SCIS 2002 The 2002 Symposium on Cryptography and Information Security
Shirahama,Japan, Jan.29-Feb.1,2002
The Institute of Electronics,
Information and Communication Engineers

電子権利流通方式対に関する特性分析

副島　晋*　　松浦　幹太*　　今井　秀樹*

Abstract— 電子権利を安全に流通させる技術は、電子社会を構成する上で極めて重要である。電子マネーもその一種であると見なせる。従来、個々の電子権利流通方式それぞれ単体で研究がされてきた。しかし本来、権利を渡す場合には何らかの対価となるものとの交換がなされると考えるのが自然である。その対価も広義には権利であり、電子権利流通方式は、２つのシステムが稼働している環境で考察すべき研究対象である。本論文では，ある具体的な電子権利流通方式について方式単独では可能となってしまう攻撃例を取り上げ，対価と交換するという状況での攻撃防止法を提示して方式対を考察することの重要性を説く．

Keywords: 電子権利　対価　耐タンパー性　権利定義　トークン

1　はじめに

広義の電子権利を流通させる技術は，電子社会を構成する上できわめて重要である．例えば電子マネー [1]–[3] もその一種であるとみなせる．従来，個々の電子権利流通方式は各々単体で研究がされてきた．しかし本来，権利を渡す場合には何らかの対価との交換がなされると考えるのが自然である．その対価も広義には権利であり，電子権利流通方式は，2 つのシステムが稼動している環境で考察すべき研究対象である．しかし，電子権利の流通に関して，このような視点での本格的な分析はなされてこなかった．

例えば，ある電子権利流通方式に，何らかのセキュリティ上の問題点があったと仮定する．この場合でも，対価を構成するための流通方式と同時に稼動させる際に何らかの工夫をすれば，その問題点を解決できる可能性がある．本論文では，その具体例を挙げることによって，電子権利流通方式の研究で二つのシステムの組み合わせ方が実際の安全性にとって重要であることを示す．

そのために，まず第二章で，電子権利流通方式基盤のための汎用的な原本保証方式 [4] を紹介し，その方式単独で考えた場合の問題点を指摘する．続いて第三章では，対価と交換されながら，その電子権利が流通していくモデルを記述し，そのモデルの下で問題点を克服する仕組みを提案する．

* 東京大学生産技術研究所　情報システム部門　〒 153-8505 東京都目黒区駒場 4-6-1 , Infomation and Systems Department , Institute of Industrial Science, The Univercity of Tokyo, 4-6-1 Komaba, Meguro-ku, Tokyo 153-8505, Japan, Email:soejima@imailab.iis.u-tokyo.ac.jp,{imai,kanta}@iis.u-tokyo.ac.jp

2　汎用的な原本性保証方式 [4]

文献 [4] の方式（以後，同文献著者の頭文字を並べ THFS 方式と記す）の特徴は，バランス型の電子現金システムの問題点を解決し，様々な権利の発行者が，様々な種類の権利を発行することを可能にした点である．

文献 [4] で著者は電子権利の流通を可能にするための条件として，多様性への対応，安全性の確保，実用性の確保をあげている．多様性への対応のための要素は，権利の多様性，発行者の多様性，安全性の確保に必要な要素に，改竄防止，偽造防止，複製防止，プライバシーの保護，公平性の確保，実用上の確保のための要素として，オフライン性，スケイラビリティ，プライバシーの保護である．公平性の確保とは，権利の移送が完了したにもかかわらず，権利を受け取った人物がまだ，受け取っていないと主張することを防ぐことにより，権利の送信者にとって不公平な状態になることを防ぐことである．これらは従来の電子証明書，電子現金に求められる安全性の要素と同じである．しかし，両者ともに，そのままで電子権利流通に適しているわけではない．

