M-002

利用者の利便性を考慮した匿名権利譲渡方式の提案

A Proposal of Rights Trading System Considering User's Anonymity, Fairness and Usability

廣田 啓一 † 山本 隆二 † 萬本 正儒 † 山室 雅司 †
Keiichi Hirota Ryuji Yamamoto Masanobu Manmoto Masashi Yamamuro

1. はじめに

電子チケットなどのいわゆる電子権利の流通において，譲渡の利便性と安全性の両立は重要な課題である．権利を所有し譲渡するユーザ（譲渡元ユーザ）と権利を譲り受けるユーザ（譲渡先ユーザ）の双方にとって従来手間であった権利譲渡を，電子メールや掲示板などの幅広い自由なチャネルで非同期に行う事ができれば，その利便性は高い．さらに，権利譲渡が匿名かつ安全にできれば，電子権利の転々流通の機会は飛躍的に増加し，権利流通の活性化が期待できる．

また，電子権利の流通には公平な譲渡取引を行うための明確な枠組みが必要とされている．現実世界における権利譲渡でも，対価を支払ったにも関わらず権利が譲渡されない，または権利の譲渡に対して対価が支払われないなどの違法行為や，不当な買占めと譲渡価格の吊り上げといった不正行為が横行しており，電子権利の分野でも同様の問題への対応が求められている．

本稿では，譲渡者間において匿名であって，安全かつ公平な譲渡売買を可能とする権利譲渡方式を提案する．本方式は，秘密情報の部分的な復元を可能とする復元制御型秘密分散法 [1] を応用したもので，譲渡元ユーザが作成する権利譲渡を宣言する情報（権利譲渡情報）の内，権利の識別情報と譲渡条件のみ譲渡先ユーザに復元・確認を許し，電子権利を一元的に管理する権利管理者において譲渡に必要な全情報を復元して譲渡を遂行する．

本稿では，電子チケットの譲渡を例として，提案方式の詳細とその利便性，安全性について議論する．

2. 提案プロトコルの概要

本章では，提案する権利譲渡プロトコルの概要を述べる．本プロトコルは，譲渡元ユーザにおいて権利譲渡情報を生成・分散符号化する譲渡情報生成フェーズと，譲渡先ユーザにおいて権利譲渡情報を部分的に復元・確認する譲渡情報確認フェーズと，権利管理者において権利譲渡情報を完全に復元し，譲渡処理を遂行する譲渡実行フェーズの３つのフェーズからなる（図 1）．以下，各フェーズにおける処理を順に説明する．

2.1 譲渡情報生成フェーズ

譲渡情報生成フェーズにおいて，譲渡元ユーザは権利譲渡情報を作成し，所有する権利の譲渡を宣言する．権利譲渡情報は，譲渡の対象となる権利を一意に識別する識別情報としてチケット ID，譲渡元ユーザ自身を一意に識別する認証情報としてユーザ名とパスワード，権利譲渡の条件として設定する譲渡金額などからなるものとする．この権利譲渡情報を，復元参照を許す部分情報 S_1 と

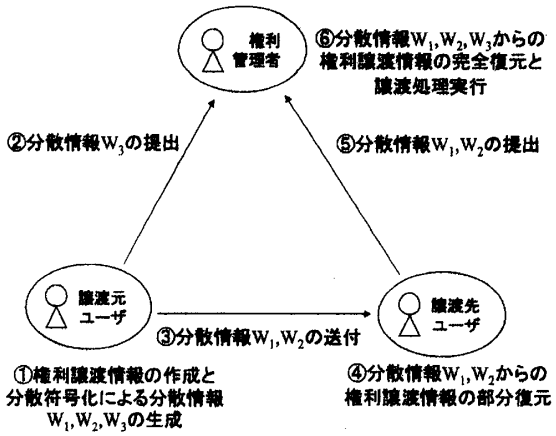

図 1: 提案プロトコルの概要

復元参照を許さない部分情報 S_2 とに分割した後，復元制御型秘密分散法により３つの分散情報 W_1，W_2，W_3 に分散符号化する．

ここで，復元制御型秘密分散法とは (k,n) 閾値秘密分散法および (d,k,n) 閾値秘密分散法 [2] を拡張したもので，特殊な分散関数を用いる事により，閾値数未満の分散情報であっても特定の組み合わせでそろった場合には $f(x)$ に関する連立方程式から特定の部分情報 S_1，S_2，$\cdots$，S_{d-1} のいずれかを算出でき，元の秘密情報 S を部分的に復元可能とする特殊な秘密分散法である．

