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

2005－DPS－122（26）
2005－CSEC－28（26）
2005／3／22

モバイルホストのユーザ情報を秘匿するアドレス配信プロトコルの提案

高橋秀郎[†]　川島　潤[†]
中西　透[††]　舩曳信生[††]

携帯電話，無線ＬＡＮなどのモバイル通信では事業者にユーザの位置などのプライバシー情報が漏れる問題がある．本稿では，匿名証明書及びグループ署名を用いてユーザ認証を行い，通信に必要なＭＡＣアドレスやＩＰアドレスを一時的に与えることで，ユーザのプライバシー情報を渡すことなく，通信を可能とするプロトコルを提案する．

A Proposal of an Address Delivery Protocol Hidding Mobile User Information

Hideo Takahashi,[†] Jun Kawashima,[†] Toru Nakanishi[††]
and Nobuo Funabiki[††]

In mobile communications using the mobile phone and the wireless LAN, etc., there is a problem that privacy information such as user's locations is leaked to the access provider. This paper proposes a protocol that realizes the communication without passing the access provider user's privacy information by the user authentication of the anonymous certificate and the group signature, and by giving a temporarily Media Access Control address and Internet Protocol address.

1. はじめに

近年，携帯電話，ＰＤＡやノートＰＣなどのインターネットに接続可能なモバイル端末が普及している．また，モバイル端末の普及とともに，アクセスポイント（以下，ＡＰ）と呼ばれる無線を利用したインターネットの接続サービスが，駅，空港，ホテルやファーストフード店などの主要な公共施設において，インターネット接続事業者（以下，ＩＳＰ）により提供されている．ＡＰの利用者は，ＩＳＰと契約して利用権を得ることで，インターネットに接続できる．

ＡＰにおいて，ＩＳＰは，契約した利用者のみに接続サービスを提供したい．これを実現するために，利用者にユーザ認証を行わせ，契約していることを確認してから，接続サービスの提供を行う．ユーザ認証の目的は本人確認であるため，ＩＳＰは確実に，アクセスしてきている利用者の名前を把握できる．これにより，ＩＳＰと契約をしていない不正な利用者からのアクセスを拒否できる．

その一方でプライバシー問題を起こし得る．何故なら，その利用者がどこの場所にあるＡＰからいつ接続したか，また，インターネットでどこに接続したかを示す履歴をＩＳＰは把握できるためである．もし，これらの履歴情報を他にリークされたとしても，ユーザは全く関知できない．その対策が大きな課題である．

ここで問題となっているのが，ＡＰに接続するユーザ認証においてＩＳＰに利用者を特定できる情報が渡り，利用者が行う通信をＩＳＰに知られることである．そこで，本稿では，利用者を特定できる情報を渡さずにユーザ認証をする匿名認証の方法について示す．

2 章において，匿名認証を実現できるディジタル署名として，匿名証明書とグループ署名について示す．3 章では，それらを用いて，モバイルホストに対する匿名のユーザ認証プロトコルを提案する．4 章において提案プロトコルの安全性について検討する．5 章において本稿のまとめを示す．

2. 匿名認証を実現できるディジタル署名

匿名認証を実現できるディジタル署名について示す．匿名認証をおこなう目的は，「誰かはわからないが，確かに登録した利用者である」ことを証明することであ

† 岡山大学大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama University, E-mail:{hitaka, kawasima}@sec.cne.okayama-u.ac.jp
†† 岡山大学工学部通信ネットワーク工学科
Department of Communication Network Enginnering, Faculty of Engineering, Okayama University, E-mail:{nakanisi,funabiki}@sec.cne.okayama-u.ac.jp

