超流通における使用記録の回収とプライバシー保護

大瀧保広[†] 河原正治[††]

超流通は，所有ではなく利用に応じた課金を行うコンテンツ流通システムであり，利用者間のコンテンツのコピーを無制限に認めることができる．超流通に基づくシステムでは，使用状況の記録を決済センターが回収し，それに基づいて利用者からコンテンツ提供者へのコンテンツの料金を精算するのが一般的である．回収される使用記録にはユーザ ID とコンテンツごとの利用量の情報が含まれており，これらは，料金の徴収と分配を正当かつ公平に行うために不可欠な情報である．そのため，決済センターは利用者がどのコンテンツをどれくらい使用したのか把握できる．多くの利用者はこれを快適でないと感じるようになるだろう．料金の徴収にはコンテンツごとの明細は不要であり，また料金の分配にはユーザ ID は不要である．末松らはこのことに着目し，決済センターにおける徴収と分配の機能を分離したセンター分割方式を提案した．しかしこの方法では，センターへの送信が一括して行われるためセンター間の通信が利用者に不透明である．またセンターへ送信されるデータの内容の確認ができない．このため依然として心理的に不安が残る．本論文では，それぞれのセンターに必要な情報のみを個別に送信することで利用者のプライバシーをよりよく保護する．また，送信される情報を利用者自身が確認できる送信手法を提案する．

Protecting User's Privacy while Collecting Usage Records on Superdistribution

Yasuhiro Ohtaki[†] and Masaji Kawahara[††]

Superdistribution is a method of distributing digital information in which a fee is charged based on the amount of usage. Mere possession of a copy requires no payment. Transmitting the information to others is not just legal; it is encouraged. There is no need to report it to the contents providers. Usage records are automatically sent to a clearing agency, which then collects the fees from users and distributes them to the contents providers. The usage record contains, at a minimum, a user-ID, a content-ID, and the amount of usage, since without this information there is no way to determine and transfer the appropriate fee. The clearing agency itself has access to these records unless specific provision is made for limiting the uses to which that information can be put. Suematsu et al have proposed an implementation of superdistribution that achieves a greater degree of privacy by using two separate agencies: a fee collection agency and a fee distribution agency. Suematsu's implementation makes use of the fact that the collection agency does not need access to the content-ID, nor does the distribution agency need access to the user-ID. In this paper we present an enhanced version of that implementation. We describe how the information sent to the fee collection agency and the information sent to the fee distribution agency are kept to a minimum and are transmitted separately. We also describe a facility that enables users to investigate what information has been transmitted to the agencies.

1. はじめに

超流通[1)]は，ディジタルコンテンツの自由な流通と利用とを可能にする基盤技術として注目されている．コンテンツの「所有」に対して課金するのではなく，「利用」に対する使用記録を管理し，それを回収することによって，対価を受け取る権利を有する者などへ収益を分配する．したがって，従来のようにコピーを制限する必要はなく，CD-ROM やインターネットなど様々な経路を使って無制限に配布することができる．多くの場合，対価を受け取る権利を有する者は，コンテンツの提供者自身であると考えられるので，以下では単に「コンテンツ提供者」と記述することにする．

プライバシーの保護は，インターネット利用者の主

† 茨城大学工学部情報工学科
Department of Computer and Information Sciences, Ibaraki University
†† 筑波技術短期大学教育方法開発センター
Research Center on Educational Media, Tsukuba College of Technology

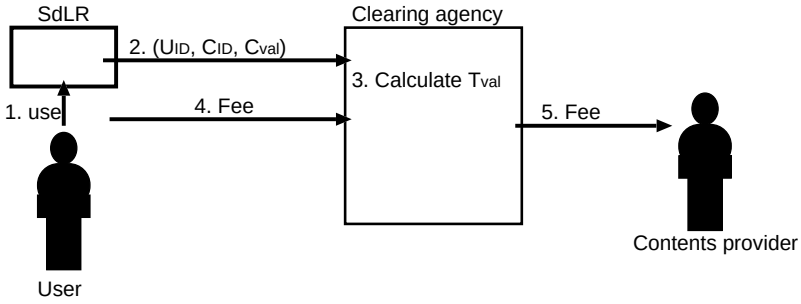

図 1 通常の超流通における使用記録の回収
Fig. 1 Traditional protocol to collect usage records.

