電子印紙システムの設計と実現

新保 淳[†] 加藤岳久[††] 才所敏明[††]

官公庁に対する各種申請文書において手数料が必要なものがあり，主に印紙が利用されている．近年，申請の電子化が検討されているが，印紙に代わる申請手数料の電子化手段が必要となっている．今回，プリペイド型バリューを充填したICカードを利用して申請手数料の支払い事実を証明することをベースとするスキームを考案し，システムを試作した．この方式は電子マネーの一変形であるが，現在の印紙で実現されている手数料納付の仕組みにより近く，受付側での支払確認処理がより少ない利点がある．特に，支払証明書の作成は申請側のローカル環境で完了するため，申請文書とともに支払証明書を添付して送ることができる．このように，手数料納付にかかわるプロトコルの簡便性に特徴がある．

Design and Implementation of Electronic Revenue Stamp System

Atsushi Shimbo,[†] Takehisa Kato[††] and Toshiaki Saisho[††]

In administrative fields, applicants have to pay fees for some applications. Currently, revenue stamp is used for such payment. In order to realize electronic application system, one issue is how to pay the commission through the communication network. This paper proposes a commission payment system that is a variant of electronic money systems. We use digital certificate of fee payment as the electronic revenue stamp, which is generated by smart card issued to applicants. Since the electronic stamp is generated at the applicants locally, the stamp can be transmitted with applications. The feature of the proposed system is that the payment procedure is handled in the same way as the current paper-based system. Therefore the payment verification processes at application receivers and the protocol between the applicants and the application receivers become simpler.

1. はじめに

インターネットに代表されるオープン・ネットワークを利用して各種業務や取引きを電子化し，その合理化を狙った電子商取引が企業間，企業対消費者間等の様々な応用分野で検討されている．行政側でも国民等との間の様々な申請や届出等の手続を電子的に実行可能とするシステムが検討されている．このような申請文書の電子化における課題に，手数料の納付方法がある．すなわち，申請文書には手数料の必要なものがあり，現在は印紙の貼付が行われている．したがって，現在の印紙による手数料納付法を代替する電子的決済手段が必要となり，本文はこうした手段を検討したものである．

手数料は，申請の内容によって必要な金額が変わるものの，一般には少額である．したがって，クレジットカードや銀行の口座振替え等では金融機関が要求する新たな手数料の額が無視できない．一方，ネットワーク上での少額決済に向いた方法には，各種の電子マネー[2)~9)]がある．電子マネーが普及すればそれを利用した申請手数料の納付は原理的には可能と考えられる．しかし，電子マネーのスキームをより細かく調べると申請手数料の納付という場面では不要と思われる機能が盛り込まれている方式が多い．たとえば，匿名性[2)~4)]と転々性[7)]があげられる．申請書には申請者の氏名を記入するものがほとんどであろうし，印紙を他人に譲渡することはほとんど行われていないと想像される．また，電子マネーの受渡しに専用のプロトコルが必要であり，申請書の通信手順と単純には一体化できないうえに，電子マネー送信時のトランザクションを保護する必要も生じうる．電子マネーの活用では，こうした機能やプロトコル設計がシステム構成を複雑化する可能性がある．

そこで，現在の印紙による手数料納付に近い運用形態で利用できるスキームを新たに設計し，試作した．

† 株式会社東芝研究開発センター
Research & Development Center, Toshiba Corporation
†† 株式会社東芝情報・社会システム社SI技術開発センター
System Integration Technology Center, Toshiba Corporation

本システムは現在の印紙による手数料の納付に近い手順となっており，申請者と申請受付機関との間に手数料支払いのための特殊なプロトコルを必要としない特徴がある．このため，システム構築や運用上の負担が少ないものと期待できる．

2. 開発方式の特徴

開発システムはストアド・バリュー型の IC カード電子マネーシステムに近く，技術的には，耐タンパー性のあるデバイスにディジタル署名機能を実装し，所持者すら知りえない署名鍵を搭載する方式[6]，電子証書型のバリューを任意の金額に分割使用する方式[8]を利用している．

ただし，ストアド・バリュー型電子マネーをそのまま申請時の手数料納付に用いた場合にはいくつかの問題が考えられる．ここでは，開発方式の特徴を電子マネーを利用した手数料支払システムと対比しながら説明する．

