電子権利流通基盤のための汎用的な原本性保証方式

寺田雅之[†] 花舘蔵之[†]
藤村考[†] 関根純[††]

本論文では，証券やチケットなどの紙片を用いて表象されている様々な権利を電子化し，電子的な権利として流通させるための原本性保証方式である FlexToken を提案する．本方式では，電子的な権利を，権利内容を定義する権利定義と原本性を表象するトークンの 2 つの情報に分離し，後者の複製のみを耐タンパ装置を用いて防止することにより，任意の大きさや形式を持つ権利の原本性を IC カードなどの限られた容量の耐タンパ装置を用いて保証することを可能にする．さらに，それぞれの権利発行者が信頼する耐タンパ装置の条件を定義する「信任情報」を用いて流通時の認証を行うことにより，任意の発行者による権利を安全に流通可能にすることを特長とする．

Copy Prevention Scheme for Rights Trading Infrastructure

Masayuki Terada,[†] Masayuki Hanadate,[†] Ko Fujimura[†]
and Jun Sekine[††]

This paper proposes FlexToken, a new copy prevention scheme for electronic rights such as tickets or coupons, which are circulated as pieces of paper in the real world. The important feature of this scheme is that electronic rights are represented using two separate types of information: the definition and the token of the rights. The token represents the “genuineness” of the rights and distinguishes the genuine electronic rights from copies. A token is stored and circulated using tamper-proof devices such as smartcards while the definitions can be held in any storage medium. This approach decreases the amount of memory required of the tamper-proof devices. Furthermore, circulating the identity of the right issuer and accredited information, which specifies the tamper-proof devices trusted by the issuer, along with a token makes it possible to protect any type of electronic right, regardless of the issuer.

1. はじめに

現在，権利は主に紙媒体を介して，たとえば証券やチケットなどの形をとって流通される．これらの権利を印刷された紙ではなく電子情報として流通させることにより，Internet を介したチケットの購入や，発行および改札コストの低減などを可能にし，利便性を向上させる試みが提案されている[1),2)]．

これらの試みを実現するためには，権利を表象する電子情報（電子権利）が本物かどうかを判別する手段，すなわち電子権利の原本性を保証する手段が必要となる．

本論文では，このような電子権利の原本性を保証する方式である FlexToken を提案する．本提案方式は，実世界におけるチケットなどと同様に，それぞれの権利所有者が電子権利を保持するアーキテクチャを採る．また，複製の防止などの不正を防止するために，権利所有者は IC カードなどの耐タンパ装置を用いて電子権利を保持する．

ただし，それぞれの電子権利は互いに異なる様々な権利の内容（たとえばコンサートチケットなら，名称，会場座席の種別など）や行使の条件（有効期限や年齢制限など）を持つため，記憶容量や入出力性能に制限がある IC カードに電子権利をそのまま格納することは実用的ではない．また，電子権利は（電子現金などとは異なり）企業や団体，個人などの様々な発行者により発行されうるため，Mondex[3)] などの電子現金システムのように，IC カードが発行者の認証情報をあらかじめ保持しておくことは困難である．

本方式は，以下のような手法を採ることによりこれらの問題を解決している．

まず，IC カードの記憶容量の制限の中で様々な内容や形式を持つ電子権利の流通を可能とするために，それぞれの電子権利を，権利の内容や条件を定義する情

† NTT 情報流通プラットフォーム研究所
NTT Information Sharing Platform Laboratories
†† NTT 情報流通基盤総合研究所
NTT Information Sharing Laboratory Group

報（権利定義）と原本性を表象する情報（トークン）の 2 種類の情報に分離して構成する．ここで，権利定義は通常の電子情報と同様に格納および転送され，トークンのみが IC カードに保護されて移送される．これにより，耐タンパ装置に必要となる性能や容量を小さく抑えつつ，多用な権利を統一的に扱うことを可能としている．

また，様々な発行者により発行された電子権利を安全に流通させるために，それぞれのトークンに発行者の鍵に対応する情報を持たせるとともに，発行者が信用する IC カードの条件を発行者ごとに規定する手段（信任情報）を提供している．これらの情報を用いて流通時の認証を行うことにより，それぞれの IC カードが個々の発行者ごとに認証情報をあらかじめ保持する必要がなくなり，様々な発行者による権利を単一の IC カードで扱うことを可能としている．

以下，2 章では，本論文が扱う対象とする権利の性質とその流通モデルについて述べるとともに，これらの権利を電子的に流通させるための要求条件と，従来技術を適用する際の問題点について示す．3 章では，本論文の提案方式において電子権利を流通させるために用いる情報の構成と，それぞれの流通処理の実行手順を示し，4 章において，多様性への対応，安全性の確保，実用性の確保のそれぞれの要件に対する充足性について考察する．最後に，5 章において，関連技術との比較を行う．

2. 電 子 権 利

本章では，本論文が扱う対象とする権利の性質とその流通モデルについて述べ，これらの権利を電子的に流通させるための要求条件と，従来技術を適用する際の問題点について示す．

2.1 対象とする権利

本論文では，一般に「権利」と呼ばれるもののうち，主として流通性を持ち，行使によってサービスや物品などの対価を得られる性質を持つもの☆を対象にする．これらの権利は，しばしば紙片により表象され，紙片の保持者が権利の所有者であるとされる．たとえば，商品券，証券，定期券，入場券などがこれに相当する．

それぞれの権利には，その価値を裏付ける者，すなわち行使によって得られる対価を保証する者☆☆が存在する．この価値の保証者を発行者と呼び，発行者が他者に権利を付与する行為を発行と呼ぶものとする．

☆ これらの性質を持つ権利は，法学上の分類[4] では私権のうち請求権（債権）に属する場合が多い．

☆☆ 請求権における債務者に相当する．

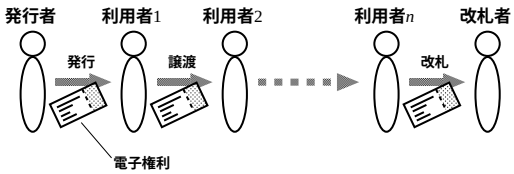

図 1 権利のライフサイクル
Fig. 1 Lifecycle of rights.

