グループウェアと
ネットワークサービス 43−13
（２００２．３．２３）

Ｐ２Ｐ型ローカルマネー交換プロトコルの提案

並河 岳史　秋山 和隆　手塚 一郎　菊池 宏徳　山根 信二　村山 優子

岩手県立大学 ソフトウェア情報学部

ローカルマネー（地域通貨）は法定通貨とは性質や運用形態が大きく異なるため，ネットワーク上で実装する場合には従来の電子マネーの場合とは違った形式を取るべきである．本研究では，地域通貨をＰ２Ｐネットワーク上に実装する場合の交換プロトコルを提案する．

A proposal of a new protocol for local money exchange on P2P system

Takeshi Namikawa Kazutaka Akiyama Ichiro Tezuka Hironori Kikuchi
Shinji Yamane Yuko Murayama
Faculty of Software and Information Science
Iwate Prefectural University

We propose a protocol for local money exchange on a P2P system. Until now, legal tender is used for electric commerce with the client-server model. Another model may fit better for local money due to its difference from legal tender in characteristics and operations.

1　はじめに

現在，世界的にローカルマネーが注目を集めている．日本においても，加藤敏春が提唱するエコマネー [3] や森野栄一が提案するＷＡＴ [4] など，各地で取り組みが行われている．これらはセキュリティ上の問題をはじめ，多くの問題を抱えながら，加速度的に普及が進みつつある．

本稿では，ローカルマネーの特徴およびＰ２Ｐとの親和性について述べ，ＰｕｒｅＰ２Ｐネットワーク上での認証およびローカルマネーの交換プロトコルを提案する．

本研究の目的は，ローカルマネーのネットワーク上での可能性を探ることである．

主な研究内容は以下の 3 点である．

- ローカルマネーを P2P 型システムとして設計及び実装を行う．
- 大学内にて１００人規模で実証実験を行い，ローカルマネーの可能性を探る
- 電子商取引をとりまく法的問題について考察する

本稿では，次節でローカルマネーを紹介する．３節では，提案するＰ２Ｐ型のローカルマネー交換システムの概要を述べ，４節でプロトコルの詳細について述べる．５節では実施予定の実証実験を紹介する．

2　ローカルマネーについて

ローカルマネーには実験的な面もあり，世界各地で多様な形態で運用されている．本節では，それらに共通する性質を挙げた上で，本稿が対象とするローカルマネーについて述べる．

2.1 貨幣としての特徴

貨幣には，経済学の分野では以下の３つの機能が定義されている．

A） 交換の媒介
B） 価値の保存
C） 計算単位

Aは，物や労働力を交換する際に，貨幣を介することで，経済活動を活発にする機能である．経済活動とは物財や労働や時間の交換であり，それを媒介するのが貨幣である．

Bは，生肉や労働力のような貯めておけない価値を，保存して蓄える機能である．

Cは，さまざまな物の価値を計る際に使われる機能である．

現状では，ほとんどのローカルマネーはAの機能しか持たない．ローカルマネーの多くは数年後も流通しているかどうかもわからないため，BやCの機能は期待しづらい．

利子によって価値が増えていくことがないため，人々は手に入れたローカルマネーを，なるべく早く使ってしまおうとする．そのため，ローカルマネーは一般の通貨よりも速く流通し，物や労働力の交換を促進する．ローカルマネーで取引される商品には，昔から近所付き合いの中にあるちょっとしたサービスなども多く，コミュニティを活性化させる効果が表れる．

ローカルマネーには多種多様な形態があり，様々な視点から分類が行われている．

本稿で扱うのは，以下のような特徴を持つローカルマネーである．

- 参加者は誰でもマネーを発行できる
- 無担保で参加することができる
- 法定通貨とのつながりを保証していない

日本の各地で市民の手によって運営されているＬＥＴＳ型 [5] およびＷＡＴ型 [4] のローカルマネーのほとんどが，上記の特徴を持つ．本稿では，単にローカルマネーと記した場合，上記の特徴を備えたものを指す．