IC カードによる署名 IC カード上のチップにディジタル署名機能を備えており，個々のチップに記録された署名鍵の安全性は高い．また，すべてのカードは署名鍵で個別化されているので，署名鍵も含めてカードの偽造・複製が発生したとしてもシステム全体に影響が及ぶことはない．

この性質は IC カード型の電子マネーと同じである．

環流不要なバリュー 電子的な金額情報であるバリューの発行体は国もしくはその代理組織とすることを想定している．したがって，使用されたバリューを申請受付機関から発行体に環流しなくても手数料は前納で国庫に入る．すなわち，使用されたバリューに対して現金化のための環流は不要であり，運用負担の軽減につながると考えられる．

一方，電子マネーの場合には受領した電子マネーを発行機関である金融機関に環流する手続きが必要であること，国庫への入金が遅れること等の問題がある．

申請文書と一体化可能 カードがバリューを減額したことを証明するディジタル署名データを手数料の支払証明書と見なしている．この支払証明書は申請側でローカルに生成できるため，たとえば電子メールで申請文書と一緒に送信できる．また，フロッピーディスクに申請文書と支払証明書を記録して提出するオフライン申請にもそのまま対応できる．すなわち，手数料支払を目的とした特殊なプロトコルは申請者と申請受付機関との間で不要であり，システム構築が容易となる．

一方，電子マネーでの支払いの場合，受取側と支払側でインタラクションが必要であり，リアルタイムでの支払いには受取側とのオンライン接続が必要である．したがって，オフライン申請には原理的に対応できない．また，電子マネーの受渡しに利用する専用のプロトコルが必要であり，電子マネー通信時のトランザクションの保証を考慮するとシステムが複雑化する．

二重使用の防止 バリューは使用の都度，使用目的を一意に表す形式で支払証明書が作成され，一度作成されると，他の使用目的に転用することは困難である．使用目的は毎回変化する必要があるが，本システムでは申請文書そのものが使用目的をユニークに定めるものであり，しかも日付等を含めてまったく同じ内容の申請が行われることは意味をなさないとの解釈のもとで，申請文書のハッシュ値を使用目的のユニーク化に利用している．

電子マネーでも二重使用は防止されているが，本手法に比べると複雑であり，先に述べたように受取側からのチャレンジを必要とする．

匿名性と転々性の排除 電子マネーで重要視されている匿名性や転々性を排除している．このことが，運用負担の軽減のみならず，万一セキュリティ上問題が生じた場合にも不正者/不正デバイスを特定しやすいという特徴につながっている．

IC カード型電子マネーでは匿名性や転々性を備えた方式が存在するが，運用負担を下げるためにこれら機能を外している場合も多い．

バリューの分割使用と再充填 申請者の利便性を配慮し，カードに充填されたバリューを任意の額面に分割して使用可能としている．また，カードにはバリューを再充填可能とし，カード内に少額のバリューが残った場合にカードを複数枚利用しなければならない等の不便はない．

この性質は多くの IC カード型電子マネーと共通している．

3. 電子印紙システムの概要

3.1 全体構成

図 1 は，本システムの全体構成とプロトコルの概要を表している．本システムは，支払証明書を発行する申請者カード，申請者カードを装着し申請者とのインタフェースを司る申請ホスト，申請者カードが生成した支払証明書の正当性を検査する申請受付機関（支払検査ホスト），申請者カードおよびバリューを発行す

