Vol. 48 No. 2 情報処理学会論文誌 Feb. 2007

モバイル向け証明書検証システムの開発

梅澤克之[†,††] 笈川光浩[†] 洲崎誠一[†]
手塚悟[†] 平澤茂一[††]

近年，インターネット環境においては，電子入札，電子納税，商業登記申請等の公共サービスや，社外から社内へのリモートアクセス等，不正行為を防止するために PKI 技術に基づく認証機能を有するサービスが増加しており，そこで使われる証明書の厳密な検証を行うようになってきている．一方，モバイル環境においては，携帯通信事業者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て一般のサービス提供者からサービスを享受する機会が急増している．このような状況から，インターネットの脅威がそのままモバイル環境においても成り立つ状況になってきており，モバイル環境においても証明書の利用による PKI 技術を用いた認証方式の確立は必須であると考えられる．すでにモバイル環境でも証明書の利用が始まっているが，携帯電話端末側でサーバ証明書が失効されていないかを確認する有効性確認は行われていない．モバイル環境においても不正が許されないクリティカルなサービスが今後ますます増加することが予想でき，そのようなサービスでは有効性確認を含む厳密な証明書の検証を行うことが必要である．本論文では，有効性確認を第三者に依頼する CVS 方式に基づいて開発した携帯電話端末の処理時間や通信速度等のモバイル環境特有の制約を考慮したモバイル向け証明書検証システムを提案し，性能，安全性，利便性の観点で評価を行う．

Development of a Certificate Validation System for a Mobile Network

Katsuyuki Umezawa,[†,††] Mitsuhiro Oikawa,[†] Seiichi Susaki,[†]
Satoru Tezuka[†] and Shigeichi Hirasawa[††]

In the Internet environment in recent years, services having an authentication function based on PKI technology have been increasing in order to prevent unauthorized activities. Some examples are remote accessing, electronic bidding, electronic payment of taxes and so on. In such services, strict verification of the certificate has become more and more important. On the other hand, in a mobile environment, mobile service using not only service in the mobile carrier net but also the Internet has increased. It is thought that PKI technology is important in a mobile environment in such a situation. Two or more mobile carriers already support PKI technology. But strict verification that confirms whether the certificate was revoked or not is not done. In a mobile environment, it is necessary to carry out the verification of the certificate strictly. In this paper, we propose a certificate validation system for mobility. The system is based on the CVS method. And it corresponds to the peculiar restrictions of mobility and the environments of the processing speed and the transmission rate, etc. of the cellular phone terminal. Furthermore, we evaluate the performance, safety and the convenience of the system.

1. はじめに

近年，インターネット環境においては，不正サイトのフィッシング詐欺によるクレジットカード番号やパスワードの流出，通信路の盗聴，ID の偽造・改ざん等，インターネットを利用したサービスにおいて不正行為が増加している．安心してサービスを提供・享受するためには，サービスを提供する側とサービスを享受する側が正しく相互に認証し合うことが重要である．PKI 技術を用いて相互認証を行うことにより通信相手を確認することはできるが，不正な利用者やサービス提供者を正確に見極めるためには，通信相手が提示する電子証明書（以下，証明書）が失効されていないかを確認する有効性確認を行う必要がある．このような証明書の有効性確認まで行う厳密な証明書検証を行う認証機能を備えたサービスの例としては，電子政府（GPKI）等の認証基盤を利用した電子入札，電子納

† 株式会社日立製作所システム開発研究所
Systems Development Laboratory, Hitachi Ltd.
†† 早稲田大学大学院理工学研究科
Graduate School of Science and Engineering, Waseda University

税，商業登記申請等の公共サービスや，民間企業における社外から社内へのリモートアクセス等があげられる．これらのサービス以外にも，高額決済をともなうようなけっして不正が許されないサービスにおいては，そこで使われる証明書の厳密な検証を行うようになってきている．

一方，モバイル環境においては，携帯通信事業者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，特定の携帯通信事業者の公式サイトからだけではなく，一般のサービス提供者からサービスを享受する機会が急増している．このような状況から，インターネットの脅威がそのままモバイル環境においても成り立つ状況になってきており，モバイル環境においても証明書の利用によるPKI技術を用いた認証方式の確立は必須であると考えられる．すでに複数の携帯通信事業者において証明書の利用が始まっているが，携帯電話端末側でサーバ証明書が失効されていないかを確認する有効性確認は行われていない．モバイル環境においても不正が許されないクリティカルなサービスが今後ますます増加することが予想でき，そのようなサービスでは有効性確認を含む厳密な証明書の検証を行うことが必要である．

