

電子印紙による手数料支払システム

Commission Payment System Using Electronic Revenue

加藤 岳久 新保 淳 才所 敏明
KATO Takehisa SHIMBO Atsushi SAISHO Toshiaki

インターネットが普及し、企業間取引きや電子商取引(エレクトロニック コマース)が広まりつつある。行政においても、申請・届出などの電子化を推進する動きがある。一つの課題として、申請文書が電子化された場合の申請手数料納付の方法が挙げられている。そこで、当社は電子マネー技術をベースにした手数料支払システムを提案し、システムを試作している。このシステムは、電子紙幣型バリューを利用し、ICカード内で電子印紙の生成を行うことにより、簡便でセキュリティの高いシステムを構成した。また、電子印紙と申請文書とをリンク付けることにより、電子印紙の二重使用を防止することを可能とした。

As the Internet continues to expand, electronic transactions between companies and electronic commerce are spreading. In administrative fields also, electronic processing is being promoted in such areas as applications and notifications.

One issue that has been mentioned has been the payment of commissions when applications are submitted through the communications network. In response, Toshiba has proposed a commission payment system that is based on electronic money technology, and has fabricated such a system as an experiment. This system uses a smart card which stores an electronic bill type value. It was found that this system is easy to use and offers a high level of security when generating electronic revenue within a smart card. Moreover, double use of electronic revenue is prevented by link attachment of the electronic revenue and an application.

1 まえがき

CALS(Commerce At Light Speed)やEDI(Electronic Data Interchange)に見られるように、企業間においてインターネットを利用した取引きや連携が盛んに行われるようになった。

また民間では、SCJ(Smart Commerce Japan)に代表されるように、電子マネーなどの電子決済方式を利用して商品を売買するエレクトロニック コマースが盛んになってきている。

行政においても、1997年7月18日に情報システム各府県連絡会議において「電子化に対応した申請・届出等手続きの見直し指針」が出されている。このなかでは、現在紙ベースで行われている行政機関への申請・届出処理を、まずフロッピーディスク(FD)などの記録媒体を用いたオンラインによる電子化を目指し、将来インターネットなどを利用したオンライン化を目指すとしている。そこでの共通的課題として、印紙に代わる手数料の納付方法も挙げられている。

当社は、現在使用されている印紙による手数料の納付と同様のスキーム(方式)で、申請手数料の支払いが可能な電子印紙を利用した手数料支払システムを提案している。

ここでは、まず代表的な電子決済方式について述べ、申請が電子化された場合の手数料の納付に適用する場合につ

いて検討する。そして、検討結果を基に当社が提案している電子印紙を利用した手数料支払システムについて紹介する。

2 電子決済方式の分類^[1]

現在、多くの電子決済方式が実験、運用されている。ここで、電子決済方式を流通方式と支払い方式に着目し分類する。

2.1 流通方式

(1) オープンループ型 発行された電子的な価値情報が転々と流通する。このため利便性は高いが、発行体による電子的な価値情報の追跡が困難という問題がある。電子マネーのMONDEXやNTTマネーなどが、この方式にあたる。

(2) クローズドループ型 発行体は電子的な価値情報の発行額、利用額を追跡管理可能である。電子マネーのVISA Cash、Geld Kalte、PROTON、e-cashなどが代表的である。現在のクレジットカードやデビットカードも、この分類に入る。

2.2 支払い方式

(1) クレジット型 現行のクレジットカードがベースで後払いである。ネットワーク上での利用を前提に設計されたSET(Secure Electronic Transaction)が、

この方式にあたる。

- (2) プリペイド型 事前に預金口座から現金を支払って、電子的な価値情報を購入するタイプである。電子的な価値情報として電子マネーがある。ICカードに電子的な価値情報を格納して使用するストアドバリューカードなどが、この方式になる。
- (3) デビット型 利用者の口座から、自動的かつ即時に相手の口座に振り替えるタイプである。国内ではJ-Debitがサービスを開始している。
- (4) 小切手型 電子小切手帳をICカードまたはPC内部にもち、代金支払い時に電子小切手を振り出す後払いのタイプである。小切手を発行する金融機関が振り出し、小切手を保証するギャランティチェックを行う。CheckFreeが、このタイプである。