ここで，権利の発行を受けることにより，権利を所有しうる者を利用者と呼ぶものとする．利用者は，発行者から権利を発行されるか，他の利用者から権利を譲り受けることによって権利の所有者となる．後者の利用者間における権利の受け渡しを譲渡と呼ぶ．権利の譲渡にともない，譲渡側が所有する権利は消滅する．権利の譲渡は，贈与，委託販売，古物商（いわゆる金券ショップ）による再販などの際に行われる．

また，利用者からの権利の行使を受け，権利に応じた対価を提供☆☆☆する者を改札者と呼ぶものとする．当該する権利の発行者自身が改札者として対価を提供することもあるが，通常は発行者となんらかの契約を結んだ別の者が改札者として対価を提供する（たとえば，映画の前売券における配給会社と映画館など）場合が多い．行使には，行使された権利が消滅する場合（消費と呼ぶ）と，権利は消滅せずに利用者が権利を所有していることの確認だけがなされる場合（提示と呼ぶ）がある．後者は，たとえば定期券の行使などに相当する．

2.2 電子権利流通モデル

本論文では，（紙片の代わりに）前節で示したような権利を表象する電子情報を電子権利として定義する．前節の議論によれば，これらの電子権利が流通する過程は，発行者，利用者，改札者の 3 種の参加者間における発行，譲渡，行使の 3 種の流通処理としてモデル化することができる（**図 1**）．この権利流通モデルにおけるそれぞれの参加者と流通処理の役割を以下に示す．

発行者 利用者への発行処理によって電子権利を生成し，生成された電子権利の価値を保証する．

利用者 電子権利を保持することにより，権利の所有者となる．電子権利を保持する利用者（権利の所有者）は，譲渡処理により権利を他の利用者に譲渡することや，または行使処理により改札者に対して権利を行使することができる．

改札者 利用者からの行使処理に応じて電子権利を回収もしくは検証し，（発行者に代わって）利用者に

☆☆☆ 請求権における債務の履行に相当する．

対して権利の内容に応じた対価を提供する．

発行処理 発行者と利用者との間で行われる，電子権利の生成過程．発行処理により生成された電子権利は，利用者に所属する．

譲渡処理 利用者間での電子権利の移送過程．譲渡処理により，移送元の利用者が保持する電子権利は消滅し，移送先で再生成される．

行使処理 利用者と改札者との間で行われる，電子権利の回収もしくは検証過程．前者を消費処理とし，後者を提示処理とする．消費処理の際は利用者が保持する電子権利は消滅するが，提示処理の際は単に電子権利の存在を検証するのみであり，電子権利の状態に変化は生じない．前述のように，行使処理の際には利用者に対して電子権利の内容に応じた対価が提供される．

2.3 要求条件

前節で述べた電子権利の流通を可能にするためには，流通に際して電子権利の原本性を保証する手段が必要となる．

すなわち，従来のように紙片（券片）を用いて権利を表象する場合には，紙片の複製や偽造，改竄などが事実上困難である☆ことから，その紙片が「本物」であること（紙片の原本性）が保証されてきた．その一方，電子情報はこれらの紙片と異なり複製や改竄が容易であるため，単に従来は紙に印刷されていた情報を電子情報に置きかえるだけではなく，それらの電子情報の原本性を保証し，複製や偽造などの不正から保護するための手段が必要になる．

ここで，この原本性保証方式には，(1) 様々な電子権利の原本性が保証できること，(2) 偽造や改竄などの不正を防止できること，(3) オフラインでの利用を可能にするなど利便性を保ち，かつ実用的なコストで実現可能なこと，などの要件が求められる．これらの要件について詳細を以下に示す．

- 多様性への対応
  - **権利の多様性** 商品券や証券，入場券など，様々な種類や内容の権利を扱えること．
  - **発行者の多様性** 電子現金のように特定の発行者（銀行など）が発行する通貨だけを扱うのではなく，様々な発行者による権利を扱えること．
- 安全性の確保
  - **改竄防止** 流通過程において権利の内容が改竄されることを防止できること．
  - **偽造防止** 権利の偽造を防止できること．すなわち，他人の名を騙って権利を発行することが防げること．
  - **複製防止** 流通過程における権利の複製を防止できること．
  - **公平性の確保** 流通相手の不正により，権利の移送の事実が否認されることを防止できること．たとえば，すでに権利の移送が終了したにもかかわらず「まだ受け取っていない」と主張されることなどを防げること．
  - **プライバシーの確保** プライバシーの侵害を防ぐために，ある権利を保持していること，もしくは過去に保持していたことは秘匿可能であること．
- 実用性の確保
  - **オフライン性** 必ずしも権利の行使や譲渡がネットワーク上で行われるとは限らないため，ネットワークを利用できない環境でも権利の流通が可能であること．
  - **スケイラビリティ** 扱える権利の数に制約が生じないこと．たとえば，負荷が集中するようなサーバを前提にしないことが望ましい．
  - **コスト効率** 発行や利用のためのコストが十分に低いこと．また，高価なデバイスに依存しないこと．

2.4 従来技術

以上にあげた電子権利の要件は，特に安全性の確保に関して電子証明書や電子現金に求められる要件と類似している．本節では，それらの手法を適用して電子権利を実現する方式について，その適用可能性と問題点について議論する．

まず，電子証明書の適用について議論する．ここで電子証明書とは，電子署名が付与された電子情報のことを指すものとする．電子証明書を電子権利に適用する場合，電子署名の署名者が発行者，署名対象となる電子情報が権利の内容をそれぞれ表すことになる．ここで，電子署名については（公開鍵暗号系における秘密鍵を持つ）任意の者により付与することができ，電子情報についても任意の情報を記述することが可能であるため，電子証明書による電子権利は多様性への対応の条件を充足する．また，電子署名により改竄や偽造からも保護されている．

電子証明書自身は複製を防止する手段を持たないため，電子証明書を電子権利としてそのまま利用することはできない．ただし，PKIX[5] における属性証明書

☆ ただし，近年では複製技術の向上によりこの仮定が崩れつつあることが問題になっている．

のように，証明書の被発行者に対応する情報☆を権利の所有者として電子証明書に含めることにより，他者による複製の利用を防止することが可能になる．しかしながら，この場合は所有者が被発行者に固定されることになるため権利を譲渡することができず，譲渡を必要としない電子権利に適用が限定される．

また，SPKI[6] における権限証明書では，証明書の被発行者がさらに（元の証明書と関連づけられた）証明書を発行することにより，権限を委譲することを可能にしている．しかしながら，SPKI における権限の委譲は，委譲元にも権限が残る（権限が委譲先に複製されてしまう）という点で権利の譲渡とは性質が異なるため，これを電子権利の譲渡手段として用いることは困難である．

次に，電子現金システムの適用について議論する．電子現金の実現方式は，大別すると口座型，履歴検証型，バランス型の 3 種の方式に分類できる☆☆．これらのうち，口座型の方式はそれぞれの利用者が保持する額面をサーバ上の「口座」で集中的にする方式であり，流通の際に必ずサーバ上の口座を更新する必要があるため，オフライン性に関する要件を満たすことができない．また，履歴検証型の方式は還流時に流通履歴を検証することによって二重使用を事後検出する方式であり，複製を事前に防止する手段を持たないため，複製防止の要件を満たすことができない．したがって，これらの方式を電子権利に適用することは困難であるか，もしくは限定された用途の権利にしか適用できない．

バランス型のシステムは，IC カードを（現金の）額面の管理や移送に用いることにより，ネットワーク上のサーバへアクセスすることなく流通過程における不正な権利の複製を事前に防止することを可能にしている．このようなバランス型の電子現金システムとしては，Mondex[3),7)] などがあげられる．

ここで，IC カードによる管理の対象を額面ではなく電子権利を表す情報とし，この情報を IC カードで保護しつつ移送することにより，これらのシステムを電子権利の原本性を保証する手段として用いることが可能となる（**図 2**）．

しかしながら，この手法による電子権利の実現には以下のような問題がある．

まず，現在の IC カードの記憶容量（数 KB〜数十 KB）や入出力性能（9,600 bps）は，様々な内容や条件を持つ電子権利の情報量に対して不十分である．そのため，1 枚の IC カードで扱える電子権利の数は限られたものとなり，また，流通時における IC カード間の電子権利のやりとりに時間がかかることになる．

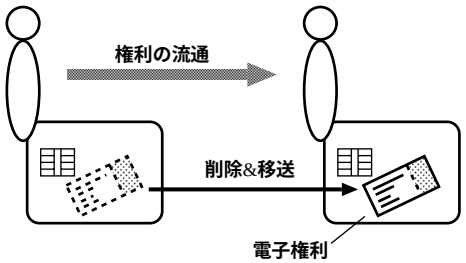

図 2 IC カードに封入された電子権利の移送
Fig. 2 Transfer of an electronic right stored in a smartcard.

