New Technology Reports

移動端末間の電子価値流通技術

安全な電子商取引を実現するためには，取引の公平性を保証する必要がある．貨幣やチケットなどを「電子価値」として実現し，安全かつ公平に取引するための方式を確立するとともに，試作評価を通じて実用性の検証を行った．

寺田 雅之　森 謙作
石井 一彦　本郷 節之

1. まえがき

2004年にサービスが開始された「おサイフケータイ」は，移動端末を通話やメールのやり取りなどの通信手段にとどまらせることなく，その名のとおり電子的な「お財布」とした画期的なサービスである．

「おサイフケータイ」は，専用端末を備えた店頭での支払いの際に小銭がいらない，などの利便性を利用者に提供している．「お財布」としての利用シーンは，現在はまだ店頭決済などに限られたものとなっているが，今後は移動端末が備えるネットワーク機能などを活用して適用領域を拡げていくことにより，さらなる利便性を提供していくことが期待される．

そのような「おサイフケータイ」の将来に向け，お金だけではなく，例えば各種のポイントやクーポン，チケットやコンテンツ再生権などのさまざまな電子的な価値を，移動端末を持つ任意の利用者との間でネットワークを介して安全に取引するための技術について研究開発を進めてきた．

本技術は，電子マネーや地域通貨，ポイントカードなどの貨幣的なものから，施設利用券などの各種入場券，ギフト券や割引クーポンなどのクーポン類，さらには音楽や映画，電子書籍などの電子コンテンツに対する視聴権などを「電子価値」として実現し，それらの売買や交換を可能とする．例えば，「視聴権」を電子価値として実現することにより，著作権を保護しながら電子コンテンツを売買・レンタルしたりすることが可能となる．すなわち，利用者によるフェアユースと著作権保護を両立したコンテンツ流通・取引環境を実現することができる．

また，本技術を用いた電子価値は誰でも生成，発行が可能である．この特長を活用することにより，学生サークル

やアマチュアバンドなどが自前でチケットを作成，販売するなど，利用者自身によるさまざまな応用も考えることができる．

このようなさまざまな電子価値の取引を，単一のプラットフォームで統一的かつ安全に実現可能とすることで移動端末は単なる「電子財布」を超えて「携帯可能な電子マーケット」となる．すなわち，本技術は単に電子チケットや電子クーポンを実現するのみならず，それらを安全に利用者間で取引するための新たな電子市場を創出し，移動端末をさらに生活に密着したツールとするものである．

本稿では，上記のようなサービスを実現するための技術である「電子価値取引のための楽観的な交換プロトコル」[1]について，その設計目標と技術の概要について紹介するとともに，IC カードを用いた実装評価の結果を示す．

2. 実現すべき目標

本技術は，単なる「お金」のみならず，チケットやクーポン，視聴権などの多種多様な権利や価値を，誰とでも安全に取引できるようにすることを目標としている．

そのような環境を実現するためには，さまざまな内容を持つ多様な種類の権利や価値を統一的に扱えること（多様性），それらの権利や価値が流通の過程で改ざんされたり複製されたりしないこと（安全性），少なくとも現在の貨幣や紙のチケットと同等の流通性を持ち，さらに利用者の数や取引頻度の増加に対して著しい性能劣化を起こさないこと（実用性）などが求められる[2] [3]．これらの要件を満たした形で実現された，権利や価値を表象する電子情報を「電子価値」と呼ぶ．

しかし，実際に利用者が安心してさまざまな相手と電子価値を取引できる環境を実現するためには，上記の安全性に加え「取引の公平性」を実現することが必要となる．ここでの取引の公平性とは，取引を行う当事者の双方ともが，取引の際に相手から「もらうべきもの」をもらうことなしに相手に「渡すべきもの」を失うことはない，という条件を満たすことを指す．以下，例を用いて説明する．

利用者が「1,000円分の商品を購入できる電子クーポン」を表す電子価値を使って，商店から（1,000円で販売されている）「コンテンツ視聴権」を表す電子価値を，ネットワーク経由で購入することを考える．これは電子クーポンとコンテンツ視聴権との交換取引となる．

