IMES DISCUSSION PAPER SERIES

インターネット等のネットワークを使った個人間の電子マネー送金方法について

―― 電子メールによる電子マネー送付の可能性 ――

中山靖司・赤鹿秀樹・森畠秀実

Discussion Paper No. 99-J-15

IMES

INSTITUTE FOR MONETARY AND ECONOMIC STUDIES

BANK OF JAPAN

日本銀行金融研究所

〒100-8630 東京中央郵便局私書箱 203 号

IMES Discussion Paper Series 99-J-15
1999年5月

インターネット等のネットワークを使った個人間の電子マネー送金方法について

―― 電子メールによる電子マネー送付の可能性 ――

中山 靖司[*]・赤鹿 秀樹[**]・森畠 秀実[**]

要　旨

ネットワーク環境における電子マネーの支払いは、通常、支払者と受取者がインターネット等のネットワークによってオンラインで接続され、数回の情報のやり取りをリアルタイムで行うことによって実現されている。受取者が電子商店等の場合には、通常、いつでも顧客からの取引の申し出を受付けられるようにサーバーをインターネットに常時接続しているため、電子マネーの支払いの申し出に対しても、リアルタイムにレスポンスでき、顧客である支払者の都合によっていつでも取引を行うことが可能と考えて差し支えない。しかしながら、個人間で電子マネーの譲渡を行おうとした場合に、電子マネーの受取者となる一般の利用者は、インターネットを利用する度にパソコン等の機器をダイヤルアップで接続していることが多く、いつでも電子マネーの受け取りができるような待機状態にあるとはいえない。したがって、このような取引を行うことは現実的には運用上困難と考えられる。

そこで、支払者と受取者がネットワークでオンライン接続されている必要がなく、リアルタイムで通信を行わなくても、例えば電子メールに情報を添付することなどにより電子マネーを支払う（送金する）ことが可能な方法をいくつか提案する。また、それらの方法のうち、最も実装が容易であると考えられる方法について、IC カードを用いて実際に実装を試みた過程で生じた問題点およびその対策についてまとめる。

キーワード　電子マネー、非リアルタイム、チャレンジ－レスポンス、電子メール
JEL classification: L86、L96

[*]日本銀行金融研究所研究第２課（E-mail: nakayama@imes.boj.or.jp）
[**]日本電信電話(株)情報流通プラットフォーム研究所
（E-mail: akasika@isl.ntt.co.jp, hidemi@isl.ntt.co.jp）

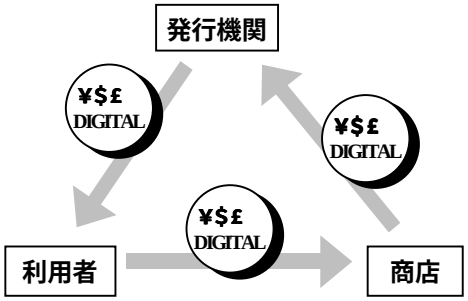
（目　次）

頁

1．はじめに

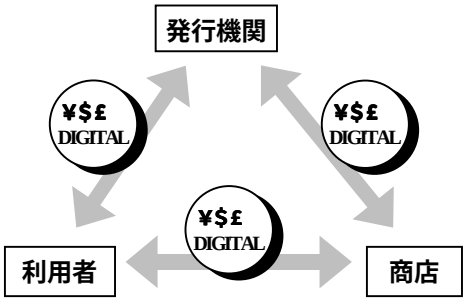
これまでに、数多くの電子マネー実現方式が提案されている。実際に実験プロジェクトとして実装されたり、さらに、実運用に移行しているものも存在するが、こうした電子マネーの多くは現実的なコストで一定のセキュリティを実現し易いと考えられるクローズドループ型の電子マネーである（図表 1 参照）。クローズドループ型の電子マネーは、実店舗あるいはインターネット上の仮想店舗といった商店を相手にした決済手段として使用することを想定したものであり、受け取った電子マネーは必ず発行体に還流させなくてはならない等の制約がある。これに対し、オープンループ型の電子マネーは、必ずしも受け取った電子マネーを発行体に還流させる必要はなく、さらに転々と別の利用者に受け渡して流通させることができる高い利便性を持つものである（図表 2 参照）。このタイプの電子マネーでは、その受け渡しに関して商店と一般の利用者の機能的な区別はなく、誰もが何の制約も受けずに電子マネーの受け手になることもできる[1]ため、現金と同様に個人間で電子マネーを受け渡すことによって、譲渡したり決済手段として用いたりと、様々な幅広い用途で使われる可能性がある。

（図表 1）クローズドループ型



※　クローズドループ型では、電子マネーの流れは一方向で、利用者と商店は機能的に異なる。

（図表 2）オープンループ型



※　オープンループ型では一般の利用者と商店の間には機能的な差はほとんどなく、商店も利用者の一つ。電子現金が利用者間を延々と流通し続け、なかなか発行機関に還流しないことが有り得る。

ところで、これまでに研究され、提案されてきた電子マネー実現方式のほとんどは、電子マネーによる支払いを行う際、「支払い相手との間がオンラインで結ばれ、リアルタイムに情報のやり取りを行える」ということが前提となっている。これは、いつでも取引が行えるよう待機状態にある商店に対して支払いを行ったり、個人間で実際に対面の上で電子マネーの受け渡しを行う場合には自然な前提である。しかしながら、インターネット等のネットワークを介して個人間で電子マネーを送金する場合には、「受取者の PC ないし電子財布がネットワークに常時接続されていていつでもリアルタイムにレスポンスできる」と考えることはあまり現実的ではなく、こうした前提を置くことが問題となってくる。この場合、「取引時間

[1] クローズドループ型の電子マネーでは、商店と一般の利用者は機能的に区別されることが多く（例外は Digicash 社の ecash）、個人が電子マネーの受け手になるには、商店としての機能を別途入手する必要があるなどの制約がある。

を予め決めておき、時間になったらネットワークに接続してもらう」とか、「電話等の他の手段によって強制的に取引相手を呼び出し、ネットワークに接続させる」、等の対応が考えられるが、実運用上不便である。そこで、これを改善する方法として、受取者がネットワークに接続して待機状態にある必要がなく、支払者と受取者がリアルタイムで情報のやり取りを行わないでも、例えば電子メールに情報を添付することなどにより、電子マネーを受け渡すことが可能な方法をいくつか提案する。また、それらの方法のうち、最も実装が容易であると考えられる方法について、IC カードを用いて実際に実装を試みた過程で生じた問題点およびその対策についてまとめる。

2．本稿で扱う電子マネー実現方式

これまでに様々な電子マネー実現方式が提案されているが、本稿では、［藤崎・岡本 96］、［中山・森畠・阿部・藤崎 97］、［森畠・赤鹿・菅沼・高橋 98］といった、オフライン性、転々流通性等の条件[2]を満たす電子証書型[3]の電子マネー実現方式を基に検討を行う。これらの方式に共通する特徴は、支払いに使用する電子コイン[4]等に対し、利用許可証[5]に対応する秘密（署名）鍵でデジタル署名を行うことにより、転々流通性を実現しているところである。ただし、本稿の基本的な考え方はデジタル署名の代わりに他のゼロ知識証明等を使う方式を含む多くの電子証書型電子マネー[6]においても応用可能なものである[7]。