な関心事の 1 つであり，超流通のようなコンテンツ流通技術においても，洗練されたプライバシー保護機構が組み込まれているかどうかは成功の重要な鍵である[2]．超流通において，利用者のプライバシーにかかわると考えられることには次のようなものがあげられる．

一般的な超流通システムでは，決済センターによって回収される使用記録に基づいて料金の徴収が行われる．この使用記録は，ユーザ ID，コンテンツ ID，コンテンツ利用量などを含む．これらの情報は，料金の徴収とコンテンツ提供者への料金の分配を正確かつ公平に行うために必要な情報であり，決済センターは，だれがどのコンテンツをどれだけ使用したかを把握できる．

しかし，このようにコンテンツの詳細な使用状況が決済センターに知られるということは，個人のプライバシーが決済センターに対して守られてないともいえるため，不快と感じる利用者がいるかもしれない．

本論文では，決済センター側での業務に必要な情報の確保と，利用者側のプライバシー保護という 2 つの要求を両立する使用記録の回収方法を提案する．2 章では超流通の概要を述べ，従来の手法とその問題点について検討する．3 章では提案手法について解説し，4 章では結論を述べる．

2. 超流通と使用記録の回収

2.1 超流通の概要

超流通システムにおけるコンテンツには，超流通ラベルと呼ばれる使用許諾条件が付加されている．一般的には「料金の支払い」が指定されることになるだろう．超流通ラベルやコンテンツは暗号によって保護される．利用者の手元の装置には，超流通ラベルリーダ（SdLR: Superdistribution Label Reader）がある．SdLR は超流通ラベルを復号し，その内容に基づいて適切な権利処理の下にコンテンツの利用を許諾し，使用記録を管理する．

SdLR は，システム管理者ではなく利用者の手元で料金の精算にかかわるデータを取り扱う．そのため利用者がだれにも監視されずに攻撃ができることを想定したシステム設計が重要となる．たとえば，SdLR では認証やコンテンツの復号など様々な場面で暗号技術を利用するが，それらの暗号鍵は利用者に対しても秘密にされる．SdLR が作成する使用記録も利用者による改ざんから保護されなければならない．これらの防御は，たとえば耐タンパー・モジュールに SdLR を納めることによって実現される．

2.2 使用記録の回収（図 1）

使用記録は，たとえば一定期間ごとに決済センターに回収される．このセンターは必ずしも集中管理とは限らず，むしろインターネットサービスプロバイダのように，広く分散して配置される可能性が高い．回収の方法は，システムの設計によって様々な形態が考えられる[3]．たとえば，コンビニエンスストアに設置された回収用端末に使用記録が格納された IC カードを挿入することで回収する方法，自宅からインターネットサービスプロバイダを通してセンターに接続して回収する方法などが考えられる．滞納を抑制するために，未回収の使用記録の料金が一定額を超過した場合には，使用記録の回収以外の機能を停止する．決済センターでは，回収した使用記録に基づいて利用者から料金を徴収し，コンテンツ提供者に料金を分配する．

SdLR から回収される使用記録の 1 つのレコードには論理的に以下の項目が含まれる．

- ユーザ ID（U_{id}）：超流通システムにおいて利用者を識別するための情報である．超流通システムの利用契約時に発行され，料金を引き落とすための口座との対応付けなどが行われる．
- コンテンツ ID（C_{id}）：超流通システムで流通するコンテンツを一意に識別するための情報である．コンテンツ ID からコンテンツ提供者を特定でき