証明書の検証方式には，検証を行う主体が自ら有効性確認を行う方式（CRL方式）や，有効性確認を第三者に依頼する方式（OCSP方式，SCVP方式，CVS方式）等，複数の方式が提案されている．このような検証方式をモバイル環境に適用する場合，携帯電話端末の性能やモバイル網の通信路帯域幅等のモバイル環境特有の問題を考慮する必要がある．筆者らは文献1)〜3)，15)において，携帯電話端末の処理時間やモバイル網を経由した通信速度等の関係から，証明書検証に要する平均時間の観点で各方式の比較評価を行った．携帯電話端末への証明書検証モジュールの実装を行う場合，実装の容易性等も考慮しなければならない．たとえばOMA WPKI[16]では，モバイル環境特有の問題のためにCRL方式やOCSP方式はモバイル環境における証明書の有効性確認には向いておらず，有効性確認が不要なShort-lived証明書の利用が提案されている．しかしこの方式では，すでに一般的なX.509サーバ証明書等で運用を開始しているサービス提供者（サーバ）側に変更を強いるという問題が生じる．これに対し，OMA OCSP Mobile Profile[17]やIETF Lightweight OCSP Profile[18]等では，OCSPプロトコルの様々なオプションを制限し，モバイル環境で利用しやすいようなOCSPプロファイルを定義している．しかしOCSP方式では，有効性確認以外の証明書検証に関わる処理は依然として携帯電話端末に実装しなければならないという問題がある．筆者らは，携帯電話端末に対して追加のハードウェア実装やネイティブアプリケーション開発を行うことなしに，既存の携帯電話端末に最小限のアプリケーションモジュールを追加することで実現可能な方式を検討した．これにより携帯電話端末では今まで実現されていなかったCVS方式に基づく厳密な証明書検証を実現した．また，携帯通信事業者のCRLを無条件に公開すると解約者の絶対数や増加率等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は適切に取り扱う必要がある．筆者らはCRLを公開することなく厳密な証明書検証が行える方式を検討した．

以上の理由から本論文では，モバイル環境に適すると考えられる有効性確認を第三者に依頼するCVS方式に基づいて開発したモバイル向け証明書検証システムを提案し，性能，安全性，利便性の観点で評価を行う．

以下では，まず，2章で証明書の検証に関する従来技術について記述する．3章でモバイル環境における証明書の有効性確認のモデルを示し，4章でモバイル環境においてCVS方式に基づいた証明書検証システムを構築する際の課題を明確化する．5章で実現方式の詳細を示し，6章で実測値，安全性，利便性の評価を行う．そして最後に7章でまとめと今後の課題を示す．

2. 従来技術

2.1 証明書検証技術

証明書を検証するための手順は，ITU-T X.509 (2000)[4]やRFC3280[5]にて規定されている．実際に証明書検証者が行う検証手順は，大別して「認証パスの構築」「認証パスの検証」の2つである．

2.1.1 認証パスの構築

「認証パスの構築」とは，検証者が信頼している認証局（以下トラストアンカと記す）の証明書から，検証対象となる証明書までの証明書チェーンを構成する証明書の組合せ（認証パス）を探索する技術である．検証者は，認証パス上の証明書をすべて取得しないと検証処理を行うことができない．そのため，署名者が送付する署名データに証明書群を添付するか，検証者がリポジトリにアクセスして必要な証明書を取得しなければならない．認証パスは，認証局のモデルに大きく依存する．認証局のモデルは，大きく分けると以下の3つであり，モデルによって認証パスの構築の困難性は異なってくる．

- 単純な階層構造をとる階層型モデル
- 相互認証の中継点としてブリッジ認証局を設けるブリッジ認証局型モデル
- 複数の認証局間が相互認証することによって複雑なメッシュ状になっているメッシュ型モデル

2.1.2 認証パスの検証

「認証パスの検証」では，構築された認証パス上の証明書の正当性を確認するため，主に以下の項目を実施する必要がある．

- 証明書のチェーン（信頼鎖）が正しいこと
- 認証パスの最上位証明書が検証者のトラストアンカであること
- 検証対象証明書の証明書ポリシが検証者の受入可能な証明書ポリシに適合していること
- 検証日時が証明書の有効期間内であること
- 証明書が失効されていないこと（有効性確認）
- 認証パス中の証明書が証明書の拡張部分に記載された各種制約条件に違反していないこと

証明書の失効を確認すること以外は，すべてオフラインで処理することが可能である．しかし，認証パスの検証において，与えられた入力が同じでも，検証するアプリケーションによって検証結果が異なってしまっては，検証対象である証明書が有効なものであるかどうかを客観的に判断することができなくなる．そのため，RFC3280 では，検証するアプリケーションがサポートすべき範囲を規定している．しかし携帯電話端末は一般的なパソコン等と比べ，処理速度・メモリ容量・通信速度・通信安定性・バッテリ容量等のモバイル特有の制約がある．そのため，モバイル環境においては，必ずしも RFC3280 において規定されている仕様を実装できるとは限らない．したがって，非力な携帯電話端末においても検証可能な方法を確立する必要がある．

2.2 証明書検証方式

証明書検証方式は，「認証パスの検証」処理中の「有効性確認」の方法の違いや，「認証パスの構築」や「認証パスの検証」を行う主体の違いにより，CRL（Certificate Revocation List）方式[4),5)] や，OCSP（Online Certificate Status Protocol）方式[6)]，CVS（Certificate Validation Server）方式[7),8)] 等に分類できる☆．以下にその概要を示す．

2.2.1 CRL 方式

CRL 方式は，「認証パスの検証」処理中の「有効性確認」を，自らが CRL を参照することで実現する証明書検証方式である．CRL は失効された証明書のシリアル番号の一覧であり，一般的には認証局（Certification Authority: CA）単位で発行・管理される．ある証明書の有効性を確認したい場合，その証明書を発行した認証局のリポジトリから CRL を取得し，CRL 内にその証明書のシリアル番号が記載されているか否かをチェックすることで判断する．

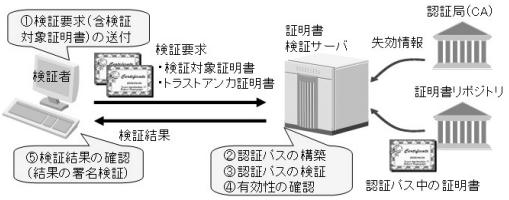

図 1 CVS 方式の概要
Fig. 1 Outline of CVS system.

