社団法人　情報処理学会　研究報告
IPSJ SIG Technical Report

2004－ＣＳＥＣ－26　(22)
2004／7／20

マーケティング情報が保護された委託配信システムにおける通信頻度の削減

藤原 晶† 岡村 真吾† 吉田 真紀† 藤原 融†

†大阪大学大学院情報科学研究科 〒565-0871 大阪府吹田市山田丘 1-5

E-mail: †{a-fujiwara, s-okamur, maki-yos, fujiwara}@ist.osaka-u.ac.jp

あらまし　ディジタルコンテンツ配信において，コンテンツ提供者が配信基盤をもつISP等に配信と課金を委託する形態を考える．配信サービスにおけるマーケティング情報としてコンテンツの視聴動向（コンテンツがどのような視聴者にどのぐらい配信されたか）がある．これはコンテンツ提供者にとって利益に関わる重要な情報である．著者等はこれまでにコンテンツの視聴動向をコンテンツ提供者だけが知ることのできるような委託配信システムを提案した．委託配信システムではコンテンツ提供者と委託先間の通信頻度が少ないことが望まれるため，本稿では課金に関する通信の頻度を従来システムより削減したシステムを提案する．なお提案方式においても従来システムで保証されていた加入者のプライバシ保護や，請求金額の正しさは保証される．

キーワード　コンテンツ配信，委託配信，視聴動向，プライバシ保護

Reducing Frequency of Communication on the Consignment Delivering System Protecting Marketing Information

Akira FUJIWARA† Shingo OKAMURA† Maki YOSHIDA† and Toru FUJIWARA†

† Graduate School of Information Science and Technology, Osaka University

1-5 Yamadaoka, Suita-shi, Osaka, 565-0871 Japan

E-mail: †{a-fujiwara, s-okamur, maki-yos, fujiwara}@ist.osaka-u.ac.jp

Abstract　A digital contents delivering system is considered, where contents providers consign delivering and charging to distributors who have infrastructures of delivering, e.g. Internet Service Providers (ISP). One of marketing information in delivering services is the result of an audience rating survey. This information is important for contents providers, since it is useful to make their profit. We proposed a consignment delivering system in which only a contents provider can know the result of an audience rating survey for contents of which he consigned delivering. In this paper, the system is improved to reduce the frequency of communication relating charging. The privacy of subscribers is protected and the correctness of charging is guaranteed in the improved system as in the previous system.

Keyword　consignment delivering of contents, audience rating survey, protection of privacy

1 まえがき

ディジタルコンテンツ配信サービスのサービス形態として，コンテンツをもつ制作会社等が配信基盤と利用料金徴収基盤をもつインターネットサービスプロバイダ等に配信と課金を委託する形態が増えつつある．このような形態の配信サービスを**委託配信サービス**と呼び，コンテンツをもつ者をコンテンツ提供者，配信基盤と利用料金徴収基盤をもつ者を配信者と呼ぶ．

委託配信サービスではコンテンツ提供者は配信者にあらかじめコンテンツを渡しておく．配信者は自らが確保した加入者からの要求に応じてコンテンツを配信する．また，一定期間ごとに配信者は加入者に対して利用料金の請求・徴収を行い，コンテンツ提供者は配信者に対して，配信者が徴収した利用料金の一部である分配金の請求・徴収を行う．

委託配信サービスにおけるコンテンツ提供者の利点は，多くの配信者に委託することで加入者の確保が容易にできることである．また，自らが配信基盤と利用料金徴収基盤を準備する必要もない．一方，配信者の利点は，多くのコンテンツ提供者から受託することでコンテンツの収集が容易にできることである．

委託配信サービスで満たされるべき安全性要件と

して，サービス参加者の利益に関わる要件と加入者のプライバシ保護に関わる要件が挙げられる．まず，サービス参加者の利益に関わる要件として三つ示す．一つ目の要件は，配信者が委託されたコンテンツを，コンテンツ提供者に無断で配信(横流し)できないことである．二つ目は，利用料金と分配金の請求が正しく行われることである．具体的には，請求金額について，請求する側が正しく把握できるようにした上で，過大請求を防止することである．三つ目は，コンテンツの視聴動向を，そのコンテンツの配信を委託したコンテンツ提供者だけが把握し，それ以外の者から秘匿することである．なお，コンテンツの視聴動向とは，各コンテンツの配信回数と各コンテンツがどのような加入者に視聴されたかという情報である．この情報は，コンテンツ提供者にとって利益に関わる重要な情報であるため，この要件を満たすことが要求される．加入者のプライバシ保護に関わる要件として，加入者の視聴履歴をその加入者以外の者から秘匿することが挙げられる．加入者の視聴履歴とは，その加入者がどのコンテンツを視聴したかという情報である．

