The 29th Symposium on Information Theory
and its Applications (SITA2006)
Hakodate, Hokkaido, Japan, Nov. 28 - Dec. 1, 2006

モバイル向け属性証明書検証システムの開発

Development of an attribute certificate validation system in mobile environments

梅澤 克之*† 笈川 光浩† 小林 賢† 平澤 茂一*
Katsuyuki Umezawa Mitsuhiro Oikawa Ken Kobayashi Shigeichi Hirasawa

Abstract—
A common authentication infrastructure that is avairable for all service providers and users is necessary for improving security and interoperability of mobile services. Not only the ID authentication but also a variety of attribute authentications make the user convenient. In this report, we propose an attribute certificate validation system for mobility. The system 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 of the system.

Keywords— Mobile, PKI, Attribute Certificate, Verification, CRL, OCSP, CVS

1 はじめに

近年，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セキュア基盤の構築が必須と考えられる．具体的には，モバイル網がインターネットに接続されることによって生じる可能性のある網内・網間を流れるデータの偽造・改ざんを防止する技術や，携帯電話端末の処理速度，メモリ容量，通信速度，通信安定性等のモバイル特有の制約を解決するためにモバイル特有のセキュリティ技術の実現が必要であると考えられる．さらに，これらのセキュリティ対策は，各携帯通信事業者が独自に取り組むのではなく，相互運用性が確保された共通的に利用され得るインフラとならなければならない．

こうした状況を踏まえ，利用者およびサービス提供者が，利用するモバイル網によらず，相互運用性が確保された共通的でセキュアなモバイルサービスを享受・提供するためのモバイルセキュリティ基盤の開発を（株）NTTドコモ，（株）日立製作所，日本電気（株），（株）KDDI研究所の4社コンソーシアムによって実施している．

本稿では，携帯電話端末を用いたモバイル通信情報サービスにおいて，属性証明書を用いてサービス提供者の資格や属性を正しく判断するための属性証明書検証技術について報告する．

以下では，まず，2章で従来技術として属性証明書の一般的な検証技術について記述する．3章で今回開発したモバイル向け属性証明書検証システムについて記述し，4章で性能を評価する．そして最後に5章でまとめと今後の課題を示す．

2 属性証明書検証技術

情報通信サービスにおいて，利用者およびサービス提供者の存在のみを確認するだけでは十分対応できないケースが考えられる．そのため，権限や権利等の属性情報を認証する仕組みが必要である．属性証明書 (以降 AC) を用いて通信相手の属性を確認するためには，公開鍵証明書 (以降 PKC) と同様に AC 検証が必須となる[1]．AC を検証するための手順は，ITU-T X.509(2000) [1] や RFC3281 [2] にて規定されているように，大別して「AC の内容の正当性の検証」「正当な AC 保有者であることの検証」の2つである．

2.1 AC の内容の正当性の検証

「AC の内容の正当性の検証」では，以下の処理を行う必要がある．(以下，PKC の発行機関を CA，AC の発行機関を AA と記す.)

- 保有者の AC に付与されている AA の署名を検証
- AA の PKC に付与されている CA の署名を検証
- CA の PKC が，自身の信頼している CA の PKC であるかどうかを確認
- AA の PKC が失効されていないことを確認
- 保有者の AC が失効されていないことを確認

2.2 正当な AC 保有者であることの検証

前節の処理によって，AC の内容の正当性を確認することができる．しかし，AC 自体は，AC 保有者以外の人でも入手することが可能であり，相手が本当に AC 保

* 〒169-8555 東京都新宿区大久保 3-4-1，早稲田大学大学院理工学研究科，Graduate School of Science & Engineering, Waseda University, 3-4-1 Okubo Shinjuku-ku Tokyo, 169-8555 Japan.
† 〒212-8567 神奈川県川崎市幸区鹿島田 890 日立システムプラザ，(株) 日立製作所 システム開発研究所，Hitachi Ltd., Systems Development Laboratory, Hitachi System Plaza Shinkawasaki, 890 Kashimada, Saiwai-ku, Kawasaki-shi, Kanagawa, 212-8567 Japan.