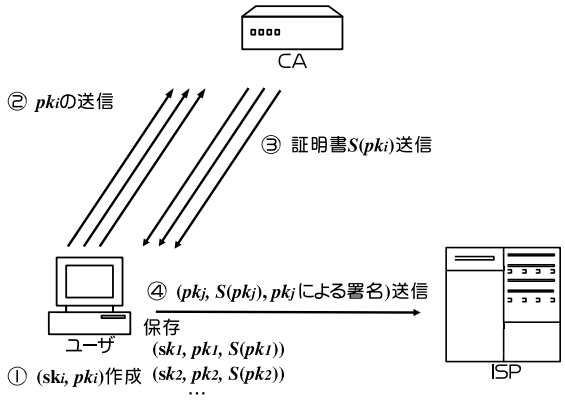

図 1 匿名証明書を使ったユーザ認証

る[1)]．

この匿名認証の方法として，

- 匿名証明書
- グループ署名

がある．

2.1 匿名証明書を用いるユーザ認証

匿名証明書を用いるユーザ認証の流れを，図 1 に示す．

まず，ユーザはディジタル署名における自身の秘密鍵 sk と公開鍵 pk を生成する．そして，pk を認証局（ＣＡ）に送信する．ＣＡはユーザの身分を証明する証明書 $S(pk)$ を発行する．ここで，$S(\cdot)$ はＣＡのディジタル署名生成関数である．また，証明書はユーザを特定する情報を含んでいないことに注意して欲しい．ユーザはＩＳＰへの接続の際に，この証明書により保証された pk を用いるディジタル署名を生成し，ユーザ認証をおこなう．これにより，ユーザはプライバシーに関する情報を渡すことなく，登録されたユーザであることを示せる．

ここで，同一の $(pk, S(pk))$ をくり返し用いた場合，証明書がリンク可能であることが問題である．すなわち，同一の $(pk, S(pk))$ をくり返し用いることで，誰かはわからないが，利用者の利用履歴がＩＳＰに特定されてしまう．このため，もし仮に利用者が判明した場合，リンクされた利用履歴からそのユーザの全ての履歴が判明してしまう．また，匿名の利用履歴から利用時刻，利用場所，利用頻度，習慣，嗜好などを抽出することが可能であるため，これらの情報を利用して利用者が特定できる可能性もある．

そこで，証明書がリンクされるのを防ぐために，あらかじめ複数の証明書 $(pk_1, S(pk_1))$，$(pk_2, S(pk_2))$，$\cdots$ を発行しておき，認証の際に証明書を使い分ける方法がある．しかし，複数の証明書を発行する際には，その都度ＣＡに証明書発行の負荷がかかる．さらに，これを複数のユーザにくりかえすことになると，ＣＡにかかる負荷はさらに大きくなり，証明書発行が満足におこなえないことが想定される．

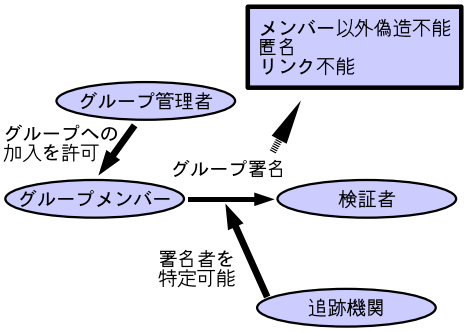

図 2 グループ署名の性質

2.2 グループ署名を用いる匿名認証

グループ署名[2)3)] は以下の性質を満たす（図 2）．

偽造不能性 ：
ある特定のグループメンバーのみが署名を作成できる．

匿名性 ：
通常の検証者は，どのメンバーが署名を作成したのか判断できない．

リンク不能性 ：
通常の検証者は，任意の二つの署名が同じものにより作成されたかどうかを判断できない．

追跡可能性 ：
何か不正が発生した際に，指定された追跡機関のみは，署名の署名者を特定できる．

グループ署名では，上記の追跡機関に加えて，**グループ管理者（ＧＭ）**と呼ばれる特別な機関を必要とする．ＧＭは，ある利用者がグループに加入し，メンバーとなることを許可する権限を持つ．本稿では，ＧＭが追跡機関も兼ねるモデルを想定する．

