ソフトウェアベースの音楽配信プラットフォーム

宇田隆哉[†] 砂田智[†] 井上亮文[†]
重野寛[†] 松下温[†]

デジタル記憶媒体の小型化，大容量化，低価格化にともない，近年，デジタル音楽をネットワークを通じて安全に配信する仕組みが研究されている．デジタル音楽は劣化することなくネットワーク上を流通できる利点を持つ反面，複製が非常に容易であり，つねに著作権侵害の危機にさらされている．また，ハードウェアを用いてセキュリティを実現しているシステムは，規格の不統一や規格のバージョンアップなどの際に機器全体を買い換えなければならず，ユーザへの浸透に歯止めをかけている．そこで，本論文では安全で安価なソフトウェアベースのデジタル音楽コンテンツ配信を提案する．公開ネットワーク上を自由に流通可能な自己展開型の音楽コンテンツカプセルと，定期的にアップデート可能なセキュリティモジュールを保持する音楽プレイヤの使用により，不正利用からコンテンツを保護するとともに，確実な利用履歴の回収により，聴いた回数に応じた課金（PayPerListen）や課金の一部を肩代わりするなどのような，ユーザへの幅広い課金方式を実現する．さらに，ユーザが気に入った曲を加工して，新しい音楽コンテンツとして容易に二次利用可能な環境も実現している．コンテンツの利用や課金の方式に自由度を持たせ，ソフトウェアベースによる安価で安全な音楽の流通方式は，次世代の音楽流通プラットフォームを形成する主要な条件を満足していると考えられる．

Software-based Music Delivery Platform

Ryuya Uda,[†] Akira Sunada,[†] Akifumi Inoue,[†] Hiroshi Shigeno[†] and Yutaka Matsushita[†]

Downsizing, down-pricing and volume-increasing of digital media have promoted the study of some secure delivery systems of digital music contents through networks. Digital music has an advantage of being delivered through networks with no debasement of music quality, but the fact that it could be copied easily brings the copyright violation. The existent systems using hardware security protection are not convenient for users, because security standard for digital music has not been established and revising the standard is difficult. So, this paper describes a secure and inexpensive software-based digital music contents delivery systems. Self-extracting capsules freely delivered through open networks and security modules updated regularly are used in our music player system. They protect the music contents from illegal use. A user can choose PayPerListen for payment or can take over other user's payment. Furthermore, a user can easily arrange the music for secondhand use. Consequently, our software-based music delivery system, being flexible, inexpensive and secure, will certainly bring the satisfactory conditions to be a new music platform for the next generation.

1. はじめに

コンパクトディスクが普及してから，音楽のデジタル化には目覚ましい発展があり，MP3 の登場によってそのデジタル化にさらに拍車がかかっている．デジタル形式の音楽は高音質を劣化なく保てる特徴があり，記憶媒体の小型化，大容量化によってさらなる利便性を増している．そして，インターネットが普及して以来，一般家庭のコンピュータも公開ネットワークに接続できることはもはや常識にまでなっており，ネットワークの高速化，低価格化がデジタルコンテンツ配信を普及させる原動力になっているといえる．

デジタル形式の音楽は，アナログ形式と異なり，劣化することなく流通し続けられるという利点を持つが，反面，著作権者に利益が還元されることなく複製物が横行してしまうという危険性をはらんでいる．現在，送信可能化権[12)]や不正競争防止法のようなデジタルコピープロテクトを法的に保護する動きも見られるが，個人利用の範囲[12)]などの現行の法律が著作権法に存在しており，デジタルコンテンツ配信時代を迎えるには，まだまだ法的な仕組みも配信システムも不十分な

† 慶應義塾大学理工学部情報工学科
Faculty of Science and Technology, Keio University

表 1 SDMI との比較
Table 1 Comparison with SDMI.

	SDMI	本システム
保有するコンテンツの複製	3 回まで	無制限
他人へのコンテンツの複製	不可	可能
利用料金支払いの自動代行	不可	可能
音楽の PayPerListen	不可	可能
音楽の二次利用	不可	可能

段階にあるといえる．

本論文では安価で安全なソフトウェアベースのデジタル音楽配信を提案する．本システムは，プレイヤ部分がソフトウェアベースであるが，コーデックや再生デバイスはプレイヤ内に保持しないので，プレイヤプログラム本体が書き換え可能な音楽再生装置であれば，家庭用のパソコンから民生用のデッキ，携帯型の専用端末など，あらゆる情報機器に搭載可能である．

本システムは常に進化するソフトウェアベースの音楽配信プラットフォームであり，エンドユーザが任意の音楽コンテンツを二次利用可能な自由度の高いサービスを提供できる．安価なセキュリティシステムを駆使して，音楽著作権者の権利を侵害することなくこのようなシステムを実現することが本論文の狙いである．

