DVD-Audioにおけるコンテンツ保護技術

Content Protection Technology for DVD-Audio

加藤　拓　KATOH Taku
遠藤　直樹　ENDOH Naoki
山田　尚志　YAMADA Hisashi

DVDは，高品質なデジタルデータを記録するメディアとしての地位を確立してきている。更に，デジタルデータは，品質劣化なく容易にコピー可能であるという特長を持つ。そのため，映画や音楽の著作権所有者たちは，自分たちのコンテンツをデジタルデータとして流通させる際には，コンテンツが不正にコピーされないような保護技術を求めている。

その要求に対して，DVD-AudioではCPPM（Content Protection for Prerecorded Media）と呼ばれる技術が採用されている。CPPM技術は，著作権所有者の要求に合致するとともに，民生機器とパソコン（PC）システムの両方の環境に適した技術である。

DVD is growing into a major storage medium for storing high-quality audiovisual data. Copies of the digital data can be made without difficulty that are exactly the same as the original data. Therefore, the copyright holders of entertainment contents such as movies and music strongly require content protection technology that prevents unauthorized copies from being made when their contents are published.

In order to meet this requirement, Content Protection for Prerecorded Media (CPPM) technology has been adopted as a content protection technology for DVD-Audio. CPPM is suitable for both consumer electronic equipment and PC system implementations.

1 まえがき

DVD-Videoは，1996年に発売されて以来，現在のセル・レンタル市場では既にビデオテープを超える存在となってきた。その大きな要因の一つとしては，ビデオテープに比べて高画質であることが挙げられるだろう。このような高品質コンテンツへの欲求に合わせて，音楽でもCDに代わる存在としてDVD-Audioが注目を集め始めてきている。しかし，コンテンツ提供者（著作権所有者）は，その扱いには非常に慎重であり，CDがCD-R（Recordable）に不正かつ手軽にコピーされている状況を繰り返さないためにも，DVD-Audioにはより強力なコンテンツ保護方式を要求している。逆に言えば，コンテンツ提供者の認める方式でなければ，彼らのコンテンツはDVD-Audioディスクでは発売されず，DVD-Audioの市場も立ち上がらない。

ここでは，DVD-Audioに採用されたコンテンツ保護技術であるCPPMについて述べる。CPPMは，当社，及び松下電器産業（株），Intel社，IBM社の4社（以下，4Cと略記）で技術開発し，ライセンスを実施している技術であり，ライセンスの仕様書や契約書類の請求に関する情報は“4C Entity, LLC ”のWebサイトhttp://www.4Centity.com/から入手可能である。なお，CPPMのライセンス開始によって，米国では2000年末に，日本では2001年になってDVD-Audioディスクが発売されている。

CPPMは，コンテンツ提供者の次の要求に合うように設計されている。

⑴ 十分な耐性とリニューアビリティ
⑵ オーディオとビデオの両方に適用可能
⑶ PCと民生機器の両方に適用
⑷ 様々な読出し専用メディアに適用可能

実際にCPPMは，次の要素技術を備えている。

⑴ リムーバブルメディアに適した鍵（かぎ）管理
⑵ コンテンツ暗号化
⑶ メディアによる不正機器の無効化

これらの要素技術が盛り込まれたCPPMシステムを，簡略的に図1に示す。

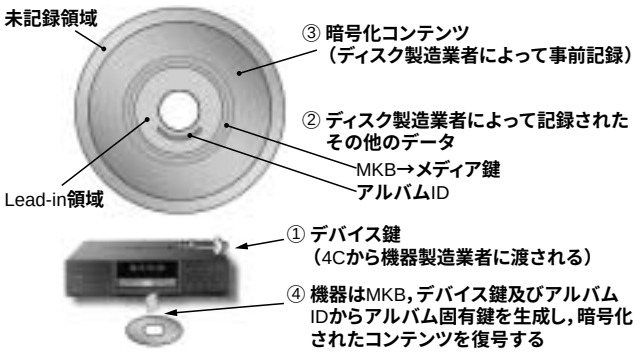

図1．CPPM技術の概要　CPPMではコンテンツの暗号化だけでなく，MKBによってリニューアビリティが備わっている。
Components of CPPM technology