さて，この取引において，利用者と商店のどちらが先に自分の電子価値を送ればよいだろうか．対面で商品と現金がやり取りされる現実世界の商店と違い，ネットワーク経由の取引では「同時に」データを送受信することは困難である．相手から電子価値を受け取る前に自分の電子価値を送ってしまうと，送った電子価値を「持ち逃げ」されてしまうリスクが発生する．利用者が正しくクーポンを送ったとしても，商店（もしくは商店のふりをした詐欺師）はクーポンを受け取ったあと視聴権を送らずに取引を中断し，そのまま音信不通になってしまうかもしれない．

上記の例のように電子価値を持ち逃げされた状態，すなわち電子価値の交換において「相手から受け取るべき電子価値を受け取ることなしに自分の電子価値を失った」状態を「不公平な状態」と定義する．ネットワーク経由で見知らぬ誰とでも利用者や商店が安心・安全に取引するためには，取引における電子価値の持ち逃げを防ぎ，不公平な状態で取引が終了することがないように取引の当事者双方に対して保証する，すなわち取引の公平性を保証する必要がある．

本技術は，電子価値に求められる基本的な要件である多様性，安全性，実用性の3つの要件に加え，取引の公平性を実現することにより，利用者が安全にさまざまな電子価値を取引できる環境を実現する．

3. 技術の概要

本技術は，例えば移動端末などに備え付けられたIC カードに格納されたさまざまな内容を持つ電子価値を，安全かつ公平に取引する手段を提供する．本技術において，電子価値は「発行者の識別子」「権利・価値の内容」からなる電子情報として構成される．この電子情報がIC カードの中に格納されているとき，その利用者は発行者に対して，記載された内容の権利・価値を行使する権限を有する．すなわち，その利用者が電子価値を所有しているとする．

本技術の取引は，「楽観的」[4]に行われる．ここで楽観的とは，通常は当事者間のみで取引の遂行を試み，もし何らかの異常により当事者間だけでは取引を公平に終了させることができなくなった場合には，信頼できる第三者により公平な状態に回復することを意味する．

すなわち，それぞれの取引は当事者である二者間の相互通信によって行われる．通信障害などにより取引の途中で通信が途絶することがなければ，この二者間通信のみで取引は完了し，取引相手以外との通信は一切発生しない．この場合，拡張性の障壁となる集約サーバに依存することなく取引が可能であるため，多数の移動端末が同時並行に取引を行ったとしても性能劣化は発生しない．

また，通信の途絶や取引相手による不正の試みなどにより，2章で述べたような「不公平な状態」で取引が中断されてしまった場合には，ネットワーク上に配置された調停

サーバを用いることにより取引の公平性を回復する．この回復は取引相手とのやり取りは一切必要としないため，もし取引相手と音信不通になってしまったとしても，取引を必ず公平に終了させることができる．

3.1 主プロトコル

本技術を用いた電子価値の取引は，移動端末内のICカード間で2往復のメッセージをやり取りすることによって行われる．これを主プロトコルと呼ぶ（**図1**）．主プロトコルは，電子署名およびハッシュ関数[*1]を用いることにより，電子価値の改ざんや複製を防ぎつつICカード間で電子価値を安全に取引する．主プロトコルが正常に終了すると，取引対象となる電子価値v1およびv2について，利用者AのICカードに格納されていた電子価値v1は利用者BのICカードへ，利用者BのICカードに格納されていた電子価値v2は利用者AのICカードへそれぞれ移送され，取引は完了する．ここで電子価値の移送とは，移送元のICカードからの電子価値の削除と，移送先のICカードへの電子価値の格納を意味する．

