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

2007－ＣＳＥＣ－38（16）
2007／7／19

コンテンツの閲覧制御方式

加藤 岳久†

E-mail : Kato.Takehisa@toshiba-sol.co.jp

†東芝ソリューション株式会社

IT 技術研究所

〒183-8512 東京都府中市片町 3-22

概要 ネットワークの普及に伴い，国内外で無料の動画配信サービスが普及し，利用者が急増している．しかし，そのサービスの多くが広告収入に頼った無料の配信である．このため，配信されるコンテンツの前に流れる広告を閲覧しないと本編のコンテンツが再生されない仕組みを導入しているサービスも出てきた．本論文では，(k, n)しきい値秘密分散法を応用し，意図した順番で閲覧させたり，広告を閲覧させたりすることで本編が再生されるコンテンツの閲覧を制御する方式を示し，秘密分散法を使うことの有効性を示す．

キーワード (k, n)しきい値秘密分散法，コンテンツ配信，閲覧制限

A Method to Limit Appreciation of Content

Takehisa KATO†

E-mail : Kato.Takehisa@toshiba-sol.co.jp

† Toshiba Solutions Corporation

3-22, Katamachi, Fuchu-shi, Tokyo 183-8512, Japan

Abstract.

Free content delivery service spreads worldwide as the network spreads, and the number of users increases rapidly. However, many of the content delivery service rely on advertisement income. Therefore, some services are introduced that uses a mechanism, if the advertisement that should be played ahead of the delivered content is not played. In this paper, we proposed a method to control the content playing that the main volume is played after playing the advertisement by the use of secret sharing scheme.

Keyword (k, n)threshold secret sharing scheme, contents delivery, limited appreciation

1. はじめに

国内では，急速なネットワークの普及に伴い，様々なサービスが展開されている．

そのサービスの一つに，電子書籍や動画に代表されるコンテンツ配信がある．現在，様々な配信業者により展開され，有料，無料を問わず国内で視聴サービスを受ける利用者は急速に伸びている[1]．

2005 年前半までは視聴料収入型の配信モデル，いわゆる有料コンテンツ配信サービスが主体だった．しかし，2005 年後半から広告収入型の視聴サービスに切り替わり，さらに利用者数を伸ばした．

この広告収入型視聴サービスの多くが，本編のコンテンツを再生する前にスポンサーの広告を流し，利用者が閲覧する広告の配信で得られる広告収入により成り立っている．また，本編のコンテンツをダウンロードしている空き時間を埋める，という副次効果もある．

これらの広告は、インターネット上で様々な形態で表示され，呼称も様々である．例えば，ネット CM，動画広告，ストリーミング広告，リッチバナー，フラッシュバナー，などである．

本稿では，テレビ放送で使われるような動画を用いた広告映像を取り扱う．この様な広告をインターネット広告推進協議会では，インターネット CM（コマーシャル）として，以下の様に定義[2]している．

- インターネット，携帯電話を含む通信回線上のサービス（広告主が管理する Web サイトを除く）の広告スペースにおいて，広告主の広

告やマーケティング活動を目的として掲載されるもの
- 広告表現として映像および音声(音楽・ナレーション)を使用し，テレビCMのように時間軸で展開される広告
- 映像技術，配信技術についての区別は特にしないが，配信方式は大きく分けてストリーミング方式(ユーザー側の端末にデータが残らない再生方式)とダウンロード方式(ユーザー側の端末にデータの複製を作成し再生する方式)があり，許諾の条件が違うために区別し，どちらであるか明記が必要

本稿では，インターネット CM が抱える問題点を挙げ，問題点を解決するための方式を提案する．また，それを応用したTV放送におけるCMスキップを対策する方式を提案する．

2. インターネットCMの問題点

現在，無料インターネット動画提供サービスが急速に伸びている．例えば，株式会社 USEN が提供している無料動画配信サービスの視聴登録者数は，2007年4月時点で1,400万人を越えている．他のサービスも，全般的に利用者数を伸ばしている．

