# 柔軟な多対一決済に関する研究

西郷　悟　　三浦　史光　　高橋　修
（株）NTT DoCoMo マルチメディア研究所

あらまし　近年、インターネットを介した匿名な決済を実現する方法として SET、Ecash をはじめとした様々な電子決済方式が提案されている[1,2]。しかし、これらの電子決済方式の多くは、一店舗対一ユーザ間の決済のみを対象としており、一店舗対複数ユーザ間の決済に対しては考慮されていない。そのため現金による決済において有効な支払方法の一つである複数ユーザ間で支払価格に傾斜配分をつける等の柔軟な支払比率の調整、或いは、団体割引等の柔軟な課金サービスを実現するには従来技術単独では不十分である。本発明は、既存の一店舗対一ユーザ間決済（Ecash）を用いて、上記で述べた一店舗対複数ユーザ間における柔軟な決済を実現するための決済方法を提案する。

キーワード：インターネット、電子決済、一店舗対複数ユーザ間決済、Ecash

## A Study on flexible payment system

Satoru Saigo　　Fumiaki Miura　　Osamu Takahashi
NTT DoCoMo Multimedia Laboratories Co., Ltd.

Abstract　To realize an anonymous payment on the internet, many payment mechanisms (SET and Ecash are typical ones) were already proposed [1,2]. By the mechanisms only one client can buy some contents from a merchant, but multiple clients can't do, because a target of the mechanisms is the only forward case. While by the paper-based payment we generally use, multiple clients can flexibly distribute their amounts, and easily accept flexible account services (ex. a group discount service). This paper proposes a new payment system that is partly based on Ecash, to realize an above flexible payment for multiples clients.

Keywords：Internet, digital payment, payment for multiple clients, Ecash, flexible payment

## １．研究背景

インターネットを介した匿名な決済を実現する方法には、SET、Ecash をはじめとした様々な電子決済方式[3,4]が存在しており、これらの多くは一店舗に対して一ユーザ存在する場合を対象としている。しかし、メールやチャット、掲示板、ネットゲーム等の普及が示すように、現在インターネットは複数のユーザ間での情報共有のための道具としての重要度が増しており、例えば音楽配信/映像配信サービスの共同購入のように複数ユーザが同一店舗から課金サービスを共同で購入するような利用用途も今後想定される。このような一店舗対複数ユーザ間の決済の利点は、複数ユーザ間で支払金額の比率を柔軟に調整できる（ワリカン、傾斜をつけて支払う、おごる等）、或いは、団体割引等の柔軟な課金サービスが実施できる等であるが、従来技術単独ではこれら対象外のサービスには対応できない。本研究では、既存の一店舗対一ユーザ間の決済方式を活用して、上記の柔軟な一店舗対複数ユーザ間の決済を実現するための方式を提案する。

## ２．従来技術（一店舗対一ユーザ間決済）を組み合わせたアプローチの検討

本稿では、一店舗対一ユーザ間の決済方式としてもっとも代表的な SET 及び Ecash を応用した場合における一店舗対複数ユーザ間の決済について検討を行う。ここで SET と Ecash の特徴についてまず簡単に説明する。SET はクレジットカード決済をベースとした決済方式で、購入情報/支払情報を分離し、それぞれを店舗/クレジットカード会社の公開鍵を用いて暗号化することで、必要な相手に対して必要な情報のみを通知し、取引の匿名性を実現している。一方、Ecash はネット上の現金に相当する電子コインをベースとした決済

