2005－CSEC－29（11）
2005／5／19

ネットワーク接続サービスに対する クライアント上での課金方式の提案と評価

星野玲子　青野博　本郷節之

株式会社 NTT ドコモ

あらまし：近年、アドホックネットワークや無線 LAN など様々なネットワーク技術が開発され、利用できるようになった。しかし、これらのネットワーク接続サービスの利用に対して課金を行う場合、利用者は事前にそれぞれのネットワークに登録する必要があるため、未登録も含めた任意のネットワークにおいてシームレスにサービスを享受できなかった。本稿では、利用者がその場で選択したネットワーク接続サービスをその提供者への事前の登録なしに利用できる環境を実現するため、利用と一体で同時進行性を持って課金され、支払いをクライアント上で行う方式を提案し、その実装とその評価について報告する。

The proposal of the payment system on the client for network connection service

Reiko Hoshino　Hiroshi Aono　Sadayuki Hongo

NTT DoCoMo, Inc.

Abstract: Recently, a variety of network technology such as ad-hoc network and wireless LAN has been invented and available. To be able to charge for network connection service, it is necessary that the users subscribe to each network connection service provider. They cannot be charged and pay seamlessly. In this paper we propose the charging system on the client without subscription by inseparable processing of network service and charging, and describe an implementation and an evaluation of it.

1. はじめに

近年、アドホックネットワークや公衆無線 LAN など様々な通信ネットワーク技術が開発され、利用できるようになった。それにより、人々はその場で選択したネットワーク接続サービスを利用するようになるだろう。一方、従来のネットワーク接続サービスでは、利用者とネットワーク接続サービスを提供する事業者が事前に契約を行い、事業者は課金のための情報（個人情報、利用履歴など）の管理をする必要がある。その場合、事業者を信頼する必要があった。

しかし、さまざまなネットワークをその場で選択して使用する場合、利用する事業者ごとに事前に登録を行うのは現実的ではない上、個人情報を管理させるほど事業者を信頼できない場合もある。

そこで、本稿では、その場で選択したネットワーク接続サービス提供者に対し、事前の登録無しに、課金され、支払いをクライアント上で行う方式を提案し、その実装について報告する。その際、アドホックネットワークを含む様々なネットワーク形態に対応可能である。

2. 背景

背景として、接続する網の種類とその繋ぎ方で分類した接続種別を述べ、それぞれの課金方式に対する要求条件について述べ、それらへの課金方式の対応について述べる。

2.1. 接続種別

接続種別は利用者間の網の種類とその繋ぎ方で分類した。ここで網を 2 つに分類する。1 つ目は公衆網（例えば、ISP、無線 LAN 事業者、携帯電話事業者などの提供する基地局やアクセスポイントを介してバックボーンインフラに接続する網）、2 つ目はそれ以外の網（例えば、イントラネット、アドホックネットワ

ーク、プライベート無線 LAN など。以下プライベート網と呼ぶ）とする。

それらの繋ぎ方には、①１つの公衆網を介した接続、②公衆網を複数介した接続、③公衆網へのアクセスのために、少なくとも１つプライベートな網を介した接続、④１つのプライベートな網を介した接続、⑤プライベートな網のみを複数介した接続に分けることができる。

2.2. 接続種別ごとの課金方式への要求条件

まず、接続種別①の課金方式の要求条件は以下のとおりである。

①-i. サービス提供者はリソース提供に対する対価が得られること
①-ii. サービス利用者は支払う分サービスを受けられること
①-iii. 現在、存在する課金が可能なこと（属性、従量課金等）

接続種別②の課金方式の要求条件は以下のとおりである。

②-i. サービス提供者はリソース提供に対する対価が得られること
②-ii. サービス利用者は支払う分サービスを受けられること（途中までしかサービスが提供されないならば、支払わない）
②-iii. サービス利用者は利用する全てのサービス提供者に対して個別に利用者登録し、課金情報を管理される必要は無い
②-iv. 現在、存在する課金が可能なこと（属性、従量課金等）

