小口決済の現状と動向

岩瀬 詔子，小村 昌弘，鳥居 悟，伊藤 裕康

1．はじめに

近年，WWW（World Wide Web）に代表される情報公開・検索サービスがブームの火付け役となり，インターネットが多くの注目を集めている．これまでは単なる通信路にすぎなかったインターネットを商業目的で利用するために，多くの研究開発が進められている［1］．

なかでも，電子商取引をインターネット上に実現しようとする動きが盛んである［2］．これが実現すると，販売店がWWWなどの情報公開サービスを用いて商品をサイバースペース上に陳列することで，消費者はいつでもどこからでも商品の参照が可能となり，さらに，気に入ったものがあればその商品の購入・代金支払が可能となる．

このような電子商取引を円滑に進めるために，さまざまな電子決済の方式が提案され，実用化に向けた社会実験が行われている［3］．現在提案されている電子決済方式は，クレジットカード決済をベースとするもの（SET, SEPP, iKP, CyberCash），銀行における小切手／手形などの決済をベースとするもの（NetBill, NetCheque, FSTC），現金決済をベースとするもの（Ecash, CAFE, NetCash, Mondex）などがある．

これらの決済方式は，既存の決済機構をベースとしているため利用者にとって親和性が高く，高いセキュリティを実現していることが特徴といえる．反面，販売店における初期費用・仲介手数料が高価であり，また，購入・決済ごとの認証処理が複雑・高コストである．

このため，情報・音楽・画像・ゲームなどのコンテンツ販売といった比較的単価が小額の決済にこれらの電子決済方式を利用するには，採算性，利便性などに問題が生じる場合がある．

そこで，小額の決済を行うことを主ターゲットとした決済方式，すなわち，小口決済方式（micropayment）が提案されている．既存の電子決済方式の一部にはこれらの小額の決済が可能なものもあるが，最近では，小口決済が，電子決済方式のひとつの分野として位置づけられている［4］．

本稿では，小額の決済を電子的に行うことを目的とした小口決済方式に関して，提案されている各方式の処理概要と機能的特徴を紹介する．具体的には，2章にて，代表的な小口決済方式の概要を示す．3章では，安全性と処理コストの観点から，各方式を比較評価する．最後に，各方式の課題と動向を中心に，まとめを行う．

2．小口決済方式の概要

小口決済方式は，決済に用いる情報の観点から，疑似現金ベース，チケットベース，課金ベースの3つに分類できる．

疑似現金ベースの方式では，それ自身が価値を示すもの（例えば，商品券に相当）を用いて決済が行われる．チケットベースの方式では，決済金額を示す識別子を含んでいるもの（例えば，回数券やタクシーチケットに相当）を用いて決済が行われる．課金ベースの方式では，決済に用いる情報には，価値や決済金額に関する情報が含まれていない．

2.1 疑似現金ベース

2.1.1 Millicent

Millicent［5］は，文字どおり1/10セントの決済を行うことを目的に，DECで開発された決済プロトコルである．

Millicentでは，scripと呼ばれる残高を表す擬似現

いわせ しょうこ，こむら まさひろ，とりい さとる
富士通研究所 Sプロジェクト部，いとう ひろやす，同，企画調査室
〒211-88 川崎市中原区上小田中4-1-1

金を決済に用いる．scripには，各販売店が発行する商品購入用のvender scripと，各ブローカが発行するvender scrip購入用のbroker scripがある．どちらもブローカから購入できる．

