局所的に複製と譲渡が可能な権利管理手法

山崎, 知美
九州大学工学部

中村, 徹
九州大学大学院システム情報科学府

馬場, 謙介
九州大学大学院システム情報科学研究院

安浦, 寛人
九州大学大学院システム情報科学研究院

SCIS 2007 The 2007 Symposium on Cryptography and Information Security
Sasebo, Japan, Jan. 23-26, 2007
The Institute of Electronics, Information and Communication Engineers

局所的に複製と譲渡が可能な権利管理手法
A Right Management Scheme with Local Copies and Delegations

山崎 知美* 中村 徹† 馬場 謙介‡ 安浦 寛人‡
Tomomi Yamasaki Toru Nakamura Kensuke Baba Hiroto Yasuura

あらまし 近年，様々なサービスが電子化されるようになり，電子権利を取引する場面が多くなった．そのため，サービス提供者には安全で利便性の高い権利の管理が求められている．実際のサービス提供システムでは，サービスを受けられる人が状況に応じて変化する（つまり，権利が変化する）ことが便利な場合がある．さらには，鍵の貸与など，権利を変化させる裁量がある程度ユーザに与えられているならば，さらに有用なシステムの実現が可能である．すべてのユーザが常にサービス提供者との情報伝達が可能で，ユーザの裁量による権利の変化もサービス提供者によって行われるならば，やはり正当な審査を行うことが可能である．以下，２つのユーザ間のみで情報のやり取りが行われ，これによって権利を変化させるしくみを考える．

キーワード 電子権利，権利譲渡，電子錠

1 はじめに

近年，情報技術の進展やネットワーク基盤の普及に伴い，多くのサービスが電子化されるようになった．特に携帯電話の普及・発展によって音楽のダウンロードや電子マネー・電子チケットなどユーザにとって利便性の高いサービスを提供できるようになった．これらの電子データは価値・権利に対応するものであり，本稿ではこれらの電子データを**電子権利**と呼ぶ．電子データは現実世界の紙のチケットや紙幣と異なり，品質を劣化させることなく全く同じデータを作り出すことが可能である．その場合，元のデータと作り出されたデータとでは見分けがつかず，どれが正規の電子権利であるかを判別することが難しい．そのため不正に電子権利が作り出されたとしても，その電子権利に対応した権利を行使することができないような権利管理システムが求められる．

この要求に対し，現行のサービスにおける一般的な方法としては，サービス提供者が電子権利を用いた権利の取引を一括管理し，監視することにより不正な電子権利を防止している．つまり，ユーザと権利のやり取りを行う前に認証を行い，そのユーザと権利を確実に紐付けることにより，サービス提供者は権利の所在を常に把握することができる．

サービスの中には，状況に応じてユーザ同士で権利がやり取りできることが便利な場合がある．このようなサービスはサービス提供者を介することでユーザ間で権利の受け渡しを行うという方法をとっているが，電波状況によっては利用できない，頻繁にやり取りするものに関しては通信コストがかかる，などの問題がある．よってサービス提供者を介さずにユーザ間で権利のやり取りを行えることが便利な場合も考えられる．これは，権利を管理する裁量をある程度ユーザに与えることになり，より柔軟なサービス提供を実現することができる．

そこで，本稿ではユーザ間で局所的に権利のやり取りを行うことが可能で，かつ権利の安全な管理を実現する手法を提案する．電子権利のやり取りによる権利の変化として，譲渡と複製を考える．権利の譲渡とはあるユーザが保持していた権利を他のユーザに与え，かつ元のユーザが権利を持たない状態となることをいい，権利の複製とはあるユーザが保持していた権利を他のユーザに与え，かつ元のユーザも権利を保持し続けることをいう．これらを実現するシステムの安全性として，権利の譲渡では権利をもつユーザの数が一定に保たれることを，権利の複製ではサービス提供者が想定する権利の有無の判断と，システム全体の判断が一致することを評価の対象とする．

