2001-CSEC-15-7

ネットワーク上のローカルマネーシステムの提案

秋山 和隆　並河 岳史　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

ローカルマネーとは用途や流通するコミュニティが限定された通貨の類似物である．本研究では，最近注目されているローカルマネーの可能性およびその P2P 型システムとの構造上の親和性に着目し， ネットワーク上で P2P 型ローカルマネー運用システムを提案し，構築する．本稿では，現在構築中のシステムの概要と P2P マネー制御プロトコルを紹介する．

The proposal of the local money system on the network

Kazutaka Akiyama Takeshi Namikawa Ichiro Tezuka Hironori Kikuchi Shinji Yamane Yuko Murayama
Iwate Prefectural University, Fuculty of Software and Infomation Science

Local money is a similar form of currency, whose use and market domain are restricted. In this research, we try and use a local money to investigate its possibility. A local money system looks similar to P2P in terms of system structure. We propose a P2P local money system on the Internet.This paper introduces our system proposal and the P2P money control protocol.

1　はじめに

ローカルマネーとは用途や流通するコミュニティが限定された通貨の類似物である．

本研究ではローカルマネーの P2P 型システムとの構造上の親和性に着目し，ネットワーク上での P2P 型ローカルマネー運用システムを構築している.研究目的は最近注目されているローカルマネーの可能性をネットワーク上で探ることである．

主な研究内容は以下の 3 点である．

・ローカルマネーを P2P 型オンラインマネーとして設計及び実装する
・大学内の実験店舗で実証実験を行い，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，現在構築中のシステムの概要と P2P マネー制御プロトコルを紹介する．

2　関連研究

まず背景について説明する。近年ローカルマネーの運動が盛り上がっており，LETS(Local Exchange and Trading System) [3]やスイスの WIR など欧米 1500 以上の地域で導入されている．

日本でも経済産業省の加藤氏が提唱するエコマネー[8]や，博報堂と LETS の提唱者マイケル・リントン氏が共同で行っている Openmoney[9]など全国 20 以上の地域で導入されている．

法定通貨があらゆる価値を一元的に数値化し交換する手段であるのに対して，ローカルマネーとは用途や流通するコミュニティが限定された通貨の類似物である． 法定通貨は，日本銀行のような中央銀行によって発行されるが，ローカルマネーはそれぞれのサービスやコミュニティごとに発行される．

LETS が代表的なコミュニティマネーであるが，WAT 精算システム[5]など新たな決済システムも登場している．

WAT 精算システムとはゲゼル研究会の森野栄一氏が提唱したシステム[5]で，借用証書型の多角間決済システムである．

3　システムモデル

今回採用するのはローカルマネーの中でも，LETS に代表されるコミュニティマネーの一種である WAT 精算システムである．

WAT 精算システムは，通帳記入型の LE

TS と違い多角間決済システムであるため P2P システムとの親和性が高い.

本研究で提案するシステムは以下の行程で動作する.

(1) 無料配布の紙券に日付・署名を入れて，ワット券を切り離し，右半分を相手に支払う．この行為を振り出し取引という.

(2) すでに振り出されたワット券は，裏書きをして，新たな支払いに使用することができる.

(3) 発行した人に借用証書が戻ってくれば，その借用証書は無効，すなわち清算される.

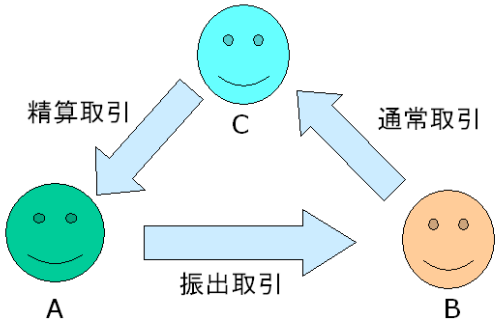

図 1　WAT 精算システム

このように，WAT 清算システムは，振出取引→通常取引→清算取引という経路をたどる多角間の清算システムとなっている(図 1 参照).