接続種別③の課金方式の要求条件は以下のとおりである。

③-i. サービス提供者はリソース提供に対する対価が得られること
③-ii. サービス利用者は支払う分サービスを受けられること（プライベート網に関しては、途中までしかサービスが提供されなければ、その分しか払わない）
③-iii. 現在、存在する課金が可能なこと（属性、従量課金等）
③-iv. サービス利用者は利用する全てのサービス提供者に対して個別に利用者登録し、課金情報を管理される必要は無い

接続種別④の課金方式の要求条件は以下のとおりである。

④-i. サービス提供者はリソース提供に対する対価が得られること
④-ii. サービス利用者は支払う分サービスを受けられること
④-iii. サービス提供者とサービス利用者間でサービス提供と対価の支払いがその場で完結すること

接続種別⑤の課金方式の要求条件は以下のとおりである。

⑤-i. サービス提供者はリソース提供に対する対価が得られること
⑤-ii. サービス利用者は支払う分サービスを受けられること（途中までしかサービスが提供されなければ、その分しか払わない）
⑤-iii. サービス提供者とサービス利用者間でサービス提供と対価の支払いがその場で完結すること

2.3. 課金方式の種類

ここで、課金とはある課金体系に従って、課金/支払い額を決定することを指し、それがどこで行われるかで、課金方式を分類した。１つは、サービス時にネットワーク側で課金が行われるネットワーク課金方式とサービス時にクライアント側で課金が行われ、支払いをするクライアント課金方式がある。

それぞれの課金方式が接続種別ごとの課金に対する要求条件を満たすかどうかを以下の表で示す(○は対応可能、△は一部対応可能、×は対応不可能)

表 1　接続種別の各課金方式の対応

接続種別	ネットワーク課金方式	クライアント課金方式
①	○	△ iii ファミリー割引など端末を跨る割引はできないが、それ以外は対応可能
②	△ iii 提供者が互いにローミング契約を行う必要がある	△ iii ファミリー割引など端末を跨る割引はできないが、それ以外は対応可能
③	× ii プライベート網までしかサービスが提供されなかったときの課金が対応不可能 iv すべて提供者が互いにローミング契約を行う必要がある	△ iii ファミリー割引など端末を跨る割引はできないが、それ以外は対応可能
④	× iii 利用者は利用するすべての提供者に課金のための情報を提供し、認証してもらう必要があるが、現実的ではない	○
⑤	× iii 利用者は利用するすべての提供者課金のための情報を提供し、認証してもらう必要があるが、現実的ではない	○

クライアント課金方式は各種の接続種別の様々なサービス提供者に対して対応可能な方式であると言える。本研究では、クライアント課金で実現される一方式について提案する。

3. 関連研究

クライアント上での課金方式には，以下の 2 種類の手法がある。1 つ目はパケットに対価を添付して、転送ノードがそれを取って転送することで支払いをするパケット添付方式である。アドホックネットワーク向けとしては Nuglet 方式[1][2]があり、通信事業者向けとしては専用トークン利用方式[3][4]がある。2 つ目の仲介者ノード方式[5]は、端末同士のマルチホップ通信に対するインセンティブ機能と PKI 補助機能を比較的リソースの多い仲介者ノードが提供することで、ノード自身がポイントを管理し、ルーティング方式に

依存しない方式を実現している。

ここで、1 つ目はアドホック、通信事業者両方とも対応する方式は無く、また、パケットが相手に到達しなくても、転送するだけで対価を支払わなければならない。また、2 つ目は必ず中継には関わらない仲介者ノードが存在しないとならないため、サービスに関わる当事者のみのネットワークには対応しない。

従来の方式では、2 章で述べた①から⑤に対応するものはなかった。

4. ネットワーク接続サービスと不可分な演算処理によるクライアント上での課金方式

4.1. サービスモデル

筆者らは、その場で選択した様々な立場のサービス提供者に対して、クライアント上でネットワーク接続サービスと支払い処理を同時に行うことにより、サービス提供者は提供したリソースへの対価を徴収することができ、サービス利用者はサービス提供者ごとに課金情報を登録してから利用するというわずらわしさが無くなり、自由に通信サービスを享受することができる方式を提案する。