本稿では，権利管理の一部をユーザが担うことができ，ユーザにとって柔軟な権利管理システムを実現することを目標とする．また，鍵の貸与などにおいては誰から誰

* 九州大学工学部，〒 819-0395 福岡県福岡市西区元岡 744 番地
School of Engineering, Kyushu University, 744 Motooka Nishi-ku Fukuoka 819-0395
† 九州大学大学院システム情報科学府，Graduate School of Information Science and Electrical Engineering, Kyushu University
‡ 九州大学大学院システム情報科学研究院，Faculty of Information Science and Electrical Engineering, Kyushu University,
{yamasaki,toru,baba,yasuura}@c.csce.kyushu-u.ac.jp

に鍵が貸されたのかといった情報が有益である場合も考えられるため，匿名性を考慮せず，サービス提供者が履歴を参照できるようなシステムとする．

本稿の構成は以下の通りである．第 2 章で本稿で提案する手法の概要を述べ，第 3 章では用語の定義と定式化を行う．第 4 章では基本となる権利管理システムのプロトコルを述べ，第 5 章ではシステムの拡張を行う．第 6 章で関連研究について紹介し，第 7 章で今後の課題を述べ，本稿をまとめる．

2　提案する手法の概要

2.1　想定される応用例

本節では，本稿で提案する手法が想定している例として電子錠サービスと回数券の例を挙げる．それぞれの場合において，どのようにして鍵の複製（譲渡）を用いると利便性の高いサービスを提供できるかを考える．

応用例 1 (住居の鍵) 一般的な住居の例を考える．現在の物理的な鍵では，家族や友人に対して合鍵を渡すことは頻繁に行われている．そのため，電子錠サービスでも鍵を複製して人に渡せる機能を備えている方が便利だと考えられる．

ただし，部屋の持ち主の意に反するような鍵の複製が行われるのは問題である．例えば，持ち主が知らないところで鍵が大量に複製され，配布される事態は非常に危険である．そのような事態が起こらないようにするためには，部屋の持ち主以外は鍵の複製が行えないようにする，複製回数を制限できる，などの機構が必要となる．

また，ホテルやウィークリーマンションなど短期滞在型の住居の例を考える．この場合の特徴として，短期間で利用者が替わるという点が挙げられる．そのため，管理者は利用者が替わるたびに鍵を回収/配布しなければならず管理のコストがかかる．また，安全性を考慮すると利用者が替わるたびに鍵を付け替えた方がよいが，コストがかかるため複数の利用者が同一の鍵を使用しているという問題もある．

この問題を解決するには，管理者が利用者の鍵の失効を簡単に行える，鍵の有効期限などを設定できる，などの方法が行えることが望ましい．これにより，管理者は鍵を回収する手間を省くことができ，かつ前の利用者によって不正に鍵が使われるのを防止することもできると考えられる．

応用例 2 (回数券) 例えばバスや映画のチケットなど，回数券の種類によっては複数の利用者が回数券を分割して使ってもサービス提供者には不都合がない場合がある．そのような場合，利用者同士で回数券を分割できる機能があると便利である．回数券の例では利用者が多いことが考えられるため，サービス提供者を介さずに受け渡しを行うことができると，サービス提供者への負荷を軽減する効果も期待できる．

応用例 3 (公共施設の鍵) 公共施設では，複数の人間が同時に鍵を用いるという状況が考えられる．例えば，グループで体育館を借りた場合，グループに一つしか鍵が渡されないと，鍵を持っている人が一番先に体育館に行って鍵を開けなくてはならず，非常に不便である．このような事態に対して，グループ全員に鍵を渡しておき，一番最初に体育館に着いた人だけが鍵を使用できる，などという制限をつけることができたら利便性は高まると考えられる．

