

実用化迫るデジタルマネー

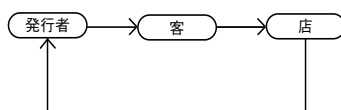
1. はじめに

新聞や雑誌、インターネットニュースなどでデジタルマネーの文字を見かけない日はないほど、デジタルマネーは注目を集めている。デジタルマネーや電子マネーという言葉には、最新テクノロジーを駆使している進歩的なイメージがあるので、最近では似たようなものはすべてそう呼ぶ傾向があり、かなり広義な意味で使用され混乱や誤解をまねている。ここでは、デジタルマネーの種類について整理し、それぞれの実験や実用化について説明してみよう。

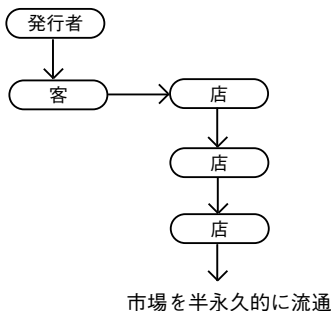
2. デジタルマネーの形態

本稿では、デジタルマネーは「価値がデジタルデータの形で保持されており」、「支払の際には価値がただちに相手方に移動するもの」ととらえることにする。後者の意味からいうと、現金、トラベラーズチェック、商品券、テレホンカードなどをデジタル化したものはデジタルマネーに当てはまるが、クレジットカードなどは当てはまらない。

デジタルマネーを、その流通方式、デジタル財布の種類、デジタル財布使用形態の3つの部分に注目して分類してみる。



(1) クローズドループ型



(2) オープンループ型

1) デジタルマネーの流通方式

デジタルマネーには、その流通方式に注目すると「クローズドループ型」と「オープンループ型」の2方式がある。

クローズドループ型は現金というより、商品券やトラベラーズチェックのような小切手をデジタル化したようなもので、一度使用されると再使用はできない。つまり、店の人は客から受け取ったマネーを他の店に持って行って使用することはできず、銀行などに持って行って現金と変えてもらうという使用方法になる。したがって、一度発行されたデジタルマネーは、「発行者（銀行など）」→「客」→「店」→「発行者」というように一巡して使命を終えるという流通形態になる。

それに対しオープンループ型は、デジタルマネーを受け取った人が、現金と同じようにそれを他の店への支払いに使用することができる。この場合、一度発行されたデジタルマネーは、市場で多くの人の手を渡り続け、半永久的に流通することになる。

デジタルマネーは多くの会社がいろいろなタイプの商品の開発を進めているが、すでに実用化実験が始まっている、または近く始まるものを例にあげると、オープンループ型のデジタルマネーには、DigiCash社のEcash、MONDEX社のMONDEX、NTTと日本銀行の方式などがある。クローズドループ型には、VISA

図1 デジタルマネーの2つの流通形式

International社のVISA Cash、MasterCard International社のMasterCard Cashや、CyberCash社のCyberCoin、JCBや東京三菱銀行、あさひ銀行、富士銀行のものなどがある。

2) デジタル財布の種類

形のないデジタルマネーをどのような方法で保持したり出し入れしたりするか。デジタルマネーを保持し、必要に応じて出し入れするためのデジタル財布についても「汎用ディスク型」と「スマートカード型」の2方式がある。

汎用ディスク型は、デジタルマネーを通常使用しているパソコンなどのハードディスクなどに、PIN (Personal Identification Number) などで保護して保持する方法である。特別なデバイスを必要としないので、初期投資をほとんど必要とせずに簡単に利用することができる。インターネット上のバーチャルなショップで買い物をする場合などはパソコンからしか支払いを行わないのでこの方法でもよいが、リアルな店舗での使用はできない。この方式の場合、デジタルマネーの2重使用を防止するために、マネーの授受するたびにいちいち発行元（銀行など）のコンピュータと通信を行わなければならない。発行元のコンピュータでは、過去に発行し現在も流通しているすべてのマネーデータを管理しなければならないので多くの資源を必要とし、本格的実用化の際はこの部分のブレイクスルーが必要となってくる。

