ICカードを利用した電子印紙システム

1L－8

加藤 岳久†, 新保 淳††, 才所 敏明†
†(株)東芝 SI技術開発センター, ††(株)東芝 研究開発センター

1. まえがき

近年，ネットワークを活用した企業間の取引や連携・協力が進展しつつある．行政側においても，申請・届出等の電子化を業務内容に即して推進すること等の取組みが推進されている．現在官公庁では，申請手数料が必要な場合，その支払いに主に印紙を利用している．従って，申請・届出等を電子化し申請手続きをインターネットを経由して提出する場合には，手数料納付の電子的手段が必要となる．

そうした場面を想定し，本稿では，プリペイド型バリューを充填したICカードを利用し申請手数料の支払いを証明するスキームを提案し，試作したシステムを紹介する．

2. 提案システム

本稿では，現在の印紙による手数料納付の仕組みを，ほぼそのまま電子的に実現することが好ましいと考え，以下の要件を挙げる．

- 申請する申請文書と電子印紙とをリンクでき同時に送信可能
- 電子印紙は対象となる申請文書に対応し，他の申請への二重使用が不可能
- 電子印紙が生成されると同時もしくは事前に申請手数料の支払いが完了
- 審査側は送られてきた電子印紙を簡単に検証可能

上記要件を考慮し本システムでは，ディジタル署名機能を装備したICカードを利用する．このICカードに充填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カードが発行し，これを電子的な印紙とみなすスキームを開発した．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出来る．図1に本システムの概略を示す．

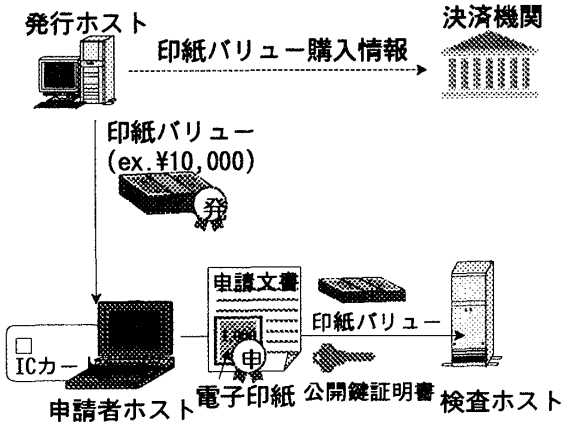

図1.提案システムの概略図

本システムは，電子印紙を発行するICカード，ICカードを装着し申請者とのインタフェースを司る「申請者ホスト」，ICカードが生成した電子印紙の正当性を検査する「検査ホスト」，ICカードを発行する「発行ホスト」，決済ネットワークに接続され決済を実施する「決済機関」から構成される．

試作システムでは，ICカードを発行時に，申請者は氏名，住所などの申請者情報と印紙バリューの購入金額を含む登録申請書と購入金額を所定の窓口に提出することを想定している．窓口では登記簿謄本または運転免許証などの証書を確認した上で申請書を受理する．後日，ICカードが郵送されるものとする．

3. プロトコル

本システムの主なプロトコルとして，印紙バリューの充填，電子印紙の生成，印紙バリューの少額残高処理の3つがある．

発行されたICカードには，カードID(CID)，申請者が申請した購入額に相当する印紙バリュー(value)，ICカードのRSA秘密鍵，ICカードの公開鍵証明書(card_cert)，発行ホスト公開鍵などが書き込まれる．ICカードで，印紙バリューの未使用額も管理される．

- 印紙バリューの充填

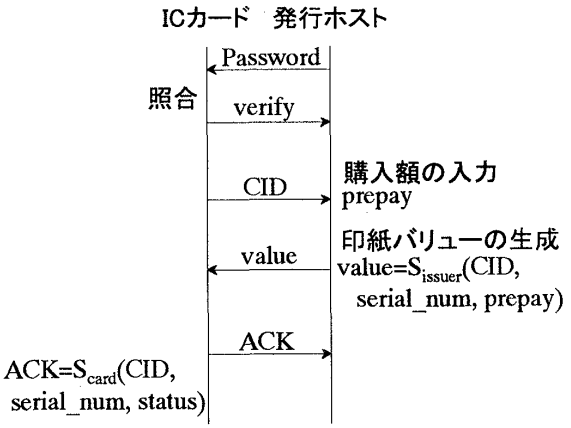

図2.印紙購入のプロトコル

① 申請者はICカード発行申請時に印紙バリュー購入金額(prepay)を指定する．

② カード発行ホストは，ICカードからカードIDを読み出し，印紙バリューを生成してICカードへ送信する．印紙バリューは発行ホストが生成した署名データであり，下記フォーマットである．

$$value=S_{Issuer}(\ CID,\ serial\_num,\ prepay\ )$$

Electoronic Revenue Stamp System Using IC Cards
Takehisa Kato†, Atsushi Shimbo††, Toshiaki Saisho†
††TOSHIBA Co. Security Technology Center, ††TOSHIBA Co. R&D Center
†3-22 Katamachi,Fuchu,Tokyo 183-8512, ††1 Komukai-Toshiba,Saiwai,Kawasaki,kanagawa,Tokyo,210-0901