2.2　提案する手法の要件

前節で示したようなサービスを提供するために求められる要件を以下に示す．

要件 1 (局所性) 権利の複製（譲渡）を，ユーザ間での対話のみで実現できる

要件 2 (柔軟性) ユーザは他のユーザに権利を複製（譲渡）するか否かを決定できる

要件 3 (追跡性) サービス提供者は複製（譲渡）された権利が行使されるとき，その履歴を得ることができる

要件 4 (制限可能性) 権利の付与・複製・譲渡の際に，権利の複製（譲渡）の許可/禁止，もしくは複製回数の制限を設定することができる

要件 5 (付加情報) 権利の付与・複製・譲渡の際に，権利の利用回数や使用時間などの制限を付加することができる

要件 1 はサーバを介さずにユーザ間で権利の複製（譲渡）を行うことを示している．また，要件 2，4 は応用例 1，3 を実現するのに必要な条件である．また，要件 5 は応用例 2 に対応している．さらに，鍵が誰から誰に複製（譲渡）されたかの情報を得ることは鍵の管理を行う上で必要な情報であると考えられるので，要件 3 を加えている．

以上の要件を満たすシステムを実現する手法を提案する．

3　定式化

3.1　権利管理システム

権利管理システムとは，何かしらの権利を行使しようとする者と，その権利の有無を検証する者，および，その二者の間に与えられる対話のプロトコルによって構成されるものとする．権利を行使しようとする者を**ユーザ**と呼び，$u_1, u_2, \ldots \in U$ によって表す．各 $u_i \in U$ に対

し権利の有無を判断する者を**サーバ**と呼び，s で表す．s が，与えられたプロトコルにそって $u_i \in U$ と対話を行い，権利の有無を判断することを**検証** と呼ぶ．以下，サーバがひとつだけのシステムを考える．

s による検証によって，U 中の任意のユーザについてのある権利の有無が必ず決まるものとする．このとき，権利が有ることを 1，無いことを 0 で表すことによって得られる関数 $F : U \to \{0,1\}$ を，この**システムによる権利関数**と呼ぶ．この関数による出力は，与えられるプロトコルによっては，必ずしも s が想定するものとは一致しない．上と同様にして，各 $u_i \in U$ についての s が想定する権利の有無を表す関数 $F_s : U \to \{0,1\}$ を考え，**サーバ s による権利関数**と呼ぶ．ある権利管理システムは，任意の $u_i \in U$ について $F_s(u_i) = 1$ ならば $F(u_i) = 1$ のとき，F_s に対して**完全**であるという．また，$F_s(u_i) = 0$ ならば $F(u_i) = 0$ のとき，F_s に対して**健全**であるという．

3.2 権利の複製

$u_i, u_j \in U$ は $F(u_i) = 1$ かつ $F(u_j) = 0$ を満たすとする．今，u_i と u_j の間で何かしらの手続きを行うことが可能であるとして，これによって，F が $F'(u_i) = 1$ かつ $F'(u_j) = 1$ となるように変化し，その他の $u \in U$ については変化しないとき，この手続きを u_i から u_j への**権利の複製**と呼ぶ．ここで，権利管理システムの定義を，ユーザ間の対話プロトコルも含むものへと拡張する．

ある $u_i \in U$ について，u_i の持つ権利を $u_j \in U$ に対して複製するかどうかを 0（複製しない）または 1（複製する）によって表すとする．このとき，関数 $F_{u_i} : U \to \{0,1\}$ を**ユーザ u_i による権利関数**と呼ぶ．s による**複製を許した権利関数**とは，以下を満たす関数 $F_s^{(1)} : U \to \{0,1\}$ である．

- $F_s(u_i) = 1$ または，$F_s(u_j) = 1$ かつ $F_{u_j}(u_i) = 1$ である $u_j \in U$ が存在するとき，$F_s^{(1)}(u_i) = 1$ であり，
- それ以外のとき，$F_s^{(1)}(u_i) = 0$ である．