まず，電子証明書について考える．電子証明書とは，文献 [4] では電子署名を施された電子情報と位置付けられている．電子署名は誰でも利用できるので，多様性への対応を満たす．また，電子署名は改竄防止，偽造防止も満たす．しかし，電子署名は複製を防止する手段をもたない．複製を防止する方法には，PKIX[5] や SPKI[6], [7] などがあるが，PKIX は権利の所有者は，その権利を発行された人物に限定され，SPIK は権利を他社に委譲するときに，委譲元に権利が残ってしまうという欠点がある．

次に，電子現金システムについて整理する．電子現金

システムは，文献 [2] によると，口座型，履歴検証型，バランス型の 3 種類のシステムに大別される．口座型は，電子現金等の電子権利の所持，使用記録をサーバー上で集中管理するシステムである．二重使用の検出は，口座に対する更新処理の矛盾をつくことによりできる．しかし，このシステムでは利用時にサーバーと交信する必要があるので，オフライン性が損なわれてしまう．また，履歴検証型は電子権利の流通時に，権利に流通履歴を付随させ，還流時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．しかし，この方式では二重使用を事後検出するので，流通時に不正を検出できず，権利の有効性を流通時に保証できない．バランス型の電子現金システムは耐タンパー性が権利の二重使用を防ぐので，流通中の権利の有効性が保たれる．しかし，このシステムでは限られた発行者に発行された権利を，限られた発行者の認証情報を固定的に記録した耐タンパーデバイスで扱うことを前提としているので，限られた発行者が発行した権利しか扱えない．

THFS 方式は，従来方式では完全に満たすことができなかった電子権利流通を可能にするために，バランス型電子現金方式に近いけれどもその問題点を解決したものとなっている．これにより電子権利の改竄，偽造，複製を防いでいる．さらに，トークンの移送には電子署名を用いて権利，発行者の多様性を確保している．

2.1 方式の概要

THFS 方式は，電子化した証券やチケットなどの権利を，権利の原本性を保証した状態で送信するための手法である。複製などの不正を防止するために，IC カードなどの耐タンパー性を有するデバイスを用いて権利を保持し，取引に利用する．このシステムでは，発行者，利用者，改札者が存在する．

- 発行者： 利用者へ電子権利を発行し，発行した権利を保証する
- 利用者： 権利の所有者で，改札者に対し権利を行使したり，他の利用者に権利を譲渡することができる
- 改札者： 利用者から電子権利を回収し，権利の内容に応じた対価を提供する

発行者は権利を発行する役割を，利用者は権利の譲渡，実行を，改札者は権利を行使した利用者に対し，対価を提供する役割を果たす．また，発行者の認証情報を IC カードに固定させないため，任意の発行者が IC カードに対して，権利を発行できる．以下，図 1 に権利の流通過程を示す．

この方式では電子権利を権利定義とトークンに分割して，トークンを IC カードなどの耐タンパー性を有するデバイスに記録する．権利定義とは，権利を行使して得られる対価の内容を記述した情報である．また，トークンとは権利の発行者が利用者に対して，権利の原本性を保証する情報である．権利を発行するとき，および譲渡するときは，まず発行元および譲渡元の人物が，発行先および譲渡先の人物に権利の定義を渡し，相手のフィンガープリントなどを受け取ったあと，トークンを自身から削除，移送するという手順を踏む．フィンガープリントは，権利を発行される人物および譲渡される人物が権利を複製することを防ぐために発行するものである．本論の以下の節では，権利の譲渡処理が行なわれる過程をまとめる．そして，この方式単独で考えた場合に可能となる攻撃を 1 つ指摘する．