我々は[1]で上記の要件がすべて満たされる委託配信プロトコルを提案した．そのプロトコルでは加入者がコンテンツを要求する度に，コンテンツ提供者と加入者が配信者を介して通信することにより要件が満たされる．しかし，委託配信システムではコンテンツ提供者と配信者間の通信頻度が少ないことが望まれる．

そこで本稿では，[1]で提案したプロトコルと同じ安全性要件を満たしつつ，コンテンツ提供者と配信者間の通信頻度を削減したプロトコルを提案する．委託配信サービスでは請求が一定期間ごとに行われるため，請求の正しさを保証するための通信は請求に合わせて一定期間ごとに行われることが望ましい．そこで，提案プロトコルでは請求の正しさを保証する部分の通信頻度を削減した．これにより一定期間内に $n(\geq 1)$ 回の配信と 1 回の請求が行われた場合，[1]のプロトコルでは総通信回数が $(10n+1)$ 回であるのに対し，提案プロトコルでは $(9n+2)$ 回となる．通信回数は，コンテンツ提供者から配信者へデータが送信された場合，もしくは配信者からコンテンツ提供者へデータが送信された場合を 1 回とする．提案プロトコルの総通信量は[1]のプロトコルとほぼ同じである．

なお，請求の正しさを保証する部分以外の通信頻度も削減し，配信時におけるコンテンツ提供者と配信者間の通信をなくすことは考えない．その理由は，本稿では実装の容易さを維持できるように[1]と同じ暗号技術だけを用いて設計することを考えており，その設計方針において配信時の通信を行わない現実的なプロトコルを設計することは困難と判断したためである．

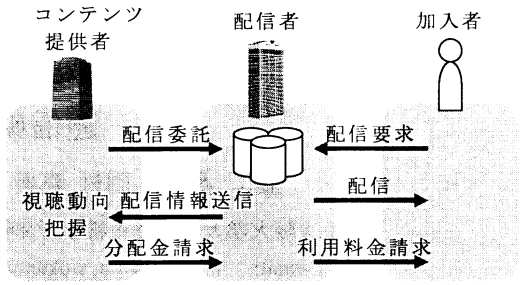

図 1 サービスモデル

ただし，通信を行うことによる利点もある．それはコンテンツ提供者がリアルタイムに視聴動向を把握でき，視聴動向から得た情報を即座に配信サービスに反映させることができるという利点である．それによって例えば，人気のないコンテンツの配信期間を短縮することが可能となる．

本稿の構成を以下に示す．2 章ではサービスモデルについて述べ，3 章では提案プロトコルの前提条件を示す．なお，この前提条件は[1]と同じである．4 章では[1]のプロトコルの概要を述べる．5 章で[1]のプロトコルより通信頻度を削減したプロトコルを提案し，6 章で安全性と効率を評価する．最後に，7 章で全体のまとめと今後の課題について述べる．

2 サービスモデル

2.1 各参加者が行う処理

委託配信サービスのモデルを図 1 に示す．本モデルでは，コンテンツ提供者と加入者が直接通信することはなく，配信者を介して通信する．また，コンテンツ提供者は複数の配信者に配信を委託でき，同様に配信者は複数のコンテンツ提供者から配信を受託できるものとする．以下では，図 1 に示した各参加者が行う処理について述べる．

- **コンテンツ提供者** コンテンツをあらかじめ各配信者に渡しておくことで配信を委託する．委託した配信者から配信に関する情報として，分配金の金額に関する情報及び，視聴動向の把握に必要となる情報を得る．一定期間ごとに，各配信者から配信されたコンテンツの利用料金の総額を計算し，分配金を配信者に請求する．また，各コンテンツについて，配信先の加入者の属性情報を得て，それを元に各コンテンツの視聴動向を得る．属性情報とは性別，年齢等，加入者の性質に関する情報である．ただし，氏名，住所等，個人を特定できる情報は含まないものとする．本稿では，加入者個人を特定できる情報を属性情報と区別して個人特定情報と呼ぶ．
- **配信者** 各コンテンツ提供者から委託されたコンテ

ンツを，自分が確保した加入者に対して要求に応じて配信する．また，配信に関する情報としてコンテンツ提供者に，分配金の金額に関する情報及び，視聴動向の把握に必要となる情報を送信する．一定期間ごとに，各加入者の利用料金の総額を計算し，利用料金を加入者に請求する．また全加入者の利用料金の総額をコンテンツ提供者ごとに整理することで，コンテンツ提供者からの分配金の請求金額が正しいかどうか確認する．

- **加入者** 加入先の配信者にコンテンツを要求し，配信してもらう．一定期間ごとに利用料金の総額を計算し，配信者からの利用料金の請求金額が正しいかどうか確認する．