---

[2] ［中山・森畠・阿部・藤崎 97］では、電子マネーに対する要求条件を次のとおりに整理している。
（安全性）
(a)事前対策（コピー等の不正な行為が行えないこと等）
(b)事後対策（不正が行われた場合不正者が発覚すること等）
（電子マネー特有の利便性）
(c)分割利用可能性（保有する価値を任意の単位に分割して利用可能）
(d)店頭・ネットワーク双方にて支払い可能（価値が情報のみで構成されるため、店頭での支払いはもちろんネットワーク経由での支払いも可能であること）
(e)効率的な電子マネー発行管理（電子マネーの発行・管理を効率的に行い、発行コストを抑えると共に、高速な処理を可能とすること）
（現金が持つメリットの継承）
(f)プライバシー保護
(f-1)追跡不能性（利用者の購買に関するプライバシーが小売店や金融機関等が結託しても露見しないこと）
(f-2)関連づけ不能性（同一利用者により使用された電子マネー情報が相互に関連づけられないこと）
(g)オフライン性（第三者の介入を必要とせず取引当事者のみで支払処理が可能なこと）
(h)転々流通性（受け取った電子マネーをそのまま他への支払い等に使用可能なこと）
(i)携帯性（IC カード等の持ち運び可能な媒体で処理できること）
(j)複数金融機関対応（複数の金融機関が同一の電子マネーを扱えること）

[3] 電子証書型電子マネー：個々の電子マネーが額面金額、識別番号等の情報を持ち、貨幣のようにそれぞれを区別することができるもので、これを受け渡すことによって支払いや受け取りを処理するタイプの電子マネーのこと。電子貨幣型、電子コイン型、電子紙幣型電子マネー等と呼ばれることもある。これに対し、電子財布等に充填されている残高金額（度数）を増減することにより、支払いや受取りを処理する方法を残高管理型電子マネーという。

[4] 電子コイン（Coin）：個々の電子マネーが個性を持ち、現実の銀行券の記番号の如く各々区別できることから、特に個々の電子マネーを指す時は電子コインという表現を使用することがある。

[5] 利用許可証（License）：電子マネー利用者の公開鍵および利用者固有情報等に発行機関（ないし登録機関）がデジタル署名した一種の公開鍵証明書。電子コインを構成する情報の一部となり、現時点における電子コインの保有者を示すためのものとして機能する。

[6] ゼロ知識証明を使用した電子マネー実現方式としては、[Okamoto and Ohta 89], [Okamoto and Ohta 91]等がある。今回は IC カード等への実装等を考慮し、比較的処理負荷の軽いデジタル署名を使用する方式を直接の検討対象とした。

[7] さらに、一部の考え方は残高管理型電子マネーにおいても応用可能である。

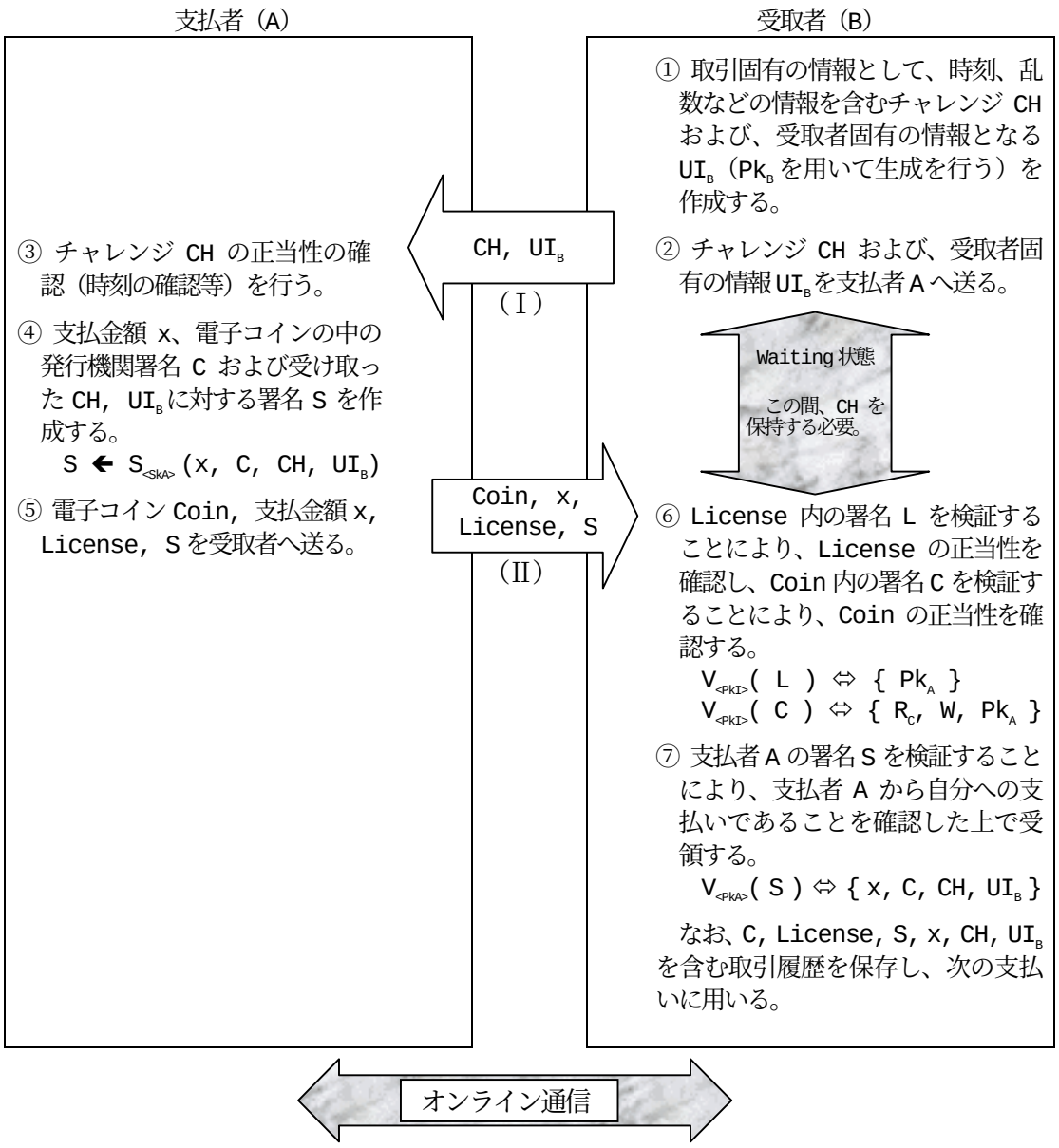
なお、非リアルタイムの情報交換手段により電子マネーを他の利用者に転々流通させる方法としては、①支払プロトコル[8]を改良する方法、②発行プロトコルを改良する方法（発行時に他人の利用許可証を埋め込んだ電子マネーを発行してもらう方法）、③預け入れプロトコルを改良する方法（電子マネー預け入れ時に他人の口座に対する預け入れを指示する方法）等が考えられるが、特に①の支払プロトコルを改良する方法を採り上げて検討を行うことにする[9]。

本稿では、まず、［藤崎・岡本 96］、［中山・森畠・阿部・藤崎 97］、［森畠・赤鹿・菅沼・高橋 98］の３つの電子マネー実現方式を基に、図表１のような簡略化した基本的な処理からなる支払プロトコルのモデルを考え、これを対象に検討を行う。なお、前提として、支払者(A)は、発行機関(I)より、利用許可証(License)および電子コイン(Coin)の発行を受けているものとする。また、License は利用者の公開鍵(Pk_A)、およびこれに対する発行機関のデジタル署名(L)からなり、電子 Coin は利用者の公開鍵(Pk_A)、額面金額(W)、番号(R_c)、およびこれらに対する発行機関の署名(C)からなるものとする。

[8] ここでは、「支払プロトコル」を、電子マネーが発行機関に還流することを前提に商店等に支払うプロトコルのほか、利用者間を転々と流通させるために他の利用者に譲渡するプロトコルを含んだ意味で使用している。