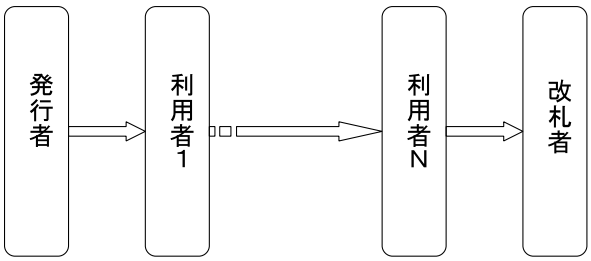

図 1: 権利の流通過程

2.2 権利の譲渡処理

プロトコルの説明にあたり，以下の用語と記号と定義する．

- トークン交換形式 (TEF)： トークン，チャレンジ，権利の送り手の公開鍵と電子署名
- チャレンジ： 権利の受け手のフィンガープリントと受け手が任意に生成するセッション番号
- 信任情報： IC カードの耐タンパー性を証明する情報. 耐タンパー性を保証する第 3 者のフィンガープリントの集合,

これらの情報のほかに，利用者と改札者が保有するセッション集合 S と，発行者リスト L がある．

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．これは，利用者や改札者が各々管理するもので，セッション番号を発行するごとに，有効セッション集合に付け加える．有効セッション集合は IC カードによって管理され，不正に削除されることはないものとする．セッション番号については後で述べる．

また，発行者リスト L は，利用者，改札者が信頼して扱える権利を発行する発行者が掲載されているリストである．このリストは，発行者のフィンガープリントの集

合であり，発行者リスト L に自身のフィンガープリントが含まれる発行者が発行した権利だけが，利用者，改札者ともに扱うことができる．原本の汎用性は，このリストによって確保されるものと考えられる．

2.3 譲渡プロトコル

権利の譲渡は，権利定義とその権利の発行者 I に対応するトークンを，権利を譲渡する利用者から譲渡を受ける利用者へ移送することで，成立する．ここでは，権利を譲渡する利用者を U_1，権利を譲渡される利用者を U_2 として，譲渡の過程を説明する．

1. U_1 は，耐タンパー証明と，譲渡する権利の権利定義，信任情報を U_2 に送信する．
2. U_2 は，チャレンジを作成し，チャレンジの中のセッション番号を有効セッション集合 S_{U_2} に加える．チャレンジは，U_2 のフィンガープリントと，セッション番号の組み合わせで，セッション番号は譲渡を受ける利用者が生成する．
3. U_2 が U_1 に対し，チャレンジ C_{U_2} を送信する．
4. U_1 はトークンを削除し，TEF である E_{U_1} を作成する．
5. U_1 は U_2 に E_{U_1} を送信する．U_1 は E_{U_1} を保持する．
6. U_2 は E_{U_1} を検証する．
7. 上記の検証によって，E_{U_1} の正当性が確認されたら，U_2 は有効セッション集合 S_{U_2} からセッション番号を削除し，トークンを IC カードに格納する．
8. U_2 から U_1 に対して，受領証 R_{U_2} を送信する．受領証 R_{U_2} は，U_2 の公開鍵と，U_2 がチャレンジに対して電子署名したものである．
9. U_1 は R_{U_2} を確認し，正当性が認められたら保持していた E_{U_1} の複製を消去する．

以上のプロセスを通じて，権利が U_1 から U_2 に譲渡される．上記のプロセスを図 2 に示す．

2.4 セキュリティ上の問題点

この方式には，不正な受領証で引き起こされるセキュリティ上の欠陥がある．権利を受領するユーザーがセッション番号を一意的に作成でき，かつ耐タンパー性を有するデバイスでセッション番号 s を管理したとしても，チャレンジ s を平文で送信する以上，通信路上で複製・再送される攻撃にあう恐れがある．

U_2 が権利を受け取っていながら，受け取っていないと主張する場合を説明する．U_1 から U_2 へ権利定義 m であらわされる権利の受け渡しが，今行なわれているとする．また，同じ権利定義 m であらわされる権利の受け渡しが過去に U_1 以外の相手である U_3 とあったとする．今行なわれている受け渡しで U_2 が発行するセッション番号を s:=$c_{2_{now}}$，過去に U_3 から U_2 に対して行なわれた受け渡しで U_2 が発行したセッション番号を s':=c'_2 とする．