4　システム設計

本研究で提案するシステムは三段階に分けて構築する.

まず、第 1 段階目はサーバクライアント型で構築する。

つぎに、第 2 段階目は HibridP2P 型で構築する。

最後に、第 3 段階目は PureP2P 型で構築する。

4.1　クライアントサーバ型(ASP 型)

第 1 段階は現在一般的なクライアントサーバ型での実装で，価値の移動はユーザーの口座間で移動し，サーバー内で完結する(図 2 参照).

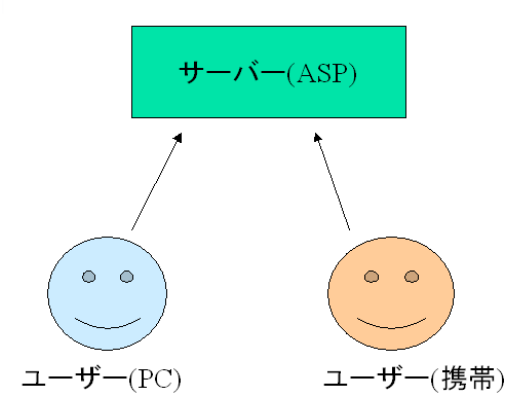

図 2　クライアントサーバ型

4.2　HibridP2P 型

第 2 段階は発行記録サーバを利用したシステムで以下のような段階を経て価値の移動が行われる(図 3 参照).

(1) 買い手はマネーを渡すことを発行記録サーバ(発行者)に通知する.

(2) マネーの額面が取引金額より大きい場合，売り手は発行記録サーバ(発行者)に分割・再発行をリクエストする.

(3) 買い手は売り手にマネーを送信する.

(4) 売り手は受け取ったマネーを発行記録サーバ(発行者)に送信し所有者を確認する.

(5) 発行記録サーバ(発行者)はマネーの所有者を書き換える.

(6) 売り手と買い手は発行記録サーバ(発行者)に了解したことを通知する.

(7) 発行記録サーバ(発行者)は了解通知が届いたら取引終了を通知し取引を終了する.

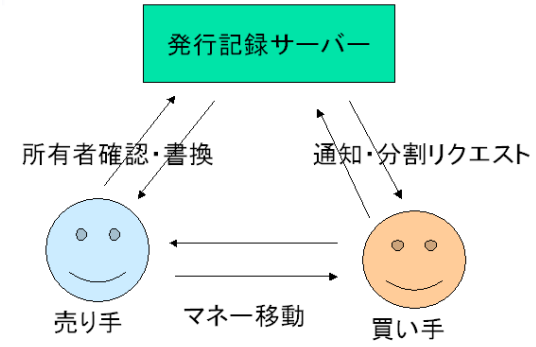

図 3　HibridP2P 型

4.3 PureP2P 型

第三段階は発行者が常時ネットワークに繋がっているのを前提としたシステムで，発行記録サーバーが発行者になる以外は基本的に HibridP2P 型と同じシステム・プロセスである(図４参照)．

