2004－CSEC－27　(3)
2004／12／20

安全な電子価値交換プロトコルの IC カード実装

森　謙作† 寺田雅之† 石井一彦† 本郷節之†
†ＮＴＴドコモ ネットワークマネジメント開発部

電子価値を公平に交換可能なプロトコルを IC カードへ実装し，プロトコルの実用性の検証を行った．実装にあたり，電子財布などの取引アプリケーションからの利用が容易であること，および電子価値の交換を電子商取引として実用的な速度で行えることを目的とした．また，IC カードの I/F 設計において分散 IC カード環境のためのフレームワークである TENeT を利用することにより，IC カード間のメッセージのやり取りをアプリケーションから隠蔽し，IC カードとアプリケーションとの I/F を簡素化することができた．実装の結果，プロトコルのコードサイズは約 6KB，プロトコル処理時間は約 1.8sec であり，現在市販されている IC カードを用いて，上記プロトコルを実用的な性能で実現可能であることを示した．

Implementation of a Fair Exchange Protocol on Smartcards

Kensaku Mori†, Masayuki Terada†, Kazuhiko Ishii†, Sadayuki Hongo†
†Network Management Development Dept., NTT DoCoMo, Inc.

This paper reports the result of our implementation of the fair exchange protocol for electronic rights on smartcards. In this implementation, we adopted TENeT, a framework which enables smartcards to directly communicate one another, to simplify the interface between smartcard and application programs. Our implementation built on current smartcards can exchange electronic rights in less than 1.8sec, which is practically sufficient for electronic rights trading markets.

1. はじめに

今日 Edy[1]など IC カードを用いた電子商取引が広く使われるようになりつつある．また電子現金のみならず電子チケットや音楽コンテンツなどの電子価値を IC カードを用いて流通させる方式として FlexTicket[2]や TRN[3]が提案されている．これらの方式は IC カードを用いた利用者間の電子価値の譲渡，すなわち転々流通を可能としているため，利用者間で価値を相互に譲渡することにより電子価値の売買などの取引を行うことが可能である．しかしながら，単に電子価値を相互に譲渡するだけでは，取引の公平性が担保されないことが問題となる．すなわち，先に相手の電子価値を受理した利用者が取引を止めて電子価値を持ち逃げすることができる．

電子価値の取引を公平に行うために，信頼できる第 3 者（TTP : Trusted Third Party）を仲介させる方式がある．この方式では公平性は担保されるが，すべての取引を仲介する TTP に負荷が集中するという問題を持つ. この TTP への負荷集中を解決する方式として，電子価値の楽観的な交換プロトコル[4]が提案されている．このプロトコルでは，正常時には TTP を仲介させず 2 者間で交換を行い，交換相手の不正や通信路の障害などにより不公平な状態で交換が中断された時に TTP を利用して公平性を回復する．

このプロトコルをたとえば第 3 世代の携帯電話が備える IC カードである USIM に実装することができれば，携帯電話同士で電子チケットや音楽コンテンツなどの電子価値の取引を，低い TTP 運用コストで行うことが可能になる．

本稿では，電子価値の楽観的な交換プロトコルを IC

カード上に実装し，コードサイズや処理性能などの定量的な評価を行い，該プロトコルが IC カード上で実用的に実現可能であることを示す.

2. 電子価値の楽観的な交換プロトコル

電子価値の楽観的な交換プロトコルは，電子価値の所有者同士がお互いの電子価値を公平に交換可能な方式である．特徴は，正常時は所有者間で 2 往復のやり取りで交換を完了すること，および不公平な状態で処理が中断した場合には，各所有者が交換相手とのやり取りを復旧しなくとも TTP を利用して公平性を回復できることである．ここで公平性とは，交換を行っている各所有者が共に自分の電子価値を持つ，あるいは共に相手の電子価値を受理している状態となることである．TTP は公平性を保証する調停者の役割を持つ.

プロトコルの手順について説明する．登場人物は，H_A, H_B, U_A, U_B, TTP である．H_X は電子価値の売買や交換などの取引アプリケーション（AP）を操作する電子価値の所有者, U_X は H_X が所有する耐タンパ装置（たとえば IC カード）である．電子価値は U_X 内に格納されている.

交換プロトコルは主プロトコルと中止依頼プロトコルと完了依頼プロトコルの 3 つのプロトコルから構成される． H_A と H_B は，正常時は主プロトコルのみを実行する．U_A と U_B は，交換中の状態遷移を管理するセッション集合 S_A および S_B をそれぞれ保持し，TTP は中止許可済みの交換を表す集合 S_{abort} と完了許可済みの交換を表す集合 $S_{resolve}$ とを保持する.