図 2 の　の通信している過程で U_2 がセッション番号 s を昔の s' にすりかえるとする．次に，　のトークン交換形式が U_1 から送信されてきたときに，E_{U_1} の中に含まれる s' を s に戻す．戻す理由は，もともと U_2 は s をセッション番号として生成しており，さらに自身の ID カードの耐タンパー性によって自身の ID カードに収納されている s を s' に変更することができないからである．そのまま，U_1 からの TEF に s' が含まれたままであれば，TEF 受け取りができないので，通信路上で s' を s に戻す必要があるのである．そして，　の過程で受領証 R_{U_2} の $S_{PkU_2}(c_{1_{now}}||c_{2_{now}})$ を $S_{PkU_2}(c_{1_{now}}||c'_2)$ にすり替える．ここで，$S_{PkU_2}(a)$ とは，U_2 がメッセージ a に対して電子署名を行なったという意味である．こうして，U_2 は U_1 から権利を受け取って，U_1 にかつて U_1 以外の人に対して発行した受領証とまったく同じ物を発行できる．

権利の譲渡処理が終わったあと，権利を受け取ったはずの U_2 が「権利をまだ受け取ってない」と U_1 に対して主張する．U_1 は権利を渡した証拠として，U_2 に対し，受領証 R_{U_2} を提示する．すると，U_2 はその受領証を見て,「それは昔，U_3 から権利を受け取ったときに発行した受領証だ.」と主張できる．

2.5 問題の解決法

耐タンパー性をもつデバイスの中で，すべてのエンティティで同期している時計を共有していれば，チャレンジにタイムスタンプを添えることによって，先ほど指摘した攻撃を防ぐことができる．しかし，そのような信頼できる時計の仮定は，大変強い仮定である．そこで，本論文では，そのような強い仮定に頼らず，権利を交換するもうひとつのプロセスとのリンク関係を巧みに利用することにより，実現できる対策を示す．

3 権利交換プロトコル

3.1 概要

前のセクションで述べた安全性に対する問題点を解決するために，図 2 で説明したプロトコルに，U_2 から U_1 に対して電子的な対価を送信するプロトコルを組み合わせた権利の交換プロトコルを提案する．

実際の電子商取引などの権利の流通に際しては，例えば図 2 のケースで言えば，U_1 と U_2 の間では U_1 から U_2 へ単に権利の譲渡が行なわれるよりは，U_2 から U_1 に対して何らかの対価が渡されることが自然であると考えられる．そこで，権利交換プロトコルでは，電子権利とそれに対する電子権利の対価の交換が行なわれるとする．以降，電子権利に対する対価を「電子対価」と記述する．