想定する端末は IP リーチャブルで JAVA の動く携帯電話である．

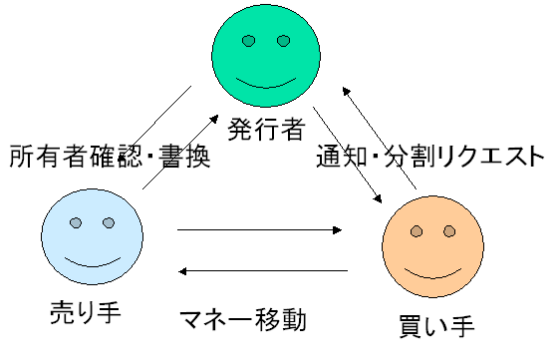

図４　PureP2P 型

4.4 システムの全体像

本研究で構築するシステム完成時の全体像は図５のような構成となり，段階が進む毎に端末機能が増えていく．

また，これら３方式は独立して排他的に動くのではなく，ユーザーがどのインターフェースから利用するか任意に選ぶことが可能である．

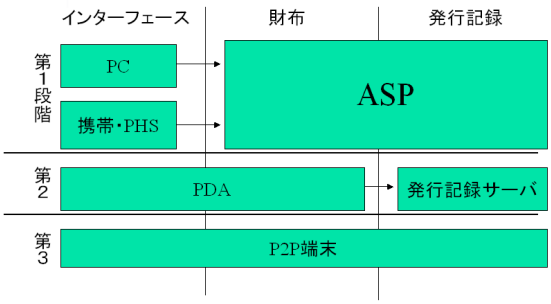

図５　システムモデルの全体像

5　実装計画

第一段階のシステムはクライアントサーバ型で構成し，ＡＳＰとして提供することになる．

使いにくいインタフェースはローカルマネー運用システム自体の普及に直接響く．従ってポータルサイトの作成段階でユーティリティやユーザビリティの問題を考慮する．

サイト構築に関して，この問題を操作性，認知性，快適性の３つに分けて取り扱う．

5.1 サイト利用の流れ

サイト利用のおおまかな流れを以下に示す．

（１）　ユーザはサイトにアクセスしてアカウントを取得
（２）　与えられたＩＤを使ってログイン
（３）　グループ情報確認してグループ参加の手続きをする
（４）　参加しているグループの取引情報を参照，提供してもらうサービスを選ぶ，または自分が提供できるサービスを公開
（５）　取引相手とメールで交渉
（６）　マネーを支払い，サービスを受ける

5.2 サイト構成

サイトは主に以下のページで構成される．

・インデックス（ログインフォーム）
・システム利用のマニュアル
・ローカルマネーの説明
・ユーザ登録，グループ登録
・個人，参加グループ情報（ログイン後）
・提供サービス情報
・マネー受け渡し
・コミュニケーションボード

"ネットワーク上でのマネー取り扱い"，"限られたコミュニティでの利用"といった性質から，ユーザに匿名性を持たせない．登録時の個人情報入力は最小限とし，第三者には個人に関する一切の情報を公開しない．

5.3 実装及び運用計画

本システムの実装は JAVA 言語を用いてサーブレット方式で実装している．

運用についてのシステムの実証実験は岩手県立大学関係者内で行なう．本大学では学生，教員，職員のすべてがネットワークに接続できる環境が整っている．加えて研究室，サークルといった多数のコミュニティが存在し，さらにコミュニティの発生が期待できる．また岩手県立大学は学生の携帯電話所有率が高いので，将来的なモバイル環境におけるローカルマネー運用を実現しやすいと考えられる．

実験の目的は以下のとおりである．

・プログラムのテスト
・インタフェースの質の向上
・セキュリティ対策の改善
・法的問題の解消
・ローカルマネーの認知・普及

現在システムは開発中であり評価・考察には至らないが，「お金」・「個人情報」を取り扱うため，考えられるあらゆる状況の推察と実験結果とで比較評価を行なう．

6　本システムにおけるマネーとその流通プロトコル

本システムのプロトコルはＰＫＩを基礎とし，全ての通信路はＳＳＬによって暗号化されていることを前提とする．グループ内のすべてのメンバーは，あらかじめ互いの公開鍵を持ち合っているものとする．P2P 型においては，グループのすべてのメンバーは，常時ネットワークに接続されていることを前提とする．この項で記述するプロトコルは，P2P を実現するのに十分な性能を持った携帯端末がリリースされた時に実装する予定の仕様であり，現行のシステムはクライアント・サーバモデルでエミュレートしたものである．

