情報処理学会論文誌 Vol. 49 No. 7 2382–2391 (July 2008)

ブローカ仲介モデルによるC2B2C権利交換プロトコルと権利流通システムの設計

廣田 啓一[†1] 曽根原 登[†2]

電子権利の流通，特にC2C間での権利と対価の交換を考えた場合，技術的な観点から強い安全性と高い利便性の両立が権利交換プロトコルには求められる．一方，経済的な観点からは，取引機会の増加が市場発展の重要な要素の1つである．従来のC2C型の権利流通は必ずしもユーザにとって便利ではなく，取引機会の創出のために権利の買い手の探索および対価と支払方法の交渉に多くのトランザクションを必要とするという問題がある．一方オークションのようなC2B2C型の権利流通では，ビジネスプレーヤの介在によりユーザのコストが軽減されるが，その反面市場が限定的かつ排他的になり，取引機会が減少する場合がある．我々は，オークションとは異なるC2B2C型の権利流通として，ユーザが権利取引をブローカに預託し，ブローカが取引機会を増加させる，ブローカ仲介モデルに着目し，C2B2C権利交換プロトコルと，それを用いた権利流通システムを検討した．提案システムは権利取引の機密性と完全性を満たし，かつトランザクションの最少性，非同期性といった効率性の良い機能を提供することから，取引機会の増加による市場発展が期待できる．本稿では，提案プロトコルおよびシステムの概要を示し，その安全性と利便性について述べる．

C2B2C Rights Trading Protocol and System Design for Broker Mediated Market Model

Keiichi Hirota[†1] and Noboru Sonehara[†2]

Considering electronic rights trading, especially C2C trading in which rights and values are exchanged among users, high usability and strong security are required to the rights trading system. From viewpoint of economics, the increase of trading opportunity is also one of the important factors for market development. C2C trading is not so efficient for users because it needs a lot of transactions for search and negotiation. C2B2C model like auctions held by business player helps to reduce such costs and efforts, but market may become limitative and exclusive so the trading opportunity will decrease. We focused on C2B2C model, broker-mediated market, different with auction models and designed secure C2B2C rights trading protocol and system. It enables users the safe and secure deposit of trading information to brokers. From results of security and usability analysis, we consider our system is effective to increase the trading opportunity. It achieves strong confidentiality and integrity of trading, and also provides efficiency from minimality and asynchronicity of transactions. In this paper, we first describe C2B2C rights trading protocol and rights trading system design, and then discuss its security and usability.

1. はじめに

近年，電子商取引の1つである電子チケットや電子マネーといった電子的な権利の流通市場が急速に拡大しつつある．電子権利の普及は著しく，たとえば劇場や映画館などのチケット，航空券といった身近なものから，株券，債権や不動産登記といった資産価値の高い権利まで，様々な分野に広がりを見せている．こうした動きにともなって，ユーザ間での権利流通，すなわち二次流通を実現するシステムがすでにいくつか提案されている[1)–3)]．技術的な観点から，強い安全性と高い利便性の両立が権利流通システムには求められる．しかしながら，経済的な観点からいえば，取引機会の増加もまた市場発展のための重要な要素の1つである．

従来の権利交換プロトコル[4)–8)]は安全なC2C[⋆1]取引の実現のために設計されてきたが，利用者にとっての利便性[9),11)]や取引機会の創出あるいは増加といった要素はあまり考慮されていなかった．実際問題として，C2C取引はユーザにとってあまり便利なものではなく，取引の対象となる相手を見つけ，取引価格や支払方法などを交渉するために多くのトランザクションを必要とする．一方，オークションや取引掲示板などのC2B2C[⋆2]型のサービスはユーザのそうしたコストを軽減させる[12),13)]が，単一の場で提供されるサービスのため市場が限定的かつ排他的になり，また市場内で競合が起こる場合もあるため．結果として取引機会の減少につながることも多い．

我々は，オークションとは異なるC2B2C型の市場モデルとしてブローカ仲介モデルに着目し，C2B2C権利交換プロトコルと，それを用いた権利流通システムの設計を検討した．

†1 日本電信電話株式会社 NTT 情報流通プラットフォーム研究所
NTT Information Sharing Platform Laboratories, NTT Corporation
†2 独立行政法人国立情報学研究所
National Institute of Informatics
⋆1 Consumer to Consumer
⋆2 Consumer to Business to Consumer

ブローカ仲介モデルは，ユーザが所有する権利の取引をブローカに預託し，ブローカが取引機会を最大化するための販促活動を行うもので，権利取引が成立した場合に利益が売り手とブローカの双方に分配されるインセンティブベースの市場を形成する．提案システムは権利取引の機密性と完全性を満たし，かつトランザクションの最少性，非同期性といった効率性の良い機能をユーザおよびブローカに提供することから，取引機会の増加による市場発展が期待できる．

本稿では，提案する C2B2C 権利交換プロトコルおよび権利流通システムの概要を示し，その安全性と利便性について述べる．まず 2 章で権利の二次流通市場の概要と要件定義を示し，3 章において権利交換プロトコルの概要を示す．次いで 4 章に権利流通システムの構成を示し，売り手，買い手，権利管理機関およびブローカの各プレイヤにおける処理とトランザクションを記述する．5 章において提案システムの安全性と利便性について議論し，6 章でまとめを述べる．

2. C2B2C 型市場モデルの分析

権利の二次流通市場とは，一般のユーザが所有する権利を他のユーザの持つ対価と取引するための場である．二次流通の市場モデルには大きく分けて C2C 型と C2B2C 型の 2 つがある[13),18)]．