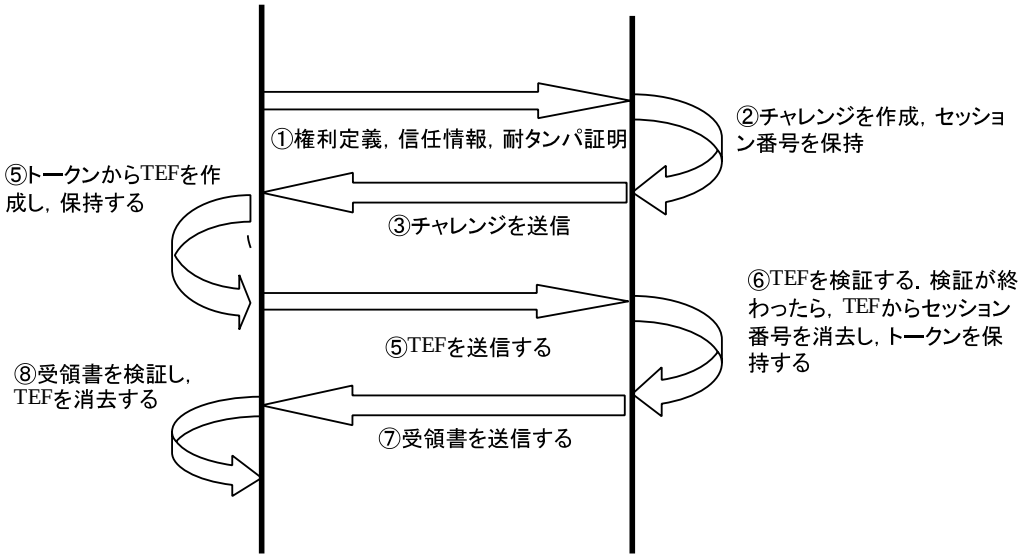

図 2: 権利の譲渡プロトコル

3.2 プロトコルの詳細

提案するプロトコルは図 2 で説明したプロトコルと原理は同じである．ただし，U_2 から U_1 に対して電子対価が送信されるプロトコルは，U_1 から U_2 に対して電子権利が送信されるプロトコルより一往復の半分だけ遅れて始まり，一往復遅れて終了する．ここでは，権利を送信する側の人物を図 2 と同じく U_1，権利を受け取り対価を U_1 に対して送信する人物を U_2 とする．また，U_1 が生成するセッション番号を $s_{1_{now}}$，U_2 が生成するセッション番号を $s_{2_{now}}$ とする．以下図 3 にプロトコルの説明図を掲載する．図 3 の中で網掛けをして説明している部分は，U_2 から U_1 へ権利を渡すプロセスである．また，以下の説明では，分かりやすいように U_1 から U_2 へ権利を渡すプロセスはプロセスの説明の前に $U_1 \rightarrow U_2$，U_2 から U_1 へ権利を渡すプロセスはプロセスの説明の前に $U_2 \rightarrow U_1$ と記述する．なお，以下の説明番号が同じ物に関しては，$U_1 \rightarrow U_2$ と $U_2 \rightarrow U_1$ のプロセスが同時に行なわれるものとする．

1. $U_1 \rightarrow U_2 : U_1$ は U_2 へ自身の耐タンパー証明と，U_2 へ渡す権利の権利定義，信任情報とセッション番号 $s_{1_{now}}$ と U_1 のフィンガープリントに対して電子署名（以下これを $c_{1_{now}}$ とする）をしたものを送信する．
2. $U_1 \rightarrow U_2 : U_2$ はチャレンジを作成する．このチャレンジを C_{U_2} とする．C_{U_2} の中身は，U_2 のフィンガープリント，U_2 が作成したセッション番号 $s_{2_{now}}$，そして $c_{1_{now}}$ である．
3. $U_1 \rightarrow U_2 : U_2$ から U_1 に対して，チャレンジを送信する．
   $U_2 \rightarrow U_1 : U_2$ は自身の耐タンパー証明，U_1 に渡す電子対価の定義，信任情報とセッション番号 $s_{2_{now}}$ と U_2 のフィンガープリントに対して電子署名（以下これを $c_{2_{now}}$ とする）をしたものを送信する．
4. $U_1 \rightarrow U_2 : U_1$ はチャレンジを確認し，TEF_{U_1} を作成し自身に複製を記録する．また，トークン T_1 を消去する．ここで TEF_{U_1} は U_1 から U_2 へ渡す権利のトークン交換形式で，T_1 は U_1 から U_2 へ渡す権利のトークンである．
   $U_2 \rightarrow U_1 : U_1$ は，U_2 から受ける電子対価に関するチャレンジを作成する．このチャレンジを C_{U_1} とする．C_{U_1} の中身は，U_1 のフィンガープリント，U_1 が作成したセッション番号 $s_{1_{now}}$，そして $c_{2_{now}}$ である．
5. $U_1 \rightarrow U_2 : U_1$ から U_2 へ TEF_{U_1} を渡す．
   $U_2 \rightarrow U_1 : U_1$ から U_2 へ C_{U_1} を送信する．
6. $U_1 \rightarrow U_2 : U_2$ は TEF_{U_1} を確認し，T_1 を記録する．さらに，U_1 から T_1 を受け取った受領証である R_{U_2} を作成する．R_{U_2} は U_2 のチャレンジ C_2 に対する電子署名と，U_2 の公開鍵の組み合わせである．
   $U_2 \rightarrow U_1 : U_2$ はチャレンジを確認し，TEF_{U_2} を作成し自身に複製を記録する．また，トークン T_2 を消去する．ここで TEF_{U_2} は U_2 から U_1 へ渡す電子対価のトークン交換形式で，T_2 は U_2 から U_1 へ渡す電子対価のトークンである．
7. $U_1 \rightarrow U_2 : U_2$ から U_1 へ R_{U_2} を渡す．
   $U_2 \rightarrow U_1 : U_2$ から U_1 へ TEF_{U_2} を渡す．
8. $U_1 \rightarrow U_2 : U_1$ は R_{U_2} を受け取る．
   $U_2 \rightarrow U_1 : U_1$ は TEF_{U_2} を確認し，T_2 を記録する．さらに，U_2 から T_2 を受け取った受領証である R_{U_1} を作成する．R_{U_1} は U_1 のチャレンジ C_1 に対する電子署名と，U_1 の公開鍵の組み合わせである．
9. $U_2 \rightarrow U_1 : U_1$ から U_2 へ R_{U_1} を渡す．