2.2.2 OCSP 方式

OCSP 方式とは，「認証パスの検証」処理中の「有効性確認」を，OCSP レスポンダとよばれる検証局（Varidation Authority: VA）にオンラインで問い合わせることで実現する証明書検証方式である．要求メッセージとして有効性を確認したい証明書の情報（証明書の ID 等）を送付すると，その応答として，有効（good），失効（revoked），不明（unknown）の 3 つのいずれかが返信される．

2.2.3 CVS 方式

CRL 方式や OCSP 方式には，証明書検証者が認証パスの構築や証明書の検証を行わなければならず，証明書検証者側の負担が大きいといった問題がある．この負担を軽減するために考えられた方式が CVS 方式である．CVS 方式は，本来の証明書の検証者に代わって，認証パスの構築および有効性確認を含めた認証パスの検証を証明書検証サーバが代行する方式である．検証者が，証明書検証サーバに検証対象となる証明書と信頼する認証局の証明書を送付すると，検証対象証明書の正当性を確認した結果が返信される．CVS 方式の概要を**図 1** に示す．本方式に基づいて実装されたシステムとして政府認証基盤（GPKI）[7)] における証明書検証システムが知られており，また，様々な高速化の技術が提案されている[8)~13)]．

2.3 モバイル向け証明書検証技術

OMA WPKI [16)] では，モバイル環境向けの PKI に関する仕様が規定されている．その中で，有効性確認に関しては，端末性能や通信路の帯域幅等の問題があり，CRL 方式や OCSP 方式はモバイル環境の PKI には向いていないため，有効性確認が不要な Short-

☆ このほかに SCVP 方式[14)] があるが，現在ドラフト版のため今回の評価からは除外する．

lived 証明書を利用する方式が提案されている．しかしこの方式では，すでに一般的な X.509 サーバ証明書等で運用を開始しているサービス提供者（サーバ）側のシステム変更を強いるという問題が生じる．また，OMA OCSP Mobile Profile [17] や IETF Lightweight OCSP Profile [18] では，OCSP プロトコルの様々なオプションを制限し，モバイル環境で利用しやすいような OCSP プロファイルを定義している．前者では，たとえば CertID の値のハッシュ計算のアルゴリズムを SHA-1 に限定したり，レスポンスのサイズの最大値を 3,000 バイトに限定したりしている．また，後者では，リクエストにはクライアントの署名をつけないことや，サーバからのレスポンスには拡張領域を含めてはならないこと等が規定されている．どちらのプロファイルも，モバイル環境での証明書の有効性確認を可能にさせようとするものであるが，OCSP 方式では，有効性確認以外の証明書検証に関わる処理は依然として携帯電話端末に実装しなければならないという問題がある．

3. モバイル環境における証明書の有効性確認のモデル

前章で示したように，CVS 方式は証明書の検証に関する大部分の処理を証明書検証サーバが代行する方式であり，非力な携帯電話端末が検証者となるモバイル環境での証明書検証方式に向いていると考えられる．本章では，モバイル環境に CVS 方式に基づいた証明書検証システムを構築する際に，証明書の検証をだれが（携帯電話端末やサービス提供者等）行うのか，検証を行う証明書検証サーバをどこに（通信事業者内や第三者環境等）設置するのかという観点から，証明書の検証モデルの整理を行う．整理した結果を**表 1** に示す．

4. 課題の明確化

今回開発する証明書検証システムは表 1 のすべてのモデルに対応できなければならない．本章では，CVS 方式をモバイル環境に適合させるための課題を明確化する．

4.1 サーバ側（サービス提供者）の課題

モバイル環境では，複数の通信事業者が認証局を設置し，それぞれが独立して証明書を発行する運用が考えられる．その場合，サービス提供者は，携帯電話端末を認証する際に，どの通信事業者の認証局が発行した証明書においてもシームレスに検証できる仕組みが必要となる．

表 1 証明書検証モデルの分類
Table 1 Certificate verification model.

		証明書検証者	
		サービス提供者	携帯端末
証明書検証サーバ設置位置	通信事業者	通信事業者が証明書検証サーバを設置し，サービス提供者が携帯端末の証明書を検証する	通信事業者が証明書検証サーバを設置し，携帯端末がサービス提供者の証明書を検証する
	第三者	第三者が証明書検証サーバを設置し，サービス提供者が携帯端末の証明書を検証する	第三者が証明書検証サーバを設置し，携帯端末がサービス提供者の証明書を検証する

4.2 クライアント側（携帯電話端末）の課題

RFC3280 [5] では，検証するアプリケーションがサポートすべき範囲を規定しているが，非力な携帯電話端末において有効性確認を含む証明書検証の処理を PC と同様に実装することは現実的ではない．さらに，証明書の有効性確認を行う際，検証者側は複数の認証局へのアクセスが必要となり，ネットワークに負荷がかかる．そのため，通信コストの高騰や通信途絶によるサービス中断等，ユーザにとっても通信事業者にとっても大きなデメリットとなるという課題がある．