U_A 内の電子価値 v1 と U_B 内の電子価値 v2 の交換手順を図 1 に示す．また記法を表 1 に示す.

表 1 プロトコル内の記号

H_A, H_B	耐タンパ装置の所有者
U_A, U_B	H_A,H_B がそれぞれ所有する耐タンパ装置
v1, v2	U_A, U_B に格納された電子価値
n1, n2	U_A, U_B が生成する乱数
h(x)	ハッシュ関数
s1	v1, v2, n1 から生成されるハッシュ値
s2	n2 から生成されるハッシュ値
$(m)P_{kX}$	m に対する X の公開鍵による署名
CertX	P_{KX} の公開鍵証明書

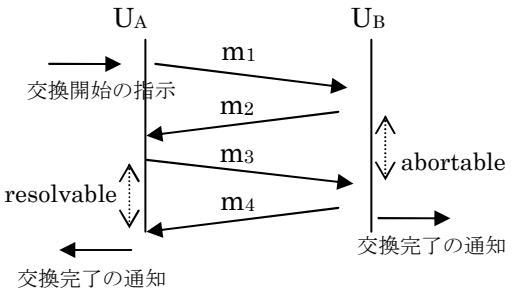

図 1 主プロトコル 手順

2.1.1. 主プロトコル

1.H_A は交換の指示メッセージ{v1,v2}を送付する

2.U_A は指示を受理して，U_B へ交換の提案メッセージ m_1:{v1, v2, n1}を送付する.
U_A は v1,v2,n1 を S_A へ格納する.

3. U_B は m_1 で示される v1 と v2 の交換に承諾すれば，v2 を削除し，s1=h(v1|v2|n1), s2=h(n2)を生成する.
U_Aへ交換の承諾メッセージ
m_2:{(s1|s2)P_{kB}, CertB} を送付する.
U_B は v1, v2, n1, s1, s2 を S_B へ格納する.
承諾しない場合は交換処理を終了する.

4. U_A は m_2 の検証後に v1 を削除し， U_B へ交換の実行メッセージ m_3:{(s2)P_{kA}, CertA} を送付する.
U_A は s1, s2 を S_A へ格納する.

5.U_B は m_3 の検証後に v1 を格納し， U_A へ交換の完了メッセージ m_4:{n2}を送付する.

6.U_B は H_B に交換が完了したことを通知する.

7.U_A は m_4 の検証後に v2 を格納し交換処理を完了する.

8.U_A は H_A に交換が完了したことを通知する.

図 1 で，abortable/resolvable 区間は不公平な状態である．この区間で処理が中断した場合には，H_X が U_X に中止/完了依頼プロトコルの実行を指示して，公平な状態に回復する.

U_B は abortable 区間（m_2 の生成から m_3 の受理までの間）の任意の時点において自分だけが電子価値を紛失している状態であるので，TTP との間で中止依頼プロトコルを実行して処理を中止（電子価値を復元）させることができる. 同様に，U_A は resolvable 区間（m_3 の生成から m_4 の受理までの間）の任意の時点におい

て，TTP との間で完了依頼プロトコルを実行することにより処理を終了させることができる．

以下，中止依頼プロトコルと完了依頼プロトコルの手順である．

2.1.2. 中止依頼プロトコル

1. U_Bは交換中止の依頼メッセージ
   m_{a1}:{(**abort**|s1) P_{kB}, CertB}を TTP へ送付する．
2. TTP は m_{a1}を検証後，s1 が $S_{resolve}$になければ， 交換中止の許可メッセージ
   m_{a2}:{(**abort**|s1)P_{kT}, CertT}を U_Bへ送付する．
   TTP は s1 を S_{abort}へ格納する．
   TTP は m_{a1}を検証後，s1 が $S_{resolve}$にあれば，
   交換完了の許可メッセージ
   m_{r2}:{(**resolve**|h(n2))P_{kT}, CertT}を U_Bへ送付する．
3. U_Bは m_{a2}を受領した場合は，m_{a2}を検証後，v2 を復元する(交換の中止)．
   U_Bは m_{r2}を受領した場合は，m_{r2}を検証後，v1 を格納する(交換の完了)．

