DVDのコンテンツ保護

Content Protection on DVD

石原　淳

■ISHIHARA Atsushi

DVDは高品位の映像や音楽をデジタル記録することから，そのコンテンツ保護は当初から不可欠のものと考えられている。DVDビデオ，DVDオーディオ及び記録型DVD向けにこれまでに策定された各種コンテンツ保護規格は，単にコンテンツを暗号化して保護するだけでなく，製品の様々な側面に関与するものとなっている。

Content protection has been considered to be indispensable for DVD since its birth, since it can record high-quality motion picture and audio contents in digital form.　The content protection schemes specified for DVD-Video, DVD-Audio, and recordable DVD not only protect the contents of these media by encryption, but also affect various aspects of DVD products.

1　まえがき

DVDは高品位の映像や音楽をデジタル記録することから，そのコンテンツ保護はDVD規格制定当初から不可欠のものと考えられている。1996年DVDフォーラム[(1)]においてDVDビデオ規格が制定されるにあたり，MPAA（Motion Picture Association of America），RIAA（Recording Industry Association of America）に代表される映画音楽業界，コンピュータ業界，及び民生電子機器業界は，CPTWG（Copy Protection Technical Working Group）と呼ばれるグループを結成して，DVDビデオコンテンツの保護方式の策定を開始した。CPTWGでは，以下の原則が確認された。

⑴　一般ユーザーが身近な機器を使って不正にコピーを行うカジュアルコピーの防止を目的とする。

⑵　保護されるべきコンテンツは暗号化する。

これらの原則に従い，かつコンテンツ提供者の様々な要求を満たす方式として，東芝と松下電器産業（株）が提案した暗号化方式を基に，CPTWGは97年にCSS（Content Scramble System）と呼ばれる方式を策定し，DVDフォーラムもこれを採用した。CSSは，現在DVD CCA[(2)]（DVD Copy Control Association）によってライセンスされている。

これに続くDVDオーディオ及びDVD-RAM，DVD-R（Recordable），DVD-RW（ReWritable）の記録型DVDについては，CPTWGの中核メンバーである東芝，松下電器産業（株），Intel社，IBM社の4社（4C）が開発したCPPM（Content Protection for Prerecorded Media）及びCPRM（Content Protection for Recordable Media）と呼ばれるコンテンツ保護技術が各々採用されている。CPPM及びCPRMはCSSを発展させたものであり，ワッセナー アレンジメント[(3)]で輸出許可される暗号鍵長が98年末に56ビットに拡張されたことを受けての暗号鍵長の56ビット化，及びライセンス違反機器の無効化機能が新たに盛り込まれている。CPPM及びCPRMは，4C Entity[(4)]により2000年からライセンスされている。

2　CSS

DVDビデオ用のコンテンツ保護方式であるCSSでは，以下が規定されている。

⑴　3階層の暗号鍵管理とコンテンツ暗号化

⑵　パソコン（PC）システム用バス認証

⑶　記録型DVDディスク上のCSSコンテンツ

⑷　アナログビデオ出力に関する規定

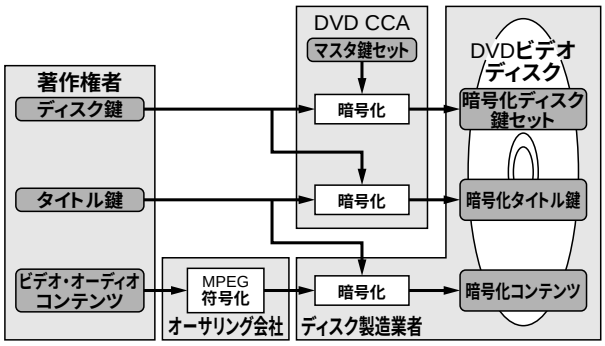
⑸　デジタルビデオ，オーディオ出力に関する規定

⑹　RPC（Region Playback Control）

2.1　3階層の暗号鍵管理とコンテンツ暗号化

CSSではタイトル鍵，ディスク鍵，マスタ鍵の3種類の40ビット暗号鍵が使用される。タイトル鍵はコンテンツの暗号化に，ディスク鍵はタイトル鍵の暗号化に，マスタ鍵はディスク鍵の暗号化に，各々階層的に使用されている。これら3種類の鍵を用いて，コンテンツ及び鍵を暗号化してディスクに記録する手順を**図1**に示す。