4.3 通信事業者側の課題

モバイル環境では，各通信事業者がそれぞれ個別に認証局を設置し，自社モバイルサービスの契約者に対して証明書を発行し，解約者等を識別するために CRL を発行すると考えられる．CVS 方式では証明書検証サーバが証明書の有効性確認を行う際に CRL を参照する必要がある．携帯通信事業者に依存しないシームレスな認証基盤を構築するためには，自社の CRL を競合他通信事業者へ提供しなければならない．モバイル環境において，携帯通信事業者の CRL を無条件に公開すると解約者の絶対数や増加率等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 は適切に取り扱う必要がある．

また，携帯電話端末からの証明書の有効性確認要求とサービス提供者からの有効性確認の要求の両方に対応できるような，携帯通信事業者に依らない相互運用性が確保された共通的に利用されうるインフラとならなければならないという課題もある．

5. 実 現 方 式

政府認証基盤 [7] 等で用いられている従来システム [8] を拡張し，前章の課題を解決したモバイル向け証明書検証システムを開発した．開発したシステムの概要を**図 2** に示す．認証相手の証明書を受け取った証明書検証者（携帯電話端末やサービス提供者）が，証明書検証サーバに対して証明書の検証要求を行い検証結果を受け取るシステムである．図 2 に示したモバイル向け証明書検証システムの下記の開発項目に関して次節以降で詳細に述べる．

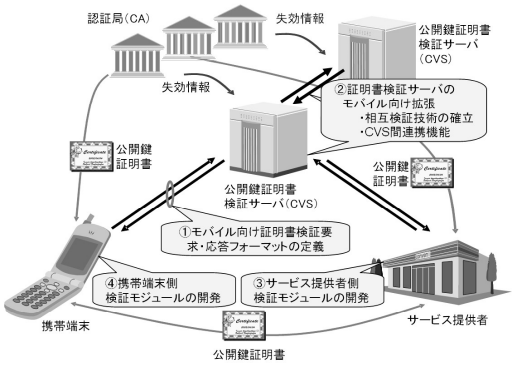

図 2 開発システムの概要
Fig. 2 Outline of developed system.

表 2 検証要求メッセージのフォーマット
Table 2 Request data format.

フィールド	データ型	設定値の例
(OCSP Request)	SEQUENCE	(OCSP要求)
(Extensions)	SEQUENCE SIZE (1..MAX) OF	(拡張群) ※本フィールド階層下には、必要な個数分の拡張が列挙される
(SubscriberCert)	SEQUENCE	(SubscriberCert拡張) ※CVSでは、本拡張は必須項目である
extnValue	OCTET STRING	SubscriberCert拡張の 値 (検証対象証明書)
(IntermediateCerts)	SEQUENCE	(IntermediateCerts拡張) ※CVSでは、本拡張はオプション項目である。また、本拡張は複数指定可能である。複数指定する場合、認証パスのトラストアンカー証明書に近い順に指定する
extnValue	OCTET STRING	応答ステータスを応答者の秘密鍵で署名した値
(TrustAnchorCert)	SEQUENCE	(TrustAnchorCert拡張) ※CVSでは、本拡張はオプション項目である。本フィールドが省略された場合、CVSで設定されているルートCA証明書をトラストアンカーとして処理される
extnValue	OCTET STRING	TrustAnchorCert拡張の 値 (トラストアンカー 証明書)

- モバイル向け証明書検証要求・応答フォーマットの定義
- 証明書検証サーバのモバイル向け拡張
- サービス提供者側の検証モジュールの開発
- 携帯電話端末側の検証モジュールの開発

5.1 モバイル向け証明書検証要求・応答フォーマットの定義

証明書検証要求フォーマットや証明書検証プロトコル等，モバイル環境に適した方式の検討を行い，できるだけサイズを小さくするために冗長なデータを省いたモバイル向けの証明書の有効性確認要求・応答フォーマットを定義した．検証者が証明書検証サーバに対して送信する要求メッセージを**表 2** に，証明書検証サーバが検証者に対して返信する応答メッセージを**表 3** に示す．表 3 のハッチングの項目は証明書検証サーバのポリシにより省略可能であることを示している．

なお，検証要求プロトコルとしては，現状の多くの携帯電話端末でサポートされている HTTP プロトコルの POST メソッドを用いることで実現した．

表 3 検証応答メッセージのフォーマット
Table 3 Response data format.

フィールド	データ型	設定値の例
(OCSP Response)	SEQUENCE	(OCSP応答)
responseStatus	ENUMERATED	応答ステータス ※以下のいずれかの 値が 記載される。 successful(0) malformedRequest(1) internalError(2) tryLater(3) sigRequired(5) unauthorized(6)
signatureAlgorithm	SEQUENCE OPTIONAL	(署名アルゴリズム)()
algorithm	OBJECT IDENTIFIER	署名アルゴリズムのオブジェクト識別子
Parameters	ANY	署名アルゴリズムに 必要なパラメータ
signature	BIT STRING	応答ステータスを応答者の秘密鍵で署名した値
certs	[0]EXPLICIT OPTIONAL	(証明書群)
(-)	SEQUENCE OF	(証明書群) ※本フィールドの階層下には、署名検証に必要な認証パス中の証明書が格納される
(Certificate)	Certificate	上記署名値の 検証に必要な公開鍵証明書
:	:	:

表 4 開発した証明書検証サーバの機能
Table 4 Functions of certificate validation server.