2 暗号アルゴリズム

CPPMでは，コンテンツの暗号化や鍵の暗号化にC2（Cryptomeria Cipher）と呼ばれる鍵長56ビットの64ビットブロック暗号を採用している。C2は，ハードウェアとソフトウェアの両方での実装を考慮して，当社と松下電器産業（株）が中心となって開発した暗号アルゴリズムである。なお，アルゴリズムは，ソースプログラム（印刷物）として既に公開されている。

鍵の暗号化／復号のように処理対象データが64ビットブロックの場合には，C2をECB（Electronic CodeBook）モード（関数名：C2_E/C2_D）で使用し，コンテンツ暗号化／復号にはC-CBC（Converted Cipher Block Chaining）モード（関数名：C2_ECBC/C2_DCBC）が使用される。

また，C2暗号を利用した一方向性関数（関数名：C2_G）も規定されており，CPPMのコンテンツ暗号化鍵の管理などに利用されている。

3 鍵管理技術

CPPMでは，MKB（Media Key Block）のシステムリニューアビリティによる不正機器の無効化機能が備わっている。MKBを用いた鍵管理処理を図2に示す。プレーヤは，あらかじめ秘密に割り当てられているデバイス鍵を使ってMKBを処理することによって，メディア鍵を再生する。デバイス鍵はプレーヤごとに異なるものが割り当てられているが，プレーヤが無効化されていない限り，どのプレーヤでも同じMKB（同じディスク）からは同じメディア鍵を再生できるようになっている。更に，一方向性関数を用いて，そのメディア鍵とアルバムID（IDentification）からアルバム固有鍵が生成される。

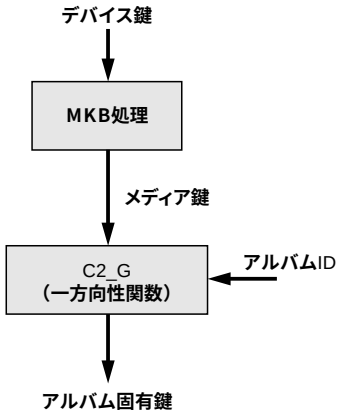

図2．MKBを用いた鍵管理処理　デバイス鍵，MKB及びアルバムIDからアルバム固有鍵が生成される。
Key management procedure

3.1 デバイス鍵

CPPMで暗号化されたDVD-Audioコンテンツを再生するためには，プレーヤはデバイス鍵と呼ばれる56ビットの鍵を16個持たなければならない。一つひとつのデバイス鍵には各々に対応する行と列の番号があり，それらの番号はMKBを処理する際に必要となる。なお，一つのプレーヤに割り当てられる16個のデバイス鍵は，すべて対応する列番号が異なるが，行番号は同じになることもある。

デバイス鍵は，4C Entity, LLCからライセンスされる極秘情報であり，プレーヤ製造業者はこの鍵が露呈しないようにプレーヤを製造しなければならない。もしも，この鍵情報が露呈してしまった場合には，MKBの機能によって，当該プレーヤではその後発売されるDVD-Audioディスクが再生できなくなってしまう。

3.2 アルバムIDとアルバム固有鍵

CPPMでは，DVD-Audioタイトルごとに異なる“ アルバムID ”と呼ばれる64ビットの固有IDが用意されており，MKBを処理することによって得られるメディア鍵とアルバムIDを一方向性関数で処理することによって，56ビットのアルバム固有鍵が生成される。なお，アルバムIDはLead-in領域（ディスクの管理情報などを記録する領域）に記録される。

3.3 MKB

MKBは，4C Entity, LLCによって生成される鍵管理情報の一つであり，データ領域に記録される最大で約3Mバイトのデータである。MKBは，秘密であるはずのデバイス鍵が露呈してしまったなど，その時点で無効化の対象となっているプレーヤの情報を反映して作成される。そのため，無効化の対象となったプレーヤは，そのMKBが記録されたDVD-Audioディスクを再生することができなくなる。