C2C 型の権利流通はユーザ同士が直接取引を行うもので，その意味では 1 つの形態しかない．権利を売りたい売り手と，買いたい買い手の双方が存在し，取引の合意が成立したときに，直接的な権利交換プロトコルがユーザ間で実行される．安全な C2C 間での取引を実現する権利交換プロトコルはこれまで多数提案されているが，こうしたプロトコルのほとんどは権利交換そのものを行うためのものであって，権利取引のために必要な処理は考慮されていない．したがって，ユーザはまず取引相手となる権利の買い手を見つけなければならず，また何を対価として権利交換を行うかを買い手と合意しなければならない．そうした探索処理や取引価格および支払方法の交渉などに多くのトランザクションを必要とするため，ユーザにとってあまり便利なものではない．また，権利交換の公平性[4)]を実現するために，プロトコルの多くが複雑なトランザクションで構成され，同期的な処理が必要となっている．こうしたプロトコルの煩雑さはユーザの利便性を損ねるだけでなく，取引機会の損失にもつながり，流通市場の発展を促すことは難しい．

一方の C2B2C 型の権利流通は，売り手と買い手の間にビジネスプレイヤが介在し，取引を管理する三者モデルである．ビジネスプレイヤがどういう機能を提供するかによって，いくつかのバリエーションがある．

まず，典型的な C2B2C 型の市場としてオークションがあげられる．オークションは，運営企業が売り手と買い手のためのオークションサイトを開設し，権利を売りたいユーザが売り希望を作成してサイトに投稿すると，掲載された売り希望に対して複数のユーザがより高い価格を入札していき，最終的に最も高い価格を入札したユーザが買い手となる仕組みである．オークションは探索と交渉および取引にかかるユーザのコストを軽減させ，売り手にとっては買い手が多ければより高い利益を得ることができるというメリットがある．その反面，サービスが単一の場でのみ提供されるため，市場が得てして限定的かつ排他的になりやすく，結果として市場内での競合が起こり，逆に取引機会が減少することも考えられる．

企業によるリセールもまた C2B2C 型の市場モデルである．この形態は，運営企業がユーザから権利を買い戻した後に，他のユーザに対して再販するもので，売り手となるユーザは確実に取引が成立するというメリットがある．しかし，ユーザにとっては，取引機会は保証されるものの，手数料などで通常の価格よりも安く買い戻されることが多いため，利益を得られることはなく，デメリットの方が大きいと考えられる．さらに，リセールモデルでは，権利交換プロトコルが売り手から企業へと，企業から買い手への 2 回実行される必要があるため，取引効率が良くない．また，企業は買い戻しのための費用や在庫管理などのコストがかかり，買い戻した権利が売れ残る損失リスクもある．したがって，この形態の取引を行う企業は実際にはあまり存在しない．

我々が着目した C2B2C 型の市場モデルは，ブローカ仲介モデルである．ブローカ仲介モデルでは，権利を売りたいユーザが売り希望を作成してブローカに預託し，ブローカが取引機会を最大化するための販促活動を行う．リセールモデルと異なりユーザが希望する価格を設定できるため，ユーザの利益が保証される．また，取引が成立すると，利益は売り手であるユーザとブローカの双方に分配されるため，一種のインセンティブベースの市場として機能し，取引機会の増加が期待できる．ブローカ市場ではユーザのコストが低減され，またリソース集中の結果としてブローカのコストも比較的低く抑えられる．

なお，売り手と買い手の間に第三者が仲介する異なる市場モデルとして，アフィリエイトがある．一般ユーザが企業の商品などを他のユーザに対してプロモートし，商品が売れた場合に一定の利益を得る仕組みである．このモデルは本来 B2C2C 型のモデルであるため一概には比較できないが，ブローカの介在による取引機会の増加の有効性は広く認知され，実際にシステム運用されている．

二次流通の市場モデルについての簡単な比較を**表 1** にまとめた．C2B2C 型のブローカ仲

介モデルは，権利取引にかかるユーザのコストを軽減させるだけでなく，ユーザの利益を保証したまま取引機会を増加させるため，権利の二次流通市場として良い市場を形成することが期待できる．

現在，実社会においてシステム化され，最も用いられている市場モデルは，オークションである．しかしながら，前述したようにオークションは取引の価格と相手を決定するためのものであり，実際の取引にはユーザ間で C2C 型の権利交換プロトコルを実行する必要がある．ユーザ同士が対面しての直接交換は現実的ではなく，ネットを介した交換あるいは郵送による間接交換がほとんどだが，その際に口座番号や住所・氏名などの個人情報の交換が必要となる場合が多いため，心理的抵抗感が強く，普及の 1 つの阻害要因となっている．また，間接交換では権利と対価を同時にかつ公平に交換することは難しいため，受取り否認や不払いといった詐欺行為が発生しやすく，社会的な問題となっている．最近になって，運営企業が仲介することでユーザ間での情報交換を不要とするエスクローサービスが提供され始めたが，取引の完了に時間がかかるため，普及するに至っていない．

リセールモデルをシステム化したサービスもいくつか存在する[14),15)]．ただし，前述したように企業のコスト負担が大きいため，リセールモデルの対象となる権利は限定される．たとえば MLB（Major League Baseball）の場合，シーズンチケットのような元々単価の低い権利を買い戻し，通常のチケットよりも安い価格で再販することで，利益をあげるビジネスモデルとなっている．

一方，取引掲示板などの形で第三者が権利取引の仲介を行うサービスは従来から数多く存在し，一種のブローカ仲介モデルを形成していて，利用者も多い．しかし，こうしたサービスはシステム化されたものではなく，オークションと同様に，取引の合意が成立した後にユーザ間で C2C 型の権利交換を実行する必要があるため，様々な問題が生じることがある．また，実社会ではチケットショップなどユーザから預託された権利の販売を行うサービスが普及しているが，電子商取引の世界ではまだそのようなサービスは存在していない．

表 1　二次流通の市場モデル
Table 1　Models of secondary market service.