実際のサービスでは利用料金や分配金の請求を行った後に，それらを徴収する処理も必要となるが，この処理は金融機関等により正しく行われるものとして，本稿では考えない．

2.2 安全性要件

1 章で述べた要件を 2.1 節の処理にあわせて詳しく述べる．サービス参加者の利益に関わる要件が要件 1〜3 に，加入者のプライバシ保護に関わる要件が要件 4 に対応する．

要件 1（無断で配信されないことの保証） 配信者が委託されたコンテンツを配信した場合，委託したコンテンツ提供者は配信が行われたことを知ることができる．

要件 2（請求の正しさの保証） 配信者がコンテンツを配信した場合，その配信者は配信コンテンツ特定情報を知らなくても配信コンテンツに対する利用料金を正しく把握できる．コンテンツ特定情報とは，コンテンツ名等，コンテンツを特定できる情報である．また配信者は利用料金として正しい金額を請求した場合はその正しさを証明できるが，過大な金額を請求したとしてもその正しさを証明できない．コンテンツ提供者は，各配信者に委託したコンテンツが配信された場合，配信コンテンツに対する分配金を正しく把握できる．またコンテンツ提供者は分配金として正しい金額を請求した場合は正しさを証明できるが，過大な金額を請求したとしてもその正しさを証明できない．

要件 3（各コンテンツの視聴動向の秘匿） 各コンテンツの視聴動向は，そのコンテンツの配信を委託したコンテンツ提供者だけが正しく把握でき，そのコンテンツ提供者以外の者は把握できない．各コンテンツの視聴動向とは，各コンテンツの配信回数及び，コンテンツの配信を要求した加入者の属性情報と配信コンテンツ特定情報の対応である．

要件 4（各加入者の視聴履歴の秘匿） 各配信における配信先の加入者の個人特定情報と配信コンテンツ特定情報の対応は，配信先の加入者以外の者は把握できない．

なお，本稿では，利用料金から視聴動向や視聴履歴が把握されることを防止することは対象外とする．また，加入者によるコンテンツの不正コピーの流出など，一度加入者に配信されたコンテンツの再配信は対象外とする．

3 前提条件

本稿で提案するプロトコルでは，以下の 4 つの条件を前提とする．なお，この条件は[1]と同じであり，その妥当性については[1]を参照のこと．

条件 1 加入者はあらかじめ，コンテンツ提供者と配信者の署名検証鍵（認証局の証明書付）を入手している．また，コンテンツ提供者は配信者の，配信者はコンテンツ提供者の署名検証鍵（認証局の証明書付）を入手している．

条件 2 加入者はあらかじめ，個人特定情報，利用料金請求先情報（クレジットカード番号等），署名検証鍵（認証局の証明書付）を配信者に登録している．

条件 3 加入者はあらかじめ，属性情報と署名検証鍵を匿名でコンテンツ提供者に登録しており，コンテンツ提供者から個人識別子（ID）を発行されている．ただし，コンテンツ提供者に登録する署名検証鍵は認証局には登録しない．なぜならば認証局に登録した場合，証明書により個人特定情報が知られてしまうからである．また，ID と署名検証鍵は，配信者も把握しており，個人特定情報とともに保存される．

条件 4 コンテンツ提供者と配信者間，配信者と加入者間の各通信は安全である．通信が安全であるとは以下を満たすことをいう．

- 盗聴により通信内容が漏洩することはない．
- 通信内容が改ざんされた場合，データ受信者が改ざんを検知できる．
- なりすまして通信することはできない．

4 従来の委託配信システム

本稿で提案するプロトコルは，[1]のプロトコルを改良したものである．そこで[1]の設計方針とプロトコルの概要について述べる．

4.1 設計方針

プロトコル全体の設計方針として，実装が容易にできるように既存の一般的な暗号技術(例えば対称・非対称鍵暗号，ディジタル署名等)だけを用いている．また，プロトコルの安全性が特定の暗号化方式，署名方式等に依存しないようにしている．

委託配信システムにおいて最も問題となるのは，配信者の不正である．なぜならば，コンテンツ提供者と加入者は直接通信することがなく，必要な情報は配信者を介して入手するためである．よって，配信者が仲介データを改ざんした場合や，過去に送られたデータにすり替えた場合に，そのデータを受信するコンテンツ提供者や加入者が改ざんやすり替えを検知できるようにする．

改ざんやすり替えを検知できるようにするために，コンテンツ提供者や加入者がデータを送信する際に，トランザクションごとに異なる処理識別子を含め署名を付けた上で送信する．トランザクションとは配信処理の開始から終了までのことである．また，加入者が署名を付ける際は，前提条件3でコンテンツ提供者に登録した署名検証鍵を用いる．以下では，配信者による改ざんやすり替えを検知できるという前提のもとで，2.2節の要件を満たすための[1]の設計方針を述べる．

