モバイル向け属性証明書検証サーバの開発
モバイルセキュリティ基盤技術の研究開発 V

梅澤 克之†‡　高橋 礼†　内山 宏樹†　坂崎 尚生†　笈川 光浩†
小林 賢†　平澤 茂一‡

†(株) 日立製作所 システム開発研究所
212-8567 神奈川県川崎市幸区鹿島田 890 日立システムプラザ新川崎

{katsuyuki.umezawa.ue, aya.takahashi.uh, hiroki.uchiyama.tm,
hisao.sakazaki.qc, mitsuhiro.oikawa.hn, ken.kobayashi.kj}@hitachi.com

‡ 早稲田大学大学院理工学研究科
169-8555 東京都新宿区大久保 3-4-1

{ume,hirasawa}@hirasa.mgmt.waseda.ac.jp

あらまし モバイル環境における異なる携帯通信事業者間の電子証明書の相互認証・相互検証技術，携帯電話端末のセキュリティ機能を代行するモバイルサービス代行技術，モバイル環境での利用者の属性情報の安全で適切な利用技術等の研究開発を，(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．筆者らは，携帯電話端末等を用いたモバイル情報通信サービスにおいて属性証明書を厳密に検証できるモバイル向け属性証明書検証サーバを開発した．本稿では開発した検証サーバの概要を示し性能評価を行なう．

Development of an attribute certificate validation server in mobile environments

Katsuyuki Umezawa†‡　Aya Takahashi†　Hiroki Uchiyama†　Hisao Sakazaki†
Mitsuhiro Oikawa†　Ken Kobayashi†　Shigeichi Hirasawa‡

†Hitachi, Ltd. Systems Development Laboratory
Hitachi System Plaza Shinkawasaki, 890, Kashimada, Saiwai-ku, Kawasaki-shi, Kanagawa, 212-8569, Japan

{katsuyuki.umezawa.ue, aya.takahashi.uh, hiroki.uchiyama.tm,
hisao.sakazaki.qc, mitsuhiro.oikawa.hn, ken.kobayashi.kj}@hitachi.com

‡Graduate School of Science & Engineering, Waseda University
3-4-1, Okubo, Shinjuku-ku, Tokyo 169-8555, Japan

{ume,hirasawa}@hirasa.mgmt.waseda.ac.jp

Abstract This report shows the verification technology of an attribute certificate in mobile environments. We developed an attribute certificate validation server. 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. We describe the outline of the proposed server and evaluate the performance of it.

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を開発を（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情報通信サービスにおいて，属性証明書を用いて厳密な認証やアクセス制御を行なうため際の属性証明書の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サーバについて記述し，4 章で性能を評価する．5 章で成果の展開の例を示し，そして最後に 6 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．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．以降，PKC の発行機関を認証局 (CA)，AC の発行機関を属性認証局 (AA) と記す．

- 保有者の AC に付与されている属性認証局 (AA) の署名を検証
- 属性認証局 (AA) の PKC に付与されている認証局 (CA) の署名を検証
- 認証局 (CA) の PKC が，自身の信頼している認証局 (CA) の PKC であるかどうかを確認
- 属性認証局 (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 保有者であるか否かを確認する必要がある．「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．

- 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 に付与されている認証局 (CA) の署名を検証
- 認証局 (CA) の PKC が，自身の信頼している認証局 (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の開発

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，属性認証局 (AA) およびAC保有者のPKCの検証を行い，さらに保有者のACの検証を行う必要がある．モバイルPKCは，携帯通信事業者が発行することが想定されるが，モバイル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等，第三者が属性認証局 (AA) を運営することが考えられる．携帯通信事業者を含め複数の属性認証局 (AA) がACを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を効率的に検証する技術は必要不可欠である．ACの検証はPKCに比べて更に複雑な処理を要するため，特に非力な携帯電話端末においては，より効率的なACの検証方法が求められている．上記状況を鑑み，本研究では，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検証システムを開発した．本節では，図1におけるAC検証サーバについての概要を示す．

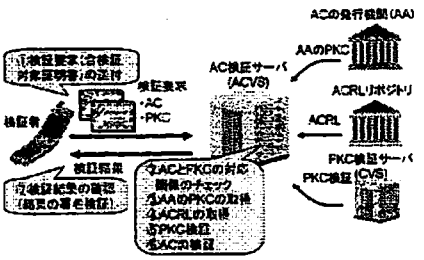

図 1: モバイルAC検証システム構成図

3.1 モバイル向けAC検証サーバの機能モジュール

「モバイル向けAC検証サーバ」に関しては，①AC検証要求データの解析とAC検証応答データの生成を行うAC検証フォーマット解析生成機能，②AC検証のための認証パスの構築やCVS[3][4][5]と連携し関連するPKCの検証を行うAC検証制御機能，③ACの有効性確認等を行なうAC検証機能，④モバイル向けプロトコルとACVSプロトコルの相互接続を行うモバイル向けプロトコルの解析生成機能等を実現したモバイル向けAC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1に示す．また，表1のモジュール機能の関係図を図2に示す．

