Vol.37 No.4　　情 報 処 理　　Apr. 1996

特別論説

情報処理最前線

電子現金の最近の動向†

大塚 玲††　篠原 健††

1. はじめに

最近のインターネットの急速な拡大により，インターネットを用いて通信販売や情報サービスなどを行ういわゆるサイバビジネスが急増している．全体の規模はまだまだ小さいが，国内の店舗数は95年9月の145店から3カ月後の12月には414店[1]へ激増しており，米国で既に約8,000店が開業していることを考えると，今後もその勢いは衰えそうもない．

特に情報サービスを主とするサイバビジネスでは，デジタルライブラリやソフトウェアの利用課金といった新しい商品と販売形態が提案されており，今後のコンピュータネットワークの進展に加速されて大きく発展すると思われる．これらの販売形態は，たとえば百科事典の1ページを10円で販売するなど，10円や100円といったきわめて小額の取引いわゆるマイクロペイメントが主流となると言われており，電子現金はこのような少額商品・サービスの有望な決済手段として注目されている．

電子現金の実体は，額面の価値を保証するために銀行の署名が施されたデジタル情報である．現金をデジタル情報化する利点は，現金そのものが持つ(1)匿名性(顧客の購買に関するプライバシーが店舗や銀行に漏れない)，(2)相対性(取引に顧客と店舗以外の第三者が介在しない)に加えて，新たに(3)移転性(ネットワークなどを介して電子的に価値を移動できる)を現金に付与できるので，少額の現金に対しても世界中を瞬時に移動するほどのモビリティを持たせることができ，遠隔地への支払いに要するコストをほぼゼロにできる点にある．

現在，社会実験の段階にある電子現金は(1)ICカード型と(2)ネットワーク型に分類することができる．(1)ICカード型は，実現する上で耐タンパー性(装置内の内部情報に対する不正な読み出し，書き込みが難しい)を持つハードウェアが不可欠な電子現金である．これに対して(2)ネットワーク型はコンピュータネットワークの存在を仮定し，ネットワークに接続されているパソコンで利用できる電子現金である．ICカード型には利用者による取扱いが便利な反面，大規模な設備投資にかかる費用負担をサービス提供者と利用者の間でどのように配分するかという課題があり，一方ネットワーク型には，既存のネットワーク資源を活用するためサービス提供者に必要な設備投資は少ないが，コンピュータ設備を持つ人だけに利用が制限されるという課題がある．

本稿では，まず海外における電子現金の社会実験を紹介し，電子現金の基本的な仕組みと最近の研究動向を解説する．

2. 電子現金の社会実験プロジェクト

本格的に電子現金が普及するまでには，技術的な研究開発だけではなく，社会的に受け入れられるための消費者の啓蒙や法制度の見直しが少なからず求められる．こうした技術は多数の消費者を対象にしてある程度大きな規模の社会実験を行わない限り明らかにならない問題も多数ある．すでに海外では，イギリスのNational Westminster銀行とMidland銀行が中心となって進めているMondexや，オランダのDigiCash社が中心に進めているecashなどの先駆的な社会実験が開始されており，ここではまずこれらの社会実験がどのように進められているかを説明する．

---

† On Electronic Cash by Akira OTSUKA and Takeshi SHINOHARA (Center for Advanced Social Systems Research, Nomura Research Institute, Ltd.).