- **無断で配信されないことの保証** 配信者は加入者からの配信要求をコンテンツ提供者へ転送したとき，そのときに限り，要求されたコンテンツを配信できるようにする．そのために，コンテンツ提供者はコンテンツを暗号化して配信者へ渡しておく．配信者が加入者からの要求をコンテンツ提供者へ転送したときに，コンテンツ提供者はコンテンツを復号するための鍵を，要求元の加入者だけが復号できるように暗号化して配信者へ渡す．
- **請求の正しさの保証** 各配信においてコンテンツ提供者は加入者からの配信要求を受け取ることで利用料金を正しく把握できる．したがって，配信者がコンテンツ提供者の把握する分配金を実際よりも減らして，実際の金額との差分を利益として得るという不正が防止される．また，配信者が利用料金を正しく把握できるようにするために，コンテンツ提供者は利用料金を加入者に提示し，加入者はその金額に同意したことを配信者に示す．

  次に，コンテンツ提供者と配信者が請求の正しさを証明できるようにするために，配信時にコンテンツ提供者は配信者から，配信者は加入者から利用料金に対する署名をもらう．そして，コンテンツ提供者と配信者が署名を得たとき，かつそのときに限り，要求されたコンテンツが加入者へ配信されるようにする．配信者は利用料金に対する加入者の署名を加入者に提示して利用料金の請求を行い，コンテンツ提供者は利用料金に対する配信者の署名を配信者に提示して分配金の請求を行う．これによって請求の正しさが証明されるとともに，コンテンツ提供者や配信者が請求金額を水増しして，実際の金額との差分を利益として得るという不正が防止される．
- **各コンテンツの視聴動向の秘匿** コンテンツ提供者は加入者からの配信要求を受け取ることで視聴動向を正しく把握できる．また，加入者が配信要求を，そのコンテンツを提供しているコンテンツ提供者だけが復号できるように暗号化して送信することで，視聴動向をそのコンテンツ提供者以外の者から秘匿できるようにする．
- **加入者の視聴履歴の秘匿** コンテンツ提供者がコンテンツの視聴動向を得られるようにするため，コンテンツ提供者に対しては各配信において，配信コンテンツ特定情報を秘匿せずに配信先の加入者の個人特定情報を秘匿する方針[2][3]で視聴履歴を秘匿できるようにする．また，配信者からはコンテンツの視聴動向を秘匿する必要があるため，配信者に対しては各配信において，配信先の加入者の個人特定情報を秘匿せずに配信コンテンツ特定情報を秘匿する方針[4][5]で視聴履歴を秘匿できるようにする．具体的には，コンテンツ提供者は配信者にコンテンツを暗号化して渡しておき，配信時に要求した加入者だけが復号できるようにして配信する．

表1 プロトコルにおける表記

P	コンテンツ提供者(Provider)
D	配信者(Distributor)
S	加入者(Subscriber)
SK_P	認証局に登録された，P の署名生成鍵
SK_D	認証局に登録された，D の署名生成鍵
SK_S	認証局に登録された，S の署名生成鍵
$SK_{S'}$	P に登録された，S の署名生成鍵
$E_K(X)$	対称鍵暗号化方式によって対称鍵 K でデータ X を暗号化した結果
$S_{SK}(X)$	データ X と署名生成鍵 SK で生成された X に対する署名の組
$A\|\|B$	2つのデータ A，B を連結したデータ

4.2 プロトコルの概要

4.1節の設計方針で設計された[1]のプロトコルの概要を以下に示す．プロトコルは配信委託処理，配信処理，請求処理から構成される．以降の表記は表1にしたがう．

- **配信委託処理** コンテンツ提供者 P は各コンテンツを異なる対称鍵で暗号化する．P は暗号化コンテンツを配信者 D へ渡し，配信を委託する．
- **配信処理** 本処理は，配信準備，要求内容の送信，要求内容の確認，要求コンテンツの配信という4つの部分処理から構成される．以下に各部分処理の概要を述べる．
  - **配信準備処理** 配信に関わるコンテンツ提供者 P，配信者 D，加入者 S が処理識別子 TC を共有し，更に P と S が対称鍵 K を共有する．処理識別子はコンテンツ提供者名，配信者名，加入者の個人識別子，番号等で構成され，トランザクションごと