タイトル鍵はディスクに記録されるタイトルごとに著作権者が自由に設定する鍵であり，ディスク鍵で暗号化されたタイトル鍵はディスク上のセクタヘッダ領域に記録される。ディスク鍵もディスクごとに著作権者が自由に設定する鍵であ



MPEG：Moving Picture Experts Group

図1．CSS 暗号化手順 ― 3種類の暗号鍵を用いて，コンテンツ及び鍵を暗号化してディスクに記録する。

Content scramble system (CSS) scrambling process

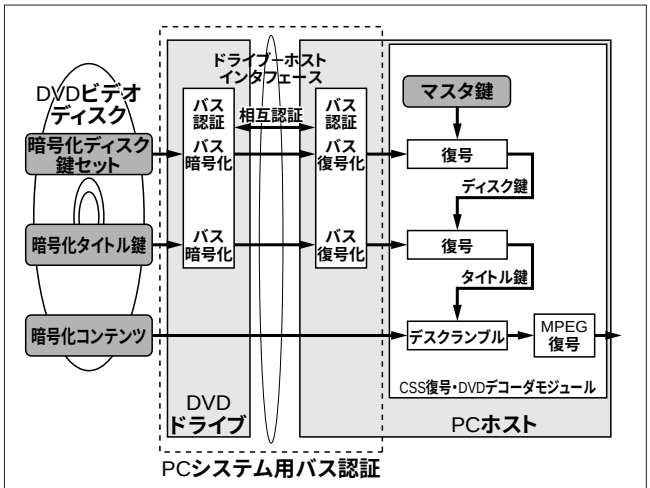


図2．PC システムにおける CSS 復号手順 ― 機器のマスタ鍵から鍵及びコンテンツを復号する。インタフェースでは相互認証による保護も行われる。

CSS descrambling process on PC system

り，これをすべてのマスタ鍵で暗号化した結果を並べたディスク鍵セットがディスクのリードイン領域に記録される。マスタ鍵はCSS機器製造ライセンス受領者に個別に与えられる鍵であり，CSSを復号する機器にセキュアに実装される必要がある。

コンテンツ及び鍵の復号は，CSSライセンス機器がセキュアに保持しているマスタ鍵を用いてディスク鍵を復号し，このディスク鍵を用いてタイトル鍵を復号し，このタイトル鍵を用いてコンテンツを復号することにより行われる。

2.2　PC システム用バス認証

PCシステムにおいては，CSS暗号化されたコンテンツ及び鍵を読み出すDVDドライブとこれらを復号するDVDデコーダとが分離しており，その間のインタフェース上で鍵情報をセキュアに伝送する必要がある。このため，DVDドライブとDVDデコーダはSFF（Small Form Factor Committee）8090規格で定められたプロトコルに従って相互認証を行い，相互認証が成功した場合にのみ鍵情報の伝送を行う。伝送に際しては，相互認証時に共有され，毎回異なる値を取るバス鍵で鍵情報を暗号化している。PCシステムにおけるディスクからのコンテンツ及び鍵の復号手順を**図2**に示す。

2.3　記録型 DVD ディスク上の CSS コンテンツ

CSSで暗号化されたDVDビデオコンテンツは，再生専用型DVDディスク上にのみ正規に存在する。このことを利用して，記録型DVDディスクの識別及び記録型DVDディスク上のCSSコンテンツ再生に関するルールが以下のとおり定められている。

⑴　CSSコンテンツに含まれるCCI（Copy Control Information）がコピー不可を意味するときは再生禁止

⑵　民生用DVDプレーヤにおいてはCSS復号禁止

⑶　DVDドライブにおいては相互認証禁止

元はCSS暗号化で保護されていたコンテンツが，何らかの不正手段で復号された後，記録型DVDディスク上に記録されている場合の再生禁止手段として，電子透かし（WM：WaterMark）を利用することが検討されている。