本方式は、課金インフラ提供者，サービス利用者、サービス提供者、ターゲットからなる（図 1 参照)。課金インフラ提供者が各者にネットワーク接続用プログラムの配布を行う。また、利用の前に、サービス利用者は課金インフラ提供者にアクセスして、利用料金を支払い、プリペイドマネーを得る。

ネットワーク接続サービス時には、サービス利用者はサービス利用者のクライアント上で支払いを行い、支払いの証拠を生成し、サービス提供者に送信する。サービス提供者は、支払いの証拠を検証すると、ターゲットとの間のネットワーク接続サービスを提供する。

サービス提供者は集めた支払いの証拠をサービス提供履歴として課金インフラ提供者に送付すると、サービスに対する報酬が得られる。

従来のネットワーク接続サービスは、通信事業者などのサービスを提供する者に対して信頼をおいていたが、本サービスにおいてはサービス提供者が必ずしも信頼のおける者とは限らないためサービス提供者には信頼をおかない。一方、課金インフラ提供者の配布するネットワーク接続用プログラムにより本サービスは成り立つため、課金インフラ提供者が不正を行った場合サービスを実現することは困難である。そこで、課金インフラ提供者には信頼を置くこととする。

4.2. サービス要件

以下に本方式のサービス要件を示す。

- サービス提供者はサービス利用者の個人情報、利用履歴などの保存・管理を必要としない
- サービス利用者、サービス提供者、ターゲットはそれぞれの間で予め秘密情報の共有を必要としない
- サービス利用者はサービス提供者と相互認証した後に、サービス提供者に接続先を通知する
- サービス提供者によりターゲットと接続の可能性の確認が済まないと、サービス利用者は支払いを行わない
- サービス利用者が支払はないと、サービス提供者はサービス利用者にネットワーク接続サービス（ターゲットとの通信）を提供しない

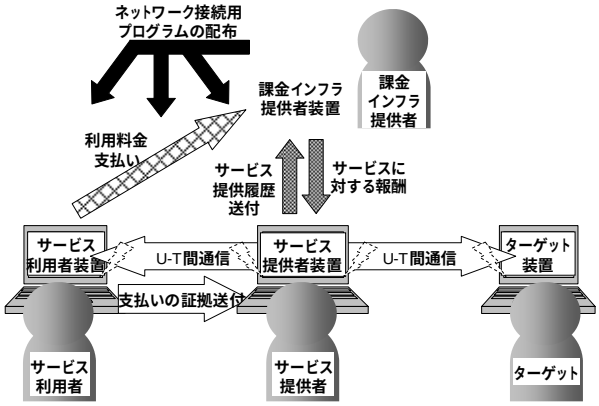

図 1　本サービスにおける全体像

4.3. 脅威

対処するべき脅威を以下に示す。

1. ユーザトラフィックデータ、制御データへの盗聴、改ざんといった脅威が考えられる。
2. リプレイアタックなどのプロトコルを模した攻撃
3. 債務履行否認(repudiation)
   - 料金ルール(Tariff)の改ざんによる過少支払い
   - 支払いの証拠の捏造によるサービスに対する報酬の過大請求
4. サービスへの不正アクセス

4.4. セキュリティ要件

以下が、対処するべき脅威に対するセキュリティ要件である。

1. ユーザトラフィックデータまたは制御データへの盗聴困難、改ざん検出可能
2. リプレイアタックなどのプロトコルを模した攻撃を検出可能
3. 債務履行否認(repudiation) への対処として、料金ルール(Tariff)の改ざん、支払いの証拠の捏造を検出可能
4. ネットワーク接続サービスへは正しい手順でのみアクセス可能