2.2 Ｐ２Ｐシステムとの親和性

クレジットカードのオンライン決済やモバイルバンキングなど，法定通貨を電子化したサービスはこれまでクライアント・サーバ型（Ｃ／Ｓ型）で提供されてきた．このモデルにおいては，クライアントはサーバを提供している会社に信用が置けるかどうかを吟味した上で，サービスを利用することになる．しかし，他の利用者を信用するかどうかは，考慮する必要がない．これは，法定通貨のあり方とよく似ている．法定通貨は政府および中央銀行が価値を保証している．法定通貨を利用する際には，他の利用者の信用を考えなくても良い．図１のように，法定通貨とＣ／Ｓ型システムは，信用の流れにおいて共通している．

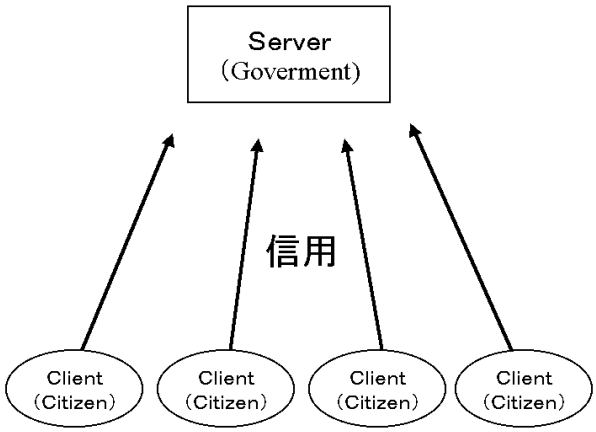

図 1: 法定通貨およびクライアント・サーバ型システムにおける信用の流れ

ローカルマネーにおける信用の流れは，法定通貨のそれとは異なる．ローカルマネーの価値は，たとえば政府のような，木構造における上位の一者の「信用」に支えられているのではなく，利用者間の対等な関係における互いの「信用」に基づいている．このあり方は図２のように，Ｐ２Ｐ型システムによく似ている．Ｐ２Ｐでの通信は，接続したホスト同士が，互いを信用することで成り立っている．そのため，あるホストが信用できなくても，他の多数のホストが信用できるなら，Ｐ２Ｐ型システムは有効に働く．

コミュニティを持つＰ２Ｐ型システムにおいては，信用できないホストからのアクセスを，皆が拒否することも起こりうる．このような防御作用は，ローカルマネーのコミュニティにおいても有効に働くであろう．

ローカルマネーを C/S 型システムで運用する場合，クライアントは他の利用者を信用する前提として，まずサーバを信用しなければならない．これは，上下関係のないローカルマネーのコミュニティには

適さない．ローカルマネーは，C／S型よりもP2Pとの親和性が高い．

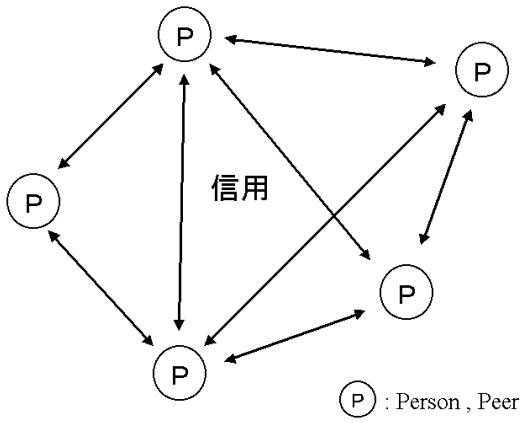

図 2: ローカルマネーおよび P2P 型システムにおける信用の流れ

3 提案方式

本方式は公開鍵暗号基盤を基礎とする．PureP2Pであることを重視し，認証局には依らない．すべての Peer は，1 日の大半の時間においてネットワークに接続されているものとする．