2. サービスプラットフォーム

本章では，本システムにおける音楽コンテンツ配信の仕組みについて述べる．なお，現在 SDMI（Secure Digital Music Initiative）で策定中のデジタル音楽配信技術に関する著作権保護体系との比較を**表 1** に掲載した．

SDMI では，コピー回数の制限が，米国著作権法の First Sale Doctrine（初回販売の原則）に反する可能性があるとして問題視されているが，本システムではコンテンツを自己展開型カプセル化することで複製に関する問題を解決し，さらにコンテンツの二次利用や PayPerListen までもが可能である．

2.1 ソフトウェアベースの配信

小型化，低価格化されたメモリメディアの影響で，デジタルコンテンツの音楽配信は徐々に開始され始めている．現行の携帯型音楽端末の中には，様々な形式のコーデックをソフトウェア的に追加できるものも登場しているが，本システムはプレイヤ本体ごとソフトウェアとして書き換え可能な特徴を持っている．これにより，最新のアルゴリズムによる暗号モジュールへの対応が可能となり，つねにセキュリティ面での向上を図ってゆける．音楽の再生に必要な専用の音楽プレイヤは，公開ネットワークを通じて常時最新のバージョンが無償で提供される．

2.2 PayPerListen

通常，音楽をメディアとして購入する際，支払う金額はその音楽の末端価格全額である．これは，音楽著作権管理団体側で，ユーザの音楽コンテンツ使用状況が完全に把握できないことに機縁する．送信可能化権[12)]などによる著作権料の徴収も同様である．

本システムでは，サービスが提供するすべての音楽コンテンツについて，ユーザの利用状況を完全に把握可能である．そのため，音楽コンテンツへの課金を，買い取り型のみでなく，聴いた回数に応じた PayPerListen 型にも対応可能なのである．このシステムにより，ユーザは非常に安価に任意の音楽コンテンツを再生可能になるため，いわゆるインディーズと呼ばれる新興の音楽アーティストたちがオリジナルの曲を公開する場を広げることにもつながり，金銭的にそれほど裕福でない若年層にも幅広い音楽を提供できる．結果として，音楽ビジネス界全体に，消費者の立場からも音楽製作者の立場からも利益をもたらすシステムであると考えられる．

2.3 音楽の二次利用

ユーザは，音楽を鑑賞して楽しむだけでなく，積極的に創作活動にも参加可能である．二次利用の利用料金を支払ったうえで，任意の音楽コンテンツ内容を変更し，独自のコンテンツとして公開でき，利用料金の負担，二次コンテンツ利用料の徴収なども行える．二次利用の詳細は，6 章に記す．

2.4 スケーラビリティ

本システムの適用範囲は，家庭用パソコンからモバイル端末に至るまで，プレイヤ本体がソフトウェアとして定期的にアップデート可能なすべての情報機器に及ぶ．ただし，コンテンツの再生時に，必ず権利管理サーバとの交信が必要となる．ダイアルアップ型の家庭用端末では，コンテンツ利用料に対してかなり高額な通信コストが生じてしまうと考えられるが，本システムが想定するのは CATV などによる固定料金の常設回線などである．現在では，ADSL や高速無線通信による固定料金サービスも開始されており，固定回線下でのサービス提供では，回線コストの問題は回避可能であると考えられる．そしてモバイル端末などに適用した場合の移動体通信に関しても，現在は携帯電話のパケット通信サービスなども展開されており，交信時の通信量の点（5.2 節参照）から，本システムによるサービスは広範囲に展開可能であるといえる．

2.5 システムの全体像

本システムの全体像を**図 1** にまとめた．本システム

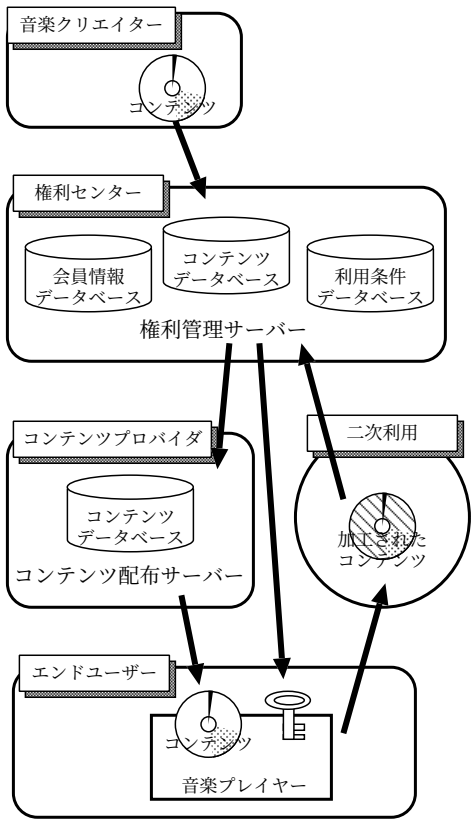


図 1 デジタル音楽配信システム
Fig. 1 Digital music delivery system.