市場モデル		ユーザコスト	ユーザ利益	取引機会
C2C	—	×	○	×
C2B2C	オークション	△	◎	△
	リセール	○	×	○
	ブローカ仲介	○	○	◎
B2C2C	アフィリエイト	—	—	◎

ユーザが安心かつ安全にブローカに権利取引を預託できる権利流通システムを実現できれば，電子商取引市場に大きなインパクトを与える可能性がある．我々は，こうした分析からブローカ仲介モデルの二次流通市場に焦点を当てて，第三者に預託可能な C2B2C 権利交換プロトコルを提案し，セキュアな権利流通システムの設計を行った．

3. ブローカ仲介モデルによる C2B2C 権利交換プロトコル

3.1 提案プロトコルの概要

まず最初に，本稿で提案する C2B2C 権利交換プロトコルの概要を示す．提案プロトコルは情報量的な安全性を持つ匿名権利交換プロトコル[16)] の拡張で，権利取引の申し出となる情報を第三者に安全に預託することを可能とし，非同期かつ最少のトランザクション回数で権利と対価の交換を実現することができる．安全性についての議論は 5 章で行う．

提案プロトコルの概要を**図 1** に示す．本プロトコルは，ユーザが初期登録を行う登録フェーズと，以降任意の時点で権利の取引を行う取引フェーズとに分かれる．さらに取引フェーズは，売り手による取引情報の生成と分散によるブローカへの預託（1a〜1c），買い手による部分復元と同意に基づく執行依頼（2a〜2c），そして権利管理機関による完全復元と執行（3）の 3 つのステップからなる．なお，登録フェーズにおいて，売り手となるユーザはあらかじめ自分の個人情報とユーザ個別鍵 K_U を権利管理機関に登録し，認証情報としてユーザ ID とパスワードを取得しているものとする．

以下，取引フェーズの各ステップについて，詳細を説明する．

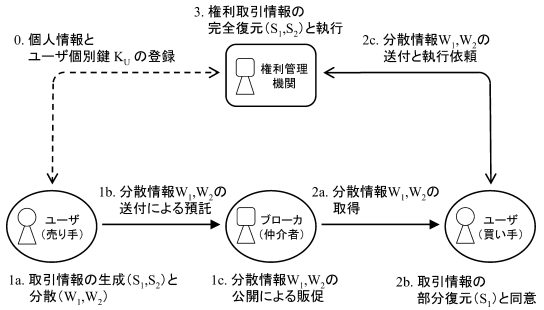

図 1　C2B2C 権利交換プロトコルの概要
Fig. 1　Overview of C2B2C rights trading protocol.

図 2　チケット取引情報の構成例
Fig. 2　Constitution example of ticket trading information.

3.1.1　取引情報の生成と分散

売り手はまず最初に所有する権利の取引を宣言する取引情報を生成する．取引情報は，誰でも復元可能な開示情報である S_1 と，権利管理機関だけが復元可能な非開示情報である S_2 とからなる．本稿における取引情報の例として，後に 4 章で述べるチケット取引情報の構成例を**図 2** に示す．開示情報 S_1 は，たとえば売買の対象となる権利を一意に特定する識別情報（チケット ID），売り手が指定する権利の希望対価，取引情報の有効期限，預託先を一意に特定する識別情報（ブローカ ID）および権利管理機関において復元処理のために用いられる一時情報 K_T などから構成される．一時情報 K_T は，取引の時点で任意に生成した情報でよく，たとえば取引情報を生成した時刻情報やシーケンシャルな番号を用いることができる．一方の非開示情報 S_2 は，売り手であるユーザを一意に特定する認証情報（ユーザ ID，パスワード），および S_1 の検証のために用いられる，S_1 とユーザ個別鍵 K_U とを連結した値のハッシュ値などから構成される．なお，ここで示した取引情報の構成は限定的なものではなく，S_1 および S_2 ともに上に示した以外の情報を含んでいてもかまわない．

次に，売り手はユーザ個別鍵 K_U と一時情報 K_T とを用いて，売り手と権利管理機関だけが生成することのできる共通分散情報 W_C を算出する．W_C の計算方法は特に限定されるものではないが，本稿では次のように定める．

$$W_C = K_U \times K_T \pmod{P}^{\star 1} \tag{1}$$

その後，売り手は W_C と $(2,3,n)$ 復元制御型秘密分散法[19] に基づく多項式関数 $f(x)$ を使って，S_1 と S_2 からなる取引情報を 1 組の分散情報 W_1 と W_2 に分散符号化する．復元制御型秘密分散法とは閾値秘密分散法[20] およびランプ型秘密分散法[21] を拡張したもので，多項式関数 $f(x)$ を使って生成した n 個の分散情報のうち，閾値 k 個以上から元の秘密情報を復元可能とし，k 個未満の分散情報からは秘密情報を復元することができない．しかしながら，閾値 k 個未満であっても特定の分散情報の組合せからは元の秘密情報の一部分を一意に復元できる性質を持つ．この性質をうまく利用すると，分散情報の組合せを使った秘密情報の開示制御が実現できる．本稿では，$f(x)$ として以下の式を使用する．

$$f(x) = S_1 + S_2(x-7) + R(x-1)(x-5) \tag{2}$$

この関数 $f(x)$ を使って生成された分散情報からは，たとえば $W_1 = f(3)$ と $W_2 = f(4)$ の組から S_1 が，$W_2 = f(4)$ と $W_3 = f(2)$ の組から S_2 がそれぞれ復元可能である．また 3 つ以上の任意の分散情報の組合せから S_1 と S_2 の両方が復元可能となる．しかしながら，個々の分散情報からは S_1，S_2 および R に関するいかなる情報も推定することはできない．

