1G－14

電子マネーによる複数受領者宛て支払い方式の検討

柿添 智也、 佐藤 賢一
NTT 情報流通プラットフォーム研究所

現在の NTT 電子マネー支払いプロトコル[1]では、一度の支払処理において受領者を一人に限定している。この電子マネープロトコルを拡張することで、受領者の数が一人に限定されない電子マネー支払プロトコルが提案されている[2]。この複数受領者当て支払プロトコルを使ったサービスとして、公共料金の代行徴収といったものが考えられるが、実際にサービスを行うに当たっていくつかの問題点が考えられる。本稿では、その問題点を解決したプロトコルを提案し、従来の複数受領者当て支払プロトコルを含む、それぞれのプロトコルの適用可能領域を考察する。

1. 従来の複数受領者宛て支払プロトコル

【プロトコル 1】受領者がチャレンジを作成(図 1)[2]

現在の NTT 電子マネー支払プロトコルは、受領者が作成した、自分の受領権限（ID）を含むハッシュ値（以下チャレンジ）に対して、支払者が秘密鍵で支払署名を作成、受領者に送信することで行われる。それに対して、これまでに提案されている複数宛支払プロトコルは、1 つのチャレンジに複数受領者の受領金額と受領権限を格納することで、”一度の支払処理で複数受領者が受領可能な電子マネー”を実現する。支払者が支払う総額を x、受領者 1 の受領額を x1、2 次受領者の受領額を x2 とする。支払者は自分の支払額、各受領者は自分が受領する金額のみを知っている。

各受領者は、自分の受領する金額と ID、乱数 R を含むチャレンジを作成する。受領者 2 は受領者 1 にチャレンジを送信し、受領者 1 は Chall1 と Chall2 をハッシュする事で支払用チャレンジ ChallT を作成、支払者へ送信する。支払者は ChallT と x に対する支払署名 S を作成し、受領者 1 に送信する。各受領者は S を検証後、ChallT に自分の受領権限と受領金額が含まれている事を確認出来れば、電子マネーを受領する。

このプロトコルの特徴は、受領者数が増加しても支払者のプロトコルは既存の物から変化しないことである。

・既存プロトコルの問題点

このプロトコルでは支払チャレンジを作成する受領者 1 に悪意があれば、支払チャレンジを受領者 1 のチャレンジにとして支払者に送信することで受領者 2 に支払われるべき電子マネー全額を横領することが可能である。この問題は受領者が支払チャレンジを作成することに起因している。

2.問題解決のための新規プロトコル

上記問題点を解決したプロトコルを以下に提案する。

【プロトコル 2】支払ー受領に関係ない第三者(TTP)がチャレンジを作成(図 2)

このプロトコルでは前提として、TTP (Trusted Third Party) の存在を仮定する[3]。TTP とは、支払者、各受領者の個人的な情報の漏洩や改竄等を行わない、完全に信用できる第三者機関である。支払用チャレンジは TTP が作成し、支払者は TTP から受け取った支払用チャレンジに署名を行うことで支払いを行う。支払用チャ

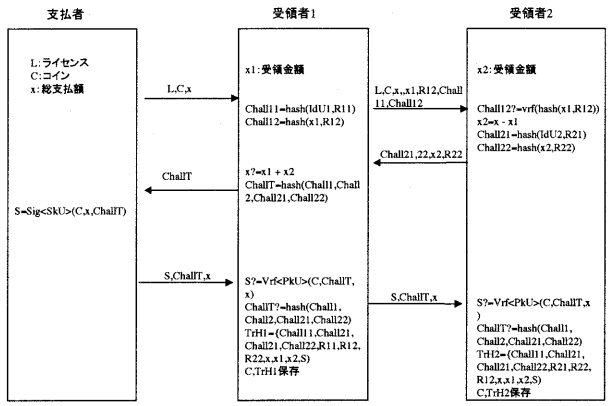

図1 プロトコル1(受領者が支払チャレンジを作成)

An Application of Multicast of Electronic Money
Tomoya Kakizoe, Kenichi Sato
NTT Information Sharing Platform Laboratories
1-1 Hikarinooka, Yokosuka-shi, Kanagawa, 239-0847, Japan