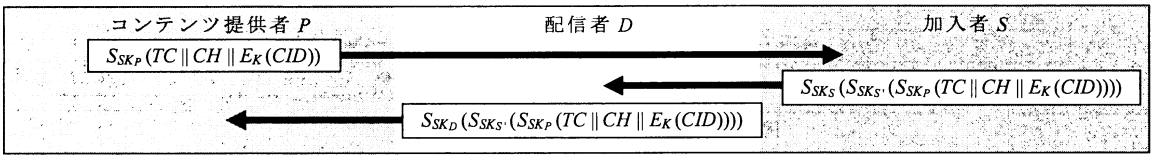

図 2 文献[1]における要求内容の確認処理

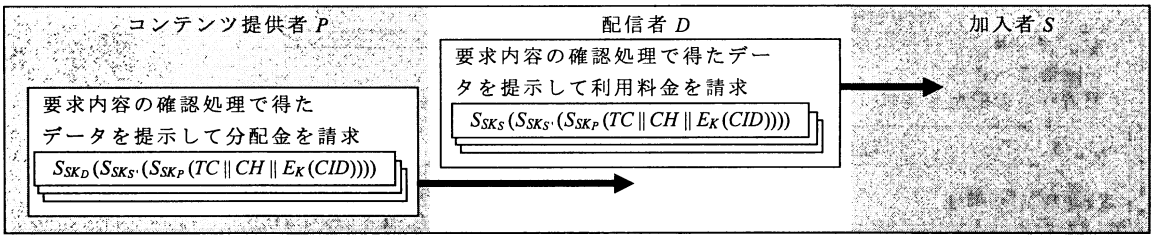

図 3 文献[1]における請求処理

に異なる値をとる．処理識別子共有後の通信データには必ず処理識別子が含まれるとともに，送信者によって生成された署名が付けられる．

- **要求内容の送信処理** S は K で要求コンテンツ特定情報 CID を暗号化し，D を介して P へ送信する．P は S の要求と属性情報（前提条件 3 参照）から，コンテンツの視聴動向を得る．
- **要求内容の確認処理** 処理の流れを以下に示す（図 2 参照）．
  1. P は要求されたコンテンツに対する利用料金の金額 CH と，要求されたコンテンツの特定情報 CID を K で暗号化したものを，D を介して S へ提示する：$S_{SK_P}(TC \| CH \| E_K(CID))$．
  2. S は受信データに付けられた署名から，そのデータが P により生成されたものであることを確認する．そして CH と CID が正しければ，受信データに $SK_{S'}$ を用いて生成した署名を付け，更に SK_S を用いて生成した署名を付けて D へ送信する：$S_{SK_S}(S_{SK_S'}(S_{SK_P}(TC \| CH \| E_K(CID))))$．ここで，$SK_{S'}$ による署名は S が CH と CID に同意したことを，P が確認するために用いられる．また，SK_S による署名は S が CH に同意したことを，D が確認するために用いられる．
  3. D は P が署名を付けて提示した CH に対して，S が同意したことで CH を後で請求できると判断する．D は受信データを，請求時に請求金額の正しさを証明するためのデータとして保存する．そして，SK_S により生成された署名を取り外し，署名を取り外したデータに SK_D を用いて生成した署名を付けて P へ送信する：$S_{SK_D}(S_{SK_S'}(S_{SK_P}(TC \| CH \| E_K(CID))))$．
     SK_S による署名を取り外す理由は，この署名は D が S に利用料金を請求する際に必要となるデータであり，P には必要がないからである．また，SK_D による署名は D が CH に同意したことを，P が確認するために用いられる．
  4. P は受信データから，S が CH と CID に同意したこと及び，D が CH に同意したことを確認する．P は受信データを，請求時に請求金額の正しさを証明するためのデータとして保存する．
- **要求コンテンツの配信処理** P はどの暗号化コンテンツを配信すべきかを D に指示するとともに，暗号化コンテンツを復号するための鍵を K で暗号化し，D を介して S へ送信する．D は P から指示された暗号化コンテンツを S へ配信する．S は暗号化コンテンツを P から受信した鍵を用いて復号する．

- **請求処理** 処理の流れを以下に示す（図 3 参照）．
  一定期間ごとに，配信者は加入者に利用料金を請求し，コンテンツ提供者は配信者に分配金を請求する．請求の際，配信者とコンテンツ提供者は配信処理で保存しておいたデータを提示して，請求金額が過大でないことを証明する．

5 提案プロトコル

4 章で述べた従来プロトコルを改良し，請求の正しさを保証する部分の通信頻度を削減したプロトコルを提案する．前述のように[1]では実装が容易にできるように既存の一般的な暗号技術だけを用い，安全性が特定の暗号化方式や署名方式などに依存しないようにプロトコルを設計している．本稿では[1]と同じ暗号技術だけを用いたままで通信頻度を削減する．なお総通信量は従来プロトコルとほとんど変わらない．以降では，改良方針と改良したプロトコルについて述べる．