†† (株)野村総合研究所　新社会システム研究センター

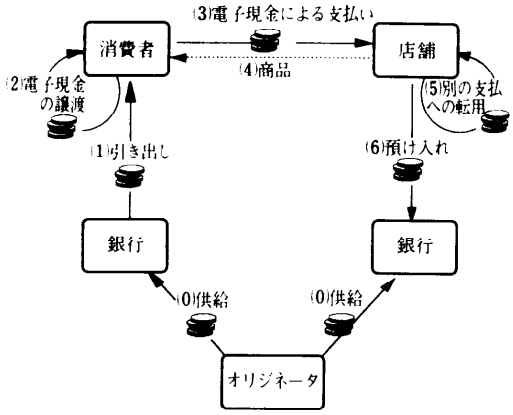

図-1 Mondex の電子現金システム

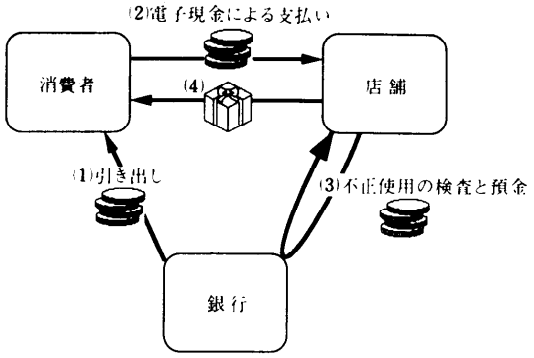

図-2 DigiCash の電子現金システム

2.1 Mondex

Mondex は耐タンパー性のある IC カードで実現された電子現金システムであり，イギリス最大の National WestMinster 銀行と Midland 銀行が中心となって実験を進めている．利用者には Mondex カードと呼ばれるマイクロプロセッサが埋め込まれたクレジットカード大のカードが配られる．このカードには電子現金が蓄えられ，Mondex 加盟銀行の ATM や Mondex 電話と呼ばれる専用の電話を利用して預金口座から Mondex カードへ電子現金を引き出せるようになっている．店舗には Mondex カードの読み取り装置が設置してあり，消費者は店頭で商品と引き替えに Mondex カードを提示し，店舗に設置してあるカード読み取り装置を使って決済を行う．また，Mondex 電話や Mondex 財布などの機器を使えば個人間での送金も可能になっている．

95 年 7 月からロンドン近郊の Swindon で実験が進められており，1,000 近くの店舗と約 8,000 人の消費者が実験に参加している．Mondex カードの使用料は当初の 6 カ月はプロモーションのために無償としているが，その後は月 1.5 ポンドの定額料金が必要になる．しかし支払い手数料は無料であり，何回使っても手数料はかからない．Mondex 電話を利用すれば遠隔地への送金にも利用でき，将来はインターネットでの利用も計画されている．サービスの提供主体の立場から見ると，当初は消費者に Mondex カードを配布する必要があるため，社会インフラを構築するまでの初期投資が大きい点に難があるが，いったん普及すれば処理が完全に分散された安価な電子現金システムとなる．Mondex の電子現金システムは**図-1** に示すような構成になっており，銀行が共同出資で設立したオリジネータが，銀行に電子現金を現金と交換で供給するしくみになっている．Mondex はカナダ，アメリカ，日本でもすでにコンソーシアムを設立して実験の計画を進めている．

2.2 DigiCash

DigiCash 社は後述の Chaum がアムステルダムに 1989 年に設立した会社で，偽造の難しい電子現金(ecash)をソフトウェアのみで実現している．このため，ネットワークに接続したパソコンがあれば誰でもすぐに電子現金を利用できるようになる点が大きな特徴である．**図-2** にこのシステムの概要を示す．

94 年 10 月から現実の通貨とは交換しない仮想通貨による社会実験を開始している．この実験では，インターネット上に銀行といくつかの店舗を開き，参加希望者に 100Cyberbucks(Cyberbuck は仮想通貨の単位)を配布し，店舗を通してデジタル商品を売買できる環境を提供している．参加者は自らの商品を持ち寄って，インターネット上で自由に店舗を開設できるようになっており，約 150 の店舗がすでに開業している．95 年末の時点で 60,000 人が参加する大規模な社会実験である．

さらに 95 年 10 月からセントルイスにある Mark Twain 銀行により、米ドルと交換する ecash の実験が開始された．米ドルと電子現金の交換時に 2% ～ 5% 程度の手数料と月額 2 ドルか