＊1　ハッシュ関数：入力から一定長のデータを出力する一方向性関数．代表的なものにSHA-1がある．

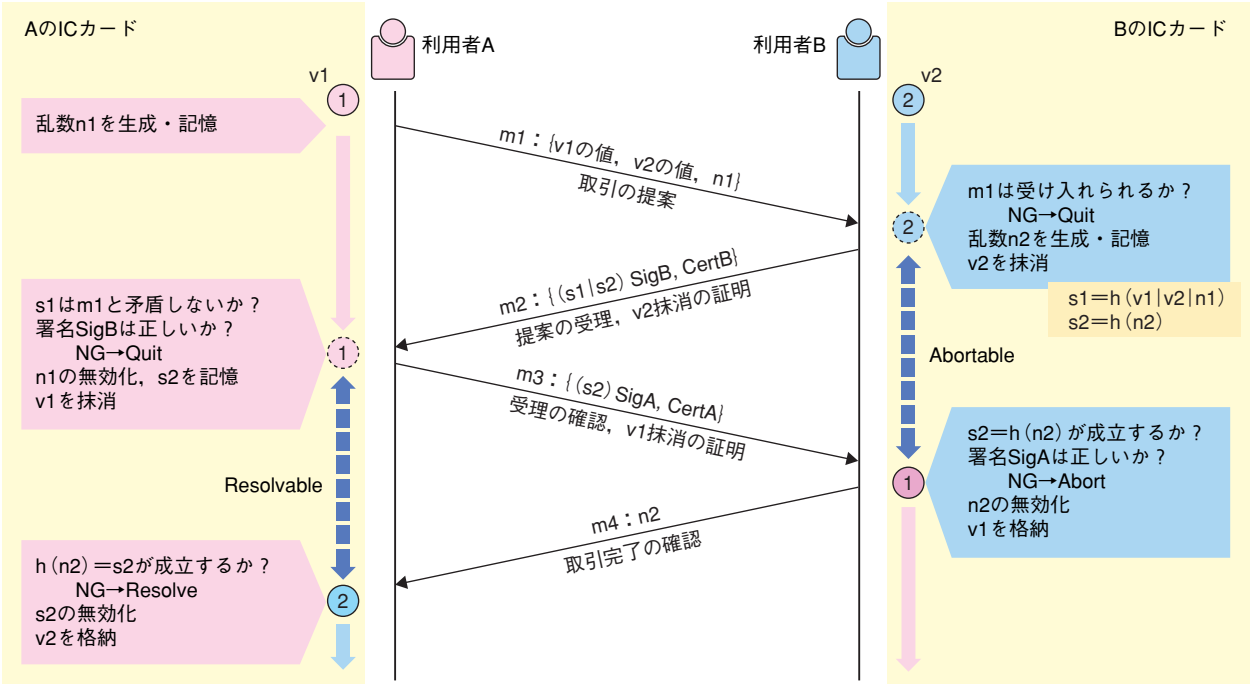
3.2 公平性の回復

主プロトコルの実行途中で取引相手との通信が途絶し，再接続も不可能となった場合，「不公平な状態」で取引が中断される可能性がある．例えば，図1のResolvable区間において，利用者Aは電子価値v1を失っているが，電子価値v2をまだ受け取っていない．またAbortable区間においては，利用者Bはv2を失っているがv1を得ていない．

本技術は，不公平な状態で主プロトコルが続行不能となった場合に，ネットワーク上の調停サーバと1往復のメッセージのやり取りすることにより取引の公平性を回復する手段を提供する．これを回復プロトコルと呼ぶ．これらの回復プロトコルにより取引の公平性を回復する際には，取引相手と通信をする必要はない．不公平な状態で相手との通信が途絶してしまったとしても，調停サーバと通信が可能か，もしくは取引時点で通信可能な環境になかったとしても後から調停サーバと通信することができれば，その時点で不公平な状態を解消することができる．

3.3 回復プロトコル

回復プロトコルは，利用者Aから取引の完遂を依頼するためのResolveプロトコル（**図2**）と，利用者Bから取引の中止を依頼するためのAbortプロトコル（**図3**）から構成される．



v1, v2：取引対象とする電子価値
CertA, CertB：A, Bそれぞれの公開鍵証明書
h（m）：一方向ハッシュ関数によるmのハッシュ値
（m）SigX：mにXの署名を付与した署名つき文書