売り手は式 (1) で決定した共通分散情報 W_C の値を使って，関数 $f(x)$ 中の乱数 R の値を算出する．このとき，$W_C = f(I)$ の引数となる変数 I も同様に W_C の値から決定する．ここでは例として $I = 6$ と決定したものとして，以下の式により R を計算する．

$$W_C = f(6) = S_1 - S_2 + 5R \tag{3}$$

$$R = \frac{W_C - S_1 + S_2}{5} \tag{4}$$

最終的に S_1，S_2 および求めた R の値を関数 $f(x)$ に代入して，1 組の分散情報 $W_1 = f(3)$ と $W_2 = f(4)$ を生成する．

$$\left.\begin{aligned} W_1 &= f(3) = S_1 - 4S_2 - 4R \\ W_2 &= f(4) = S_1 - 3S_2 - 3R \end{aligned}\right\} \tag{5}$$

この W_1 と W_2 を仲介者となるブローカに対して送信することで，売り手による権利取引の預託が成立する．ブローカは預託された分散情報 W_1，W_2 について，買い手となるユーザに対する販促活動を行う．

3.1.2　取引情報の部分復元と同意

売り手ユーザからの預託を受けたブローカ，およびブローカから 1 組の分散情報 W_1，W_2 を取得した買い手となるユーザは，取引情報の一部である復元可能な開示情報 S_1 を部分復元し，取引の対象となる権利についての情報や売り手の希望する対価，有効期限などを確認することができる．開示情報 S_1 は，分散情報 W_1 と W_2 から以下に示す式で簡単に求められる．

$$S_1 = 4W_2 - 3W_1 \tag{6}$$

買い手となるユーザが取引の申し出に同意し，権利を購入する場合には，売り手から受け取った 1 組の分散情報 W_1 と W_2 を権利管理機関に送信し，権利取引の執行を依頼する．取引に同意しない場合は分散情報を廃棄して，プロトコルを終了してよい．

⋆1 P は S_1 および S_2 よりも大きな素数とする．以下，すべての式は有限体 Z_P 上で計算されるが，簡単のため記述を省略する．

なお，分散情報の組を取得したユーザが非開示情報 S_2 を復元することは情報量的に不可能である．分散情報の組を表す式 (5) からは乱数 R と S_2 の関係を表す式 (7) しか導くことができないため，S_2 の値は決定できず，したがって権利管理機関を除く第三者が非開示情報 S_2 に含まれる売り手の認証情報などを得ることはできない．

$$S_2 = W_2 - W_1 - R \tag{7}$$

3.1.3　取引情報の完全復元と執行

買い手となるユーザから権利取引の執行依頼を受けた権利管理機関は，式 (6) により同様に開示情報 S_1 を部分復元し，取引の対象となる権利の識別情報，希望対価，および一時情報 K_T などを取り出す．

次いで，権利管理機関は権利を所有する売り手ユーザの個別ユーザ鍵 K_U を取得し，K_U と K_T から式 (1) により共通分散情報 W_C を算出する．最終的に，権利管理機関はすべての分散情報 W_1，W_2 と W_C を得るため，取引情報の一部である非開示情報 S_2 を復元することができる．S_2 は 3 つの分散情報についての連立方程式を解くことで算出できる．本稿の例では，式 (3) と式 (5) から，以下の式により求められる．

$$S_2 = \frac{-8W_1 + 9W_2 - W_C}{6} \tag{8}$$

非開示情報 S_2 は売り手の認証情報であるユーザ ID とパスワードを含むため，権利管理機関は権利の所有者情報と照合することで，取引情報の有効性を検証できる．また，S_1 とユーザ個別鍵 K_U とを連結した値のハッシュ値から，S_1 が改竄されていないことを検証できる．復元した取引情報が有効である場合には，対象となる権利の対価の支払いを買い手から受け，権利の所有者を売り手から買い手に変更する．これにより，権利の取引が完了する．

3.2　関連研究との比較

第三者への預託を可能とする権利交換方式を実現する試みとして，久野らの方式[9] がある．久野らは本来 C2C 型である権利交換方式[6),10)] の拡張として，交換対象の権利を示すトークンとトークンの利用権とを分離し，トークンのみを第三者に預託し，利用権はユーザ間で直接送付することにより，安全な預託を可能とした．しかしながら，この方式では預託されたトークンの譲渡と利用権の譲渡とが分離しているため，多くのトランザクションが必要であり，かつ利用権に関しては売り手と買い手の間で直接的な譲渡プロトコルを行うため，部分的には C2C 型のプロトコルである．また，権利の譲渡に対する対価の支払いについては言及されておらず，権利交換の公平性は考慮されていない．

一方，権利取引の際の対価を第三者に預託する試みとして，千田らの方式[17] がある．千田らは電子入札を対象として，買い手となるユーザが電子マネーを供託機関に預託し，取引が成立した場合にのみ清算を行う方式を，離散対数問題に基づいて実現した．しかしながら，取引成立時の没収プロトコルや落札証明書の交換プロトコル，不成立時の返還プロトコルなど，複数の処理およびトランザクションが必要であり，多くのべき乗演算を要するため計算量が大きい．また，この方式は離散対数問題に基づくもので，その安全性は計算量的である．

