SPECIAL REPORTS

ホームデジタルコンテンツの保護技術

Home Digital Content Protection Technologies

田中　哲男　　山影　朋夫　　村谷　博文
■ TANAKA Akio　■ YAMAKAGE Tomoo　■ MURATANI Hirofumi

デジタルコンテンツを視聴・記録するデジタルAV機器では，コンテンツ保護機構を備えることが必要不可欠である。ここでは，暗号を用いた最近の保護システムを紹介し，今後の役割が期待されている“電子透かし”の技術について解説する。

Digital audiovisual appliances must protect copyrighted contents that are played and recorded on them. This paper describes recent encryption-based protection technologies and an emerging new information-embedding technology called the digital watermark.

1 まえがき

デジタル技術の進歩により，高品質な映像・音楽を視聴することができるようになってきた。パッケージメディアの形で配布されるDVDビデオをはじめとして，様々なコンテンツが様々なメディアを通じて供給される(**図1**)。コピーや再生の際に品質の劣化がないデジタルコンテンツでは，不正な複写などを防止するコンテンツ保護技術が強く求められる。適切な保護手段を備えていることが，良質なコンテンツの低価格での流通を可能にするからである。

ユーザーの利便を考えたとき，コンテンツの権利保護を実現したうえで，同時に実現すべき重要課題はインターオペラビリティ(相互運用可能性)である。同種のメディアを用いる機器間でインターオペラビリティが確保されなければ，利用者には受け入れられない。また，演奏・表示機器や記録機器の間でもこの性質が確保されなければならない。

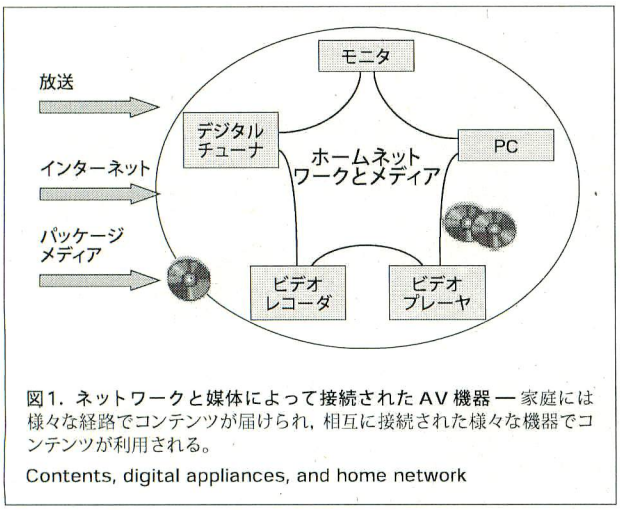

図1．ネットワークと媒体によって接続されたAV機器 ― 家庭には様々な経路でコンテンツが届けられ，相互に接続された様々な機器でコンテンツが利用される。
Contents, digital appliances, and home network

ここでは，まず，暗号技術を応用しインターオペラビリティに注意を払って開発されたCPPM(Content Protection for Pre-recorded Media)[1]，CPRM(Content Protection for Recordable Media)[2]，DTCP(Digital Transmission Content Protection)[3]などの保護規格を例として，媒体や機器での権利保護システムについて述べ，更に，次世代の保護規格の中に導入されると期待されている“電子透かし”技術について述べる。

2 記録メディアに書かれたコンテンツの保護

記録メディアには，読出し専用の媒体と書込みができる媒体とがある。DVDビデオやDVDオーディオなどの読出し専用媒体用に開発された保護規格がCSS(Content Scramble System)，CPPMであり，DVD-RAMやSDメモリカードなど書込み可能な媒体用に開発された保護規格がCPRMである。

これらの媒体を用いたときに重要なことは，媒体そのものの存在がコンテンツを操作する際の必要条件であることである。このような媒体を用いることによって，利用者は任意の機器へその媒体を運んで(あるときは居間のオーディオ装置で，あるときは電車の中でポータブル機器を使って)再生することができる。