は，コンテンツの二次利用まで含めた統合的な音楽配信プラットフォームである．

2.5.1 音楽クリエイタ

音楽クリエイタは作成した音楽を権利センターに登録する．これは，現行の音楽管理方式と同様であり，著作権管理の委託である．この登録以後，コンテンツは権利センターの管理下に置かれる．このとき，委託内容情報が権利センターに登録され，この情報に基づいてこのコンテンツの配信，二次利用が行われる．なお，音楽クリエイタには，作詞家，作曲家のみでなく，著作隣接権[12)]を有する演奏家も含まれ，コンテンツの利用に対する利益分配の対象となる．

2.5.2 権利センター

権利センターは音楽クリエイタから委託されたコンテンツをコンテンツデータベースに登録する．このとき，登録情報および音楽コンテンツには暗号化が施され，暗号化コンテンツとなる．暗号化コンテンツの鍵（3.1 節参照）は権利センターが保管し，エンドユーザ端末からの個別の要求に対する応答以外には送出されることはない．音楽クリエイタからの委託内容情報には，コンテンツ配信および二次利用時の条件も含まれており，この条件に応じてエンドユーザであるコンテンツ利用者へ課金を行う．権利センターは，音楽コンテンツの配布元として，コンテンツプロバイダを利用する．暗号化コンテンツはコンテンツプロバイダに送られ，管理される．原則として，権利センターが 1 つであるので対し，コンテンツプロバイダは複数存在しうる．

2.5.3 コンテンツプロバイダ

コンテンツプロバイダは，権利センタから暗号化コンテンツを受け取る．コンテンツプロバイダは複数存在しうるので，すべての音楽コンテンツを管理する必要はなく，任意のジャンル，もしくは任意の音楽アーティストといったように，特定の音楽コンテンツに限って管理する．暗号化コンテンツは，コンテンツプロバイダ内において専用の Encapsulator（4.1 節参照）を用いてカプセル化（4.1 節参照）される．このカプセルは配布に制限がなく，公開ネットワークを通じて，また雑誌の付録 CD-ROM，ユーザ同士の交換といった形で自由に流通可能である．

2.5.4 エンドユーザ

エンドユーザはあらゆる手段において音楽コンテンツカプセルが入手可能である．ジャンルごと，アーティストごとの検索であれば，コンテンツプロバイダの保有するコンテンツ配布サーバを検索することが最も容易な方法であろう．エンドユーザは再生を望む曲を選択し，専用の音楽プレイヤの再生ボタンを押すだけで，コンテンツの再生が可能である．このとき，カプセルは権利センターとの交信によって暗号化コンテンツを復号するための鍵を得，カプセル自体を自己展開する．この内容については，4.1 節参照のこと．この交信時に，権利センター側にはユーザが再生したコンテンツの ID などが記録され，この記録に応じて PayPerListen 型または買い取り型の課金が行われる．

また，ユーザは，気に入った任意のコンテンツを二次利用可能である．二次利用されたコンテンツは，コマーシャルとして，またホームページの装飾，別のユーザへのプレゼントなどとして幅広い利用が可能となる．二次利用の詳細については，6 章で解説する．

3. 暗号化コンテンツ

3.1 コンテンツ鍵

コンテンツ鍵とは，音楽データ本体および著作権情報/利用条件などの情報ヘッダ部分を暗号化する鍵のことである．この鍵はコンテンツごとにユニークであり，権利センターが発行し管理する．再生時には，自

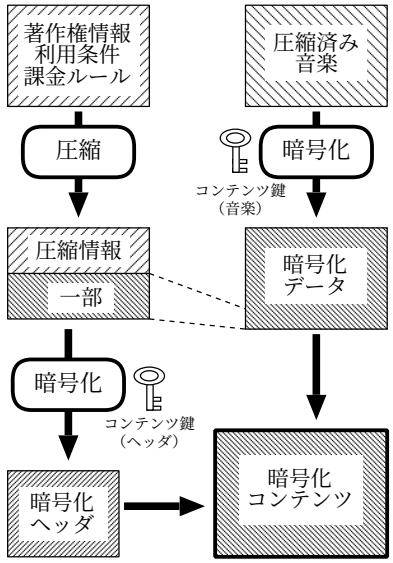


図 2 暗号化コンテンツの生成
Fig. 2 How to make encrypted contents.

表 2 DES 復号化の時間
Table 2 Time for DES decryption.

bytes	millisec	bytes	millisec	bytes	millisec
1,000	80	10,000	100	100,000	260
2,000	80	20,000	120	200,000	441
3,000	80	30,000	130	300,000	631
4,000	80	40,000	150	400,000	801
5,000	90	50,000	160	500,000	991
6,000	90	60,000	190	600,000	1342
7,000	90	70,000	200	700,000	1392
8,000	100	80,000	210	800,000	1622
9,000	100	90,000	230	900,000	1823

表 3 各暗号化モジュールの復号化パフォーマンス
Table 3 Decryption performance of each crypt module.