マネーの平文データの書式は，図６のようになる．マネーが保持するデータは，発行者，額面，発行日，発行シリアルの４個である．データはテキスト形式で保持される．項目が記述される順序はランダムであり，各行の前後には nonce が挿入される．これらのデータが記載されたテキスト文書は，発行者の秘密鍵で署名される．暗号文の状態で流通するので，秘密鍵を知られない限り改竄することはできない．復号は，メンバーであれば誰でも可能である．

取引時のエンティティは，「支払者（Payer)」「受取者（Accepter)」「発行者（Issuer)」の３者である．メンバーは，時と場合によって入れ替わりながら，３者すべての立場に立って取引に関わることになる．振出取引，分割，通常取引，清算取引の４つの場合に通信が行われる．

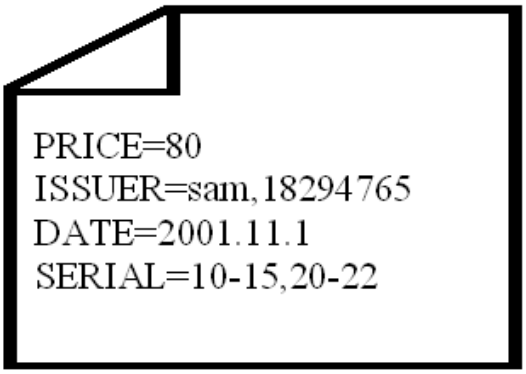

図６　マネー書式

メンバーが持つデータは，所持しているマネー，発行したマネーの所有者を記録するバンクテーブル，取引の証拠となる証明書，の３つに分けられる．このうち所持しているマネーとバンクテーブルは常にローカルで持っていなければならないデータだが，証拠となる証明書は各自が適当なホストに保存しておくことができる．

6.1　振出取引プロトコル

振出取引（図７を参照）では，支払者が受取者にマネーを発行する．この時，支払者は自分の発行限界高を超えない範囲で，マネーを発行することができる．発行したマネーは，支払者・発行者の秘密鍵で暗号化した状態で，受取者に送信する．以後，マネーは暗号化された状態で流通することになる．発行者は，発行したマネーとその所有者を自身のバンクテーブルに記録する．

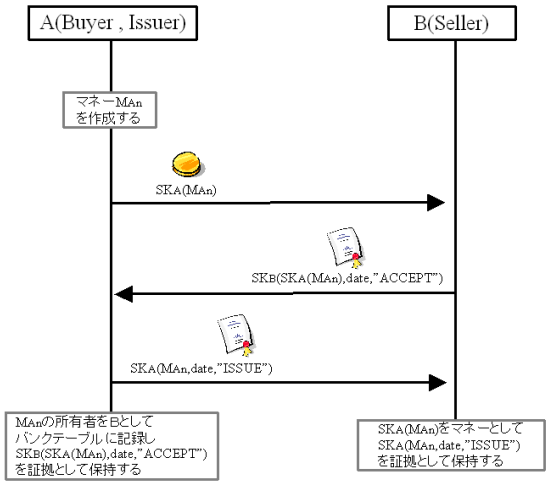

図７　振出取引プロトコル

6.2　分割プロトコル

マネーには額面が設定されており，取引の際の支払額と額面が合わない場合がある．法定通貨の紙幣であれば，受取者がつり銭を返す場面だが，全てのマネーに発行者が明記される本システムにはそぐわない．本システムでは，発行者が分割（図８を参照）を行う形式を採用する．まず，支払者は分割したいマネーを発行者に送信する．発行者は，新たに２つのマネーを作成して，支払者に送信する．支払者は元のマネーを破棄する．原則として，分割は通常取引の直前に行われる．