これらの媒体上に記録されているコンテンツに対して行われる操作は，再生，複写，移動などである。これらの操作に対する制限は，コンテンツ供給者と利用者との間の契約によって定められている。例えば，あるコンテンツは“複写禁止”であろうし，あるコンテンツは“n回まで逐次複写可能”な

どと指定される。これらのコンテンツに対する操作許可条件を記述するのが，CPPMやCPRMでのCCI(Copy Control Information)である。

2.1 コンテンツ保護機構への要求事項

コンテンツ保護機構には，次のような事項が要求される。

(1) CCIで認められた操作だけが実行できること
(2) CCI自身は改ざんが行われないようにすること
(3) 正当な機器だけが再生し記録できること
(4) 認められていないコンテンツを系から排除すること
(5) コンテンツ保護機構を実装した機器は，保護機構が暴露されないよう十分に耐性を持って作られること
(6) 違反した機器又は改ざんされ迂回(うかい)機器となった不正機器があれば，それを系全体から排除(revoke)するようシステムが更新可能性(renewability)を持つこと

2.2 コンテンツ保護機構の実現

前述の要求を満たすべく，CPPMやCPRMでは以下のようにコンテンツ保護が実現されている。なお，パソコン(PC)はここでいう“機器”ではなくて，PCの“ソフトウェアプレーヤ”が一つの機器に対応すると考えるのがよい。

(1) 保護対象であるコンテンツは暗号化される。暗号化されていないコンテンツを保護することはできない。
(2) CCIもコンテンツとともに暗号化される。暗号化されないCCIもコンテンツといっしょに配布されるが，暗号化されているCCIと一致しなければ不正であるとみなす。
(3) 機器は媒体が正しいものであることを認証する。例えば，PC上のプレーヤは，媒体のドライブ装置との機密通信によって，ドライブ及び媒体を認証する。
(4) コンテンツは機器あるいは媒体に関連付ける。可搬媒体に関連付けられたコンテンツは，媒体とともに移動できるが，機器に関連付けられたコンテンツは，機器から離れて存在することはできない。
(5) 正当な機器だけが暗号の鍵を入手することができる。CPPM，CPRMでは，このための機構としてMKB(Media Key Block)が用意されている。MKBは，媒体の中に改変できない方法で記録されている。MKBを用いた正しい復号鍵の生成と，不正機器の排除の仕組みを**図2**に示す。
(6) 機器の排除又はシステムの更新は，新たなMKBを配布することによって行う。

家庭で使われる機器は，まずそれ1台だけで利用されるのが原則であり，媒体を用いた保護の仕組みが実現されている。また，正しい媒体はどの機器においても利用できるように保護の仕組みが作られている。

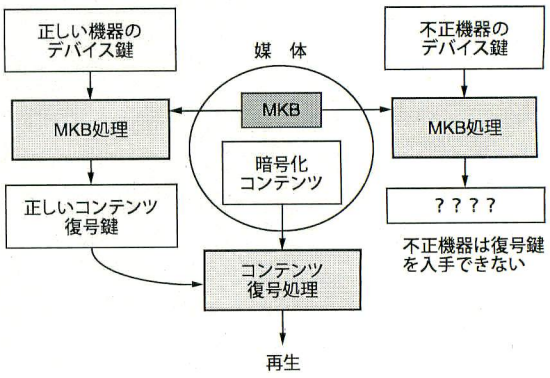

図2. CPPM/CPRMにおけるメディアキーブロック ― 正しい機器だけが暗号を解いてコンテンツを再生することができる。
Media key block in content protection for prerecorded media/ content protection for recordable media (CPPM/CPRM)

3 家庭における機器の接続と保護

家庭における機器は原則としてスタンドアロンで動作すると述べたが，それは基本的な動作に関してであって，機器がホームネットワークなどによって相互に接続されることにより，更なる利便を得ることができる。消費者が所有する機器が物理的に接続され，更にコンテンツ保護の観点からもインターオペラブルに動作することが重要である。