4 CPPMコンテンツ保護システム

4.1 データ作成と再生処理

ディスク製造及び再生手順を図3に示す。ディスクは以下の手順で製造される：

step 1　4C Entity, LLCからライセンスされたMKBと乱数生成器などを使って作成されたアルバムID（ID_{album}）をLead-in領域に書き込む。

step 2　MKBに対応するメディア鍵（K_m）とアルバムIDから一方向性関数によってアルバム固有鍵（K_{au}）を生成する。なお，この際のメディア鍵は正当なプレーヤのデバイス鍵を使ってMKBから得られる鍵と同じものである。

step 3　2,048バイトのデータパックごとに，最初の128バイトの決められた位置から抜き出された“ 鍵変換データ（D_{kc_i}, i=1, …, 5）”を繰り返しアルバム固有鍵に作用させることにより，コンテンツ鍵（K_c）を生成する。

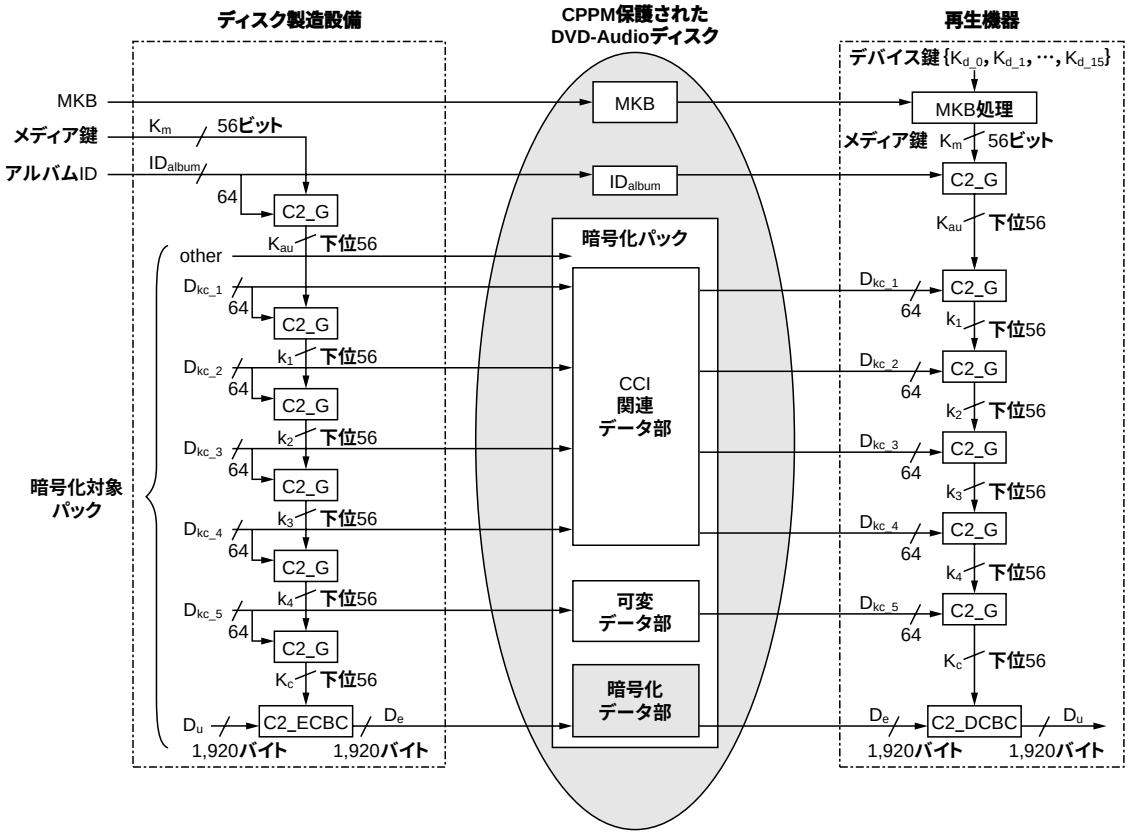

図3．CPPM保護されたDVD-Audioコンテンツの製造と再生処理　ディスク製造時にはライセンスされたメディア鍵を使用し，ディスク再生時にはデバイス鍵とMKBから復号されたメディア鍵を使用する。
Encryption and decryption process of CPPM-protected DVD-Audio content