また，バランス型の電子現金システムは，（中央銀行などの）限られた発行者により発行された通貨のみを扱うことを前提にしており，発行者の認証情報をそれぞれの IC カードに固定的に保持させているため，あらかじめ定められた特定の発行者しか電子権利の発行を行うことができない．そのため，それぞれの発行者は独自に IC カードの発行や管理を行う必要があり，また，利用者は発行者ごとに IC カードを用意する必要がある．

これらの問題は，利用者の利便性を損なうとともに，発行者の新規参入コストや維持運用コストの増加要因となるため，電子権利を普及させるうえでの障害となる．

2.5 提案方式

本論文では，前節で述べたバランス型の電子現金方式における問題を解決し，様々な発行者による様々な種類の電子権利を流通可能とする，電子権利の原本性保証方式 FlexToken を提案する．

本方式では，多様な種類の電子権利を効率良く扱うことを可能にするために，電子権利を権利定義とトークンの 2 つの情報に分割し（**図 3**），トークンのみを IC カードなどの耐タンパ装置を用いて管理する．権利定義は，権利の内容や行使の条件について定義した情報であり，（ハードディスクなどの）通常の格納媒体に格納される．一方，トークンは電子権利の原本性を表象する情報であり，IC カードの耐タンパ性を用いて不正な複製などから保護される．トークンは，権利定義のハッシュ値であるマニフェストと，発行者の公開鍵のハッシュ値である発行者情報の 2 つの情報の組として構成され（**図 4**），そのデータ量は IC カードの記憶容量や I/O 性能に対して十分小さい（ハッシュ関数

☆ より正確には，被発行者の公開鍵を特定する情報．
☆☆ 詳細については 5 章で議論する．

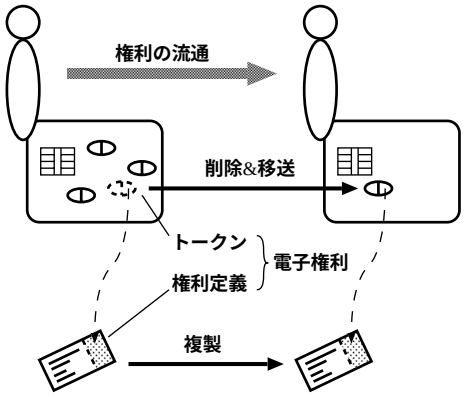

図 3 電子権利の分離
Fig. 3 Separation of an electronic right.

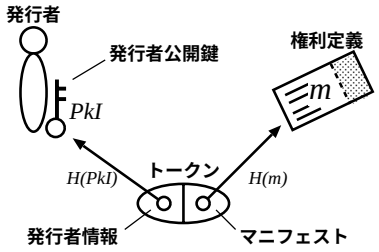

図 4 トークンの構成
Fig. 4 Structure of a token.

に SHA-1 を用いた場合で 40 byte）．電子権利は，権利定義が対応するトークンと照合できたとき，すなわち電子権利の原本性が確認されたときにのみ有効と見なされる．

電子権利の流通は，権利定義の複製とトークンの移送により行われる．流通にともなう改竄や複製を防ぐため，トークンの移送時には，電子署名を用いてトークンの認証がなされる．ここで，任意の発行者による電子権利を安全に流通させることを可能にするために，それぞれの発行者が信用する IC カード発行機関を指定する情報である信任情報と，IC カード発行機関が IC カードの耐タンパ性を保証する情報である耐タンパ証明とを用いて電子署名の検証を行う．信任情報には複数の IC カード発行機関を指定することができ，それぞれの発行者は任意の IC カード発行機関を信任情報に記述することができる．この検証方式により，トークンの流通はそれぞれの発行者が信用できる IC カードのみを介して行われることが保証される．本方式における流通プロトコルの詳細については 3 章で述べる．

3. 電子権利流通プロトコル

2 章において，電子権利が流通する過程は，発行者，利用者，改札者の 3 種の参加者間における発行，譲渡，行使の 3 種の流通処理としてモデル化することができるとした．本章では，これらの流通過程の実現に用いる情報の構成と，それぞれの流通処理の実行手順を示す．

3.1 情 報 構 成

以下において，2 章で示したそれぞれの参加者 X は，RSA [8] などの公開鍵暗号系における鍵ペア，すなわち公開鍵 PkX と秘密鍵 SkX を保持することを前提とする．ただし，利用者の秘密鍵は利用者の IC カードによって保持され，（利用者本人も含め）外部から直接に操作・参照できないものとする．一方，発行者と改札者の秘密鍵は HDD などの通常の記憶媒体に格納してもよいが，保持者本人以外からは秘匿されているものとする．

本方式では，秘密鍵 SkX は電子署名を生成するために用いられる．以下において，メッセージ m に対する SkX による電子署名を $S_{PkX}(m)$ と表記する☆．電子署名 $S_{PkX}(m)$ は，対応する公開鍵 PkX を用いた検証関数 $V_{PkX}(\cdot,\cdot)$ を用いて検証可能である．この検証関数は，以下の値をとる．

$$V_{PkX}(m,s) = \begin{cases} \text{true} & (s = S_{PkX}(m)) \\ \text{false} & (s \neq S_{PkX}(m)) \end{cases}$$

また，$H(\cdot)$ は，SHA-1 [9] などの一方向ハッシュ関数である．SPKI などと同様に，この関数による公開鍵のハッシュ値 $H(PkX)$ をそれぞれの参加者 X の識別子として用いる．この $H(PkX)$ を以後フィンガープリントと呼ぶこととする．

本方式による流通過程の実現に用いる情報の構成を以下に示す．

権利定義 行使により得られる対価や，その行使の条件などの権利の「中身」を定義する情報である．本方式では，任意の形式で権利定義を記述することが可能であり，たとえば XML Ticket [10),11)] や XML Voucher [12)] などを権利定義の記述言語として用いることができる．以降において，権利定義を m と表記する．

トークン 権利の原本性を表象する情報であり，2 つ組 $(t_1, t_2) = (H(m), H(PkI))$ として構成される．ここで，PkI は権利発行者の公開鍵である．