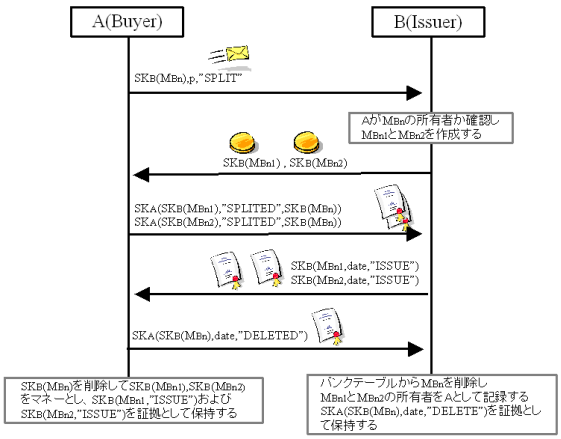

図８　分割プロトコル

6.3　通常取引プロトコル

通常取引（図９を参照）では，支払者と受取者と発行者の３者の間で通信が行われる．まず，支払者が取引証明書を作成し，受取者に送信する.受取者は内容を確認し，そのまま発行者に送信する．発行者はバンクテーブルを確認し，マネーの所有者を書き換えて,発行証明書を受取者に送信する．受取者はマネーを受け取ったことを支払者に伝える．支払者は，支払いに用いたマネーのバックアップを削除する．

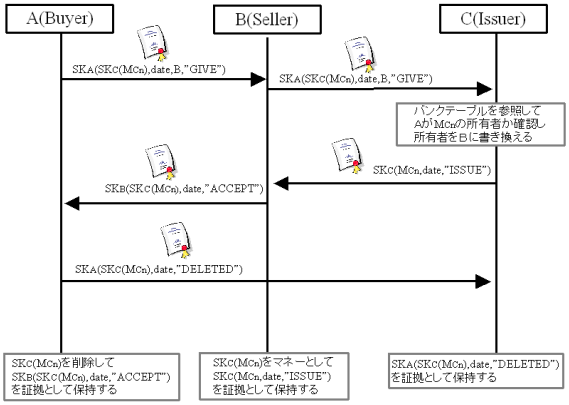

図９　通常取引プロトコル

6.4　精算取引プロトコル

清算取引は，受取者が発行者を兼ねていた場合に行われる．マネーは発行者の元に返り，削除される(図 10 参照)．

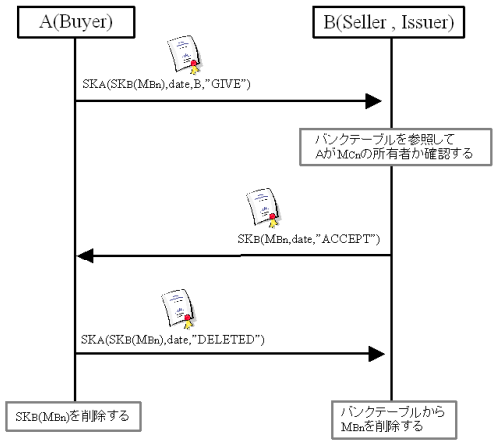

図１０　精算取引プロトコル

7　想定される問題と対策

本システムはユーザーに簡易なインタフェースを提供し，通信プロトコルはブラックボックスになっている．細部のやりとりは自動化されており，ユーザーは一切関与しない．しかし，不正対策においては，メンバーがプログラムを不正に改造して，本来は不可能な操作を行うことを想定している．本来は不可能な操作とは，たとえば任意のタイミングで通信を切断してレスポンスを返さず，データを受け取ったことを否認したり，わざと間違ったデータを送信することである．不正対策においては，利便性を損なわない範囲で最大限の安全性を得ることを目標とする．

まず，マネーを発行限界高を超えて発行することが考えられる．発行限界高は，シ

リアルナンバー（図６を参照）によって管理される．たとえばＡの発行限界高が５０単位だった場合に１０単位を支払うと，シリアルに１－１０，またはは１－５，１１－１６などのように記載しなければならない．Ａの発行限界高はグループ内で公開されており，シリアルが重複するマネーが流通すればＡの不正は露見する．本システムにおいては，誰がどのマネーを持っているかを集中管理するサーバは存在しない．そのため，短期間で発覚することを前提に言えば，ある程度の不正は可能である．しかし，コミュニティに参加したばかりの頃は発行限界高は低く設定されており，正当な取引を多く行うことで発行限界高が上がる仕組みになっている．本システムは限定された範囲で活発に流通するマネーを扱うため，この不正では行為者は労力に見合う利益を得られないだろう．