Cipher Total	Bytes	Time	Bytes/Second
DES	262144	1.252	209380
Twofish	524288	0.952	550722
Blowfish	524288	0.781	671303
CAST–128	131072	0.811	161617

己展開型カプセルと権利センターとの交信の中で，暗号化されたデータの一部として送信される．

3.2 暗号化コンテンツの生成手順

権利センターにおいて暗号化コンテンツを生成する手順を**図 2** に説明する．

権利センターは，音楽クリエイタから受け取った音楽を圧縮する．この圧縮形式は再生する音楽プレイヤのコーデックが対応していればどんな形式でもかまわない．今回の実装にあたっては MP3 フォーマットを用いている．次に，この圧縮済み音楽データを音楽本体用のコンテンツ鍵で暗号化する．この暗号化に使われる暗号は，その時点でのバージョンで，音楽プレイヤが対応しているアルゴリズムであれば何でもよい．また複数の暗号化アルゴリズムを組み合わせることもできる．この点は，自己展開型カプセルの暗号化モジュールの利用と同様なので，4.2 節を参照のこと．今回の実装では，輸出規制が解除されている暗号アルゴリズムの中から DES[4]，Twofish[5]，Blowfish[6]，CAST–128[7]を用いた．こうして得られるのが，暗号化された音楽データ部である．

権利センターは，音楽クリエイタによって登録された著作権情報，利用条件，課金ルールなどの情報ヘッダ部を圧縮する．この圧縮情報と，先に暗号化した音楽データの一部を合体させ，ヘッダ部用のコンテンツ鍵で暗号化する．ここで，圧縮情報に音楽部分の一部を結合させるのは，音楽部分のクラッキング耐性を増すためと，圧縮情報部分のデータに余分なデータを結合させてある程度データサイズを大きくすることによって，著作権情報を強引なクラックから守るという 2 つの目的を兼ねている．データの各部分を重ね合わせる方法については，4.3 節でのカプセルの暗号化にて詳細を述べる．データサイズと暗号化の速度に関しては，**表 2** の DES の復号化速度および**表 3** の各暗号化モジュールの復号化パフォーマンスの比較を参照のこと．なお，DES による復号化時間は，連続したコンテンツブロックを復号化した場合のものである．実装時のシステム環境は 8 章参照．

こうして暗号化音楽データ部と暗号化ヘッダ部とを合わせたものが，暗号化コンテンツとしてコンテンツプロバイダに渡される．

4. 自己展開型カプセル

4.1 自己展開型カプセルの生成

自己展開型カプセルは専用の Encapsulator によって自動的に生成される．カプセル化の具体的な仕組みについては本章で後述する．コンテンツプロバイダは権利センターから受け取った暗号化コンテンツを Encapsulator によってコンテンツカプセル化する．このカプセルは自己実行型のプログラムを含み，音楽プレイヤの署名を認証したりカプセルを展開して音楽データを取り出したりする機能を保有する．カプセル鍵は，自己展開型カプセル内部に含まれる．これにより，エンドユーザはコンテンツ再生時に権利センターとのみ交信することによって曲の再生が可能となる．

4.2 モジュールの利用

自己展開型カプセルは，音楽プレイヤ側が持つ暗号化モジュールを使用する．これにより，カプセルのデータサイズを縮小することができるとともに，様々なタイプの暗号化方式を，用途に応じて使い分けることが可能である．また，音楽プレイヤは随時バージョンアップ可能であるので，新しい暗号化方式のモジュールを音楽プレイヤ側に追加することによって，新しく作られるカプセルは，この暗号化方式を利用することができる．この方法であれば，従来のカプセルも，音楽プレイヤとの互換を失うことなく使用できるので，カプセルの寿命期間を，音楽プレイヤのバージョンアップの頻度よりもずっと長く保つことができる．カプセル流通の面では，これは非常に重要であると考えられる．

ここで，本システムに対し，一番のクラッキングのポイントは音楽プレイヤ本体であると考えられる．音楽プレイヤ本体には，デジタル権利センターの証明書が付いているが，同じバイナリデータを持つ音楽プレイヤが何年もの期間にわたって利用されれば，この程度の証明書は偽造の対象になるのが当然であると推測される．また，一度不正に改竄されたプレイヤが作られると，驚くほどの早さで公開ネットワークを通して改竄プレイヤが流通する．過去に前述のような被害にあった高価なアプリケーションソフトは数少なくない．本システムでは，音楽プレイヤを定期的にバージョンアップさせることによって，現行バージョンの音楽プレイヤの改造版が公開ネットワーク上に流通する前に，新しいバージョンの音楽プレイヤを登場させる仕組みとなっている．この点において，新しく登場するコンテンツカプセルが，新しいバージョンの音楽プレイヤのみ対応ということになれば，ユーザの音楽プレイヤ更新意欲の増進にもつながるだろう．