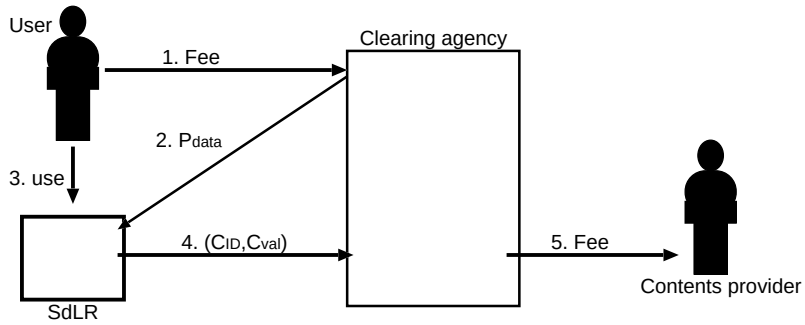

図 2 プリペイド方式における使用記録の回収
Fig. 2 Protocol to collect usage records in a prepaid-system.

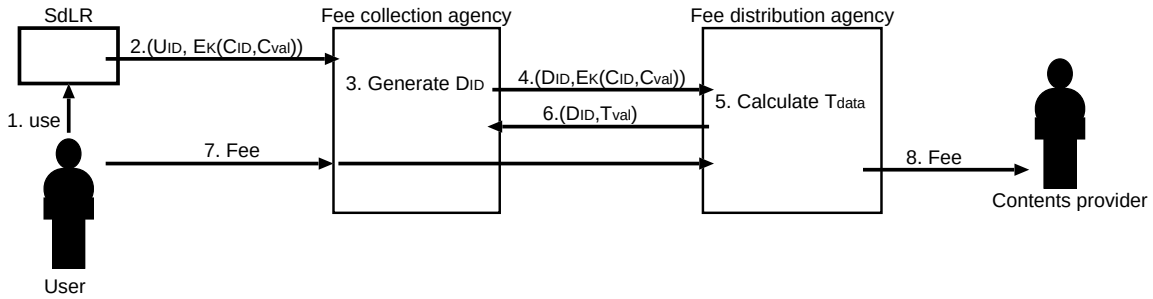

図 3 センター分割方式での決済方法
Fig. 3 Protocol to collect usage records with two agencies.

るので，料金の支払先を判断することができる．

コンテンツ利用量（C_{val}）：料金徴収の基となる情報であり，コンテンツの利用にともなって SdLR が更新する．

超流通システムにおいて，使用記録の回収が必要である理由は，料金の徴収と分配の相手と額とを決定するためである．これらの情報はすべて決済センターに回収されるため，決済センターは，だれが（ユーザ ID），どのコンテンツを（コンテンツ ID），どれだけ使用したか（コンテンツ利用量）をすべて把握できる．

個人のコンテンツの利用状況が，決済センターに知られない超流通システムの形態として,「プリペイド方式」と「センター分割方式」がある．

2.3 プリペイド方式（図 2）

利用量に基づく課金を行うためには，料金の分配の相手と額を決定するための情報は不可欠である．一方，料金の徴収の相手と額の情報は，コンテンツを利用してから料金を徴収するという後払い方式ではなく，プリペイド方式を採用すれば，使用記録に含める必要がない．プリペイド方式では，分配の対象となる代金はすでに決済センターに集められており，あとは分配の相手と額とを決定する情報のみが必要となる．したがって利用者個人に結び付くユーザ ID は回収すべき情報としては不要であり，匿名のままコンテンツを利用することができるので，利用者のプライバシーが守られる．

プリペイド方式の手順を次にあげる．ここで P_{data} はコンテンツ利用可能額を意味する．

(1) 決済センターは料金とひきかえに SdLR に料金分の P_{data} を送信する．
(2) コンテンツの利用にともなって P_{data} が減算され，使用記録が作成される．
(3) 一定期間経過するか P_{data} の残が 0 になった時点で，SdLR は決済センターに (C_{id}, C_{val}) を送信する．
(4) 決済センターは各 C_{id} について C_{val} を集計し，コンテンツ提供者へ料金を分配する．

