電子チケット流通制御方式

1S－6

久野 浩　松山 一雄　藤村 考
NTT 情報流通プラットフォーム研究所
{kuno, matsuyama, fujimura}@isl.ntt.co.jp

1. はじめに

電子商取引の活性化を目的として、現在、筆者らは多様な権利をディジタル化して流通させる、新しい情報流通メディア「電子チケット」の確立を目指している。電子チケットによって流通させうる権利には、例えばコンサートチケット、航空券、宿泊券、食事券、会員券、ソフトウェアライセンスのような、権利商品全般が含まれる。

本稿では、筆者らが現在開発を進めている電子チケット流通システムのうち、システム概要と流通制御方式について述べる。

2. 電子チケットシステム概要

図 1 に電子チケットシステム概要について示す。権利商品の取引形態は多種多様であるが、権利の流通に関わる処理のみに着目すると、権利の流通は、発行・譲渡・改札の 3 つの基本トランザクションから構成される。つまり、電子チケットは発行機関にて生成され、直接、あるいはネットワークを経由して、利用者に対して転送される(発行)。発行された電子チケットは、利用者間を転々流通し(譲渡)、最後に、サービス提供機関にて、サービスと引き換えに消費される(改札)。この時、チケットによっては、利用可能な回数が減少、あるいは無効化される。

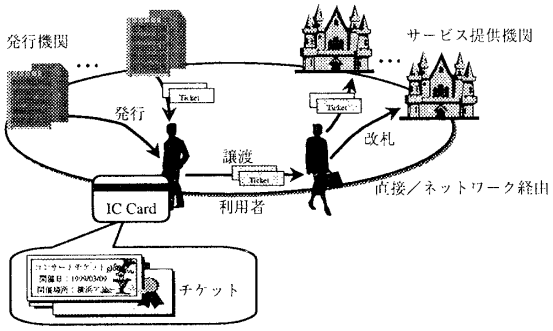

図 1 電子チケットシステム概要

本電子チケットシステムの特徴としては、複数の発行機関、利用者、およびサービス提供機関が共存する環境にて電子チケットを利用できることが挙げられる。また、電子情報に価値を持たせて流通させるため、利用者は電子チケットを IC カードなどの携帯端末に格納して持ち歩き、場所を問わず利用することができる。

3. 電子チケットに対する要求条件

電子現金は、電子情報に価値を持たせて流通させるという点で、電子チケットと共通点が多い。そこで、電子チケットに対する要求条件を、紙のチケットの分析、および電子現金に対する要求条件[1]を基に、以下の様に整理した。

表 1 電子チケットに対する要求条件

1	安全性	A	機械解釈性
2	匿名性	B	状態推移性
3	携帯性	C	組み合わせ可能
4	転々流通性	D	流通制御性
5	オフライン性	E	既存システムとの適合性
6	分割利用性		

このうち、1-6については、電子現金の分野で多くの検討がなされているため、本稿の範囲外とする。また、A-C は電子チケット固有の要求条件であるが、既に筆者らによって文献[2]で述べているため、本稿では、本電子チケットシステムの特徴である D について述べる。

4. 電子チケット流通制御方式

表 2 に、流通制御という観点から、権利商品の性質について分類した結果を示す。権利商品には、これらの性質を持つものと持たないものがあり、権利商品毎に多様な流通制御がシステムに対して要求されることがわかった。そのため、これらの性質を制御情報として電子チケットに記述した。これにより、電子チケットシステムは電子チケットを参照して動的に流通を制御することができ、電子チケット毎のシステム設定を不要にできる。尚、著者らは多種多様な電子チケットの表現方法として、電子チケット記述言語の検討を進めている[2]。

A Digital Ticket Circulation Architecture
Hiroshi KUNO, Kazuo MATSUYAMA, Ko FUJIMURA
NTT Information Sharing Platform Labs.