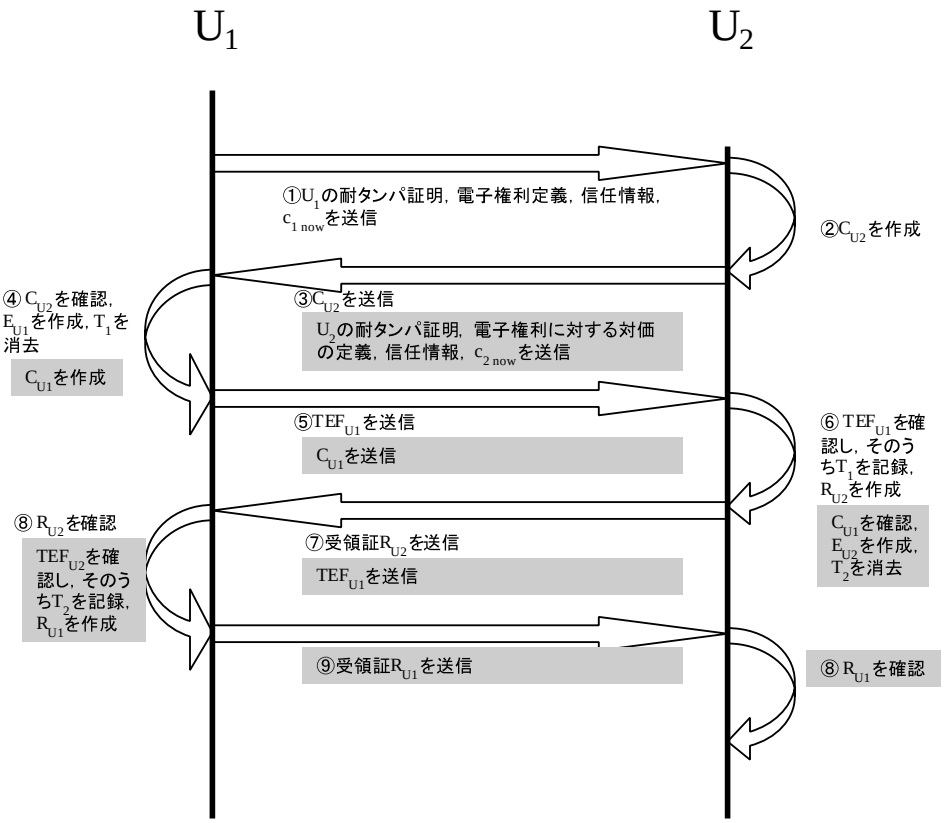

図 3: 権利交換プロトコル

10. $U_2 \rightarrow U_1$：U_2 は R_{U_1} を受け取る．

なお，U_1 と U_2 が所有するデバイスは耐タンパー性が保証されるものとする．

4 安全性解析

図 3 で説明したプロトコルで利用される利用されるセッション番号は，$s_{1_{now}}$ と $s_{2_{now}}$ で，セッション番号を含むパラメタは $c_{1_{now}}$ と $c_{2_{now}}$ である．従って，攻撃の対象となるものは上記の四つである．