グループ署名では，2.1 節での問題が以下のように解決される．まず，ＧＭはサービス提供を許可する利用者のみをグループに加入させる．インターネット接続の認証時には，各利用者はグループのメンバーとして乱数 r とそのグループ署名 $GS(r)$ を生成し，$(r, GS(r))$ をＩＳＰに送信する．このとき，匿名性，リンク不能性から，利用履歴が漏洩する問題が発生しない．また，ＧＭ・ユーザ間は加入時の処理のみでよく，匿名証明書におけるＣＡに対する負荷のような問題は起こらない．

グループ署名の問題点として，グループ署名の生成・

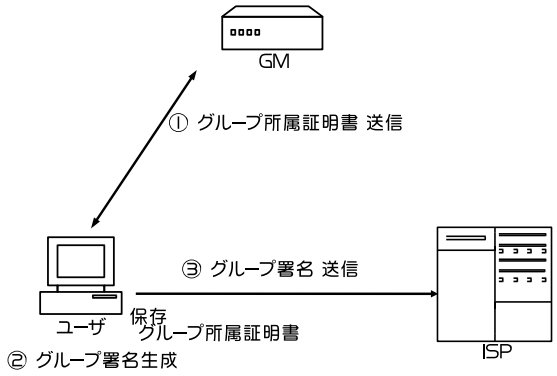

図 3 グループ署名を用いた匿名認証

検証にかかる時間が，通常のディジタル署名のそれと比較して約１０倍以上であることがあげられる．しかし，モバイル端末はＰＣより性能が劣るため，モバイル端末でのグループ署名の生成・検証は容易でない．

グループ署名を用いる匿名認証の流れを，図３に示す． グループ署名はグループ所属証明書を用いて作成する．ここで，グループ所属証明書とは，GMに登録した利用者のみに与えられる証明書である．グループメンバーは，この証明書を用いてグループ署名を作成し，ユーザ認証を行う．

3. 提案プロトコル

本節では，モバイルホストによる匿名のインターネット接続を提供する認証プロトコルを提案する．提案プロトコルでは，ＩＳＰには利用者の情報はいっさい渡さずにユーザ認証を行う．また，ユーザ認証の際に，匿名証明書とグループ署名を併用する．これは以下の理由からである．

(1) モバイルホストとＡＰ・ＩＳＰとの通信にはMACアドレスが必要である．MACアドレスとは，各 Ethernet カードに付けられたユニークな番号で，全ての Ethernet カードに割り当てられている．これを元に通信が行われる．しかし，MACアドレスはユニークであるため，通信をリンクされてしまう．通信がリンクされないためには，MACアドレスを付け替える必要がある．そこで，ＩＳＰに委託された機関が，利用可能なMACアドレスを配布すことを考える．MACアドレスの正当性保証にグループ署名を用いた場合，MACアドレスによりリンクされてしまうため，グループ署名のリンク不能性が活かされない．そこで，提案プロトコルでは，グループ署名よりもより効率的な匿名証明書をＩＳＰでのユーザ認証に用いる．

(2) リンク不能性を保持するために，付け替えるMACアドレス毎に匿名証明書を発行する必要があり，ＣＡに負荷がかかる．そこで，提案プロトコルではＣＡを複数設置し，負荷を分散する．分散ＣＡはMACアドレスの貸し出しを行う（MACアドレス発行局と呼ぶ）．

(3) ＣＡを分散すると，プライバシ漏洩のリスクが大きくなる．そこで，MACアドレス配布局への依存度の低減のため，１台セキュリティの高いＣＡを設ける．

(4) このＣＡをGMとしてグループ署名を用いる．MACアドレス配布時にはグループ署名で認証を行う．これにより，MACアドレス発行局に対してユーザ名を秘匿できる．