2.1.3. 完了依頼プロトコル

完了依頼プロトコルの手順は，中止依頼プロトコルとほぼ同様である．

1. U_Aは交換完了の依頼メッセージ
   m_{r1}:{(**resolve**|h(n2)) P_{kA}, CertA}を TTP へ送付する．
2. TTP は m_{r1}を検証後，s1 が S_{abort}になければ， 交換完了の許可メッセージ m_{r2}を U_Aへ送付する．
   TTP は h(n2)を $S_{resolve}$に保存する．
   TTP は m_{r1}を検証後，s1 が S_{abort}にあれば，
   交換中止の許可メッセージ m_{a2}を U_Bへ送付する．
3. U_Aは m_{r2}を受領した場合は，m_{r2}を検証後，v2 を格納する(交換の完了)．
   U_Aは m_{a2}を受領した場合は，m_{a2}を検証後，v1 を復元する(交換の中止)．

3. 交換プロトコルの実装

本章では 2 章で示したプロトコルを IC カードに実装する際の，IC カードの入出力メッセージの設計方針について説明する．

3.1. 実装への要求条件

IC カードの入出力メッセージの設計にあたり，以下の 2 点を要求条件とする．

AP の利用の容易性

AP は IC カードと必要最小限のメッセージのやり取りのみで取引が実行できること．AP と IC カードがやり取りするメッセージが少ない程，AP は作成が簡単かつコードサイズが小さくなり，携帯電話への実装が容易になる．

処理性能

電子価値の取引が実用的な時間内で終了すること．ここで電子商取引では利用者を 8 秒以上待たせてはいけないという 8 秒ルール[6]が知られているので，本稿では 8 秒以内で終了することを最低限の要求条件とおく．

3.2. 設計方針

前述の 2 つの要求条件を満たすために，本実装では以下の設計方針を採ることとした．

AP の利用の容易性

まず，AP にとって IC カードとやり取りする必要がある最小限の情報を考える．H_Aにとっては交換の開始の指示（誰と，何と何を交換）とその結果の通知である．また受け手側の H_Bにとっては，U_Aから来た交換の提案内容の確認と，その承諾の指示である．これら以外の情報のやり取りについては，AP は意識しないで済むのが望ましい．

しかし， ISO7816-4 準拠の IC カードを用いて本プロトコルを実装すると，以下の問題が発生する．

IC カードは端末などから送られた APDU メッセージを受理してレスポンスを返却する処理を行うのみで，自ら他の IC カードや他端末上の AP と直接通信することはできない．それらとの直接通信を実現するには同端末内の AP が明示的に IC カードと他の装置とのやり取りを中継する必要がある．つまり，AP は APDU を解釈して通信の相手先を抽出し，適切な端末へネットワークを介してやり取りすべき情報を送付するなどの仲介処理が必要となる．

従って，交換プロトコルのように IC カード間でメッセージの送受を複数回繰り返す場合には，AP はメッセージ送受毎に APDU の解釈する必要があり処理

が煩雑になる．

上記のような IC カード同士での直接通信を支援するためのフレームワークとして，TENeT[5]が提案されている．TENeT はネットワーク上に分散して存在する IC カード間での直接のメッセージのやり取りを可能にする．また TENeT は，ネットワークから来たメッセージについて AP がその内容を確認するためのメッセージ監視機構を持つ．

TENeT を用いることにより，AP は IC カード間のやり取りを明示的に中継する必要がなくなり，煩雑な処理を軽減できる．

そこで本実装では、交換プロトコルの各メッセージを TENeT のメッセージである eTP メッセージとしてマッピングすることとした．

ただし，単に上記のマッピングを行うだけでは，交換の提案内容を示すメッセージ（m_1）は U_A と U_B 間で直接やり取りされるため，H_B がそれを承諾する機会を持てないという問題が発生する．この問題に対しては，以下のいずれかの方法により H_B に通知することができる．

1) TENeT のイベント通知機能を用いて m_1 を監視し，m_1 を U_B に送付する前に AP へ通知する．
   AP が拒否した場合には m_1 は廃棄する．
2) m_1 を交換相手の IC カードではなく AP へ送付する．
   AP は m_1 を承諾すると，宛先を IC カードとする提案内容の承諾(m_1')を出力する．

1), 2)共に実装可能であり，処理時間などにも差はないが，本実装では提案内容を承諾した利用者を明確とするため，2)の方法を選択した．

上記の方針に従い設計した IC カードの入出力メッセージを表 2 に示す．主プロトコルの入出力メッセージ手順を図 2 に示す．

処理性能

処理性能に影響するのは，(1)カードー端末間通信時間と(2)EEPROM の書き込み処理時間および(3)暗号処理時間である．このうち暗号処理時間は暗号アルゴリズムや鍵長が決まれば， IC カード自体の性能に依存するため，議論の対象外とし，残りの 2 点について議論する．