本稿で用いる記号を以下に示す．

SK_i：ユーザー i の秘密鍵
PK_i：ユーザー i の公開鍵
CK：セッションの共通鍵
M_i：ユーザー i が発行したマネー

3.1 グループと認証

本方式では，最初の 1 人がグループを発足させる．この時点で会員は 1 人であるが，他のユーザーを招き入れることで会員を増やしていくことになる．

新会員はグループに参加した時点で，紹介した会員からグループ共有情報（グループのＩＤ・識別番号，会員全員のＩＤ・識別番号・公開鍵・発行限界高）を受け取り，自分の情報を加えて更新する．新会員は更新したグループ共有情報を会員全員に送信し，全員のグループ共有情報が更新される．接続できなかった会員に対しては，定期的に遅延送信を繰り返す．

全員が互いの公開鍵を持ち合っているので，会員Aが会員Bと通信する際には $\{CK\}_{PKB}\}_{SKA}$ を送信する．これにより認証とセッション鍵の交換を行い，以後の通信を開始する．

3.2 マネーと証明書の書式

本方式で使用するマネーはテキスト形式であり，図 3 のように額面，発行者，所有者，発行日時，ロット，シリアル，および必要に応じて前の所有者，分割元のマネーが記載されている．額面は，紙幣のように千や万などの単位で区切る必要がなく，小切手のように必要な額面だけ発行される．発行者の項目には，そのマネーを発行した会員のＩＤと識別番号が記入され，所有者にはマネーの所有者のＩＤと識別番号が記入される．

ロットは，マネーの発行上限高を管理するためのデータである．ある会員Aの発行上限高が 200 だった場合，Aは発行するマネーに 0 から 199 までのロットを割り当てることができる．

たとえば，100 単位のマネーを発行する場合には，ロットの項目に 0-99 のように記入して，自分が使えるロットの中のどの範囲を割り当てたのかを明確にしなければならない．ロットの中の複数の範囲を使用する場合には 20-59,110-169 のようにカンマ区切りで記入する．Aが発行上限高を超えた額のマネーを不正に発行するには，ロットが重複するマネーをコミュニティ内に振り出す必要があり，誰かの手の中でロットが重複した時点でAの不正が発覚する．

```
PRICE=170
ISSUER=foo,18294763
OWNER=bar,44334747
DATE=2002.1.31
LOT=0-150,200-220
SERIAL=15
FROM=rex,54963849/* 譲渡された場合 */
SPLITED=11,9        /* 分割された場合 */
```

図 3: マネーの書式

シリアル番号は，その会員が今までに発行したマネーの通し番号である．マネーを発行者以外から入手した場合は，前の所有者のＩＤと識別番号が記載される．マネーが分割されたものだった場合には，分割前のマネーのシリアル番号が記載される．

証明書は，マネーに証明書発行日時とメッセージを加えて，発行者や所有者がデジタル署名又は暗号化を施したものである．本プロトコルにおいては，証明書は紛争解決に用いられる．各証明書の役割は図 4 の通りである．

証明書名	効果
OFFER	支払い取引の意思表示．取引の意思を証明する． GIVE よりも弱い．
GIVE	譲渡証明書． ISSUE を反証する．
SPLIT	分割の意思表示．マネーの所有権を破棄する代わりに，分割された２つのマネーを要求する． ISSUE を反証する．
ISSUE	発行証明書．マネーの有効性を証明する．
ACCEPT	受諾証明書．取引の意思を証明する．

図 4: 紛争解決用の証明書

3.3 証明書の保存

本プロトコルでは，各端末に多くのデータを保存することを想定している．グループの会員全員のＩＤと識別番号および公開鍵は通信するたびに使われるが，証明書は紛争解決の際の証拠としてしか使われない物が多い．

将来的に登場すると思われる固定ＩＰアドレスを持つ携帯電話などでは，端末の記憶領域に証明書が入りきらない場合も考えられる．そのため，証明書はＰＣなどに転送して保存しておき，必要な時に端末に読み込める仕様にする必要がある．

4 交換プロトコル

本プロトコルでは，ローカルマネーを交換する４つの場合の情報の送受信を規定する．振出取引は，新たにマネーを発行して支払いに用いる場合の取引である．分割は，持っているマネーを発行者に送信して，マネーを２つに分けて再発行してもらうやりとりである．通常取引は，持っているマネーを支払って物やサービスを購入する取引である．