4 複製を考慮した権利管理

権利の複製を，ユーザ間の対話のみで実現するシステムを考え，その性質を調べる．

4.1 基本となる検証プロトコル

まず，権利管理システムを考える上での前提をあげ，複製を考慮しない場合の検証プロトコルについて考える．

仮定 1 s および U のうち任意の二者間で理想的な識別を行うことができる．つまり，各 s および $u_i \in U$ がそれぞれ持つ識別子 n_s および n_i を確認できる．

上の仮定は，理想的な識別がこの識別子によって行われることを主張しているわけではない．理想的な識別を実現するための具体的な手法は本稿では議論しないが，この仮定の下でも，現実的に有用なシステムの実現が自明でないことが，第**??**章の応用例からわかる．以下，各プロトコルの前に識別が行われることを明示しない．

仮定 2 任意の $u_i \in U$ は s へ情報の安全な提出が可能である．つまり，任意の $u_i \in U$ は，u_i が暗号化でき，s のみが復号化できる，暗号化を行う関数 f_{u_i} を持つ．

これにより，s は n_i から復号化を行う関数 $f_{u_i}^{-1}$ を選ぶことができるものとする．

仮定 1 から，s が各 $u_i \in U$ の識別を行うことで検証を行うならば，F に対して完全かつ健全なシステムが容易に実現可能である．

プロトコル 1 (検証 0) s は，u_i の識別子 n_i を確認し，$F_s(u_i) = 1$ のとき 1 を出力し，それ以外のとき 0 を出力する．

4.2 複製プロトコル

ユーザ間の何かしらの手続きによって複製が行われたことが，随時 s に伝えられるならば，その度に F_s を変更することによって，$F_s^{(1)}$ に対して完全かつ健全なシステムの実現が可能である．オンラインで複製を行う現行のシステムは随時 s に複製が行われたことを伝えることができる．

以下，ユーザ間で局所的に複製を行った場合でも $F_s^{(1)}$ に対して完全かつ健全なシステムを考える．つまり，複製が行われたことが s に伝えられなくても権利の行使を行えるプロトコルを提案する．

以下は，u_i と u_j の間で行われる複製のプロトコルである．

プロトコル 2 (複製 1) u_i は，$F_{u_i}(u_j) = 0$ のとき手続きを終え，それ以外のとき，u_j に $K = (n_i, f_{u_i}(n_j))$ を提出する．

そして，検証のプロトコルを下のように変更する．ただし，$K[1]$ および $K[2]$ はそれぞれ対 K の 1 番目の要素と 2 番目の要素を表すものとする．

プロトコル 3 (検証 1)

(1) $F_s(u_j) = 1$ のとき 1 を出力する．それ以外のとき，

(2) $F_s(u_i) = 0$ のとき 0 を出力する．それ以外のとき，

(3) $f_{u_i}^{-1}(K[2]) = n_j$ のとき 1 を出力し，それ以外のとき 0 を出力する．

仮定 2 より，u_i 以外のユーザが K によって権利を認められることはない．また，関数の引数の識別子を他の識別子に変更することもできない．よって，プロトコル 2 および 3 により実現されるシステムは，$F_s^{(1)}$ に対して完全かつ健全である．

5 複雑な権利管理への拡張

5.1 再帰的な複製

前章のプロトコル 2 および 3 では，複製回数が 1 回に限定されていた．本節ではこれらのプロトコルを，複数回の複製が可能なプロトコルへと拡張する．

以下，u_i から u_j へ複製された権利の，u_l への複製を実現する仕組みを考える．

プロトコル 4 (複製 2) u_j は，$F_{u_j}(u_l) = 0$ のとき手続きを終え，それ以外のとき，u_l に $K = (n_j, f_{u_j}(n_l, K_{u_i}))$ を提出する．