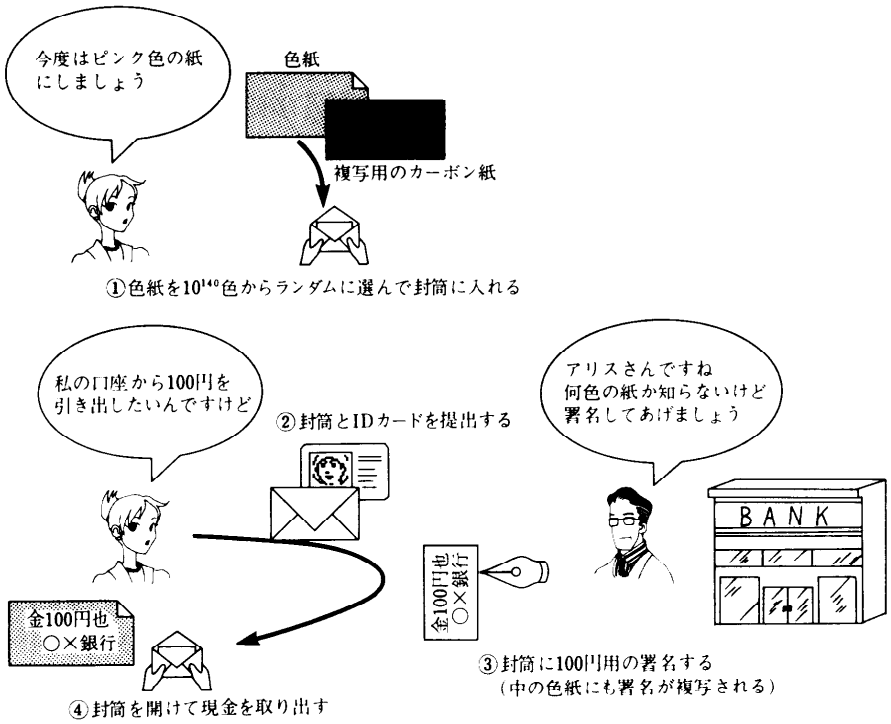

図-3 オンライン型電子現金の預金引き出しプロトコル

ら5ドルのサービス料金が必要となる．昨年12月末までのわずか2カ月で数千人の消費者と20店舗ほどが参加している．Mark Twain銀行のecashは，現在のところMark Twain銀行でしか米ドルと交換できず，Mondexのような銀行の組織化は進んでいない．96年3月からはフィンランドにおいてインターネットプロバイダーEUnetとフィンランド最大の銀行Meritaによって同様のサービスが開始された．これを受けて今後，これら複数の銀行がどのように組織化されるかが注目される．

3. 電子現金の基本方式

電子現金の基本的なアイディアは80年代の前半にChaumによって発明され，88年にChaum, Fiat, Naorらによって示された電子現金システム[5]がその後の多くの研究の基礎になっている．

ここではまず，最も単純なオンライン型の電子現金[4,5]について解説する．オンライン型電子現金は，取引時に店舗が銀行とオンラインで接続されている必要があるため，はじめに電子現金の特徴として述べたような相対性はないものの，移転性や匿名性を満たすはじめての決済手段として重要である．

以下では，まずこのプロトコルを色紙と封筒を使って説明し，その後に数式による説明を加える．利用者が銀行から電子現金を引き出す際のプロトコルを**図-3**に示す．

(1) 利用者は10^{140}色ある色紙の中から1色を選び(480bit程度を仮定)，複写用のカーボン紙と共に封筒に入れる．

(2) 次に銀行から口座の持ち主であることを証明するIDカード(預金通帳でもよい)と引き出したい金額を銀行に伝え，ステップ1で作成した封筒を銀行に渡す．

(3) 銀行はIDカードによって利用者を認証すると，利用者の口座から指定された金額を引き落とし，封筒の上から銀行の署名を施す．

(4) 利用者はこの封筒を開封し，中の色紙に銀行の署名があることを確かめる．

このプロトコルでは，利用者がランダムに選んだ色紙を封筒に入れ，中を見せないようにして銀行に署名させることにより(ブラインド署名)，現金の匿名性が実現されている．後にこの紙幣(署名された色紙)が銀行に預け入れられても，この紙幣がもともとどの利用者によって引き出された