スマートカード型は、クレジットカードやキャッシュカードと同じ大きさのスマートカード (ICカード) をデジタル財布として使用し、その中にデジタルマネーを入れて使用するという方法である。スマートカードの中にはマイクロコンピュータと小型の記憶デバイスが入っており、デジタルマネーは暗号化された上で記憶される。使用するにはPINを入力しなければならない。スマートカードは暗号の世界で言うタンパーフリーの性格を持つことができ、分解して中身を解析したり、記憶デバイスを操作して不正を働くことを防ぐような構造を取れるので、デジタルマネーを入れるデジタル財布にはうってつけのデバイスだといえよう。ただし、本当の意味でスマートカードの利点を生かすためには、公開鍵暗号方式を使用し、カード内で公開鍵暗号の鍵発生や暗号化計算を行う必要があるが、そこまで行っているデジタルマネーはまだ大変少なく、中途半端な使い方をされているのが現状である。

汎用ディスク型のデジタルマネーでスマートカードでも使用できるように考えられているものも多い。汎用ディスク型はEcash、CyberCoin、スマートカード型はVISA Cash、MasterCard Cash、MONDEX、JCBなどがあげられる。NTT-日銀方式は両方を混在して使用できる。



図2 1996年10月、長野県駒ヶ根市で導入された商店街ICカードシステム (沖電機)

3) デジタル財布使用形態

スマートカード型のデジタルマネーの場合、そのデジタル財布の使用形態によって、「プリペイド型」と「リローダブル型」の2方式がある。

プリペイド型のデジタルマネーは、発行者があらかじめ一定の価値が入ったスマートカードを作成し販売するという形態を取る。利用者はこのカードを使用して買い物をしていき、カード内のデジタルマネーがなくなった時点で、そのスマートカードは価値がなくなる。テレホンカードのようなものが、多くの店でいろいろなことに使用できると思えばよい。

リローダブル型は、プリペイド型と違い、スマートカード内のデジタルマネーが少なくなったら、何度でもデジタルマネーを補充して使用することができる。

VISA Cashには、プリペイド型とリローダブル型の2種類があり、アトランタオリンピックのときはプリペイド型が多く発行された。他のデジタルマネーはほとんどがリローダブル型である。

流通方式	プリペイド型 ループ無し (使い捨て)	ストアードバリュー型 クローズドループ	バーチャル指向の現金型 オープンループ	リアル指向の現金型 オープンループ
デジタル財布種類	スマートカード	スマートカード	汎用ディスク	スマートカード
財布使用形態	プリペイド	リローダブル	リローダブル	リローダブル
具体例	VISA Cash	VISA Cash MasterCard Cash GeldKarte JCB 日本の銀行系	Ecash CyberCoin NTT-日銀	MONDEX NTT-日銀

表1 デジタルマネーの種類と具体例

3. デジタルマネーの実用化実験

1) VISA Cash

クレジットカード会社VISA International社のデジタルマネー。スマートカード型で使い捨てのプリペイド型とリローダブル型の2種類ある。1996年にアトランタでプリペイド型の実験を行った。アルゼンチン、オーストラリア、カナダ、コロンビア、アルゼンチンなどでも実験を行っている。日本でも、通産省のECOM（<http://www.ecom.or.jp/>）の19のプロジェクトのうちのひとつであるスマートコマースジャパンの実証実験として、1997年に神戸で実験が行われる予定。1998年の夏には渋谷で、銀行のキャッシュカードとの融合型のデジタルマネーの実験も行われる予定になっており、実験レベルではいちばん進んでいる。VISA Cashは、コストを重視してISO準拠の秘密鍵暗号型のスマートカードを使用して実験を行ってきたが、それだとしてもセキュリティ面で不安が残るため、渋谷で実験を行う時期くらいからは、EMV規格（<http://www.mastercard.com/emv.html>）の公開鍵暗号型スマートカードが使用できるようになる予定。