図1　主プロトコルの流れ

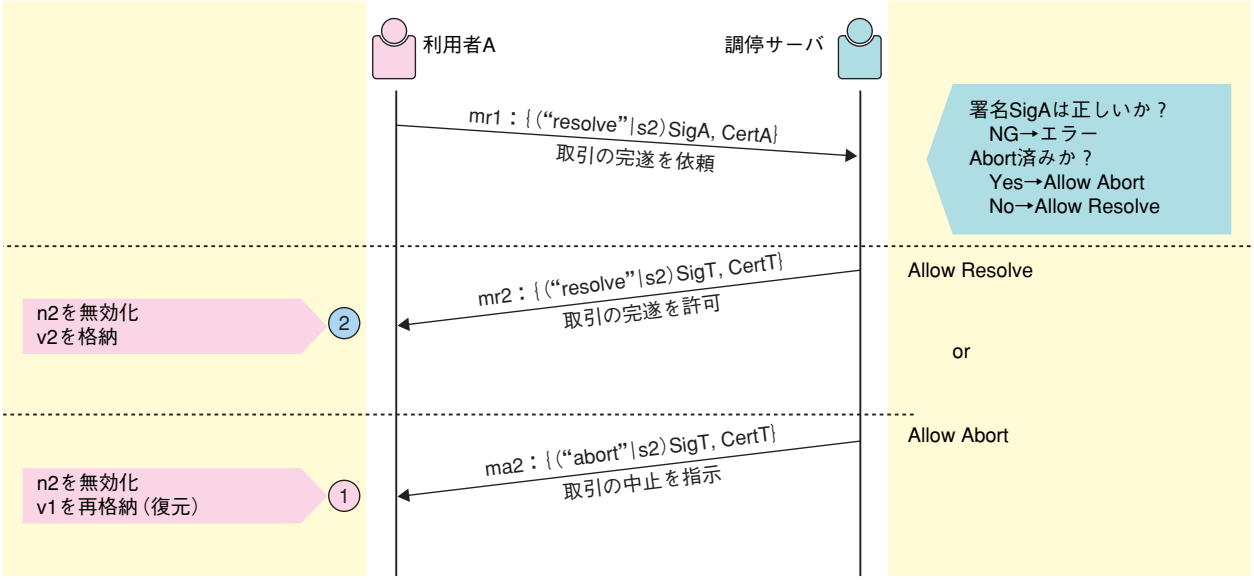


図2　Resolveプロトコルの流れ

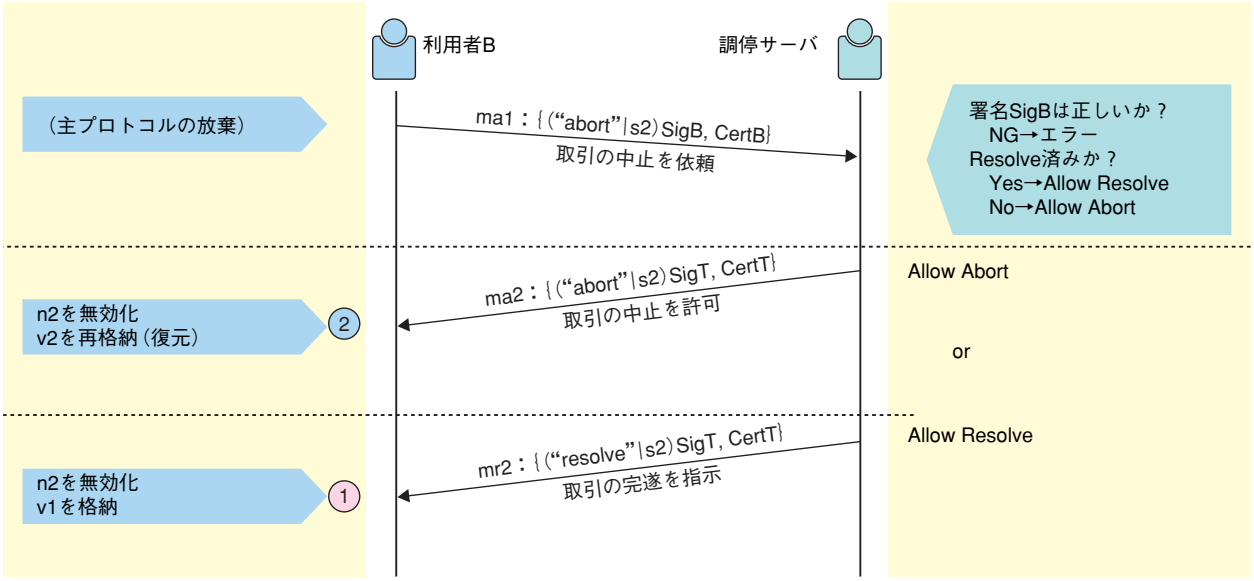


図3　Abortプロトコルの流れ

利用者AによりResolveプロトコルが実行されると，調停サーバは回復対象の取引がすでに中止済み（その取引について利用者Bとの間でAbortプロトコルを実行済み）か否かを判断する．まだ中止されていない場合，調停サーバは利用者Aに対して取引の完遂を許可し，利用者AのICカードには受け取るべきだった電子価値v2が格納される．中止済みであった場合，完遂を許可する代わりに取引の中止を指示し，利用者AのICカードには元のv1が再格納される．どちらの場合でも，利用者Aの不公平な状態は解消される．利用者BによるAbortプロトコルの場合も同様に，完遂済み（Resolveプロトコルを実行済み）か否かを判断した結果，未完遂の場合は中止許可により利用者BのICカードに電子価値v2が再格納され，完遂済みの場合は完遂指示によりv1が格納される．