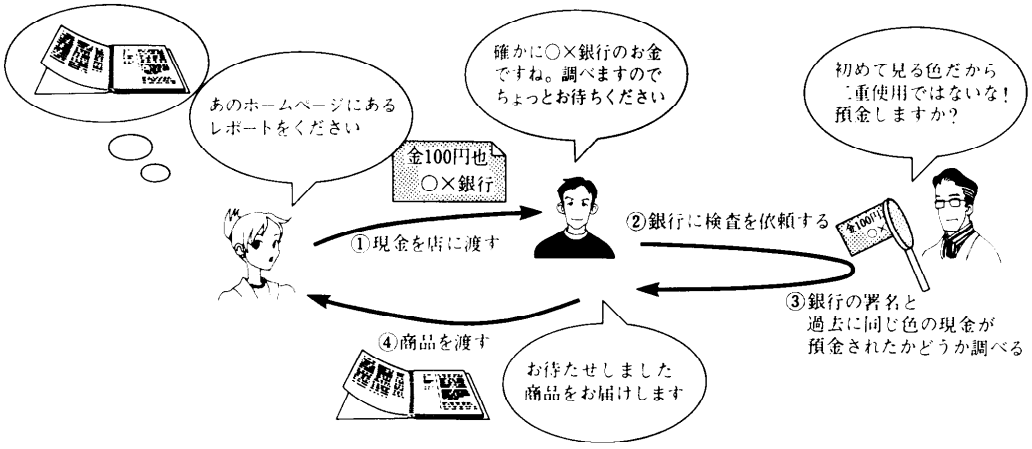

図-4 オンライン型電子現金の支払プロトコル

ものかは銀行にはまったく分からない．したがって，利用者は匿名性を保ったまま紙幣を支払いに当てることができる．

この紙幣を使った支払いプロトコルは**図-4**のようになる．

(1) 利用者と店舗の間で商品と金額についての交渉が成立すると，利用者は商品を指定して先ほどの紙幣を店舗に渡す．

(2) 店舗は紙幣を受け取るとすぐに二重使用の有無を銀行に検査してもらう．

(3) 銀行はまず紙幣に施されている銀行の署名を確認し，次に同じ色の紙幣が過去に預金されたことがないかどうかを銀行にあるデータベースを使って調べる．もし，預金されていなければ新たに預金し，データベースにこの紙幣の色を登録する．

(4) 店舗はこの紙幣が銀行に正しく預金されたことを確認すると，商品を利用者に届ける．

電子現金はデジタル情報なので，完全なコピーを得るのはきわめて容易である．したがって，銀行から正当に引き出した電子現金をコピーして複数の店舗に対して支払うといった種類の不正利用は非常に簡単にできてしまう．このプロトコルでは，過去に銀行に預け入れられた紙幣の色をすべてデータベースに記録しておき，新しく預金される紙幣との色の重複をチェックしている．もし同じ色の紙幣が預け入れられた場合には，二重使用と見なして預金を拒否する．一見，荒っぽい方法に見えるかもしれないが，色の種類は 10^{140} もあるので，良い乱数生成アルゴリズムを用いれば，同じ色を選択する確率は膨大な紙幣の流通量を考慮しても無視できるほど小さい．

次に，このオンライン型電子現金を数式を用いて表す．以下の演算はすべて mod n（n は銀行の RSA 剰余）で行う．

オンライン型電子現金における紙幣は（x, $f(x)^{d_B}$）の形で表される．ここで x は利用者が作成した乱数，f は適当な一方向性関数，d_B は紙幣の額面に対応した銀行の秘密鍵（銀行は紙幣の額面に対応した複数の秘密鍵を持っている）．オンライン型電子現金における紙幣は，乱数とその乱数に対する銀行の RSA 署名の 2 項組で構成されており，この紙幣の偽造は RSA 署名の偽造が難しいことに依存している．

この紙幣の匿名性は以下の預金の引き出しプロトコルで実現される．

(1) 利用者は x とブラインド変数 r をランダムに選び，引き出したい金額に対応する銀行の公開鍵 e_B を使って $B=r^{e_B}f(x)$ を計算する．