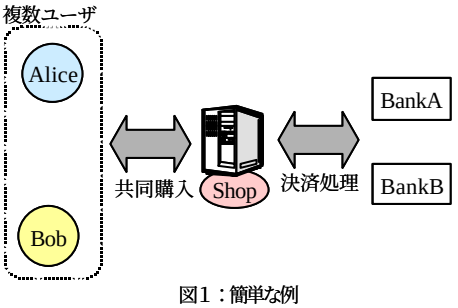


図1：簡単な例

方式で、匿名なコインを用いることにより取引の匿名性を実現している。特徴的な性質として、ユーザが同じコインを二重使用した場合に、それを検出することができると共に二重使用したユーザをも特定することができる。以降、これらの特徴を活かし、SET 及び Ecash をまず単純に組み合わせて利用した場合のアプローチについて検討を行う。ただし、例として図１に示すように、Alice と Bob がそれぞれの取引金融機関（クレジットカード会社、銀行）BankA、BankB を用いて店舗に支払いを行う最も簡単な構成で考えることにする。

### ２．１．従来技術を組み合わせたアプローチの検討

一店舗対一ユーザ間の決済方式を組み合わせて、一店舗対複数ユーザ間の決済を実現するためのアプローチには、典型的なものとして次の二つの方法が考えられる。一つはユーザとの間で個別に行った決済を店舗が正しく対応付けて決済処理を行う方法で、もう一つは一人のユーザがまとめて店舗に支払う方法である。以降、それぞれのアプローチにおける問題点及び実現性に関する検討を行う。

#### ２．１．１．個別決済の対応付け

図２にその概要図を示す。店舗は Alice と Bob との間で SET/Ecash を用いて個別に決済を行う。その際、店舗はそれぞれの決済が Alice/Bob が望む相手のものであるか否かを認証し、独立した二者の決済を正しく対応付けることにより、一店舗対複数ユーザ間の決済を実現する。しかし、取引の匿名性を重視する SET/Ecash においては、この認証行為自体がそもそもの目的と反する。また、決済の許諾を判断するパーティーが判断結果によって利害を伴う店舗のみであるため、店舗自体が不正行為を行う場合が起こり得る危険性があるうえに、それを立証する手段がない。

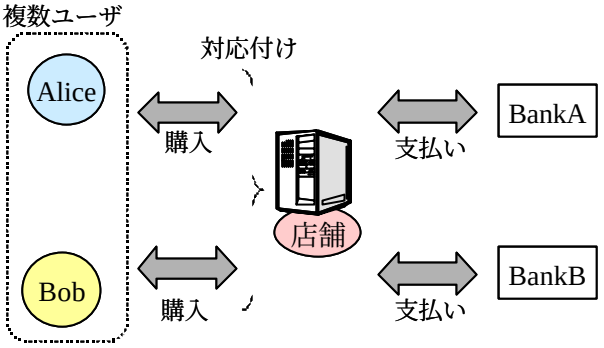



図２：個別決済の関連付け

#### ２．１．２．まとめて支払

次に、図３にまとめて支払の概要図を示す。Alice は Ecash を用いて Bob に支払を行い、Bob は店舗に対して Alice の分の支払いをまとめて行う。ここで、まとめて支払ではユーザからユーザへの支払が存在するため、ユーザから店舗への支払のみを対象としている SET は利用できない。この方法を用いることにより、個別決済において匿名性を損なう原因となった決済間の対応付けそのものが必要なくなる。しかし一方で、Alice が Bob に適切に支払いを行ったにも関わらず、Bob が店舗への支払を行わずお金を持ち逃げすることができる、或いは、Bob が Alice の承諾なしに勝手に購入サービスを変更してしまう等の別の問題が起こり得る。また、個別決済の対応付けと同様に、この決済方法においてもユーザ/店舗の不正行為が発生した場合にそれを検出する方法も立証する方法もない。