プリペイド方式では，利用者はコンテンツの利用に先だって電子的な貨幣を購入しなければならない．したがって，超流通システムとしては徴収洩れの危険性が低いという利点がある．しかし，利用者の利便を考慮した多様な課金が提供できないという欠点がある．

2.4 センター分割方式（図 3）

使用記録に基づいて決済センターが行う主な業務は,「利用者からの料金の徴収」と「コンテンツ提供者への料金の分配」に分けられる．ここで，前者の処理に

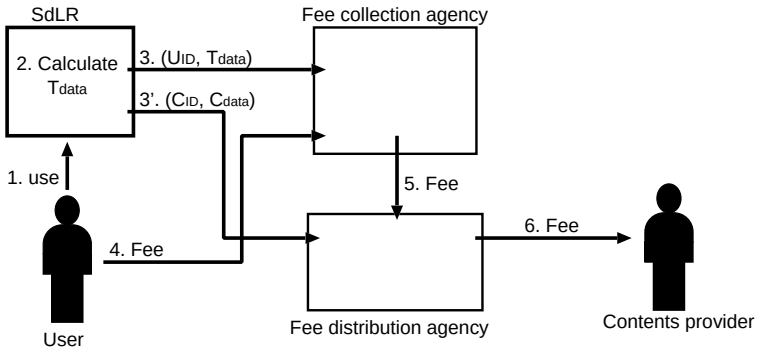

図 4 分割されたセンターに個別に送信する方法
Fig. 4 Protocol to collect usage records separately with two agencies.

ついてはコンテンツ利用量の細目が不要であり，また後者の処理にはユーザ ID が不要である．末松らはここに着目し，利用者のプライバシー保護を目的とした「センター分割方式」を提案した[4]．

センター分割方式では，ユーザ管理センターとソフト管理センターの 2 つの管理センターを置く．ユーザ管理センターは SdLR からの使用記録の回収と利用者からの料金の徴収とを行い，ソフト管理センターはコンテンツ提供者への料金の分配を行う．この 2 つの役割の分割は本質的であるので，本論文ではより明確な表現として，それぞれを「料金徴収センター」と「料金分配センター」と呼ぶことにする．

センター分割方式では，利用者から送信される使用記録は料金徴収センターによって回収される．しかし，コンテンツ ID とその利用量の部分については，料金分配センターの暗号鍵を用いて暗号化されており，料金徴収センターでは復号できない．料金徴収センターは，ユーザ ID を，ユーザ ID とは独立した別の ID に変換してから料金分配センターに送信する．そのため，料金分配センターでは利用者を特定できない．

すなわち，使用記録内のそれぞれの情報が，必要とされる各センターによってのみ入手あるいは復号可能とすることで，利用者のプライバシーを保護している．しかし，この方式では，次のような理由から，実際にプライバシーが保護されているかどうかを利用者が判定することができず，このため依然として心理的な不安が残る．

- 利用者は，料金徴収センターと料金分配センターの間でどのような通信が行われているのかを知ることができない．
- 料金徴収センターに送信されるデータは暗号化されており利用者は内容を確認できない．

3. 提案手法

本章では，上で述べた問題点を解決する使用記録の回収方法を次のような方針に基づいて構築する．

(1) 料金徴収センターと料金分配センターとに，それぞれの業務で必要なデータのみを送信する．
(2) 送信されたデータの内容を利用者が確認できる．

3.1 各センターに送信すべきデータ（図 4）

料金分配センターの主たる業務は，コンテンツ提供者への料金の分配である．分配の相手はコンテンツ ID から判断でき，分配額は，個々のコンテンツごとに利用者すべての利用量の総計が計算できればよい．このために SdLR が料金分配センターに最低限送信しなければならない情報は，コンテンツごとの利用量である．これは提案手法でも単独のセンターを使った超流通システムでも同じである．ただし，提案手法においてはユーザ ID が不要である点が異なる．つまり，プリペイド方式における決済センターと同じ業務を行うことになる．

一方，料金徴収センターでの主たる業務は，利用者が使用したコンテンツの代金の総額を徴収することである．そのためにはユーザ ID と使用料金の合計のみが分かればよく，コンテンツ ID やコンテンツ利用量は不要である．