また，通信中のいくつかの個所で，偶然または人為的に通信が切断されることが考えられる．これはプログラムを改変しなくても実行が可能であるため，発生する可能性は高い．本プロトコルでは，重要なメッセージを証明書として，メンバー固有の秘密鍵で暗号化することで，プロトコルの要所に証拠が残るように設計されている．これにより，通信のどの箇所で断絶が起こっても，不正を防ぐことができる．証拠同士が相反する場合，優先順位は以下のとおりである(図 11 参照)．全ての紛争は，証拠を提示しあうことで解決することができる．

ＡＣＣＥＰＴ，ＩＳＳＵＥ ＜ ＧＩＶＥ ，ＳＰＬＩＴＥＤ ＜ ＤＥＬＥＴＥＤ
図 11 優先順位

証拠による紛争解決の一例として，支払者Ａが使おうとしたマネーを，発行者Ｂが認めない，という場合が考えられる．

考えられる不正は２つで，支払者Ａが他者に支払ったマネーを削除せずに保持していた場合と，発行者Ｂがそのマネーの所有者は支払者Ａであるのに事実を否認した場合である．支払者Ａは発行者Ｂの署名が付いた「ＩＳＳＵＥ」証明書によって，自らの所有権を主張することができる．これに対して，発行者がより優先度の高い，支払者Ａの署名付きの証明書「ＤＥＬＥＴＥＤ」「ＧＩＶＥ」「ＳＰＬＩＴＥＤ」を提示すれば，自らの正しさを証明できる．発行者Ｂが「ＩＳＳＵＥ」証明書を反証できなかった場合は，支払者Ａのそのマネーは効力を持つ．

証明書は，端末の記憶領域を多く占有することになると考えられる．証明書は各個人ごとに適当なホストに蓄積しておくことができるようにする．転送の手段としては第三者機関に頼らない方式が好ましく，ＰＧＰによって暗号化されたＥメールなどを検討中である．

一般的にローカルマネーの認知度はまだ低いといえる．ユーザに対しローカルマネーの特徴を十分理解してもらったうえで利用できるシステムが必要である．

本研究では，マネー制御プロトコルの開発と並行してポータルサイトを構築．実証実験において実際にローカルマネーシステムを運営し，ユーザの利用環境をサポートしていく．

８　まとめ

本発表ではシステムの概要からユーザービリティに至るまで，ローカルマネーシステム全般について考察した．

今後，ローカルマネーシステムの実証実験を通してセキュリティ対策の改善など一つずつ問題を解決していきたい．

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,2001

[2]D.Chaum,"Security without Identification: Card Computers to make Big Brother Obsolete,"ACM,CACM October,pp1030-1044,1987

[3]LETS system home page,http://www.gmlets.u-net.com/(2001 年 11 月 19 日参照)

[4]HotWired Japan -- Matrix vol.0025 --,http://www.hotwired.co.jp/matrix/0104/(2001 年 11 月 19 日参照)

[5]ゲゼル研究会,http://www.grsj.org/(2001 年 11 月 19 日参照)

[6] u-site,http://www.usability.gr.jp/(2001 年 11 月 20 日参照)

[7] 「WebSiteDesign vol.1&2」,技術評論社,2001 年 6 月 15 日

[8]エコマネーネットワーク,http://www.ecomoney.net/(2001 年 11 月 22 日参照)

[9]OPEN MONEY PROJECT,http://www.j-lets.net/(2001 年 11 月 22 日参照)