certificateと呼ばれる，発行者（販売店，ブローカ）だけがscripから作成可能な値（ハッシュ値注）が，scripの正当性を検証するために使用される．

さらに，secretと呼ばれる，発行者と消費者だけが知る値（ハッシュ値）が，消費者の正当性を検証するために使用される．消費者はこれを安全に保管する必要がある．

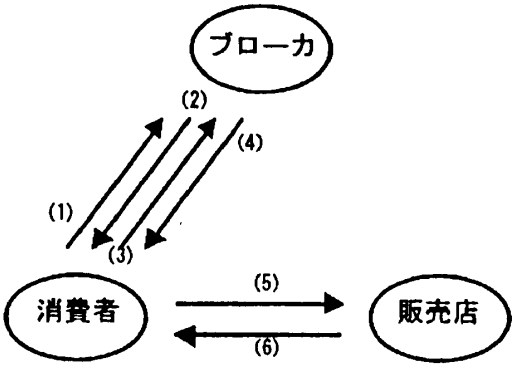

図1　Millicentの決済の流れ

1．消費者はブローカからbroker scripを購入する．
broker scrip購入時の支払方法はMillicentでは規定されていない．
2．ブローカは消費者にbroker scripを送る．
certificate，暗号化されたsecretを同時に送る．
3．消費者はブローカからvender scripを購入する．
消費者はvender scrip購入の『申込書』とbroker scripとsecretから求めたハッシュ値を，『申込書』とbroker scripとcertificateと共にブローカに送る．
4．ブローカは消費者にvender scripを送る．
ブローカは消費者の正当性と，broker scripの正当性を確認後，vender scripとcertificateと暗号化されたsecretを送る．必要ならおつりとなるbroker scripとcertificateを送る．
5．消費者は販売店から商品を購入する．
消費者は商品購入の『申込書』とvender scripとsecretから求めたハッシュ値を，『申込書』とvender scripとcertificateと共に販売店に送る．
6．販売店は消費者に商品を送る．
販売店は消費者の正当性と，vender scripの正当性を確認後，商品を送る．必要ならおつりとなるvender scripとcertificateを送る．

scripの二重使用はscrip中のシリアル番号を検査することで検出される．scripの盗難による第三者の使用はsecretから求めたハッシュ値の比較で防止される．しかし，販売店の不正請求は防止できず，消費者のscrip紛失時の再発行はできない．

2.2　チケットベース

2.2.1　PayWord

PayWord [6] は，MITのR.Rivestらによって提案された決済プロトコルである．paywordと呼ばれるハッシュ値が決済に用いられる．

消費者はまず，任意の値からハッシュ値を求める．さらに，その値からハッシュ値を求める．これを繰り返し行い，得られたハッシュ値を逆順に並べる．このハッシュ値列の先頭の値（一番最後に得られた値）をpayword rootと呼ぶ．残りをpayword chainと呼ぶ．payword chainとは，チケットの綴に相当する．paywordのpayword chainでの位置はindexで表される．

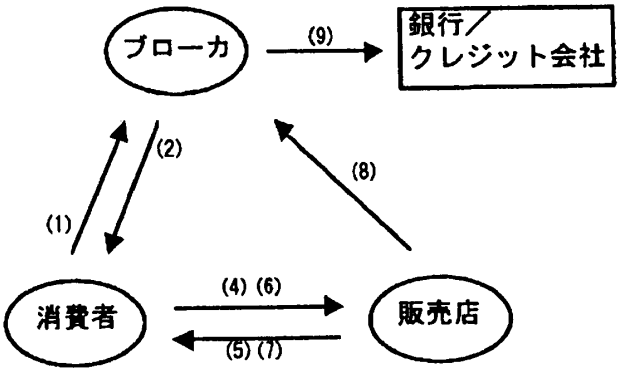

図2　PayWordの決済の流れ

1．消費者はブローカに『証明書』を要求する．
2．ブローカは消費者に『証明書』を送る．
3．消費者はpayword root，payword chainを生成する．
4．消費者は販売店から商品を購入する．
消費者はpayword rootやブローカが発行する『証明書』を含む情報（commitmentと呼ばれる）に電子署名 [7] をつけて販売店に送る．payword chainのindex番目のpaywordとindexを販売店に送る．