図3 VISA International社のホームページ
<http://www.visa.com/cgi-bin/vee/sf/cashmain.html>

2) MasterCard Cash

クレジットカード会社Master Card International社のデジタルマネー。1995年にオーストラリアのキャンベラで実験を行った。実験には公開鍵暗号型のスマートカードを使用し、技術的には進んでいるが、VISA Cashに比べて知名度はいまひとつである。Master Cardは、1997年2月にMONDEX社の株式を51パーセント取得した。EMV型のMasterCard Cashと、秘密鍵暗号方式をベースとした独自方式を採用していたMONDEX方式は技術的にはかなり違ったものであり、今後どちらの方式をメインとしていくのか注目される。予想としては、MONDEXのブランドを前面に出して行くものの、内容的には従来のMasterCard Cashと同じくEMVをベースとした公開鍵暗号型を採用し、VISAとの統一規格を続けていくことになると思われる。

3) MONDEX

イギリスのMONDEX社のデジタルマネー。1995年からイギリスのスインドンで実験を行っている。97年2月までに使用者は約13,000人、加盟店数が約700件で、莫大な費用をかけて実験したにもかかわらず、多くの点で当初のもくろみより低調で実験としては失敗をしたといえる。MONDEXを使用した実験はスインドン以外でも数カ所で行われているが、どれも数百人から数千人規模でしか行われていない。1996年9月から始まった香港の実験では35,000人規模を目指している。

MONDEXはオープンループ型であるので現金に近い使い方ができ、クローズドループ型のVISA Cashなどと比べて大変高度なセキュリティ技術が必要になってくるが、当初は秘密鍵暗号型の簡易な仕組みしか使用していなかった。しかし、最近ではRSA Data Securityのライセンスを取得し、公開鍵暗号型に仕様を変更してより高い技術的安全性を目指している。また、技術的な問題の他にも、一枚のスマートカードに保持できるデジタルマネーの金額の上限設定の問題、万が一MONDEXという一私企業の経営が順調でなくなってきた場合の流通マネーの保証の問題など、ポリシーの問題も多く抱えており、Master Cardの傘下に入ったこれからの期待される。

4) Ecash

アメリカとオランダに会社があるDigiCash社のオープンループ型デジタルマネー。スマートカードなどの特別なデバイスを必要としない方式であるが、デジタルマネーの移動の際は発行元（通常銀行）のコンピュータにアクセスし、不正がされていない本物のマネーかどうかチェックが行われ、履歴が記録される。DigiCash社の創立者であるDavid Chaumは日本のNTTと共にブラインドシグネチャー技術の発明者であり、その技術のおかげで履歴記録を調べてもそのマネーが誰から誰に渡ったのか追跡ができず、使用者の匿名性確保に配慮した方式になっているのが特徴である。もし、Ecashが入っているハードディスクがクラッシュ



図4 MasterCardのホームページ

<http://www.mastercard.com/>

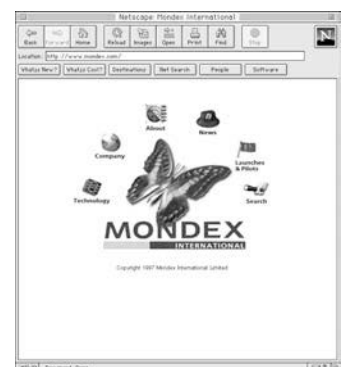


図5 MONDEXのホームページ
<http://www.mondex.com/>



図6 Ecashのホームページ
<http://www.digicash.com/>



図7 CyberCoinのホームページ
<http://www.cybercash.com/>



図8 GeldKarteのホームページ
<http://www.germany->



図9 NTT-日本銀行方式のホームページ
http://www.nttinfo.ntt.co.jp/dlij/NR_J/9609/960911A.html

した場合は、発行元に頼めば復元してもらえる。

1994年からインターネット上で実験を行っており、約30,000人の利用者がいる。1995年9月にはアメリカのMark Twain Bank、1996年5月にはドイツ銀行が、1996年10月にはオーストラリアのAdvance BankがEcashの発行を開始し、すでに実用化されている。