[9] なお、オフライン性を持たないクローズドループ型電子マネーにおいて、電子メールを使った電子マネーの送金を実現しているものとしては、Digicash 社の ecash がある。

（図表 1）モデル化した電子マネー支払プロトコル



発行（登録）機関 I の公開鍵、秘密鍵：Pk_I, Sk_I
支払者 A の公開鍵、秘密鍵：Pk_A, Sk_A
受取者 B の公開鍵、秘密鍵：Pk_B, Sk_B
チャレンジ（時間、乱数等）：CH
受取者固有の情報（受取者の公開鍵 Pk_A を用いて生成）：UI_B
支払額：x
支払者 A の利用許可証：$License = \{ L, Pk_A \}$
ただし、 $L = S_{<SkI>}(Pk_A)$
支払者 A に発行された電子コイン：$Coin = \{ C, R_C, W, Pk_A \}$
ただし、乱数（識別番号）：R_C
電子コインの額面金額：W
$C = S_{<PkI>}(Rc, W)$

署名作成関数： $S_{<署名鍵>}(\cdot)$
署名検証関数： $V_{<検証鍵>}(\cdot)$

3．非リアルタイム通信環境下での課題

2 章でモデル化した電子マネー支払いプロトコルは、支払者⇔受取者 間が基本的にオンラインで結ばれ、リアルタイムで情報のやり取りが行えることを前提に考えられている。そのプロトコルの概要を整理すると、① 受取者から支払者に対し電子マネーを作成するのに必要な情報(署名対象となるチャレンジ[10]および受取者固有の情報)を送付＜図表１における(Ⅰ)＞、②支払者から受取者へ電子マネーを送付＜図表 1 における（Ⅱ）＞、の最低 2 回の情報のやり取りから構成されていることになる[11]。これを、オンラインで接続されていることを仮定しない非リアルタイムの情報交換手段（電子メールやファイル交換等の非同期の対話手段）によって行う場合、最も簡単に考えられる方法は、先の支払いプロトコルにおける情報のやり取りの内容をそのまま電子メール等によって送るというものである。しかしながら、この方法では、利用者が支払いを行おうと思った時に、まず、受取者から電子メール等の非リアルタイムで支払いに必要な情報が届くのを待たなければならないなど、続けて行う一連の操作で支払い処理を終えることができないほか、受取者にとっても、電子メール等の非リアルタイムの情報のやり取り（非同期通信）を往復で 2 回終えるまで受領待ち状態が続くといった問題がある。したがって、非リアルタイムでの情報のやり取りを支払者から受取者への片道1回のみに減らすようにプロトコルを改良することによって支払者の待ち時間をなくしたり、たとえ支払いに時間がかかり受領者の受領待ち状態が長らく続いたとしても、複数の取引を同時並行的に扱えるようにすることによって他の利用者を待たせないなどの工夫を講じることが必要となる。

そこで、①の受取者から支払者に対し送付する電子マネーを作成するのに必要な情報である (1)チャレンジおよび (2)受取者固有の情報を分析し、どのようなことを考慮してプロトコルを改良すればよいかを検討して整理する。

(1) チャレンジ情報

電子マネーの支払プロトコルでは、支払者は、与えられたチャレンジに対して動的に反応して、これに対応した正しいレスポンス（例えばデジタル署名等）を行えるということを受取者に示すことによって、支払おうとしている電子マネーが他人の電子マネーの複製ではなく、確かに支払者の保有する電子マネーであるということを証明している。したがって、チャレンジは、①個々の取引に固有であること（一意性の確保）、②支払者の意思によらずに決定されること、③支払者・受取者ともにこの一意性を確認できること、といった要件を備えていることが必要となる。また、非リアルタイムの情報交換手段によって支払いを行う場合、一つの取引が終了する前に別の取引を並行して行う可能性も高く、現実的には複数の相手と

[10] チャレンジとは、検証者が、署名者を認証するために提示する値のこと。署名者は提示された値（チャレンジ）に署名をして返す（レスポンス）ことによってその正当性を証明する。なお、検証者は、毎回異なる値（チャレンジ）を生成して提示することによって、これが再利用されることを防いでいる。

[11] 特に、支払者から支払処理を起動しようとした場合は、さらに、まず最初に受取者に対して支払いの意思表示を行う必要もある。

取引が行えるよう、チャレンジの発行･管理を行うことが必要となることから、以下のような事項が課題としてあげられる。

（a）取引に対する一意性の確保

チャレンジが取引に固有の情報であること（一意性）を確保するとともに、支払者・受取者がこれを確認することができようにすることが求められる。仮に、同一のチャレンジが使用可能であるとすると、過去に使用された電子マネーのコピーが故意ないし過失によって使われた場合に、受取者がこれを判断することができないという問題が発生する。こうした事態を防ぐためにもチャレンジの一意性を確保することは必要なことである。オンラインでリアルタイム通信を行う際には、受取者がチャレンジを生成し、かつチャレンジの中に時刻情報を入れることが可能である。そのため、受取者にとっては、情報をやり取りする間のみ、自分が作成したチャレンジを保持していればチャレンジの一意性を確認できるほか、支払者にとっても、時刻情報を確認することにより比較的容易にこの一意性を確認できる。しかしながら、リアルタイムでの情報のやり取りを行わずに支払いを行う場合には、チャレンジが何らかの方法で決定され、支払者がこれを入手し、さらに入手したチャレンジに基づいて電子マネーを支払う、という一連の工程が終了するまでにはタイムラグがあり、時刻情報が取引の一意性を確保するための有用な情報とはなり得なくなるため、別途一意性を確保するための手段を講じる必要がある。

（b）チャレンジの発行・管理を誰が行うか

チャレンジは支払者の意思によらずに決定されることが必要な条件であり、必ずしも受取者から提示されなくてもよい。そのため、当事者間のみで電子マネーの受け渡しを行う場合には、受取者がチャレンジを発行せざるを得ないが、第三者の介在を許すのであれば、チャレンジの発行や管理を支払者と結託することのない信用できる第三者機関（TTP: Trusted Third Party）に代行させることも可能である。支払者も受取者も TTP に対して秘密の利用者情報（プライバシーに関する情報）を示す必要がない仕組みであれば、これによって匿名性が失われる心配もない。チャレンジの一意性確保に関しても TTP が保証を与えるスキームが可能である。

（c）複数の電子マネーの受領を考慮する問題

2 章でモデル化した電子マネー支払いプロトコルでは、通常、オンラインで結ばれた単一の相手と、取引を行うことを前提としており、複数の相手からの支払いあるいは同じ相手からの複数の支払いを同時並行的に扱うことは想定されていない。しかしながら、非リアルタイムの情報交換手段によって支払いを行う場合には、取引を終えるまでにかなりの時間経過があることも考えられるため、受取者が一つの取引が終了するまで別の取引が行えないというのでは問題がある。この電子マネー支払いプロトコルを用いて、受取者が複数の支払いを同時に受け入れることを可能にするには、受取者が既に別の取引の途中であっても、支払者がチャレンジを入手することができ、かつそれらの取引がそれぞれ完了するまで、受取者はチャレンジを複数保持する必要がある。なお、TTP にチャレンジの発行・配布を委託することに

よってこうした問題を解決することも可能である。

（2）受取者固有の情報

2 章でモデル化した電子マネー支払プロトコルにおいてチャレンジとともに送付する「受取者固有の情報」は、電子マネーの所有者を示す情報を新たな所有者である受取者に書き換えるために必要な情報である。また、転々流通性を実現するための署名の連鎖を形作るためにも使われる。すなわち、支払者は受取者に受け渡す電子マネーの情報中に「受取者固有の情報」を埋め込ことによって、受取者が新たな電子マネーの保有者であるということを証明できるようにし、たとえ第三者によって盗聴が行われ電子マネーをコピーされたとしても、これを不正に使われることのないように防ぐことができる。したがって、支払者は何らかの方法でこの「受取者固有の情報」を入手することが必要である。なお、受取者固有の情報は、取引ごとに設定する場合と、取引にかかわらず固定である場合の両方が考えられる。