表 1: 開発したAC検証サーバの機能

機能	説明
①AC検証フォーマット解析生成機能	AC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AC検証制御機能を実行する．また，AC検証制御機能から返却された検証結果を基に，AC検証応答フォーマットデータを生成する．
②AC検証制御機能	ACとPKCのマッチング検証，ACを発行した属性認証局 (AA) のPKCの取得，ACRLの取得，ACに紐づいたPKCの検証を行う．
③AC検証機能	ACの署名・有効期限検証，ACRLの署名・有効期限検証，ACRLによるAC検証（有効性確認）を行なう．
④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ACVSプロトコルの相互接続を行う．

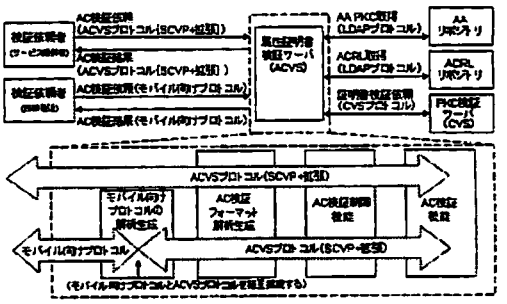

図 2: モジュール関係図

ここで，表1のAC検証制御機能における「ACとPKCのマッチング検証」に関しては，DN(Distinguished Name) 形式で表現されているACのholderフィールドのentityName情報と，PKCのSubjectフィールドを比較する．従来からの一般的な考え方ではPKCの有効期間はACの有効期間より長いが，モバイル環境では，携帯電話端末の頻繁な買い替えや番号ポータビリティ制度の導入により携帯通信事業者の

乗り換え等が発生するためPKCの有効期間がACより短くなる場合が考えられる．そのため，モバイル向けPKCでは過去の発行枚数を把握する為にPKCのSubjectフィールド内に，カウンターとしての役割を持つ"Title"の値が『T=n』（nは自然数）という形式で記述されている．上述のマッチング処理では"Title"以外のDNを比較対象とすることで世代管理を行なっているモバイルPKCとのマッチングが可能となる．

また，AC検証制御機能における「ACを発行した属性認証局(AA)のPKCの取得」先は，AC中の機関アクセス情報(authorityInfoAccess)，「ACRLの取得」先は，AC中のCRL配布点(cRLDistributionPoints)に記載のURIより行なうものとする．

3.2 AC検証要求・応答フォーマット定義

3.2.1 サービス提供者からのAC検証要求・応答フォーマットの定義

図3，4に，インターネット等の通信網を利用してサービス提供者と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．本フォーマットはSCVP [6] で規定されているフォーマットに基づいている．

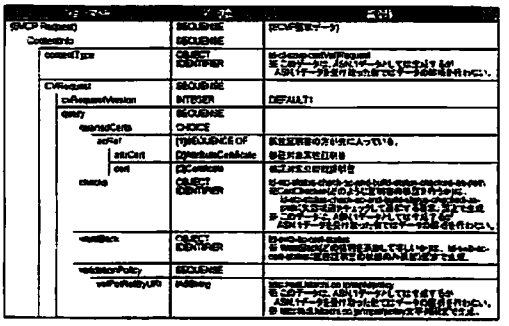

図 3: 検証要求フォーマット

3.2.2 携帯電話端末からのAC検証要求・応答フォーマットの定義

図5，6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

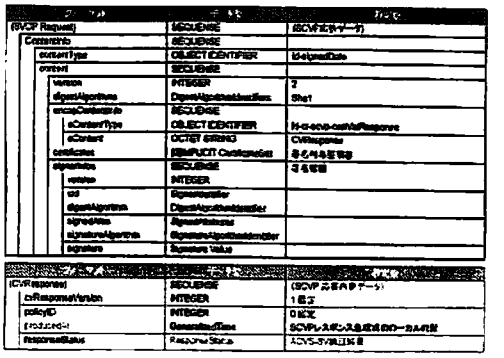

図 4: 検証応答フォーマット

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bit (1byte)	ACの長さの下位bit (1byte)	PKCの長さの上位bit (1byte)	PKCの長さの下位bit (1byte)	AC (DER)	PKC (DER)

図 5: 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 (128bit)	属性および属性値を表すHTMLソース (可変長)

図 6: モバイル向け検証応答フォーマット

また，図6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7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 7: 属性および属性値を表す HTML ソースの例