4.3 カプセルの暗号化

4.3.1 ブロックの分割

自己展開型カプセルは，その生成時にランダムに暗号化のパターンを決定する．**図 3** のように，コンテンツは通常，複数の部分に分割され，異なる暗号化方式または暗号化の鍵で暗号化される．なお，この分割はコンテンツの重要性のレベル（登録時に決定される）に応じて 1〜10 分割程度で行われる．現段階ではブロックの分割によるオーバヘッドはほとんど生じていないが，セキュリティレベルの向上のために分割数を増加する場合は，オーバヘッドによる速度低下も考慮する必要が出てくるだろう．

4.3.2 コンテンツブロックの重複

暗号化されるコンテンツの各パーツは，部分的に重複していることが望ましい．これによって，一部分の暗号化を解くにも，そのブロックと重複している別の暗号化ブロックの暗号を解かなければならなくなる．あらゆる暗号化アルゴリズムの弱点に通じている者は，一部の暗号化アルゴリズムに通じている者よりも少数になるのは当然なので，多重に暗号化をかけるこの方法により，カプセルのセキュリティは大幅に向上する．なお，重複部分が多くなるとそれだけコンテンツの容量が増大し，パフォーマンスの低下を招くため，今回の実装では各暗号ブロックの先頭のわずかな部分のみを重複させた．

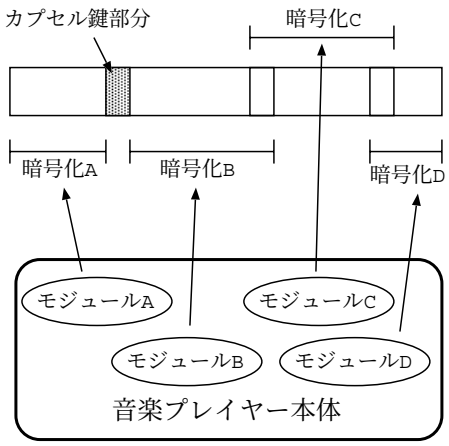


図 3 モジュールを利用したカプセルの中身
Fig. 3 Capsules with modules.

4.3.3 シャッフル型暗号との併用

ここで，使用する暗号化モジュールの組合せであるが，重複ブロックを持つ特性から，データブロックをシーケンシャルに暗号化していくタイプの暗号化方式のみではなく，指定されたブロック内部をさらに細分化し，そのブロックどうしをシャッフルするアルゴリズムとの併用が重要である（**図 4**）．これにより，部分的な音楽データストリームの復元も阻止することが可能である．なお，今回の実装では，復号化時間に比べシャッフリング時間はわずかであった．

4.3.4 鍵正当性の非確認

暗号鍵の正当性の確認パターンにおいては，簡単なチェックビットによるハッシュなどを用いて，与えられた鍵が正しいのか間違っているのかを瞬時に計算してしまうものがあるが，これは音楽プレイヤに組み込まれる暗号化モジュールとしては望ましくない．順番に鍵をあてはめて，コンピュータの計算速度に任せて鍵をこじ開けようとするクラッカがいるためである．

コンテンツの暗号化において，用いるのに望ましいのは，どのような鍵を与えても，その鍵を暗号化関数

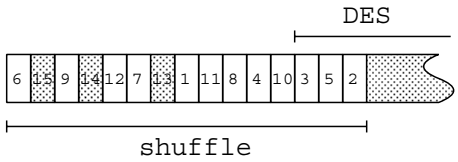


図 4 シャッフルとシーケンシャルの組合せ
Fig. 4 Shuffle and sequential algorithm.

の初期値として，対象のブロックすべてを復号化してしまうようなタイプである．この方法であれば，最後に展開された状態のコンテンツが，音楽データストリームとして再生できるかどうかを確認しなければならず，音楽ストリームの特性上この確認もかなり困難である．これにより，高速なコンピュータを用い，鍵を順番にあてはめてゆくタイプのクラックは防げる．

4.3.5 鍵の保管場所

カプセルが自己展開型であるだけに，カプセル鍵はその内部に保持しなければならない．鍵の位置が簡単に特定でき，その内容が容易に割り出されてしまっては，コンテンツを暗号化している意味をなさない．カプセルは専用の Encapsulator から自動的にランダムなアルゴリズムで生成されるため，Encapsulator を複数の形式で配布することによって，また，Encapsulator のバージョンを一定期間で更新していくことによって，特定のクラックツールが流通することは回避可能である．しかし，バイナリコードの意味を理解できる人間にとって，カプセルの構造が容易に解明されてしまえば，音楽データを取り出されてしまう．