4．非リアルタイム通信環境下での支払い方式

前述のとおり、非リアルタイムの情報交換手段によって支払いを実現する方法として、最も簡単に考えられるものは、支払プロトコルにおける情報のやり取り内容をそのまま電子メール等の情報交換手段によって送るというものである。しかしながら、取引当事者以外にリアルタイムで通信が可能な信用できる第三者機関（TTP: Trusted Third Party）を介在させる場合を想定すると、さらに多様な方法が実現可能となる。以下では、3 章で整理した課題を考慮した非リアルタイムの通信環境下で電子マネーの支払いを行う方式を示す。ただし、非リアルタイムの情報交換手段（電子メールやファイル交換等）で行うのは、主に支払者⇔受取者 間の通信であり、TTP⇔支払者 間、TTP⇔受取者 間の通信はほとんどの場合リアルタイムで行われるものとする。

この前提のもとでは、様々な方法が考えられるが代表的なものとして、(1) 受取者がチャレンジを直接発行する方法、(2) TTP がチャレンジを発行する方法、(3) TTP がチャレンジを発行し、受取者にも通知する方法、(4) TTP が受取者ごとに発行したチャレンジをテーブルにて管理する方法、(5) 受取者が作成したチャレンジを事前に TTP へ登録しておく方法の 5 つを提案する（各方法の比較表は図表 8 参照）。

（本章で使用するノーテーション）

支払者 A の TTP に対するチャレンジ：CH_A
支払い情報作成用チャレンジ：CH_T
支払い情報作成用チャレンジに対するデジタル署名：CS_T
受取者の ID ごとに管理するチャレンジ発行番号：CN_{TB}
受取者の ID：ID_B
受取者固有の情報（受取者の公開鍵 Pk_A を用いて生成）：UI_B
事前に登録した k 番目の受取者固有の情報：UI_B_k
支払額：x 支払者 A の利用許可証：License = { L, Pk_A }
ただし、$L = S_{<SkI>}(Pk_A)$
支払者 A に発行された電子マネー：Coin = { C, R_C, W, Pk_A }
ただし、乱数（識別番号）：R_C
電子コインの額面金額：W
$C = S_{<PkI>}(Rc, W)$
チャレンジおよび C に対するデジタル署名（支払情報）：S

TTP の公開鍵、秘密鍵：Pk_T, Sk_T
支払者 A の公開鍵、秘密鍵：Pk_A, Sk_A
受取者 B の公開鍵、秘密鍵：Pk_B, Sk_B
署名作成関数： $S_{<署名鍵>}(・)$
署名検証関数： $V_{<検証鍵>}(・)$

リアルタイム通信：⇔
非リアルタイム通信：⇨⇨⇨

(1) 受取者チャレンジ発行型

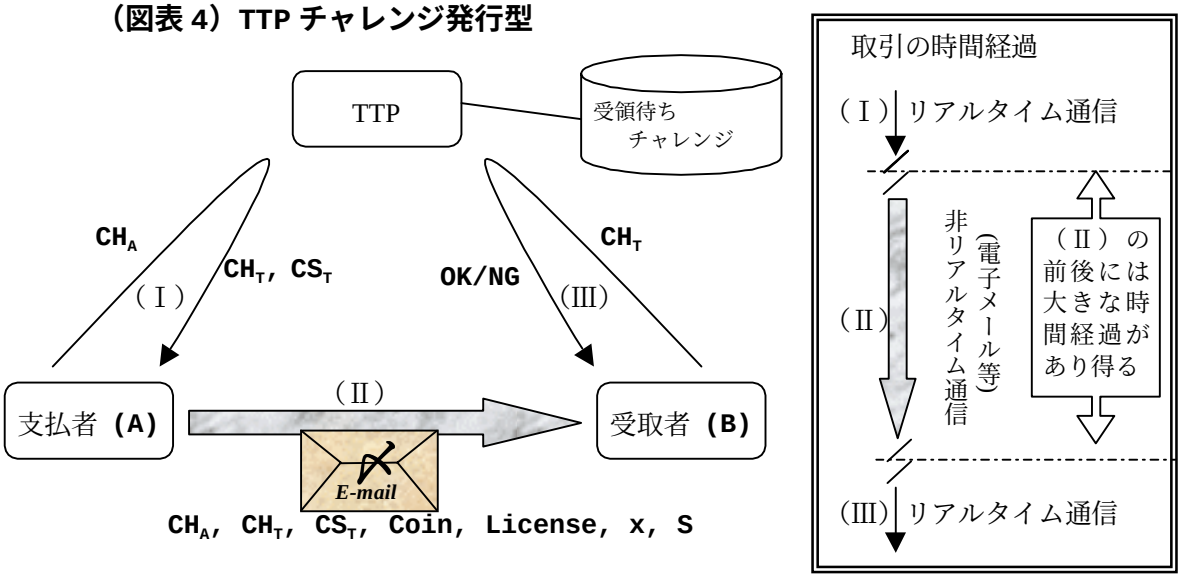
2 章で説明した電子マネー支払プロトコルを、基本的にはそのまま電子メール等の非リアルタイムの情報交換手段で行う方法である。支払者がきっかけとなって支払いを行う場合には、①チャレンジの要求（支払いの申し出）、②チャレンジの送付、③レスポンス等の送信、と 3 回のやり取りが発生する。一方、受取者がきっかけとなって支払いを行う場合には、①チャレンジの送付（支払請求）、②レスポンス等の送信、と 2 回のやり取りが発生する（詳しくは、次章で説明）。

（2）TTP チャレンジ発行型

TTP が支払いの際に使用するチャレンジを代行して発行することにより、非リアルタイムの通信回数を減らす方法である（図表 4）。なお、TTP の公開鍵証明書は支払者・受取者とも、事前に入手し保持していることを前提とする（以下で説明する TTP を介在させる他の方法においても同様）。

この方法では、支払者は予め受取者固有の情報(UI_B)を入手している必要がある。また、TTP がチャレンジの一意性を管理するとともにこれを保証する必要がある。具体的には、TTP がチャレンジ(CH_T)内に時刻情報を入れる等で一意性を確保するとともに、発行したチャレンジをデータベースに記録しておき、受取者からの取引終了時のチャレンジの正当性確認依頼がある度にデータベースでチェックし、これを消し込んでいくという管理が必要となる。

（図表 4）TTP チャレンジ発行型



（支払プロトコル）

（Ⅰ）支払者 ⇔ TTP（リアルタイム通信）

①支払者はチャレンジ CH_A を作成し、TTP に送る。

②TTP はチャレンジ CH_T および CH_A, CH_T に対するデジタル署名 CS_T ($= S_{<SkT>}[CH_A, CH_T]$) を作成し、支払者へ送る。なお、TTP は CH_T を取引終了の確認をするまで記録して保持する。

（Ⅱ）支払者 ⇨⇨⇨ 受取者（非リアルタイム通信）

①支払者は、CH_A, CH_T, CS_T, Coin, License, x とともに CH_T, C, UI_B に対する署名 S ($= S_{<SkA>}[CH_T, C, UI_B]$)を受取者へ電子メール等で送る。

