デジタルコンテンツ二次利用システム

5D－5

宇田 隆哉　砂田 智　井上 亮文　重野 寛　松下 温

慶應義塾大学 理工学部 情報工学科 松下・重野研究室

1 はじめに

パソコンが各家庭に普及し、インターネットも身近な存在になってきた。情報検索は図書館からホームページへ、音楽や動画もCDやビデオといった物理媒体からデジタル放送配信といった形態に移行しつつある。コンピュータも飛躍的に発展し、デジタルデータの保存媒体も大容量のものが安価に購入できるようになり、24時間分の放送データを家庭用ホームサーバーに蓄積できる日も近い。

デジタル形式の音楽や動画は劣化することなく流通しつづけられる利点を持ち、圧縮技術などの応用により、非常に大容量のデータを小さい媒体や周波数帯に乗せることが可能となってきた。すでに日本国内でも2000年12月からデジタル放送が開始されようとしており、これを境にさらにデジタルコンテンツ配信は盛んになっていくものと思われる。

今まで、テレビやラジオの放送は、ＮＨＫの受信料を除いて民間放送会社では無料で配信が行われてきた。近年、一部の有料放送サービスが開始されたが、国民の意識には放送されるものは無料であるという考えがいつの間にか根付いてしまっていると言える。確かに、放送された動画像や音楽を家庭用の機械で録画または録音し、好きなときに再生して楽しむのは、著作権法の個人利用の範囲でも保証されていることであり、個人の自由である。しかし、これからのデジタルコンテンツ配信の時代を迎えるにあたって、複製による劣化のないデジタルコンテンツは、著作権法侵害の危機にさらされている。有料放送をデジタル録画またはデジタル録音したデータが、自由に個人や友人間で再生されてしまえば、著作権者に利益が還元されない状態で多くのコンテンツが出回ることになってしまう。また最近は、中古CDや中古ゲームソフトの販売が問題となっているが、これらも著作権者に利益が還元されずに利用者が広がっていくという、非常に製作者側にとって望ましくない状態を招いている。このようなデジタルデータの販売や複製や貸与に関しては、現在の法律で著作権者が保護されていない状態であるため、コンテンツ制作側はシステム部分で自衛する以外に対処方法がないと言えよう。

我々はこの問題に対し、音楽のネットワーク配信に対応した統合されたコンテンツ配信システムを提案する。現在、デジタル音楽コンテンツに関しては、国内のネットワークを通じて非合法に他人の曲を公開した人間が逮捕されたりするなどの事件が起きており、非常に著作権問題が危ぶまれている。デジタル音楽の主流ともいえるまでに広まってきたMP3フォーマットも、従来のMDプレイヤーよりも小型軽量の携

Second Hand Using System of Digital Contents

Ryuya Uda, Akira Sunada, Akifumi Inoue, Hiroshi Shigeno, Yutaka Matsushita

Matsushita Laboratory, Fuculty of Science & Technology, Keio University

3-14-1 Hiyoshi, Kouhoku Ward, Yokohama City 223-8522, Japan

帯型簡易再生プレイヤーが続々登場する中で、さらなる隆盛を極めていくものと考えられる。一方、国内メーカーは非合法に音楽コンテンツが流通しないように、特殊なフォーマット形式のハードウェアプレイヤーを開発し、新たなデジタル音楽コンテンツ市場の参入をはかっている状況である。ここで我々の提唱する音楽配信システムは、音楽フォーマットの種類などにしばられず、また高価なハードウェアも必要としないものである。さらに、利用者は既製の曲を聴くだけでなく、再配布や加工するといった二次利用も行うことが可能である。そしてコンテンツの登録から二次利用に至る運営までが、デジタルで一貫されたシステム内において実行されるため、非常に安価かつ簡潔なシステムとなっている。本システムを利用することにより、ユーザーは安全にデジタル音楽を活用し楽しむことができる。

2 システムの概要

デジタル音楽コンテンツのネットワーク配信サービスは徐々に行われつつある。形態としてはいくつかあり、著作権利者に許可を取った上で曲の一部を無料で試聴させ、気に入った曲を販売するシステムや、アーティストのデータベースか内から直接販売すると言ったものが一般的である。これらのシステムは、次世代音楽コンテンツ配信の足がかりともいえるものであるが、まだネットワークを通して全体的な流れが完結しているシステムとは言い難い。これには根強い地域レコード店の反発や、CD プレス業者などの圧力といった、音楽業界全体の問題が密接に絡み合っているように思われる。