☆ そのため，以降では秘密鍵 SkX は陽に表記されることはない．

利用者が，発行者に信任された（後述）IC カード内にトークン $(H(m), H(PkI))$ を保有しているとき，その利用者は I によって価値が保証され，権利定義 m により内容が定義された権利を所有しているものとする．

トークン交換形式 権利流通にともないトークンを移送する際に用いられる 6 つ組 $(e_1, \ldots, e_6)$ であり，トークンとチャレンジ（後述）の組に対して送り側の署名を付与することによって構成される．以降において，トークン交換形式を TEF（Token Exchange Format）と略記する．TEF の詳細は次節で述べる．

チャレンジ TEF の再利用による権利の複製を防ぐために，トークン流通時にトークンの受領者によって生成される 2 つ組 (c_1, c_2) である．ここで，c_1 は受領者のフィンガープリントであり，c_2 は受領者がそれぞれ一意に生成するセッション番号である．セッション番号としては，たとえば十分な長さを持つ乱数や，1 回の流通ごとに単調に増加する連番などを用いることができる．

耐タンパ証明 IC カードの耐タンパ性を第三者（保証人☆）が保証した証明書であり，2 つ組 (g_1, g_2) として構成される．ここで耐タンパ性を持つとは，(1) 保有するトークンおよび有効セッション集合（後述）に対する（本方式で定められた流通手順以外による）不正な追加や改竄を防止できること，(2) 保持する秘密鍵に対する（利用者本人を含めた）外部からの操作や参照を防止できること，の両者が充足可能であることを指す．g_1 は IC カードの公開鍵に対する保証人による電子署名であり，g_2 は保証人の公開鍵である．それぞれの IC カードは，あらかじめ適切な耐タンパ証明を保持しているものとする．

信任情報 発行者が「信用」できる保証人を指定するために用いられる 3 つ組 (a_1, a_2, a_3) である．a_1 は保証人のフィンガープリントの集合であり，それぞれの IC カードは，その耐タンパ証明の保証人が a_1 に含まれる場合に，発行者から信任されていると見なされる．a_1 は，発行者による a_1 に対する電子署名 a_2 と発行者の公開鍵 a_3 によって偽造や改竄から保護される．

受領証 TEF を受理したことを示すために，トークンの受領者によって生成される 2 つ組 (r_1, r_2) である．それぞれ，r_1 は（受理した TEF の）チャレンジに対する受領者の電子署名，r_2 は受領者の公開鍵である．

これらの情報のほかに，それぞれの利用者と改札者は有効セッション集合 S と発行者リスト L を管理する．

有効セッション集合 S は，有効なチャレンジを識別するためのセッション番号の集合である．有効セッション集合 S の初期状態は空集合であり，それぞれのセッション番号はチャレンジの生成時に S に追加され，対応する TEF の受理時に S から削除される．ここで，利用者に属する S は IC カードにより管理され，利用者が（チャレンジ生成以外の手段により）不正に S に値を追加することは許さないものとする．

発行者リスト L はそれぞれの利用者や改札者が信用する発行者のリストであり，発行者のフィンガープリントの集合として構成される．発行者リスト L に含まれる発行者によって裏付けられた権利のみが，それぞれの利用者や改札者にとって「価値がある」権利であると見なされることになる．L は，それぞれの利用者や改札者により任意の時点で更新可能である．

3.2 流通手順

以下において，上記の情報を用いた権利の発行処理，譲渡処理，行使処理の実行手順についてそれぞれ説明する．なお，以下の説明において，$A \to B : X$ とは送信者 A から受信者 B に情報 X を送信することを意味する．

3.2.1 発行処理

発行とは，権利定義 m と発行者 I に対応するトークン $(H(m), H(PkI))$ を生成し，発行者 I から利用者☆☆ U に移送する処理である．発行者 I から利用者 U への電子権利の発行は以下の手順で行われる（**図 5**）．

(1) 発行者 I は，信任情報 $A_I : (a_1, a_2, a_3)$ を生成する．ここで，A_I は次のように構成される：

$$a_1 := \{H(PkG_1), ..., H(PkG_n)\}$$
$$a_2 := S_{PkI}(H(PkG_1)||...||H(PkGn))$$
$$a_3 := PkI$$

信任情報 A_I は発行時の検証には用いられないが，以降の譲渡や行使の際に用いられる．

(2) 発行者 I は，権利定義 m とともに A_I を利用者 U に送信する $(I \to U : \{m, A_I\})$．

(3) U はチャレンジ $C_U : (c_1, c_2) := (H(PkU), s)$ を生成する．ここで，s は U により生成されるセッション番号である．チャレンジ生成後，s

☆ 典型的には，IC カードの発行機関などが保証人の役割をすることになると考えられる．

☆☆ より正確には，利用者が所有する IC カード．

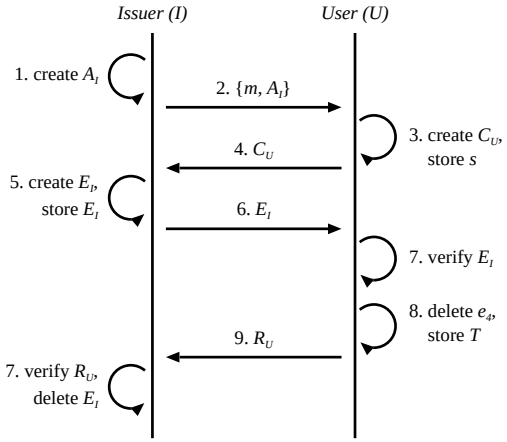

図 5 発行プロトコル
Fig. 5 Issuing an electronic right.

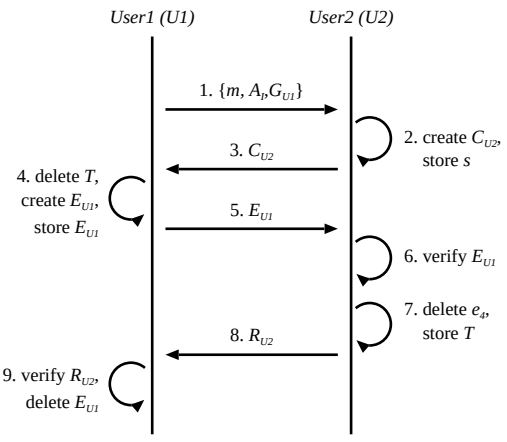

図 6 譲渡プロトコル
Fig. 6 Transferring an electronic right.

は有効セッション集合 S_U に追加される．

(4) U はチャレンジ C_U を I に送信する $(U \to I : C_U)$.

(5) I は TEF $E_I : (e_1, ..., e_6)$ を生成する．TEF は次のように構成される：

$$e_1 := H(m)$$
$$e_2 := H(PkI)$$
$$e_3 := c_1$$
$$e_4 := c_2$$
$$e_5 := S_{PkI}(e_1||e_2||e_3||e_4)$$
$$e_6 := PkI$$

I は，なんらかの異常によってプロトコルが中断されたときのために，E_I の複製を保存しておく．この複製は，対応する受領証を発行者が受信するまでの間保持される．

(6) I は TEF E_I を U に送信する $(I \to U : E_I)$.