提案プロトコルは，ブローカと買い手ユーザとの間での販促に関するトランザクションを除けば，売り手ユーザからブローカへの分散情報の送付による預託と，買い手ユーザから権利管理機関への分散情報の送付による取引執行のただ 2 回のトランザクションで権利交換を完了することができる．また，これらのトランザクションはそれぞれ非同期に実行でき，かつ買い手ユーザが権利管理機関に対価を支払った時点で権利が譲渡されるため，公平かつ即時的な取引が可能である．このように，本プロトコルはユーザの利便性と取引効率の向上を重視して実現されている．また，本プロトコルは秘密分散法を基にしたもので，情報量的な安全性を有する．

4.　権利流通システムの設計

本章では，提案プロトコルを用いた権利流通システムの構成とその処理概要を示す．なお，説明のために以下では流通対象である権利を電子チケットに限定し，チケット管理センタ（Ticket Management Center，以下 TMC），ブローカ，売り手および買い手の 4 種類のプレイヤから構成される，電子チケットの二次流通市場を想定する．権利流通システムの構成を**図 3** に示す．

TMC は管理サーバを有し，ユーザおよびブローカの登録・認証と，電子チケットの発行・使用・取引の管理を行う．ユーザはまず個人情報とユーザ個別鍵 K_U を管理サーバに登録し，認証情報としてユーザ ID とパスワードの発行を受け，ユーザクライアントを取得する．

ユーザがチケットを購入すると，管理サーバは対応するチケット ID とユーザ ID の組を所有者情報としてチケット管理 DB に記録する．ユーザがチケットを使用する場合，所有者としての認証処理に成功することでチケットが示す権利を行使できる．使用されたチケットに関する記録はチケット管理 DB から消去あるいは使用済みチケットの管理 DB に移行される．これが一般的な電子チケットの一次流通における処理である．

一方，ユーザが購入したチケットを他のユーザに譲渡あるいは売買する場合に，C2B2C 権利交換プロトコルに基づく処理が実行される．取引が完了すると，管理 DB 上の所有者情報が売り手のユーザ ID から買い手のユーザ ID に書き換えられる．これにより新しい所有

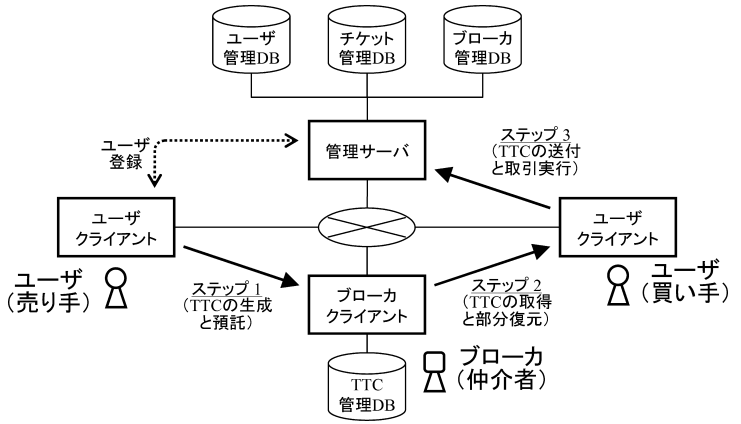

図 3　権利流通システムの構成
Fig. 3　Overview of rights trading system.

者がチケットを使用，または譲渡売買する権利を持つようになる．これを二次流通という．

ブローカもまた同様の登録処理を行って，ブローカ ID とパスワードの発行を受け，ブローカクライアントを取得する．ブローカは売り手ユーザからチケット取引の預託を受け，買い手となるユーザに対して販促を行う．取引が完了すると，ブローカは TMC から利益の分配を受けることができる．

以下，各プレイヤにおける機能と処理の概要を簡単に説明する．

4.1　売り手のユーザ・クライアントにおける処理

売り手ユーザが所有するチケットを売りたいとき，ユーザ・クライアントを用いてまず最初にチケット取引情報（Ticket Trading Information，以下 TTI）を構成し，TTI を分散符号化したチケット取引コード（Ticket Trading Code，以下 TTC）を生成して，任意のブローカに預託する．

TTI は誰でも復元可能な開示情報 S_1 と，TMC だけが復元可能な非開示情報 S_2 とから構成される（図 2）．ユーザ・クライアントは，取引対象のチケットの指定，所有者の希望対価の設定，預託先ブローカの選択，有効期限などの設定をユーザ・インタフェースとして提供し，あわせて一時情報 K_T を生成して，S_1 を構築する．同様に，売り手ユーザの認証情報であるユーザ ID，パスワードおよびユーザ個別鍵 K_U の入力を受け付けて，S_1 とユーザ個別鍵 K_U を連結した値のハッシュ値を計算し，S_2 を構築する．

提案プロトコルのステップ 1（3.1.1 項）に基づき，クライアントは TTI の分散符号化によりできる 1 組の分散情報 W_1，W_2 を連結して TTC を生成し，預託先ブローカの有するブローカ・クライアントに送信する．これにより，売り手ユーザによるチケット取引のブローカへの預託が成立する．

4.2　ブローカ・クライアントにおける処理

TTC の送信を受けたブローカ・クライアントは，ステップ 2（3.1.2 項）に基づき，TTI の一部である開示情報 S_1 を部分復元し，記されたブローカ ID と有効期限の妥当性を検証する．次に，チケット ID を使って管理サーバからチケット情報を取得し，預託を受けたブローカが TTC を販促するために必要な情報を提供する．