単独のセンターを使った超流通システムでは，使用料金の総額は，コンテンツごとの使用記録を基に決済センターが計算する．提案手法においては，コンテンツ ID は料金徴収センターに知られたくない情報であるから，利用総額は SdLR が計算し，その結果のみを送信する．このことによって集計処理が分散化され，負荷が決済センターに集中しないという利点もある．

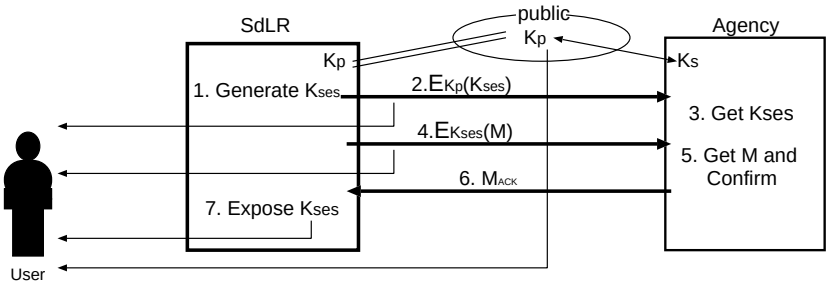

図 5 利用者が送信内容を確認できる通信方法
Fig. 5 Protocol of which users can confirm the message.

3.2 利用者が送信内容を確認できるデータの送信方法（図 5）

料金徴収センターや料金分配センターに送信するデータは，料金の精算に使われるデータであり，利用者による改ざんなどから保護されなければならない．したがって，データを暗号化して送信する必要がある．しかし，暗号通信を行うと，不適切なデータがセンターに送信されていないことを利用者が確認できない．

すなわち，(1) 利用者が攻撃者となりうるという前提の下で SdLR からセンターに対して安全にデータを送信でき，かつ，(2) 利用者が送信内容を確認できるという 2 つの条件を満足しなければならない．

そこで，本節では，SdLR から各センターに，データを安全に送信し，かつ利用者に送信内容の確認が可能な通信方法を提案する．なお，料金徴収センターと料金分配センターがあるが，通信手順は同一であるので以下では単にセンターとする．

3.2.1 準　　備

センターは，公開暗号系鍵のペア K_S，K_P を生成し，公開鍵 K_P を公開する．また，利用者の手元にある SdLR には製造時に K_P が書き込まれているものとする．

3.2.2 送 信 手 順

SdLR とセンターは，相互の認証を行い通信路を確立した後[5),6)]，次の手順でメッセージ M を送信する．

(1) SdLR は，セッション鍵 K_{ses} をランダムに生成する．この時点で K_{ses} は利用者に対して秘密である．

(2) SdLR は，K_{ses} をセンターの公開鍵 K_P で暗号化し，センターに送信する．送信されるメッセージ M_1 は，
$$M_1 = E_{K_P}(K_{ses})$$
である．

(3) センターは，秘密鍵 K_S を用いて，M_1 を復号し，K_{ses} を得る．

(4) SdLR はセンターに対して，送信すべきデータ P をセッション鍵で暗号化して送信する．送信されるメッセージ M_2 は，
$$M_2 = E_{K_{ses}}(P)$$
である．

(5) センターは，セッション鍵 K_{ses} を用いて，M_2 を復号し，P を得る．

(6) センターは受信したデータ P の内容を検証し，問題がなければ，SdLR に受信完了のメッセージ M_{ack} を送信する．

(7) SdLR は，M_{ack} を受信後，利用者に対してセッション鍵 K_{ses} を開示する．

3.2.3 利用者による送信内容の確認方法

ここでは，利用者が送信内容を確認する方法について述べる．

利用者は送信されたメッセージを記録することで M_1 および M_2 を入手することができる．さらに，利用者は，SdLR がセンターにデータを送信した後に，そのとき使用されたセッション鍵を入手できる．利用者はこの鍵が K_{ses} と同一であるかどうかこの時点では判断できないので K'_{ses} とする．なお，利用者にとって，センターの公開鍵 K_P および暗号アルゴリズム $E()$ は既知であるとする．