注）ハッシュ値とは，指定された値から一方向ハッシュ関数［7］を用いて計算し，得られた値のこと．

5．販売店は消費者に商品を送る．
販売店は電子署名により消費者を認証する．さらに，paywordからindex回ハッシュ値を計算し得られた値とpayword rootとを比較し，paywordを検証する．販売店ではcommitmentとpaywordとindexを保管する．

6．消費者は販売店から引き続き商品を購入する．
消費者はpaywordとindexを販売店に送るだけで良い．

7．販売店は消費者に商品を送る．
販売店は新しいindexと保管しておいたindexとの差分の回数だけ新しいpaywordから求めたハッシュ値と，保管しておいたpaywordと比較することでpaywordを検証する．販売店ではpaywordとindexを新しいものに置き換える．

8．販売店はブローカに決済を依頼する．
販売店は保管しておいたcommitmentとpaywordとindexを送る．

9．ブローカは決済処理をする．
ブローカはcommitmentの電子署名を検証し，paywordを検証し，決済処理をする．

PayWordでは，二重使用・不正請求はハッシュ値の比較で防止する．消費者側でpaywordを紛失した場合には，paywordを新規発行すればよい．しかし，盗難による第三者の使用は防止できない．

2.2.2 Mini-Pay

Mini-Pay [8] は，WWWの情報公開サービスで提供される小額商品の取引に用いることを目的に，IBMのA.Herzbergらによって提案された決済プロトコルである．特殊な支払指示（payment order）をやり取りすることで決済が行われる．

1．消費者はブローカに『証明書』を要求する．

2．ブローカは消費者に『証明書』を送る．

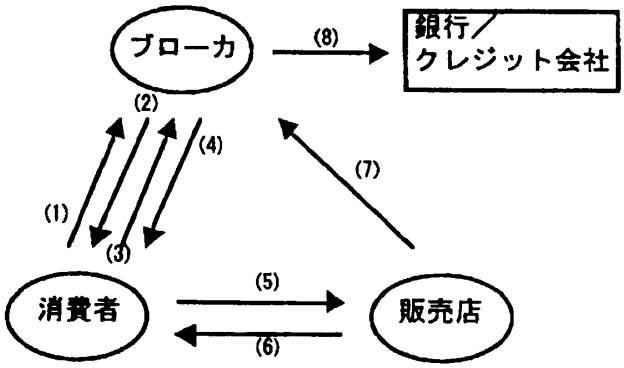

図3　Mini-Payの決済の流れ

3．消費者は毎日，ブローカに『デイリー証明書』を要求する．
この時，消費者は前日の使用合計額を申告する．『デイリー証明書』は消費者に支払い能力があることを販売店に証明するものである．

4．ブローカは消費者に『デイリー証明書』を送る．
消費者が申告した使用合計額をチェックし，販売店が依頼してきた決済金額と同じなら，『デイリー証明書』を送る．ここで，前日分の決済処理が行われる．（下記の手順8を参照）

5．消費者は販売店から商品を購入する．
消費者は『支払指示』を送る．『支払指示』にはその日のこれまでの使用金額が含まれており，『デイリー証明書』で電子署名がつけられている．

6．販売店は消費者に商品を送る．
販売店は電子署名を検証し，正しければ，『支払指示』を保管し商品を送る．

7．販売店はブローカに決済を依頼する．
販売店は，消費者が送ってきたすべての『支払指示』を，電子署名をつけて送る．

8．ブローカは決済処理をする．
ブローカは，販売店のつけた電子署名と『支払指示』の電子署名とを検証する．正しければ，翌日に，消費者が申告する前日の使用合計額と，販売店から送られた『支払指示』が示す決済金額とを比較した後，正しければ決済処理を行う．

Mini-Payでは二重使用・不正請求・盗難による第三者の使用は電子署名の検証で防止する．消費者の紛失は新規発行すればよい．

2.3 課金ベース

2.3.1 SubScrip

SubScrip [9] は，インターネット上のpay-per-viewサービス向けに，Newcastle大学（豪州）のA.Furcheらによって提案された決済プロトコルである．