2.4　アナログビデオ出力に関する規定

CSSで暗号化されたDVDビデオコンテンツを復号してテレビ（TV）などに出力するアナログビデオ信号がビデオテープレコーダ（VTR）などで録画されないようにするため，概略以下のルールが定められている。

⑴　NTSC（National Television System Committee）及びPAL（Phase Alternation by Line）方式の映像端子から出力する場合には，APS（Analog Protection System）及びCGMS-A（Copy Generation Management System for Analog）を付加すること。APSとしては，AGC（Automatic Gain Control）信号とカラーストライプ信号の2種類を使用する。

⑵　民生用DVDプレーヤにおいてはRGB（赤，緑，青）出力禁止。ただし，SCART（欧州で主流の出力方式）端子は，並行して出力するコンポジット信号にAGC信号を重畳し，このコンポジット信号を同期信号として使う場合は認める。

2.5　デジタルビデオ，オーディオ出力に関する規定

CSSで暗号化されたDVDビデオコンテンツを復号してビデオ信号又はオーディオ信号をデジタル出力することに関するルールは，以下の状況となっている。

⑴　DTCP（Digital Transmission Content Protection）及びHDCP（High-band width Digital Content Protection）で保護されたセキュアなインタフェースへの出力を許可することが検討されているが，この原稿執筆時点ではまだ認められていない。

⑵　オーディオ信号についてはSCMS（Serial Copy

Management System）が正しく付加され，48 kHz，16ビット以下の圧縮オーディオ，又はリニアPCM（Pulse Coded Modulation）の出力が認められている。

2.6 RPC

CSSでは，コンテンツ提供者の意向によってコンテンツの再生可能な地域を限定するための機能がルール化されている。具体的には，世界を6地域に分割して各々に地域コードを付与し，この地域コードを民生用DVDプレーヤ及びDVDドライブの機器に埋め込む。CSSで保護されたディスクを再生する際には，ディスクに設定されている地域コードが機器側の地域コードと一致しなければ再生を行わない。

3 CPPM及びCPRM

DVDオーディオ向けコンテンツ保護方式であるCPPM，及びDVD-RAM，DVD-R，DVD-RWの記録型DVD向けコンテンツ保護方式であるCPRMは，対象が再生専用ディスクであるか記録型ディスクであるかの違いはあるが，ほぼ同一の方式であり，CSSを発展・改良したものとなっている。CPPM及びCPRM では以下が規定されている。

⑴ 暗号アルゴリズム
⑵ 暗号鍵管理とコンテンツ暗号化
⑶ ライセンス違反機器の無効化機能
⑷ PCシステム用バス認証
⑸ 記録型DVDディスク上のCPPMコンテンツ
⑹ CPRM記録時の入力に関する規定
⑺ オーディオ出力に関する規定
⑻ ビデオ出力に関する規定

3.1 暗号アルゴリズム

CPPM及びCPRMでは，C2（Cryptomeria Cipher）と呼ばれる鍵長56ビットの64ビット ブロック暗号が，コンテンツ及び鍵の暗号化に使用される。C2暗号は，ハードウェアとソフトウェア双方での実装を考慮して，東芝と松下電器産業（株）を中心に開発された暗号である。

3.2 暗号鍵管理とコンテンツ暗号化

CPPMではデバイス鍵，MKB（Media Key Block），アルバムID（IDentification）の3種類の鍵情報が使用される。CPRMではデバイス鍵，MKB，メディアID，タイトル鍵の4種類の鍵情報が使用される。デバイス鍵は4C Entityからライセンス受領者に個別に与えられる鍵であり，CPPM及びCPRM対応機器にセキュアに実装される必要がある。他の鍵情報はディスクに記録される。これらの関係を**図3**に示す。