しかし、表 2 に示す性質のうち、流通範囲限定のチケットに関しては、対象となるチケット単体では制御できず、流通範囲を限定する方式の確立が必要である。

表 2 権利商品の分類

性質		例
利用回数	1回	コンサートチケット、乗車券
	有限回	回数券、ポイントカード
	無限回	定期券、免許証、証書
有効期間	期間限定	期間限定割引券
	無期限	図書券、食事券
複製可否	複製可能	割引クーポン券
	複製不可能	テーマパーク入場券
譲渡性	譲渡可能	印紙、図書券
	譲渡不可能	社員証、学生証
流通範囲限定	流通範囲非限定	乗車券、商品券
	流通範囲限定	会員限定サービス券

流通範囲限定チケットの例として、免許証あるいは保険証がなければ発行されない会員権が挙げられる。ここでは、免許証あるいは保険証という、会員権にとって流通範囲を表す(別の)権利によって流通範囲が指定されていると考えることができる。

そこで、本稿では、権利の流通範囲を、あらかじめ配布しておいた別の権利が存在しているかどうかによって制御する方法を提案する。尚、その別の権利の流通もまた、別の権利によって制御する。筆者らはこのモデルを、玉ねぎモデルと呼んでいる(図 2)。

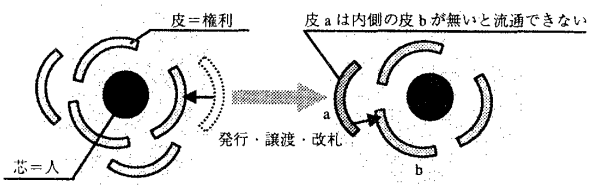

図 2 玉ねぎモデル

これは、取引当事者を玉ねぎの芯に、権利をその皮として表現し、芯と芯の間にトランザクションが発生する事をモデル化したものである。また、皮の上に存在している皮は、その内側に別の権利がなければ発行、譲渡あるいは改札することができない事を表している。これらのトランザクション毎に権利の流通を制御できるように、発行・譲渡・改札のトランザクション毎に、その前提となる権利(電子チケット)を流通対象の電子チケット自身に流通条件として記述するようにした。表 3 に、電子チケットを特定の会員の間で流通させるための、流通条件の記述例を示す。

また、全ての権利を電子チケットで実現することにより、電子チケットシステム以外に公開鍵インフラ等を必要とせず、さらに第3者に権利の所有を問い合わせることなく、オフラインで安全に処理することができる。

表 3 流通条件記述例

トランザクション	送信側条件	受信側条件
発行	発行機関証明書	会員証
譲渡	会員証	会員証
改札	会員証	改札機関証明書

5. 電子チケット流通プロトコル概要

図3に発行時における電子チケット流通プロトコルの概要を示す。まず、電子チケットの制御情報を受取側に通知するため、受取側に電子チケットを転送する。ここではチケットの所有権の移動は伴わない。次に、電子チケットに記述されている流通条件の検証を行い、発行の前提となる権利の検証が行われる。流通条件を満足していれば、譲渡証明部を転送する。これによって、チケットの所有権は移動される。以上がチケット発行の概要である。譲渡・改札についても同様である。筆者らは、既にこれらのプロトコルを、Java 言語を用いて実装し、その実現性を検証している。

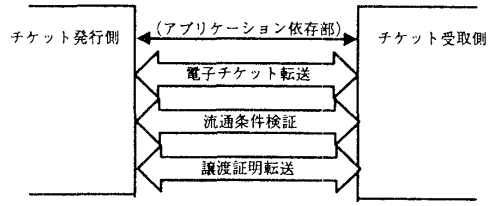

図 3 電子チケット発行プロトコル概要

6. まとめ

新しい情報流通メディアである電子チケットの、流通システムの検討を行った。本システムの特徴である、電子チケットによって別の電子チケットの流通を制御する流通モデルを提案した。本方式により、電子チケットの組み合わせで電子チケットの流通を変化させられる、動的な電子チケット流通制御方式を実現した。

参考文献

[1] T. Okamoto and K. Ohta, "Universal Electronic Cash," *CRYPTO '91*, LNCS 576, 1991.

[2] K. Fujimura and Y. Nakajima, "General-purpose Digital Ticket Framework," *3rd USENIX Workshop on Electronic Commerce*, 1998.