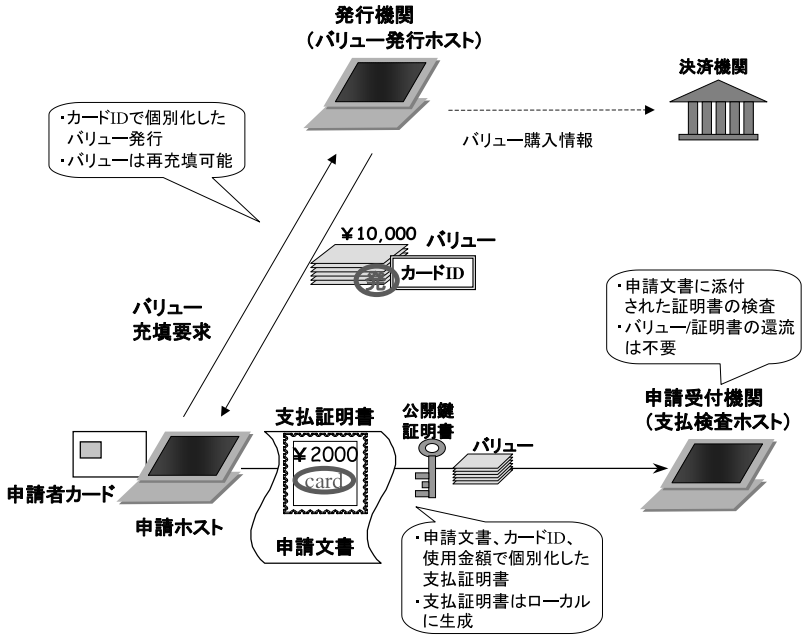

図 1 システムの構成
Fig. 1 System overview.

る発行機関（バリュー発行ホスト）から構成される．

さらに，バリュー代金の決済に，クレジットや銀行等の口座振替を利用する場合には，それらの決済機関が必要となる．

以降の説明で発行機関はカードの公開鍵証明書の発行，バリューの発行，カード自体の発行の各機能をすべて行うものとしているが，これらの機能を分離して，たとえばカード公開鍵証明書の発行は一般の Certification Authority を活用してもよい．

3.2 プロトコルの概要

- バリューは電子証書型であり，1つずつ識別可能な形式で発行され，カード内で管理される．バリューにはカード ID が指定されており，そのカードでしか利用できない．
- 申請者カードにはバリューが格納され，その残高がカウンタで管理される．カードは支払証明書をディジタル署名により作成し，そのたびにカウンタを減額する．支払証明書はカード ID と申請文書のダイジェストで個別化されるので，他の申請文書への転用や二重使用はできない．
- 支払検査時には，申請文書と支払証明書のリンクをダイジェストの一致により確認し，さらに支払証明書を署名検証する．これらの検証処理は支払検査ホストがローカルに実行でき，申請者カードの耐タンパー性を破るような不正を考慮しない場合には，使用済みの支払証明書をシステム側で集中管理する必要はない．ここで耐タンパー性を破る不正の具体例は，カード内の残高カウンタを改変したり，カード内の秘密鍵を読み出したうえで，このカードをシミュレートする偽造ソフトを作成する等である．
- 申請者カードへのバリューの再充填では，カード内のバリューを全額使用済みとする残高支払証をカードが作成し，同支払証および追加する前納額と引換えに新規バリューをバリュー発行ホストから充填する．再充填時のバリューの額面は，追加の前納額にカード内の残高を加算したものとする．

3.3 鍵 管 理

申請者カードにはカード固有の署名鍵が記憶される．以降では $S_{dev}(M)$ により dev の保持する署名鍵を用いたメッセージ M に対するディジタル署名を表す．

カードの署名鍵に対応する公開検証鍵（CardPubKey）は，発行機関（Issuer）の発行したカード公開鍵証明書（CardCert）を用いて正当性を確認できる．公開鍵証明書にはカード ID（CID），有効期限（ValidDate）が添付されている．

$$CardCert = S_{issuer}(CID, CardPubKey, ValidDate)$$

公開鍵証明書の正当性を検査するために必要な発行機関の公開検証鍵は，各申請者カードおよび各支払検査

ホストに保有される．

3.4 カード格納データ

申請者カードには，以下のデータエリアが設けられる．

- カード ID
- 署名鍵（申請者カード固有の署名鍵）
- 公開鍵（カード公開鍵証明書，発行機関の公開検証鍵）
- バリュー
- バリュー残高，バリュー累積利用額
- ログ（支払証明書，残高支払証等の履歴を記録）
- 申請者個人情報（氏名，住所等）

各エリアは IC カードのアクセス制御機構により外部からの不正アクセスが防止されている．たとえば，署名鍵は読み出し・書き換え禁止，バリュー残高や累積利用額は書き換え禁止，バリューの書き込みにはカード所持者の PIN 照合が必要等である．