販売店から購入したTicketと呼ばれる匿名性のあるアカウントにより課金が行われる．Ticketは，販売店で管理する課金情報へのポインタであり，内部にaccount-IDが格納されている．account-IDは，

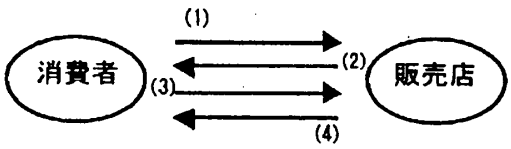

図4　SubScripの決済の流れ

Ticketを使用するたびに，新規に重複されることなく生成される．

1．消費者は販売店からTicketを購入する．
　Ticket購入時の支払方法はSubScripでは規定されていない．
2．販売店は消費者にTicketを送る．
3．消費者は販売店から商品を購入する．
4．消費者はTicketを送る．
　販売店は消費者に商品を送る．
　販売店はTicketから販売店で管理する課金情報を探し出し，あれば，課金情報を更新し，商品を発送する．商品の金額に応じて必要ならおつりとなるTicketを作成し消費者に返す．

SubScripでは，二重使用をTicket内のaccount-IDを検査することで防止する．また，消費者の紛失によるTicketの再発行は可能である．しかし，販売店の不正請求，盗難による第三者の使用は防止できない．

3．各方式の比較評価

提案されている小口決済方式は，消費者の認証処理を簡略化することで処理コストの減少を図っている．そこで，安全性と処理コストとの2つの観点から各方式の比較を行う．

3.1　安全性

認証処理を簡略化することにより，当事者および第三者の不正，争議の可能性が高まる．そこで，安全性を不正防止，争議の防止，紛失の観点からとらえ，それぞれに対する各方式の対策を比較する．

不正防止 消費者側が，すでに使用し利用価値がなくなったものを，不正に再度使用することを，販売店側で検出・防止できるのが望ましい（二重使用の防止）．

消費者が実際に購入した金額以上の請求が，販売店側で行えないのが望ましい（不正請求の防止）．

第三者が，正規の消費者からの通信データを搾取するなどして入手した決済情報を不正使用した場合，これを検出・防止できるのが望ましい（盗難使用の防止）．

争議の防止 悪意のあるなしに関わらず発生しうる，相手のミスや不正の所在を明確にできるのが望ましい．

紛失の回復 消費者側で何らかのトラブルが発生し，保存データ等が紛失した場合に，その直前の状態に回復可能であるのが望ましい．

表1 決済方式の安全性比較

	Millicent	PayWord	Mini-Pay	SubScrip
二重使用の防止	○	○	○	○
不正請求の防止	×	○	○	×
盗難使用の防止	○	×	○	×
争議の防止	×	×	○	×
紛失の回復	×	○	○	○

3.1.1　各方式の安全性比較

各方式の評価結果を，**表1**にまとめる．表中において，○印は対策可能なもの，×印は対策が不可能なものを示す．

Mini-Payは，すべての項目に対応しており，安全性が最も高い．

盗難使用の防止は運用により比較的簡単に対処することが可能であり，PayWordの安全性も高いと言える．ただし，争議の防止は信頼のおける第三者機関の設置・運用が必要となり，対処策を講じるのは困難である．