本研究のシステムが提供するサービスは、これら音楽コンテンツに対し、音楽クリエイターからデジタル権利センターへのコンテンツ委託登録、それを配信するコンテンツプロバイダへの利用許諾、エンドユーザーへのコンテンツ配信と課金、著作隣接権者を含む権利者への利益分配、エンドユーザーによる二次利用コンテンツの製作と登録から二次利用課金までをネットワークを通してデジタルのうちに完結することを可能としている。

本システムでは、音楽クリエイターから委託登録されたコンテンツを権利センター内で暗号化し、著作権情報や課金情報などの必要なヘッダ部分を埋め込んだ後、コンテンツプロバイダでコンテンツカプセル化して配信する。エンドユーザーが曲を再生するためには、最終的には権利センターで暗号化された音楽データを展開するためのコンテンツ鍵が必要なのであるが、その取得のためのネットワークプロトコルを生成するのは、自己展開型のコンテンツカプセルであり、さらに自己展開型カプセルは、専用再生プレイヤー自体の権利センターによる証明書を確認する仕組みになっており、これら三者間で取り交わされる暗号鍵とワンタイム暗号化データ列により、エンドユーザーによる不正の横行を防ぐことが出来る。

本システムを利用することにより、エンドユーザーは従来のシステムより遙かに安価に音楽を鑑賞することが出来、音楽アーティストはレコード会社との専属契約や多額の投資なしに自分たちのオリジナル曲を全世界にデビューさせることが可能となるのである。さらに著作権者の利益を保護した上で、複雑な申請手続きなしに誰でも安価に曲の二次利用が可能となり、これにより音楽界全体に対してコンテンツの流通を活性化させる核となるサービスが構築されるであろう。

システム全体の流れを図１に示した。

音楽クリエイターは、製作した曲をデジタル音楽コンテンツとして権利センターに登録する。このときに、作詞家・作曲家などの直接の曲の権利者だけでなく、その曲のレコーディングに携わった演奏家なども著作隣接権者として権利者リストに加えられ、コンテンツ再生時に利益分配の対象となることが出来る。この登録の時点で、買い取り型の料金の他に、聴いた回数に応じた課金(PayPerListen)型の料金も設定され、さらに二次利用時の利用条件や課金の上乗せ上限なども決定される。これらの権利者／利用条件情報とデジタル化された音楽データは、権利センターのサーバーに蓄積され、管理される。

コンテンツプロバイダは、自己展開型カプセルの形でコンテンツを配信する。権利センターから利用許諾を受け、専用の Encapsulator でコンテンツをカプセル化する。カプセルはそれぞれ異なった展開アルゴリズムを持ち、プロトコル部はワンタイムの冗長ビットを含むデータ列パターンを生成可能である。

エンドユーザーは、権利センターにユーザー登録を行う。このとき、ユーザー固有の ID と鍵が与えられ、以後、ユーザーはこの鍵で署名や暗号化を行うことができる。ユーザーは好みの音楽コンテンツをコンテンツプロバイダなどからダウンロードしたり、他人からカプセルの状態で受け取ることが出来る。これらのカプセルはそれ自体では再生することが出来ない状態になっているので、自由にネットワーク間や物理媒体を介して流通しても問題ないのである。よって、各ユーザーが一度ダウンロードしたカプセルに関しては、保存や再配布は自由に行うことが出来る。ユーザーはコンテンツの再生時に権利センターのサーバーと交信し、コンテンツ鍵を取得し曲を再生する。この交信時に権利センターのサーバーにユーザーの利用記録が残り、この記録に基づいてユーザーごとの決済が後に一括して行われる。

さらに、エンドユーザーは気に入った曲を、利用条件に基づいて自由に二次利用できる。二次利用された曲は新たなコンテンツとして権利センターに登録され、コンテンツプロバイダから新しいコンテンツカプセルとして配信される。二次利用の詳細については、本論文で後述する。