4.5. システム構成

前述の要件を満たすシステムの基本構成を図 2 に示す。本稿においては、課金インフラ提供者を除く各者が IC カード等耐タンパーハードウェアを持つ。

課金インフラ提供者装置は、ネットワーク接続用プログラムを各者に配布する。このプログラムを利用して、以下の処理を行う。まず、サービス利用者装置は課金インフラ装置にアクセスして、IC カードにプリペイドマネーを充てんする。その際、サービス利用履歴を送信する。

ネットワーク接続サービスを受ける際、サービス利用者は、サービス提供者 IC カードから送られた料金ルールに基づきサービス利用者 IC カード内で支払い

を行い、支払いの証拠を生成し，サービス利用者装置に送信する。支払いの証拠を受け取ったサービス提供者装置は、サービス提供者 IC カードでその内容を検証する。検証結果が正しければ，サービス提供者はサービス利用者にサービスを提供する。

サービス提供者装置は IC カードの支払いの証拠を課金インフラ提供者装置にサービス提供履歴として送信し、サービス提供の報酬を受け取る。

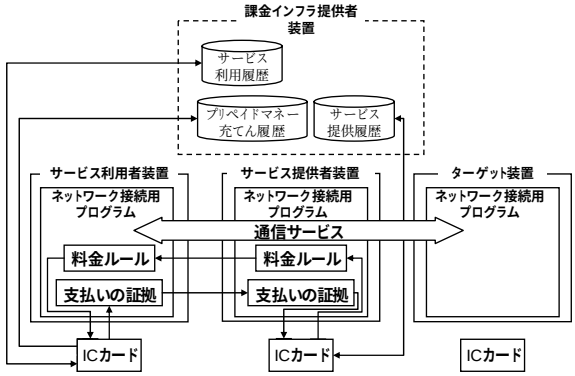

図 2　システムの基本構成

4.6. 脅威への対策

前述のセキュリティ要件を満たすために、プロトコルは以下の処理を実現する。

1. ユーザトラフィックデータまたは制御データの盗聴へはデータを暗号化する。また鍵など重要なものについては改ざん検出のため署名を付ける
2. リプレイアタックに対しては、支払いの証拠は識別可能な ID を含むことで、サービス提供者が重複した支払いの証拠を受け取らないようにする
3. 債務履行否認(repudiation)に対しては、改ざん検出のため料金ルールにサービス提供者の署名を着け、支払いの証拠にもサービス利用者の署名を付ける。また、課金インフラ提供者は支払いの証拠のコピーを送りつけられても、検証可能とするため、支払いの証拠にはすべてのサービスに対して、一意になるサービス ID を付ける
4. サービスへの不正アクセスに対しては、成りすましを防ぐため、３者で相互認証を行う

4.7. プロトコル

前述のサービス要件、セキュリティ要件を満たすプロトコルについて述べる。本方式には、サービスを行なう際にサービス利用者、サービス提供者、ターゲット間で行なわれるネゴシエーションプロトコルと、サービスが行なわれている間、課金のタイミングごとに行なわれる支払い・証拠送付プロトコルがある。また、サービス提供者がサービス提供料を申請する際に、課金インフラ提供者とサービス提供者の間で行なわれるサービス提供料申請プロトコル、サービス利用者がプリペイドマネーを申請する際に、プリペイドマネー充てんプロトコルがある。

図 3 にネゴシエーションプロトコル概要を示す。

1．サービス利用者 IC カード～サービス提供者 IC カード間で互いに証明書を送付する
2．サービス利用者 IC カードへサービス提供者 IC カードから鍵の配布をする
3．サービス提供者 IC カード～ターゲット IC カード間で互いに証明書を送付する
4．支払い処理として、受け取った料金表のとおりに支払いを実行し、支払いの証拠を送付する
5．サービスが開始され、サービス利用者 IC カード～ターゲット IC カード間で互いに証明書を送付する
6．ターゲット IC カードからサービス利用者 IC カードへ鍵の配布をする