このプロトコルで防ぐべき攻撃は，受領証を改竄し，権利を受け取ったのに，受け取っていないと主張する攻撃である．

U_1 から U_2 へ権利を送信する場合，権利を持ち逃げしようとする U_2 が攻撃対象とするのは U_2 が受領証に書き込む C_{U_2} に含まれる $s_{2_{now}}$，$c_{1_{now}}$ である．以下では，ここで挙げた四つのパターンの攻撃に対する耐性を示す．

なお攻撃を受ける側はできる限りの防御策をとっているものとする．

4.1 U_2 の $s_{2_{now}}$ に対する攻撃

$s_{2_{now}}$ に対する攻撃は U_1，U_2 の利用しているデバイスに耐タンパー性があるので，U_1U_2 間のネットワーク層で行なわれる．ここで，U_2 が過去の権利の受け取りに際して生成したセッション番号を $s_{2_{old}}$，U_1 が過去に電子対価の受け取りに生成したセッション番号を $s_{1_{old}}$，また $s_{1_{old}}$，$s_{2_{old}}$ に U_1，U_2 がそれぞれ電子署名を施したものを $c_{1_{old}}$，$c_{2_{old}}$ とし，以後この表記を用いて説明する．

U_2 が過去に U_1 から今回受け取るのと同じ権利 m を受け取ったことがあり，そのとき利用した $s_{2_{old}}$ を U_2 はどこかにとっておいてあったとする．図 3 の　で U_2 はセッション番号 $s_{2_{now}}$ を作成する．それによって U_2 は自身の耐タンパーデバイスの中に $s_{2_{now}}$ をもつことになる．しかし，U_2 は U_1 に昔のセッション情報を受け取らせたいので，ネットワーク層で $s_{2_{now}}$ と $s_{2_{old}}$ を入れ替える．すると，　で U_1 は $s_{2_{old}}$ を受け取り，これを記録する．U_2 は　で受け取る U_1 からのチャレンジを含む TEF_{U_1} には $s_{2_{old}}$ が含まれているので，$s_{2_{now}}$ に戻す．さらに，　で U_1 に渡す R_{U_2} に含まれるチャレンジに含まれる $s_{2_{now}}$ を $s_{2_{old}}$ に変えて U_1 に渡す．

U_2 は　までのプロセスが完了してから，受け取っているにもかかわらず「U_1 からは権利を受け取っていない，U_1 が今もっている受領証はかつて権利を受け取ったときの受領証だ」と主張する．すると U_1 は今回受け取った受領証と過去に受け取った受領証を証拠として調停者に提示する．U_1 が $s_{1_{old}}$ と $s_{1_{now}}$ をまったく変えないで権利を渡していた場合には，U_2 が今回作成した偽の受

領証と過去の受領証が一致してしまい，攻撃が成立してしまうが，U_1 は攻撃から自身を守るべきなので，$s_{1_{old}}$ と $s_{1_{now}}$ は別なものを利用していると考えるのが自然である．従って，U_1 がセッション番号を間違えて重複利用しない限り，U_2 の主張は退けられる．

4.2 U_2 の $c_{1_{now}}$ に対する攻撃

4.1 では，U_1 がセッション番号を再利用しないという仮定の下で攻撃をふせげた．そこで，$c_{1_{now}}$ を $c_{1_{old}}$ と入れ替える攻撃を U_2 が行なう場合を考える．