将来のコンテンツ保護が行われた映像配信を例にとって，機器の接続の際に求められる保護の仕組みについて考える。配信された映像が，家庭の中の相互に接続された機器によってどのように取り扱われるかを**図3**に示す。セットトップボックス(STB)やPCが，コンディショナルアクセスの契約に従って映像配信を受信する。ここでは，その映像を家庭内で視聴し，一つだけ複製を作って保持することが認められて

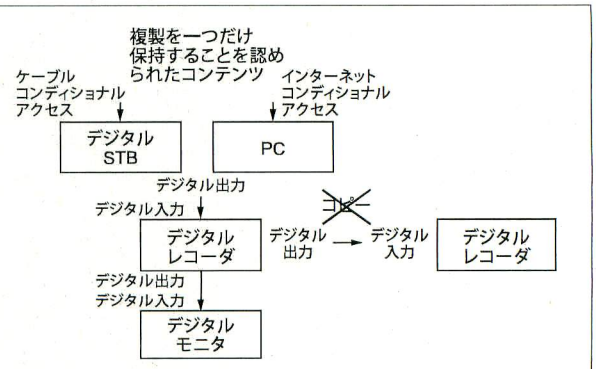

図3. ホームネットワークでの保護 ― コンテンツを保持したまま，ネットワーク上でコピーを作ることはできない。
Content protection in home network

いるものとしよう。利用者はその映像をSTBやPCから，ホームネットワークを介してデジタルレコーダに転送し，複製を作って保持することができる。利用者は後で，デジタルレコーダが保持している映像をネットワーク経由でデジタルモニタに表示し，楽しむことができる。これらの操作は，各機器が正当な機器であるときにだけ可能である。

しかし，利用者がデジタルレコーダの出力を他のデジタルレコーダに転送して，二つ目の複製を作ろうとしても，それは実行できない。権利者の許諾を受けていないからである。

ネットワークでの通信は傍受される可能性があり，またネットワークで接続される相手は，本来は“身元不明”の機器であるから，不用意に伝送すると不正な複製が行われる可能性がある。このようなネットワーク上でコンテンツを保護するための規格としてDTCPがあり，DTCPでは以下のようにコンテンツ保護が実現されている。

(1) 伝送路上のコンテンツはすべて暗号化する。
(2) コンテンツとともにCCIの伝達を行う。
(3) 伝送に先立って，通信相手がDTCPの規格に合致した正しい機器であることを認証する。
(4) 不正機器と認定された機器はシステムから排除される。この情報を伝達するためにSRM(System Renewability Message)が定められている。

DTCPとCPPM，CPRMなどが互いに相手を承認し，相互に協調し合うことによって，家庭における現在のコンテンツ保護が実現している。また，これらの機器が協調するためのシステムアーキテクチャとして，CPSA(Content Protection System Architecture)が提案されている[4]。

4 映像用電子透かし

映像や音楽などのコンテンツは，小さな変更が加わっても，元のコンテンツとほとんど変っていないように認識される。電子透かし(digital watermarking[5])とは，この冗長性を利用してコンテンツの中に別の情報を埋め込むことをいう。ヘッダ情報のようにコンテンツに付加された情報の場合には，そのヘッダ部分を取り除くことで容易にコンテンツとヘッダ情報を分離することができるのに対して，電子透かしの場合には，コンテンツと不可分な形で別の情報を保存，伝送できることが特長である。

暗号技術が，メッセージの授受の途中でメッセージを改ざんされたり盗み見られたりすることを防ぐ技術であるのに対して，電子透かし技術は，いったん受信者の手に渡ったメッセージ(コンテンツ)が，復号後においても不正に利用されることを防ぐことを主要な目的とする。