5.1 改良方針

改良する部分は，4.2 節で述べた配信処理における要求内容の確認処理及び，請求処理である．文献[1]では，配信者が要求されたコンテンツを加入者へ配信

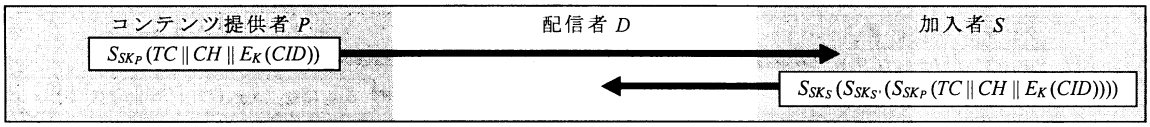

図 4 提案法における要求内容の確認処理

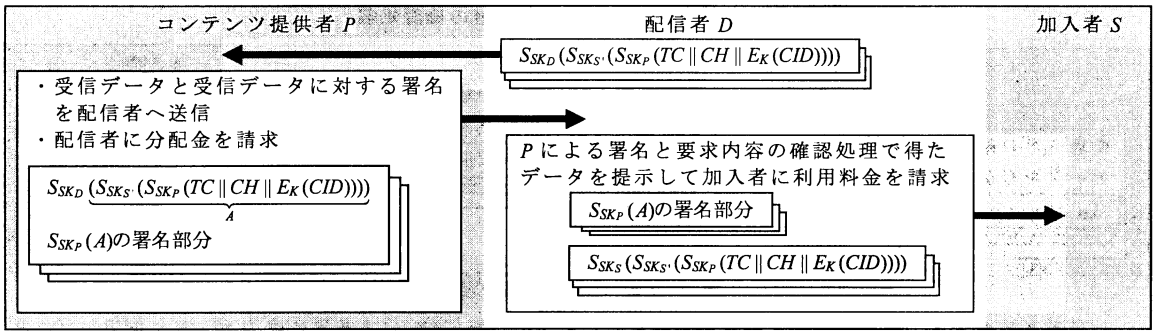

図 5 提案法における請求処理

できるのは，利用料金の金額に対する配信者の署名付きデータをコンテンツ提供者へ送信したとき，かつそのときに限る．提案プロトコルでは通信頻度を削減するために，配信時には，配信者は利用料金の金額に対する自身の署名付きデータをコンテンツ提供者へ送信しなくてもコンテンツを加入者へ配信できるようにする．その代わりに，一定期間ごとに，配信者は利用料金の金額に対する自身の署名付きデータをコンテンツ提供者へ送信する．ただしこのままでは，配信者は利用料金の金額に対する自身の署名付きデータを減らしてコンテンツ提供者へ送信することができる．

そこで，本稿では配信者はコンテンツ提供者が把握した利用料金の金額についてだけ，請求の正しさを加入者に証明できるようにすることを考える．つまり，配信者が利用料金の金額に対する自身の署名付きデータを減らしてコンテンツ提供者へ送信した場合は，加入者に請求の正しさを示すことができる金額も実際よりも少なくなってしまうようにする．これによって，配信者が署名付きデータを減らしてコンテンツ提供者へ送信することを抑止する．

具体的な方針としては，配信者による請求において，請求金額の正しさを示す証拠となるデータを変更する．文献[1]では，利用料金の金額に対して加入者の署名が付けられたデータを証拠とみなしていた．提案プロトコルでは，利用料金の金額に対して加入者の署名が付けられたデータに対して，更にコンテンツ提供者の署名が付けられたデータを証拠とみなす．一定期間ごとにコンテンツ提供者は，分配金の請求金額の正しさを示す証拠，すなわち利用料金の金額に対する配信者の署名付きデータを得られたときに，配信者が請求時に必要とする証拠を生成し配信者へ送信する．

配信処理の残りの部分である要求内容の送信処理及び，要求コンテンツの配信処理における通信の頻度は削減しない．この部分の通信頻度を削減するためには，配信者はコンテンツ提供者と通信することなく（コンテンツ提供者の代わりに），加入者から要求されたコンテンツのコンテンツ特定情報を知ることなく，正しい利用料金に対する加入者の署名を入手でき，暗号化されたコンテンツを要求した加入者だけが復号できるようにして配信する必要がある．しかし，[1]と同じ暗号技術だけを用いて，現実的なプロトコルを設計することは困難と判断し，他の方針で改良することを今後の課題とする．

5.2 プロトコルの改良

5.1 節の設計方針に基づいて改良したプロトコルについて述べる．改良する部分は，配信処理における要求内容の確認処理と，請求処理である．改良後のそれぞれの処理の流れについて以下に示す（図 4，5 参照）．

- **配信処理における要求内容の確認処理**

1. コンテンツ提供者 P は要求されたコンテンツに対する利用料金の金額 CH と，加入者と共有している対称鍵 K で要求されたコンテンツの特定情報 CID を暗号化したものを，配信者 D を介して加入者 S へ提示する：$S_{SK_P}(TC \| CH \| E_K(CID))$．
2. S は受信データに付けられた署名から，そのデータが P により生成されたものであることを確認する．そして，CH と CID が正しければ，受信データに SK_S を用いて生成した署名を付け，更に SK_S を用いて生成した署名を付けて D へ送信する：$S_{SK_S}(S_{SK_S'}(S_{SK_P}(TC \| CH \| E_K(CID))))$．
   ここで，SK_S による署名は S が CH と CID に同意したことを，P が確認するために用いられる．ま

