電子化知的財産・社会基盤　8－6
（2000．6．2）

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

茨城大学 工学部 情報工学科

超流通では，所有ではなく利用に応じた課金を行なうために，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とコンテンツ毎の利用量の情報が含まれているため，決済センターはユーザ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．末松らは，ユーザのプライバシ保護のために，決済センターにおける徴収と分配の機能を分離するセンタ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なわれ，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とから，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ユーザのプライバシーをより良く保護する．また，送信される情報をユーザ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

OHTAKI Yasuhiro

Department of Computer and Information Sciences,
Ibaraki University

Superdistribution is a method of distributing digital information in which a fee is charged based on the amount of usage. Usage records are automatically sent to a clearing agency, which then collects the fees from users and distributes them to the copyright holders. The usage record contains, at a minimum, a user-ID, a content-ID, and the amount of usage. 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.

In this paper we present an enhanced version of that implementation. We describe how the information sent to the agencies 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」ではなく「利用」に対する使用記録が管理され，それを回収することによって，コンテンツ提供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さまざまな経路を使って無制限に配布することができる．

プライバシーの保護は，インターネット利用者の主な関心事の一つであり，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，ユーザ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挙げられる．

一般的な超流通システムでは，決済センターによって一定期間毎に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なうために必要な情報であり，決済センターは，誰がどのコンテンツをどれだけ使用したかを把握できる．

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ことは，多くのユーザにとって快適ではない．本稿では，決済センター側での業務に必要な情報の確保と，ユーザ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 超流通における使用記録の回収の概要

超流通システムで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．利用者の手元の装置には，超流通ラベルリーダ (SdLR, Superdistribution Label Reader) があり，コンテンツに付加している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を行ない，使用記録を管理する．

使用記録は，あらかじめ定められルールに基づいて決済センターに転送される．たとえば，ある一定期間が経過する，または未回収の使用記録の料金が一定額を超過した場合などの条件を指定することができる．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一つのレコードには論理的

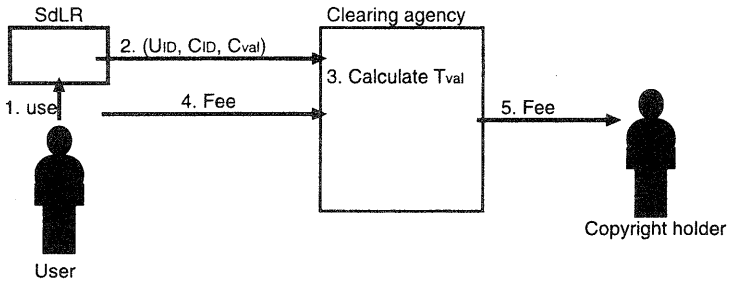

図 1: 通常の超流通における使用記録の回収

に以下の項目が含まれる．

- ユーザ ID U_{id}
- コンテンツ ID C_{id}
- コンテンツ利用量 C_{val}

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，誰が (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) を全て把握できる．

2.1 プリペイド方式

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，前述のように，料金の徴収と分配の相手と額とを決定するためである．このうち料金の分配方法を決定するための情報は，利用量に基づく課金を行なうために不可欠である．

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，プリペイド方式では，利用者個人に結び付くユーザ ID が不要であり，匿名のままコンテンツを利用することができるので，ユーザ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挙げる．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. 一定の期間や P_{data} の残が 0 になると SdLR は決済センターに (C_{id}, C_{val}) を送信する．
3. 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ため，徴収洩れの危険性が低いという利点がある．しかし，後払い方式のほうがユーザの利便を考慮した多様な課金が提供できる．そこで本稿では後払い方式を前提とする．