(7) U は E_I を検証する．この検証は，次の式がすべて満たされる場合に成功する：

$$e_3 = H(PkU) \quad (1)$$
$$e_4 \in S_U \quad (2)$$
$$V_{e6}(e_1||e_2||e_3||e_4, e_5) = \text{true} \quad (3)$$
$$H(e_6) = e_2 \quad (4)$$
$$e_2 \in L \quad (5)$$

式 (1)，(2) はチャレンジの正当性の検証であり，式 (3) は E_I が I によって生成されたものであるかどうかの検証である．式 (4) は，I が正しく「自分を発行者とする」権利を発行しているか，すなわち他人の権利を偽造していないかどうかの検証である．また，式 (5) は，権利の有効性の検証である．

(8) 上記の検証に成功した場合，U は S_U から e_4 を削除し，トークン $T : (t_1, t_2) := (e_1, e_2)$ を格納する．

(9) U は受領証 $R_U : (r_1, r_2) := (S_{PkU}(c_1||c_2), PkU)$ を I に送信する $(U \to I : R_U)$.

(10) I は R_U を検証する．この検証は，次の式がすべて満たされる場合に成功する：

$$V_{r2}(e_3||e_4, r_1) = \text{true} \quad (6)$$
$$H(r_2) = e_3 \quad (7)$$

式 (6) は，送られてきた受領証が送信した TEF に対応していること，および受領証の作成者が r_2 であることの検証であり，式 (7) は受領証の作成者（r_2）が TEF の送信先（c_1）と同一であることを検証している．上記の検証が成功したら，I は先に保存した E_I の複製を消去する．

以上の手順により，利用者 U は権利定義 m とトークン $(H(m), H(PkI))$ を保持することとなった．すなわち，権利定義 m により定義され，発行者 I によりその価値を裏付けられた権利が，利用者 U に所有された．

3.2.2 譲渡処理

譲渡とは，権利定義 m と発行者 I に対応するトークン $(H(m), H(PkI))$ を利用者間で移送する処理である．利用者 $U1$ から利用者 $U2$ への電子権利の譲渡は以下の手順で行われる（**図 6**）．

(1) $U1$ は耐タンパ証明 $G_{U1} : (g_1, g_2) := (S_{PkG}(PkU1), PkG)$ を A_I や m とともに $U2$ に送信する $(U1 \to U2 : \{m, A_I, G_{U1}\})$.

(2) $U2$ はチャレンジ $C_{U2} : (c_1, c_2) := (H(PkU2), s)$ を生成し，s を有効セッション集合 S_{U2} に追加する．

(3) $U2 \to U1 : C_{U2}$.

(4) $U1$ は格納されているトークン ($H(m)$,$H(PkI)$) を削除し，TEF E_{U1} を生成する：

$$e_1 := H(m)$$
$$e_2 := H(PkI)$$
$$e_3 := c_1$$
$$e_4 := c_2$$
$$e_5 := S_{PkU1}(e_1||e_2||e_3||e_4)$$
$$e_6 := PkU1$$

発行と同様に，$U1$ は E_{U1} の複製を保存しておく．

(5) $U1 \rightarrow U2 : E_{U1}$.

(6) $U2$ は E_{U1} を検証する．この検証は，次の式がすべて満たされる場合に成功する：

$$e_3 = H(PkU2) \quad (8)$$
$$e_4 \in S_{U2} \quad (9)$$
$$V_{e6}(e_1||e_2||e_3||e_4, e_5) = \text{true} \quad (10)$$
$$V_{g2}(e_6, g_1) = \text{true} \quad (11)$$
$$H(g_2) \in a_1 \quad (12)$$
$$V_{a3}(a_1, a_2) = \text{true} \quad (13)$$
$$H(a_3) = e_2 \quad (14)$$
$$e_2 \in L \quad (15)$$

式 (8)，(9)，(10) は，発行における式 (1)，(2)，(3) と同様である．式 (11) は，保証人 g_2 が権利の譲渡側 IC カード e_6 を保証していることを検証している．式 (12)，(13)，(14) は，保証人 g_2 が発行者 e_2 によって信用されていることを検証している．また，式 (15) は，権利の有効性の検証である．

(7) 上記の検証に成功した場合，$U2$ は S_{U2} から e_4 を削除し，トークン T を格納する．

(8) $U2 \rightarrow U1 : R_{U2}$.

(9) 発行と同様に，$U1$ は R_{U2} を検証し，E_{U1} の複製を削除する．

以上の手順により，利用者 $U1$ からトークン $(H(m), H(PkI))$ が失われ，利用者 $U2$ に移送された．すなわち，利用者 $U1$ から利用者 $U2$ への権利の譲渡が行われた．

3.2.3 行使処理

行使は，利用者と改札者との間で譲渡と同様な手順により行われる．以下に行使プロトコルと譲渡プロトコルとの差異を示す（**図 7**）．

- チャレンジ C には，「消費」と「提示」のどちらを求めるのかを示す情報を含める．たとえば，以下では c_2 が負の場合は提示と見なすものとする．
- 「消費」が求められた場合（c_2 が正の場合，など）にのみ，TEF 生成の際にトークンを削除する．

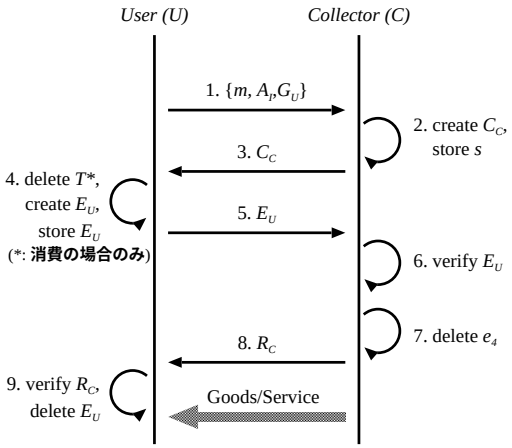

図 7 行使プロトコル
Fig. 7 Redeeming an electronic right.