た，SK_Sによる署名はSがCHに同意したことを，Dが確認するために用いられる．

3. DはPが署名を付けて提示したCHに対して，Sが同意したことでその金額を後で請求できると判断する．受信データは請求処理で必要となるため保存する．

- **請求処理**

1. Dは要求内容の確認処理においてSから受信したデータから，SK_Sにより生成された署名を取り外す．取り外す理由は従来プロトコルと同じである．更に署名を取り外したデータにSK_Dを用いて生成した署名を付けてPへ転送する：
$S_{SK_D}(S_{SK_S}(S_{SK_P}(TC \| CH \| E_K(CID))))$．
SK_Dによる署名はDがCHに同意したことを，Pが確認するために用いられる．

2. Pは受信データから，SがCHとCIDに同意したこと及び，DがCHに同意したことを確認する．更に，受信データからDによる署名を取り除いたデータに対する署名を，SK_Pを用いて生成する．受信データ及び，SK_Pを用いて生成した署名をDへ送信する：
$S_{SK_D}(\underbrace{S_{SK_S}(S_{SK_P}(TC \| CH \| E_K(CID)))}_{A}) \| (S_{SK_P}(A)$の署名部分)．
SK_Pによる署名は，Sへの利用料金の請求をPが認めたことを，Dが確認するために用いられる．Pは返信した受信データを請求の正しさを示す証拠として，Dに分配金を請求する．

3. Dは要求内容の確認処理の3において保存したデータ及び，本処理の2においてPから受信したPの署名を請求金額の正しさを示す証拠として，Sに利用料金を請求する．Dが本処理の2において受信したPの署名だけでなく要求内容の確認処理の3におけるデータも提示する理由は，SK_Sによる署名がSによる署名であることを証明するためである．

6 評価

提案プロトコルが2.2節で述べた安全性要件を満たしていることを示す．また，提案プロトコルの通信頻度を[1]と比較する．

6.1 安全性

提案プロトコルでは，[1]と同様にコンテンツ提供者や加入者は送信データに処理識別子を含めた上で署名を付けてから送信しているため，配信者による仲介データの改ざんやすり替えを検知できる．以下では改ざんやすり替えを検知できるという前提のもとで，2.2節の安全性要件が満たされていることを示す．

- **無断で配信されないことの保証** コンテンツ提供者はコンテンツを暗号化して配信者へ渡しており，コンテンツ復号鍵は配信を要求した加入者だけが復号できるように暗号化されて，コンテンツ提供者から加入者へ送信される．そのため，配信者が加入者からの要求をコンテンツ提供者へ転送したとき，そのときに限り，要求元の加入者だけがコンテンツ復号鍵を入手し，コンテンツを得ることができる．したがって，コンテンツ提供者は委託したコンテンツが配信された場合，そのことを知ることができる．
- **請求の正しさの保証** 加入者にコンテンツが配信されるときには，コンテンツ提供者は必ず加入者から要求内容を受け取っている．したがって，コンテンツ提供者は要求内容から配信者への分配金の請求金額を正しく把握できる．また，配信者が一定期間内に配信した各コンテンツの利用料金の金額に対する自身の署名付きデータを実際よりも減らしてコンテンツ提供者へ送信した場合，加入者への請求における証拠は送信した金額に対するものになってしまう．つまり，配信者が加入者に請求できる金額が実際よりも少なくなってしまう．そのため，配信者が署名付きデータを減らしてコンテンツ提供者へ送信することは抑止され，コンテンツ提供者は分配金について正しい金額を請求した場合は，配信者の署名付きデータを提示することでその正しさを配信者に証明できるが，過大な金額を請求したとしてもその正しさを証明できない．一方配信者は各配信において，コンテンツ提供者が提示した利用料金の金額に対して加入者の署名が付けられたデータを入手できるため，加入者への請求金額を正しく把握できる．また，配信者はコンテンツ提供者から，一定期間内に配信した各コンテンツの利用料金の金額に対して加入者とコンテンツ提供者の署名が付けられたデータを得ることができる．したがって，配信者は利用料金について正しい金額を請求した場合は，加入者とコンテンツ提供者の署名付きデータを提示することでその正しさを加入者に証明できるが，配信者が過大な金額を請求したとしてもその正しさを証明できない．
- **各コンテンツの視聴動向の秘匿** 各配信において，コンテンツ提供者は加入者からの要求を受信することで，要求コンテンツ特定情報を得ることができる．また，要求には処理識別子が含まれており，処理識別子には要求元の加入者の個人識別子が含まれる．個人識別子から，あらかじめ登録された要求元の加入者の属性情報がわかる．したがって，コンテンツ提供者は各コンテンツの視聴動向を正しく把握できる．また，前提条件4より，視聴動向は通信相手以外の者から秘匿されている．更に，加入者の要求と