上のプロトコルは再帰的に適用され，初期状態として s からの権利の複製が $K_s := \phi$ を用いて行われるものとする．

このとき，検証プロトコルを以下のように変更する．

プロトコル 5 (検証 2) s は，u_l から K を受け取り，

(1) $F_s(u_l) = 1$ のとき 1 を出力する．それ以外のとき，

(2) $k = f_{u_j}^{-1}(K[2])$ を計算し，$k[1] \neq n_l$ のとき 0 を出力する．それ以外のとき，

(3) $k[2] = \phi$ かつ $F_s(u_j) = 1$ のとき 1 を出力する．それ以外のとき，

(4) $n_l = n_j$ かつ $K_{u_j} = k[2]$ として手順 (2) へ移る．

プロトコル 4 および 5 は，それぞれ，プロトコル 2 および 3 の単純な拡張である．よって，プロトコル 4 および 5 により実現されるシステムは，$F_s^{(1)}$ に対して完全かつ健全である．

5.2 付加情報による拡張

以上のプロトコルでは，権利の種類はただひとつとして議論しているが，例えば，権利の照合の手順を加えることで，サーバが複数の権利を管理する場合へ単純に拡張することができる．また権利の利用回数，使用期限など権利に対する制限を行う場合への拡張も可能である．この際，権利についての様々な情報をやり取りする必要がある．よって，さらに以下の前提が必要である．

仮定 3 s は，s が暗号化でき，s のみが復号化できる，暗号化を行う関数 f_s を持つものとする．

R を権利についての情報とする．各権利関数は R に依存するように拡張されるとする．また，各暗号化関数の入力が適切に変更されるとして，以下の手順で s による権利の付与が行われるものとする．

プロトコル 6 (付与 3) s は，$F_s(R, u_i) = 1$ ならば u_i に $K = (R, f_s(n_i, R))$ を提出する．

前節と同様に，u_i から u_j へ複製された権利の，u_l への複製を実現する仕組みを考える．u_i から u_j へ K' が提出されているものとする．

プロトコル 7 (複製 3) u_j は，$F_{u_j}(R, u_l) = 0$ のとき手続きを終え，それ以外のとき，u_l に $K = (R, f_{u_j}(n_l, K'))$ を提出する．

このとき，検証プロトコルを以下のように変更する．

プロトコル 8 (検証 3) s は，u_l から K を受け取り，

(1) $F_s(R, u_l) = 1$ のとき 1 を出力する．それ以外のとき，

(2) $k = f_{u_j}^{-1}(K[2])$ を計算し，$k[1] \neq n_l$ のとき 0 を出力する．それ以外のとき，

(3) $k[2] = \phi$ かつ $F_s(R', u_j) = 1$ のとき 1 を出力する．それ以外のとき，

(4) $n_l = n_j$ かつ $K_{u_j} = k[2]$ として手順 (2) へ移る．

プロトコル 7 および 8 は，それぞれ，プロトコル 4 および 5 の単純な拡張である．よって，プロトコル 7 および 8 により実現されるシステムは，$F_s^{(1)}$ に対して完全かつ健全である．

5.3 権利の譲渡

$u_i, u_j \in U$ は $F(u_i) = 1$ かつ $F(u_j) = 0$ を満たすとする．u_i と u_j の間の手続きによって，F が $F'(u_i) = 0$ かつ $F'(u_j) = 1$ となり，その他の $u \in U$ については変化しないとき，この手続きを u_i から u_j への**権利の譲渡**と呼ぶ．

F による**権利の総量**とは，$F(u_i) = 1$ である U 中の u_i の数であり，$|F(U)|$ によって表すものとする．

権利の譲渡を実現する方法は，権利の複製を単純に拡張することで容易に実現できる．複製の場合では権利の総量が増えるのに対し，譲渡の場合には権利の総量が一定である．そのため，譲渡の場合は s による検証の際に権利の総量が増えないことを保証する必要がある．