本稿では，復元制御型の分散関数 $f(x)$ の例として，

$$f(x) = S_1 + S_2(x-7) + R(x-1)(x-5) \pmod{P} \quad (1)$$

を用いる．本分散関数は，$f(3)$ と $f(4)$ から S_1 が，$f(2)$ と $f(4)$ から S_2 がそれぞれ部分的に復元可能であって，任意の３つの分散情報からは秘密情報 S が完全に復元可能となる分散関数である．ただし，個々の分散情報 $f(2)$，$f(3)$，$f(4)$ からは元となる部分情報 S_1，S_2 および乱数 R を導出する事は全くできない．

譲渡元ユーザは，本分散関数 $f(x)$ により，部分情報 S_1，S_2 および任意の乱数 R から，３つの分散情報を $W_1 = f(3)$，$W_2 = f(4)$，$W_3 = f(6)$ として生成する．

$$\left.\begin{aligned} W_1 &= f(3) = S_1 - 4S_2 - 4R \\ W_2 &= f(4) = S_1 - 3S_2 - 3R \\ W_3 &= f(6) = S_1 - S_2 + 5R \end{aligned}\right\} \pmod{P} \quad (2)$$

生成した分散情報は，W_3 を権利管理者に，W_1 と W_2 を譲渡先ユーザにそれぞれ送付する．権利管理者は譲渡元ユーザの認証を行い，送付された分散情報 W_3 を例えば譲渡対象のチケット ID と関連付けて記録しておく．

† 日本電信電話株式会社 サイバースペース研究所

2.2 譲渡情報確認フェーズ

譲渡元ユーザが作成した分散情報 W_1, W_2 を入手した譲渡先ユーザは，分散情報から権利譲渡情報の復元を試みる事ができる．入手した分散情報は閾値よりも少ないため，権利譲渡情報の完全な復元はできないが，前述したように復元制御型秘密分散法により部分情報 S_1 すなわちチケットIDと譲渡金額を部分的に復元できる．

分散情報 W_1 と W_2 からの部分情報 S_1 の算出は容易で，分散情報の計算式 (2) より次のように求められる．

$$S_1 = 4W_3 - 3W_2 \pmod{P} \qquad (3)$$

一方，部分情報 S_2 については $S_2 + R = W_2 - W_1$ という関係式しか得られず，R が任意の乱数であるため S_2 を求める事は全くできない．したがって，譲渡先ユーザはチケットIDと譲渡金額のみ復元・確認でき，部分情報 S_2 すなわち譲渡元ユーザのユーザIDとパスワードは復元できないため，譲渡元ユーザの匿名性が保たれる．

S_1 の復元により譲渡対象の権利と対価である譲渡金額を確認・了承した譲渡先ユーザは，分散情報 W_1, W_2 を権利管理者に提出して権利の譲渡実行を依頼する事ができる．譲渡金額を了承しない場合には，譲渡プロトコルを放棄しても良いし，逆に自分の希望する譲渡金額による権利譲渡情報を作成して，再度譲渡プロトコルを譲渡元ユーザから実行する事もできる．いずれの場合も譲渡先ユーザは譲渡元ユーザに自分の認証情報を教える必要はなく，譲渡先ユーザの匿名性が保たれる．

2.3 譲渡遂行フェーズ

譲渡先ユーザから分散情報 W_1, W_2 の提出と譲渡実行依頼を受けた権利管理者は，まず権利譲渡情報の部分復元を行い，同様に譲渡対象のチケットIDと譲渡金額を復元する．次にチケットIDと関連付けて記録された，譲渡元ユーザの作成した分散情報 W_3 を取得し，全ての分散情報を元に権利譲渡情報の完全復元を行う．