本システムのカプセルでは，鍵データの格納場所を，コンテンツデータのブロックの隙間に分散している．さらに，分散した鍵データはかなりの冗長ビットを含み，カプセル本体に記録されている正しい部分のデータを，簡単な数式に通せば鍵が得られる仕組みとなっている（**図 5**）．

5. コンテンツの再生

5.1 コンテンツ再生の手順

ユーザ側の視点から見たコンテンツの再生は非常にシンプルである．選曲の後，**図 6** の音楽プレイヤの再生ボタンを押すだけである．自己展開型カプセルは，音楽プレイヤの権利センターによる証明書[8]を確認する．証明書が正しければ権利センターと交信し，再生要求を送った後，コンテンツ鍵を取得する．コンテンツ鍵の取得プロトコルについては，5.2 節で解説する．そして，復号化された音楽データが音楽プレイヤ上で再生されるのである．

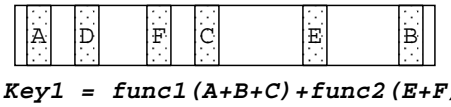


図 5 鍵の格納と数式による導出
Fig. 5 Key embedding and extracting with functions.

図 6 音楽プレイヤ
Fig. 6 Music player.

5.2 鍵取得プロトコル

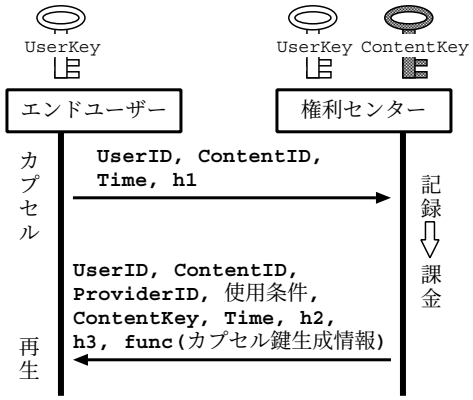
コンテンツ再生時のプロトコルの流れを**図 7** にまとめた．図 7 のように，鍵取得プロトコルに使われる認証はハッシュのみであり，非常に高速な計算であるためシステム全体が安価に使用可能である．また，ワンタイムな冗長ビットをランダムな位置に付加しているため，データを盗み取った者がその内容を知ることは容易ではない．これは，プロトコルで交わされる内容が特定のデータパターン特性を持たないことを利用している．このとき交信される冗長ビットを含むデータのサイズは，128 もしくは 256 バイトとなるように設計されている．これは，携帯電話におけるパケット通信のサイズと一致させるためである．

6. 二次利用

6.1 二次利用の種類

二次利用の方法は 3 種類に大別できる．1 つはオリジナルの音楽にまったく手を触れずに，課金条件だけを変更する方法である．このように二次利用されたコンテンツは，特定の友人になどにプレゼントとして贈るのに向いている．友人が特定回数以内で再生した場合，その課金対象を贈り主に設定することができる．

次の二次利用方法として追加方式がある．原権利者によって定められた場所に別の音楽や会話などの音データを追加できる．この方式により作られたコンテンツは，コマーシャルなどに有効である．曲の演奏前にあるコマーシャル部分を聞いてからでないと曲の演奏が始まらないようにすれば，一部の課金を負担する代わりにコマーシャルを放送できるのである．コマーシャル付きのコンテンツはエンドユーザにとってオリ



h1 : hash[UserID, ContentID, UserKey, Time]

h2 : hash[ContentKey, UserKey, UserID, ContentID, ProviderID, 使用条件, Time]

h3 : hash[ContentKey, func(カプセル鍵生成情報), UserID, ContentID, ProviderID, 使用条件, Time]

func : 自己展開型カプセルが生成する1回限りの関数

図 7 鍵取得プロトコル
Fig. 7 Key obtaining protocol.

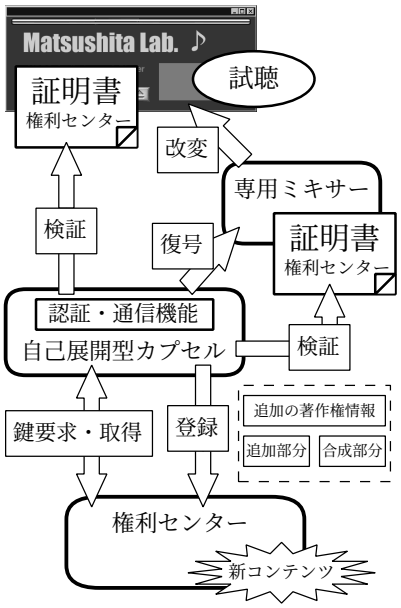


図 8 二次利用手順
Fig. 8 Procedures of secondhand use.