3.1 プロトコルのモデル

提案プロトコルのモデルを示す．本プロトコルは以下の５者間の通信により成り立つ．また，想定している前提条件も示す．

ＩＳＰ ：インターネット接続サービスをおこなっている事業者．
ＡＰの管理を行う．また，利用者が用いるMACアドレスを保有する．

ＡＰ ：街中にあるアクセスポイント．
ＩＳＰ，またはＩＳＰと契約した者により設置される．

利用者ＰＣ ：利用者が保有するＰＣ．
事前にグループ証明書を取得する．グループ署名を用いるユーザ認証により，MACアドレスとその匿名証明書を取得する．

利用者モバイル端末 ：利用者の所有するモバイル端末．
屋外でＡＰからインターネットに接続する際に利用する．ＩＳＰに対して匿名証明書によりユーザ認証をおこなう．このとき，利用者のプライバシーに関する情報は渡さない．

ＧＭ ：グループ所属証明書の発行と，不正を行った利用者の追跡をする機関．
利用者のプライバシーに関する情報を登録する．そして，登録利用者に対してグループ所属証明書を発行する．不正アクセスなどに対するセキュリティを確保した，信頼できる機関であると仮定する．

ＭＡＣアドレス発行局 ：利用者に利用可能なMACアドレスを配布する機関．

ＭＡＣアドレスの配布と共に，匿名証明書の発行も行う．複数台が稼動し，匿名証明書を作成する負荷を分散処理で軽減する．GM程の信頼はなくてもよい（理由については 4 節で述べる）．