CPPMにおいては，デバイス鍵でMKBをC2暗号処理し，その結果をアルバムIDでC2暗号処理して得られる結果がコンテンツを暗号化及び復号する暗号鍵となっている。当初のMKBは，異なるデバイス鍵でC2暗号処理しても同一の結果が得られるように構成されている。MKBは4C Entityから提供され，ディスクのデータ領域に記録される。アルバムIDは,ディスクごとに著作権者が自由に設定する値であり，ディスクのリードイン領域に記録される。

CPRMにおいては，デバイス鍵でMKBをC2暗号処理し，その結果をメディアIDでC2暗号処理して得られる結果を

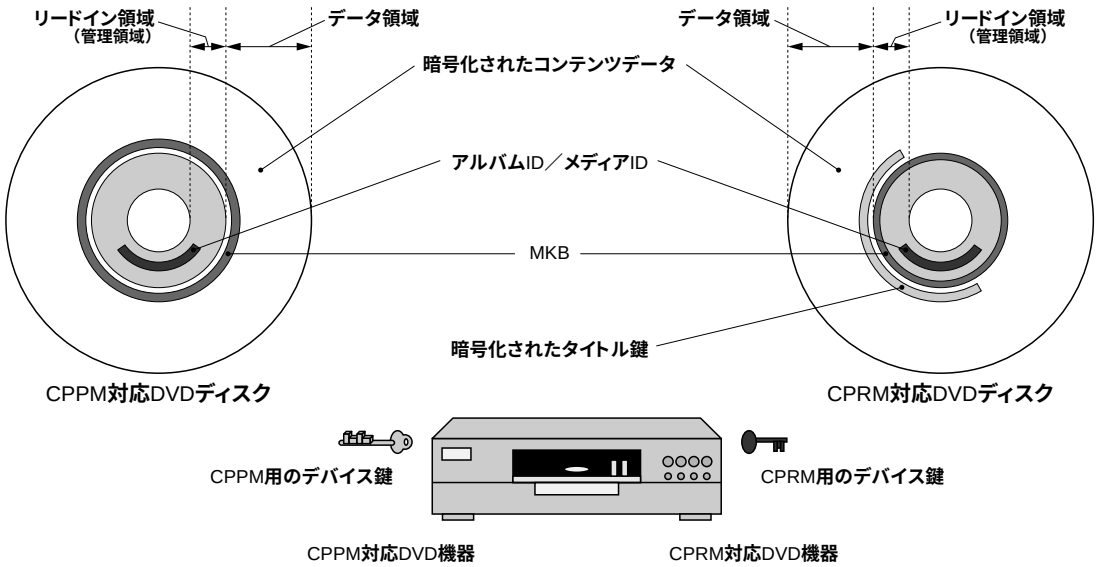


図3．CPPM及びCPRMにおけるコンテンツ及び鍵情報の配置 ― デバイス鍵はCPPM及びCPRM対応機器に，他の鍵情報及びコンテンツはディスクに記録される。

Layout of content and key information in content protection for prerecorded media (CPPM) and content protection for recordable media (CPRM)

用いて，コンテンツを暗号化及び復号するためにタイトルごとに自動設定されるタイトル鍵を暗号及び復号する。CPPMと同様に，当初のMKBは異なるデバイス鍵でC2暗号処理しても同一の結果が得られるように構成されている。

MKBは4C Entityから提供され，CPRMの場合はディスクのリードイン領域に記録される。メディアIDは，4C Entityから提供される枠組みの下でディスク製造業者によりディスク1枚ごとに異なる値が付与され，ディスクのリードイン領域に記録される。暗号化されたタイトル鍵は，ディスクのデータ領域に記録される。

3.3 ライセンス違反機器の無効化機能

CPPM及びCPRMでは，MKBによるライセンス違反機器の無効化機能が備わっている。無効化する場合には，MKBを新たに作成する際に，対象となるデバイス鍵でC2暗号処理を行っても正規の結果が得られないようにする。このため，無効化された機器では正しい暗号化又は復号が行えなくなる。MKBは，この処理を行うために適した数学的構造を持っており，また同じ目的からCPPM及びCPRMライセンス機器には16個のデバイス鍵が付与されている。