機能	説明
通信制御機能	証明書検証要求の受信，証明書検証応答の送信を行う．なお，モバイル向けプロトコルと CVS プロトコルを適切に振り分ける機能を有する．
証明書検証フォーマット解析生成機能	証明書検証要求フォーマットデータを解析し，取得した検証要素を基に証明書検証制御機能を実行する．また，証明書検証制御機能から返却された検証結果を基に，証明書検証応答フォーマットデータを生成する．
証明書検証制御機能	自検証サーバ内で証明書の検証を行うか，あるいは，他証明書検証サーバへ検証要求を行うかの制御を行う．
認証パス構築・検証機能	検証対象証明書からトラストアンカ証明書までの認証パスを構築し，証明書検証を実行する．
モバイル向けプロトコルの解析生成機能	モバイル向けプロトコルと CVS プロトコルの相互接続を行う．

5.2 証明書検証サーバのモバイル向け拡張

「モバイル向け証明書検証サーバ」に関しては，複数の認証局が発行した証明書に対し，検証するために必要な認証パスの構築を行う機能，非力な携帯電話端末に代わり RFC3280 に則した認証パスの検証を行う機能，多数の認証局へのアクセスを代行し検証対象の証明書および認証パスを構成するすべての証明書の有効性検証を行う機能，他の携帯通信事業者が運営する証明書検証サーバと連携する機能を実現したモバイル向け証明書検証サーバを開発した．検証サーバのモジュール機能一覧を**表 4** に示す．また，表 4 のモジュール機能の関係図を**図 3** に示す．なお，CVS プロトコルとは，政府認証基盤（GPKI）[7] 等で用いら

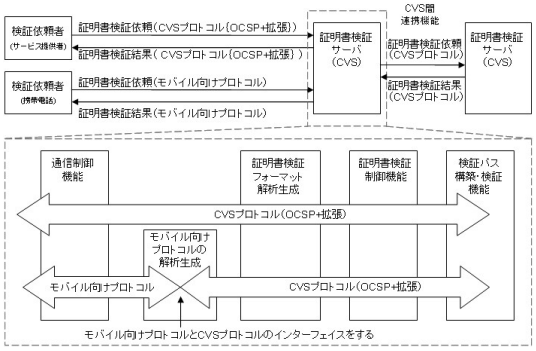

図 3 モジュール関係図
Fig. 3 Relations between modules.

れている従来技術としての CVS 方式による証明書検証要求・応答プロトコルを指す．このように従来システムにモバイル向けプロトコル解析・生成機能を付加することでモバイル環境においてもインターネット環境においてもシームレスに機能する証明書検証サーバを開発した．

以下の項で，モバイル向けプロトコルの解析生成機能に関して，モバイル向け証明書検証要求の受信機能および送信機能の詳細を述べる．さらに，他の証明書検証サーバとの連携を制御する証明書検証制御機能の詳細を述べる．

5.2.1 モバイル向け証明書検証要求の受信機能

本機能は，モバイル向けプロトコルと CVS プロトコルの証明書の検証要求に関する相互接続を行う．証明書の検証要求を以下の手順で処理する．

- モバイル向けプロトコルの通信ヘッダを受信（通信制御機能）
- モバイル向けプロトコルの検証要求データを取得（通信制御機能）
- 取得したデータを CVS プロトコルの検証要求へ変換（モバイル向けプロトコルの解析生成機能）

図 4 にモバイル向け証明書検証要求の受信機能の処理フローの詳細を示す．

5.2.2 モバイル向け証明書検証結果の送信機能

本機能は，モバイル向けプロトコルと CVS プロトコルの証明書の結果応答に関する相互接続を行う．証明書の結果応答は以下の手順で処理する．

- 証明書検証結果を CVS プロトコルの検証結果形式で受け取る（証明書検証フォーマット解析生成機能）．
- 取得したデータをモバイル向けプロトコルの検証結果へ変換（モバイル向けプロトコルの解析生成機能）．

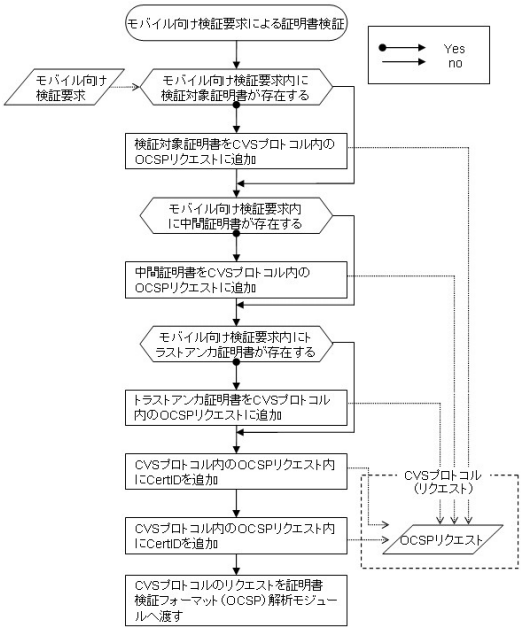

図 4 検証要求処理フロー
Fig. 4 Request flow.