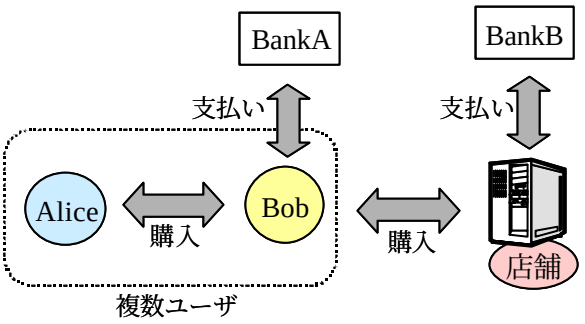



図3 :まとめて支払い

### ２．２．従来技術を組み合わせたアプローチのまとめ

以上の検討結果より、上記で挙げた SET/Ecash を単純に組み合わせた典型例はいずれも一店舗対複数ユーザ間の決済においては十分ではないことが分かる。また、SET はユーザが店舗に支払う決済のみに対応しているため、それ以外のユースケースでの利用は適切ではなく、代わりに Ecash を利用する場合においても複数ユーザ間の支払ではコイン単体だけではなく取引情報（ユーザ間で合意したサービス/支払い比率等）が必要であることが分かる。以降、上記の結果を踏まえて、Ecash をベースとした一店舗対複数ユーザ間の決済を実現する方法を提案する。

## ３．提案方式（一店舗対複数ユーザ間決済）

### ３．１．アーキテクチャ

前節の検討結果を踏まえたアーキテクチャを図４に示す。Alice が Bob にコインを払うのは上記の従来技術の組み合わせと同じアプローチであるが、その際に問題となる Bob によるお金の持ち逃げは、Ecash の特徴を活用して

回避する。Ecash では、ゼロ知識証明を用いたコインに対するチャレンジ/レスポンスを行うことで、コインを送信してきた相手がコインの正当な持主であるか否かを検証する。店舗は検証に利用したコインに対するチャレンジ/レスポンスとコインを Bank に送信することにより、Bank から支払い受ける。つまり、Bank から支払いを受けるためには、コインだけでなくコインに対するチャレンジ/レスポンスが必要である。そこで本提案方式では、まずコインと取引情報のみを Bob がまとめて支払い、コインに対するチャレンジ/レスポンスは Alice/Bob がそれぞれ店舗と個別にやり取りすることで、支払いに必要な情報を部分的に Bob に隠匿し、Bob によるお金の持ち逃げを防止する。また、Bob が Alice との間で合意した取引情報を勝手に変更してしまう問題に関しては、Alice と店舗間で共有した秘密情報を用いた MAC で防止する（詳細は３．２．１．で説明する）。以上、本アーキテクチャを用いることにより上記で挙げた従来技術の問題を解決することができる。しかし、その一方で、Ecash に新たに取引情報等が追加する等の変更が必要となるため、取引の匿名性、不正行為発生時の証拠の残し方等検討すべき課題が新たに生じる。以降、これらの課題を整理し、それぞれの解決方法を提案する。

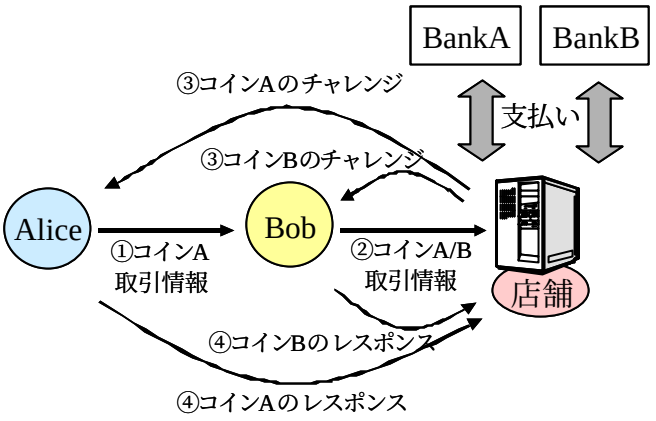



図４:提案アーキテクチャ

### ３．２．課題及びその解決方法

上記のアーキテクチャで現金による支払と同程度の一店舗対複数ユーザ間の決済を実現するためには、次の３つの課題を解決することが重要である。一つ目は、取引の匿名性である。決済に使用する情報には、ユーザ嗜好等のプライベートな情報を含んでいるため、これらの情報が不必要な第三者に漏洩しないための方法が重要である。二つ目は、決済が片方だけ失敗した場合における処理方法である。Ecash では、Bank は取引ユーザのコインの正当性のみを検証し店舗への支払を実施するため、ユーザ間の決済が一つでも失敗した場合にその支払を中断する、或いは、コインを返金してもらうための方法が必要である。そして、最後は、証拠の利用方法である。ユーザ/店舗等、取引結果により利害が発生するパーティーが不正行為を実施した場合に、それを検出/立証するための方法が電子決済においては重要である。以降、それぞれの課題及びその解決方法を説明する。