ブローカは取引機会を最大化するための販促に任意のチャネルを使うことができる．単に TTC と関連情報をサイトや blog，BBS，チャットといった場に公開するだけでもよいし，電子メールやメーリングリストなどの手段で顧客ユーザに直接送付することもできる．ブローカは複数の売り手の TTC を集約して販促を行うため，効率的なプロモートができる．

4.3　買い手のユーザ・クライアントにおける処理

TTC をブローカから取得した買い手ユーザは，ユーザ・クライアントを用いて TTC の処理を行う．ユーザ・クライアントはブローカ・クライアントと同様，ステップ 2（3.1.2 項）に基づいて，開示情報 S_1 を部分復元してチケット ID や希望対価などを抽出し，必要に応じて管理サーバからチケット情報を取得して，ユーザに提示し，購入判断を促す．ユーザがチケット取引に同意する場合は，TTC を管理サーバに対して送信し，取引執行を依頼する．取引執行に際しては，ユーザ・クライアントを介して買い手ユーザの認証処理および対価の決済処理を行う．ユーザが同意しない場合は単に TTC を廃棄するか，あるいは保管しておくかを選択することができる．また，ユーザは複数のブローカから提供される任意の TTC を選択することができる．

4.4　管理サーバにおける処理

ユーザ・クライアントから TTC の送付と執行依頼を受けた管理サーバは，ステップ 3（3.1.3 項）に基づいて，TTC から開示情報 S_1 を部分復元し，チケット ID，希望対価，有効期限，一時情報 K_T などを抽出する．次に管理サーバはチケット ID と関連付けて記録された所有者のユーザ ID をチケット管理 DB から取得し，ユーザ ID に対応する個別ユーザ鍵 K_U をユーザ管理 DB から取得して K_U と K_T から共通分散情報 W_C を算出し，非開示情報 S_2 を復元して，TTI を完全に復元する．

管理サーバは TTC の有効期限を確認し，S_2 に含まれる売り手のユーザ ID とパスワード

をチケット管理 DB およびユーザ管理 DB に記録されたチケットの所有者情報と照合する．また，S_2 に含まれるハッシュ値から，S_1 に対する改竄の有無を検査する．問題がなければ管理サーバは TTI を有効であると見なし，買い手の認証処理および対価の決済処理を実行する．そして，チケット管理 DB 上の所有者情報を売り手のユーザ ID から買い手のユーザ ID に書き換え，チケット取引を執行する．

取引が完了すると，S_1 に記述されたブローカ ID および対価に基づいて，成功報酬がブローカに支払われる．

4.5　TTC のマネージメント

売り手により生成され，預託された TTC は，ブローカの手で二次流通市場に広められる．したがって，売り手とブローカの双方が TTC のライフサイクルに責任を持ち，管理しなければならない．本システムでは，以下のような管理機能を提供する．

4.5.1　ブローカ・クライアントにおける管理機能

ブローカは預託されたすべての TTC に対して責任を有する．取引が完了するか，S_1 に記された有効期限が過ぎると，TTC は無効となる．したがって，ブローカ・クライアントは所有する TTC の有効期限を管理し，必要に応じて TTC の有効性を管理サーバに問い合わせる機能を有する．一方の管理サーバは，TTC の有効性をチェックする機能を有する．また，取引成立後は，ブローカのサイトや掲示板などに該当取引の終了通知を掲載することが望ましい．

4.5.2　ユーザ・クライアントにおける管理機能

売り手ユーザは，自分が預託した TTC について，取引のキャンセルおよび取引条件の変更が可能であり，また複数の異なる取引条件を設定することもできる．

取引のキャンセル　売り手がチケット取引を中止する場合，まだ取引が成立していなければ TMC に申請して TTC を無効化できる．ユーザ・クライアントは TTI の構築時に用いた一時情報 K_T を記録管理し，キャンセル時には管理サーバによる認証を受けて，この情報を登録する．管理サーバは登録された一時情報を無効化のための情報として使い，TTC が送付されたときに復元した一時情報との照合を行って，無効化されているかどうかの判定を行う．これによりキャンセル後の取引は実行されない．

取引条件の変更　チケット取引の有効期限や希望価格などを変更したい場合，上記の手順により古い TTC を無効化したうえで，新たな TTC を生成してブローカに預託すればよい．無効化された古い TTC はブローカ・クライアントあるいは管理サーバが適切な処理を行う．

複数取引条件の設定　売り手は 1 つのチケットに対して複数の取引条件を設定することもできる．すなわち有効期間や取引価格，ブローカ ID などの異なる TTI を複数構築し，異なる TTC を生成して複数ブローカに預託できる．ただし，生成した TTC のうち有効なのは，最初に TMC に持ち込まれて取引が成立した TTC だけである．1 度取引が成立すると他の TTC はすべて無効となり，ブローカの管理の下に処理される．

5.　安全性と利便性の評価

5.1　安　全　性

提案した権利流通システムは，C2B2C 型のブローカ仲介モデルに基づく．ブローカは売り手が生成した TTC の預託を受け，TTC を一定の期間掲示・宣伝して買い手となるユーザに広く公開し，取引機会を創出する．この間任意のユーザが TTC を取得できるため，TTC の安全性が機密性と完全性の両方の点から保証される必要がある．

5.1.1　機密性（Confidentiality）

売り手が構築した TTI は，チケット ID や価格などの開示情報だけでなく，ユーザ ID やパスワードといった秘密情報を含む．したがって，まず最初に機密性の議論が必要である．システム内で実際に流通する TTC は，TTI の分散符号化により生成された閾値よりも少ない 1 組の分散情報であるため，秘密分散法の安全性に基づき，TTC から秘密情報が漏れることはない．