3.4 PCシステム用バス認証

CPPM及びCPRMが開発される以前に出荷されたDVDドライブとの互換性を最大限確保するため，CPPM及びCPRMのPCシステム用バス認証はCSSの場合とほぼ同一にされている。具体的には，CPPMの場合はCSSと同一，CPRMの場合はCSSのバス認証にインタフェース上でのデータ改ざんを防ぐ機能を追加したものとなっている。

3.5 記録型DVDディスク上のCPPMコンテンツ

CSSの場合と同様に，CPPMで暗号化されたDVDオーディオコンテンツは再生専用型DVDディスク上にのみ正規に存在する。このことを利用して，記録型DVDディスクの案内溝のウォブル（波状のうねり）を検知することによる記録型DVDディスク識別及びCPPMコンテンツ再生に関するルールが定められているが，機器側の対応が進んでいないことから，このルールは現時点では停止されている。

また，CPPM及びCPRMでは暗号化されていないオーディオ信号を再生する際にWM検出を義務づけており，WMが検出され，それがコピーフリー以外を示すものであった場合にはオーディオ再生を禁止するルールとなっている。ここでWMとは，4C Entityから別にライセンスされるVerance-4C Audio Watermarkとして知られるWMを指す。なお，このルールはCD-RやMD（ミニディスク）などの旧来のメディアには適用されない。

3.6 CPRM記録時の入力に関する規定

CPRM暗号化を使用して入力信号を記録する場合については，概略以下のルールが定められている。

⑴ セキュアな入力については，CCIに従い記録する。

⑵ セキュアな入力以外については，WM検知を行い，問題がなければCCIに従い記録する。

3.7 オーディオ出力に関する規定

CPPM及びCPRMを用いて保護されているオーディオコンテンツを復号して出力する際のルールは，概略以下のように定められている。

⑴ デジタル出力する場合は，下記⑵を除き，CCIとISRC（International Standard Recording Code information）を正しく伝送するセキュアな出力のみ認める。

⑵ IEC-958（国際電気標準会議規格958），IEC-60958，IEC-61937，USB（Universal Serial Bus）オーディオデバイスクラスの旧来デジタル出力については，以下の条件の下にCD音質以下の出力を認める。

ⓐ SCMSを付加できる場合には，SCMSを1世代コピー可に設定する。

ⓑ IEC-958，IEC-60958の使用は，2005年10月1日までとする。

⑶ アナログ出力はCD音質以下，等倍速を認める

3.8 ビデオ出力に関する規定

CPRMを用いて記録されているビデオコンテンツを復号して出力する際のルールは，概略以下のように定められている。

⑴ デジタル出力する場合は，下記⑵を除き，セキュアな出力のみ認める。

⑵ コンピュータ モニタ用出力を認める。

⑶ アナログ出力する場合は前記2.4節に同じである。

4 あとがき

DVDのコンテンツ保護は，単にコンテンツを暗号化して保護するだけでなく，製品の様々な側面に関与するものとなっている。当社はこの分野で先行しており，今後登場するDVDオーディオ レコーディングや高精細映像を記録する次世代DVDにおいても，市場，映画音楽業界，コンピュータ業界，及び民生電子機器業界が享受できるコンテンツ保護規格の開発を推進していく。

文 献

⑴ DVD Forum. <http://www.dvdforum.org/>, (accessed 2003-4-2).

⑵ DVD Copy Control Association.<http://www.dvdcca.org/>, (accessed 2003-4-2).

⑶ The Wassenaar Arrangement on Export Controls. <http://www.wassenaar.org/>, (accessed 2003-4-2).

⑷ 4C Entity. <http://www.4centity.com/>, (accessed 2003-4-2).

石原 淳 ISHIHARA Atsushi

デジタルメディアネットワーク社 コアテクノロジーセンター 光ディスク開発部参事。光ディスク機器の開発，規格化，コンテンツ保護業務に従事。

Core Technology Center