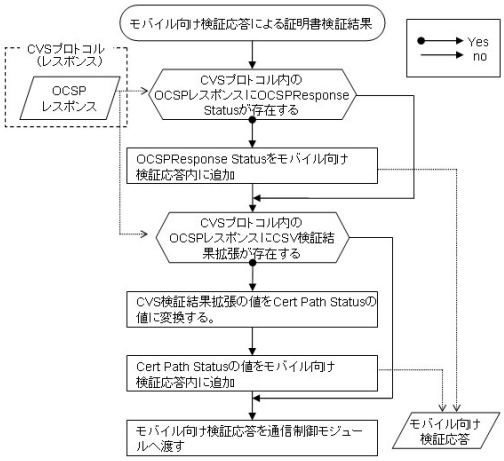

図 5 結果応答処理フロー
Fig. 5 Response flow.

- モバイル向けプロトコルの検証結果データを送信（通信制御機能）．

図 5 にモバイル向け証明書検証結果の送信機能の処理フローの詳細を示す．

5.2.3 証明書検証制御機能

CRL を携帯通信事業者間で共有しないための CVS 連携機能について記述する．表 4 の証明書検証制御機能において，自検証サーバ内で検証を行うか，あるいは，他検証サーバへ検証要求を行うかの制御を行う．具体的には，検証対象証明書中の ISSUER から該当

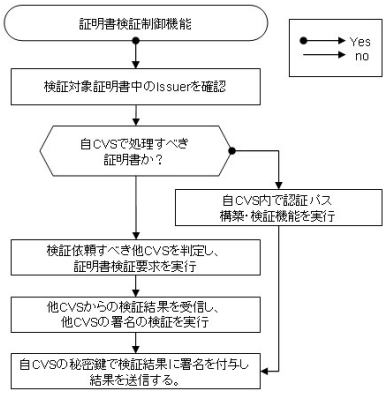

図 6 CVS 連携処理フロー
Fig. 6 CVS relation flow.

表 5 携帯電話端末用ブラウザの開発ステップ数
Table 5 Step count of developed web browser.

対象	ステップ数 [行]
ブラウザ全体	1,671
検証モジュール部	580

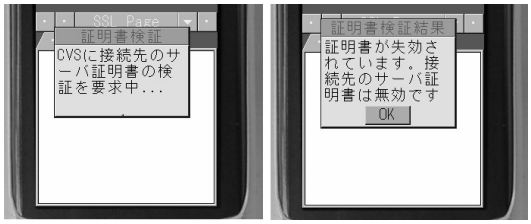

図 7 証明書検証モジュールを組み込んだ携帯用ブラウザ
Fig. 7 Mobile browser with certificate verification module.

する他 CVS を判断し，新たに CVS リクエストを生成し，送信する．他 CVS へのリクエストを行う場合は，自 CVS では認証パスの構築や検証は実行されない．**図 6** に処理フローの詳細を示す．

5.3 サービス提供者側の検証モジュールの開発

「サービス提供者側の検証モジュール」については，SSL ハンドシェーク時に，携帯電話端末から提示された証明書の有効性確認を証明書検証サーバへ問い合わせるモジュールを実装した☆．また，複数の通信事業者が認証局および証明書検証サーバをそれぞれ独立に設置するモデルにおいては，携帯電話端末から受け取った各証明書を各通信事業者の証明書検証サーバに適切に振り分ける必要が生じるため，本開発では，サービス提供者側の検証モジュールにおいて各証明書の検証要求を適切に振り分ける機能も実現した．

5.4 携帯電話端末側の検証モジュールの開発

「携帯電話端末側の検証モジュール」については，処理速度・通信速度等のモバイル特有の制約を考慮する必要があるため，非力な携帯電話端末上で動作する検証モジュールを開発した．具体的には，5.1 節で示したように，証明書の検証に必要な最低限の情報をモバイル向け検証要求フォーマットとし，証明書検証サーバにアクセスする機能を有する携帯電話端末用ブラウザを開発した．**表 5** に開発した携帯電話端末用の証明書検証機能付ブラウザのステップ数を示す☆☆．このように，検証機能の大部分をサーバ側で処理するため携帯電話端末への実装は容易になる．

図 7 に携帯電話端末での証明書検証モジュールの動作画面を示す．ブラウザに組み込み，SSL 認証時に証明書検証サーバへの問合せを行う．検証結果には証明書検証サーバの署名が付与されており，携帯電話端末でその署名を検証することにより，検証結果の正当性を確認することができる．

6. 評　　価

6.1 実測値の評価

クライアントとして CDMA 1x WIN 規格の携帯電話端末（BREW 端末）およびサーバとして CPU に Intel(R) Pentium(R) 4 プロセッサ 3.4 GHz，メモリ 2 GB，OS に Windows(R) XP operating system を搭載したコンピュータで実装したモバイル向け証明書検証サーバの性能評価を行った．

表 6 に，サーバの処理時間，および携帯電話端末における証明書有効性確認要求の開始から確認結果の受信終了までのレスポンス時間を示す．ただし CRL の取得時間および携帯電話端末内での検証結果の署名検証時間は含まれない．また，証明書検証要求データサイズは，検証対象証明書サイズが 675 [byte]，トラストアンカ証明書サイズが 569 [byte]，その他のデータが 5 [byte] の計 1,249 [byte] である．なお，表 6 は 100 回の計測の平均値である．このように，通信時間を含む証明書検証のレスポンス時間を 1 秒未満に抑えることができた☆☆☆．

6.2 安全性の評価

本節では，開発した証明書検証システムの安全性評価について述べる．

☆ 具体的には Apache へ SSL 機能を追加する mod_ssl モジュールに証明書検証サーバへの問合せ機能を追加した．

☆☆ ただしレンダリングエンジン等のコア機能としてのライブラリ化されている部分は含まない．

☆☆☆ ただし今回の計測には証明書検証サーバの負荷は考えていない．実際には負荷分散の機能を有しているので検証要求の頻度が高くなった場合でも適切に多重化することで今回の実測値に近づけること可能である．

表 6 レスポンス時間の実測値
Table 6 Measurement value of response time.