(1) 利用者は，公開されているセンターの公開鍵 K_P を用いて，SdLR が開示したセッション鍵 K'_{ses} を暗号化する．
$$M'_1 = E_{K_P}(K'_{ses})$$

(2) $M'_1 = M_1$ であれば，SdLR が開示した K'_{ses} が K_{ses} に等しいと判断できる．また，M_1 で送信された平文が K_{ses} であり，ほかにメッセージが含まれていないことが確認できる．

(3) さらに利用者は，SdLR が開示した K_{ses} を用いて，メッセージ M_2 を復号し，送信されたメッセージ
$$P = D_{K_{ses}}(M_2)$$

を確認することができる．

料金徴収センターと料金分配センターの双方に，個別にデータの送信が行われるため，利用者の手元のSdLRの未回収使用記録は，両方のセンターからの受領確認信号 M_{ack} が得られた時点で送信済みとマークされ，必要に応じて消去できる．

3.3 提案手法に対する議論

本提案手法では，通信内容は暗号化されているため通信を中継する第三者が通信内容を知ることはできないが，通信を妨害することは可能である．この場合，使用記録の回収が正常に完了しないので，SdLR内の使用記録は削除されることはない．したがってこの攻撃によって精算が不正に行われたり，個人情報が漏洩したりすることはない．

一般に分割された送信データを結合する攻撃が考えられる．しかし，提案手法において第三者が傍受できるデータは，それぞれ別個のセッション鍵で暗号化されているため，2つのセッション鍵を入手しない限り平文を得ることができない．セッション鍵を得るには，使用された暗号を解読するか，データ送信の最後の段階で利用者に対して開示されるセッション鍵の情報を得るかのいずれかが必要である．したがって，実用的に十分な強度を持つ暗号方式を採用し，かつ，利用者がセッション鍵を適切に管理すれば，第三者によるデータ結合はできない．

本提案手法では，SdLRから料金分配センターへ直接通信が行われる．特定のSdLRと1対1通信を行うことになり，利用者が特定される可能性が残る．この問題は，(a) センターとSdLRの認証時にSdLRが特定される，(b) 物理レイヤーで通信機器が特定される，という2つの側面から検討する必要がある．

(a) については，センターは正当なSdLRであることさえ確認できれば，本提案のシステムは適切に機能する．このためには，たとえば，すべての正当なSdLRが共通に持つ秘密情報を利用した認証方式を設定することにより，SdLRの個体を識別するマシンIDの使用を回避できる．

一方 (b) については，本提案手法がどのような通信網を利用するかに依存する．特にネットワークによる直接通信の場合には，本提案手法に限らず，一般に起こりうる問題である．物理レイヤーでは通信機器を特定する情報が原理的に不可欠であるが，アドレスの動的割当てや中継サーバなどの既存の技術を用いてセンターに間接的に接続することで，個体の情報をセンターに対して隠蔽することができる．

3.4 検証用データIDの付加

末松らによる方式では，センターは分割されているが，SdLRからの通信は一度でよく，そのため各センター間でのデータの対応付けは最初にデータを受け取るユーザ管理センターが生成すればよかった．

しかし本提案手法では，SdLRから両センターへそれぞれ直接に通信が行われる．したがって，なにか問題が発生した場合に，両センターへ送信された通信の整合性を検証できる手段を設けておくことが必要である．

センター分割方式の場合には，料金徴収センターが，ユーザIDを独立したデータIDに変換することによって，その機能を実現していた．本手法では，両センターに送信されるデータは個別であるため，このデータIDに相当するものは発信元であるSdLRが生成することになる．