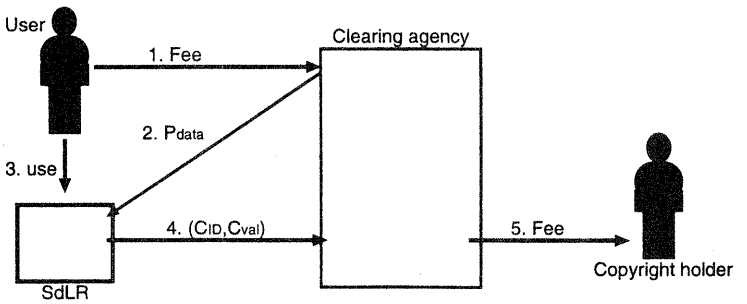

図 2: プリペイド方式における使用記録の回収

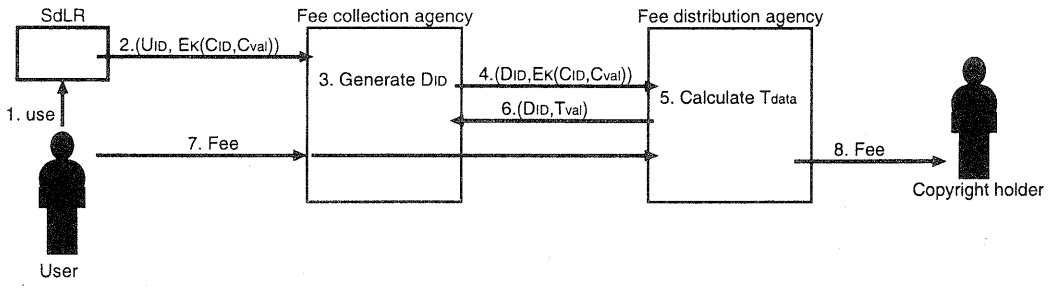

図 3: センター分割方式での決済方法

2.2 センター分割方式

使用記録に基づいて決済センターが行なう主な業務は,「ユーザからの料金の徴収」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 [3].

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ユーザからの料金の徴収とを行ない，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なう．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．これらのセンターは必ずしも集中管理を意味せず，むしろコンビニエンスストアの窓口のように広く分散して配置される可能性が高い．

ここで，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が，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，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．

この方式では，つぎのような理由から，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ない．

- 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な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．

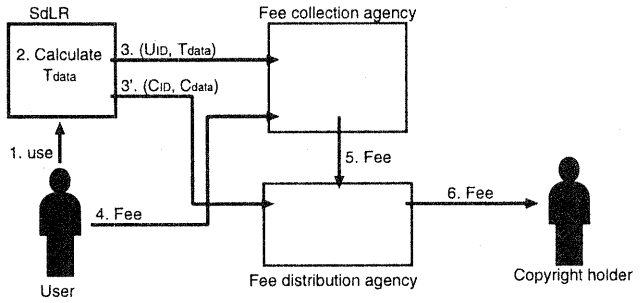

図 4: 分割されたセンターに個別に送信する方法

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

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．分配先はコンテンツ ID から判断できるので，あとはコンテンツ毎の利用量の総計がわかれば十分である．

SdLR では，コンテンツ毎に使用記録を管理しているため，コンテンツ毎の利用量を送信しなければならない．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．

一方，料金徴収センターでの主たる業務は，ユーザ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わかればよく，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，コンテンツ毎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 自体が計算し，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．

3.2 利用者が送信内容を確認できるデータの送信方法

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，暗号通信を行なうと，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元で 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，本章では，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．

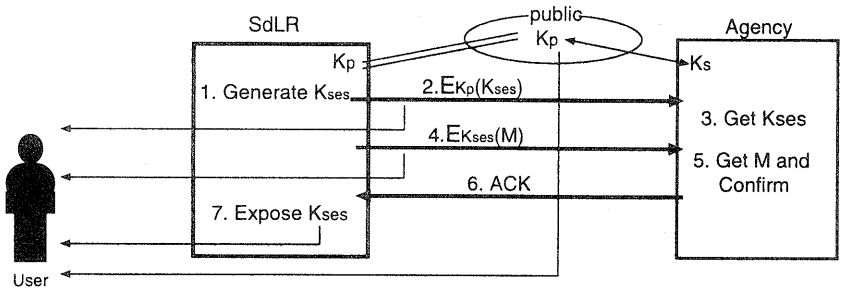

図 5: 利用者が送信内容を確認できる通信方法

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，ユーザの手元にある 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，相互の認証を行ない通信路を確立した後 [4, 5]，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，その時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，他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なわれるため，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 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づけは最初にデータを受け取るユーザ管理センタが生成すればよかった．

しかし本提案手法では，SdLR から両センターへのそれぞれ直接に通信が行なわれる．従って，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 などのユーザを特定する情報が得られないこと
- 異なるユーザや通信に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．

そこで，データ ID ID_{data} は，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．なおデータ IDID_{data} は一方向性関数の性質から，厳密にユニークとなる保証はないが，同一のデータ ID が生成される確率は十分に低く，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することは十分可能であろう．

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．

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，この情報にもとづいて料金の徴収とコンテンツ提供者への分配が行なわれる．このとき回収される使用記録には，ユーザ ID とコンテンツ毎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，決済センターに安全に精算のためのデータを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．

本稿では，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, 情報処理学会誌, Vol. 40, No. 4, pp. 388–390 (1999).

[3] 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).

[4] 岡本龍明, 山本博資: 現代暗号, 産業図書 (1997).

[5] 情報理論とその応用学会: 暗号と認証, 培風館 (1996).