Millicent，SubScripは，Mini-Pay，PayWordに比べ，安全性に課題を残していると言えよう．

3.2　処理コスト

小口決済方式では，暗号計算のなかでも低コストな一方向ハッシュ関数を用いて認証処理の軽量化を図っている．

そこで，各決済方式の処理コストとして，暗号計算に要するCPU時間を求めた．SubScripは暗号計算を必要としないので対象から除外した．

3.2.1　基本コスト

決済方式を以下の各フェーズに区分し，それぞれにおける暗号計算回数と1日あたりの処理回数を整理した．これを**表2**に示す．

購入準備時 購入を開始するにあたって，あらかじめ行っておく必要がある処理．1月に一度の処理と，1日に一度の処理がある．

購入時 消費者と販売店間における購入処理．

請求時 販売店とブローカ間でやりとりする，請求処理．

表2において，消費者の数をC，販売店の数をV，1人の消費者が1日にアクセスする販売店の総数をVc，1つの販売店が1日にアクセスを受ける消費者の総数をCv，1人の消費者が1日に1販売店あたりにアクセスする件数をNとした．比較のため，Millicentのscripの有効期限をPayWord，Mini-Payに合わせ

表2　決済方式の暗号計算回数と1日あたりの処理回数

		Millicent			PayWord			Mini-Pay			1日あたりの処理回数
		復号化	暗号化	ハッシュ	復号化	暗号化	ハッシュ	復号化	暗号化	ハッシュ	
購入準備	消費者	—	—	—	0	2	0	1	1	0	1/30
(月に1度)	ブローカ	—	—	—	2	0	0	1	1	0	C/30
購入準備	消費者	1	0	1	—	—	—	1	1	0	Vc
(日に1度)	ブローカ	0	1	3	—	—	—	1	1	1	CVc
購入	消費者	0	0	N	1	0	0	N	0	0	Vc
	販売店	0	0	3N	0	1	N	0	N	0	Cv
請求	販売店	—	—	—	0	0	0	1	0	0	Cv
	ブローカ	—	—	—	0	1	N	0	N+1	0	CvV

1日とした.

3.2.2　モデルにおける処理コスト

復号化処理（署名）は0.5秒，暗号化処理（署名検証）は0.005秒，一方向ハッシュ関数は0.00005秒のCPU時間を要すると言われている［6］.

そこで，**表3**のようにモデルを設定し，消費者，販売店，ブローカでの，1日あたりの暗号計算に要するCPU時間を求め，パラメータの変化によるCPU時間の変化を求めた．この結果を**表4**に示す.

3.2.3　各方式の処理コスト比較

Mini-Payは，消費者，販売店，ブローカのそれぞれにおいて，多くのCPU時間を必要とする．これは，電子署名の作成・検証処理が原因と考えられる.

基本モデルの結果において，MillicentとPayWordとを比較すると，消費者にとっては差異が見られないが，販売店，ブローカにおいては，若干Millicentが低コストであると言える.

また，パラメータ変更時の処理コストの変化では，各方式でほぼ同様のふるまいを見せることが明らかになった.

ユーザがアクセスする件数が増加した場合（モデル4）には，販売店におけるCPU時間の増加率が，MillicentよりPayWordの方が低い．これはPayWordでは，初回アクセスのコストが高いが，2回目以降のアクセスのコストが低いためであり，PayWordとMillicentとのCPU時間上の優劣が逆転する.

表3　モデル

モデル	基本	1	2	3	4
消費者の数C	10,000	10倍	1倍	1倍	1倍
販売店の数V	100	1倍	10倍	1倍	1倍
消費者がアクセスする販売店の数Vc	10	1倍	1倍	10倍	1倍
販売店がアクセスされる消費者数Cv	1,000	10倍	1/10倍	10倍	1倍
消費者のアクセスする件数N	10	1倍	1倍	1倍	10倍

4．課題と動向

今回紹介した4つの小口決済方式は，安全性と処理コストに関してそれぞれ一長一短があり，これらから最良の方式をひとつ選択することはできなかった.

すなわち，Mini-Payは，唯一すべての項目を満たしており最も安全性が高いが，処理コストは一番大きい．逆に，最もコストを抑えたSubScripは安全性に課題を残している．Millicentは，PayWordよりも処理コストを抑えることに成功しているが，そのぶん安全性が犠牲になっている.