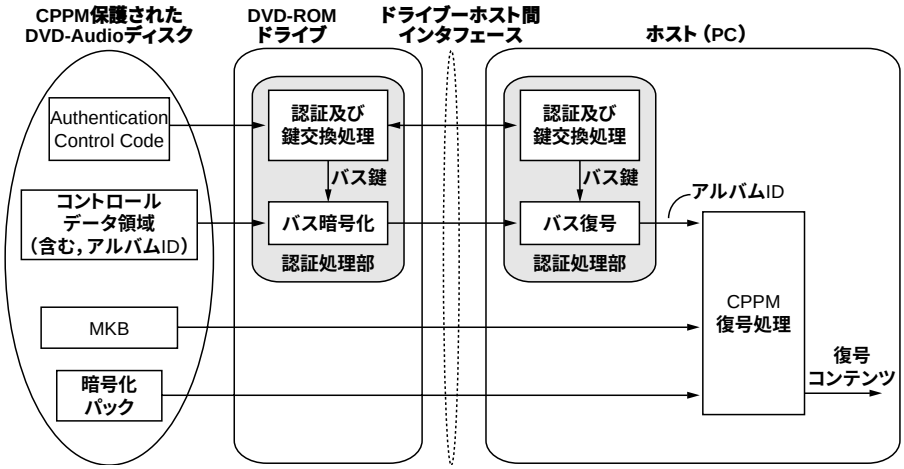

図4．PCシステムにおける再生処理
DVD-ROMドライブとホスト間では，アルバムIDは暗号化されて伝送される。
Decryption process in PC-based system

step 4　データパックの残り1,920バイトを，コンテンツ鍵によってC2 C-CBCモードで暗号化する。

step 5　step 3で使用した128バイトとstep 4で暗号化された1,920バイトを一つのデータパックとして，ユーザー領域に記録する。

以上の処理をすべての暗号化対象データに施す。

このようにして製造されたDVD-Audioディスクを再生するために，プレーヤではディスクに記録されたMKB，アルバムID及びプレーヤ自身が持っているデバイス鍵からアルバム固有鍵を生成し，各データパックをC2 C-CBCモードによって復号する。

4.2　PCシステムにおける再生処理

PCシステムにおいて，CPPMで保護されたDVD-Audioディスクを再生するためには，4.1節の処理に加えて，DVD-ROMドライブとPC上のホスト（ソフトウェア／ハードウェア）との間でもう一つ処理が必要となる。

DVD-Audioディスクが発売される以前からDVD-ROMドライブが既に流通しており，PC上にホスト（ソフトウェア／ハードウェア）を用意することによってDVD-Videoを再生することが可能となっている。そのため，DVD-Audioでも，既存のDVD-ROMドライブで再生が可能な仕組みが採用されている。

単体のプレーヤとの違いは，**図4**に示すようにドライブが読み出したアルバムIDをPC上のホストに安全に（途中で改変されないように）伝送するための機能が追加されている。アルバムIDを伝送するために，ドライブとホストの間であらかじめ定められた手順によって相互認証を行ったうえで，両者でアルバムID伝送用の使い捨ての鍵が共有される。アルバムIDは，その鍵によってスクランブルされ伝送される。

5 コンテンツ保護技術ライセンス

これまで述べてきたように，DVD-Audioディスク上では，コンテンツは十分な強度を持った暗号によって暗号化されたうえで記録されているが，そのコンテンツを再生するためには，どこかで暗号化されたコンテンツを復号し，最終的には，ベースバンド信号（DVD-Audioでは人間が聞く音）に戻す必要がある。