4. 電子印紙プロトコル

以下，プロトコルの各フェーズをより詳細に説明する．このプロトコルは，申請者カード発行，支払証明書生成，支払証明書検査，バリュー再充填の手順から構成される．

4.1 申請者カード発行手順

申請者は，新規にシステムを利用する場合やカードの有効期限が切れた場合に，発行機関でカードの発行を受ける（**図 2** 参照）．

カード発行は発行機関でローカルに行われ，カード署名鍵と公開鍵証明書の作成が行われた後，カードにカード ID，署名鍵，公開鍵，個人情報が書き込まれる．さらに，新規バリューの発行を行い，バリューに相当する金額（バリュー代金）の決済が行われる．

バリューは以下の形式であり，カード ID（CID），バリュー番号（Num），バリュー金額（PrePay），カード乱数（CRand）を含んでいる．カード乱数は，バリュー充填の過程でカードが発生し，バリュー発行ホストに出力する値である．

$$Value = S_{issuer}(CID, Num, PrePay, CRand)$$

申請者カードは，バリューの正当性を署名検証により確認する．正当性が確認された場合には，バリューをカード内に記憶し，さらにカード内のバリュー残高をバリュー金額分に設定する．処理が完了したら，購入手続きの完了を示す受領確認（ACK）をカード発行ホストに送信する．

$$ACK = S_{card}(CID, Num)$$

異常の場合には ACK 以外のエラー信号を返す．

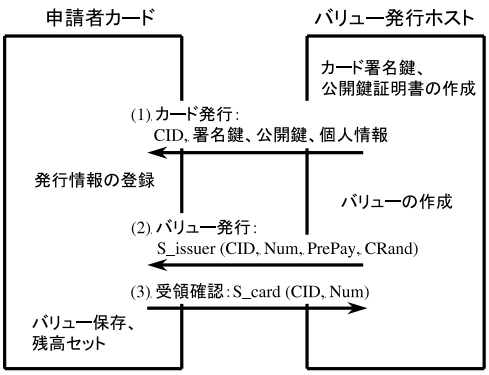

図 2 申請者カード発行手順
Fig. 2 Procedure of applicant's card issuance.

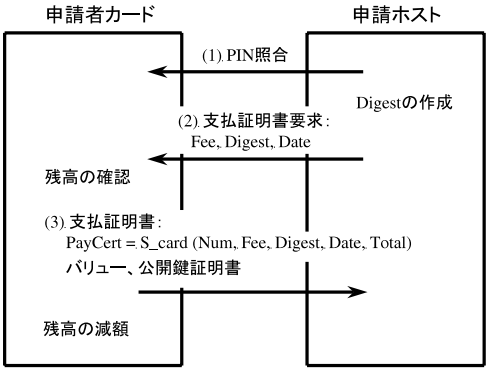

図 3 支払証明書作成手順
Fig. 3 Procedure of payment certificate generation.

4.2 支払証明書生成手順

支払証明書は，申請者カードがカード内バリューの減額処理を実行したことの証明となるデータである．支払証明書の生成は，申請者カードとそれを装着した申請ホストの間で以下のステップで実行される（**図 3** 参照）．

(1) カードに対する申請者の照合を PIN により行う．

(2) 申請者は申請ホストで，申請文書データと，必要な申請手数料（Fee）を指定する．
申請ホストは，選択された申請文書データをハッシュ処理した文書ダイジェスト情報（Digest）を作成し，申請手数料と日付（Date）とともに申請者カードへ送る．

(3) 申請者カードは，申請者カード内のバリュー残高を検査する．要求された申請手数料未満の残高しかない場合には残高不足のメッセージを返して終了．

(4) 申請者カードは，まず申請者カード内のバリュー残高を申請手数料分だけ減額し，累積利用額をその額だけ増やす．さらに，支払証明書を作成する．支払証明書（PayCert）は，バリュー番号（Num），申