処理内容	時間 [ms]
サーバの処理時間	28
携帯電話端末におけるレスポンス時間	907

表 7 送信データの偽装，改ざんへの対処
Table 7 Method for preventing attack on transmission data.

方式	偽装，改ざんへの対処方法
CRL 方式	CRL へ付与された署名の検証
OCSP 方式	OCSP レスポンスへ付与された署名の検証
提案システム	CVS レスポンスへ付与された署名の検証

6.2.1 通信中の検証結果の完全性

証明書検証サーバが検証結果を検証クライアントへ返信する際に，検証結果に証明書検証サーバの秘密鍵を用いて署名を付与するようにした．また，検証クライアントに自身が検証を要求する証明書検証サーバの証明書をあらかじめ登録しておき，検証結果に付与されている署名を検証するようにした．これにより，証明書検証サーバ–検証クライアント間の通信中に検証結果が改ざんされても，検証クライアントは改ざんを検知することができる．**表 7** に各方式の送信データの偽装，改ざんへの対処方法を示す．このように提案システムにおける送信データの安全性は他方式と同等であるといえる．

6.2.2 CRL 非公開方式の実現

証明書検証サーバに証明書検証サーバ間連携機能を設け，通信事業者が CRL を公開しなくても，他通信事業者あるいは第三者設置の証明書検証サーバで通信事業者が発行した携帯電話端末の証明書を検証することを可能とする方式（CRL 非公開方式）を実現した．

CRL 非公開方式では，他 CVS へ検証要求を行う CVS（以降 CVS_1）と，CVS_1 から要求を受ける CVS（以降 CVS_2）の間で通信が発生するため検証結果の改ざん等が行われる可能性がある．そのため，CVS_2 が CVS_1 へ検証結果を返信する際に，検証結果に署名を付与し，CVS_1 においてその署名を検証するようにした．これにより CVS 間の通信中に検証結果が改ざんされても検知することができる．しかし，CVS_1 が，CVS_2 の署名付きの検証結果を検証クライアントへ返信すると，CVS_2 の存在に感知しない検証クライアントはその署名を検証できない．そのため，CVS_1 において，自身の秘密鍵を用いて検証結果に署名を付与しなおすようにした．これにより，検証クライアントへすべての CVS の証明書を登録しなくても，自身が検証を要求する CVS（この場合は CVS_1）の証明書のみ登録しておけば，検証結果に付与されている署名を検証することができるようになった．

表 8 CRL 公開の必要性
Table 8 Necessity of exposing CRL.

方式	CRL 公開の必要性
CRL 方式	検証者（クライアント）に公開される
OCSP 方式	検証者には公開されないが VA に公開される
提案システム	検証者にも VA にも公開されない

本方式により，通信事業者は解約者情報等を含む CRL を他者に対して開示する必要がなくなった．**表 8** に示すように，従来方式に比べて提案方式が優れているといえる．

6.3 利便性の評価

6.3.1 携帯通信事業者に依存しない認証基盤の実現

サービス提供者は，クライアントとしての携帯電話端末がどの通信事業者の端末でも今回開発したサービス提供者側検証モジュールが適切に検証サーバに振り分けるので通信事業者ごとの証明書の差異を意識することなく，適切に証明書の検証が行え，サービス提供に注力することができるようになった．

6.3.2 ユーザの利便性

携帯電話端末のユーザは，特別なソフトウェアを起動する必要なく，SSL 通信のネゴシエーション時に意識せずに証明書の厳密な検証が行われるので，携帯電話端末ユーザの利便性を損ねることはないといえる．また表 6 より，携帯電話端末からの証明書検証のレスポンス時間は 1 秒未満であるので，体感的にも許容範囲に抑えることができた．

7. まとめと今後の課題

証明書の検証モデルの整理を行い，モバイル特有の制約を考慮した証明書検証システムを開発した．また，開発したシステムの実測値を評価するとともに安全性および利便性の評価を行った．

本開発の成果として，携帯電話端末と，モバイル網/インターネット網で構築されるサービス提供者のセキュアな相互認証を実現することができるようになった．具体的には，サービス提供者にとっては複数の携帯通信事業が発行した証明書をシームレスに検証できるようになった．また，携帯通信事業者にとっては CRL を他社に公開せずに他社の携帯電話端末の証明書を検証でき，かつ，携帯電話端末からの検証要求もサービス提供者からの検証要求も同一サーバで処理できるようになった．さらに携帯電話端末ユーザにとっては，サービス提供者が提示する証明書を厳密に検証することは，不正なサービス提供者を見極めるうえで重要で

あるにもかかわらず，非力な携帯電話端末では困難であったが，本開発の成果により携帯電話端末側での証明書の厳密な検証を実現することができた．このようにモバイル環境特有の制約を考慮したモバイルセキュリティ認証基盤が構築でき，利用者およびサービス提供者は利用する携帯通信事業者網によらず，共通的でセキュアなモバイルサービスを享受・提供することができるようになった．