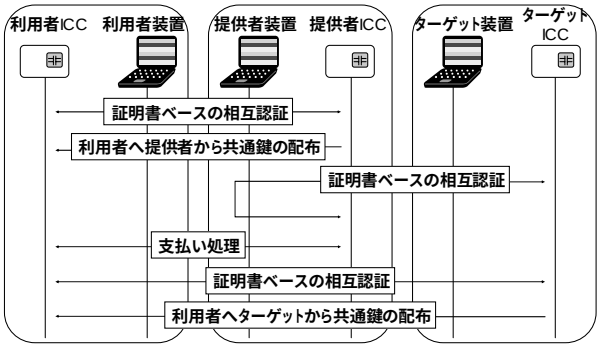

図 3 ネゴシエーションプロトコル概要

4.8. 安全性評価

前述のシステム構成、プロトコルがセキュリティ要件を満たすかどうか分析する。

1. ユーザトラフィックデータまたは制御データへの盗聴、改ざん

盗聴については、ユーザトラフィック、制御データは共有鍵で暗号化されている。改ざんについては、ユーザトラフィックは MAC などを付けるという対策もあるが、通話のように必ずしも完全性が保証されなくてもいい場合もある。制御データについては、支払いの証拠や料金ルールに署名を付ける。

2. リプレイアタック攻撃

支払いの証拠には識別可能な ID が含まれているので、リプレイアタック検出可能。

3. 債務履行否認(repudiation)
   - 料金ルール(Tariff)の改ざん

料金ルールには署名が付いており、改ざん検出可能。

   - 支払いの証拠の捏造

支払いの証拠には識別可能な ID が含まれ、サービス利用者の署名がついているため、サービス提供者が捏造することはできない。

4. サービスへの不正アクセス

3 者で相互認証するため、成りすましできない。

5. 実装と評価

前章で述べた課金方式の実装について述べる。

5.1. ネゴシエーションプロトコル詳細

ネゴシエーションプロトコル詳細について述べる。

1. **サービス提供者 ID 問合せ**：サービス利用者装置からサービス提供者装置にサービス提供者 ID を問合せ、サービス提供者 ID を得る
2. **ID 書き込み**：サービス利用者装置は受信したサービス提供者 ID と操作入力したターゲット ID をサービス利用者 IC カードへ書き込む
3. **証明書検証（サービス利用者）**：

(ア) サービス利用者装置からサービス提供者装置を通じて、サービス提供者 IC カードにサービス利用者証明書を送信する
(イ) サービス提供者 IC カードでサービス利用者証明書を検証する

4. **鍵配送**：
(ア) サービス利用者証明書の検証が OK ならば、サービス提供 IC カードは以下の処理を行う
a すべてのサービスに対して一意なサービス ID、共有鍵を生成する
b サービス ID とサービス利用者との共有鍵の結合に対する署名を生成する
c サービス ID と共有鍵の結合と署名をサービス利用者の公開鍵で暗号化する
d サービス提供者装置に暗号文を送信する

5. **証明書検証（サービス提供者）**：
(ア) サービス提供者装置は暗号文とサービス提供者証明書をサービス利用者装置を通じてサービス利用者 IC カードに送信する
(イ) サービス利用者 IC カードはサービス提供者証明書の検証をする

6. **鍵配送**：
(ア) サービス提供者証明書検証 OK ならば、サービス利用者 IC カードで以下の処理を行う
a 暗号文を復号化し、署名を検証する
b サービス提供者との共有鍵をサービス利用者装置に送信する

7. **ターゲット ID 通知**：サービス利用者装置でターゲット ID をサービス提供者との共有鍵で暗号化し、サービス提供者装置に送る

8. **証明書検証（サービス提供者）**：
(ア) サービス提供者装置はターゲット装置を通じてターゲット IC カードにサービス提供者の証明書を送信する
(イ) ターゲット IC カードはサービス提供者の証明書を検証する

9. **証明書検証（ターゲット）**：
(ア) 検証 OK ならば、ターゲット装置はターゲット証明書をサービス提供者装置を通じてサービス提供 IC カードに送信する
(イ) サービス提供 IC カードはターゲット証明書を検証する