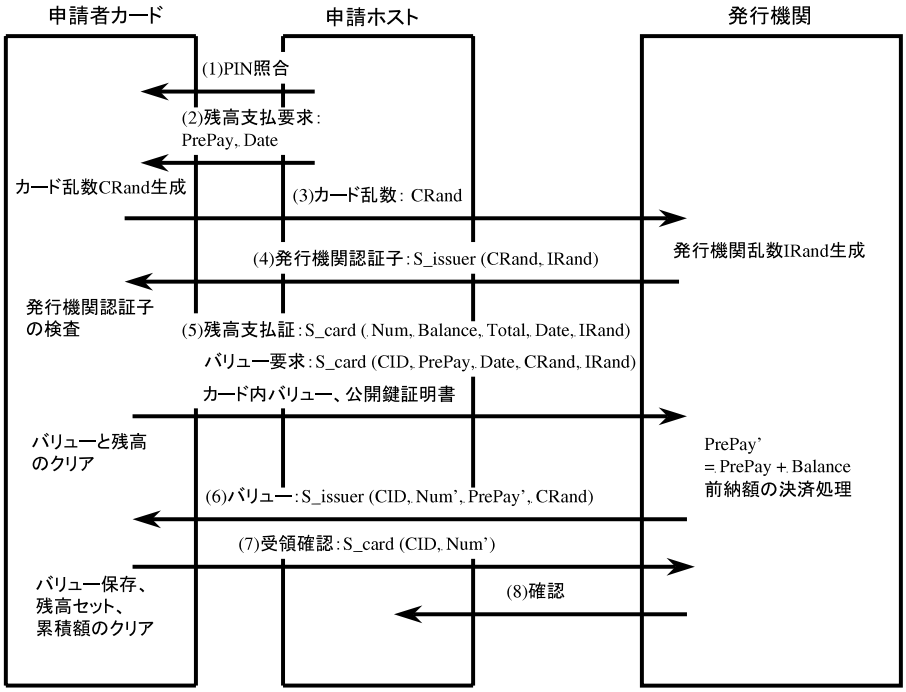

図 4 再充填手順
Fig. 4 Procedure of value reloading.

請手数料，申請文書ダイジェスト（Digest），日付（Date），累積利用額（Total）に対する申請者カードの署名データである．

$$PayCert = S_{card}(Num, Fee, Digest, Date, Total)$$

生成された支払証明書は，カード内のバリュー（Value）と公開鍵証明書（CardCert）とともに申請ホストに出力される．

4.3 支払証明書付き文書送信

支払証明書付き申請文書の送信は，申請ホストから申請受付機関に向けて行われるが，メールのような非同期型の通信でもよいし，WWW のようなリアルタイムの通信でもよい．送信するデータは，申請文書，支払証明書，カード公開鍵証明書，バリューとする．ここで，申請受付機関が発行機関等から発行済みのバリューに関する情報を取得できる場合には，バリューを送信データに含める必要はない．

4.4 支払証明書検査手順

支払検査ホストでは以下の手順により支払の検査を行う．

(1) 支払検査ホストは，受信した電子文書に対し，支払証明書の正常/異常を判定する．

検証すべきポイントは，1）支払証明書，バリュー，公開鍵証明書の署名検証，2）支払証明書内の文書ダイジェスト情報と申請文書のハッシュ値との一致確認，3）支払証明書内のバリュー番号（Num）とバリュー内の番号との一致確認，4）公開鍵証明書内のカード ID とバリューのカード ID との一致確認，5）支払証明書内の申請手数料（Fee）が累積利用額（Total）以下であり，累積利用額がバリューの金額（PrePay）を超えていないことの確認，6）支払証明書内の日付（Date）が公開鍵証明書内の有効期限（ValidDate）を超えていないことの確認である．

(2) さらに支払証明書内の申請手数料が申請に適当な額であること，支払証明書内の日付が申請受理日や申請文書に記載されている日付と照合して異常がないこと等の検証を行う．

(3) オプションとして，支払検査ホストは申請ホストに対して，受信した電子文書の手数料支払が承認されたかどうかを表す信号を返す．なお，カードの耐タンパー性を破る不正を考慮する場合にはさらに別の二重使用の検査が必要となる．この点については 5.1 節でふれる．