表1に、上記分類と具体的なシステムをまとめます。

表1. 電子決済の分類

Classification of electronic payment schemes

方 式	具 体 例
プリペイド型	VISA Cash
	Geld Karte
	PROTON
	e-cash
クレジットカード型	MONDEX
	NTTマネー
	SET
デビット型	J-Debit
小切手型	CheckFree

3 従来の電子決済を利用した手数料支払い

ここでは、従来の電子決済を利用して申請手数料を支払う場合に考えられる、システム構成と問題点について述べる。

表1に見られるように、現在多くの電子決済方式、電子マネーが提案されている。

現在の印紙を考えると、以下の特徴が考えられる。

- (1) 転々流通の必要性はない
- (2) 匿名性の必要は無い
- (3) 少額決済が中心である

そこで電子申請における手数料支払いでは、プリペイド型で転々流通のないクローズドタイプの電子決済方式が好ましいと判断できる。

図1は、プリペイド型で転々流通のないクローズドループ型の電子決済方式を利用した手数料支払システムの流れを示す。

電子マネーを利用する場合、申請者は金融機関に電子マ

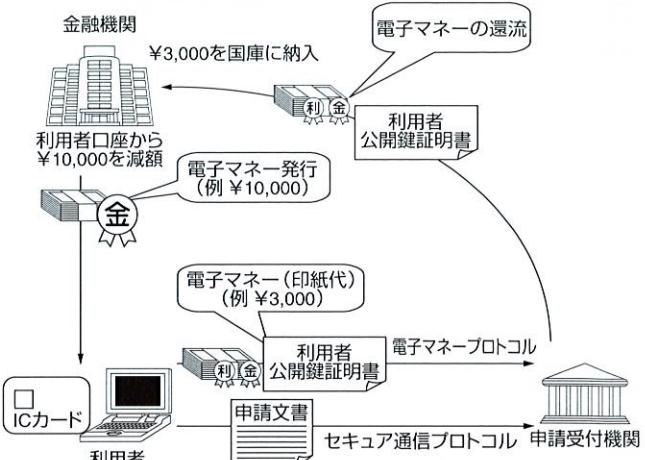


図1. クローズドループ型電子マネーを利用した手数料支払システム 従来の電子決済による手数料の支払いでは、申請に電子マネーと申請文書とで異なるプロトコルが必要となり、さらに電子マネーの還流が生ずる。

Fee payment system using closed-loop type electronic money

ネーの発行を要求する。発行された電子マネーは、利用者が保持する端末に接続されたICカードに格納される。図1の例では、10,000円の電子マネーが発行されている。

申請者は申請文書のテンプレートを、例えばインターネットを経由して手に入れ、必要事項を入力して申請文書を作成する。

完成した申請文書を、申請者はSSL(Secure Socket Layer)やS/MIME(Secure/Multipurpose Internet Mail Extensions)などのセキュア通信プロトコルを利用して申請受付機関へ送信する。

さらに、申請手数料分の電子マネーを申請受付機関へ送信する。電子マネーの送信には、送り手と受け手との間で専用のプロトコルを利用する。この電子マネープロトコルは、申請者と申請受付機関との間でのインタラクションを伴う。このインタラクションは、電子マネーの二重使用を防止するために必須(す)である。図1の例では、申請手数料は3,000円としている。

申請受付機関では、送付された申請文書に必要事項が記入されているかチェックする。また、電子マネープロトコルで送られた電子マネーが申請者から送られてきたものかチェックする。

申請文書のチェックと電子マネーのチェックとが正しいと判定されたならば、送られた電子マネーを金融機関へ還流する。金融機関では電子マネーのチェックの後、手数料が国庫に納入される。図1の例では3,000円が国庫へ納入されている。