(2) 利用者は ID カードを提示し，引き出したい金額（100 円）とともに B を銀行に渡す．

(3) 銀行は B に 100 円に対応する署名を施した B^{d_B}(mod n) を計算し，利用者に送る．同時に，利用者の口座から 100 円を引き落とす．

(4) 利用者は B^{d_B} を r で割って，$C=f(x)^{d_B}$ を得る．一応，$C^{e_B}=f(x)$ で銀行の署名を確認しておく．

このプロトコルにおいて銀行は B しか受け取

らないので，x や C の値についてはいっさい分からない．しかし，利用者の ID カードが提示されているので適切な口座から指定金額を引き落とすことができ，実際に紙幣として用いられる C の内容を知らずに B に署名しても銀行にリスクはない．この結果得られる B^{d_B} は，$(r^{e_B})^{d_B} \equiv r \pmod n$ より $r \cdot f(x)^{d_B}$ の形になっているはずであり，利用者がこれを r で割ると最終的に銀行の署名が施された正当な紙幣 $(x, f(x)^{d_B})$ を得ることができる．

この紙幣を使った支払いは次のプロトコルで実現される．

(1) 利用者は (x, C) を店舗に渡す．

(2) 店舗は，これを受け取るとすぐに銀行へ連絡して同じ (x, C) の組がすでに預金されていないか調べてもらう．

(3) 銀行は，この紙幣の署名を $C^{e_B}=f(x)$ で確認し，もし預金されていなければ (x, C) を預金する．

(4) 預金を確認すると店舗は商品を利用者に渡す．

この節の前半で述べたように，銀行は過去に預け入れられた紙幣をすべてデータベースに登録しており，新しく預金される紙幣をこのデータベースと比較することにより二重使用を検出する．

4. 最近の研究動向

Chaum らによるオンライン型電子現金を起点として，その後さまざまな電子現金方式が提案されてきた．これらの経緯を**図-5** に示す．ここではこれらの中でも特に基礎的な成果として (1) オフライン型電子現金 (2) オブザーバ (3) Single-Term Coin (4) 分割利用可能性を中心に紹介する．

4.1 オフライン型電子現金

オンライン型電子現金でも電子現金としての最小限の機能を持っているが，支払いの度に銀行へのアクセスが必要になるので，取引量が増加すると銀行の負荷が無視できなくなる点に問題がある．これに対して，オフライン型電子現金は消費者と店舗だけで取引が行われ，たとえば 1 日の終わりなどの適当な時間に，店舗が電子現金をまとめて銀行へ預け入れることができる電子現金である．これによってはじめに述べた相対性が実現され，支払いを迅速に行えるようになる．

しかしこの方式の最大の問題は，悪意のある利用者により電子現金が二重使用された場合に，店舗が二重使用と気づかずに商品を渡してしまうのを避けられないことにある．Chaum ら[5] はこの問題に対する 1 つの解として，あらかじめ紙幣の中に利用者の ID を埋め込んでおき，通常の使用では利用者の ID に関する情報はまったく漏れないが，二重使用したときには非常に高い確率でこの ID を発覚させることで二重使用を抑止する方式を示した．

この方式では，まず利用者があらかじめ定められた方法を使って自分の ID を色紙の中に埋め込んでおき（実際には，両方が揃うと利用者の ID が求められるような 2 つのヒント A, B を一方向性関数で隠して色紙に入れておく），この色紙に対して **3.** で述べたのと同様に色を銀行に明かさずに署名させて紙幣を作る（ブラインド署名）．しかし，これだけでは利用者が正直に紙幣の中に自