今後は，未解決な安全性の課題をどのレベルでどのように解決するか，が焦点になるであろう．方式レベ

表4　各モデルの1日あたりのCPU時間と増加率

		Millicent	PayWord	Mini-Pay
基本モデル	消費者	5.0秒	5.0秒	55.1秒
	販売店	1.5秒	5.5秒	550.0秒
	ブローカ	515.0秒	883.3秒	56173.3秒
モデル1	消費者	1倍	1倍	1倍
	販売店	10倍	10倍	10倍
	ブローカ	10倍	10倍	10倍
モデル2	消費者	1倍	1倍	1倍
	販売店	1/10倍	1/10倍	1/10倍
	ブローカ	1倍	1倍	1倍
モデル3	消費者	10倍	10倍	10倍
	販売店	10倍	10倍	10倍
	ブローカ	10倍	6.7倍	10倍
モデル4	消費者	1倍	1倍	9.2倍
	販売店	10倍	1.8倍	1.8倍
	ブローカ	1倍	1.5倍	1.8倍

ルでは安全性が低い Millicent, SubScrip においても，運用方法や制度面の充実などにより安全性に対する不安が解消され，社会的に受け入れられる可能性が残されている．

今回紹介した方式の一部は，すでに実験段階に入っている．IBM の Mini-Pay はプロトコル検証レベルの実験を開始した [10]．DEC の Millicent はすでに実証実験を終え，今秋に一般参加者を含めた運用実験に入る予定である [11]．これらの実験状況とその結果に注目したい．

5．まとめ

本稿では，小額の決済を行うことを主ターゲットとして提案されている Millicent, PayWord, Mini-Pay, SubScrip の 4 方式を紹介し，それぞれを安全性と処理コストの面から比較評価した．

紹介した小口決済方式は，安全性と処理コストに関してそれぞれ一長一短があり，最良の方式をひとつ選択することは困難であった．われわれは比較評価の観点として安全性と処理コストを挙げたが，これ以外にも，流通性，利便性，匿名性（プライバシー保護）等，さまざまな観点が考えられるであろう．

決済方式が実用化され広く一般に普及するためには，方式レベルだけではなく，消費者の利便性，販売店やブローカの収益構造，運用方法や制度面の充実などを含めた広範囲の検討が必要である．商業目的での利用にあたっては，今後の実証実験，運用実験の結果をみながら，実際の運用形態に即した決済方式を選択することが必要であろう．

本稿が，決済方式の選択のひとつの判断材料となれば幸いである．

参考文献

[1] 特集 エレクトロニック・コマース，情報処理，Vol.38, No.9, 1997.

[2] エレクトロニック・コマースの技術的課題と社会的効果，1996年 電子情報通信学会基礎・境界ソサイエティ大会 パネル討論会，電子情報通信学会基礎・境界ソサイエティ，1996.

[3] 「電子決済，電子現金とその利用環境整備に関する調査研究会」報告書，郵政省電気通信局，1996.

[4] Donal O'Mahony, Michael Peirce, Hitesh Tewari. *Electronic Payment Systems*. Artech House, 1997.

[5] Steve Glassman, Mark Mannase, Mart Abadi, Paul Gauthier, Patrick Sobalvarro. *The Millicent Protocol for Inexpensive Electronic Commerce*. Digital Equipment Corporation, 1995.

[6] Ronald L. Rivest, Adi Shamir. *PayWord and MicroMint: Two simple micropayment schemes*. MIT, 1996.

[7] 櫻井 幸一 監訳，暗号理論の基礎，共立出版，1996.

[8] Amir Herzberg, Hilik Yochai. *Mini-Pay: Charging per Click on the Web*. IBM, 1997.

[9] Andreas Furche, Graham Wrightson. *SubScrip - An efficient protocol for pay-per-view payments on the Internet*. Department of Computer Science The University of Newcastle, 1996.

[10] Mini-Pay Home Page
http://www.ibm.net.il/ibm-il/int-lab/mpay/

[11] Millicent Web Site
http://www.millicent.digital.com/index.html