[1] PKC の検証に関しては，筆者らはモバイル環境向けの PKC 検証サーバ (CVS)[3][4][6] を開発済みである．

有者であるかどうかを判断することはできない．そこでACを提示してきた相手が，正当なAC保有者であるかどうかを確認する．「正当なAC保有者であることの検証」は，具体的に以下の処理を行う必要がある．

- 署名データに付与されている保有者の署名を検証
- 保有者のACが指し示すPKCが，保有者のPKCであることを確認
- 保有者のPKCに付与されているCAの署名を検証
- CAのPKCが，自身の信頼しているCAのPKCであるかどうかを確認
- 保有者のPKCが失効されていないことを確認

3 モバイル向け属性証明書検証システム

前章に示したように，「ACの内容の正当性の検証」と「正当なAC保有者であることの検証」を行うためには，AAおよびAC保有者のPKCの検証・有効性確認を行い，さらに保有者のACの有効性確認を行う必要がある．

モバイル環境において，携帯電話端末がAC保有者となる場合には，PKCは携帯通信事業者が発行することが想定されるが，ACは会員制サービスを行うサービス提供者が属性を付与するなど，第三者が属性認証局を運営することが考えられる．通信事業者を含め複数の属性認証局がAC発行する複雑なモデルにおいても，正しく相互に認証しあうためにはACを検証する技術は必要不可欠である．

また，サービス提供者サーバがAC保有者となる場合には，ACの検証はPKCに比べて更に複雑な処理を要するため，非力な携帯電話端末において効率良くACを検証する方法が求められている．

上記状況を鑑み，図1に示すように，AC検証者に代わって有効性確認を含むACの厳密な検証を効率的に実現するモバイル向けAC検証サーバを開発した[6]．本稿では，図1における「検証者」が，携帯電話端末となる場合の検証者側モジュール（AC検証クライアント）についての概要を示す．

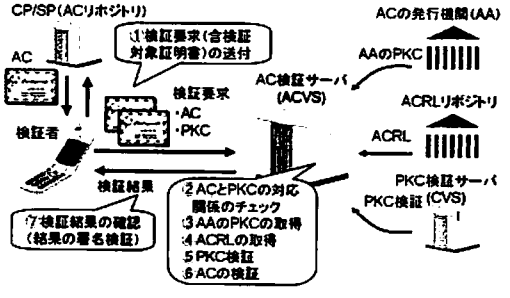

図 1: モバイル環境におけるAC検証システム構成図

3.1 携帯電話端末向けAC検証クライアントの機能

「携帯電話端末側の検証モジュール」については，処理速度・メモリ容量・通信速度・通信安定性・バッテリー容量等のモバイル特有の制約を考慮する必要がある．そのため，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．本モジュールでは，署名を検証する機能および属性証明書検証サーバにアクセスする機能を実現した．表1に携帯電話端末側の検証モジュールの機能を示す．

表 1: 携帯電話端末側の検証モジュールの機能

機能	説明
CP/SP接続	サービスを利用するために，サービス提供者（CP/SP）に接続する．このとき，通信路での盗聴を考慮し，SSLサーバ認証によるSSL暗号通信を行う．
PKC取得	利用するCP/SPのSSLサーバ証明書(PKC)を取得する．
PKC検証	利用するCP/SPのSSLサーバ証明書(PKC)の検証を行う．携帯電話端末は，PKC検証サーバ(CVS)にPKCを送信し検証要求を行う．CVSは検証結果にデジタル署名を付加して携帯電話端末に返却する．
AC取得	利用するCP/SPのサービスに対応した属性証明書(AC)を取得する．
AC検証	利用するCP/SPのサービスに対応した属性証明書(AC)の検証を行う．携帯電話端末は，AC検証サーバ(ACVS)にPKCとACを送信し検証要求を行う．ACVSは検証結果にデジタル署名を付加して携帯電話端末に返却する．

3.2 モバイル向けAC検証要求・応答フォーマットの定義

図2，3に，モバイル網を利用して携帯電話端末とAC検証サーバとの間で送受信される検証要求・応答フォーマットを示す．本フォーマットに関しては，モバイル環境に適した方式の検討を行い，ACの検証に必要な最低限の情報（PKCとAC，および各証明書のバイト数）を含むモバイル向けフォーマットを定義した．ここで，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(S)プロトコルのPOSTメソッドを用いることで実現した．なお，応答者のなりすましやセッションのすりかえ，メッセージの改ざん等の不正を防止するためには既存のSSL/TLS等の技術を用いて適切なセッション管理を行なう必要がある．

証明書の数 (1byte)	ACの長さの上位8bit (1byte)	ACの長さの下位8bit (1byte)	PKCの長さの上位8bit (1byte)	PKCの長さの下位8bit (1byte)	AC (DER)	PKC (DER)