ここで，$S_X(Y)$はXの秘密鍵を用いたYに対するディジタル署名を表す．serial_num は印紙バリュー通し番号，prepay はバリュー購入金額である．印紙バリューを受信したカードは，その正当性を確認し未使用残高を購入金額分だけ増加する．そして，カードが署名したACKを発行ホストに送信し，購入手続き完了を通知する．

$$ACK=S_{card}(CID, serial\_num, status)$$

status は状態コードで，正常終了／異常原因などを表す．

- 電子印紙の生成

電子印紙の生成は，ICカードを装着した申請者ホストで実行される．

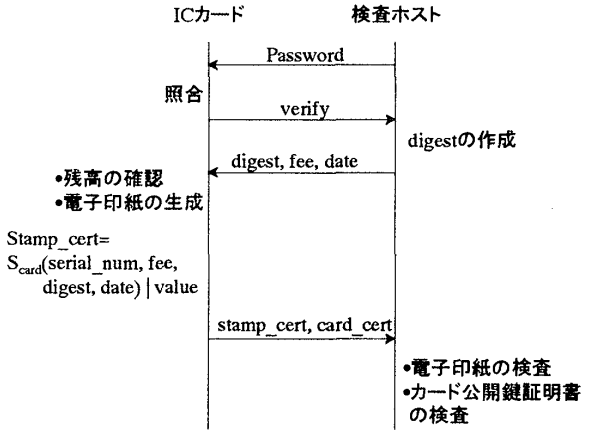

図3.電子印紙の生成と使用

① 従来の印紙貼り付け文書に相当する対象文書データと，必要な申請手数料(fee)を入力する．

② 選択された対象文書データをハッシュ関数で圧縮したダイジェスト(digest)を作成し，申請手数料と日付(date)と共にICカードへ送る．

③ ICカードは未使用残高を検査し，要求された手数料未満の残高しかない場合には，不足金額を含むメッセージを返す．

④ IC カード内の未使用残高が要求された手数料以上の場合には，電子印紙(Stamp_cert)を作成する．電子印紙のフォーマットは下記である．

$$Stamp\_cert = S_{Card}(\ serial\_num,\ fee,\ digest,\ date\ ) \mid value$$

IC カードは，電子印紙と公開鍵証明書とを申請者ホストに送り，未使用残高を手数料分だけ減額する．

- 印紙バリューの少額残高処理

IC カード内の未使用残高が少なくなっても，半端な未使用額が使われずに残らない様にした．即ち，申請者はカード内の残高が手数料に満たない場合，カード発行機関へカードを持参し，新たな印紙バリューの購入を行う．この時，カード内残高を加えた印紙バリューが発行されるようにしている．

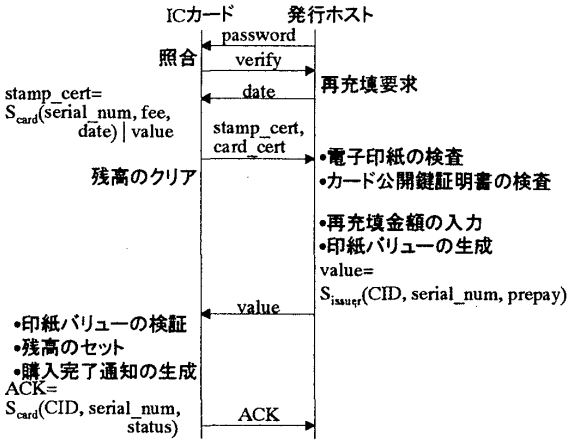

図4.印紙バリューの再充填

① 発行ホストより再充填要求を出す．

② カードは，残った未使用印紙バリューの電子印紙を発行する．

③ 発行ホストは，新規購入金額に未使用額を合算した額面の印紙バリューを生成しICカードへ送る．

④ IC カードは受け取った印紙バリューの正当性を確認し，ACK を発行ホストへ返す．

4. リスクと対策

本システムでは，下記リスクに対して対策を施している．

- 印紙バリュー，電子印紙の偽造
  カードまたは発行ホストのディジタル署名を施すことにより偽造が困難
- 印紙バリューのコピー使用
  電子印紙の生成にはカード内の秘密鍵が必要で，秘密鍵はカードの耐タンパー性により保護
- 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
- カード内の未使用残高の改変
  カードの耐タンパー性により残高の改変が困難

5. あとがき

以上，申請・届出等をネットワークを利用して行うICカードを利用した電子印紙システムを紹介した．

謝辞

本発表は，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」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ものである．

関係各位のご支援に感謝する．

参考文献

[1] "デジタルマネーのすべて"，日経デジタルマネーシステム編，日経BP社