10. **鍵配送**：
(ア) ターゲット証明書検証 OK ならば、サービス提供 IC カードは以下の処理を行う
a 乱数、署名を生成する
b ターゲットの公開鍵で暗号化する
c サービス提供者装置に暗号文を送信する
(イ) ターゲット装置は暗号文をターゲット IC カードに送信する
(ウ) ターゲット IC カードは暗号文を復号化し、署名を検証し、乱数を取り出し、ターゲット装置に送信する
(エ) ターゲット装置は乱数を乱数自身で暗号化し、サービス提供者装置を通じて、サービス提供者 IC カードに送信する
(オ) サービス提供者 IC カードは復号化し、結果と照合し、一致する場合は、サービス提供者はターゲットと通信可能と判断して、処理を続けるが。一致しない場合は、エラー処理を行い終了する。

11. **支払い処理**：
(ア) サービス提供者装置は料金表をサービス提供者 IC カードに送信する
(イ) サービス提供者 IC カードは料金表に署名し、サービス提供者装置を通じて、サービス利用者 IC カードに送信する
(ウ) サービス利用者 IC カードで署名を検証し、支払い可能かどうかチェックを行い、支払いの証拠を作成し、サービス提供者装置を通じて、サービス提供者 IC カードに送信する
(エ) サービス提供者 IC カードは支払いの証拠を検証し、保存し、サービスの開始の許可をする

12. **証明書検証・鍵交換**：サービス利用者とターゲットはサービス提供者が提供する通信サービスにより通信を行い、双方で証明書ベースの相互認証を行い、ターゲットからサービス利用者に共有鍵が送付される

5.2. 実装環境

今回実装した実装環境を表 2 に、システム使用した暗号、署名アルゴリズムを表 3 に示す。

表 2 実装環境

(1)課金インフラ提供者サーバ

CPU	Intel® Pentium®Ⅱ
OS	Red Hat Linux 8.0
その他環境	Openssl 0.9.6b, PostgreSQL 7.2.2-1, Apache 2.0.49, Tomcat 5.0.24

(2)サービス利用者、サービス提供者、ターゲット装置

OS	Windows XP, 2000
IC カード	Gemplus 社製 GemXpress Pro チップサイズ 64kbyte

表 3 暗号、署名アルゴリズム

署名アルゴリズム	SHA-1 with RSA1024 PKCS#1 CRT
公開鍵アルゴリズム	RSA1024 PKCS#1 CRT
共通鍵アルゴリズム	Triple DES 24byte 鍵 CBC Padding なし

今回の実装では支払いの証拠は、サービス利用者 ID(8 byte)、サービス提供者 ID(8 byte)、ターゲット ID(8 byte)、料金表(16 byte)、料金額(2 byte)、決済方法(2 byte)とそれら情報に対する署名(128 byte)からなり、サイズは 172byte である。また、証明書はすべて標準仕様、X.509v3 形式であり、今回の実装ではサイズは 1538 byte ある。

5.3. 実装評価

プライベート網へのアクセスポイントであるサービス提供者がサービス利用者に対して、プライベート網を介した先のターゲットへの接続を提供する接続種別④の環境において、要件通りの課金を行うことができた。

その際、装置の処理、IC カードの処理、また装置と IC カードの間の転送処理時間の合計はネゴシエーションプロトコルでは約 48 秒、そして、支払い・証拠送付プロトコルでは約 7 秒であった。つまり、性能面の問題あるため、提案方式を実現するために適した要素技術の改善が必要であることが分かった。

6. 考察

6.1. 従来研究との比較･利点

3 章で述べた従来研究との方式の比較を行った（表 4)。以下に、他方式と比較した提案方式の利点を述べる。

(Ⅰ) 従来方式の場合、初めて利用する通信事業者ごとに専用トークンの購入や認証のために、第三者とのインタラクションが必要であると、その場にいる当事者のみで課金を行うことができなくなってしまい、様々な接続種別に対応しなくなる(γ,δ)。本方式では、初めて利用する通信事業者のサービスを受ける際、第三者とのインタラクションの必要がないため、様々な接続種別にも対応できる。