売り手が同一のチケットについて複数の TTC を生成し，複数のブローカに預託したときに，そのすべてを攻撃者が収集して解析したとしても，売り手の認証情報が漏れる恐れはない．なぜなら，S_1 の値はたとえば預託するブローカ ID や一時情報 K_T の値により異なり，S_2 の値は S_1 とユーザ個別鍵 K_U とを連結した値のハッシュ値を含むため，やはり異なる値となる．さらにシステム上で流通しない共通分散情報 W_C の値が異なるため，引数 I および乱数 R の値はつねに異なり，毎回異なる TTC が生成される．したがって，攻撃者が仮にあるユーザに関するすべての TTC を集積したとしても，S_2 の値を推定することはできない．

5.1.2　完全性（Integrity）

TTC はブローカに預託され，取得した任意のユーザにより TMC に提出される．したがって，ブローカとユーザの双方が TTC を改竄する攻撃者となりうる．

TTC は 1 組の分散情報 W_1，W_2 からなり，これらの間には単純な関係が成立している．攻撃者は TMC において復元される S_1 の値を変えるために，TTC の値を任意に書き換え

ることができる．ただし，TTC が改竄された場合でも，TMC は検証によりそうした攻撃を検出できる．TTC が改竄されると S_1 の値だけでなく S_2 の値も変わるため，検証はつねに失敗する．攻撃者が共通分散情報 W_C の値から決まる $W_C = f(I)$ の引数 I を知らない限り，S_2 の値を変えずに S_1 の値だけを変えることはできない．したがって，攻撃者にとって TTC を改竄することは事実上不可能である．

売り手の認証情報すなわちユーザ ID とパスワードを取得するフィッシング攻撃への対策は，本稿における検討の対象ではない．しかし，万が一ユーザ ID とパスワードが漏洩しても，あらかじめ登録されたユーザ個別鍵 K_U が漏洩しない限り，TTC の偽造は不可能である．TTI を構成するハッシュ値および共通分散情報 W_C の値は K_U なしに算出できないため，攻撃者が有効な TTC を生成することはできない．さらにいえば，本システムではすべての取引にかかるトランザクションのログを TMC が記録することで，所有者の権利が不正に取引された場合でもログを基に不正な取引を取り消す機会がある．こうしたフォレンジクス[⋆1]の考え方は，安全なシステム設計のために重要である．

5.2 利　便　性

提案システムは，前述した強い安全性だけでなく，高い利便性をユーザに提供し，取引機会を増加させることを目的とする．以下では提案プロトコルにより得られる本システムの利便性について述べる．

5.2.1 最少性（Minimality）

本システムにおける取引は，売り手ユーザからブローカ，ブローカから買い手となるユーザ，買い手ユーザから TMC の，ただ 3 回のトランザクションで完了する．提案システムの構成は 4 者モデルであることから，取引におけるトランザクションは最少性を満たす．なお，提案プロトコルはブローカを介さず売り手と買い手の間で直接的に実行することもでき，その場合のトランザクションは 2 回で，やはり最少性を満たす．

これにより，売り手と買い手または売り手と TMC の間のトランザクションが不要なため，買い手となるユーザは希望するチケットをワンクリックで購入できる．こうしたトランザクションの即時性は取引効率を向上させ，取引機会創出のために有効である．

5.2.2 非同期性（Asynchronicity）

売り手からブローカ，ブローカから買い手となるユーザへの TTC の送付は特にレスポンスを必要としないため，非同期なトランザクションとして実行できる．したがって，ブローカは販促の手段として，たとえば電子メールなどを使って特定の顧客ユーザに TTC を送付してもよいし，掲示板や Blog などで不特定多数のユーザに公開してもよい．また，TTC を取得したユーザが他のユーザに再送することもできる．

こうしたトランザクションの非同期性は TTC の流通チャネルを増大させ，場に限定されないサービスが実現できる．これにより二次流通の市場が拡大し，全体的な取引機会の増加による市場発展が期待できる．

5.2.3 匿名性（Anonymity）

提案システムでは，売り手の認証情報は TTC に秘匿され，買い手の認証情報は TMC のみが管理する．したがって，売り手・買い手の双方がお互いに対して，またブローカに対して，ユーザ ID などの個人を特定する情報を伝える必要はいっさいなく，システム内でユーザの匿名性を保つことができる．

これによりユーザのプライバシが保護されるため安心感の向上につながり，ネット上の顔の見えない相手と取引する際の意識的な抵抗感の低減が期待できる．たとえば BBS や SNS などのコミュニティサイト上で知り合った，知らないユーザとも気軽に権利取引できるため，取引機会の増加につながる．

6. おわりに

我々は，電子権利の二次流通市場の形成と発展を目的として，C2B2C 型のブローカ仲介モデルに着目し，第三者預託可能な C2B2C 権利交換プロトコルによるセキュアな権利流通システムを提案した．提案する C2B2C 権利交換プロトコルは秘密分散法をベースとしたもので，少ない計算量で処理が可能であり，かつ情報量的な安全性により取引情報の機密性が保証される．また，提案システムは完全性を満たすよう設計され，悪意の攻撃者が改竄や偽造を行っても不正な取引が成立しない．

本システムはブローカ仲介型の権利流通システムであるため，取引にかかるユーザのコストを軽減させるだけでなく，インセンティブベースの販促活動により，ユーザの利益を保証したまま取引機会を増加させることが期待できる．さらに，提案プロトコルを用いて実現したシステムは，取引にかかるトランザクションの最少性，非同期性，匿名性といった高い利便性をユーザに提供し，取引の効率性を向上させるため，取引機会の増加につながる可能性が高い．