表 2 IC カード入出力メッセージ

主プロトコル	
交換の開始を指示	exchange [P_A, U_A, (V1, V2)]
交換の提案（m_1）	offer [U_A, P_B, m_1]
交換の提案（m_1'）	accept [P_A, U_A, m_1]
交換の承諾（m_2）	agree [U_B, U_A, m_2]
交換の実行（m_3）	confirm [U_A, U_B, m_3]
交換の完了（m_4）	commit [U_B, U_A, m_4]
完了依頼/中止依頼プロトコル	
完了/中止依頼の指示	req_ttp [P_A, U_A, h(s1)]
完了/中止依頼	rec_req [U_X, TTP, m_{a1} または mr_1]
完了/中止許可	rec_alw [TTP, U_X, m_{a1} または mr_1]
通知メッセージ	
交換の終了を通知	committed [U_X, P_X, h(s1)]

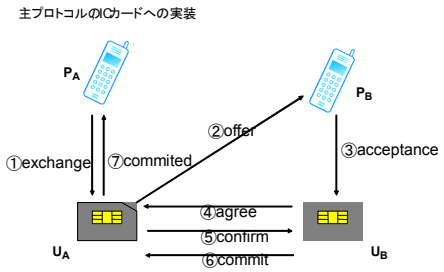

図 2　IC カード入出力メッセージ手順

(1)カードー端末間通信時間

カードー端末間の通信時間を小さくするためには，カードに入出力されるデータ量を削減しなければならない．交換プロトコルで用いられるデータの中では，v1, v2 を除くと，署名長やハッシュ長が主であり，ハッシュ長や乱数などと比較して特に署名長が支配的なサイズとなる．署名長は暗号アルゴリズムと鍵長に依存する．たとえば RSA 署名とすると署名長は 1024 ビットであるが，同程度の安全性を持つ ECDSA 署名は 160 ビットである．安全性は保ったままデータ量の削減が可能であるため，ECDSA を採用する．

(2) EEPROM の書き込み時間

交換プロトコルでは m_1～m_4 の送受において，交換

対象となる電子価値 v1 と v2 のほか，乱数 n1 と n2 と交換の識別子 s1, s2 が EEPROM 上で更新される．

ここで, EEPROM は 64 バイト単位でデータの書き込みを行うため，たとえば 20 バイトのデータである s1 の書き込みのみでも 64 バイト単位で更新を行う必要がある．このように，EEPROM 内で各値をばらばらに管理すると性能劣化の原因となるため，プロトコル内で同時に更新する値を状態管理テーブルとしてまとめることにより，書き込み回数を減らして処理時間を短縮する．

4. 実装結果

4.1. カードへの実装

実装する IC カードは, ECDSA の暗号演算に用いる暗号コプロセッサを備える Infineon 社製 SLE66CLX 320P を選定した．主な仕様を表 3 に示す．

表 3 IC カードの主な仕様

IC カード	EEPROM	ROM	RAM
SLE66CLX320P	32(KB)	132(KB)	5(KB)

上記の IC カード上へ交換プロトコルを実装した結果の，カード内のコードサイズの内訳を表 4 に示す．

表 4 IC カード内プログラムサイズ

プログラム	サイズ（KBytes）
1)トランザクション管理など	5.6
2)通信ライブラリ	14.0
3)暗号ライブラリ	5.0
4)交換プロトコル	6.0
計	30.6

交換プロトコルのプログラムサイズは約 6.0KB であった．また汎用的なライブラリである 1)～3)のサイズは合わせて 25.6KB であった．本実装ではこれらのプログラムを EEPROM に実装したが，交換の実行によりプログラムが書き換わることはないため，ROM に配置することも可能である．

残りの領域は状態管理テーブルおよび電子価値の格納領域として利用できる．ここで状態管理テーブルの大きさは，1 回の交換あたり電子価値 v1, v2 を除いて 95Bytes であるため，IC カードは状態管理のために“(95+v1 のサイズ+v2 のサイズ)×同時に実行可能な交換の数”の領域を必要とする．この領域を除いた部分が，電子価値を格納する領域となる．

従って，1KB の領域があれば，各電子価値のサイズを 60 バイトとして，同時に 4 つの交換が可能（4 交換分の状態管理テーブルを格納可能）である．

4.2. 処理性能

性能を測定した環境を表 5 に示す．端末に接続された R/W に IC カードを挿入し, IC カードで主プロトコルを 100 回実行し，主プロトコルのメッセージについて，R/W－IC カード間の入出力時間の平均を IC カード入出力時間，IC カード内での処理時間の平均を IC カード内処理時間とした．測定結果を表 6 に示す．