それに伴い，インターネット広告費も大きくなり，2006年で3,630億円，2011年で7,558億円と，5 年間で 2 倍以上に拡大すると推測[3]されている．

インターネット CM の効果について調査した結果によれば，ユーザの接触頻度(フリークエンシー)が3〜4回で約62%，8〜10回で約75%，13回以上で約 85%まで認知率が上がる[4]という．

その一方で，将来のテレビへ期待する機能として CM カットを 43%が希望するという結果[5]もある．この様に，インターネット CM のフリークエンシーが多ければ認知度が上がり，その効果が期待できる．しかし，CM カットを要望するユーザも多い．

ここで，広告収入で成り立っている無料配信ビジネスが，インターネット CM を閲覧されないと成立しなくなるという問題を抱えている．

また，多くのビデオレコーダが搭載している CM カットや CM スキップ機能は，広告収入に頼っている民放各局にとって問題である．2004 年 11 月 12 日の民放連会長の記者会見を受けて，メディアで問題になったこともある．

ある調査で，ハードディスク・レコーダ所有者の過半数が CM の 80%をスキップし，損失額も540 億円にのぼる，という結果[8]がでた．このため，留守録された放送番組の CM スキップ対策も問題である．

3. 問題点に対する対策とその課題

2.で示したように，インターネット CM を利用者に視聴させるために，色々な対策が講じられている．

3.1. JavaScript などを使った対策

ストリーム配信されるコンテンツを再生する場合，JavaScript を使って早送りやシークバーを非表示にする，機能を使えなくするなどの対策が一般的である．

即ち，あるコンテンツを視聴する際に，インターネット CM 部分は再生速度を変えられなくしたり，シークバーを非表示にしたりするなどし，本編が始まったら表示するのである．

3.2. クリックさせる対策

3.1.では，本当に視聴したかどうか分からない．

そこで，インターネット CM が終了したら簡単なアンケートなどを取ることで，確実に視聴したことを確認する．

この対策の良い点は，アンケート内容によって消費者のニーズなど統計を取ることができる，という点である．

また最近では，クリック回数に応じてマイレージ・ポイントを付与するサービス[6]もあり，アンケート調査と連動して展開しているケースもある．

3.3. 現状方式の課題

3.1.および 3.2.のどちらも，オンライン接続された状況を想定した対策であり，オフライン環境では利用できない．

OS の環境やクライアントソフトウェアによって使えない場合があるが，ストリーム配信されるコンテンツをローカル環境にダウンロードする無料のツールが流布されている．

これらのツールを使えば，ストリーム配信されているコンテンツもネットワーク接続を必要とせず，かつインターネット CM をカットして視聴しなくても本編を閲覧することができてしまう問題がある．

このためダウンロードされても CM 部分を視聴(再生)しないと，本編が再生されない対策が必要となる．

4. 関連研究

3.で示した課題に対して，CM 部分を利用したコンテンツ保護方式として，平野が発表したコンテンツ保護方式[7]がある．

この方式は，コンテンツの権利保護という立場から有料コンテンツを閲覧できる権利保有者と，そうでない者とを区別する．有料コンテンツを閲覧できる権利保有者は，利用権に応じて有料部分のコンテンツが閲覧できる．

逆に，利用権が無い有料部分のコンテンツに対しては、CM 部分を閲覧させる．CM 部分の閲覧が終ったら，有料コンテンツを閲覧させる，という方式である(図 1)．

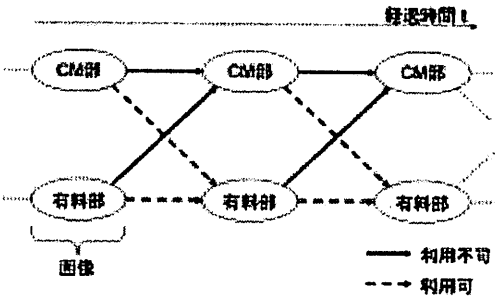

図 1. 平野のコンテンツ保護方式の処理概要

平野の方式では，利用権に従って暗号化されたコンテンツが復号して再生できるか否かを制御する．

コンテンツの保護は，先頭CM画像に暗号鍵を電子透かしとして埋め込んでおく．そして，後続のCM画像に電子透かしとして埋め込まれた暗号鍵関連情報と先の暗号鍵とから，後続する画像の暗号鍵を生成する(図 2)．