本稿では，提案する C2B2C 権利交換プロトコルおよびそれを用いた権利流通システムの

⋆1 フォレンジクスとは，本来は裁判における法的証拠を意味する言葉だが，情報セキュリティ上の事故などに対し，証拠となりうるデータを保存することあるいはその仕組みの意味で使われるようになった．コンピュータ・フォレンジクス（Computer Forensics）とも呼ばれる．

概要を示し，その安全性と利便性について述べた．今後，技術とビジネス（市場）の関係にとどまらず，社会の規範（商習慣）や公共政策，法制度との関係を含めて検討し，実用化する．

謝辞　本研究を進めるにあたり，有益な議論をしていただいた，山室雅司氏をはじめとする NTT サイバースペース研究所，NTT 情報流通プラットフォーム研究所の皆様，ならびに国立情報学研究所の皆様に感謝の意を表する．また，本稿の構成および内容に対して多数の有益なご指摘，ご助言をいただいた査読者の皆様に謹んで感謝の意を表する．

参 考 文 献

1) Fujimura, K. and Nakajima, Y.: General-purpose digital ticket framework, *Proc. 3rd USENIX Workshop on Electronic Commerce*, pp.177–186 (1998).
2) 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).
3) 三神京子，中村明日香，繁富利恵，小川貴英：匿名譲渡可能なオフライン型電子チケットシステム，信学技報，ISEC2004-65, pp.173–180 (2004).
4) Asokan, N., Schunter, M. and Waidner, M.: Optimistic protocols for fair exchange, *ACM Conference on Computer and Communications Security*, pp.7–17 (1997).
5) 松尾真一郎，森田　光：電子取引を実現する安全なプロトコル，SCIS2000 予稿集，C34 (2000).
6) 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，情報処理学会論文誌，Vol.42, No.8, pp.2017–2029 (2001).
7) 副島　晋，松浦幹太，今井秀樹：電子権利流通方式対に関する特性分析，SCIS2002 予稿集，Vol.I, pp.223–228 (2002).
8) 飯野陽一郎：公開鍵認証基盤に基づく電子チケットの理論，信学論，Vol.J85-A, No.11, pp.1254–1263 (2002).
9) 久野　浩，寺田雅之，井口　誠：安全な預託を可能とする権利流通方式，SCIS2000 予稿集，C36 (2000).
10) 寺田雅之，久野　浩，花舘蔵之：権利流通基盤実現のための原本性保証方式，CSS99 予稿集 (1999).
11) 廣田啓一，山本隆二，萬本正信，山室雅司：利用者の利便性を考慮した匿名権利譲渡方式の提案，FIT2004 論文集，pp.95–96 (2004).
12) Fujimura, K. and Terada, M.: Trading among Untrusted Partners via Voucher Trading System, *1st IFIP Conference on e-Commerce, e-Business and e-Government*, IFIP I3E (2001).
13) Jiangping, D.: A tentative study on the model of the campus e-commerce, *ICEC '05: Proc. 7th International Conference on Electronic Commerce*, pp.790–792 (2005).
14) http://www.stubhub.com
15) http://www.ticketmaster.com
16) Hirota, K. and Sonehara, N.: Simple and Secure Authentication Escrow for Rights Trading Protocol, *SAINT2007WS* (2007).
17) 千田英幸，満保雅浩，静谷啓樹：不正利用防止機能を有する電子マネー供託方式の構成法，CSS2004 (2004).
18) Iguchi, M., Terada, M., Nakamura, Y. and Fujimura, K.: A Voucher-Integrated Trading Model for C2B and C2C E-Commerce System Development, *Proc. 1st Conference on e-Commerce, e-Business and e-Government*, IFIP I3E (2002).
19) 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).
20) Shamir, A.: How to Share a Secret, *Comm. ACM*, Vol.22, No.11, pp.612–613 (1979).
21) Blakley, G.R. and Meadows, C.: Security of Ramp Scheme, *Proc. Crypto'84*, LNCS, No.196, pp.242–268 (1984).

(平成 19 年 10 月 10 日受付)
(平成 20 年 4 月 8 日採録)

廣田　啓一（正会員）

平成 7 年三重大学工学部情報工学科卒業．平成 9 年三重大学大学院工学研究科情報工学専攻修士課程修了．同年日本電信電話株式会社入社．現在，NTT 情報流通プラットフォーム研究所セキュリティ社会科学グループ研究主任．自然言語処理，権利流通，コミュニティ研究等を背景とした情報セキュリティ技術，特にプライバシ保護技術の研究開発に従事．総合研究大学院大学博士後期課程在籍．

曽根原　登

昭和 51 年信州大学工学部電子工学科卒業．昭和 53 年信州大学大学院工学研究科修了．同年日本電信電話公社（現 NTT）横須賀電気通信研究所入社．平成 16 年より国立情報学研究所情報社会相関研究系教授．現在，デジタル権利管理技術，情報信頼性評価技術等の研究に従事．工学博士．平成 5 年画像電子学会 IFS 画像符号化論文賞．著書に『サイバーインタフェースのデザイン』（電気通信協会，共著，2001 年），『コンテンツ流通』（アスキー出版，共著，2003 年），『著作権の法と経済学』（勁草書房，共著，2004 年），『c-Japan 宣言』（丸善ライブラリー，共著，2008 年）等．画像電子学会，電子情報通信学会，映像情報メディア学会各会員．