マイクロペイメント—デジタルコンテンツ流通のキーを握る決済手段—

Micropayments—the Payment Systems Which Hold the Key to the Distribution of Digital Contents by Noboru HATTORI and Masataka SUGANO (Research and Development Headquarters, NTT Data Corporaion).

服部　昇[1]　菅野　政孝[2]

1 NTTデータ通信(株)技術開発本部

1. はじめに

インターネットの急速な普及により，これを電子商取引に利用しようという取り組みが活発に行われています．その中でも，デジタル化された音楽，画像や，ソフトウェアなどのデジタルコンテンツは，商品の配送もインターネットで行える点で，電子商取引に適したビジネス形態であるといえます．このデジタルコンテンツの売買の決済手段として注目されているのが，マイクロペイメントです．すでに，内外で，いくつかのマイクロペイメントシステムが運用されつつあります．

本稿は，マイクロペイメントについてその概要や実現技術，さらに主なサービス提供者の概況を述べることを目的としています．

2. マイクロペイメントの概要

2.1 マイクロペイメントとは

マイクロペイメントとは，その名の通り「小額の決済」のことを指します．具体的には，取引のたびにクレジットカードを用いていたのでは，処理コストが決済額に対して無視できない金額の決済が，これにあてはまります．

現在，電子商取引のための決済手段として最も普及しているのがクレジットカードです．しかし，これを利用するためには，カード番号が無効なものでないか，利用限度額を超えていないかなどを確認するために，与信照会という処理が必要になります．この処理は，多くの場合，有料の専用ネットワークを用いて行われます．また，クレジットカードを受け付ける店舗は，クレジットカード会社に対して，加盟店手数料として売り上げ金額の数%を支払う必要があります．インターネット上の仮想店舗のように，実際に目の前で購買者にクレジットカードを提示させることができない，また伝票に署名をさせることもできない場合には，その分不正利用の可能性が高くなると考えられるため，実空間の店舗よりも加盟店手数料の割合が高くなるのが普通です（仮想店舗の加盟店手数料の割合は，7%程度のことが多いようです）☆．さらに，一定期間あたりの取引金額が小さいと，この加盟店手数料の割合がさらに高くなることもあります．

このため，たとえば10円の商品の売買には，クレジットカードによる支払いでは店舗が利益を上げることが困難となります．こういった小額の商品を売買するための決済手段が，マイクロペイメントです．

そして，このような小額の決済の主たる適用分野として，インターネット上での小単位のデジタル情報の売買が考えられます．具体的には，新聞などの情報の切り売り，データベースでの検索ごとの課金，あるいは小額のソフトウェアの販売や，仮想空間で実現されるサービスに対する時間課金などが考えられます．たとえば，電子新聞の場合，月額単位での契約だけでなく，読みたい記事がある日だけ，その電子新聞を購入するようなことが可能になります．さらには，実空間では困難だった，欲しい記事だけを購入するということが可能になると期待されています．いわゆる，「ペイ・パー・ビュー」，「ペイ・パー・クリック」が実現できるわけです．

2.2 マイクロペイメントシステムに必要な条件とその実現方式

マイクロペイメントシステムは小額商品の「薄利多売」を目的としています．このため，

- 決済にかかる処理コストが小さいこと，
- 処理が軽く，高速であること，

また，決済を伴うため

- セキュリティを確保すること，

が必要な条件になります．この条件を満たすために，マイクロペイメントシステムが採用している方式を以下に整理します．

2.2.1 実決済との連動回数の削減

実決済（インターネットの世界の金銭価値を実世界のお金に置き換える作業）は，多くの場合，クレジットカード会社や銀行などに接続された有料の金融ネットワークを利用して行われます．（インターネットの