SdLRが両センターに送信するデータに共通のデータIDを添付することによって，必要ならば，両センターに送信したメッセージの対応関係を検証できる．

ここで，利用者のプライバシー保護の観点から，生成されるデータIDは次の条件を満足しなければならない．

- データIDから，ユーザIDなどの利用者を特定する情報が得られないこと．
- 異なる利用者や異なる通信のセッションに対して，同一のデータIDが生成されないこと．
- データID中にその他のメッセージが格納されていないことを，利用者が確認できること．

これを満足する方法として，データID（ID_{data}）をSdLRのマシンID（$ID_{machine}$）とデータを送信した日時（$time$）を，一方向性関数 $f()$ により変換して生成する手法を提案する．

$$ID_{data} = f(ID_{machine}|time)$$

マシンIDはユーザIDとは直接関係せず，さらに，この情報をデータIDから求めることは，一方向性関数 $f()$ によって不可能である．

データID中に他のメッセージが格納されていないことは，$ID_{machine}$ および $time$ をSdLRが利用者に開示することによる．利用者は，

$$f(ID_{machine}|time)$$

を計算し，送信されたものとの一致を確認することによって，データIDに意図しないメッセージが混入していないことを確認できる．

なお一方向性関数がハッシュ性を持つ場合には，データIDは必ずしもユニークにならない．近い時刻において同一のデータIDが生成される確率が十分に小さ

ければ，セッションに付随する他の記録を補足情報とすることで，対応する両センターへの通信を特定できると思われる．ユニークであることを確実に保証したい場合には，ハッシュ性を持たない変換関数を用いればよい．

4. おわりに

超流通システムでは，コンテンツの使用記録を回収し，この情報に基づいて料金の徴収とコンテンツ提供者への分配が行われる．このとき回収される使用記録には，ユーザ ID とコンテンツごとの利用量の情報が含まれている．

SdLR とセンターとの間の通信を改ざんすることができれば，利用者は自分の支払いを免れることができる．したがって，SdLR は，攻撃者の手元に存在するという状況の下で，決済センターに精算のためのデータを安全に送信しなければならず，また，正当な利用者に対して送信内容を確認する手段を提供できることが望ましい．

本論文では，使用記録の内容を，料金の徴収に必要なデータと料金の分配に必要なデータとに分離し，それぞれを料金徴収センターと料金分配センターに送信する方式を示した．また，それぞれのデータの送信方法については，適切にセンターにデータが送信された後に，利用者が送信データの内容を確認することによって，利用者のプライバシーに関する情報が不正に送信されていないことが確認できる手法を提案した．

参考文献

1) 森　亮一，河原正治：歴史的必然としての超流通，情報処理超流通・超編集・超管理のアーキテクチャシンポジウム論文集，Vol.95, No.1, pp.67–76 (1994).
2) 工藤育男：インターネットの匿名性は強くない，むしろプライバシー侵害の方がおそろしい，情報処理，Vol.40, No.4, pp.388–390 (1999).
3) 森　亮一：コンテンツとハイパーリンクの構造，映像情報メディア学会誌，Vol.53, No.7, pp.948–955 (1999).
4) 末松俊成，今井秀樹：ユーザのプライバシー保護が可能な超流通ラベル配送形超流通システム，電子情報通信学会論文誌，Vol.J81-A, No.10, pp.1377–1385 (1998).
5) 岡本龍明，山本博資：現代暗号，産業図書 (1997).
6) 情報理論とその応用学会：暗号と認証，培風館 (1996).

(平成 12 年 4 月 20 日受付)
(平成 12 年 9 月 7 日採録)

大瀧　保広（正会員）
昭和 41 年生．平成 6 年筑波大学大学院工学研究科電子・情報工学専攻修了．同年茨城大学工学部情報工学科助手．専門は超流通システム．電子情報通信学会会員．

河原　正治（正会員）
昭和 37 年生．平成 3 年筑波大学大学院修士課程理工学研究科修了．同年筑波大学電子・情報工学系助手．平成 4 年より筑波技術短期大学助手．専門はソフトウェア超流通．電子情報通信学会，ACM，IEEE-CS 各会員．平成 12 年より本学会電子化知的財産・社会基盤研究会幹事．