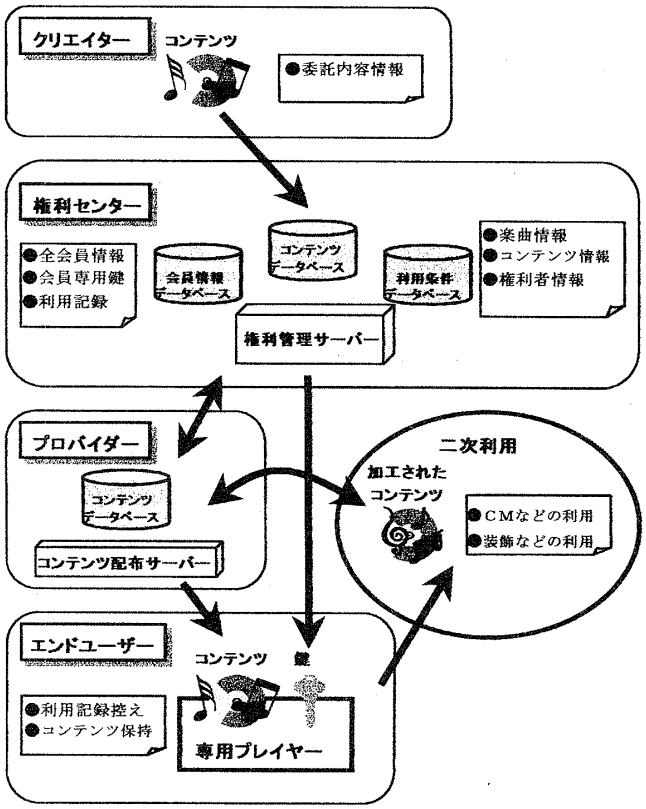

図 1: システムの全体像

3 二次利用システム

二次利用の料金などに関する取り決めは、原権利者が登録時に設定する。ここでいう原権利者とは、著作隣接権も含めたオリジナル音楽コンテンツの制作に携わった人物のことである。作詞家、作曲家の他に、演奏家や歌手なども含まれる。原権利者はコンテンツの利用料金を設

定すると同時に二次利用料金の上限を設定する。

コンテンツの利用料金がＡ円、上乗せする金額の上限がＢ円とすると、二次利用者は、二次利用によって作られる新しいコンテンツの価格を０円～Ａ＋Ｂ円の範囲に設定できる。

０円～Ａ円の間に金額が設定されたコンテンツは、いわばコマーシャル型コンテンツである。オリジナルの曲にコマーシャル用のメッセージなどを挟む代わりに、ユーザーが負担するコンテンツ利用料の一部または全額を二次利用者が代行して負担するという仕組みである。これにより、ユーザーは気に入った曲や新曲を格安の値段で聴くことが出来る。ＣＭ作成者にしてみても、一律にＣＭ料金を払うのではなくて、ＣＭ用のコンテンツが聴かれた数に応じて料金を負担することになるので、より有効にＣＭに投資できる。

Ａ円～Ａ＋Ｂ円の間に金額が設定されたコンテンツは、利益を生み出すコンテンツとなる。これは、新しいコンテンツがユーザーに再生される度に、二次利用者に上乗せ分の利益が還元される。

原権利者が二次利用により利益を生み出すコンテンツの登場を望まない場合、上乗せする金額の上限Ｂ円を０円に設定することで、この問題を回避できる。二次利用者はこのようなコンテンツに関しては、ＣＭもしくは利益も損失もない（０円の）コンテンツとして利用せざるを得ない。さらに、自分のオリジナルコンテンツをこのシステム方式では全く二次利用させたくない場合は、もろちん登録時に二次利用を拒否する設定もできる。このようなコンテンツはいかなる形でも二次利用はできない。