ResolveプロトコルとAbortプロトコルのうち，先に実行された方の結果を優先するようにして調停を行うことにより，取引結果の矛盾を防止しつつ双方の利用者に対して不公平な状態からの回復を保証する．

4. 性能評価

本プロトコルの実用性を検証するため，本プロトコルを市販のミドルレンジICカード（CPU clock：15MHz, EEPROM：32kB, RAM：5kB）に実装し，性能評価を行った[5]．

主プロトコルによる取引の開始から終了までの各メッセ

表1　性能評価結果

処理の内容	演算処理	入出力	合計
取引提案（m1 生成）	50ms	129ms	179ms
取引受理（m1 処理）	191ms	153ms	344ms
取引合意（m2 処理）	553ms	153ms	706ms
取引確認（m3 処理）	402ms	91ms	493ms
取引完了（m4 処理）	24ms	42ms	66ms
取引全体	1,220ms	568ms	1,768ms

ージの処理に要した時間を**表1**に示す．それぞれの処理時間はICカードと端末との間でメッセージを授受するための通信時間を含む．ただし端末間の通信時間は含まない．

実装の結果，本ICカード程度の記憶容量および処理能力を持つICカードを用いて本プロトコルが実装可能であること，および本プロトコルを用いた電子価値の交換は，ネットワーク通信時間を除いて2秒以内で実現できることを確認することができた．

5. あとがき

本稿では，多種多様な電子価値を誰とでも安全に交換取引するための技術について，その設計目標と技術の概要について紹介し，提案技術をICカードへ実装し，性能を評価した結果を示した．実装に基づく性能評価の結果，本技術は現在のICカードを用いて，ほぼ実用に十分な性能で電子価値を取引できることが確認された．

本稿執筆時点において，本技術を移動端末から利用するためのICカード仕様およびJava™＊2 API（Application Program Interface）仕様の策定が完了している．また，これらの仕様は標準化団体T-Engine Forumにおいて標準仕様[6]としての採択が決定しており，PDAや家電製品などの組込み分野における本技術の応用が期待される．

今後は，本技術に対してさらなる安全性の検証を行うとともに，本技術を応用した新たなサービスの可能性について継続的に検討を進めていく予定である．

＊2　Java™：JavaおよびすべてのJava関連の商標およびロゴは，米国およびその他の国における米国Sun Microsystems, Inc. の商標または登録商標．

文　献

[1] M. Terada, M. Iguchi, M. Hanadate and K. Fujimura: “An Optimistic Protocol for Trading Electronic Rights,” Proc. 6th intl. conf. Smart Card Research and Advanced Applications (CARDIS2004), pp. 255-270, 2004.

[2] K. Fujimura and D. Eastlake: “RFC3506: Requirements and Design for Voucher Trading System (VTS),” Internet Society, 2003.

[3] 寺田 雅之，花舘 蔵之，藤村 考，関根 純：“電子権利流通基盤のための汎用的な原本性保証方式,” 情処論，Vol. 42，No. 8，pp. 2017-2029，2001.

[4] N. Asokan, V. Shoup and M. Waidner: “Asynchronous Protocols for Optimistic Fair Exchange,” Proc. 1998 IEEE Symposium on Security and Privacy, pp. 86-99, 1998.

[5] M. Terada, K. Mori, K. Ishii, S. Hongo, T. Usaka, N. Koshizuka and K. Sakamura: “TENeT: A Framework for Distributed Smartcard,” Proc. 2nd intl. conf. Security in Pervasive Computing (SPC2005), LNCS 3450, Springer-Verlag, pp. 3-17, 2005.

[6] T-Engine Forum, TENeT標準仕様，2005.

用 語 一 覧

API：Application Program Interface