルート認証局が相互に認証し合うほうが効率がよい。

このような環境では，検証者が信頼するルート認証局と被検証者が信頼するルート認証局とが異なるので，検証者が信頼する認証局から被検証者が信頼する認証局までの，相互認証のパス(証明書のつながり)を探索，構築しなければならない(**図4**参照)。しかし，VAはこれらの認証パスの探索と構築を行う機能を持っているので，VAを利用することにより，携帯電話へ負荷をかけずに厳密な認証を可能にするとともに，携帯電話に変更を加えることなく，必要に応じて相互運用を行うシステムを追加していくことができる。

日立製作所は，相互認証環境に対応したVAを構築するための，CVS(Certificate Verification Server：証明書検証サーバ)を開発し，提供している。

5 日立製作所の標準化への取り組み

日立製作所は，上述した技術的な課題と解決案のほか，標準化活動も進めている。

わが国のモバイルIT(Information Technology)立国の早期実現を目的として，新世代モバイル機器や環境の研究・開発と標準化を総合的に推進するために，2001年6月に総務省の主導によるmITF(モバイルITフォーラム)が発足した。mITFのMC(Mobile Commerce)部会では，モバイル環境でECを実現するためのリファレンスモデルの作成や，実際の決済スキームの整理，また，決済を行う際の基盤として使われる認証技術の検討などが行われている。そのMC部会の中で，日立製作所は，技術専門委員会の主査として取りまとめを行っている。

6 おわりに

ここでは，モバイル環境のセキュリティの現状，そこでの公開かぎ基盤(PKI)技術の必要性，およびモバイル環境に適用する際の課題と解決策について述べた。

ここで述べたようなセキュリティ基盤技術は，単独の企業や業界だけで成し遂げられるものではなく，オペレータ，デバイスベンダー，金融・決済機関，サービス・コンテンツプロバイダーなど各業界の協力によって構築されるものである。

日立製作所は，今後も，モバイル時代のセキュリティ基盤の構築に貢献していく考えである。

参考文献

1) 手塚：ITコマースでPKIはどう利用されるのか，コンピュータ＆ネットワークLAN，2001年10月号，pp.19～25

執筆者紹介

梅澤克之
1996年日立製作所入社，システム開発研究所 第7部 所属
現在，企業情報システム，分散オブジェクトシステム，モバイルセキュリティ技術などの研究・開発に従事
情報処理学会会員
E-mail：ume @ sdl. hitachi. co. jp

鍛 忠司
1996年日立製作所入社，システム開発研究所 第7部 所属
現在，企業情報システム，分散オブジェクトシステム，モバイルセキュリティ技術などの研究・開発に従事
E-mail：t-kaji @ sdl. hitachi. co. jp

手塚 悟
1984年日立製作所入社，システム開発研究所 第7部 所属
現在，セキュリティシステム，特に電子認証の研究・開発に従事
工学博士
E-mail：tezuka @ sdl. hitachi. co. jp

松島 整
1971年日立製作所入社，情報・通信グループ ネットワークソリューション事業部 所属
現在，モバイルセキュリティ，ITS，民需ネットワークのソリューション開発・事業化に従事
E-mail：h-matsushima @ itg. hitachi. co. jp