分散情報の計算式 (2) より同様にして部分情報 S_2 を次の式で求める事ができる．

$$S_2 = \frac{1}{6}\{-8W_1 + 9W_2 - W_3\} \pmod{P} \qquad (4)$$

部分情報 S_2 は譲渡元ユーザのユーザIDとパスワードからなるため，権利管理者はチケットIDに関連付けられた権利所有者のユーザIDとパスワードによる認証を行い，認証が成立した場合には正当な権利所有者による権利譲渡の承認が確認できたものとして，譲渡先ユーザから譲渡元ユーザへの譲渡金額分の対価の支払いを代行し，該当する権利の所有者を譲渡先ユーザへと書き換える．以上の手続きにより権利の譲渡が遂行される．

なお，譲渡先ユーザが分散情報 W_1, W_2 を改ざんして譲渡金額の書き換えなどを行った場合，認証に失敗する事から権利は譲渡されず，譲渡の安全性が保証される．

3. 関連研究

本提案方式はいわゆる口座型の権利管理である．口座型の権利管理とは，電子権利を一意に表す識別情報と，電子権利の所有者を一意に表す認証情報とをサーバ上で管理するもので，権利の行使および譲渡を集中管理する事により，二重譲渡や二重使用を防止でき，公平な権利譲渡が実現できる．口座型における権利の譲渡方式として，例えば公開鍵暗号を用いた方式 [3] がある．公開鍵を用いた権利譲渡の場合，鍵情報や譲渡情報の交換などプロトコルが煩雑であり，また各ユーザが公開鍵と秘密鍵のペアを取得管理する必要がある事から利便性は低い．また，公開鍵暗号の安全性は計算量的安全性であり，総当りによる解読が必ずしも不可能ではない事から安全性の面で若干問題があると考えられる．

一方，電子権利自体を表す情報をICカードや携帯電話などの個人端末に蓄積する価値蓄積型の権利管理においても，幾つかの権利譲渡方式が提案されている．文献 [4] は，公開鍵暗号と電子署名およびハッシュ関数を用いて，端末間での権利譲渡を実現している．文献 [5] は，秘密分散法を用いて権利譲渡を実現しているが，分散符号化した権利情報自体を複数回に分けて送付するものであり，部分復元を用いた本提案方式とは用法が異なる．いずれの譲渡方式も複数回のトランザクションと検証を必要とするため処理が煩雑であり，非同期での権利譲渡には適していない．

本稿にて提案する権利譲渡方式は，各参加者が１回の処理でプロトコルを実行でき，かつ譲渡情報の匿名性および改ざんなどに対する安全性が保証される事から，任意のチャネルでの非同期な権利譲渡に適している．また，本方式は秘密分散法を用いているため情報量的安全性が保証され，ユーザ固有の鍵情報の取得・管理を特に必要としない．これらの点から，本方式は利用者にとって利便性が高い譲渡方式であると言える．

4. おわりに

本稿では，譲渡者間において匿名で，安全かつ公平な権利譲渡プロトコルの提案を行った．本プロトコルは情報量的に安全であり，かつ権利譲渡情報の改ざんが不可能な事から，掲示板やチャットといった任意の流通チャネル上での権利譲渡や譲渡者間での譲渡条件の交渉を可能とし，利用者の利便性が高い．また，口座型の権利管理であるため権利譲渡の公平性も保証する事ができる．

参考文献

[1] 廣田啓一, 北原亮, 遠藤雅和, 山室雅司: ランプ型閾値秘密分散法における部分情報の復元制御, 信学技報, Vol. 103, No. 416, pp. 57–64 (2003).

[2] 尾形わかは, 黒沢馨: 秘密分散共有法とその応用, 信学誌, Vol. 82, No. 12, pp. 1228–1236 (1999).

[3] Matsuyama, K. and Fujimura, K.: Distributed Digital-Ticket Management for Rights Trading System, *Proc. 1st ACM Conference on Electronic Commerce*, pp.110–118, ACM (1999).

[4] 寺田雅之, 花舘蔵之, 藤村考, 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, 情処論, Vol.42, No.8, pp.2017–2029 (2001).

[5] 小川博久: ユビキタス環境における権利回数制限の実装及び評価, 情処研報, 2004-UBI-3, pp.49–54 (2004).