- TEF の検証に成功した際に，トークンの格納を行う代わりに改札者から利用者へ権利定義 m により定義されている対価の提供を行う．

4. 考　　察

本章では，本論文の提案方式について，多様性への対応，安全性の確保，実用性の確保のそれぞれの観点から考察する．

4.1 多様性への対応

本方式では，権利定義とトークンにより表現可能な権利を電子権利として扱うことができる．

まず，本方式において権利の多様性は権利定義の表現能力に依存する．すなわち，権利定義 m は，任意の形式を持つことが可能であるため，権利定義の記述言語を適切に設計することにより，任意の内容や条件を持つ権利を表現可能である．たとえば，XML を用いて権利の記述を行う権利定義記述言語 XML Ticket [11] では，権利の属性として任意の情報を記述することができるほか，譲渡や行使の条件として，「○月×日まで有効」や「会員限り有効」など，時間に関する制約や他の権利との依存関係を記述することを可能にしている．

また，発行者の多様性については，論理的には公開鍵ペアを保持するすべての者が発行者となることができる．ただし，実社会において見知らぬ人による何の裏付けもない手形を信用できないのと同様に，発行した権利を「有効である」と判断してもらうためには，利用者が信用する発行者のリストである発行者リスト L に自らのフィンガープリントを含めてもらう必要がある．

発行者リスト L の管理は，本来はそれぞれの利用者がリスクを判断して行うべきであるが，本方式を用いたシステムを効率的に運用していくためには，この判断をサポートするための枠組みが必要となる．

4.2 安全性の確保

以下において，安全性の確保に関して，2 章であげたそれぞれの要件について考察する．ここでは，署名鍵の管理は適切に行われており，漏洩することがないこと，およびトークンを格納する耐タンパ装置の耐タンパ性は破られないことを前提として議論する．ただし，後者の前提については本節の末尾においてあらためて議論する．

4.2.1 改竄防止

電子権利の改竄を防止するためには，権利定義とトークンの両方を改竄から保護する必要がある．

トークンは，対応する権利定義のハッシュ値をマニフェストとして保持する．そのため，トークン自体が改竄されないという前提において，権利定義の改竄の可能性は一方向ハッシュ関数の強度に依存する．

一方，トークンは TEF として流通する際を除いて IC カードなどの耐タンパ装置内に格納されている．TEF は送信側の電子署名によって保護されているため，IC カードの耐タンパ性が破られないという前提において，トークンの改竄の可能性は TEF に対する電子署名の強度に依存する．

4.2.2 偽造防止

電子権利の偽造を防止するためには，トークン（の発行者情報部）が改竄から保護されること，および他人を発行者とするトークンの生成を防止することが必要となる．

前節の改竄防止における議論と同様に，トークンの改竄の可能性は TEF に対する署名の強度に依存する．

また，他人を発行者とするトークンの生成を防止するためには，発行者自体へのなりすましや，発行者に信任された IC カードへのなりすましを防止する必要がある．前者のなりすましは発行処理における式 (3) および (4) の検証により防止され，後者は譲渡処理における式 (11)〜(14) の検証により防止される．したがって，これらのなりすましの可能性は，フィンガープリントに用いられるハッシュ関数の強度と，TEF，信任情報，耐タンパ証明のそれぞれに対する電子署名の強度に依存する．

4.2.3 複製の防止

電子権利の複製を防止するためには，1 つの TEF から複数のトークンが不正に復元されることを防がなくてはならない．すなわち，すでにトークンに復元した TEF を再利用して，さらにトークンを復元しようとすること（TEF の再利用）や，他人宛の TEF からトークンを復元しようとすること（TEF の使い回し）を防止する必要がある．

TEF の再利用はチャレンジと有効セッション集合により防止される．不正者が TEF を再利用しようとしても，すでに有効セッション集合からチャレンジが削除されているため，式 (2) もしくは (9) の検証に失敗する．

TEF の使い回しはチャレンジに含まれるフィンガープリントにより防止される．不正者が盗聴などの手段により「横取り」した TEF からトークンを復元しようとしても，TEF の宛先となるフィンガープリントが異なるため，式 (1) や (8) の検証に失敗する．

4.2.4 公平性の確保

流通が公平であるとは，流通の任意の時点において，流通の当事者双方にとって不公平な状態が発生しないこと，もしくは流通相手の協力を得ることにより不公平な状態から回復できること，のどちらかの条件を充足可能であることと定義できる[13),14)]．前者は強い公平性（strong fairness），後者は弱い公平性（weak fairness）と呼ばれる．

ここで，権利の送付側にとって不公平な状態とは，すでに権利を送付したにもかかわらず「まだ受け取っていない」と主張されること（受領の否認）であり，権利の受領側にとって不公平な状態とは，まだ権利を受領していないにもかかわらず,「すでに渡した」と主張されること（送付の虚言）である．すなわち，本方式においては，送付側にとっては受領証を確保できること，受領側にとっては TEF を確保できることが，それぞれにとって公平性を確保するための条件となる．したがって，本方式に基づく電子権利流通の公平性は，TEF と受領証との交換の公平性に帰着される．

3 章で示した手順によれば，それぞれの流通処理が最後まで完遂した状態では，送付側は受領証を，受領側は TEF をそれぞれ確保しているため，公平性は確保されている．また，なんらかの理由により流通が中断された場合でも，権利の複製を生じることなく安全に TEF を再送することが可能であるため，中断した流通を再開する機会が必ずある（中断した流通の相手が逃げ去らない）という前提のもとでは公平性が確保可能となる．これは弱い公平性に相当する．

この前提は，たとえば利用者の公開鍵を事前登録させるなど，途中で流通を放棄した者を特定する手段を設けることにより実現可能となるが，後述するように利用者のプライバシーを確保するための留意が必要と

なる．

上記のような前提を置くことなく公平性を確保するためには，TEF と受領証の交換が（強い公平性の意味で）公平に行われることを保証できる必要がある．このような交換は，公平な交換プロトコル（fair exchange protocol）として知られる情報の交換手法を適用することにより実現することができる[14),15)]．ただし，強い公平性を確保した交換を行うためには，たとえば当事者双方の計算能力が等価であることや，もしくは第三者機関が介在することなどの前提を置く必要があり，プロトコルも複雑になる．したがって，これらの適用にあたっては，実用性とのトレードオフを慎重に検討する必要がある．本方式における効率的な強い公平性の保証については今後の課題である．

4.2.5 プライバシーの確保

本方式では，権利の送信側の署名を受信側で検証する必要があるため，受信側に対して送信側の公開鍵は知られてしまう．

しかしながら，これはプライバシーに対する大きな脅威にはならないと考えられる．本方式では利用者本人の事前登録を必要としないため，公開鍵と実世界での利用者本人とを結びつける情報は存在しない．また，利用者はこれらの公開鍵をいくつ利用してもかまわない（IC カードをいくつ保持してもかまわない）ため，プライバシー上必要であればそれらの公開鍵を「使い捨て」にしてもよい．

ただし，公平性の確保のために途中で流通を放棄した者を特定する手段を設ける場合や，後述のように TEF の履歴を権利とともに移送し，(IC カードの耐タンパ性に依存しない）より高い安全性を求める場合には，利用者と公開鍵との対応関係の事前登録が必要となる．これらの場合にプライバシーを確保するためには，公開鍵と利用者との関連づけを困難にするような鍵管理方式[16)] の導入を検討する必要がある．

4.2.6 耐タンパ性への依存について

本方式の安全性は，トークンを格納する IC カードの耐タンパ性に依存している．そのため，もしこの耐タンパ性が破られれば，電子権利の改竄，偽造，複製などの攻撃が成立する．これは，権利の発行者にとって大きなリスクになる．