今後は本認証基盤をもとに，様々な属性情報を扱えるモバイル向け属性認証基盤の研究開発に取り組む予定である．

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．

商標等に関する表示

参 考 文 献

1) 梅澤，高橋，内山，坂崎，笈川，洲崎，平澤：モバイル向け証明書検証サーバの開発，電子情報通信学会技術報告（IT），pp.49–54 (2005/9).
2) 梅澤，高橋，内山，坂崎，笈川，洲崎，平澤：モバイル向け証明書検証システムの開発と評価，コンピュータセキュリティシンポジウム 2005 論文集，pp.121–126 (2005/10).
3) 梅澤，笈川，洲崎，平澤：モバイル向け証明書検証方式の評価，第 28 回情報理論とその応用シンポジウム，予稿集，pp.587–590 (2005/11).
4) ITU-T Recommendation X.509 (2000) ISO/IEC 9594-8:2001: Information Technology — Open Systems Interconnection — The Directory: Public-key and Attribute Certificate Framework (2000).
5) Housley, R., Polk, T., Ford, W. and Solo, D.: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 3280, IETF (Apr. 2002).
6) Myers, M., Ankney, R., Malpani, A., Galperin, S. and Adams, C.: X.509 Internet Public Key Infrastructure — Online Certificate Status Protocol - OCSP, RFC 2560, IETF (June 1999).
7) 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．
8) 藤城，鍛，羽根，熊谷，手塚，証明書検証サービスの開発，電子情報通信学会論文誌 D-I，Vol.J87-D-I, No.8 (2004).
9) 羽根，藤城，橋本，手塚：X.509 証明書の高速認証パス検証アルゴリズム，情報処理学会コンピュータセキュリティ研究会研究報告書，Vol.2005, No.33, pp.55–60 (2005).
10) Hane, S., et al.: Speeding up X.509 Certificate Path Validation, *4th International Workshop for Applied PKI*, *IWAP2005* (2005).
11) 藤城，鍛，手塚：複数 PKI ドメインにおける証明書検証の高速化方式の研究，コンピュータセキュリティシンポジウム 2002, pp.373–378 (2002).
12) 藤城ほか：政府認証基盤（GPKI）における証明書検証方式の提案，電子情報通信学会技術研究報告，OFS 2001-78〜82, pp.19–24 (2001).
13) 橋本，藤城，鍛，羽根，手塚：証明書検証サービスにおける認証パスキャッシュ方式の開発，情報処理学会コンピュータセキュリティ研究会研究報告書，Vol.2005, No.70, pp.295–300 (2005).
14) Fressman, T., Housley, R., Malpani, A., Cooper, D. and Polk, T.: *Simple Certificate Validation Protocol* (*SCVP*), IETF (July 2005).
15) 梅澤，笈川，洲崎，手塚：モバイル環境での証明書検証方式の評価，電子情報通信学会論文誌 D, Vol.J90-D, No.2 (2007)（予定）．
16) WAP-217-WPKI Version 24-Apr-2001 Wireless Application Protocol Public Key Infrastructure Definition, Wireless Application Protocol Forum, Ltd. (2001)
17) Online Certificate Status Protocol Mobile Profile Candidate Version V1.0, Open Mobile Alliance Ltd. (2004)
18) Deacon, A. and Hurst, R.: Lightweight OCSP Profile for High Volume Environments, IETF PKIX Working Group Internet Draft (2006).

(平成 18 年 5 月 12 日受付)
(平成 18 年 11 月 2 日採録)

梅澤 克之（正会員）

1996 年早稲田大学大学院理工学研究科機械工学専攻修士課程修了．同年（株）日立製作所システム開発研究所入所．以来，分散オブジェクトシステム，モバイルセキュリティ技術，スマートカードセキュリティ技術等の研究・開発に従事．電気学会会員．

笈川　光浩（正会員）

1998 年上智大学大学院理工学研究科電気・電子工学専攻博士前期課程修了．同年（株）日立製作所システム開発研究所入所．以来，セキュリティ技術の研究・開発，特に電子認証の研究・開発に従事．

洲崎　誠一（正会員）

1991 年横浜国立大学工学部電子情報工学科卒業．同年 4 月（株）日立製作所システム開発研究所に入所．以来，情報セキュリティ技術の研究開発に従事．工学博士．1996 年情報処理学会第 52 回全国大会優秀賞，平成 12 年度山下記念研究賞受賞．

手塚　　悟（正会員）

1984 年慶應義塾大学工学部数理工学科卒業．同年（株）日立製作所マイクロエレクトロニクス機器開発研究所を経て，現在，システム開発研究所セキュリティシステム研究センタ勤務．パーソナルコンピュータのオペレーティング・システム，デバイス・ドライバ，LAN システムの研究を経て，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．

平澤　茂一（正会員）

1961 年早稲田大学理工学部数学科卒業．1963 年同電気通信学科卒業．同年三菱電機（株）入社．1981 年早稲田大学理工学部工業経営学科（現経営システム工学科）教授．現在に至る．情報理論とその応用，データ伝送方式，ならびに計算機応用システムの開発等の研究に従事．工学博士．1979 年 UCLA 計算機科学科客員研究員．1985 年ハンガリー科学アカデミー，1986 年伊トリエステ大学客員研究員．1993 年電子情報通信学会小林記念特別賞，業績賞受賞．1997 年 IEEE Fellow，2001 年電子情報通信学会フェロー，情報理論とその応用学会，人工知能学会，ACM 等各会員．