☆ ICカードなどを用いたSETの使用により，仮想店舗での不正利用の可能性が低くなることが期待されています．

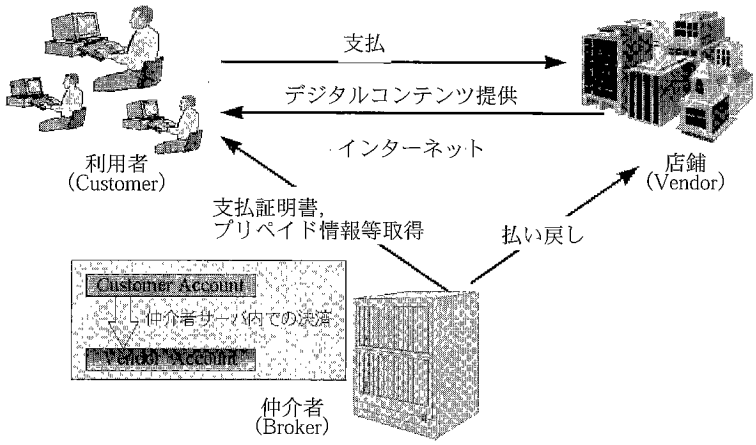


図-1 マクロペイメントシステムの構成例

世界での金銭価値を，プリペイドカードとして実世界の店舗で販売しているものもあります.）このため，この作業をまとめて行うことにより，取引1件あたりの決済コストを削減することができます．このためには，金融ネットワークとの接続は各店舗が個別に行うのではなく，第三者がまとめて行うのも有効です．

このため,多くのマイクロペイメントシステムでは，**図-1**のように，利用者，店舗のほかに，仲介者が存在する三者構成になっています．利用者および店舗は複数存在します．そして，この仲介者が，利用者および店舗のインターネットの世界での口座を管理し，取引発生の際にはこの口座間でのみ資金移動を行います．実際のお金に置き換える作業は，後でまとめてバッチ処理で，たとえば銀行口座間の資金移動などにより行われます．

2.2.2 セキュリティの簡略化

インターネットは誰でも利用できるネットワークですので,これを利用して電子決済を実現する場合には，本人認証や改竄，偽造の防止などのために，セキュリティを確保する必要があります．これには暗号化技術が用いられることが多いのですが，セキュリティを強くしようとすればするほどそのためのコストがかかります．このため，適当なセキュリティの強さはコストとのバランスで判断する必要があります．特にマイクロペイメントの場合は，セキュリティの強さをある程度下げてでも，コストを安くすることが必要になると考えられます．また，処理の高速化も必要になります．

インターネットで，本人認証および改竄の防止を保証するために広く採用されている方法は，公開鍵暗号方式を用いた電子署名です．この公開鍵暗号方式としては，RSAが広く用いられています．しかし，これはマイクロペイメントには処理に時間がかかる，またその分資源を利用するため高価であるという主張があります．このため，MITのRivestとShamirは，文献1）の中で，公開鍵暗号方式の利用回数を最小限とし，代わりに一方向ハッシュ関数を用いるPayWordという方式を提案しています．

一方向ハッシュ関数としては，MD5やSHAといったものが有名ですが，これらは以下のような特徴を持っています．

- 任意の元データから，固定長のビットパターンを作成する．
- 同じビットパターンを得る2つの元データを見つけることが困難である．(collision-resistance)

ある特定ビットパターンが抽出できるような　元データを見つけることが困難である．すなわち，逆関数の計算が困難である．(one-wayness)

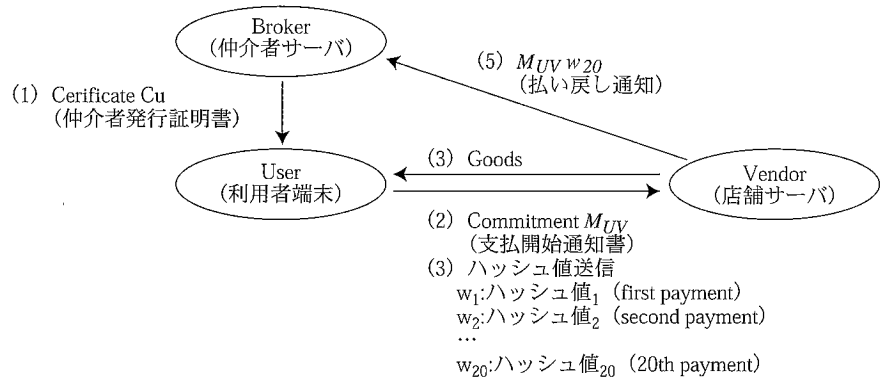
そして，この一方向ハッシュ関数は，公開鍵暗号方式による電子署名に比べて，処理速度が短いと述べています．文献1）では，典型的なワークステーション上の処理速度の大まかな見積もりとして，RSAによる電子署名は2回/秒，署名の確認は200回/秒だけであるが，これに対し，ハッシュ関数は20,000回/秒できると述べています．

図-2にPayWordの概要図を示します．PayWordは，後払いでマイクロペイメントを実現します．まず，利用者は仲介者から証明書Cuを発行してもらいます．この証明書Cuはクレジットカードのように，その利用者の信用,支払い能力などを示すものになりますが，ある程度の期間に1回（たとえば月1回）発行してもらえばよいものです．