図 2: モバイル向け検証要求フォーマット

検証リターンコード (1byte)	検証リターンコードとHTMLソースのハッシュ値 (128byte)	属性および属性値を表すHTMLソース (可変長)

図 3: モバイル向け検証応答フォーマット

また，図 3 に示した「属性および属性値を表す HTML ソース」は，携帯電話端末内で AC を解析し属性および属性値を抽出する代わりに検証サーバ側で代行し，抽出された属性および属性値を携帯電話端末に返されたものである．例を図 4 に示す．

```
<html>
<head>
<title>属性証明書内容確認</title>
<meta http-equiv="Content-Type"
content="text/html; charset=Shift_JIS">
</head>
<body>
<font size="6">属性内容確認</font><hr>
<font size="5">発行者情報:</font><br>
【発行者の属性値】<br>
<hr>
<font size="5">有効期間:</font><br>
【開始期間】<br>
から<br>
【終了期間】<br>
<hr>
【属性1】:<br>
【属性値1】<br><hr>
【属性2】:<br>
【属性値2】<br><hr>
...
</body>
</html>
```

図 4: 属性および属性値を表す HTML ソースの例

3.3 携帯電話端末がサービス提供者（CP/SP）の AC を検証する場合のシーケンス

図 5 に携帯電話端末がサービス提供者 (CP/SP) サーバにアクセスし，CP/SP サーバの AC を検証する場合のシーケンス図を示す．

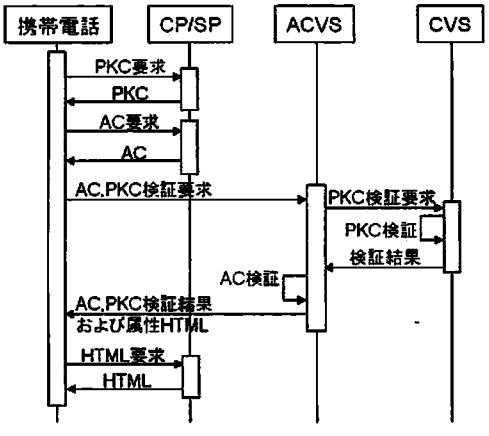

図 5: 携帯電話端末が AC を検証する場合のシーケンス図

まず，携帯電話端末がサービス提供者（CP/SP）を利用するために SSL 通信の要求を行う．携帯電話端末は，メモリ上に保有しているルート証明書と CP/SP の PKC が正しければ SSL 通信を行う．SSL のセッション確立の直前に携帯電話端末は AC を要求し，CP/SP は提供するサービスに対応した AC を携帯電話端末に送信する．携帯電話端末は，ACVS に対して AC と PKC を送信し検証要求を行なう．ACVS は PKC の検証に関しては CVS に検証依頼し，その後自ら AC 検証を行い AC と PKC の検証結果を携帯電話端末に返信する．携帯電話端末は，ACVS から受け取った検証結果のデジタル署名の確認を行う．その後，結果とともに通知された属性値を画面に表示し，携帯電話端末のユーザに確認を促した後，HTML を表示する．

3.4 携帯電話端末の画面遷移図

図 6 に携帯電話端末がサービス提供者 (CP/SP) の AC を検証する際の画面遷移を示す．

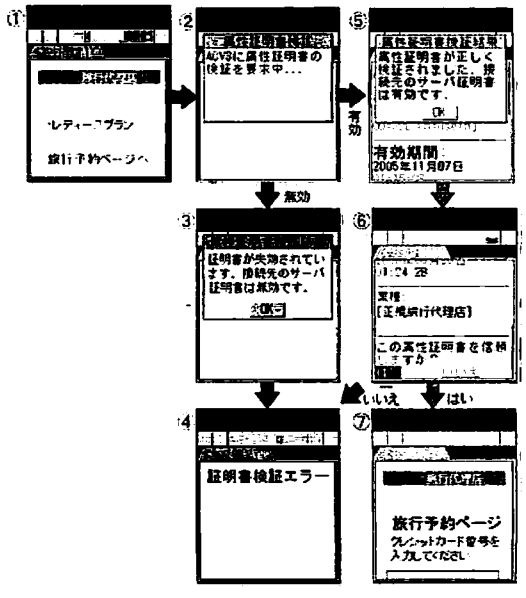

図 6: 携帯電話端末の画面遷移図

今回の例は携帯電話端末で仮想の旅行代理店にアクセスする例である．まず，携帯電話端末で旅行代理店にアクセスし，「旅行予約ページへ」のリンクを選択する (図 6①)．「旅行予約ページへ」のリンクには図 7 に示す形式で旅行代理店の AC が関連付けられている．携帯電話端末は AC を取得し，その AC を ACVS に送信し検証要求を行なう (図 6②)．検証に失敗するとその旨を表示し (図 6③)，終了する (図 6④)．検証に成功するとその旨を表示し (図 6⑤)，旅行代理店の属性が表示される (図 6⑥)．ユーザは，表示された属性を確認することで相手の正しさを判断し，次のステップに進む（図 6⑦）．