ジナルよりも安価な料金で再生できるために双方にメリットがあるといえよう．

最後に，合成方式がある．これは，オリジナルのコンテンツをバックミュージックとして会話などの音データをミキシングしてしまう方式である．友人の誕生日にメッセージ入りの音楽を贈るなどの使用方法が考えられる．

以上のように，本システムにおける二次利用は，音楽知識のない一般のユーザにとっても非常に簡単に利用でき，また二次利用したコンテンツの用途も広いため，次世代の音楽配信では非常に魅力的な要素を含んでいるといえるだろう．

6.2 二次利用の手順

追加，合成の二次利用を行う場合の手続きの流れを**図 8** に示す．

自己展開型カプセルはプレイヤ上の権利センターの証明書，および二次利用用の専用ミキサーの証明書を確認する．証明書が正しければ権利センターと交信し，コンテンツ鍵を取得する．その後カプセルを展開し，復号化された音楽データを専用ミキサーに送る．専用ミキサーは，追加または合成の改変を行い，改変された音楽データを音楽プレイヤに送って再生する．ユーザはこの時点で改変された音楽を試聴し，納得がいけばコンテンツ登録の指示を出す．プレイヤは改変部分のデータおよび追加の著作権情報のみを権利センターに送信し，容量の大きいオリジナル音楽コンテンツ本体は送信しない．そして，権利センターで二次利用コンテンツが新たなコンテンツとして登録され，コンテンツプロバイダ側で新たなカプセルが誕生する．

6.3 二次利用課金ルール

二次利用時の課金ルールはオリジナルコンテンツの著作権を保持する音楽クリエイタである原権利者がコンテンツ登録時に設定する．料金設定の仕組みは**図 9** のようになっている．通常利用料の上に二次利用時の上乗上限が設定され，二次利用者はこの範囲内で新しいコンテンツの利用料金を設定するのである．

もし，利用料金が元利用料よりも低く設定された場合は，エンドユーザが二次利用コンテンツを再生した場合，その差額を二次利用者が負担するのである．逆に，元利用料よりも高く設定した場合は利益を生むコンテンツとなり，エンドユーザが再生するたびに二次利用者に差額の利益が還元される．これは二次利用を通じて募金を呼びかける場合などに有効な手段であると考えられる．

このように本研究における二次利用による課金システムは，原権利者の意志に反せず，また二次利用者の自由度をも考慮した柔軟なシステムであるといえる．

7. 電子透かし

それぞれの音楽コンテンツデータには，電子透かしが埋め込まれている．実装したシステムではコンテンツ ID が 32 bit あるので，このデータを電子透かしと

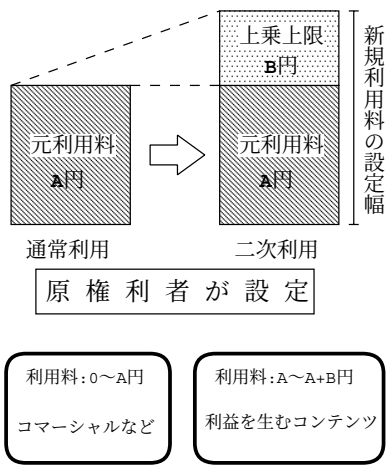


図 9 二次利用課金ルール
Fig. 9 Payment rules for secondhand use.

して 1 秒間に 32 bit ずつの透かしを埋め込んだ．電子透かしの方法は PN 系列によるマッチングを用いた．

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不正に生の音楽データを取り出した人間が公開ネットワーク上に音楽をアップロードした場合でも，その音楽がこのシステムから流出したものであることが確認できる．これは送信可能化権に違反している不正ユーザの抑制につながると考えられる．

なお，32 bit/sec の電子透かしによる音質の劣化はほとんど認められなく，実装したシステムでも音質の劣化は人間の耳では判断できなかったため，音楽の鑑賞に支障はないと思われる．

8. システム環境

本システムの実装は，Pentium Pro 200 MHz および Pentium II 266 MHz のマシン上で行った．今回の実装には，56 bit の DES，Twofish，Blowfish，CAST–128 と簡単なシャッフルのアルゴリズムを用いている．表 2 および表 3 の値は，Pentium Pro 200 MHz 上で計測したものである．実装したマシンの CPU パワーを考慮しても，コンテンツの再生には復号にかかった時間はそれほど問題ないと思われた．なお，権利センター側のマシンは Sun Sparc Station Ultra の Solaris 2.6 上で実装し，サーバ，クライアントとも C 言語で実装，通信には TCP/IP を用いた．