前節で示したプロトコル 8 を以下のように変更する．

プロトコル 9 (検証 3')

(1) u_l は，s に K を提出する．

(2) s は，u_l の識別子 n_l を確認し，$F_s(K[1], u_l) = 1$ のとき 1 を出力する．それ以外のとき，

(3) s は，$k := f_{u_j}^{-1}(K[2])$ を計算し，$k[1] \neq n_l$ のとき 0 を出力する．それ以外のとき，

(4) s は，$k[2] = f_s(n', R')$ のとき手順 (6) へ移る．それ以外のとき，

(5) $n_l := n_j$ かつ $K := k[2]$ として手順 (3) へ移る．

(6) s は，$k' := f_s^{-1}(k[2])$ を計算し，$k'[1] = n_l$ かつ $F_s(k'[2], u_j) = 1$ のとき $F_s(k'[2], u_j) := 0$ とし，1 を出力する．それ以外のとき，0 を出力する．

プロトコル 9 の (4) でサーバ s による権利関数を変更することにより，u_j は権利を行使することはできなくなる．よってプロトコル 9 によって実現されるシステムは，権利の総量を一定に保つことが可能である．

あるユーザが複数のユーザとプロトコル 7 を行い，権利の譲渡を行おうとした場合，最も早くサーバによる検証を受けたユーザに権利の譲渡が行われる．本稿では，権利の譲渡に対する安全性として，権利の総量が一定であることのみを考慮しているため，このような事態を問題とみなさない．また，この性質を用いることで，応用例 3 を実現することが可能である．

5.4 考察

プロトコル	1	2,3	4,5	6,7,8	6,7,9
複製	×	△	○	○	×
譲渡	×	×	×	×	○
要件 1	×	○	○	○	○
要件 2	×	○	○	○	○
要件 3	×	○	○	○	○
要件 4	×	△	○	○	○
要件 5	×	×	×	○	○
応用例	-	1	1	2	3

表 1: プロトコルの比較

提案したプロトコルの比較を表 1 に示す．複製（譲渡）が実現されている，もしくは要件を満たす場合には○，複製（譲渡）が実現されていない，もしくは要件を満たさない場合には×を記す．プロトコル 2，3 については 1 回限りの複製が許されているので△で示す．また，これらのプロトコルを用いて実現される応用例も併せて示す．

R に権利の譲渡であるか複製であるかを示す情報を加えることで，これらのプロトコルは同じシステム上で容易に実現可能であり，想定するサービスによって使い分けることが可能である．

6 関連研究

本章では電子権利の管理に関する関連研究を紹介する．ユーザ間で局所的に権利の譲渡を行う方法としては，ハードウェアの耐タンパー性に頼る方法が一般的である．また耐タンパー性に頼らずに匿名性を保証するシステムに関する研究も行われている．それぞれの特徴と，想定しているサービスの例を挙げる．

6.1 耐タンパー性に依存する手法

文献 [1] では，耐タンパー性を持った IC チップである eTRON (entity and economy The Real-time Operating system Nucleus) チップを用いたアーキテクチャを開発している．eTRON チップは相互認証機能と暗号化通信機能を備え，電子価値・電子権利を安全に格納する．また eTRON チップを核技術として電子価値流通プラットフォーム STeP(Securely Transferable entity Platform for eTRON) の開発を行っており，想定させるサービスとしては電子チケット販売や電子ブックの課金サービスが挙げられている．

しかし耐タンパー性に頼る方法の場合，デバイスの導入に非常にコストがかかるという問題がある．

6.2 サービス提供者への匿名性を実現する手法

文献 [2] では匿名性を保証した譲渡制限可能な電子チケットシステムが提案されている．このシステムはブラインド署名などの暗号技術を用いることで，サービス提供者及びトークン発行者に対するユーザの匿名性を保証している．