このように、従来のクローズドループ型電子マネーを用

いた申請手数料の支払いは可能である。しかし詳細に見ると、以下のようないくつかの問題点がある。

- (1) 手数料支払い時に電子マネープロトコルとセキュア通信プロトコルといった、別々のプロトコルで申請受付機関に送信する必要がある。
- (2) 電子マネーを送信する際に、申請者と申請受付機関との間でインタラクションが生ずる。
- (3) 申請文書と電子マネーとを明確に対応付ける手段が必要となる可能性がある。
- (4) 申請手数料を国庫に納入するためには、申請受付機関に送られた電子マネーを、金融機関に還流する必要がある。

そこで、これらの問題を解決できる専用の方式を設計した。

4 提案する電子印紙を利用した手数料支払システム^{(2),(3)}

4.1 システムの概要

現在の印紙による手数料納付のしくみを、ほぼそのまま電子的に実現するため、以下の要件を考えた。

- (1) 電子印紙が生成されると同時にしくは事前に申請手数料の支払いが完了する。
- (2) 支払われた電子印紙と申請文書とのリンク付けが可能である。
- (3) オフラインによる申請とオンラインによる申請の、どちらにも対応できる。
- (4) 一度生成された電子印紙を、ほかの申請へ二重使用ができない。
- (5) 審査側では送られてきた電子印紙を簡単に検証可能である。

上記要件を考慮し、このシステムではデジタル署名機能を装備し、個別の署名鍵(かぎ)を記憶したICカードを利用することにした。このICカードに充填(てん)した電子的なバリューに対し、手数料相当額を減額した証しとなるデータをICカードが発行する。そして、このデータを電子的な印紙とみなすスキームを開発した。

図2に、このシステムの概略を示す。このシステムは、発行ホスト(発行窓口)、申請者ホスト、検査ホスト(申請受付機関)からなる。このうち、発行ホストは申請者へのICカードの発行、印紙バリューの発行、カード公開鍵証明書の発行を行う。発行ホストは、国または、その代理組織が運営しているものとする。

申請者は、あらかじめ発行ホストがある発行窓口で所定の申請者登録を行うと同時に、予納金額を支払い、印紙バリューを充填したICカードの発行を受ける。このように、印紙バリューの充填時に代金を支払うプリペイド式で運用することで決済処理を簡潔にできる。

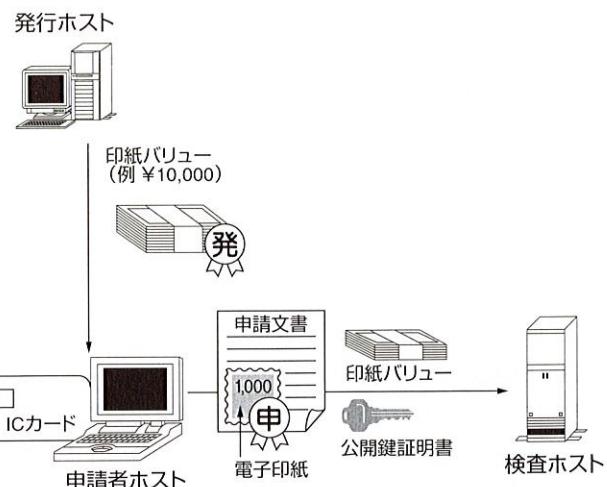


図2. 電子印紙を利用した手数料支払システム 印紙バリューを購入する時点で決済が終了し、オフライン申請にもオンライン申請にも対応できる。

Fee payment system using electronic revenue

発行される印紙バリューは、カードID(IDentification)を織り込んだ発行ホストの署名付きデータである。したがって、ICカードごとに異なる印紙バリューが発行され、あるカード用に発行された印紙バリューは、そのカードでしか利用できない。図2の例では、印紙バリューは10,000円分を発行している。