3.2 プロトコルの処理

本プロトコルにおける，利用者の利用者登録からインターネットに接続するまでの処理と，不正を行った利用者を追跡する動作を，以下の４段階に分けて示す．

(1) ＩＳＰと利用者の登録
(2) ＭＡＣアドレスと匿名証明書の取得
(3) ユーザ認証
(4) 不正利用者の追跡

(1) ＩＳＰと利用者の情報登録

ＩＳＰの登録は以下の通りである．（図 4）．

Step 1: ＩＳＰ → GM

ＩＳＰの身元の証明になる情報を登録する．

Step 2: ＩＳＰ → ＭＡＣアドレス発行局

ＩＳＰの情報を登録する．登録する情報は以下の通りである．

- ＩＳＰが所有する利用可能なＭＡＣアドレスのリスト（ユーザに配布し，匿名認証をおこなう際に使用）．

利用者の登録は以下の通りである．

Step 1: 利用者ＰＣ → GM

ユーザ登録を行う．利用者は自身の身元を証明する情報（住所，氏名，所属など）を入力する．

Step 2: GM → 利用者ＰＣ

グループ所属証明書を発行する．利用者はこのグループ所属証明書を用いてグループ署名を作成する．

ここで，利用者登録をする先はＩＳＰではなくGMであることに注意されたい．これにより，ＩＳＰには利用者のプライバシーに関する情報の一切を渡さない．

(2) ＭＡＣアドレスと匿名証明書の取得

以下により，ＭＡＣアドレスと匿名証明書を取得し，モバイルホストに転送する．（図 5）．

Step 1. 利用者ＰＣ

ディジタル署名の秘密鍵 sk と公開鍵 pk を生成する．そして，pk に対するグループ署名を作成する．

Step 2. 利用者ＰＣ → ＭＡＣアドレス発行局

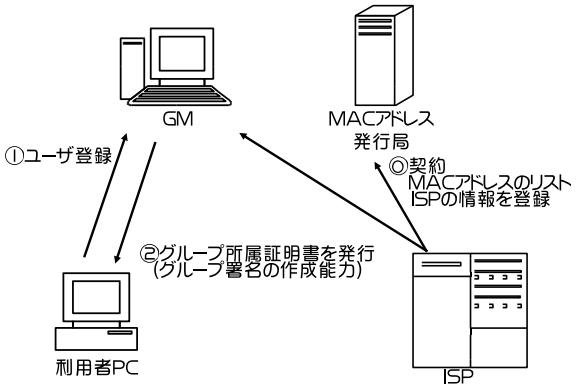

図 4 ＩＳＰと利用者の情報登録

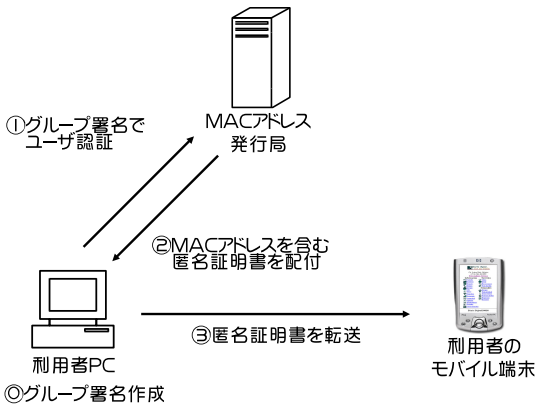

図 5 ＭＡＣアドレスと匿名証明書の取得

Step 1 で生成した pk とグループ署名を送信し，匿名認証を行う．

Step 3. ＭＡＣアドレス発行局 → 利用者ＰＣ

ユーザに，使用期限付きのＭＡＣアドレスをメッセージとして含む匿名証明書（$S(MAC$ アドレス, 使用期限, $pk)$）をＭＡＣアドレスと共に発行する．

Step 4. 利用者ＰＣ → 利用者モバイルホスト

ＭＡＣアドレスと Step 3 で取得した匿名証明書を転送する．

ここで，複数のＭＡＣアドレスを一度に取得できることに注意して欲しい．

(3) ユーザ認証

インターネットに接続する際に，利用者のモバイルホストとＡＰもしくはＩＳＰでユーザ認証を行う（図 6）．

Step 1. 利用者モバイルホスト → ＡＰ

ＭＡＣアドレスを送信する．ＡＰは受信し

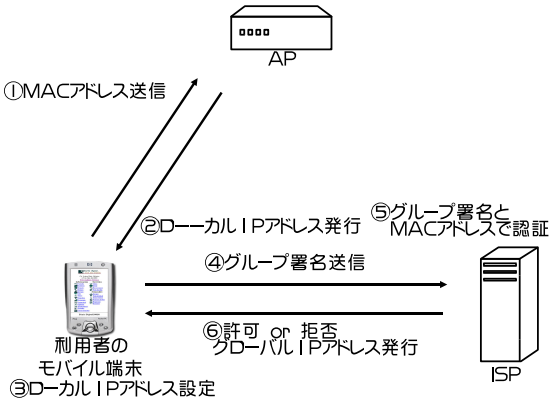

図 6 ユーザ認証

たMACアドレスが，自らの管理するMACであるならば，Step 2 へ進む．さもなければ，処理を終了する．

Step 2. AP → 利用者モバイルホスト
APはモバイルホストにローカルIPアドレスを発行する．ここで，ローカルIPアドレスとは，インターネットには接続できない一次的なIPアドレスである．

Step 3. 利用者モバイルホスト
発行されたローカルIPアドレスを設定する．

Step 4. 利用者モバイルホスト → ISP
匿名証明書を利用することにより，ユーザ認証を行う．

Step 5. ISP → 利用者モバイルホスト
Step 4 のユーザ認証により，利用者が正当な利用者であることが証明された場合，接続の許可をおこない，インターネットに接続するためのIPアドレスを発行する．このとき，ISPは利用者の匿名証明書を通信履歴として保存しておく．逆に，利用者が正当な利用者でなかった場合，接続の拒否をする．

異なる通信では，異なるMACアドレスと匿名証明書を用いて上記の接続を行うことにより，リンクを防止できる．

(4) 不正利用者の追跡

利用者が不正な通信をおこなったときなどに，利用者の身元を特定する．

Step 1. ISP → MACアドレス発行局
保存している不正な利用者の匿名証明書を送信する（利用者の身元の問い合わせ）．

Step 2. MACアドレス発行局 → GM
ISPからの問い合わせを受けた匿名証明書から，該当する利用者が送信したグループ署名を検索する．検索したグループ署名をGMに送信し，身元の開示を要求する．