図２にこれらの課金条件設定の流れを示す。

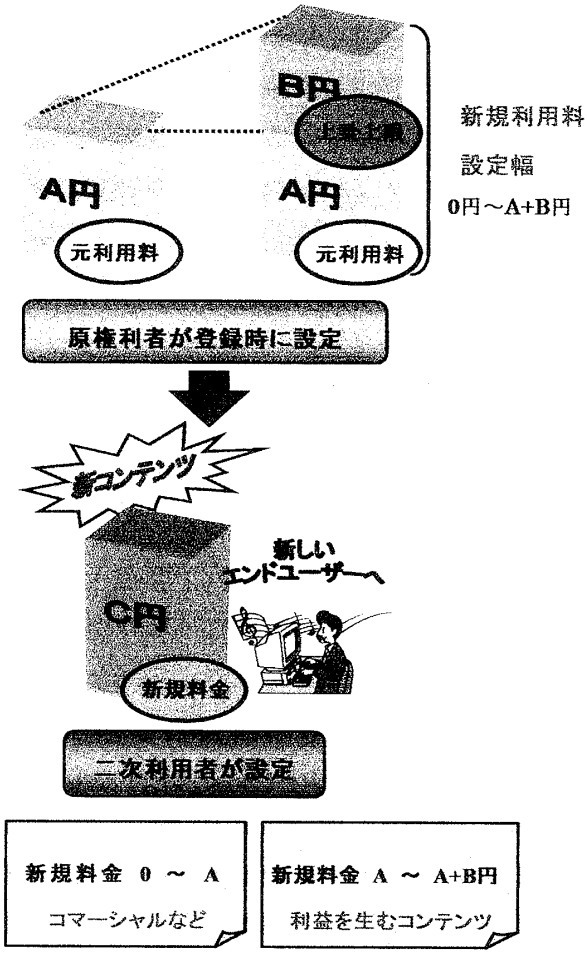

図 2: 二次利用課金条件設定

4 柔軟な二次利用システム

本システムの二次利用では、従来にないメリットを原権利者、二次利用者、エンドユーザーに提供することができる。

原権利者は二次利用時の条件を様々な項目別に詳細まで取り決めることができ、今後、誰かが二次利用する度に確認を取ったりなどの手続きに煩わされることがない。

二次利用者は、全てがデジタル化して手続きが一本化されているため、従来よりも安価に二次利用することが出来、気に入った曲であれば

誰でも平等に使用することが出来る。さらに個人では難しかった手続きもオンラインで自宅に居ながらにして非常に簡潔に済ませることができる。

エンドユーザーは二次利用されたコンテンツを簡単にデータベース検索などで見つけることが出来、試聴に際しても、ＣＭソングなどを見つけることによって、より安価に自分の好みの新曲を探すことが出来る。また PayPerListen 型の課金形態は、従来にない柔軟で安価なものであり、これがエンドユーザーにより多くの曲を聴かせる起爆剤となり、音楽界全体に対して新曲の波及効果が大きくなることが期待できるといえる。

さらに、二次利用者がＣＭ用にコンテンツを利用する場合でも、従来のＣＭでは、放送による対象に狙いが定まらず、対象としない人間に対しても放送されてしまい、その分だけ放送のコスト損失を招くこととなるが、本システムではＣＭコンテンツの利用者は少なからずＣＭやコンテンツに興味を持っているものであり、これによりＣＭ料負担分の料金は狙いとなる対象に絞られることになる。さらに、ＣＭの効果が少ない場合は、それだけコンテンツ利用者が少ないことになり、コンテンツが利用されなければ支払い額も少なくて済むことから、非常にリスクの少ない投資であるといえる。

同様な方法で、コンテンツの最後にプレゼント情報などを付加した場合、エンドユーザーはコンテンツを最後まで聴かねばならないため、ＣＭ目当てのユーザーに対しても曲全体を聴かせることも可能である。インディーズ系の音楽アーティスト達にとっては、このような場が安価に提供されることは非常なメリットを持つと言えるだろう。

5 二次利用システムの概要

本システムの二次利用には３つの形態が存在する。非加工、追加、ミキシングといった形態である。

非加工の場合は、コンテンツの音楽部分自体は何も改変されずに使用される。誕生日メッセージに曲を添えるなどの場合や、自分の好きな曲を他人に無料で（送り主の課金で）送るといった場合である。アンケートに答えてくれた人には無料で１曲プレゼントするなどの商用形態にも用いることが出来る。