### ３．２．１．取引の匿名性

取引の匿名性の保護には、必要な相手に対して必要な情報のみを通知することが重要である。本提案方式においては、Alice/Bob は店舗及び BankA/B の通信に使用する共通鍵をそれぞれの公開鍵暗号を用いて暗号化し共有する。これにより、Alice/Bob の匿名性を損なわずに、Alice/Bob と店舗/BankA/B との間でセキュアな通信路を確保することができる。Alice/Bob は、ユーザ間で合意したサービス、支払金額比率等の取引内容に関する情報の保護には、店舗との間で共有した共通鍵を用いる。店舗は Alice/Bob よりそれぞれ受信した取引情報を比較し、一致するか否かを検証することにより取引の許諾を判断する。ただし、店舗が不正な許諾判断を行う場合もあるため、取引情報のハッシュ値を BankA/B でも共有し、検証できるようにする。一方、Alice/Bob は互いの取引金融機関 BankA/B を認証するのに必要な情報、取引の識別子、error 発生時の処理方法に対する同意確認等に関する情報である同意書（必要性に関しては３．２．２で説明する）を保護するのには、BankA/B との間で共有した共通鍵を使用する。以上の方法を用いることにより表１に示す匿名性を実現する。

表１：情報の匿名性

| | Alice | Bob | 店舗 | BankA | BankB |
|---|---|---|---|---|---|
| 取引情報 A | ○ | × | ○ | △（ハッシュ値のみ） | × |
| 取引情報 B | × | ○ | ○ | × | △（ハッシュ値のみ） |
| 同意書 A | ○ | × | × | ○ | × |
| 同意書 B | × | ○ | × | × | ○ |

○：既知情報、×：未知情報

### ３．２．２．片方だけ決済が失敗した場合の処理方法

片方だけ決済が失敗した場合の決済処理方法は、一店舗対複数ユーザ間の決済でのみ起こり得る特有の問題であるが、複数ユーザ間で支払金額を柔軟に調整する、或いは、団体割引等の柔軟な課金調整を行う等の全ての決済が成功することを前提としたサービスにおいては特に重要である。しかし、Ecash はそもそも個別決済であるため、Bank は他の決済を識別することも、コインの正当性の検証結果を他の決済に反映させることもできない。一方、店舗は銀行に対して支払を要求する立場なので、Bank からの検証結果に従って支払処理の中止/返金を要求することができるが、不都合な検証結果を Bank に通知しないことは店舗が不当な利益をうる危険性もあるため、片方の Bank の検証結果をもう片方の Bank に通知する役割を店舗単体に任せることはできない。したがって、本提案方式では Alice/Bob は BankA/B との間で共有した共通鍵（３．２．１．を参照）を用いて、同意書を共有する方法を採用する。同意書にはお互いの取引金融機関 BankA/B を認証するのに必要な情報及び、取引内容を特定するための識別子、正しい Bank から error 通知を受信した場合に Bank が中断/返金等の処理を行うことをユーザが承諾したことを示す情報の３種類を含めることにより、Ecash を用いた場合においても一方の検証結果を他の検証結果に反映させることができる。図５にその一例を示す。BankB は Bob との決済に問題が発生した場合に、Bob の同意書に基づき BankA に対して error 通知（BankA の公開鍵で暗号化し、BankB の署名を付与）を行う。BankA は Alice の同意書を基に error 通知が正しい BankB から送信された情報であること検証し、Alice のコインの支払処理を中断する。以上の方法を用いることにより、複数決済のうち一つでも決済が失敗した場合に決済処理を中断することができる。ここで、error 通知が遅れて既に他の決済処理が終了してしまった場合も考えられるが、その場合はユーザが次節で述べる証拠を用い、店舗/Bank に対してコインの返金を要求することで対応できる。