Step 3. GM → ISP
グループ署名から利用者の身元を追跡する．GMは，登録している利用者の情報をISPに送信する．

なお，この不正者の追跡を行うための条件を，あらかじめ取り決めしておく必用があると考える．

4. 安全性の検討

提案プロトコルの安全性を検討する．以下の項目についてそれぞれ検討する．

(1) 利用者の不正
(2) MACアドレス発行局の登録情報の漏洩
(3) GMの登録情報の漏洩

4.1 利用者の不正

もし，利用者が不正を行った場合は，3.2 節の “不正利用者の追跡” 手順に基づいて，利用者の特定を行うことができる．

4.2 MACアドレス発行局の登録情報の漏洩

MACアドレス発行局の登録情報が漏洩した場合を検討する．MACアドレス発行局に残る利用者の情報は，

- 利用者のグループ署名
- 利用者に配布したMACアドレスと匿名証明書の対
- 利用者のPCのIPアドレス

である．

まず，グループ署名が漏洩した場合，グループ署名には利用者の情報は含まれていないため，グループ署名と利用者をリンクすることは出来ない．また，複数のMACアドレス取得もリンクできない．こうして，ISPでの異なるMACアドレスを用いた通信はリンクできない．

次に，利用者に配布したMACアドレスと匿名証明書の情報が漏洩した場合を検討する．MACアドレスはISPが配布して利用者に配布されたものであるから，利用者をリンクできる情報ではない．また，匿名証明書には利用者の情報は含まれていないため，利用者を特定することはできない．

最後に，利用者PCのIPアドレスが漏洩した場合を考える．この場合，同一のIPアドレスを使用する

なら，各ＭＡＣアドレス取得がリンクできてしまう．しかし，誰であるかはわからない．一方，ＩＰアドレスの付け替えができる場合には，リンクの問題を解決できる．

以上のことから，ＭＡＣアドレス発行局の登録情報が漏洩した場合であっても，利用者のプライバシーに関する情報を特定することは出来ない．

4.3 ＧＭの登録情報の漏洩

ＧＭの登録情報には，利用者の情報が保存してある．このため，ＧＭの登録情報が漏洩した場合は，利用者のプライバシーに関する情報が漏洩してしまう．これを防ぐために，ＧＭはセキュリティを高くし，情報が漏洩しないように防護する必要がある．

5. ま と め

モバイルホストがユーザ情報を秘匿したまま，インターネットに接続するためのアドレス配信プロトコルを提案した．提案プロトコルでは，ユーザ認証に匿名証明書とグループ署名を併用することにより，ＰＣよりも性能の低い端末でも，効率的に匿名認証を行うことができる．もし利用者が不正を行った場合でも，匿名を開示し，利用者の特定が可能である．また，提案プロトコルの安全性を検討し，実用にたるものであることを示した．

今後は，本提案プロトコルの安全性のさらなる検討と，効率面での検討を行う．また，提案プロトコルの実装も予定している．

参 考 文 献

1) 持田敏之, 舩曳信生 編著, “情報セキュリティ対策の要点 実務と理論,” コロナ社, pp.138-157, 2005.
2) D.Chaum, E.van Heyst, “Group signatures,” EUROCRYPT’91, LNCS 547, pp.257-265, 1991.
3) G.Ateniese, J.Camenisch, M.Joye, G.Tsudik, “A practical and provably secure coalition-resistant group signature scheme,” CRYPTO 2000, LNCS 1880, pp.255-270, 2000.
4) 加藤岳久, 岡田光司, 吉田琢也, “プライバシを保護する匿名認証システムの開発,” コンピュータセキュリティシンポジウム２００３, pp.569-574, 2003.
5) 岡田光司, 加藤岳久, 吉田琢也, “計算能力の低いデバイスに適したグループ署名方式, ” ２００５年 暗合と情報セキュリティシンポジウム 予稿集 Vol.Ⅲ, pp.1147-1152, 2005.