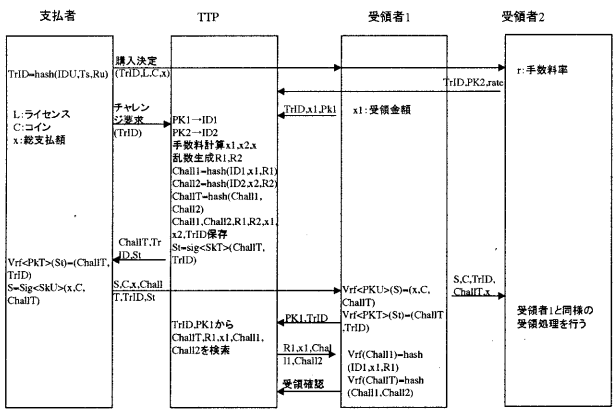

図2 プロトコル2(TTPが支払チャレンジを作成)

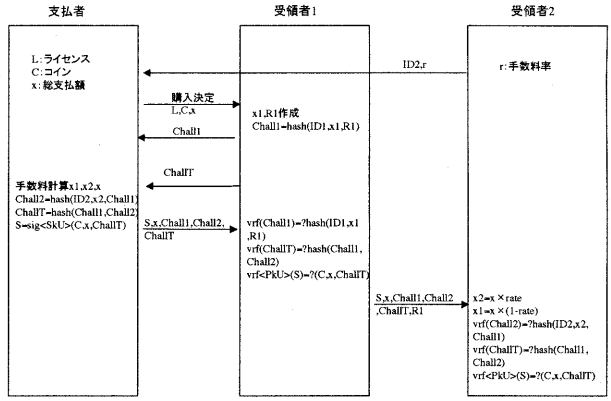

図3 プロトコル3(支払者が支払チャレンジを作成)

レンジの構成要素自体はプロトコル1と同一である。

【プロトコル3】支払者がチャレンジを作成(図3)

支払の条件として、支払者は予め受領者からチャレンジ情報(ID2、x2もしくはr2)を手に入れておく必要がある。支払者は各受領者から受け取ったチャレンジ情報から支払用チャレンジを作成し、それに対して支払署名を作成することで電子マネー支払いを行う。なお、支払用チャレンジの構成要素自体はプロトコル1と同一である。

3. 複数宛て支払プロトコルの評価

ここでは以下の二つの条件下で、各複数宛て支払プロトコルを適用した場合のビジネス性をを比較検討する。

3.1 受領者間の不正

プロトコル1では、受領者1の悪意によって支払われた電子マネー全額を横領することが可能である。したがってフリーマーケットなど各受領者間で不正が行われないという保証が無い場合、プロトコル1は不適当である。逆に受領者間で契約などによる社会的な信用が確保されている場合には、既存のNTT電子マネープロトコルからの変更が少なく、第三者の介入を必要としないプロトコル1が実装面から見て最も良い。

3.2 受領者間の通信

プロトコル2と3の特徴は、チャレンジの作成フェーズにおいて各受領者間の通信が必要でない、つまり各受領者が他の受領者の存在を意識することが無い点である。そのためネットオークションの様な、受領者(出品者)が常時ネットワークに接続していない場合にも適用可能である。

4. 複数受領者宛て支払プロトコルの適用例

4.1 代行徴収

公共料金の代行徴収などでは、プロトコル1を用いて、受領者1が受領者2の電子マネーを代行徴収する際、手数料を徴収するといったビジネスが考えられる。

4.2 バスケットの共通化

インターネット上の商店での買い物は、利用者が商店で希望の商品をバスケットに入れ、最後にバスケットの中の商品代金をまとめて支払うというバスケット方式が一般的である。ネット上のフリーマーケットのような不特定多数の出品者からの商品が一度に並んでいるサイトを考えると、出品者(受領者)間の不正の可能性が否定できないことから、プロトコル2におけるTTPをフリーマーケットサイトが行うことによりフリーマーケットサイト内でバスケットの共通化を計ることが可能である。

5. 参考文献

[1] 森畠,赤鹿,菅沼,高橋,"階層型電子現金方式,"The Proceedings of the 1998 Symposium on Cryptography and Information Security,SCIS'98-3.1.D,1998.

[2] 松尾慎一郎,森畠秀実,"複数の受領者への支払いが可能な電子現金方式," The Proceedings of the 1999 Symposium on Cryptography and Information Security,SCIS'99,1999.

[3] 中山靖司,赤鹿秀樹,森畠秀実,"インターネットなど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,"IMES DISCUSSION PAPER SERIES No.99-J-15,1999.