利用者は，店舗に対して支払いを開始する前に，

(1) 任意の乱数を選び，これをたとえばMD5などの一方向ハッシュ関数にかけます．

(2) 当面必要になる度数nを決め，(1) で算出した値



User	:利用者端末
Vendor	:店舗サーバ（情報コンテンツサービス提供サーバ）
Broker	:仲介者サーバ．利用者（User），店舗（Vendor）の口座管理を行い，利用者の証明書を発行する
Cu	:仲介者発行の利用者（User）向け証明書
M_{UV}	:利用者（User）から店舗（Vendor）に送られた該店舗向け支払開始通知書（上記Cu：仲介者発行の証明書を含む）
PayWord	:一方向ハッシュ関数によるハッシュ値

図-2 PayWord概要図

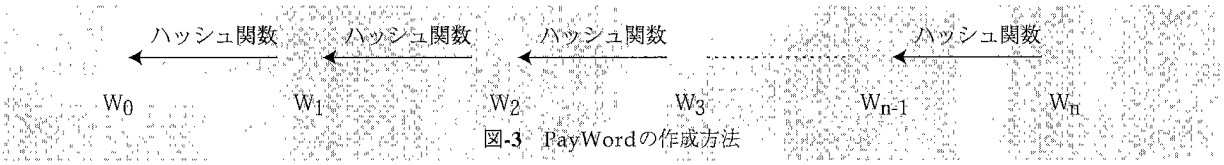


図-3 PayWordの作成方法

をW$_n$と定義します．

(3)「W$_i$を，(1) と同じ一方向ハッシュ関数にかけ，W$_{i-1}$を算出する」作業をn回繰り返して，n個のハッシュ値（W$_0$,W$_1$,…,W$_{n-1}$）を求めます（**図-3**参照）．

こうして求められた一連のW$_i$（0<i≦n）が，支払いの度数を示すものとして利用されます．W$_0$は，支払いの度数を示すものではありませんが，一連のW$_i$の根（root）として使用されます．そして，この度数に金銭価値を定義する（たとえば1度数は1円）と定義することにより，この値を支払処理に用いることができるわけです．

具体的には，まず，利用者は店舗に対して支払いを開始する際に，店舗に対して，証明書Cuと共にW$_0$の値を送信します．この際，この送信電文に利用者の電子署名を付与します．この電子署名により，店舗は利用者の認証を行います．それと共に店舗は，このW$_0$の値を保持しておきます．

その後，利用者は，仮にj度数（j>0）分の支払いを行うとすると，W$_j$の値と，度数を示すjという値を送信します．これを受け取った店舗は，W$_j$をj回，所定の一方向ハッシュ関数にかけ，その結果が保持しておいたW$_0$と同じ値であれば，その利用者による正当な支払いであると確認できます．すなわち，最初に送信した電文に電子署名を付与した利用者と，同じ利用者であることが確認できるわけです．その後，店舗は今度はW$_j$の値を保持しておきます．これにより，次回以降送信されるハッシュ値についても，店舗側で，同様な方法で正当な支払いであることが確認できるわけです．たとえば，この後，k度数分の支払いを行うときには，利用者はW$_{j+k}$（k>0）と値kを送信し，店舗はW$_{j+k}$をk回一方向ハッシュ関数にかけ，その値がW$_j$と一致すれば，正当な支払いであることが確認できます．

この方式は，処理に時間がかかる公開鍵暗号方式による電子署名の利用を，一連のW$_i$（0<i≦n）を最初に使うときのみにすることができ，その後は一方向ハッシュ関数の計算だけで支払処理が行えるため，たとえば「ペイ・パー・ビュー」に適した支払手段であると考えられます．また，ネットワーク上の不正行為に対しては，以下のような方法でセキュリティを確保できます．

- 盗聴：W$_i$（i>0）が盗聴されても，それ以降に使用するW$_{i+j}$（j>0）の値を推測するのは，一方向ハッシュ関数のone-waynessの特性によりきわめて困難です．すなわち，盗聴者には意味のない情報がネットワーク上でやりとりされます．
- 改竄：W$_{i+j}$（i>0, j>0）の値が，通信中に第三者により書きかえられてしまった場合には，一方向ハッシュ関数のcollision-resistanceの特性により，店舗側で不正が検出できます．すなわちこのとき，改竄され