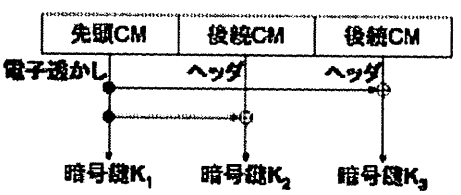

図 2. 平野のコンテンツ保護方式の暗号鍵生成

この方式の特徴は，先頭 CM を再生して電子透かしで埋め込まれた暗号鍵 K_1 を取り出さないと，後続する画像の暗号鍵が作れず再生できなくなる点にある．

平野の方式は，前述したように有料コンテンツの権利保護が目的であり，CM を閲覧させることが目的ではない．

従って，無料配信されるコンテンツに対するインターネット CM などのコンテンツを閲覧させるには，必ずしも適しているとはいえない．

また，CM の利用状況をモニタリングする必要があることから，オンラインでの閲覧が前提であり，オフラインに適用できないという課題がある．

5. 提案方式

本稿では，幾つかの利用状況に応じた方式を提案する．本稿では幾つかの場面を想定し，それぞれの場面に応じた秘密分散法により閲覧制御する方式を述べる．

5.1. 提案方式 1：順番にコンテンツを閲覧させる方式

コンテンツの製作者，もしくは配信者の意図により，例えば複数話で構成されたコンテンツを配信する場合を考える．

また，順番にコンテンツを閲覧すれば，結果的に安価にコンテンツが購入できる，ということも可能な方式である．

提案方式 1 は平野の方式に似ており，基準となる暗号鍵をスタートに，連鎖的に暗号鍵を復元するものである．

本方式では，共通鍵暗号 k_i (i=2,…, m；m はコンテンツの話数)について，例えば

$$k_{i,1} \oplus k_{i,2} = k_i$$

となるように $k_{i,1}$ と $k_{i,2}$ を決め，図 3 の様に暗号化されたコンテンツを配信する．

なお⊕は排他論理和を示し、E(K, M)はメッセージ M を鍵 K で暗号化することを示し，A ‖ B は連接を示す．図 3 の様に，$content_i$(i=1,…,12)と，次の話の暗号鍵 k_{i+1} の分散鍵 $k_{i+1,1}$ を連接し，暗号鍵 k_i で暗号化する．

またヘッダ情報の A001 は，何のコンテンツか示す ID である．001～013 は，そのコンテンツの第何番目の話であるかを示す番号で，この例では 13 話で構成されている．

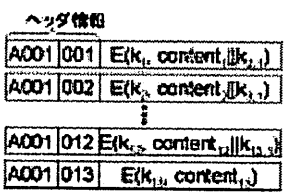

図 3. 提案方式 1 で配信する暗号化コンテンツ

図 3 の様に配信される暗号化コンテンツを順番

に閲覧するために，分散された鍵は図4の様な形式で配信される．

ヘッダ情報の A001 は図 3 と同様にコンテンツを示す ID であり，K001～K013 は第何話の分散鍵であるかを示す分散鍵 ID である．第 1 話だけは分散鍵を使わないので $content_1$ を暗号化した鍵 k_1 を配信する．

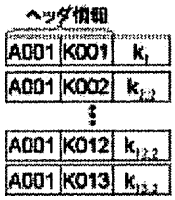

図 4. 提案方式 1 で配信される分散鍵

図 3, 4 で示す暗号化コンテンツと分散鍵を用いて，順番にコンテンツを閲覧するためのプロトコルを図 5 に示す．

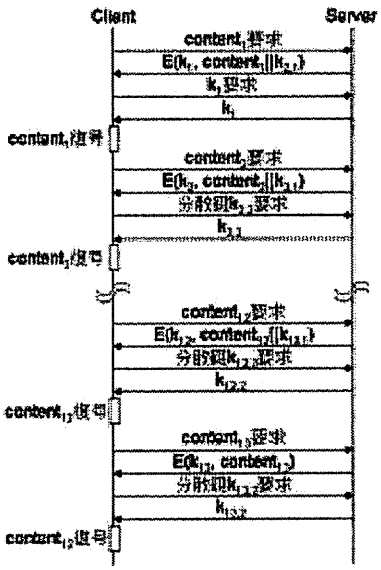

図 5. 提案方式 1 の配信プロトコル

Client から第 1 話のコンテンツ $content_1$ が要求されると，暗号化したコンテンツ $E(k_1, content_1||k_{2,1})$ を Server から送る．