処理結果の内訳として, IC カードへの入出力時間が 0.56sec, IC カード内の処理時間が 1.22sec であり，主プロトコル全体で 1.79sec であった．

表 5 実測環境

IC カード	SLE66CLX320P
CPU Clock	15MHz
Card R/W	Gemplus GemPC Twin
通信速度	(端末-R/W) 12Mbps
	(R/W-Card) 38.4kbps

表 6 交換プロトコル処理時間（ms）

メッセージ	IC カード内処理時間	IC カード入出力時間	合計
exchange	50	129	179
accept	190	153	344
agree	552	153	706
confirm	401	91	492
commit	23	42	65
全体	1,219	568	1,788

5. 考察

第 4 章で示したように，電子価値の楽観的な交換プロトコルは本実験で用いた SLE66CLX320P などの現在市販されている IC カードで，ROM または EEPROM に格納できることから，十分に搭載可能であるといえる．

以下，第 4 章の結果に対して，各要求条件について考察を加える．

AP の利用の容易性

AP が IC カードとのやり取りに利用するメッセージは exchange（交換の開始を指示）と committed（交換の結果の通知）の 2 個のメッセージだけであり，その他のメッセージは AP から隠蔽される。AP は利用するメッセージ数が少なく作成が容易となる．

従って，AP は必要最低限のメッセージで IC カードとのやり取りが可能であり，要求条件を満たしているといえる．

処理性能

本実装において，IC カードでの処理は 1.79sec で実行できた．IC カード内処理時間の内 682ms は署名生成と署名検証処理の時間である．ECDSA をより高速に実行できる IC カードが市場に出つつあるため，たとえばこれらの IC カードへ実装すれば署名生成時間が短縮でき，IC カード内の処理時間はより削減できる．

また，第 4 章の性能評価においてアプリケーション処理時間とネットワーク通信時間は考慮していないが，アプリケーション処理はメッセージの配送のみを行うため，IC カードの処理と比較すると無視できる程小さいものである．ネットワーク通信時間はネットワークの環境に依存するが，本実装においてネットワーク上でやり取りされるメッセージは今日のネットワークの性能に対して十分に小さい（電子価値のサイズを 60 バイトとした時最大 280 バイト程度）ため，通信時間はそれ程大きな値とならないと考えられる．たとえば，スループットが 300kbps，遅延が 100ms 程度の通信環境であれば，通信時間は 0.5sec 以内におさまる．これらの結果から，電子価値の取引にかかる時間を 8 秒におさえることは十分可能であると考えられる．

6. まとめ

本稿では，要求条件である処理性能と AP の利用の容易性を満たすメッセージ設計により，交換プロトコルを IC カードへ実装し，その実用性について示した．

メッセージ設計では，TENeT を利用することにより，IC カード間のメッセージのやり取りを AP から隠蔽し，IC カードの I/F を簡素化することができた．

また交換プロトコルの処理時間は，約 1.8sec であり，現在市販されている IC カードを用いて，電子商取引において実用的な時間で実現可能であることを示した．

参考文献:

1) Edy: http://www.edy.jp/.
2) 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，Vol42, No.8, 2001.
3) 倉光君郎，村上直，坂村健: TRN:耐タンパ性ネットワーク，情処論，Vol.42, No.8, 2001.
4) Terada, M., Iguchi, M., Hanadate, M. and Fujimura, K.: An optimistic fair exchange protocol for trading electronic rights, Proc. the 6th Working Conference on Smart Card Research and Advanced Application (CARDIS 2004), 2004.
5) 寺田雅之，森謙作，石井一彦，本郷節之，鵜坂智則，越塚登，坂村健: 分散 IC カード環境のためのアーキテクチャの提案，コンピュータセキュリティシンポジウム 2004, 2004.
6) アスキーデジタル用語辞典: http://yougo.ascii24.com
7) ISO/IEC Integrated circuit(s) cards with contacts – Part4: Interindustry commands for interchange, ISO/IEC 7816-4: 1995(E).
8) ISO/IEC Integrated circuit(s) cards with contacts – Part3: Electronic signals and transmission protocols, ISO/IEC 7816-3: 1997(E).
8) Rankl, W., Effing, W.: Smart Card Handbook, 2nd edn., John Wiley & Sons, 2001.