コンテンツに対して透かしを書き込む処理を埋込みといい，コンテンツに埋め込まれている電子透かしを読み取る処理を検出という。既に電子透かしが埋め込まれているコンテンツを入力して，別の電子透かしに書き換える処理はリマーキングと呼ばれる。

4.1 電子透かしの要件

電子透かしの要件には，次のようなものがある。

(1) 不可視性(transparency)　埋込みによりコンテンツ品質が劣化しない性質
(2) 頑健性(robustness)　そのコンテンツが通常受ける操作や意図的な攻撃で電子透かしが消失したり改ざんされたりしない性質
(3) ブラインド性(blindness)　検出にオリジナルが必要か否か
(4) セキュリティ　電子透かしの不正な検出，改ざん，消去，偽造に対する強さ
(5) 容量　何ビットの電子透かしを埋め込むのか

4.2 電子透かしの埋込み方式

画像に対する電子透かしの埋込み方式は，画素領域(空間領域ともいう)への埋込みと周波数領域への埋込みに大別される。画素領域への埋込みでは，各画素の値が独立に変更されるのに対して，周波数領域への埋込みでは，画素の値は，ある周波数を持った波のように変更される。一般に，周波数領域への埋込みのほうが不可視性が高い。周波数変換としては，DCT(Discrete Cosine Transform)や離散フーリエ変換やウェーブレット変換などが用いられる。

電子透かしの埋込みには，知覚モデル(perceptual model)が応用されることが多い。例えば画像の場合，人の視覚系が平坦部分よりもランダム部分やエッジ部分のノイズを認識しにくいことから，それらの部分で電子透かしを強く埋め込む方法がある。このような処理を画像適応という。

コンテンツが通常に受ける操作や意図的な攻撃によって，その情報が消失したり改ざんされにくいものを“ロバストな透かし”という。それに対して，ある想定した操作に対して埋め込まれた内容が変わることを期待されているものを“ぜい弱な透かし”という。

頑健性は，冗長な埋込みを行うことで高めることができる。スペクトル拡散法のように相関に基づく検出がその例である。

4.3 電子透かしによるコンテンツ保護

電子透かし技術をコンテンツの保護に用いるためのシステムの概念を**図4**に示す。コンテンツ作成者は，電子透かし技術を用いてCCIをコンテンツに埋め込み，記録メディアに記録する。CCIには，“コピー可”，“コピー不可”，“一世代コピー可”，一世代コピーした後の状態である“孫コピー不可”などがある。

コンテンツを再生／記録する機器は，コンテンツに埋め込まれている電子透かし信号からCCIを検出し，不正に再生／記録しようとした場合，動作を停止する。動作停止条件

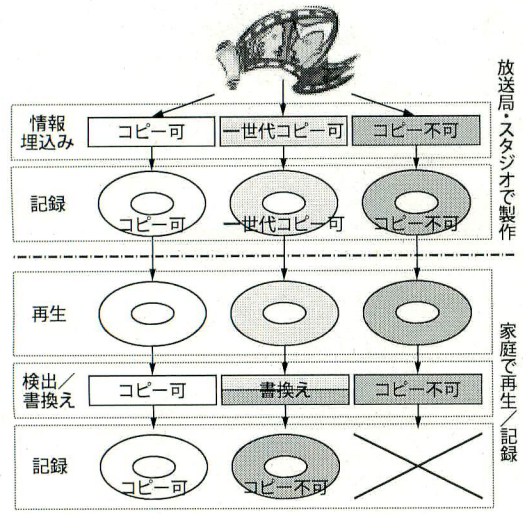

図4. 電子透かしによるコンテンツ保護システム ― コンテンツ作成時に埋め込んだ情報により，コピー作成の可否を制御する。
Content protection system using watermark