精算取引は，持っているマネーを発行者に対して支払う場合の取引である．

4.1 振出取引

振出取引は，物やサービスを買う際に新たにマネーを発行する場合の取引である．

まず，発行者Ａが受領者Ｂにマネー $\{M_A\}_{SA}$ を送信する (1.1).

$$A \to B: \quad \{M_A\}_{SKA} \tag{1.1}$$
$$B \to A: \quad \{\{M_A\}_{SKA}, "ACCEPT"\}_{SKB} \tag{1.2}$$

Ｂは M_A の内容を確認した上で ”ACCEPT” 証明書を発行し，A に送信する (1.2)． この時Ｂは M_A を受け取る意思を示したことになる．

$$A \to B: \quad \{M_A, "ISSUE"\}_{SKA} \tag{1.3}$$

Ａは ”ISSUE” 証明書をＢに送信する (1.3)． この証明書がマネーの有効性を証明する．

仮にＢが，最初のマネーを受け取った時点で故意に通信を切断して，取引をうやむやにしたとしても，後日にそのマネーを使用することはできない．Ａがマネーを無効だと宣言した時，Ｂがそれを覆すには ”ISSUE” 証明書が必要になる．

また，Ｂが ”ISSUE” 証明書を受け取りながらも,「受け取っていない」と宣言して取引を中断して，後日マネーを使おうとすることも考えられる．しかし， ”ACCEPT” 証明書がＢに取引の意思があった証拠となるので，Ａは再び ”ISSUE” 証明書を送信して，Ｂに取引の継続を求めることができる．日時が過ぎていた場合には，取引を一方的に中断したことへの賠償をＢに求めることも可能である．

4.2 分割

分割は，取引に使用する額よりも持っているマネーの額面が大きい場合に，発行者にマネーを送信して，マネーを２つに分けて再発行してもらうやりとりである．

$$B \to A: \quad \{\{M_A\}_{SA}, price, \text{"}SPLIT\text{"}\}_{SB} \tag{2.1}$$
$$A \to B: \quad \{M_{A1}, \text{"}ISSUE\text{"}\}_{SA}, \{M_{A2}, \text{"}ISSUE\text{"}\}_{SA} \tag{2.2}$$

まず，所有者Bが発行者Aに "SPLIT" 証明書を送信し (2.1)，Aは新しく２つのマネーを作成して "ISSUE" 証明書をBに送信する (2.2)．

仮にAが "SPLIT" 証明書を受け取った時点で通信を切断し，Bに新しい "ISSUE" 証明書を送らなかったとする．Bがしかたなく元のマネーを使用しようとしたときにAは "SPLIT" 証明書を提示してマネーの無効を宣言することができるが，"SPLIT" 証明書を提示することにより，分割された２つのマネーをBに送信する義務を認めることになる．

4.3 通常取引

通常取引は，すでに持っているマネーを使って物やサービスを買う取引である．

$$C \to B \quad \{\{M_A\}_{SA}, B, \text{"}OFFER\text{"}\}_{SC} \tag{3.1}$$
$$B \to A \quad \{\{M_A\}_{SA}, B, \text{"}OFFER\text{"}\}_{SC} \tag{3.2}$$

まず，支払者Cが "OFFER" 証明書を発行して受領者Bに送信し (3.1)，受領者Bは内容を確認した上でそのまま発行者Aに送信する (3.2)．

$$A \to B \quad \{\{\{M_A\}_{SA}, B, \text{"}OFFER\text{"}\}_{SC}, \text{"}ACCEPT\text{"}\}_{SA} \tag{3.3}$$
$$B \to C \quad \{\{\{M_A\}_{SA}, B, \text{"}OFFER\text{"}\}_{SC}, \text{"}ACCEPT\text{"}\}_{SB} \tag{3,4}$$