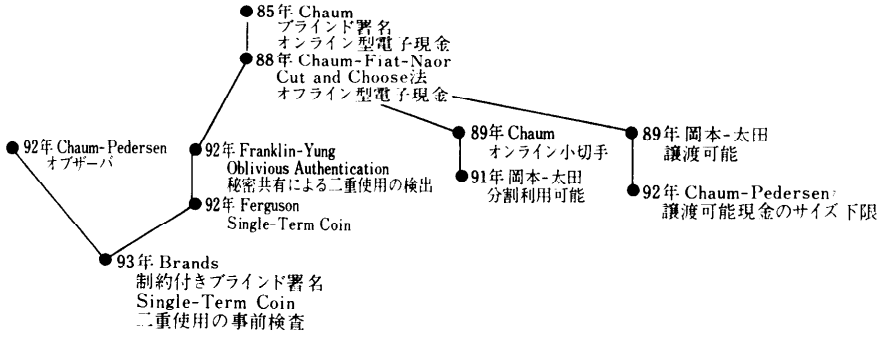

図-5 電子現金に対する研究経緯

分のIDを埋め込んだという保証が得られない．このため，彼らは“Cut and Choose法”（二人でケーキを公平に分けるには，ナイフで切る人と最初に選ぶ人を分ければよい）と呼ばれる手法を用いて利用者が自分のIDを正しく埋め込むことを保証している．すなわち，まず利用者に紙幣を40枚程度作らせ，銀行がこのうちの半分をランダムに選択し，これらが正しく作られていることを利用者に証明させる．次に，この証明に使った紙幣は捨て，残りの20枚を一枚分の紙幣として銀行が署名する．このようにすれば，利用者が故意に40枚の紙幣のうちのk枚に他人のIDを埋め込もうとしても高々$1/2^k$以下の確率でしか成功せず，正しく紙幣を作らざるを得なくなる．

次にこの紙幣を店舗に支払うには，まず先程の20枚の紙幣を店舗に渡す．次に店舗は20枚の一枚一枚について，紙幣に隠された2つのヒントA，Bの一方をランダムに選んで利用者に提示させる．後にこの紙幣を銀行に預け入れるときには，店舗は20枚の紙幣と対応する20個のヒントを銀行へ渡す．この時点で，もしこの紙幣が二重使用されており，すでに同じ色の紙幣と別の20個のヒントが銀行のデータベースに記録されていれば，銀行には同じ紙幣に対応する20個のヒントが2組揃うことになる．20個のうち少なくとも1つのヒントは，圧倒的に高い確率でA,B両方のヒントが揃うはずであり，これらのヒントを利用して利用者のIDが求められる．

4.2 オブザーバ

92年にChaum，Pedersenら[16]は，サービス提供者の指示通りに働く耐タンパー性のあるハードウェアT（オブザーバ）と，利用者が自由に制御できるコンピュータCを適切に組み合わせれば，すなわちサービス提供者とTの間のすべての通信にCが介在するように構成すれば，利用者のプライバシーなどの権利をコンピュータCで守りつつ，コンピュータCが不正な動作を行わないことをオブザーバTで保証できることを示した．

Chaumらは，耐タンパー性のあるハードウェア（ICカードなど）をサービス提供者が発行する従来方式の問題点として，利用者のプライバシーに関わる情報を勝手にこのハードウェアがサービス提供者に漏らさないことを保証できず，結局利用者はサービス提供者を信頼するしかない点を指摘し，(1)Cが予定されたプロトコルを守る限り，Cに隠れてサービス提供者とTが互いに情報を交換することはできない，(2)サービス提供者はTによって承認されたサービス要求にしか応じないので，Cが予定されたプロトコルを守りTの承認を得ない限り，利用者はサービスを享受できない，というプロトコルが実現できることを示し，このプロトコルを使えばサービス提供者への信頼のみに頼らなくても良いことを示した．

翌年の93年には，Ferguson[10]やBrands[3]によって，このオブザーバの考え方を応用して電子現金の二重使用を未然に防ぐ方式が提案された．

これらは，銀行から引き出されたすべての紙幣を利用者のコンピュータとオブザーバの両方で管理させ，紙幣を使う際には必ず紙幣にオブザーバの署名が必要なしくみになっている．すなわち，オブザーバは一度紙幣に署名すると二度と同じ紙幣には署名せず，銀行も紙幣にオブザーバの署名がなければ預金を受け付けない．したがって，店舗もオブザーバの署名がないと紙幣を受け取らないので，これによって悪意を持つ利用者がコンピュータを操作して二重使用を試みても，店舗にすぐに気付かれて二重使用は未然に防がれる．また，彼らの方式は万が一オブザーバが破壊され，オブザーバのにせ署名が二重使用された紙幣に付与されたとしても，銀行が従来通りの二重使用の検査を行えば預金時に不正利用者のIDが発覚するように二重の検査体制を構築している．