U_2 は，U_1 にかつて権利を受け取ったときとまったく同じ受領証を渡すことができれば攻撃が成功したことになる．U_2 が生成するセッション番号に対する攻撃だけでは，攻撃が成功しないので，U_1 が発行するセッション番号に対する電子署名も同様の改竄攻撃を行なう必要がある．しかし，U_1 は　において電子署名をすでに発行しているので，その後 U_2 から $C_{1_{now}}$ をすり替える攻撃を受けても U_1 自身が受領証を送付する前に気づくことができる．従って，U_2 が U_1 の発行するセッション番号に対する電子署名へ攻撃しても，成功することはない．

4.3 U_1 の $s_{1_{now}}$ に対する攻撃

次に U_1 が U_2 に対する攻撃をする場合を考える．この場合の攻撃が成功すると，U_1 は U_2 から受け取った電子対価を持ち逃げすることができる．

かつて U_1 から U_2 の間で電子対価 n の受け渡しが成功したとする．U_2 が U_1 に電子対価を送信するプロセスを開始するのは，図 3 の　からである．　において U_1 はセッション番号 $s_{1_{now}}$ を作成するが，攻撃を成功させるためには昔のセッション番号 $s_{1_{old}}$ を最終的に受領証 R_{U_1} に U_2 に（気がつかれないように）内包させて，U_2 に渡す必要がある．

しかし 4.1 と同様に，U_2 がセッション番号の再利用をしなければ，U_1 が仮に $s_{1_{old}}$ を U_2 に対して渡すことができたとしても，かつての受領証と一致することはないので，攻撃は成功しない．

4.4 U_1 の $c_{2_{now}}$ に対する攻撃

4.2 で示した場合と同様に，$c_{2_{now}}$ が改竄された場合，プロセスの途中で U_2 は $c_{2_{now}}$ が改竄されていることに気がつき，U_2 自身の受領証を発行する前にプロセスを断つ事ができる．従って，U_1 の $c_{2_{now}}$ に対する攻撃も成り立たない．

5 まとめ

本論文では，電子権利流通方式の研究において 2 つのシステムが組み合わせた電子権利交換システムを考察することの重要性を示すために，汎用性のある代表的な方式 [4] を単独で用いた場合の安全性問題を指摘した．そこで，電子権利の譲渡と電子対価の受け取り双方に両方式を用いて，組み合わせ方を工夫した．それにより，指摘した安全性問題を解決した．

第 2 章の冒頭で触れたとおり，実用化されているものも含め，電子権利流通方式には様々なものが存在する．電子権利の譲渡に利用するシステムと電子対価の受け取りに利用するシステムの組み合わせは様々なものが考えられ，それらの組み合わせによって様々な問題が起こりうると考えられる．今後は，種々の場合の特徴をまとめ，それぞれのシステムの安全面の問題点を指摘し，改善策を提案してゆく予定である．そして可能ならば，汎用性の高い組み合わせ方を探求したい．

参考文献

[1] 中山靖司，太田和夫，松本勉：電子マネーを構成する情報セキュリティ技術と安全性評価，日本銀行金融研究所，IMES Discussion Paper Series, 98-J-26, Nov. 1998

[2] Wayner, P.:*Digital Cash,* AP Professional, Chestnut Hill, Mar.1997

[3] Mondex International: Mondex electronic cash. http://www.mondex.com/

[4] 寺田雅之，花舘蔵之，藤村孝，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，情報処理学会論文誌，Vol.42 No.8 Aug.2001

[5] Farrell, S. and Housley, R.: *An Internet Attribute Certificate Profile for Authorization,* Internet Draft, IETF PKIX Working Group 2001. draft-ieft-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] 菊池浩明，川倉康嗣：SPKI/SDSI の承認証明書のフレームワークを利用した電子学生割引証．情報処理学会研究報告，99-CSEC-5-5, pp.25–30, May 1999