ただし，本方式では発行者ごとの信任情報と IC カードごとの耐タンパ証明を用いることにより，発行者が信用する耐タンパ装置の条件を指定できるようにしている．これにより，もしある耐タンパ装置の耐タンパ性が破られても，その装置に耐タンパ証明を与えた保証人を「信任してしまった」発行者のみに攻撃の被害が限定されるため，耐タンパ性が破られることによる被害を局所化することができる．これは，本方式の特長の 1 つである．

また，より高い安全性を確保するために，TEF の履歴を用いることも可能である．TEF は送信者の署名と，受信者のフィンガープリントを含むため，TEF の履歴を収集することにより署名鎖（chain of signatures）を構成することが可能となる．たとえば消費時に権利の複製が検出された場合，それぞれの署名鎖をたどり，その分岐点を検出することにより不正者（の公開鍵）が特定可能となる．

これにより，耐タンパ性への攻撃による不正の事後検出を可能とし，それらの不正に対する抑止力とすることができる．しかしながら，署名鎖の流通や検証は負荷の高い処理であること，および利用者の事前登録や署名鎖の収集が必要となるためにプライバシーの確保が困難になること，などに留意する必要がある．

4.3 実用性の確保

以下において，実用性の確保に関してオフライン性，スケイラビリティ，コスト効率のそれぞれの要件について考察する．

まず，オフライン性については，上記の各流通処理は，流通の当事者である二者間だけで行われており，ネットワークを介して第三者が介在する必要などがないため，ネットワークが利用できない環境でも権利の流通が可能である．

また，スケイラビリティについても，それぞれの流通処理は独立して行われ，スケイラビリティのボトルネックとなるような処理は存在しない．

最後に，コスト効率について議論する．本方式を実現するために必要なプログラムやトークンのサイズは，既存の IC カード上で十分に実現可能な程度であることが，Multos v3.4 および JavaCard 2.1 を用いた試作実装により確認されている[17)]．

本実装における IC カード上のプログラムのサイズは 2 KB〜3 KB 程度であり，1 種類のトークンあたりの必要記憶容量は 44 byte（マニフェスト 20 byte + 発行者情報 20 byte + 個数☆4 byte）である．したがって，EEPROM 容量が 16 KB 程度の IC カードを用いた場合，本実装では 1 枚の IC カードあたり 200 種類以上（$44 \times 200 + 3000 = 11,800$ (bytes)）の電子権利を扱うことが可能である．

☆ 本実装では，回数券などを効率良く実現するために，本論文で示した方式に対してトークンの種類ごとの個数を管理可能とする拡張がなされている．

5. 関 連 研 究

権利のような「価値」を表象する情報の複製や反復利用への対策としては，電子現金の分野で二重使用（double spending）防止技術として各種の方式が用いられている[18]．それらの方式は，大別すると以下のように分類される．

口座型 電子現金の所持状況や使用状況が記録された「口座」をサーバ上で集中管理することにより二重使用を防止する．

履歴検証型 流通時に電子現金に流通履歴を付随させ，還流時などに流通履歴を検証することにより二重使用を（事後）検出する．

バランス型 現金の額面を IC カードなどの耐タンパ装置に格納し，譲渡や行使の際には必ず減額されること，および不正な増額や二重使用がなされないことを耐タンパ装置が保証する．

口座型の手法では，二重使用が行われようとした場合，口座に対する更新処理の矛盾として異常が検出される．eCash[19] や *i*KP[20] など多数のシステムがこの手法を用いている．流通時に必ず帳簿の更新を必要とするため，この手法はオフライン環境では用いることができないが，オンライン環境を前提にすれば比較的容易に二重使用を防止することが可能である．また，IC カードを併用することにより支払い処理のみをオフライン環境で行うことも可能である[21]．なお，口座型の手法を電子権利の流通に適用した方式も提案されている[22]．

履歴検証型では，電子現金の「引き出し」時に識別子を付与し，同一の識別子を持った電子現金の重複還流を検出することにより二重使用を検出する．二重使用が検出された際には，それらの電子現金の流通履歴を比較して分岐点を抽出することにより不正者を特定することが可能である．本方式における TEF の履歴は，この手法における流通履歴に相当する．ただし，この手法では還流時まで二重使用が検出できないため，流通過程において現金の有効性が保証されない．そのため，IC カードを用いて後述のバランス型と組み合わせることにより，流通経路上での現金の有効性を保証する方式[23),24)] なども提案されている．

バランス型では，IC カードなどの耐タンパ装置が二重使用を事前に防止する．この方式は Mondex[3] や，CEN prEN 1546[25] 準拠の電子財布システムなどで採用されている．履歴検証型と異なり，耐タンパ装置により二重使用が事前に防止されているため，流通中の現金の有効性は保証されている．耐タンパ性にその安全性を依存している点やチャレンジの利用により二重使用を防止している点で本方式と共通しているが，2 章で述べたようにこれらの方式は限定された発行者（中央銀行など）による限定された種類の通貨のみを扱うことを目的としている．そのため，これらの方式では多様性を持つ権利を流通させる必要がある権利流通基盤にはそのまま適用できない．

ただし，これらの方式では発行者を限定することにより，流通時の認証手段として DES などの共有鍵方式を用いることが可能である．そのため，本方式のような公開鍵暗号による署名/検証処理を行う方式に比べ，処理能力の低い安価な IC カードを利用することができるという利点がある．

しかしながら，IC カードの実装技術の発達により，これらの機能の差異による IC カードの価格差はそれほど顕著なものではなくなりつつある．また，本方式では多様性への対応により，権利ごともしくは発行者ごとに個別にシステムを構築する必要がないため，扱う権利の種類や発行者の数が増えるほど，発行コストや運用コストが効率的に分散され，より費用対効果の高いシステムを構築することが可能となる．

したがって，扱う権利の種類が増えるほど，また，権利の発行者が増えるほど，本方式のコスト効率は従来方式と比較して有利になると考えられる．

それ以外の分野では，音楽データや画像データなどの著作物に関して，不正な複製や閲覧を防止するシステムが提案されている．たとえば DigiBox[26] や ContentGuard[27] などがこれに相当する．ただし，これらのシステムは，著作物そのものの複製や閲覧を防止することを目的としており，権利の原本性の保証とその流通を目的とした本方式とは対象分野が異なっている．

また，本論文では議論の対象外としたが，権利流通基盤を実現するためには，権利定義に記述された内容がどのような価値を有するかについて定義するための権利記述方式が必要となる．このような記述言語として，階層的な権利モデルに基づく権利記述言語 XML Ticket[10),11)] が提案されている．XML Ticket を用いて記述された権利定義の原本性を，本提案方式に基づいて保証することにより，電子権利流通システムが構築可能であることが試作により確認されている[28]．

6. ま と め

本論文では，電子権利流通のための原本性保証方式に必要とされる要件を示し，それらの要件を充足する方式として FlexToken を提案した．また，本方式に基づく権利流通の手順を述べ，その安全性について評