このシステムで注目すべき点はユーザをグループに分類し，各グループ内での権利譲渡を行う点と，同じシステムで譲渡可能・譲渡禁止の二つのパターンに対応できるという点である．本稿で提案する手法もグループ内での複製（譲渡）を前提とし，また譲渡可能・禁止のどちらにも対応できるという特徴があり，この点で先行研究といえる．ただ本稿と文献 [2] では三つの点で違いがある．一点目は本稿では匿名性を排除し，複製（譲渡）の履歴なども全て管理者によって把握が可能という点であり，二点目は文献 [2] ではグループ内のユーザか否かのみを判断して譲渡を行うのに対し，本稿ではユーザが F_{u_i} によって他のユーザに複製（譲渡）を行うかどうかを決定する点が異なっている．三点目は譲渡を行う際に文献 [2] ではチケットの発行者に問い合わせる必要があるという点である．

またサービス提供者及びトークン発行者に対して匿名性を持つことから，チケットの二重使用を検知するためには使用された全てのトークンを保持しておく必要がある．これはサービスによっては非常に多くの情報量を必要とするため，長期間にわたって行われるサービスや利用頻度が高いサービスには向かないと考えられる．

6.3 ユーザ間の匿名性を保証する手法

文献 [3] では最小のトランザクションで譲渡を行うプロトコルを提案している．このプロトコルでは非同期のトランザクションで譲渡を行うことが可能で，インターネットの掲示板やメールを介してユーザ間で電子権利の譲渡を行うことができる．更に復元制御型秘密分散法を用いることにより，譲渡先のユーザは譲渡された電子権利の内容については復号化を行うことができるが譲渡元のユーザについては情報を得ることができない．そのためユーザ間の匿名性を保証することが可能となっている．

この研究ではユーザ間で匿名性を保証しているため，譲渡対象のユーザを選択することができないという性質をもつ．文献 [3] では想定されるサービスとして，メールやインターネットを介した電子チケットの譲渡を挙げている．このサービスにおいては譲渡を正しく成立させることが目的であり，譲渡対象を選択できなくてもよいという見解である．本稿では複製（譲渡）の対象とするユーザ以外は複製（譲渡）された権利を行使することができないことを保証しており，この点がこの研究と本稿の目指すシステムの違いである．

近年，個人情報保護の観点から匿名性を保証するシステムの研究が多くなされている．上記のように，サービス提供者に対する匿名性を保証するシステム，ユーザ間での匿名性を保証するシステムなど様々なアプローチがあり，それぞれ想定するサービスによってメリットが異なっている．

7 おわりに

本稿では，権利の複製（譲渡）を行うことが可能な権利管理手法の提案を行い，ユーザが権利管理の一部を担うシステムを実現することができた．

今後の課題としてはプロトコルに対する攻撃を想定し，安全性の評価を行う必要がある．また，本稿で提案したシステムを携帯電話上で実装を行い，実用性の評価を行う．実装形式としては NTT DoCoMo から提供されている i アプリの開発環境を用いて実装し，携帯電話に搭載されている赤外線機能もしくは FeliCa チップを用いてユーザ間やサーバとの通信を行う予定である [4].

謝辞

本研究は平成 14-18 年度科学研究費補助金学術創成研究費・課題番号 14GS0218 によるものである．

参考文献

[1] 石井一彦, 寺田雅之, 森謙作, 本郷節之, “eTRON を搭載した携帯端末による電子価値・電子権利流通方式の研究”, NTT 技術ジャーナル, 2005 年

[2] 三神京子, 繁富利恵, 小川貴英, 今井秀樹, “任意に譲渡制限可能な匿名電子チケットシステム”, SCIS 2005

[3] 廣田啓一, 萬本正信, 山本隆二, “最小トランザクションによる権利譲渡プロトコルの提案”, SCIS 2005

[4] NTT ドコモ, “作ろう i モードコンテンツ”, http://www.nttdocomo.co.jp/service/imode/make/content/iappli/index.html