この方式は，ESPRITプロジェクトのCAFE（Conditional Access for Europe）[2]における電子現金システムにも応用され，開発が進められている．

4.3 Single-Term Coin

Chaumのオフライン型電子現金は，通常の使用において利用者のプライバシーが完全に守られている点で画期的だったが，電子現金システム自体についての安全性の証明がない，効率が悪いという課題が残されていた．その後，89年に岡本，太田ら[12),14]や92年にDeSantis，Persianoら[8]によってゼロ知識証明を使って，安全性が証明でき，かつより効率的なオフライン型電子現金を実現できることが示された．その後，92年にFranklinとYung[11]らはゼロ知識非対話証明と秘密共有を使って，画期的に効率の良い電子現金方式が構成

できることを示した．この方式の概要を以下に示す．まず，(1) 利用者のIDを埋め込んだ紙幣(passport)と紙幣からIDを取り出すための鍵(witness)をOblivious Authenticationと呼ばれる手法を使って銀行が利用者に発行する(ただし銀行はこの紙幣と利用者のIDを結びつけられない)．(2)支払いの際に利用者は店舗に紙幣と，鍵についてのヒントを渡す．ただしこのヒントは鍵と取引先の店舗ID，日時などからユニークに計算され，1つのヒントからは鍵に関する情報はまったく得られない．しかし，二重使用により異なる店舗，時刻を元に作られたヒントが2つ揃うと鍵が露呈し二重使用した利用者のIDが判明するようになっている．

この電子現金システムは，預金の引き出し時には2往復のメッセージが必要だが，支払いと預け入れは1メッセージで実現できるため通信量が大幅に削減される．

しかしFranklinとYungの方式は，Oblivious Authenticationを効率的に実現するために中立的なセンタの存在を仮定していた．その後，Ferguson[9,10]とBrands[3]らは，そのようなセンタの存在を仮定せず，しかも紙幣を単一の項(Single-Term)で表せる電子現金システムを提案した．これによって紙幣の保管に必要な記憶容量とプロトコルの実行に必要な通信量が劇的に削減され，オフライン型の電子現金は大幅に効率化され実用化に近づいた．

4.4 分割利用可能性

分割利用可能性は現金にもない性質であるが，小銭の管理が不要になるなどの利点がある．Mondexやプリペイドカードなどはすで　にこの性質を持っている．ただし，Mondexやプリペイドカードなどのように金額を連続値で表すシステムは分割利用は容易に実現できるが，同時に残高データを書き換えられる危険を伴うため，このような偽造から保護するために媒体の物理的な安全性に頼らざるを得ない側面がある．

一方，銀行のデジタル署名によって紙幣を表す電子現金システムでは紙幣価値の分割は容易ではない．しかし，もし紙幣の価値を分割して利用できれば，前述の小銭の管理が不要になるといった利点に加えて，電子現金の保管に必要な記憶量を少なくできる利点があり，特に記憶容量の少ないICカードでの実現に有利である．

分割利用可能な電子現金の1つとしてChaumら[5,6]は，匿名性を持つ小切手に似た仕組みを提案した．この仕組みは，一度に限り額面以下の任意の金額についての支払いが可能であるが，残金は銀行に払い戻してもらわなければならないという制約があった．その後，岡本，太田[13,15]らによって，支払い額の合計が額面の金額になるまで何回でも利用できる電子現金システムの構成法が示された．

彼らの方法の概略を以下に示す．まず，各節が親の金額の半分を表すような2分木を設定する(親が100円のときは，その2つの子はそれぞれ50円を表す)．この2分木を使うと分割利用の条件は次のように表すことができる．(1)ある節が利用されるとその節の祖先および子孫はすべて利用できない，(2)各節は一度しか利用できない．

彼らはこのような条件を実現するために，RSA剰余nにおける任意の平方剰余が持つ4つの平方根のうち，ある性質を満たす2つの平方根が判明すると，nを素因数分解できることを用いている．すなわち，もし条件に反した利用があると2つの平方根が揃い，nを素因数分解できて，紙幣に隠されていた利用者のIDが判明する．