Client は $content_1$ を復号するため暗号鍵 k_1 を要求し，Server より受信する．ここで Client と Server との通信は，SSL などを使い保護されているものとする．暗号鍵 k_1 を受信すると Client は暗号化コンテンツを復号し，$content_1$ と分散鍵 $k_{2,1}$ を取り出す．

引き続き閲覧するため，Client から $content_2$ を要求すると，暗号化コンテンツ $E(k_2, content_2||k_{3,1})$ を Server から受け取る．Client は $content_2$ を復号するため分散鍵 $k_{2,2}$ を要求し，Server より受信する．ここで，$k_{2,1} \oplus k_{2,2} = k_2$ により暗号鍵 k_2 が求められ，$content_2$ および分散鍵 $k_{3,1}$ が取り出せる．

以下，同様にして暗号化コンテンツと分散鍵を要求することで，client は順番にコンテンツを閲覧する．

Client が途中の話を飛ばしたい場合，見たいタイトルの暗号鍵を直接要求すればよい．この様に提案方式1では，分散鍵を要求しているか，暗号鍵を要求しているかを確認すれば，順に閲覧しているか区別できる．

従って，分散鍵と暗号鍵とで価格設定を変えることで，途中の話を飛ばして暗号鍵を要求された場合は価格を高くすることもできる．

また，提案方式はオンライン配信でなくてもよく，ディスクなどに格納した暗号化コンテンツを配布しても良い．

5.2. 提案方式 2：プレミアなコンテンツを閲覧させる方式

以下，提案方式 2 および 3 では，秘密分散法として(k, n)しきい値法を用いるものとする．(k, n)しきい値法は，ある情報を n 個に秘密分散し，秘密分散した任意のk個から元の情報に復元できるというものである．

異なる複数のコンテンツを閲覧した時，例えば前・中・後編からなる三部作の映画を閲覧した場合に，メイキングや特別編の様なコンテンツが見られる場合を考える．

この場合の配信するコンテンツの構成概要を図 6 に示す．

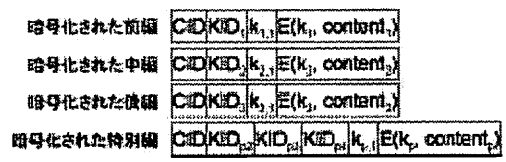

図 6. 提案方式 2 で配信するコンテンツの概要

例えば，$content_1$～$content_3$ を前編，中編，後編とし，$content_p$ を特別なコンテンツとする．そして，各々を暗号鍵 k_1～k_3 および k_p で暗号化する．暗号鍵 k_1～k_3 はしきい値 2 で，暗号鍵 k_p はしきい値 4 で表 1 の様に秘密分散される．そして，図

6 の様に構成される. ここで, CID はコンテンツの ID を, KID_i(i=1,…3, p2, p3, p4)は暗号化されたコンテンツを復号するのに必要な分散鍵を示す. そして, 表 1 の様に分散した分散鍵を, 表 2 の様に組にして配信する.

表 1. 分散鍵の構成方法

暗号鍵	分散鍵			
k_1	$k_{1,1}$	$k_{1,2}$		
k_2	$k_{2,1}$	$k_{2,2}$		
k_3	$k_{3,1}$	$k_{3,2}$		
k_p	$k_{p,1}$	$k_{p,2}$	$k_{p,3}$	$k_{p,4}$

表 2. 配信する分散鍵の組

第 1 分散鍵 Kd_1	$k_{1,2}$			$k_{p,2}$
第 2 分散鍵 Kd_2		$k_{2,2}$		$k_{p,3}$
第 3 分散鍵 Kd_3			$k_{3,2}$	$k_{p,4}$

以上の様にして, 構成されたデータを配信するプロトコルを図 7 に示す.