②受取者は、S および CS_T の正当性を検証する。

$V_{<PkA>}[S]$ ⇔ CH_T, C, UI_B

$V_{<PkT>}[CS_T]$ ⇔ CH_A, CH_T

（Ⅲ）支払者 ⇔ TTP（リアルタイム通信）

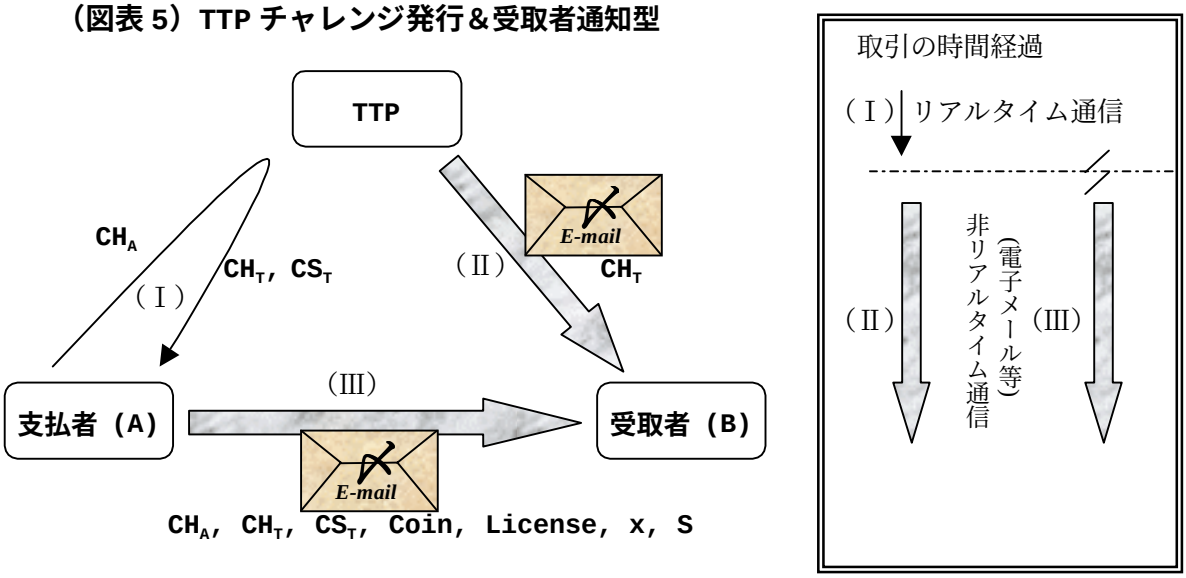
①受取者はチャレンジ CH_T を TTP へ送る。

②TTP は、チャレンジ CH_T が現在保持しているチャレンジの一つと一致するかどうかをチェックすることによって、チャレンジの取引における一意性の確認（支払者が過去の取引をコピーしていないか）を行う。また、TTP は受け取ったチャレンジ CH_T を記録から消去する。

（3）TTP チャレンジ発行＆受取者通知型

(2)の方法において、TTP が支払者に対してリアルタイム通信でチャレンジを発行した直後に、受取者には非リアルタイムの情報交換手段でチャレンジの内容を通知する方法である（図表 5）。受取者は、電子メール等の非リアルタイムの情報交換手段によって、支払者と TTP それぞれから受け取った情報を突き合わせることによって一意性の確認を行うことになる。

（図表 5）TTP チャレンジ発行＆受取者通知型



（支払プロトコル）

（Ⅰ）支払者 ⇔ TTP（リアルタイム通信）

①支払者はチャレンジ CH_A を作成し、送付先情報（メールアドレス等）とともに TTP に送る。

②TTP は、チャレンジ CH_T および CH_A, CH_T に対するデジタル署名 CS_T ($= S_{<SkT>}[CH_A, CH_T]$) を作成し、支払者へ送る。

（Ⅱ）TTP ⇨⇨⇨ 受取者（非リアルタイム通信）

①TTP は、（Ⅰ）に続けて、CS_T ($= S_{<SkT>}[CH_A, CH_T]$)を、受け取った送付先情報を使用して受取者へ送る。

②受取者は、支払者から電子マネーを受領するまで CS_T を保持する。

（Ⅲ）支払者 ⇨⇨⇨ 受取者（非リアルタイム通信）

①支払者は、CH_A, CH_T, CS_T, Coin, License, x とともに CH_T, C, UI_B に対する署名 S ($= S_{<SkA>}[CH_T, C, UI_B]$)を受取者へ電子メール等で送る。

②受取者は、S および CS_T の正当性を検証する。

$V_{<PkA>}[S] \Leftrightarrow CH_T, C, UI_B$

$V_{<PkT>}[CS_T] \Leftrightarrow CH_A, CH_T$

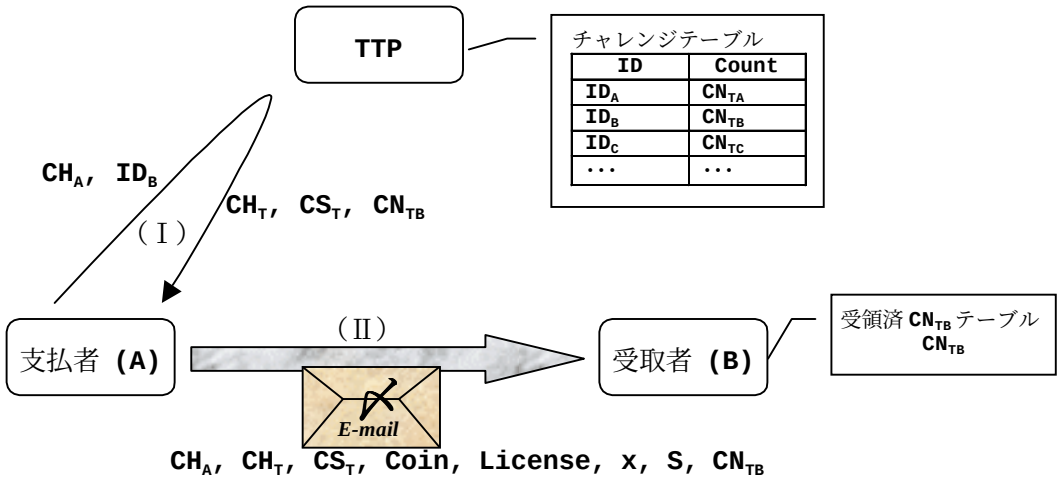
③受取者は、支払者から受け取った CS_T と TTP から受け取った CS_T の双方が揃ったところでチャレンジが一意であることを確認し受領する。

(4)TTP チャレンジテーブル使用型

(2)の方式において、受取者がチャレンジの一意性の確認を省略する方法である（図表 6）。(2)との違いは、TTP は支払者に対し、チャレンジ(CH_T)とともに TTP が受取者ごとに管理する通番(CN_{TB})を送付し、受取者は支払者から送られてくる CS_T の正当性の検証とともに CN_{TB} が以前に用いられた値でないかどうかを確認するという点である（支払者からのチャレンジは必ずしも発行順に関係なく受取者へ届くため）。これにより、受取者は TTP に問い合わせることなくチャレンジの一意性を確認することができる。

ただし、この方法では、TTP が受取者ごとにチャレンジの発行回数を管理する手間が増える[12]。また、受取者側でも使用済みのチャレンジかどうか判別するためのテーブルを持つ必要がある。

（図表 6）TTP チャレンジテーブル使用型



（支払プロトコル）

（Ⅰ）支払者 ⇔ TTP（リアルタイム通信）

①支払者は、チャレンジ CH_A を作成し、受取者 ID 情報 ID_B とともに TTP に送る。

②TTP は、ID_B ごとに管理しているチャレンジ発行番号 CN_{TB} をカウントアップし、チャレンジ CH_T、および CH_A, CH_T に対するデジタル署名 CS_T (= $S_{<SkT>}[CH_A$,