5. おわりに

本稿では最近注目を集めている電子現金の最近の動向について述べた．電子現金が今後さらに社会システムにまで成長するためには，さらなる技術・社会・法制度などからの総合的な研究が必要となる．昨年からは通産省，郵政省，(財)金融情報システムセンターなどで電子現金に関する研究会が始まり，単なる技術ではなく社会的な色彩を帯びつつある．今後はさらに，電子現金を受け入れるための法制度の改革やマネーロンダリング，取引トラブルなどの社会的問題を回避するための技術開発が求められるだろう．本稿がこのような電子現金に関わるベンチャー事業および研究開発を志す方々の一助となれば幸いである．

参考文献

1) 朝稲，村上:サイバービジネスケースバンク，http://www.ccci.or.jp/cbcb.

2) Boly J.P., et.al:The Esprit Project CAFE − High

Security Digital Payment Systems －, Proc. of ESORICS'94, pp.217-230 (1994).
3) Brands S.:Untraceable Off-line Cash in Wallets with Observers, Proc. of CRYPTO '93, pp. 302-318 (1994).
4) Chaum D.:Security without Identification: Transaction Sytems to Make Big Brothers Obsolete, Comm. of the ACM, Vol. 28, No. 10, pp.1030-1044 (1985).
5) Chaum D., Fiat A. and Naor, M.:Untraceable Electronic Cash, Proc. of CRYPTO '88, pp.319-327 (1988).
6) Chaum D.:Online Cash Checks, Proc. of. EUROCRYPT '89, pp. 288-293 (1990).
7) Chaum D. and Pedersen T. : Transferred Cash Grows in Size, EUROCRYPT '92, pp.390-407 (1993).
8) De Santis A. and Persiano G. : Communication Efficient Zero-Knowledge Proofs of Knowledge (With Applications to Electronic Cash), STACS '92, pp.449-460 (1992).
9) Ferguson N.:Single Term Off-line Coins, Proc. of EUROCRYPT '93, pp318-328 (1994).
10) Ferguson N.:Extensions of Single-term Coins, Proc. of CRYPTO '93, pp.292-301 (1994).
11) Franklin M. and Yung. M.:Secure and Efficient Off-Line Digital Money, Proc. of ICALP 93, pp.449-461 (1993).
12) Ohta K. and Okamoto T.:Disposable Zero-knowledge Authentications and their Applications to Untraceable Electronic Cash, Proc. of CRYPTO '89, pp.481-497 (1990).
13) Ohta K. and Okamoto T.:Universal Electronic Cash, Proc. of CRYPTO '91, pp.324-337 (1992).
14) 太田:ZKIP と電子現金プロトコル, 信学技報, ISEC89-57 (1990).
15) 岡本, 太田:理想的現金方式の一方法, 信学論, J76-D-I, No. 6., pp.315-323 (1993).
16) Pedersen T.P. and Chaum D. :Wallet Databases with Observers, Proc. of CRYPTO'92, pp.89-105 (1992).

（平成 8 年 2 月 26 日受付）

大塚 玲（正会員）

1966 年生．1991 年大阪大学大学院工学研究科修了．同年(株)野村総合研究所入社．現在，同社新社会システム研究センターに在籍．電子現金やプライバシー保護など，暗号技術の社会システムへの応用に興味を持つ．電子情報通信学会，IACR，ACM，IEEE 各会員．

篠原 健（正会員）

1946 年生．1975 年大阪大学通信工学科卒業．1975 年，同大学大学院卒業後，野村コンピュータシステム(現，野村総研)入社．以来，一貫して先進的情報通信システムの企画，研究，開発に従事．大規模金融オンラインシステム，グローバル通信システム，VAN，衛星通信システムなどの企画設計開発，また CASE，マルチメディア，AI 分野などの研究開発に従事．技術研究開発部長，IT 研究センター長などを経て現在にいたる．本会学会誌編集委員，電子情報通信学会員．