追加の場合は、オリジナル音楽コンテンツの前、後ろ、もしくは任意の中間部分に、新たな音のデータを追加する。曲の先頭にＣＭをはさんで二次利用する場合や、曲の最後にクイズのヒントを入れて、最後まで曲を聴いてくれた人にはクイズのヒントがわかるなどといった宣伝に用いることが出来る。どの部分にどれくらいの長さの音データを追加できるかは、原権利者が曲の登録時に設定する。

ミキシングの場合は、曲をＢＧＭとしてそこに宣伝用の台詞などを合成する。カラオケ用の声のない曲に自分の声を入れて新しいコンテンツを作成したり、最新の流行歌をバックに商品の宣伝などに利用できる。

追加、ミキシングの場合の手順について述べる。これらの作業はすべて自動的にコンピュータ内で行われており、ユーザーは難しい流れは気にせずに二次利用を行うことが出来る。

まず、自己展開型コンテンツカプセルは、専用再生プレイヤーの電子署名を確認する。これが正当なものであれば、権利センターと接続し、ワンタイムの冗長部を含む暗号データ列でコンテンツの鍵を取得する。次に専用ミキサーの電子署名を同様に確認し、これが正当なものであ

れば、複合化した音楽データをミキサーに渡す。ミキサーは追加もしくはミキシングする音データとオリジナルコンテンツを合成し、再生プレイヤーに渡して曲の試聴を行う。試聴した曲が気に入れば、新たなコンテンツとして権利センターに登録される。このとき、権利センターにはオリジナルコンテンツは送られず、追加もしくはミキシングした部分の音データと、二次利用者に関する追加の著作権情報が送られる。権利センターで暗号化された新たなコンテンツはオリジナルコンテンツと同様にプロバイダなどを経由して配信することもできる。

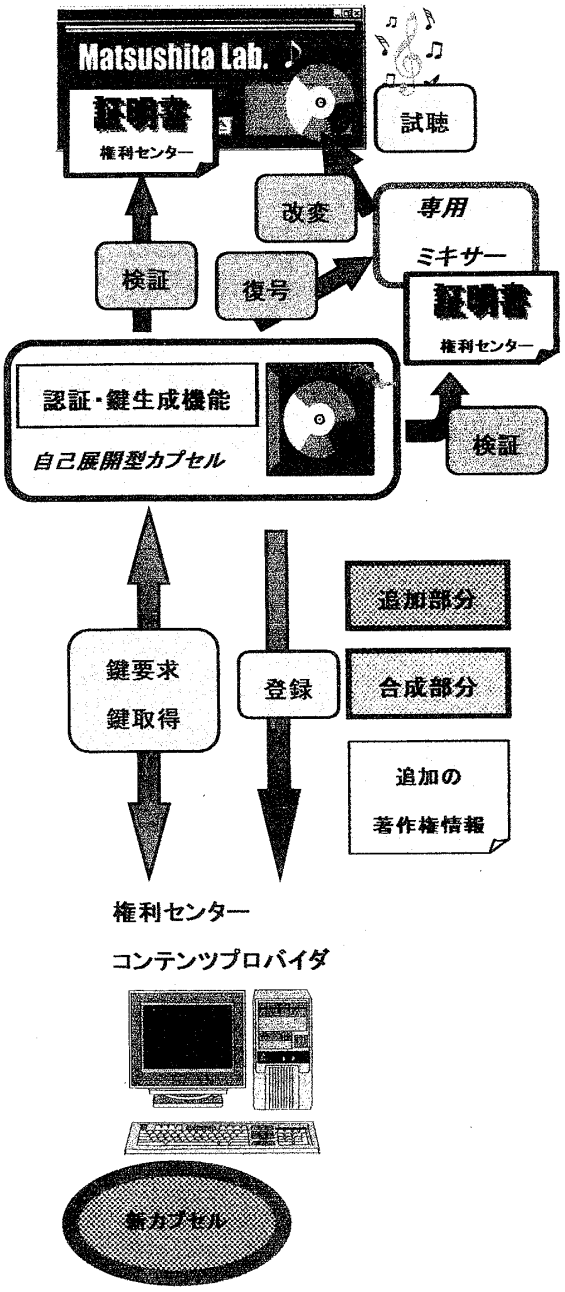

図 3: 二次利用手続きの流れ

6 自己展開型カプセルの概要

本システムでは、音楽コンテンツはカプセルという形で流通する。これらのカプセルは専用の Encapsulator によって生成される。カプセルの中身は、暗号化された音楽データ部分と著作権及び利用条件ヘッダ部分からなる。これらはそれぞれ共通鍵暗号[DES][Tuji][NTT95]による暗号化がなされており、カプセル内部に異なったアルゴリズムで格納されている。