[12] 支払者自身がチャレンジの発行回数(CN_{TB})を管理し、TTP の存在を不要とする方法も考えられる。ただし、この場合は、支払者と受取者の間で、発行回数(CN_{TB})に依存して一意に定まるチャレンジ生成ルールを予め取り決めておくことが必要となる。なお、受取者は、支払者から送られてくる CN_{TB} に基づいてチャレンジ(CH_T)がルールどおり正しく生成されているかどうか、また、CN_{TB} 以前に用いられた値でないかどうかを確認することによって、電子マネーの正当性を検証することになる。

CH_T])を作成し、CN_{TB}とともに支払者へ送る。

（Ⅱ）支払者 ⇨⇨⇨ 受取者（非リアルタイム通信）

①支払者は、CH_A, CH_T, CN_{TB}, CS_T, Coin, License, x とともに、CH_T, C に対するデジタル署名 S (= $S_{<SkA>}$[CH_T, C, UI_B])を受取者へ電子メール等で送る。

②受取者は、S および CS_T の正当性を検証する。

$V_{<PkA>}$[S] ⇔ CH_T, C, UI_B

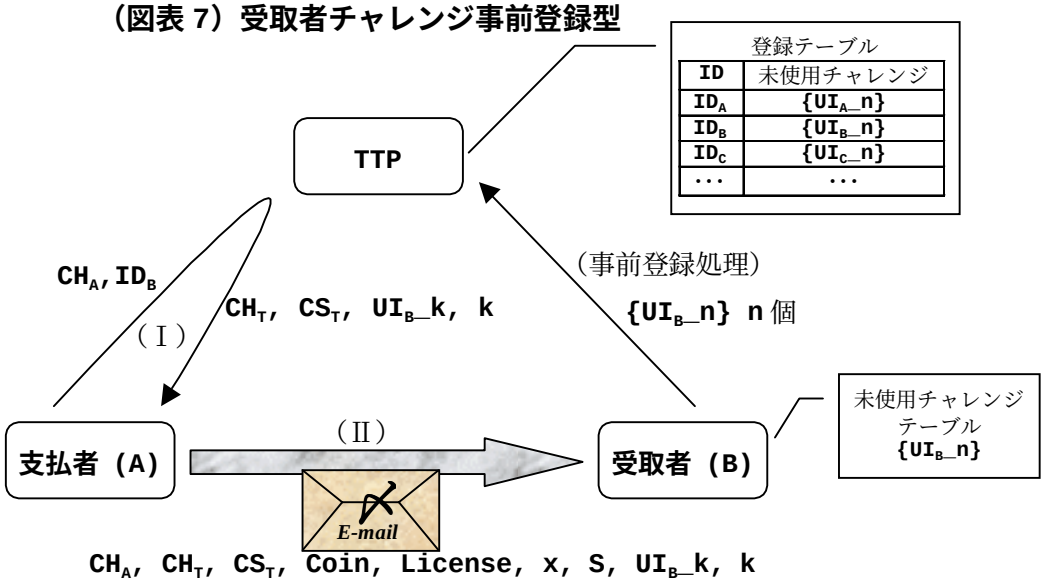
$V_{<PkT>}$[CS_T] ⇔ CH_A, CH_T

③受取者は、受領した CN_{TB} を受取者 B が管理する受領済み CN_{TB} テーブルと比較し、未受領であることを確認することによってし、CH_T の一意性を確認する。受領した CN_{TB} を受領済み CN_{TB} テーブルに記録する。

(5)TTP 受取者チャレンジ事前登録型

(2)の方法にて、支払者が受取者固有の情報(UI_B)を予め知らなくても済むように、受取者から TTP へ受取者固有の情報やチャレンジを事前に登録しておく方法である（図表 7）。支払者が作成するデジタル署名(CS_T)の署名対象の一つとして、未使用のチャレンジ(UI_B_k)が入っていることから、受取者は最後に TTP に問い合わせることなく、CH_T が過去に使われたものではなく一意性を有しているということを確認することが可能である。本方式の場合、受取者固有の情報を複数作成し、一括して TTP に登録しておくことから、受取者固有の情報(UI_B)を受取者が取引ごとに作成するタイプの電子マネー実現方式においても適用可能である。

（図表 7）受取者チャレンジ事前登録型



（支払プロトコル）

（事前処理）受取者 ⇔ TTP（リアルタイム通信）

・受取者は受取者固有の情報 { UI_B_n }（n 個）を作成し、保持するとともに、一括して TTP に登録しておく。

（Ⅰ）支払者 ⇔ TTP（リアルタイム通信）

①支払者は、チャレンジ CH_A を作成し、受取者 ID 情報 ID_B とともに TTP に送る。

②TTP は、ID_B ごとに事前に受取者によって登録されている { UI_B_n } から、まだ使用していないｋ番目の UI_B_k を取り出す。

③TTP は、チャレンジ CH_T および CH_A, CH_T, UI_B_k に対するデジタル署名 CS_T (= $S_{<SkT>}[CH_A, CH_T, UI_B\_k]$) を作成し、UI_B_k, k とともに支払者へ送る。なお、使用済みのチャレンジ CH_T および UI_B_k はテーブルから消去する。

（Ⅱ）支払者 ⇨⇨⇨ 受取者（非リアルタイム通信）

①支払者は、CH_A, CH_T, UI_B_k, k, CS_T, Coin, License, ｘとともに、CH_T, C, UI_B_k に対するデジタル署名 S (= $S_{<SkA>}[CH_T, C, UI_B]$)を受取者へ電子メール等で送る。

②受取者は、S および CS_T の正当性を検証する。

$V_{<PkA>}[S]$ ⇔ CH_T, C

$V_{<PkT>}[CS_T]$ ⇔ CH_A, CH_T, UI_B_k

③受取者は、受取者が管理している未使用チャレンジテーブルと比較して、UI_B_k, k がまだ使用されていない値であることを確認するとともに、テーブルから消去する。

（図表 8）各提案方法の比較

特　徴 提案方法名	支払者		受取者	備　　考
	チャレンジの入手 （チャレンジ作成方法）	受取者固有の情報の入手	チャレンジの一意性の確認方法	
受取者チャレンジ発行型	受取者が非リアルタイムの通信手段によって送付 （受取者が時刻情報などを元に自由に決定）	予め別途手段で入手する必要	受領待ちとして受取者が保持しているチャレンジであることを確認	非リアルタイムの情報交換が往復で発生するため取引に時間がかかる
TTP チャレンジ発行型	TTP がオンラインで通知 （TTP が時刻情報などを元に自由に決定）	予め別途手段で入手する必要	受領待ちとして TTP が保持しているチャレンジかどうか問い合わせる	受取者は、受領後に TTP に対する問い合わせを行う必要
TTP チャレンジ発行 &受取者通知型	TTP がオンラインで通知 （TTP が時刻情報などを元に自由に決定）	予め別途手段で入手する必要	受領待ちとして TTP から非リアルタイムの通信手段によって送付されたチャレンジ情報と突合	受取者は、TTP、支払者の双方から非リアルタイムの情報交換手段で情報を受け取る必要
TTP チャレンジテーブル使用型	TTP がオンラインで通知 （受取者ごとに管理する発行回数をチャレンジとともに送信）	予め別途手段で入手する必要	受取者が管理する使用済チャレンジテーブルにないことを確認	TTP が、受取者ごとにチャレンジ発行回数を管理する必要
TTP 受取者チャレンジ 事前登録型	TTP がオンラインで通知 （受取者が事前に登録したチャレンジを使用）	TTP がチャレンジと共に送付 （受取者固有の情報を受取者が取引ごとに作成するタイプの電子マネー実現方式においても適用可能）	受取者が事前に TTP に登録したものであり、かつ受取者が管理する未使用チャレンジテーブルにあることを確認	TTP が、受取者ごとに受領者固有の情報を含むチャレンジの事前登録を受けておくことが必要