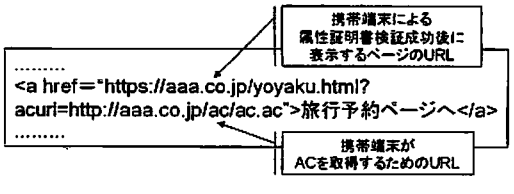

図 7: AC を指定するリンクの設定例

4 性能評価

本節では，携帯電話端末からの AC 検証要求に基いて ACVS が AC 検証をを行なう場合の性能評価を行う．

4.1 性能測定対象システムの構成

図 8 に性能測定を行うシステムの概略図を示す．ここで，ACVS は携帯電話端末からの検証要求を受け取る窓口機能，バックエンドの属性認証局 (AA) や PKC 検証サーバ (CVS) 等と連携して実際に AC の検証を実行する機能を有する．AC リポジトリは，携帯電話端末からの要求に基づいて AC を提供するサーバである．

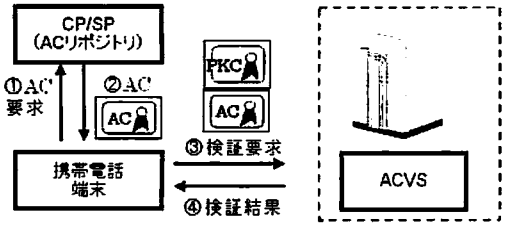

図 8: 性能測定対象システムの構成図

性能評価で用いた AC リポジトリおよび ACVS を構成する機器構成を表 2 に示す．なお，携帯電話端末は，CDMA 1x WIN 規格 (通信速度下り 2.4[Mbps]，上り 144[kbps](理論値)) の BREW 端末である．また，携帯電話端末・AC リポジトリ間および携帯電話端末・ACVS 間は，携帯電話網を経由した HTTP 通信である．

表 2: 性能測定対象システム構成機器

	AC リポジトリ	ACVS マシン
CPU	Intel(R) Pentium(R)III 700MHz	Mobile Intel(R) Pentium(R)4 3.4GHz
メモリ	256M Byte	2040M Byte
HDD	10GB	80GB

4.2 性能測定項目

今回の性能測定では表 3 に示す 2 項目の性能測定を行った．

表 3: 性能測定項目

測定項目	説明
(1) 携帯電話端末・AC リポジトリ間	携帯電話端末が AC リポジトリに対して AC 要求 (図 8①) を開始してから AC の受信 (図 8②) が完了するまでの時間を計測
(2) 携帯電話端末・ACVS 間	携帯電話端末が AC 検証要求 (図 8③) を開始してから，結果 (図 8④) の受信および結果の署名検証が完了するまでの時間を計測

4.3 評価結果

前節の測定項目の測定結果を表 4 に示す．なお，結果は 100 回測定した平均値である．AC 検証で 2 秒以内，AC 取得も含めて 3 秒以内を実現した．

表 4: 性能測定結果

測定項目	測定結果 [ms]
(1) 携帯電話端末・AC リポジトリ間	471
(2) 携帯電話端末・ACVS 間	1941

5 まとめと今後の課題

モバイル向け AC 検証システムにおける携帯電話端末側の検証モジュールを開発し，性能を評価した．本システムにより今まで不可能であった携帯電話端末でサービス提供者の属性情報を確認することができるようになった．

今後は，今回開発した属性証明書検証システムを基盤として用いることによりサービスの安全性や利便性が向上することを実験を通して実証していく予定である．

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」の一環として行なわれた．

参考文献

[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] S. Farrell, and R. Housley: *RFC 3281 - An Internet Attribute Certificate Profile for Authorization*, IETF, April 2002.

[3] 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)，p.p.49–54, 2005/9.

[4] 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，p.p.121–126, 2005/10.

[5] 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，p.p.587–590, 2005/11.

[6] 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，” コンピュータセキュリティシンポジウム 2006 論文集，2006/10 (予定)．