(Ⅱ) また、従来方式の場合、対応する接続種別が限られると、接続種別ごとに別々の課金方式となってしまい、結局シームレスに課金を行うことができなくなってしまう。このため、対応する接続種別の制限はないことが望ましい。本方式は、接続種別の制限がない。

(Ⅲ) 一方、本方式の場合、ファミリー割引など端末を跨る割引に対応できないという問題がある。しかし、本方式では、課金インフラ提供者がユーザ管理を行っているので、プリペイドマネーチャージ時に履歴を吸い上げる際、キャッシュバックする等の方法で、実質的に実現可能である。こうすることで、履歴提供のインセンティブとなることも期待できる。

(Ⅳ) なお、本方式で耐タンパーハードウェアを必要とする点はデメリットと考えられるが、特殊な機能は必要とせず、市販されている IC カードで十分実現できる。

6.2. ネットワーク課金との比較･利点

一方、ネットワーク課金と比較すると、端末に利用履歴や課金情報が入っているので、端末紛失時の影響が大きい。しかし、重要な情報を耐タンパーハードウェアに格納しておくことで、情報漏えいへの対策は可能と考えられる。なお、履歴情報は課金インフラ提供者に送信してしまえばクライアント側では不要となるので、これを削除すれば、より情報漏えいの脅威を低減させることができる。

7. まとめ

本稿では、その場で選択した通信サービスをその通信サービス事業者への事前の利用者登録なしに利用し、支払いできる方式を提案し、実装･評価を行った。

提案方式は、初めて利用する通信事業者のサービスを受ける際、第三者とのインタラクションを必要とせず、様々なサービス提供者に対応可能であることを特徴とする。実装により、本方式が実際に動作可能なことを確認することができた。

今後、下記の点に関する改善方法を検討することが課題である。

a) サービス中にサービス提供者やターゲットが変わる場合のネゴシエーションの効率

b) マルチホップ時におけるネゴシエーションプロトコル、支払い・証拠送付プロトコルの処理量

表 4　提案方式と関連研究方式の比較

比較項目	α:提案方式	パケット添付方式		δ:仲介ノード方式[4]
		β:Nuglet [1][2]	γ:専用トークン利用[3]	
(Ⅰ): 初めて利用する通信事業者のサービスを受ける際、第三者とのインタラクションの必要性	無	無	有 ※第三者：token を発行する broker	有 ※第三者：仲介ノード
(Ⅱ): 対応する接続種別の制限	無	③、④、⑤のアドホックネットワークのみ	①のみ	③のみ
(Ⅲ): 現在、存在する割引	可能	可能 ※サービス利用者の情報を個別に管理する必要がある	可能 ※サービス利用者の情報を個別に管理する必要がある	可能 ※サービス利用者の情報を個別に管理する必要がある
(Ⅳ): 耐タンパーモジュールの必要性	Yes	Yes	No ※但し、トークンと鍵を安全に格納するためには必要	Yes

8. 謝辞

本研究を進める上で有益なご助言を頂いた横浜国立大学大学院環境情報学府/環境情報研究院松本勉先生、鈴木雅貴様、加山司様、三菱総研赤井健一郎様に謹んで感謝致します。

文　献

[1] L. Blazevic, L. Buttyán, S. Capkun, S. Giordano, J. -P. Hubaux and J. -Y. Le Boudec, “Self-Organization in Mobile Ad Hoc Networks: The Approach of Terminodes”, *IEEE Communications Magazine, June 2001.*

[2] L. Buttyán and J. -P. Hubaux, “Stimulating cooperation in self-organizing mobile ad hoc networks", *ACM Journal for Mobile Networks, special issue on Mobile Ad Hoc Networks, 2002.*

[3] H. Tewari and D. O'Mahony, “Real-Time Payments for Mobile IP”, *IEEE Communications, Vol. 41, No. 2, February 2003, pp 126-136.*

[4] 安齋潤, 松本　勉, “マルチホップセルラネットワークにおけるインセンティブ機能および PKI 補助機能の統合”, *情報処理学会論文誌, Vol.45, No.12, pp2589-2599 (2004).*