5．受取者チャレンジ発行型による電子メールを使った実装例

前章で非リアルタイムの情報交換手段を利用した支払方法について、いくつかの提案を行ったが、現実に実装し、サービスを提供することを考えた場合に、TTP を設置することが困難であることも多い。そこで、TTP を用いずに取引当事者間だけで容易に実現可能な方法として、「受取者チャレンジ発行型」のプロトコルを採り上げ、支払者⇔受取者 間の通信を電子メールやファイル交換といった非リアルタイムの情報交換手段により行うことを前提に、CPU を内蔵した IC カードに実装することを試みた。その結果、いくつかの問題点があることがわかった。

(1) 問題点

(a) 複数の電子マネーの受領

2 章でモデル化した電子マネー支払プロトコルでは、受取者は、支払者が作成した署名を受け取るまでチャレンジを保持しなければならない。したがって、複数の電子マネーを並行して受領することを考慮すると、複数の支払者（同時に受領できる最大数）に対するチャレンジを同時に保持するとともに、チャレンジを発行した順番に関係なく電子マネーが送られてきても、これを処理できるような仕組みになっている必要がある。しかしながら、実際には IC カードの容量には制約があることから多数のチャレンジを保持することは困難であり、このままでは一度に受領待ちにできる電子マネーの数を制限する必要が生じる。

(b) チャレンジの誤使用

リアルタイムで情報のやり取りを行うことによって電子マネーの支払いを行う方法では、支払者はチャレンジ情報中にある時刻情報が、現在支払処理を行おうとする時刻とほとんど一致していることを確かめることにより、チャレンジの一意性をある程度確認することが可能であるほか、電子マネーの受け渡しは常に単一の相手との間でのみ行われる仕組みになっていることもあり、他人宛てのチャレンジ情報を誤って使用することもほとんど考えられない。

一方、電子メール等の非リアルタイムの情報交換手段によって電子マネーの支払いを行う方法では、チャレンジ情報に含まれている時刻情報が支払いを行おうとしている時刻とずれがあることが普通であるほか、支払者が複数の支払いを並行的に行うために複数のチャレンジ情報を同時に受け取っていることも考えられ、時刻情報程度ではチャレンジの一意性を確認することができない。そのため、支払者が複数の支払いを行おうとした場合に、どのチャレンジが正しいチャレンジであるかを錯誤して誤った支払情報を作成した結果、受取者が電子マネーを受け取れなくなる等の事態が発生し得る[13]。

[13] ①既に支払いに使われているチャレンジを再度使用してしまうケースや、②メーリングリストなどの同報メールで送られてきた他人宛てのチャレンジを使用してしまうケース等が考えられる。

(2) 問題の解決策

以下では、こうした問題点に対する解決策を検討する。

(a)複数の電子マネーの受領

支払者が電子マネーを受取者に支払う際、発行されたチャレンジを一緒に送ることによって、受取者は受領待ちになっている取引のチャレンジを IC カード内に保持する必要がなくなるように、2 章でモデル化した電子マネー支払プロトコルを改良する。

まず、受取者はチャレンジ CH を作成すると同時に、これを受取者の秘密鍵 Sk_B で暗号化した eCH（ $= E_{<SkB>}(CH)$ ）を計算し、チャレンジ CH とともに支払者に送る。さらに、チャレンジ CH のハッシュ値 hCH（ = h(CH) ）を計算し、対応する電子マネーを受領するまで IC カード内のメモリーに保存する。支払者は受取者に電子マネーを支払う際に、eCH を一緒に送る。このようなプロトコル変更により、受取者は IC カード内にチャレンジ情報全体を保存する必要はなく、受領時に受け取った暗号化されたチャレンジ eCH を、受領待ちとして保持しているチャレンジのハッシュ値 hCH と比較することにより、チャレンジ CH が自分の生成したものであるか（チャレンジの一意性）を確認することができる。受取者の IC カードのメモリーに保存するデータが CH 全体ではなくハッシュ値のみで済むため、同時に受領待ち状態にできる取引数を大幅に増やすことが可能となる。

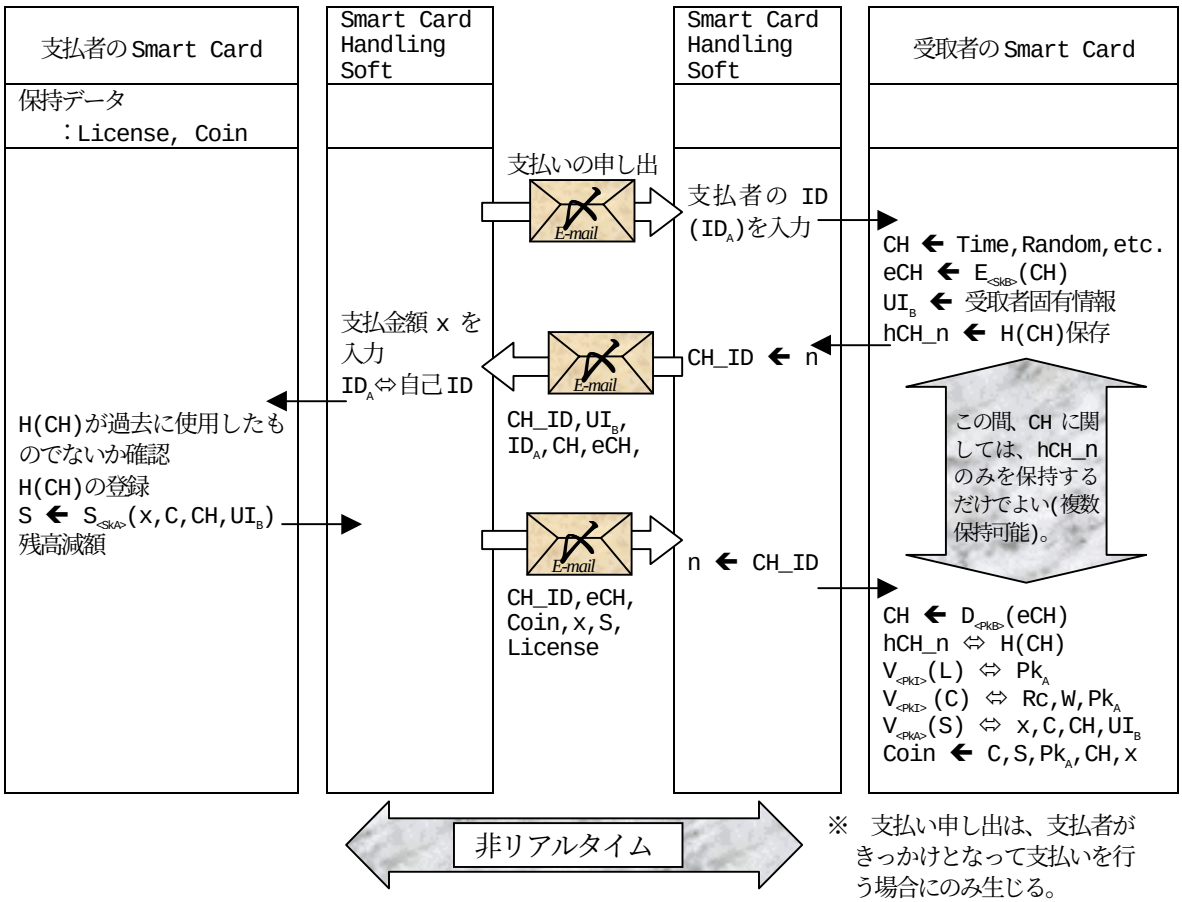
(b)チャレンジの誤使用

支払者の IC カード内に過去 N 回のチャレンジ CH のハッシュ値を持ち、過去の支払いで使用された CH かどうかを確認した上で支払いを行うようにする。これにより、支払者は過去 N 回に支払いに使用したことのあるチャレンジに対しては、誤って支払いを行うことを防ぐことができる。