4.5 バリュー再充填手順

バリュー発行ホストにインターネットを介して接続していることを想定したバリュー再充填の手順を**図 4** に示す．

(1) カードに対する申請者の照合を PIN により行う．

(2) 申請者は申請ホストにて，追加する前納額（PrePay）を指定する．申請ホストはカードに前納額と日付を送る．

(3) 申請者カードは発行機関認証時に用いるカード乱数（CRand）を出力する．カード乱数は発行機関に送られる．

(4) 発行機関はカード認証に用いる発行機関乱数（IRand）を生成し，カード乱数と連結して発行機関認証子を作成し，申請ホストに送る．

(5) 申請者カードは発行機関認証子の署名を検証し，特にカード乱数が正しく織り込まれていることを確認する．検証に成功した場合，カード内残高（Balance）の証明となる残高支払証（InitCert）とバリュー要求（ValueReq）を生成する．

$$InitCert = S_{card}(Num, Balance, Total, Date, IRand)$$

$$ValueReq = S_{card}(CID, PrePay, Date, CRand, IRand)$$

残高支払証とバリュー要求にはともに発行機関乱数を織り込んでいることに注意．残高支払証の生成後，カード内残高をクリアし，残高支払証とバリュー要求とカード内バリューと公開鍵証明書を一緒に出力する．

(6) 発行機関は受信したデータの署名検証を行う．特に発行機関乱数が残高支払証とバリュー要求に正しく織り込まれていることを確認する．さらに，残高支払証とカード内バリューと公開鍵証明書の組に関しては支払証明書検査手順と同様にバリュー番号の一致検査，カード ID の一致検査，日付の検査，金額の検査を行う．以上の検証に成功した場合，新規バリュー（Value’）を生成し，送信する．

$$Value' = S_{issuer}(CID, Num', PrePay', CRand)$$

新規バリューの額面（PrePay’）はバリュー要求の前納額と残高の合計とする．ここで，新規バリューにカード乱数が織り込まれていることに注意．

(7) カードは受信した新規バリューの署名を検証する．特に，正しいカード乱数が織り込まれたバリューであることを確認する．これは，申請者の不正により残高支払証を発行機関に対して送信せず，新規バリューとみせかけて，以前のバリューを不正に充填する行為を防止する効果がある．

さらに，額面の正当性を検査し，異常がなければバリューをカード内に保存し，残高を設定し，累積額をクリアする．確認信号として ACK を出力する．

(8) 発行機関は ACK を受信すると以上のプロトコルのログデータを消去する．このログデータはプロトコル実行中の通信エラー等によりバリューや認証子の再送が必要になった場合に利用される．すなわち，申請ホストと発行機関の間で通信エラーが生じたと疑われる場合には，申請ホストがその部分からプロトコルを再開する．同じバリューが複数回送信される場合があるが，カードに充填されない限りバリューは利用できないし，正常なカードにはバリューを 1 つしか充填できない．

5. 考　　察

5.1 リスクと対策

本システムにおいて想定される典型的なリスクとそれに対して講じられている対策をまとめる．

(1) バリュー，支払証明書の偽造

リスク 上記データの内容を改変して不正利用すること．

対策 バリューや支払証明書へのディジタル署名．

(2) バリューのコピーによる不正使用

リスク バリューをコピーして偽造カードや偽造ソフトを用いて不正使用する．

対策 バリューの使用に必要な署名鍵は，対応する申請者カードの耐タンパー性により外部への漏洩から保護．

(3) 支払証明書のコピー使用

リスク ある文書に対する支払証明書を別の文書に対する支払証明書として再利用する．

対策 支払証明書に盛り込まれた申請文書のダイジェスト情報．

(4) 申請者カード内バリュー残高の改変

リスク 申請者カード内の残高を改変し，実際の購入金額以上にバリューを使用すること．

対策 申請者カードの耐タンパー性で残高を保護．

購入したバリューを分割使用するうえで，額面金額以上に使用する (2) と (4) の不正行為の対策が，本質的にカードの耐タンパー性のみであることには注意が必要である．解読装置の開発にある程度のコストをかけた場合，IC カードの耐タンパー性は必ずしも十分ではないという事例も報告[1)]されている．したがって，この不正に対抗する手段を講ずる必要性も考えられる．

このような対策のうち最も厳密と考えられるものは，バリュー発行側にバリューに関する集中データベースを構築することである．発行したバリュー，支払証明書，残高支払証はすべてこのデータベースに集められる．集中データベースは未使用額の残っているバリュー番号と残高，バリュー発行先のカード ID の一覧を持

つ．残高が 0 になった時点でデータベースから削除する．残高がマイナスになる場合やデータベースにない場合は，二重使用があったことになるので対応するカード ID をブラックリストに登録する．ブラックリストは定期的に各申請受付機関に配布される．