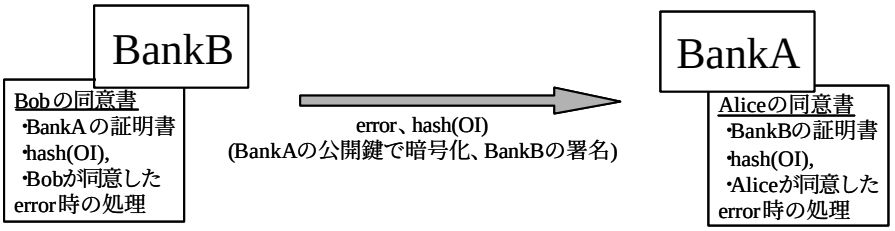



図5 :error通知

### ３．２．３．証拠の利用方法

３．２．２．で述べたように一店舗対複数ユーザ間の決済においては、個別の決済が適切に処理された場合においても他のユーザの決済処理が失敗することで取引自体が成立しない場合がある。その際、店舗が取引の不成立をユーザに通知しコイン返金等の処理を行うことが望ましいが、悪意のある店舗の場合、取引の不成立をユーザに隠匿しコインの返金等を行わないケースが起こり得る。また、個別の決済が全て適切に処理されて取引が成立したにも関わらず、ネットワークが切断されコンテンツを受信することができない等のケースも起こり得る。そこで、電子決済においては不正行為を防止するための証拠、或いは、コンテンツの再送を要求するための証拠が重要である。本提案方式では、次の方法でこれらの問題に対処する（図６）。Alice は適切なコインを用いて支払いを行ったにも関わらずコンテンツを取得することができなかった場合に、まず、BankA との間で共有してある共通鍵を使用してコンテンツ要求/コンテンツ再送要求を行う。これにより、Alice の匿名性を損なうことなく、BankA に対して要求を投げることができる。要求を受けた BankA は BankB と証拠を突き合わせることにより、取引が成立しているか否かを検証するこ

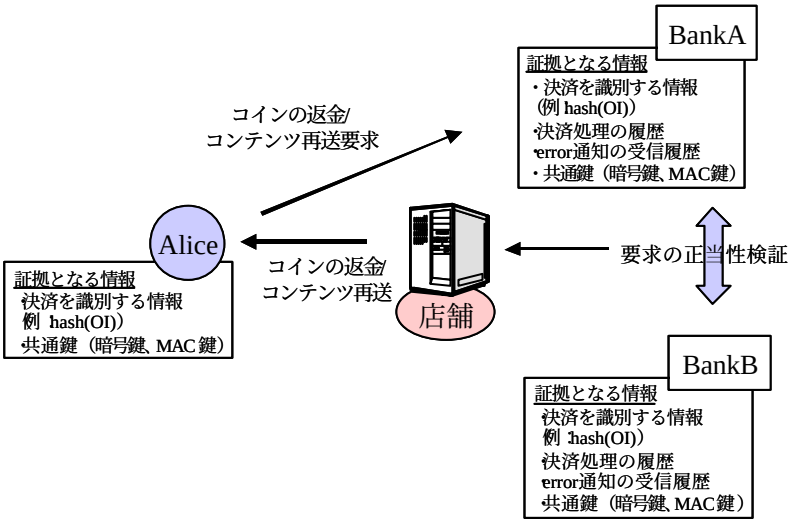



図６:証拠の利用方法

とができるため、検証結果に応じて取引店舗にコインの返金/コンテンツの再送要求を行う。これによりユーザ/店舗が不正行為を行った場合に、不正行為を検出できると共にそれを行った対象及び原因を特定することができる。