配信されるコンテンツは配信者に知られないように暗号化されているため，配信者は配信コンテンツ特定情報がわからない．したがって，コンテンツの視聴動向はそのコンテンツの配信を委託したコンテンツ提供者以外の者から秘匿される．

- **各加入者の視聴履歴の秘匿** 前提条件 4 より，視聴履歴は通信相手以外の者から秘匿されている．更に，コンテンツ提供者は各加入者を個人識別子で管理しており，各加入者の個人特定情報を把握していない．また各配信において，配信者は配信コンテンツ特定情報を把握できない．したがって，加入者の視聴履歴はその加入者以外の者から秘匿される．

6.2 通信頻度

提案プロトコルと[1]のプロトコルにおける，コンテンツ提供者と配信者間の通信頻度を比較する．配信処理と請求処理各 1 回におけるコンテンツ提供者と配信者間の通信回数を以下で比較する（表 2 参照）．通信回数は，コンテンツ提供者から配信者へデータが送信された場合，もしくは配信者からコンテンツ提供者へデータが送信された場合を 1 回とする．

- **配信処理**
  - **配信準備処理** 両プロトコルともに 6 回である．
  - **要求内容の送信処理** 両プロトコルともに 1 回である．
  - **要求内容の確認処理** 提案プロトコルは 1 回，[1]のプロトコルは 2 回である．
  - **要求コンテンツの配信処理** 両プロトコルともに 1 回である．

  配信処理全体では，提案プロトコルは 9 回，[1]のプロトコルは 10 回である．
- **請求処理** 提案プロトコルは 2 回，[1]のプロトコルは 1 回である．

ここで，$n(\geq 1)$ 回の配信が行われた後に請求処理が行われたとする．このとき，提案プロトコルにおけるコンテンツ提供者と配信者間の総通信回数は，

$$9n+2(\text{回})$$

である．一方[1]のプロトコルにおける総通信回数は，

$$10n+1(\text{回})$$

表 2 通信回数の比較

	提案法	文献[1]
配信処理		
配信準備処理	6	6
要求内容の送信処理	1	1
要求内容の確認処理	1	2
要求コンテンツの配信処理	1	1
配信処理全体	9	10
請求処理		
請求処理全体	2	1

である．したがって，任意の $n(\geq 1)$ に対して，提案プロトコルの通信頻度は[1]のプロトコルの通信頻度以下である．

提案プロトコルの総通信量は[1]のプロトコルとほぼ同じである．その理由は，[1]のプロトコルでは配信処理において配信者からコンテンツ提供者へ送信していたデータを，提案プロトコルでは一定期間ごとに実行される請求処理においてまとめて送信しているからである．ただし，提案プロトコルでは請求処理においてコンテンツ提供者から配信者へ送信されるデータにコンテンツ提供者によって生成される署名が含まれ，配信者はその署名を用いて加入者に利用料金を請求する．したがって，コンテンツ提供者と配信者間，配信者と加入者間の通信量及び，配信者のメモリ量はその署名の大きさだけ増加する．

7 まとめと今後の課題

本稿では，従来の委託配信システムに対して，コンテンツ提供者と配信者間の通信頻度を削減したプロトコルを提案した．ただし，既存の一般的な暗号技術だけを用いてプロトコルを設計することを考えているため，請求の正しさを保証する部分の通信頻度を削減した．

今後の課題として，既存の一般的な暗号技術だけでなく，様々な暗号技術を用いてコンテンツ提供者と配信者間の通信頻度を更に削減することが挙げられる．現状では，コンテンツ提供者は配信のたびに配信者と通信する必要がある．そこで，一定期間ごとにコンテンツ提供者と配信者間で通信を行えば，安全性要件が満たされるように改良する．

文　献

[1] 藤原 晶，岡村 真吾，吉田 真紀，藤原 融，“コンテンツ配信サービス提供者だけが視聴動向を把握できる委託配信システム，” SCIS2004 予稿集，Volume I，pp.487—492，2004.

[2] D. Chaum, A. Fiat and M. Naor, “Untraceable electronic cash,” CRYPTO’88, LNCS 403, pp.319—327, 1988.

[3] 小西 祥之，吉田 真紀，藤原 融，“分岐構造をもつコンテンツに対する分岐選択履歴を配信者から秘匿可能な配信システム，” CSS2003 論文集，pp.367—372，2003.

[4] B. Aiello, Yuval Ishai and Omer Reingold, “Priced Oblivious Transfer : How to Sell Digital Goods,” EUROCRYPT 2001, LNCS 2045, pp.119—135, 2001.

[5] 松尾 真一郎，尾形 わかは，“データ交換可能な多対多マッチングプロトコル，” SCIS2002 予稿集，pp.435—440，2004.