5) CyberCoin

アメリカのCyberCash社が開発した、Ecashと似たオープンループ型のデジタルマネー。Ecashと違って、特定のデジタルマネーからそれを使用した人を追跡できる。アメリカでインターネット上の店約30店舗で使用可能。1024bitのRSA暗号方式を輸出する許可を得ており、アメリカ製品であるがアメリカ外で使用する場合も安全性は高い。

6) GeldKarte

GeldKarte (ゲルトカルテ) は、ドイツの多くの銀行が発行しているスマートカード型、クローズドループ型のデジタルマネーで、1996年の春からドイツ南部でスイスとの国境に近いラーフェンスブルグ、バインガルトンの両市で実験が行われている。現在加盟店数は約500店。デジタルマネーとしては世界一の発行数を誇っている(1996年12月時点で約80,000枚)。GeldKarte用のスマートカードや対応端末は、ドイツを中心とする多くのヨーロッパ企業で開発しており、品揃えの点でもかなり進んでいる。

7) NTT-日本銀行方式

まだ実用実験などは行われていないが、重要だと思われるので掲載した。NTT-日本銀行のデジタルマネーは、技術的にはNTTが担当し、日本銀行は主に運用方式に関するアドバイスを行い、1996年9月に開発された。このデジタルマネーはオープンループ型で、スマートカードと汎用ディスクの両方を混在して使用できる。また、デジタルマネーの発行機関と銀行を別にするなど実際の運用面での工夫がされている。また、ブラインドシグネチャーの採用により、使用者の匿名性確保が保証され、追跡もできないなど、多くのデジタルマネーの良いところを集めた優れた方式といえる。現在のところ技術的にはいっばん現金に近い位置にあるといえるのではないだろうか。

8) エレクトロニックマーケットプレイス

ECOMのプロジェクトの1つで、1997年にJCBとイオンクレジットが三鷹と幕張などでプリペイド型(一部ストアードバリュー型)の実験を行う。スマートカード部分はIBMが開発する。他の日本の銀行系デジタルマネー(富士通、日立などが開発)と同じく、使用されているのはISO型スマートカードで、クローズド

ループ型であり、技術的に目新しい部分はほとんどない。デジタルマネーとクレジットカードのどちらにも使用できるスマートカードを発行して実験を行い、使用者の使い分け傾向のデータ取得や、運用面でのノウハウの蓄積が実験の主な目的となる。

4. まとめ

デジタルマネーは、他の方式に比べ支払いに必要なコストが大幅に安いため、この技術の普及は使用者にとって直接的にメリットを与える。また、リアルな店での使用の他に、インターネットなどのネットワークを通じて価値の授受が行えるというメリットがある。一方、マネーそのものは形を伴わないために管理方法が難しい。また、暗号技術を根拠としているため、将来暗号が破られたりすると一瞬にして流通しているマネーの価値がなくなるという大事件も絶対起こらないとはいえない。このようなデジタルマネーの利点と欠点をよく理解した上で実用化を進めるべきであると考える。

本格的実用化に向けた技術的な開発は急ピッチで進んできており、クローズドループ型に関しては実用化ができる水準に達しつつあるとあってよいだろう。現金と同じように手軽に使用できるようになるためには、技術面でもまだまだ十分とはいえないが、それよりも、発行機関設立、銀行間取引方法の確立などの運用面の整備や法整備などのソフト面での早急な整備が火急の課題であろう。

(浅田一憲・(株)ピー・ユー・ジー情報セキュリティプロジェクト)



図10 エレクトロニックマーケットプレイスのホームページ
<http://www.emp.or.jp/>



[インターネット白書 ARCHIVES] ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2012年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書 ARCHIVES」として以下のウェブサイトで公開しているものです。

<http://IWParchives.jp/>

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容(技術解説、データ、URL、名称など)は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者(執筆者、写真・図の作成者、編集部など)が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元(株式会社インプレスR&D)などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D(初期は株式会社インプレス)と著作権者は内容が正確なものであるように最大限に努めました。すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先

株式会社インプレス R&D

✉ iwp-info@impress.co.jp