この対策をとると，二重使用の検出が確実に行えるが，支払証の集中管理が必要となり，電子マネーと同等の運用負担が生じる可能性がある．中間的な対策として，特定のバリューに対する支払証明書や，特定の支払証明書だけを抜き打ちで集中データベースに送ることで運用負担を下げる変形法も考えられる．

5.2 申請文書の修正

前章で示した電子印紙プロトコルでは，支払証明書の二重使用を防止するためにその使用目的をユニーク化する手法として申請文書のハッシュ値を利用している．したがって，いったん提出した申請書に不備があった場合等，申請書を修正した際に修正前の申請書に対応する支払証明書は利用できない．これに対しては，修正文書を提出する際には修正前の支払証明書付きの申請書と修正後の支払証明書なしの申請書の両方を提出する等，運用手順の工夫により対処することもできるが，プロトコルを変形することで申請文書の修正に対応することも可能である．以下に具体例を示す．

支払証明書の形式を変更し，申請文書ダイジェスト（Digest）の代わりに支払証明書番号（PayNum）を署名データに含める．

$$PayCert = S_{card}(Num, PayNum, Fee, Date, Total)$$

支払証明書番号は申請者カードがシリアルに振る番号で，バリュー単位に発行される．また，システムには使用された支払証明書番号を管理するデータベースを設ける．このデータベースはバリュー番号ごとに使用された支払証明書番号を管理する．申請受付機関では，まず申請文書の受信時に支払証明書の署名検証等の仮検査を実施する．次に，申請文書の内容を確認し，これを受け付ける最終段階で支払証明書データベースにアクセスし，該当する支払証明書番号が使用済みでないこと，すなわち二重使用の有無を確認する．二重使用がない場合には，新たに該当する番号を使用済みとしてデータベースを更新する．

このようにすると，支払証明書は申請文書に依存しないため，申請の内容審査が完了しない限り，申請文書の修正ができる．ただし，欠点としては申請文書を受理するたびにデータベースへのアクセスが必要となることであり，その点はネットワーク型電子マネーがベースとしている手法[2),3)]と類似である．

注意として，支払証明書の提出には第三者の盗聴から保護された通信路を利用する必要がある．支払証明書を盗聴可能な通信路で送信すると，第三者が通信途上の支払証明書を取得し，元の申請文書の受付けが終了する前に，都合の良い申請書と一緒に支払証明書を利用する可能性があるためである．

5.3 転々性と有効期限

このほかにも現状の印紙と比較した場合の本システムの相違点はいくつかあるが，特に転々性（譲渡可能性）と有効期限があげられる．本文の冒頭で述べたように本システムの設計であえて転々性は削っており，一方，有効期限は暗号技術の性格から設定せざるをえない．

ただし，疑似的ではあるが，転々性の追加や有効期限の更新はバリュー再充填時に利用している残高支払証の出力と新規バリューの発行という機能を応用することで実現可能である．

たとえば，転々性に関しては必ず発行機関を経由してバリューを移転することにすると，送信元のカードはバリューの残高支払証を発行機関に対して出力し，発行機関は移転先のカードに対する新規バリューを発行して移転先のカードとの間でバリュー充填を実施する．ここで，新規バリューの額面は残高分とする．

同様に，有効期限に関しては新規バリュー金額を 0 としてバリュー再充填プロトコルを実行すれば，有効期限が延長されたバリューが充填でき，このときのバリュー額面は残高分となる．

6. 試　　作

本文で示した機能を実装した発行ホスト，申請ホスト，申請者カード，支払検査ホストを試作し，機能検証を行っている．

- RSA 署名の生成/検証機能を備えたコプロセッサを内蔵した IC カードを利用．このカードは EMV 仕様に準拠したコマンド体系を備えているが，さらに，バリューの充填，支払証明書の作成，再充填時残高支払証の作成の 3 つの独自コマンドを設計し，追加した．追加したコマンドの処理ソフトは，試験的な実装のため ROM ではなく EEPROM に置く形態とした．
- 申請ホストおよび受付検査ホストは WWW ベースのユーザ・インタフェースとした．検査ホストには personal web server をインストールし，ユーザ・インタフェースと処理系を CGI を利用して作成した．
- 発行ホストは PC 上に専用の GUI を備えたアプ