申請者は、インターネットを経由して申請文書のテンプレートを手に入れ、申請文書に必要事項を入力し、電子印紙を生成する。図2の例では、1,000円の電子印紙を生成している。

この電子印紙は、申請文書を一方向性関数で圧縮したダイジェスト、カードID、申請手数料である使用金額を織り込んだカードの署名付きデータである。申請文書の内容によって個別化されている点がポイントである。

電子印紙が生成されると、ICカード内の残高カウンタが更新され、未使用残高が減額される。図2の例では、残高カウンタが10,000円から9,000円に更新される。

そして申請者は、電子印紙、申請文書データ、印紙バリュー、カード公開鍵証明書を検査ホストへ送信する。

検査ホストでは、申請者の公開鍵証明書、電子印紙の署名を検証し、申請手数料が支払われたことを検査する。

またこのシステムでは、再充填時にはICカードを発行ホストに持参することで、ICカードに残った未使用残高を加算した印紙バリューの再充填を可能としている。

4.2 システムの特長

以下に、提案システムの特長を述べる。

- (1) 申請者ホストとICカードの間で電子印紙が生成され、申請者と申請受付機関との間ではインタラクション

ンが生じない。

- (2) 電子印紙、申請文書データ、印紙バリュー、カード公開鍵証明書といったデータを検査ホストへ送ればよい。このため、ネットワーク上のオンライン申請も、FDといった記録媒体を利用したオンライン申請にも適用できる。
- (3) 印紙バリュー購入時に決済を済ませることで、検査ホストは電子印紙の検査をするだけでも、印紙バリューや電子印紙の還流が生じない。

4.3 システムのセキュリティ

以下に挙げる観点で、セキュリティ対策を施している。

- (1) 印紙バリューの偽造 発行ホストのデジタル署名を施すことにより偽造が困難である。
- (2) 電子印紙の偽造 偽造のためにはICカードの署名が必要であり、秘密鍵はICカードの耐タンパ性^(注1)により保護している。
- (3) 電子印紙のコピー使用 申請文書のダイジェストを盛り込むことによりコピーによる二重使用は不可能である。
- (4) ICカード内未使用残高の改変 カードの耐タンパ性により残高の改変は困難である。

5 あとがき

電子マネーをベースとして、現在の申請手数料支払いのスキームを変えずに、簡便なプロトコルで申請手数料支払いが可能なシステムを実現した。

印紙バリューの充填をネットワーク経由で処理する仕組

(注1) 内部情報(例えば、ICメモリ)の読み書きを阻止し、かつ外部から不正操作を行なっても、内部処理の誤動作を困難にするしくみ。

みを追加することも可能である。また、ICカードの耐タンパ性が破られ、不正が行われた場合を検知するしくみの追加も可能である。

謝 辞

このシステムは、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事業”的一環として、財ニュースメディア開発協会の委託を受け、当社が開発したものである。

関係各位のご支援に感謝する。

文 献

- (1) 次世代カード社会へのQ&A. CardWave. 109, 12, 1996, p.8-22.
- (2) 新保 淳、他。“電子印紙システムの設計と試作”。1999年暗号と情報セキュリティシンポジウム予稿集、1999, p.389-394
- (3) 加藤岳久、他。“ICカードを利用した電子印紙システム”。第58回情報処理学会全国大会講演論文集(1)、1999, p.331-332

加藤 岳久 KATO Takehisa

情報・社会システム社 SI技術開発センター主務。
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、情報処理学会会員。
System Integration Technology Center

新保 淳 SHIMBO Atsushi

研究開発センター コンピュータ・ネットワークラボラトリー研究主務。暗号技術・応用システムの研究・開発に従事。電子情報通信学会、情報処理学会会員。
Computer & Network Systems Lab.

才所 敏明 SAISHO Toshiaki

情報・社会システム社 SI技術開発センター 戦略企画担当
参事。暗号・情報セキュリティの研究・開発に従事。
情報処理学会、CSI、ACM、IEEE各会員。
System Integration Technology Center