9. おわりに

本論文では，ソフトウェアベースの安全なデジタル音楽コンテンツ配信について述べた．本システムの特徴は自己展開型カプセル，二次利用システム，安価で高速なセキュリティである．不正競争防止法の適用により，日本国内で故意にハードウェアプロテクトを解除する装置の販売は禁止されたが，ハードウェアによるプロテクト技術は物理的な装置の分だけ高価なうえに，セキュリティシステムのアップデートがほぼ不可能であり，あまり望ましい形であるとは思えない．本システムでのセキュリティは，システム進化の時間的な速さによって不正ユーザのメリットおよび労力を無意味化する画期的な方法であると考えられる．不正ユーザはカプセルの仕組みを個別に解析せねばならず，音楽プレイヤのバージョンアップも頻繁に行われるため，PayPerListen 型で安価に聴くことのできる音楽を強引にクラックするメリットが考えられないのである．また，これからはネットワーク社会の時代であり，各家庭に常設のネットワーク回線が設置され，つねにオンラインで公開ネットワークと接続されているような環境に次第に移行しつつある．このような状況をふまえて，本システムは次世代音楽流通プラットフォームに即した音楽コンテンツ配信システムであるといえよう．

参 考 文 献

1) 辻井重男，笠原正雄：暗号と情報セキュリティ，昭光堂 (1990).
2) 岡本栄司：暗号理論入門，共立出版 (1993).
3) 特集 情報セキュリティ，NTT 技術ジャーナル，No.10 (1995).
4) Data Encryption Standard: *FIPS PUB 46*, National Bureau of Standards, Washington D.C. (1997).
5) Schneier, B., Kelsey, J., Whiting, D., Wagner, D., Hall, C. and Ferguson N.: *Twofish: A 128-Bit Block Cipher*, Counterpane Internet Security, Inc. (1998).
6) Schneier, B.: Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish), Fast Software Encryption, *Proc. Cambridge Security Workshop*, pp.191–204 (1994).
7) Carlisle M.A.: Constructing Symmetric Ciphers Using the CAST Design Procedure, Designs, *Codes and Cryptography*, Vol.12, No.3, pp.283–316 (1997).
8) Rivest, R.L., Shamir, A. and Adleman, L.: A Method for Obtaining Digital Signatures and Public-Key Cryptsystems, *Comm. ACM*, Vol.21, No.2, pp.120–126 (1978).
9) Kehne, A., Schonwalder, J. and Langendorfer, H.: A Nonce-Based Protocol for Multiple Authentication, *Operating Systems Review*, pp.10–14 (1993).

10) Bird, R., Gopal, I., Herzberg, A., Janson, P. A., Kutten, S., Molva, R. and Yung, M.: Systematic Design of a Family of Attack-Resistant Authentication Protocols, *IEEE Journal on Selected Areas in Communications*, Vol.11, No.5 (1993).
11) 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).
12) 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).

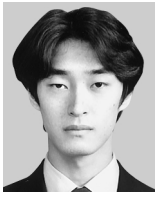
(平成 11 年 11 月 30 日受付)
(平成 12 年 6 月 1 日採録)

宇田 隆哉（学生会員）

1998 年慶應義塾大学理工学部計測工学科卒業．2000 年同大学院理工学研究科計測工学専攻前期博士課程修了．同大学院理工学研究科開放環境科学専攻後期博士課程所属．ネットワークセキュリティの研究に従事．

砂田 智

1997 年慶應義塾大学理工学部計測工学科卒業．1999 年同大学院理工学研究科計測工学専攻前期博士課程修了．同年 4 月より富士ゼロックス（株）勤務．ネットワークセキュリティの研究に従事．



井上 亮文（学生会員）

1999 年慶應義塾大学理工学部計測工学科卒業．同大学院理工学研究科計測工学専攻前期博士課程所属．ネットワークセキュリティ，分散処理システム等の研究に従事．

重野 寛（正会員）

1968 年生．1992 年慶應義塾大学大学院理工学研究科計測工学専攻前期博士課程修了．1997 年同大学院同研究科後期博士課程修了．現在，同大学理工学部情報工学科専任講師．博士（工学）．無線 LAN の構成方法，媒体アクセス制御方式，計算機ネットワークにおけるステーションのサポート，モーバイル・コンピューティング，マルチエージェントシステム等の研究に従事．著書「ネットワーク・ユーザのための無線 LAN 技術講座」（ソフト・リサーチ・センター）．電子情報通信学会会員．

松下 温（正会員）

1963 年慶應義塾大学工学部電気工学科卒業．1968 年イリノイ大学大学院コンピュータサイエンス専攻修了．1989 年より慶應義塾大学理工学部計測工学科教授．博士（工学）．マルチメディア通信および処理に関するコンピュータネットワーク，分散処理，グループウェア，ヒューマンインタフェース等の研究に従事．情報処理学会誌編集担当理事，マルチメディア通信と分散処理研究会委員長，電子情報通信学会情報システムグループ運営副委員長，情報ネットワーク研究会委員長，マルチメディアインフラストラクチャ＆サービス研究会委員長，バーチャルリアリティ学会仮想都市研究会委員長を歴任．現在，情報処理学会副委員長．「やさしい LAN の知識」（オーム社）等著書多数．1993 年度情報処理学会よりベストオーサー賞，1995 年度情報処理学会より論文賞受賞，電子情報通信学会，人口知能学会，ファジイ学会，IEEE，ACM 会員．