価した．

本方式は，原本性を表象する情報を権利内容の記述から分離することにより，任意種類の権利の流通と原本性の保証を，IC カードなどの限られた記憶容量や演算性能しか持たない耐タンパ装置を用いて行うことを可能にしている．実際に，現在市場で流通している IC カードを用いて本方式が実用的な容量や性能で実現可能であることを試作により確認した．

また，本方式は流通時の認証に信任情報と耐タンパ証明を用いることにより，発行者が信用可能な IC カードの条件を指定する手段を提供している．これにより，発行者は自らが発行した権利の流通範囲をあらかじめ特定することが可能となるとともに，IC カードの耐タンパ性が破られることによる影響範囲を局所化することができる．

現在，本方式に基づく電子権利流通システムの構築と，同システムを用いた性能評価が完了している．今後は，施設予約などの公共サービスや映画館入場券などの興行系サービスへの適用を通じて，本方式の実用性を検証していく予定である．

謝辞 本研究を進めるにあたりご協力いただいた FlexTicket プロジェクトの諸氏に感謝します．特に，本論文作成にあたり有益なコメントをいただいた中嶋良彰氏に感謝します．

参 考 文 献

1) Fujimura, K. and Nakajima, Y.: General-purpose Digital Ticket Framework, *Proc. 3rd USENIX Workshop on Electronic Commerce* (1998).
2) digitiminimi Inc.: e-ticket.net (1997). http://www.e-ticket.net/.
3) Mondex International: Mondex electronic cash. http://www.mondex.com/.
4) 内閣法制局法令用語研究会（編）：法律用語辞典，有斐閣 (1993).
5) Farrell, S. and Housley, R.: *An Internet Attribute Certificate Profile for Authorization*, Internet Draft, IETF PKIX Working Group (2001). draft-ietf-pkix-ac509prof-09.txt.
6) Ellison, C.M., Frantz, B., Lampson, B., Rivest, R., Thomas, B. and Ylonen, T.: *RFC 2693: SPKI Certificate Theory* (1999).
7) Clarke, R.: The Mondex Value-Card Scheme Mid-Term Report, *Chip-Based Payment Schemes: Stored-Value Cards and Beyond*, Xamax Consultancy Pty (1996).
8) Rivest, R., Shamir, A. and Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems, *Comm. ACM*, Vol.21, No.2, pp.120–126 (1978).
9) NIST: FIPS 180-1: Secure Hash Standard (1995).
10) 中嶋良彰，藤村　考，関根　純：権利流通基盤実現のための権利情報定義言語，コンピュータセキュリティシンポジウム'99 予稿集 (1999).
11) 中嶋良彰，寺田雅之，藤村　考：権利を階層的に定義可能な権利情報定義言語：XML Ticket，信学技報，ISEC2000-56 (2000).
12) Fujimura, K. and Terada, M.: *XML Voucher: Generic Voucher Language*, Internet Draft, IETF Trade Working Group (2001). draft-ietf-trade-voucher-lang-01.txt.
13) Gärtner, F.C., Pagnia, H. and Vogt, H.: Approaching a formal definition of fairness in electronic commerce, *Proc. 18th IEEE Symposium on Reliable Distributed Systems*, pp.354–359 (1999).
14) Asokan, N.: Fairness in Electronic Commerce, Ph.D. Thesis, University of Waterloo (1998).
15) Asokan, N., Schunter, M. and Waidner, M.: Optimistic Protocols for Fair Exchange, Technical Report RZ 2858, IBM (1996).
16) Petersen, H. and Horster, P.: Self-certified Keys—Concepts and Applications, *Proc. 3rd Conference on Communication and Multimedia Security*, Chapman & Hall (1997).
17) 花舘蔵之，寺田雅之，千綿伸之，水野康尚：スマートカードを利用した電子商取引のための原本性流通 システムの開発，コンピュータセキュリティシンポジウム 2000 予稿集 (2000).
18) Wayner, P.: *Digital Cash*, AP Professional, Chestnut Hill, MA (1997).
19) Chaum, D., Fiat, A. and Naor, M.: Untraceable electronic cash, *Proc. Crypto 88*, Springer-Verlag (1988).
20) Bellare, M., Garay, J.A., Hauser, R., Herzberg, A., Krawczyk, H., Steiner, M., Tsudik, G. and Waidner, M.: iKP—A Family of Secure Electronic Payment Protocols, *Proc. 1st USENIX Workshop on Electronic Commerce* (1995).
21) Brands, S.: Off-line Cash Transfer by Smart Cards, Technical Report CS-R9455, CWI (1994).
22) Matsuyama, K. and Fujimura, K.: Distributed Digital-Ticket Management for Rights Trading System, *Proc. 1st ACM Conference on Electronic Commerce*, ACM (1999).
23) 藤崎英一郎，岡本龍明：エスクロー電子現金，信学技報，IT95-51, ISEC95-46, SST95-112, pp.7–12 (1996).
24) 中山靖司，森畠秀実，阿部正幸，藤崎英一郎：電子マネーの一実現方式について，金融研究，

Vol.16, No.2, pp.75–86 (1997).
25) Comité Européen de Normalisation: *prEN 1546: Inter-sector electronic purse* (1995).
26) Sibert, O., Bernstein, D. and Wie, D.V.: The DigiBox: A Self-protecting Container for Information Commerce, *Proc. 1st USENIX Workshop of Electronic Commerce* (1995).
27) ContentGuard, Inc.: ContentGuard: Digital Rights Management (2000). http://www.contentguard.com/.
28) 水野康尚，千綿伸之，大嶋嘉人，松山一雄：権利流通基盤実現のための汎用デジタルチケットシステム，コンピュータセキュリティシンポジウム'99予稿集 (1999).

(平成 12 年 11 月 30 日受付)
(平成 13 年 6 月 19 日採録)

寺田 雅之（正会員）

1993 年神戸大学工学部システム工学科卒業．1995 年同大学大学院工学研究科修士課程修了．同年 NTT 入社，NTT 情報通信研究所配属．現在，NTT 情報流通プラットフォーム研究所所属．分散オブジェクト，権利流通基盤の研究に従事．

花舘 蔵之（正会員）

1997 年東北大学工学部通信工学科卒業．同年 NTT 入社．同年，NTT 情報通信研究所入所．現在，NTT 情報流通プラットフォーム研究所情報セキュリティプロジェクト所属．IC カードアプリケーションの研究に従事．

藤村 考（正会員）

1984 年北海道大学工学部電気工学科卒業．1989 年同大学大学院工学研究科情報工学専攻博士課程修了．同年 NTT 入社．現在，NTT 情報流通プラットフォーム研究所勤務．2001 年より電気通信大学大学院情報システム学研究科客員助教授．工学博士．電子商取引システム，特に，IC カードアプリケーション，電子価値取引システム，トラストモデルに関する研究に興味を持つ．

関根 純（正会員）

1982 年東京大学大学院工学系修士課程修了．同年日本電信電話公社（現 NTT）入社．以後，マルチメディアデータベース管理システム，データベース設計支援技術，オブジェクト指向ビジネス部品，権利流通基盤（電子チケット），認証，公証等の研究開発に従事．ACM 会員．工学博士．