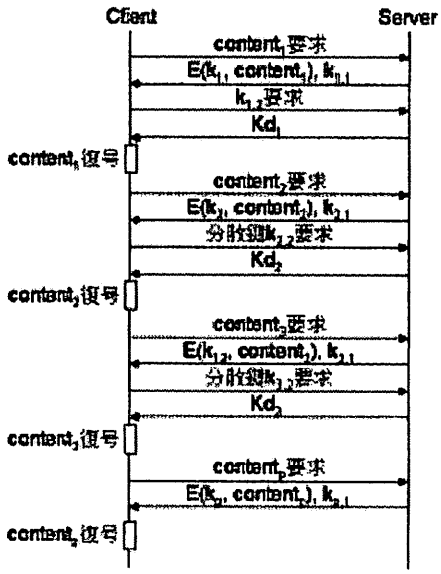

図 7. 提案方式 2 の配信プロトコル

Client から前編 $content_1$ が要求されると, 暗号鍵 k_1 の分散鍵 $k_{1,1}$ と k_1 で暗号化したコンテンツ $E(k_1, content_1)$を Server から送る.

Client は $content_1$ を復号するため分散鍵 $k_{1,2}$ を要求し, Server より第 1 分散鍵 Kd_1 を受信する. 第 1 分散鍵 Kd_1 は, 分散鍵 $k_{1,2}$ と暗号鍵 k_p の分散鍵 $k_{p,2}$ で構成される(表 2). ここで Client と Server との通信は, SSL などを使い保護されているものとする. 分散鍵 $k_{1,2}$ を受信すると Client は暗号鍵 k_1 を復元して暗号化コンテンツを復号し, $content_1$ を取り出し再生する. 同様の処理を中編 $content_2$, および後編 $content_3$ に対して行う.

全てのタイトルを再生した client は, 暗号鍵 k_p の分散鍵 $k_{p,2}$, …, $k_{p,4}$ を入手できたので, 特別編 $content_p$ を要求する. Server は暗号鍵 k_p の分散鍵 $k_{p,1}$ と k_p で暗号化した $E(k_p, content_p)$を送る. 暗号鍵 k_p は, しきい値 4 で秘密分散されているので, $k_{p,1}$, …, $k_{p,4}$ を得た client は, 暗号鍵 k_p を復元して暗号化コンテンツを復号し, $content_p$ を取り出し再生する.

5.3. 提案方式 3 : CM スキップをさせない方式

2011 年から国内で始まる地上波デジタル放送では, Copy Once が認められた. このため, 放送の留守録が可能となり, CM スキップをしながら閲覧できることになり, アナログ放送と同様に CM スキップが問題になると推測される.

そこで, 5.2 を応用した CM スキップをさせない方式を提案する. ここで説明を簡単にするため, 番組の最後の部分を暗号化する場合を考える.

TV 放送では, 概ね図 8 の様にオープニング, CM, 本編, エンディング, 予告で番組が構成されている. オープニングと本編 1, …, 本編 4 について CM が 4 つずつ挿入され, 本編 4 が暗号化されているとする. 視聴者が, 途中で流れる CM_1, …, CM_{16} を幾つか見ないと本編 4 が閲覧できないようにしたい.

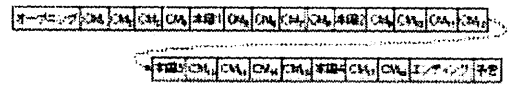

図 8. TV 番組の構成例

例えば図9の様に, 暗号鍵 k_M をしきい値 4 で秘密分散し, 分散鍵k1,…,k4 を生成し, {CM_1, …,CM_4}, {CM_5,…,CM_8}, {CM_9,…,CM_{12}}, {CM_{13},…,CM_{16}}の CM に, それぞれ分散鍵を加えて暗号化しておく. なお, CM を暗号化する暗号鍵 k_{SC} は, オープニングのコンテンツを再生時に取り出す.

この様に放送すれば, たとえ留守録された場合でも, 各本編の間に流れる CM 群の一つを再生するか, 一つ目の CM 群からは 1 番目を, 2 つ目の CM 群からは 2 番目をというように各 CM 群から順番が異なる CM を再生し分散鍵を得ないと本編 4 が閲覧できなくなる.