リケーションとして実装した．発行ホストは初回のカード発行，バリュー充填，窓口対応でのオフラインでのバリュー再充填を実行する機能を備えている．

- オンラインでのバリュー再充填に対応したバリュー発行サーバを Web Server と CGI を利用して作成した．
- 正当な支払証明書を貼付した申請文書と不正な支払証明書を貼付したものや未貼付のものを支払証明書の署名検証により判別し，視覚的に表示する機能をアプレットを利用して作成した．支払検査ホストや申請ホスト等で利用できる．

カードの RSA 署名には 512 ビットの鍵を利用し，公開鍵証明書には RSA 1024 ビットを利用した．カード新規発行，バリュー再充填，手数料支払，支払検査等いずれの処理時間もパラメータ入力後 2〜3 秒以内に終了しており，十分実用的な処理時間が達成できている．また，安全性をより向上させるためにカードの署名を 1024 ビットの RSA に変更することも可能である．その場合，より高速なコプロセッサを搭載したチップが必要となるが，そうしたチップはすでに実現されており，試作システムと同程度の処理時間となる見込みである．

7. ま と め

電子申請における手数料支払いに適した電子決済方式を設計し，電子印紙システムとして試作を行った．印紙による手数料支払を実際に本手法で実用化するうえでは技術面以外に，法制度面での変更や対応も必要となる．ただし，本文で検討したように技術的な課題はクリアできると考えている．

さらに，開発方式は申請手数料の支払い以外の用途にも応用可能と考えられる．たとえば電子商品券，電子切手，有料コンテンツのネットワーク販売等があげられる．こうした応用システムの具体化には今後の検討が必要である．

謝辞 本文は，情報処理振興事業協会が実施する平成 8 年度補正予算「特定プログラム高度利用等事業」および平成 10 年度第三次補正事業「産業・社会情報化基盤整備事業」の一環として，財団法人ニューメディア開発協会の委託を受け，当社が開発中のシステムに関する内容を含んでいる．関係各位のご支援に感謝の意を表する．

参 考 文 献

1) Anderson, R. and Kuhn, M.: Tamper resistance – a cautionary note, *2nd USENIX Workshop in Electronic Commerce* (1996).
2) Chaum, D.: Blind signatures for untraceable payments, *Advances in Cryptology CRYPTO '82*, pp.199–203 (1983).
3) Chaum, D.: Online Cash Checks, *Advances in Cryptology EUROCRYPT'89*, pp.288–293 (1990).
4) Chaum, D., Fiat, A. and Naor, M.: Untraceable electronic cash, *Advances in Cryptology CRYPTO'88* (1989).
5) Eng, T. and Okamoto, T.: Single-term divisible electronic coins, *Advances in Cryptology EUROCRYPT'94* (1994).
6) Even, S., Goldreich, O. and Yacobi, Y.: Electronic wallet, *Advances in Cryptology CRYPTO'83*, pp.383–386 (1983).
7) Okamoto, T. and Ohta, K.: Disposable zero-knowledge authentications and their applications to untraceable electronic cash, *Advances in Cryptology CRYPTO'88* (1989).
8) 森畠，阿部，藤崎，中山：電子現金方式，1997 年暗号と情報セキュリティシンポジウム *SCIS97-3C* (1997).
9) 日経デジタルマネー・システム（編）：デジタルマネーのすべて，日経 BP 社 (1997).

(平成 11 年 12 月 2 日受付)
(平成 12 年 6 月 1 日採録)

新保 淳（正会員）
昭和 62 年東京大学大学院工学系研究科電気工学専攻修士課程修了．同年（株）東芝入社．暗号，情報セキュリティ，ネットワークセキュリティの研究・開発に従事．電子情報通信学会会員．平成 7 年電子情報通信学会学術奨励賞受賞．

加藤 岳久（正会員）
平成 3 年信州大学大学院精密工学専攻修士課程修了．同年（株）東芝入社．情報・ネットワークセキュリティの研究・開発に従事．電子情報通信学会会員．

才所　敏明（正会員）

昭和 45 年東京大学工学部計数工学科卒業．同年（株）東芝入社．現在同社情報・社会システム社 SI 技術開発センター参事．暗号・情報セキュリティの研究・開発に従事．ACM, IEEE，人工知能学会，ソフトウエア科学会，応用数理学会各会員．