学位論文題目 Fair Mobile Commerce Infrastructure（邦訳：公平なモバイル電子商取引基盤）
取得年月 2008年6月　**学位種別** 博士（工学）　**大学** 電気通信大学
氏　名 寺田 雅之（（株）NTTドコモ 先進技術研究所 主任研究員）
推薦研究会 コンピュータセキュリティ
推薦文 本論文は，オークションや契約などの実務アプリケーションにおける公平性を保証するための第一歩となる基礎研究である．詐欺や偽装が横行する現状からみても，この研究の重要性が将来にわたって増すことは確実であり，ここに推薦申し上げます．

携帯電話は，「いつでもどこでも」利用者とともにあり，また，耐タンパデバイスであるICカードチップを備えることから，電子商取引を広く普及させるための基盤として有望である．しかし，現在の携帯電話を用いたモバイル商取引は，店頭での決済や交通機関での運賃支払いなどが中心であり，たとえば利用者間でチケットやコンテンツを売買することなどはできない．

本研究は，電子マネーやチケット・クーポンなどのさまざまな「価値を持つ電子情報」を統一的に「電子価値」として扱えるようモデル化し，携帯電話などのモバイル機器を用いて電子価値やディジタルコンテンツを誰とでも安全・安心に取引できるようにすることを目的としている．本論文は，これらを実現するための方式を提案するとともに，その基本部分に対してUCフレームワークによる形式証明の手段を与え，さらに提案方式を効率的に実装するためのICカード間通信フレームワークを提案する．本論文の成果は，IETF RFC，IrDA Standard，T-Engine Forum Specificationとして標準化されている．

まず，発行者や種類があらかじめ定められている電子マネーと異なり，さまざまな発行者によりさまざまな内容のものが発行され得る電子価値を統一的に扱い，効率的に流通させることができる電子価値流通方式を提案する．本方式は，電子価値を（発行者，所有者，行使により得られる対価）の3つ組から構成される請求権として統一的にモデル化し，これを記憶容量や入出力性能が限られたデバイスであるICカードを用いて実用的な性能で流通可能とする．

次に，「誰とでも安全に」電子価値を取引できるようにするために，公平性が保証された電子価値の取引プロトコルを提案する．取引の公平性が保証されることにより，利用者が互いに相手をよく知らない状況でも，取引対象の持ち逃げなどのリスクなしに安心して取引を行うことができるようになる．本プロトコルは，楽観的公平交換プロトコルの一種として位置づけられるが，従来のプロトコルと異なり，交換対象の複製防止を保証するために必要な一貫性を備える．これにより，原本性の保証が必要な電子価値の取引に適用可能としている．

また，電子価値のみならず，ディジタルコンテンツなどを含めた任意の情報を公平に取引可能とするために，合意問題の一種であるNBACの楽観的な解決に基づく公平交換方式を提案する．従来の楽観的公平交換プロトコルにおいては，交換対象の少なくとも一方は（事実上）電子署名に限定されていたことに対し，提案方式は交換対象に制約がなく，任意の情報を楽観的かつ公平に交換することができる．

図-1　本研究の目標

提案方式の基本部分の安全性は，UCフレームワークを用いて証明される．具体的には，NBACと相互に帰着可能なことが証明された理想機能を構築することにより，UCフレームワークにおいて初めて合意問題との等価性が証明された理想機能を与える．これは，本方式の安全性を形式証明するための手段を与えるだけでなく，マルチパーティ計算などの幅広い暗号応用プロトコルにおいて，証明可能な公平性を容易に与える手段を提供する．

最後に，提案方式を効率的かつ容易に実装可能とするための，ICカード間の分散通信フレームワークを示す．ISO7816-4など，従来のICカードインタフェースでは，ICカードは命令（Command）に対して応答（Response）を返すだけの存在であり，本論文で提案している交換プロトコルなどの，ICカード間での分散プロトコルの実装は非常に複雑となった．本フレームワークは，それぞれのICカードが，自律的かつ分散透過に相互通信することを可能とすることにより，これらのプロトコルの実装を容易にする．本フレームワークを用いて前述の電子価値の取引プロトコルを実装評価することにより，本論文のアプローチに基づく電子価値の取引が，ICカードを用いて実用的な性能で実現可能であることが示された．

（平成22年3月29日受付）