表-1　マイクロペイメントシステムの例とその概要

システム名	当事者名 (法人，団体など)	概　要
Millicent	Digital Equipment Corp（米国）	○顧客および店舗は，仲介者（Broker）のサーバに仮想口座を持つ．顧客は，仲介者からベンダごとのプリペイド単位（scrip）を購入し，これを店舗への支払いに使用する． ○97年より，社内実験を実施． ○公開実験に向け，コンテントプロバイダや仲介者（Broker）を募集中．日本でも募集してる．
CyberCoin	CyberCash, 社 (米国)	○96年9月からサービス開始．米First Data社と提携．同社が決済処理を代行することで，マージンの小さい決済処理を代行． ○97年より，Digital NewsStandというコンテント販売サービスを開始． ○97年8月に，日本法人を設立．円建ての小額決済のサービスも開始予定．
Ecash	DigiCash社（蘭）	○ICカードを利用しない代表的なネットワーク型の電子通貨で，支払いのプライバシー（匿名性）を厳守 ○95年10月からMarkTwain銀行により，実通貨（米ドル）の預金をEcashで引き出し／預金できるサービスが始まり，現実の通貨としてのEcash実験を開始．
MONDEX	Mondex社 (英国)	○基本コンセプトは，現金代替機能とネットワーク機能の融合であり，ICカードと端末・ネットワーク処理を連動 ○銀行を介在せず，個人・企業間を転々として流通する現状唯一のオープンループ型システム． ○実空間での支払手段のみならず，インターネットユーザに対して仮想空間での支払手段も提供． ○97年3月に，AT&Tが，Mondexの電子現金プラットフォームを利用して，現金の利便性とICカードのセキュリティをインターネットに導入すると発表された．
VISA Cash	VISA（米国）	○ICカードを利用．実空間での支払手段のみならず，インターネットユーザに対して仮想空間での支払手段も提供． ○97年夏より，Bank of Americaと，インターネット対応の実験プロジェクトを実施すると報道されている． ○97年秋より，スマートコマースジャパン（VISA，東芝，ダイエーグループ，日本信販などで構成）が神戸で実施する電子現金実験で，インターネットでの取り引きの実験も行われると報道されている．
Bitcash	ビットキャッシュ (日)	○書店などでプリペイドカードを購入し，該カードに付与された16文字のひらがなを商品購入時に入力して利用する．
NET-U	ユーカード（日）	○インターネットで，電子プリペイドカードを購入．クレジットカードまたは銀行振込でプリペイドカードの料金を支払う． ○利用者側で，専用のソフトを利用． ○国産の暗号方式（FEAL, E-SIGNなど）を利用．
サイバーチップシステム	ペガジャパン(日)	○プリペイド方式により小額決済を実現．
サンキューシステム	富士ソフトABC (日)	○プリペイド方式により小額決済を実現．
アコシス	アコム（日）	○ポストペイド方式により小額決済を実現．
電子市場	メタマート（日）	○ポストペイド方式により小額決済を実現．

た値に対して店舗がj回一方向ハッシュ関数をかけた値は，W_iとは異なる値になります．(W_iと同じ値になる確率はほぼ0とみなせます．)

• なりすまし：利用者が証明書Cuとハッシュ根W_0に電子署名を付与することにより，店舗ではこの電文の送信を間違いなく本人（該利用者）が行ったことを確認できます．さらに，この後支払いに使用するW_i (i>0) にi回一方向ハッシュ関数にかけた値がW_0と一致すれば，一方向ハッシュ関数のcollision-resistanceの特性により，このW_iは間違いなく本人が送信したものと確認できます．すなわち，一方向ハッシュ関数をi回利用してW_0という値を作成できるのは，W_iを所有していた本人のみであるとみなせます．

このほか，Digital社のMillicentというマイクロペイメントシステムでも，電子署名ではなく一方向ハッシュ関数を用いることにより，処理速度の向上を図っています．

特に，アクセスの多い店舗サーバなどでは，このような方式による負荷の軽減も有効になりうると考えられます．

3. 最近のマイクロペイメントシステムの動向

マイクロペイメントシステムは，すでに技術検証のフェーズを終え，実際にサービス展開を行いながら，このサービスの実社会での適合性，課題等を検証するフェーズにあります．このため内外で，多くのマイクロペイメントシステムが実験運用や本運用に入っています．**表-1**に，その例を示します．