発行者Aは "OFFER" 証明書に含まれているマネーがCの所有物であることを確認したうえで，"ACCEPT" 証明書を発行してBに送信する (3.3)．

BはAの "ACCEPT" 証明書を確認して，Cの "OFFER" 証明書に対して "ACCEPT" 証明書を発行し，Cに送信する (3.4)．

$$C \to B \quad \{\{M_A\}_{SA}, B, \text{"}GIVE\text{"}\}_{SC} \tag{3.5}$$

この時点で，取引についての三者の合意が成立する．Cは "GIVE" 証明書を発行し，Bに送信する (3.5)．

$$B \to A \quad \{\{M_A\}_{SA}, B, \text{"}GIVE\text{"}\}_{SC} \tag{3.6}$$
$$A \to B \quad \{M_A, \text{"}ISSUE\text{"}\}_{SA} \tag{3.7}$$

Bは "GIVE" 証明書をそのままAに送信し (3.6)，Aはバンクテーブルを更新して "ISSUE" 証明書を発行し，Bに送信する (3.7)．

この取引においては，最初の "OFFER" 証明書と "ACCEPT" 証明書のやりとりで，取引の内容を三者がそれぞれ確認して署名している．そのため，Cが送信した "GIVE" 証明書をBやAが受け取らなかったと主張しても，"ACCEPT" 証明書で取引の意思を確認しているために，Cは取引の継続を求めることができる．

4.4 精算取引

精算取引は，持っているマネーを発行者に対して支払う場合の取引である．

$$B \to A \quad \{\{M_A\}_{SA}, A, \text{"}OFFER\text{"}\}_{SB} \tag{4.1}$$
$$B \to A \quad \{\{\{M_A\}_{SA}, A, \text{"}OFFER\text{"}\}_{SB}\}_{SA} \tag{4.2}$$

まず，支払者Bが "OFFER" 証明書を発行して，発行者Aに送信する (4.1)．Aは内容を確認した上で "ACCEPT" 証明書を発行し，Bに送信する (4.2)．

$$B \{\{M_A\}_{SA}, A, \text{"}GIVE\text{"}\}_{SB} \tag{4.3}$$

それを受けてBは "GIVE" 証明書を発行してAに送信する (4.3)．

仮にAが "OFFER" 証明を受け取った時点で通信を切断したとしても，"OFFER" 証明書は "ISSUE" 証明書を反証できないので，意味はない．または，Aが "GIVE" 証明書を受け取れなかったと宣言して通信を切断し，後日に "GIVE" 証明書を提示して M_A の無効を宣言することが考えられるが，Bは "ACCEPT" 証明書を提示して取引の遂行を求めることができる．

5 実証実験

本研究では，岩手県立大学キャンパス内で流通するローカルマネー交換システムをデザインし，現在実装中である．Ｐｅｒｌ言語によるＣＧＩを用いて

おり，ＰＣやＵＮＩＸワークステーション上のブラウザおよび携帯電話からアクセスすることができる．

実装中のシステムはＣ／Ｓ型であるが，Ｐ２Ｐ型システムとの互換性を持たせられるようにする．このシステムを用いて４月から学内での運用を開始する．また，ＪＡＶＡによるＰ２Ｐのシステムを現在設計中であり，１０月までに開発する予定である．

6　まとめ

本発表では，ローカルマネーとＰ２Ｐとの親和性について述べ，ローカルマネーをＰ２Ｐネットワーク上で交換する際のプロトコルを提案した．

今後，提案したプロトコルの妥当性を実証実験を通して検証していく．

参考文献

[1] 秋山, 並河, 山根, 村山:ネットワーク型電子マネーシステムの設計と実装, 第 63 回情報処理学会全国大会論文集 5T-6,2001

[2] 秋山, 並河, 手塚, 菊池, 山根, 村山:ネットワーク上のローカルマネーシステムの提案, 第１５回情報処理学会コンピュータセキュリティ研究会論文集 p37,2001

[3] エコマネー・ネットワーク, http://www.ecomoney.net/ (2002 年 2 月 5 日参照)

[4] ゲゼル研究会,http://www.grsj.org/ (2002 年 2 月 5 日参照)

[5] LETSsystems,http://www.gmlets.u-net.com/ (2002 月 2 月 5 日参照)

[6] 「貨幣の生態学」, 北斗出版,2001 年 7 月

[7] Roger M.Needham,et al:Using Encryption for Authentication in Large Networks of Computers,Comm. of the ACM vol.21,1978