専用の Encapsulator は、カプセル毎に異なったアルゴリズムで暗号化されたコンテンツを格納し、これらは自動的に生成される。これにより、Encapsulator のバージョンアップは、システム全体の変更には影響せず、セキュリティレベルに応じて、また不正ユーザーの危険性に応じて任意に変更できる利点を有する。

もし、不正利用者が音楽データをカプセルから取り出そうとするならば、自己展開型カプセルのアルゴリズムと、暗号化された音楽データの両方に対して解析を行わねばならず、もともと安価に聴くことのできる曲に対して利益に見合わない苦労が必要となるだろう。また、カプセルのアルゴリズムも音楽データの暗号鍵も、コンテンツ毎に異なるため、不正利用者は全ての音楽コンテンツに対して１つずつ解析をせねばならず、さらなる労力を必要とする。

ここで、本システムを使用したサービスの運営に当たって、最も危惧することは、一部の有能な不正ユーザーの解析による努力の結果を、

通常の能力しか持ち得ない数多くのユーザーが安易に利用できてしまうことである。たとえば、誰か１人が改竄プレイヤーを作成し、その違法プレイヤーが公開ネットを流通することにより、多くの不正ユーザーが誕生してしまうことだけは避けねばならない。本システムでは、それぞれのカプセルが実行型のプログラムであり、専用再生プレイヤーの証明書をコンテンツ再生時に検証する点から、このような不正利用は不可能であると言える。

7 電子透かし

それぞれの音楽コンテンツカプセルに格納されている音楽データには、電子透かしが埋め込まれている。コンテンツ ID が 32bit であるので、このデータを電子透かしとして、１秒間に32bit ずつの透かしを埋め込んでいる。

電子透かしを埋め込むことにより、万一、このシステムから音楽データを生の形で取り出したユーザーがいたとしても、そのユーザーがネットに発信する音楽データには、常にこの電子透かしが付随して回ることになり、不正利用の抑制を行うことが出来る。

なお、32bit/sec の電子透かしによる音質の劣化は、人間の耳では聞き取れないほどであり、音楽の鑑賞には支障はないといえる。

参考文献

[Tuji] 辻井重男・笠原正雄　編著：　"暗号と情報セキュリティ", 昭光堂, 1990.

[Oka93] 岡本栄司,　"暗号理論入門", 共立出版, 1993.

[NTT95]　"特集　情報セキュリティ",　NTT 技術ジャーナル, 1995/10.

[DES]　"Data Encryption Standard",　FIPS PUB 46, National Bureau of Standards, Washington D.C., 1997.

[RSA97]　R. L. Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptsystems",　Communications of the ACM, Vol.21, No.2, pp.120-126, 1978.

[KSL92]　A. Kehne, J. Schonwalder and H. Langendorfer, "A Nonce-Based Protocol for Multiple Authentication",　Operating Systems Review, pp.10-14, 1993.

[CS93]　B. C. Neuman and S. G. Stubblebine, "A Note on the Use of Timestamps as Nonces",　Operating Systems Review, pp.10-14, 1993.

[MT93]　R. Molva and G. Tsudik, "Authentication Method with Impersonal Token Cards",　IEEE Symposium on Research in Security and Privacy, pp.56-65, 1993/5.

[BGHJKMY93] R.Bird, I. Gopal, A.Herzberg, P. A. Janson, S. Kutten, R. Molva and M. Yung "Systematic Design of a Family of Attack-Resistant Authentication Protocols", IEEE Journal on Selected Areas in Communications, Vol.11, No.5, 1993/6.

[ESIGN] 岡本龍明・藤岡淳・岩田雅彦, "高速ディジタル署名方式 ESIGN", NTT R&D, Vol.40, No.5, pp.687-696, 1991.

[NK97] 苗村憲司・小宮山宏之, "マルチメディア社会の著作権", 慶應義塾大学出版会, 1997.