の例を以下に示す。

(1) コピー不可又は孫コピー不可のコンテンツを記録しようとした場合（コピー不可のため）

(2) コピー不可のコンテンツを記録可能メディアから再生しようとした場合（不正にコピーしたと判断したため）

(3) 暗号化されていないコンテンツの再生時にコピー可以外のCCIを検出した場合（CCIと暗号化条件の不整合があるため）

コンテンツの伝送媒体を放送やインターネット配信などに置き換えた場合も，同様の手法でコンテンツ保護を行う。

4.4 電子透かしによるコンテンツ保護のメリット

電子透かし技術をコンテンツ保護に用いることのメリットは，以下の2点である。

(1) 不正に情報の改ざんを行おうとすると，画像全体に対する操作が必要であるとともに，操作後の画像に劣化が発生する。これはアナログビデオ信号保護の既存方式であり，ビデオ信号のブランキング期間を利用しているマクロビジョンやCGMS-A（Copy Generation Management System－Analog）に対して優位な点である。

(2) end-to-end（端末相互間）のコンテンツ保護システムを構築できる可能性を持っている。これは，コンテンツ作成後の流通（記録・配信）と消費（再生）のどの段階においても，コンテンツに埋め込まれたCCIを検出することにより，コンテンツ保護の機構を組み込むことで実現できる。

このようなメリットがある一方，電子透かし技術をコンテンツ保護に適用するには，機器側への強制力を行使する仕組みが必要になる。その理由は，電子透かし技術は暗号技術と異なり，コンテンツそのものを秘匿する技術ではなく，コンテンツに情報を埋め込む技術であるためである。そのため，電子透かしを検出しない機器（無反応機器）に対しては，コンテンツ保護の効果を発揮しない。

機器側への強制力の行使を実現する方法として，CPSAの一環として，CPPM，CPRM，DTCPなどのコンテンツを暗号化保護技術のライセンスを受けた機器では，電子透かしの検出を義務づけるというライセンス条件の拡張が審議されている。更に，上記のライセンス機器以外の機器に対しても，強制力が働く仕組みの構築についての議論が必要になる。

このようなコンテンツ保護システムが構築されれば，DVD，放送，インターネット配信などの伝送媒体を問わずセキュアなコンテンツ流通が可能になるため，コンテンツ流通が活性化することが期待される。

5 あとがき

デジタルコンテンツに対して適切な著作権保護機構を備えることが，視聴者にセキュアで快適な演奏空間を提供することにつながる。今後とも，新しい情報通信技術に適合した保護技術を開発していく。

文 献

(1) Brendan, C.; Traw, S. Protecting Digital Content within the Home. IEEE Computer. **34**, 10, 2001, p.42－47.
(2) 加藤 拓，ほか. DVD-Audioにおけるコンテンツ保護技術. 東芝レビュー. **56**, 7, 2001, p.54－57.
(3) "DTCP Specification Volume 1 Version 1.2（Informational Version）". DTLA. 入手先〈http://www.dtcp.com/〉,（参照2002-07-12）.
(4) "Content Protection System Architecture (CPSA)". 4C Entity. 入手先〈http://www.4centity.com/〉,（参照2002-07-12）.
(5) Katzenbeisser, S.; Petitcolas, F.A.P. Information Hiding Techniques for Steganography and Digital Watermarking, Artech House Books, 2000－01, 220p.

田中 晢男 TANAKA Akio
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技監。コンテンツ保護，マルチメディア情報処理などの研究・開発に従事。IEEE，IEICE，IPSJ会員。
Core Technology Center

山影 朋夫 YAMAKAGE Tomoo
研究開発センター マルチメディアラボラトリー研究主務。動画像用電子透かし及びMPEG関連システムLSIの研究・開発に従事。IEICE会員。
Multimedia Lab.

村谷 博文 MURATANI Hirofumi, D.Sc.
研究開発センター コンピュータ・ネットワークラボラトリー研究主務，理博。電子透かし技術及び情報セキュリティ技術の研究・開発に従事。IEEE，ACM，IPSJ，IEICE会員。
Computer & Network Systems Lab.