また、受取者が支払者に対してチャレンジを送る際、支払者の利用者 ID 情報をセットにして送り、支払者はチャレンジとともに送られてきた ID 情報が自分の ID と同一であることを確認した上で支払いを行うことにより、他人宛てのチャレンジに対して誤って支払いを行うことを防ぐことができる。

これらの対策を行った電子マネー支払いのプロトコルを図表 9 に示す。

（図表 9）「受取者チャレンジ発行型」の実装を考慮した支払プロトコル



発行(登録)機関 I の公開鍵、秘密鍵：Pk_I, Sk_I
支払者 A の公開鍵、秘密鍵：Pk_A, Sk_A
受取者 B の公開鍵、秘密鍵：Pk_B, Sk_B
チャレンジ（時間、乱数等）：CH
チャレンジのハッシュ値：hCH
暗号化されたチャレンジ：eCH
IC カードで管理される取引識別番号：n
IC カードに保持されている取引識別番号 n のチャレンジのハッシュ値:hCH_n
授受される取引識別番号：CH_ID
支払者の ID：ID_A
受取者固有の情報（受取者の公開鍵 Pk_A を用いて生成）：UI_B
支払額：x
支払者 A の利用許可証：License = { L, Pk_A }
ただし、 L = $S_{<SkI>}(Pk_A)$
支払者 A に発行された電子コイン：Coin = { C, R_C, W, Pk_A }
ただし、乱数（識別番号）：R_C
電子コインの額面金額：W
C = $S_{<PkI>}$(Rc, W)

ハッシュ関数： H(・)
署名作成関数： $S_{<署名鍵>}$(・)
署名検証関数： $V_{<検証鍵>}$(・)
暗号化関数 ： $E_{<暗号化鍵>}$(・)
復号関数 ： $D_{<復号鍵>}$(・)

6．おわりに

これまでに研究されてきた電子マネーの基本的なプロトコルを分析し、支払者⇨受取者 間の通信を非リアルタイムの情報交換手段（電子メール、ファイル交換等）に置き換えた場合に考慮しなければならない課題を整理した。また、こうした課題をクリアし、実装を可能とする電子マネーの支払プロトコルをいくつか提案し、そのうち特に TTP の存在を仮定することなく実現可能なプロトコルについて、実際に IC カードを用いて実装する場合の問題点およびその解決策についてまとめた。

本稿では、他の利用者に電子マネーを送金する方法として、電子マネープロトコルのうち、支払プロトコルを改良する方法を提案したが、発行プロトコルを改良する方法や預け入れプロトコルを改良する方法により、電子マネーを受取者に送る方法も可能と考えられる。今後は、これらの方法についても理論および実装にかかる研究を進めていくとともに、利用者にとってより自由度の高い利用者間での電子マネー受け渡し方法を検討していくことが必要であろう。

以　上

[参考文献]

太田和夫・岡本龍明・川原洋人、「電子現金の実用化動向とその課題」、『1997 年電子情報通信学会総合大会講演論文集』、基礎・境界 TA-4-2, pp.578-579, 電子情報通信学会、1997 年

岡本龍明・太田和夫、「理想的電子現金方式の一方法」、『電子情報通信学会論文誌』、J76-D-I、No.6、pp.315-323、電子情報通信学会、1993 年

中山靖司、「実現せまる電子マネーの現状」、『Dr. Dobb's JOURNAL JAPAN』、1998 年 2 月号、pp.70-81、翔泳社、1998 年

――――、「電子決済について」、『ITU ジャーナル』、Vol26、No.7、pp.54-62、新日本 ITU 協会、1996 年

――――・太田和夫・松本 勉、「電子マネーを構成する情報セキュリティ技術と安全性評価」、『金融研究』、第 18 巻第 2 号、日本銀行金融研究所、1998 年 4 月

――――・森畠秀実・阿部正幸・藤崎英一郎、「電子マネーの一実現方式について――安全性、利便性に配慮した新しい電子マネー実現方式の提案――」、『金融研究』、第 16 巻第 2 号、日本銀行金融研究所、1997 年 6 月

藤崎英一郎・岡本龍明、「エスクロー電子現金」、『電子情報通信学会論文誌』、IT95-51、ISEC95-46、SST95-112、pp.7-12、電子情報通信学会、1996 年

森畠秀実・阿部正幸・藤崎英一郎・中山靖司、「電子現金方式」、『1997 年 暗号と情報セキュリティシンポジウム予稿集』、SCIS'97-3C、電子情報通信学会、1997 年

――――・赤鹿秀樹・菅沼知久・高橋芳夫, 「階層型電子現金方式」、『1998 年 暗号と情報セキュリティシンポジウム予稿集』、SCIS98-3.1D, 電子情報通信学会、1998 年

BIS, "Security of Electronic Money," Report by the Committee on Payment and Settlement Systems and the Group of Computer Experts of the central banks of the Group of Ten countries, Aug 1996.（日本銀行電算情報局訳、『電子マネーのセキュリティ』、ときわ総合サービス、1997 年）

Brands, S., "Untraceable Off-line Cash in Wallet with Observers," Proceedings of CRYPTO'93, LNCS 773, pp.302-318, Springer-Verlag, 1993.

Chaum, D., "Security Without Identification: Transaction Systems to Make Big Brother Obsolete," Communications of the ACM, Vol.28 NO.10, pp.1030-1044, 1985.

――――, A. Fiat and M. Naor, "Untraceable Electronic Cash (Extended Abstract)," Proceedings of CRYPTO'88, LNCS 403, pp.319-327, Springer-Verlag, 1990.

Eng, T. and Okamoto, T., "Single-Term Divisible Electronic Coins," Proceedings of EUROCRYPT '94, LNCS 950, pp. 306-319, Springer-Verlag, 1995.

Even, S., Goldreich, O., Yacobi, Y. "Electronic Wallet," Proceedings of CRYPTO'83, A later version appeared in Proceedings of 1984 International Zurich Seminar on Digital Communications, pp.199-201, IEEE cat No.84CH1998-4.

Matsumoto, T., "An Electronic Retail Payment System with Distributed Control - A Conceptual Design -," IEICE Trans. Fundamentals, Vol.E78-A, No.1, 1995.

Nakayama, Y., Moribatake, H., Abe, M. and Fujisaki, E., "An Electronic Money Scheme -- A Proposal for a New Electronic Money Scheme which is both Secure and Convenient," IMES Discussion paper series, 97-E-4, Institute for Monetary and Economic Studies, Bank Of Japan, 1997.

Okamoto, T. and Ohta, K., "Divertible Zero-Knowledge Interactive Proofs and Commutative Random Self-Reducibility," Proceedings of EUROCRYPT'89, LNCS 434, pp.134-149, Springer-Verlag, 1989.

――――, and ――――, "Disposable Zero-Knowledge Authentications and Their Applications to

Untraceable Electronic Cash," Proceedings of CRYPTO '89, LNCS 435, pp.481-496, Springer-Verlag, 1990.

————, and ————, "Universal Electronic Cash," Proceedings of CRYPTO'91, LNCS 576, pp.324-337, Springer-Verlag, 1992.