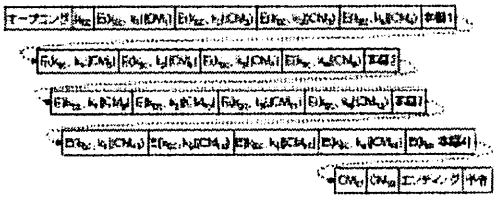

図 9. 番組のデータ構成例

図 9 のデータ構成では，本編 4 だけを CM を再生しないと閲覧できないようになっているが，本編の間に流れる CM を分割したり，本数を増やしたりすることで，本編 1～4 の閲覧を制御することも出来る．

6. 課題

今後の課題として，まず提案した各方式の実装評価がある．

また，配信するデータに含まれる暗号鍵や分散鍵，復元した暗号鍵を安全にローカル環境で保管し利用する仕組みが必要である．

さらに，コンテンツの再生時に，そのデータが不正にコピーされない仕組みも必要である．

7. まとめ

(k, n)しきい値秘密分散法を応用したコンテンツ閲覧制御方式を提案した．

提案方式 1 は，順番に閲覧していく方式であり，順番に閲覧しているか，していないか，視聴者が要求する鍵の種別で判断できる．このため，順番に閲覧しないとコンテンツが再生されない制御や，順番に閲覧している視聴者は，視聴料金が安価なり，飛び飛びに閲覧している視聴者は料金設定を高くする，といった制御ができる．

提案方式 2 は，予め設定した個数のコンテンツを閲覧すれば，特別なコンテンツが閲覧できる方式である．例えば，複数話で構成されたコンテンツを，設定した話数を閲覧すれば特別編などのコンテンツを閲覧することが出来る．

提案方式3は，CMスキップを防ぐ方式である．CM に含まれる分散鍵が所定の数が集まれば，暗号化された本編が閲覧できる．

この方式は，TV放送だけでなく無料のコンテンツ配信サービスへも適用できる．冒頭に流れる CM を閲覧して分散鍵を得ることで，本編が復号再生するものである．

またオンライン配信だけでなく，ローカル環境に保存して閲覧する場合にも，CM を閲覧しないと本編が再生されないため，ツールを使ったダウンロードや留守録された番組の CM スキップへの対策になる．

これらの方式は，動画コンテンツを対象に説明したが，公告ページを閲覧しないと次のページを閲覧できない様な電子書籍へも適用できる．

参考文献

[1] “ネットの動画コンテンツがついに開花–利用者、視聴時間が大幅拡大”，CNET Japan, http://japan.cnet.com/news/media/story/0,2000056023,20089796,00.htm (2007/5/29 アクセス), 2005/10/25.

[2] “ JIAAが「インターネット CM」の定義を発表”，インターネット広告推進協議会(JIAA), http://www.jiaa.org/download/jiaa_060328_icm.pdf (2007/5/31 アクセス), 2006/3/28.

[3] “インターネット広告費予測調査結果（2007-2011）”，（株）電通研, http://dci.dentsu.co.jp/pdf/publication_070416.pdf (2007/5/31 アクセス), 2007/4/16.

[4] “ GyaOを対象にインターネット CM の広告投下モデルを検証”，デジタル・アドバタイジング・コンソーシアム(株), http://www.dac.co.jp/dacfiles/200604gyao_tyousa.pdf (2007/5/31 アクセス), 2006/4/1.

[5] “アンケート結果発表 『7 割が欲しい” 全部入り” テレビ。DVD もネットも HD 録も』”，(株)アイシェア, http://blog.ishare1.com/press/archives/2007/03/dvdhd7.html (2007/5/31 アクセス), 2007/3/2.

[6] “ CM.net” ,(株)シュアクリックス, http://cmpoint.net/ (2007/5/31)アクセス.

[7] 平野, “コマーシャルを連携させたコンテンツ保護法式”，2001-CSEC-016, pp.259-264, 2002.

[8] “企業の広告・宣伝手法は、マスメディアから個別対応の IT メディアへ”，(株)野村総合研究所, http://www.nri.co.jp/news/2005/050531.html