## ４．まとめ

本研究では、複数ユーザ間で現金による支払を行う際に有効な支払方法である柔軟な支払金額の調整（ワリカン、傾斜配分をつけた支払、おごり等）、或いは、団体割引等の柔軟な課金サービスをネット上で実現することを目的とし、一店舗対複数ユーザ間の決済方式を提案した。まず、既存の一店舗対一ユーザ間決済の単純な組み合わせだけでは、上記のサービスを実現することが難しいことを示し、これを解決することができるアーキテクチャを提案した。また、その際に重要となる、取引の匿名性を実現するための鍵の配送/利用方法、取引が成立しなかった場合の error 通知方法、及び、取引中断/コイン返金のための証拠利用方法を考案することで、上記サービスを実現する上で重要な機能を実現した。

## ５．今後の予定

本稿では、これまであまり検討されてこなかった一店舗対複数ユーザという利用形態をターゲットとし、そのために必要な機能を整理/検討し全体像（付録 A）を考案した。今後更に詳細な検討をすすめていく共に、電子決済において重要な要素の一つであるコスト面における評価を行う。

## 参考文献

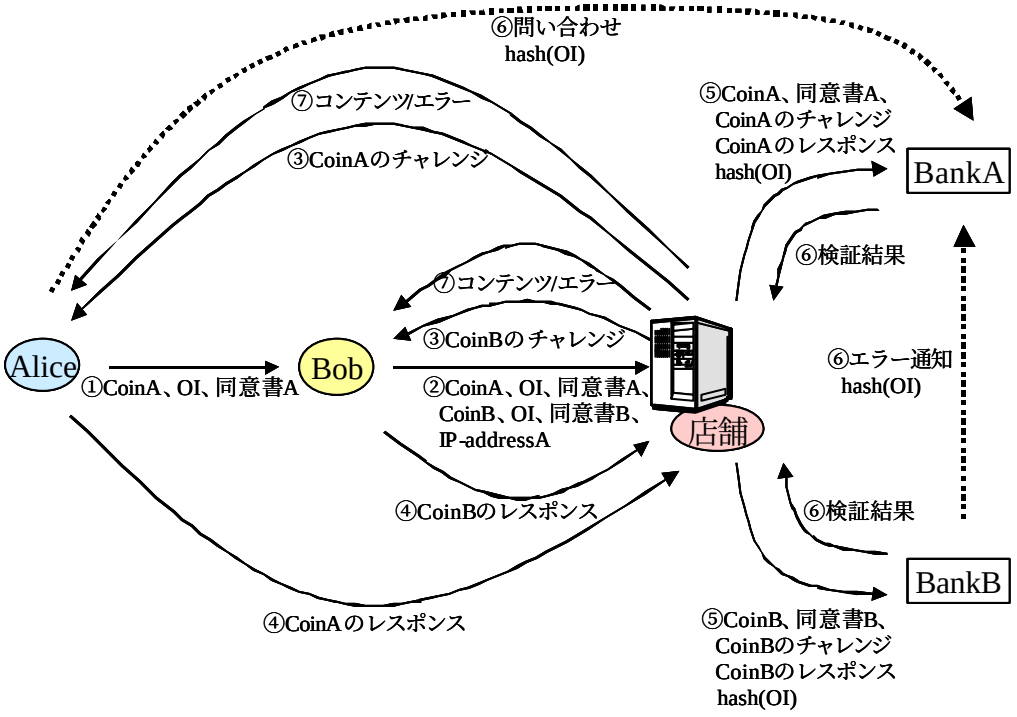

[1] Grady N. Drew 著, “SET のすべて”, 株式会社ピアソン・エデュケーション

[2] Chaum D., Fiat A., Naor M., “Untraceable Electronic Cash”, Proceedings of Crypto 88 (1988)

[3] Okamoto T, and Ohta K, “Universal Electronic Cash”, Proceedings of Crypto91 (1991)

[4] Donal O’Mahony et al, “Electronic Payment Systems”, Artech House Publishers


## 付録 A




提案方式の全体概要図