また，例として**図-4**にCyberCash社のCyberCoinのシステム構成の概要を示します．

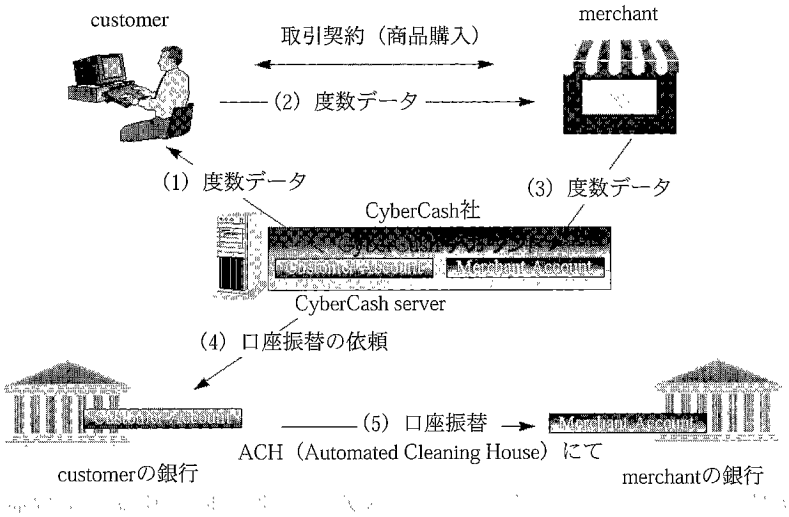


図-4 CyberCoin概要図

4. おわりに

マイクロペイメントシステムは，前章で述べたように，すでに市場で事業を開始しているものがいくつかあり，また今後もいくつかの参入があるものと想定されます．しかし今のところ，有料化に値すると利用者にみなされるデジタルコンテンツを提供できるかどうかが，大きな課題です．無料で入手できるデジタルコンテンツが大量に存在するインターネットでは，有料化に値するコンテンツには当然何らかの差別化が求められます．実店舗では入手が困難な，インターネットならではのデジタルコンテンツの提供などが鍵になると考えられます．

また，小額取引において，どのように決済サービス提供者が利益を得るのかという問題もあります．もともと売買の対象となる商品が小額ですので，相当多数の取引がなければ決済サービス提供者の収益の確保はできません．

また，売買するデジタルコンテンツの著作権の保護も，今後大きな課題となります．大量に売買されることが期待できるデジタルコンテンツ，たとえば人気アーティストの音楽などは，著作権が十分に保護されない限りは，インターネットでの配送には踏み切れないでしょう．このため，電子透かし，あるいは超流通といった著作権保護のための技術の普及が期待されています．

すでに，いくつかの業者が，電子新聞などの提供で有料化を実施していますが，その多くは，たとえば月単位，あるいは年単位の固定料金を利用者から徴収しています．マイクロペイメントは，よりきめの細かい単位での情報の売買を可能とする決済手段であり，いわゆる「衝動買い」がより実現しやすくなると期待されます．また，マスコミなどの業者が定期的に行う情報発信のみならず，たとえば個人が非定期に行う情報発信にも利用しやすい決済手段であるといえます．マイクロペイメントシステムにより，より多くの主体による，より価値の高い情報の提供や入手が，円滑に行われる世界が実現されるものと期待されています．

参考文献
1) Rivest, R. L. and Shamir, A.: MIT; PayWord and MicroMint: Two Simple Micropayment Scheme Laboratory for Computer Science
2) http://www.research.digital.com/src/millicent
3) http://a.dn.cybercash.com
4) http://www.digicash.com
5) http://www.mondex.com
6) http://www.visa.com
7) http://www.BitCash.co.jp
8) http://www.u-card.co.jp

（平成9年11月5日受付）

服部　昇（正会員）
1966年生．1989年慶應義塾大学経済学部卒業．同年NTTデータ通信（株）入社．現在，技術開発本部オープンシステムセンタに在籍．ECシステムに関する技術開発に従事．

菅野　政孝（正会員）
1950年生．1976年電気通信大学大学院修士課程修了．同年日本電信電話公社（現NTT）横須賀通信研究所入所．1988年以降，NTTデータ通信（株）においてマルチメディア通信，インターネット，イントラネットおよびECに関する技術開発，技術戦略の策定に従事．現在技術開発本部オープンシステムセンタ担当部長．著書「Java/HotJava」（共著），「ネットワークセキュリティと暗号化」（共著）など．電子情報通信学会会員．