しかし，それ以前にプレーヤ内では暗号化されたコンテンツを復号するための秘密（デバイス）鍵が存在するため，もしその鍵がプレーヤ内で正しく管理されず，秘密でなければならないはずの鍵が露呈してしまった場合には，特定ディスクにとどまらず，暗号化されたすべてのコンテンツが復号され，デジタルコピーが容易に作成されてしまう。このようにデバイス鍵が露呈してしまった場合を想定して，CPPMではMKBによる“無効化”機能が備わっている。

それだけではなく，そもそもコンテンツ保護システムではデバイス鍵などの秘密情報が露呈してしまうことを防ぐために，技術仕様書とともにコンプライアンスルールやロバストネスルールが定められており，ライセンスを受けた者はこれらの規則に従って機器を製造しなければならない。

コンプライアンスルールには，CPPMの使用目的，ディスク製造時にコンテンツに付けられるコピー制御情報（CCI：Copy Control Information）の定義規則，プレーヤの再生制御規則や出力制御規則などが規定されている。

DVD-Audioでは，コピー制御情報としては次の情報などが定義されている。

⑴ 自由にコピー可，1世代コピー可などのコピー許可情報
⑵ 1世代コピー可の場合のコピー回数制御情報
⑶ コピーを作成する場合に許可される音質情報，など

再生制御としては，電子透かし（Watermark）検出やメディアタイプ検出などが定義されている。特に電子透かしは，コピー制御情報などをコンテンツに直接埋め込む技術であり，CPPM仕様書とは別に“Verance-4C Watermark”としてライセンスされる。

出力制御としては，アナログ出力とデジタル出力に関する規則が規定されている。なお，デジタル出力としては，CDプレーヤなどに付けられている光デジタル出力のように暗号化されない従来の出力と，4Cが安全と認めた出力があり，各々に異なる規則が規定されている。

ロバストネスルールには，CPPMでライセンスされる情報の機密性の定義や，CPPM技術をプレーヤに実装する際の規則が規定されている。実装時の規定には，ソフトウェア実装とハードウェア実装ごとに規則があり，どちらの場合にも，デバイス鍵のように機密性の高い情報の安全な取扱いや，暗号化されたコンテンツの復号再生途中の情報が流出しないように，プレーヤを製造するための要件などが規定されている。

6 あとがき

ここで述べてきたCPPMは，現在のところDVD-Audio用にだけライセンスされている技術であるが，4C Entity，LLCは再生専用メディア用のCPPM技術のほかに，記録メディア用にCPRM（Content Protection for Recordable Media）技術も同時にライセンスをしている。CPRMはDVD-RAM（Rewritable）/ R/RW（Re-recordable）向けやSDメモリカード向けなどにライセンスが既に開始されており，そこで使用されている技術は，CPPMで使用されている技術と非常に類似したものになっている。

コンテンツ保護技術では，再生制御だけでなく，安全にコンテンツを伝送する手段や，安全に正当なコピーを作る手段も必要であり，それら全体システムが安全になるように考えていかなければならない。

文　献

⑴ http://www.4Centity.com/

加藤　拓 KATOH Taku，D.Eng.
e-ソリューション社 SI技術開発センター，工博。
情報セキュリティ技術及び応用システムの研究・開発に従事。電子情報通信学会会員。
Systems Integration Technology Center

遠藤　直樹 ENDOH Naoki
e-ソリューション社 戦略企画室参事。
情報セキュリティ技術及び同技術応用システムの開発に従事。電子情報通信学会，日本セキュリティマネジメント学会会員。
e-Solution Co. Strategic Planning Div.

山田　尚志 YAMADA Hisashi
デジタルメディアネットワーク社首席技監。アナログLSIの研究・開発，LSI用CAD，DVD，コピープロテクションシステムなどの開発に従事。IEEE，電子情報通信学会会員。
Digital Media Network Co.