4 性能評価

本節では，開発を行った AC 検証サーバの性能評価を行う．

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．今回の性能測定では，図 2 における「モバイル向けプロトコルの解析生成」機能とその他の機能の連携を疎結合とし，別々の機器で実現した．以降前者を LACVS，後者を ACVS-SV と呼ぶ．

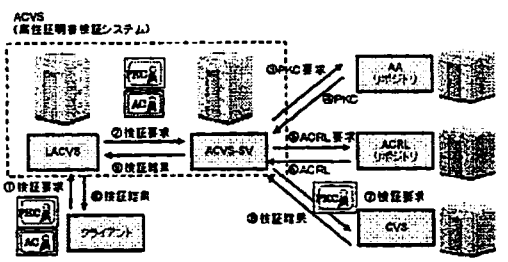

図 8: 性能測定対象システムの構成図

LACVS と ACVS-SV 間のネットワーク環境は 100Base-T(100Mbps) である．また，今回の性能測定では，バックエンドで ACVS-SV と連動する他システム（AA リポジトリ，ACRL リポジトリ，CVS）は仮想的な存在とし，ACVS-SV と同一マシン上にて構成した．また，LACVS と ACVS-SV を構成する機器は表 2 とおりである．

表 2: 性能測定対象システム構成機器

	LACVS マシン	ACVS-SV 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 5 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)LACVS・ACVS-SV 間	LACVS が ACVS-SV に対して AC 検証要求（②）を開始してから結果の受信（⑨）が完了するまでの時間を計測
(2)ACVS-SV 内の処理の開始・終了間	ACVS-SV が AC 検証要求（②）の受信を完了してから，ACVS-SV 検証結果（⑨）の送信を開始するまでの時間を計測
(3)AA の PKC 取得	ACVS-SV が AC の検証中に，AA リポジトリに対して PKC の要求（③）を開始してから，PKC を受信（④）を完了するまでの時間を計測
(4)ACRL 取得	ACVS-SV が AC の検証中に，ACRL リポジトリに対して ACRL の要求（⑥）を開始してから，ACRL を受信（⑦）を完了するまでの時間を計測
(5)CVS 検証	ACVS-SV が AC の検証中に，CVS に対して PKC（PKC）の検証要求（⑦）を開始してから，検証結果（⑧）の受信を完了するまでの時間を計測

4.3 結果一覧

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．

表 4: 性能測定結果

測定項目	測定結果 t[ms]
(1)LACVS・ACVS-SV 間	290
(2)ACVS-SV 内の処理の開始・終了間	190
(3)AA の PKC 取得	16
(4)ACRL 取得	27
(5)CVS 検証	113

表 4 より検証要求クライアントから属性証明書の検証要求を受けてからの検証サーバ内での

処理は290[ms]で完了しており十分高速といえる.

5 成果の展開例

本システムを認証基盤として用いることにより実現され得るサービスの例を図9に示す. 図9は, 旅行予約サービスの一例である. 旅行代理店のAC(旅行業認可証)を携帯電話端末で確認を行なうことで不正な旅行代理店を見極めることができるようになる. また, 携帯電話端末所有者の属性を旅行代理店で確認を行なうことで不正なユーザを見極めるとともに属性に応じたきめ細かなサービスを行なうことができるようになる. また, チケットとして発行されたACを現地(旅行先)で利用する際に不正なチケットを見極めることもできる.

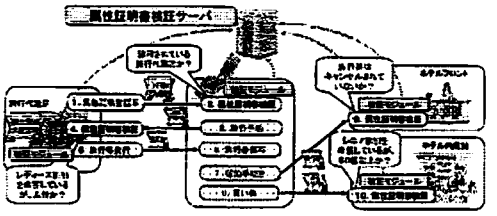

図9: 研究成果の展開例(モバイル旅行予約サービス)

6 まとめと今後の課題

携帯電話端末から属性証明書の有効性確認を含む厳密な検証を行なうことを可能にするモバイル向け属性証明書検証サーバを開発し, 実測による性能評価を行なった.

今回は, 携帯電話端末やサービス提供者装置からの利用方法に関しては対象外とした. 今後は, 本サーバを実際に利用する際の携帯電話端末側およびサービス提供者装置側のシステムについて検討および開発を行なう[7]. さらに, 開発したシステムを用いて実証実験を行い利便性等の評価を行なうことを予定している.

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] T.Fressman, R.Housley, A.Malpani, D.Cooper and T.Polk: *Simple Certificate Validation Protocol (SCVP)*, IETF, June 2006.

[7] 梅澤, 笈川, 洲崎, 平澤: "モバイル向け属性証明書検証システムの開発," 第29回情報理論とその応用シンポジウム, 予稿集, 2006/11(予定).