コンテンツ保護アーキテクチャ

Content Protection Architecture

加藤　　拓

■ KATOH Taku

コンテンツの記録機器やパソコン（PC）が手軽に利用できるようになって以来，エンターテインメントコンテンツを扱う場合には，コンテンツ保護技術が重要な要件となっている。DVDをテレビ（TV）で見る，デジタル放送をレコーダで記録するといった用途を見てもわかるように，コンテンツ保護の健全性を保つためには，コンテンツ保護技術どうしの連携が重要になっている。コンテンツ保護を考えるうえでは，個々の技術内容だけでなく，その技術を取り扱うためのライセンス内容についても十分な検討が必要であり，更に法律による対応も重要になっている。

Since content recorders and PCs became popular, content protection has been an important technology for the handling of entertainment content by users.　In situations such as users watching and recording digital TV broadcast content, it is important to preserve the soundness of the chain of content protection technologies.

In content protection architecture, it is necessary to consider both the technologies and their licenses.　It is also important to take the related legislation into consideration.

1　まえがき

1960年代から70年代にかけてコンパクトカセットやアナログビデオレコーダが登場し，個人でも音楽や映像コンテンツを手軽に記録できるようになるにつれ，コンテンツ提供者（著作権所有者）は不正コピーへの対策としてコンテンツ保護技術に関心を高めてきた。実際には，VHS（Video Home System）においてコピーガード信号が，CDでは世代コピー管理情報が導入され，これらの技術は積極的にコピー管理をしようとする機器にとっては有用な情報として扱われている。しかし，これらの情報は消去や書換えが比較的容易に行えるため，コピーガードキャンセラやPCを使用したコピーが行われているのが実情である。

そのため，特にコンテンツ提供者はデジタルコンテンツの保護には非常に高い関心を示しており，著作権主張されたデジタルコンテンツを扱うためにはコンテンツ提供者に認められたコンテンツ保護方式を使用するようになってきている。例えば，DVDビデオではデータにスクランブルが施され，DVDオーディオなどでは不正機器の無効化機能まで導入されるに至っている。

ここでは，AVコンテンツ，特にデジタルデータを扱う際に考えなければならないコンテンツ保護システムの構成（アーキテクチャ）について説明するとともに，実際に使用されているコンテンツ保護技術について述べる。

2　コンテンツ保護システムの構成

ここで扱うコンテンツ保護対象コンテンツ（以下，コンテンツと言う）とは，放送やパッケージメディア（DVDなど）などの手段によってユーザーの手もとに届くコンテンツのことであり，一般にエンターテインメントコンテンツと呼ばれるものである。そのようなコンテンツには，コンテンツ提供者から送り出される際に，コンテンツに応じて次のような様々なコンテンツ管理情報が設定されている。

⑴　コピーフリー，1世代コピー可，コピー不可といったコピー世代管理
⑵　デジタルコピーの枚数制限
⑶　アナログコピーガード信号の設定，アナログ出力時の解像度制限，デジタルコピー時の音質制限
⑷　一時蓄積の時間制限

放送受信機，DVDプレーヤといったコンテンツを扱う機器は，これらのコンテンツ管理情報に従ってコンテンツを取り扱う必要がある。なお，コピーフリーといった場合にも，ユーザーは著作権法で規定された私的使用のための複製などの制限にも注意を払う必要がある。

コンテンツを扱う機器は，コンテンツ管理情報に従ってコンテンツを次の機器に受け渡さなければならない。自分自身がいかに強固にコンテンツを保護していたとしても，コンテンツを受け渡した先の機器（技術）からコンテンツが不正に流出してしまっては意味がない。1か所にでも不正流出の

穴があればシステムに大きな影響を与えることとなる。そのため，コンテンツ保護技術のライセンス条件には，どのようなコンテンツ保護技術を搭載した機器へコンテンツを受け渡してよいかといった条件も明記されている。このように，コンテンツ保護は一つ一つの機器でのみ守られるものではなく，コンテンツを扱う機器（技術）間で連鎖的に守られなければならない（**図1**）。

コンテンツを扱う機器は，技術ライセンスを受ける際に付随するコンプライアンスルール，ロバストネスルールや運用規定に従って製造することが義務づけられており，ルールに違反した場合にはライセンス取消しだけでなく，場合によっては法律によって取締りを受ける可能性もある。

3 コンテンツ提供時のコンテンツ保護

3.1 放送コンテンツ

日本でも2000年からBS（放送衛星）デジタル放送が開始され，一部地域では2003年末までには地上波デジタル放送も開始される。これまでのアナログ放送では，一部CS（通信衛星）放送を除いて特にコンテンツ管理情報は付けられておらず，VHSなどの記録機器で自由に録画，更に録画テープのコピーを行うことができ，その記録テープは著作権法などの法律で保護されるだけであった。しかし，個々のユーザーによる不正コピーや不正使用を取り締まることは事実上不可能であるのが現状である。

それに対して，デジタル放送では，コンテンツの利用ルールを放送局が決められるようにするために，様々なコンテンツ管理情報が付けられるようになっている。デジタルコンテンツの場合には，コンテンツ保護が施されていなければ，デジタル記録機器を使用することにより，コンテンツは何度でも劣化なくコピーすることが可能であり，不正利用された場合には被害が大きくなることも考えられるため，コンテンツ管理情報が重要になってくる。

特に，デジタルコンテンツの場合にはインターネットを介してコンテンツを送受信することが簡単に行え，簡単に“私的使用のための複製”の範囲を超えてコピーをすることが可能となるため，“私的（家庭内）使用においてはコピーに制限はないが，受信コンテンツを家庭内使用の範囲外へ送信（再送信）すること”を明示的に禁止するためのコンテンツ管理情報“EPN（Encryption Plus Non-assertion）”が設定可能になっている。

日本のBSデジタル放送では，“コピーフリー”以外のコンテンツはCAS（Conditional Access System）技術方式を用いてスクランブルされるため，スクランブルされた放送を受信する受信装置を製造するためには（株）ビーエス・コンディショナルアクセスシステムズが提供するB-CASカードの支給を受けなければならない。コンテンツ管理情報に従わない，例えばコピー不可コンテンツをコピーフリーとして出力す

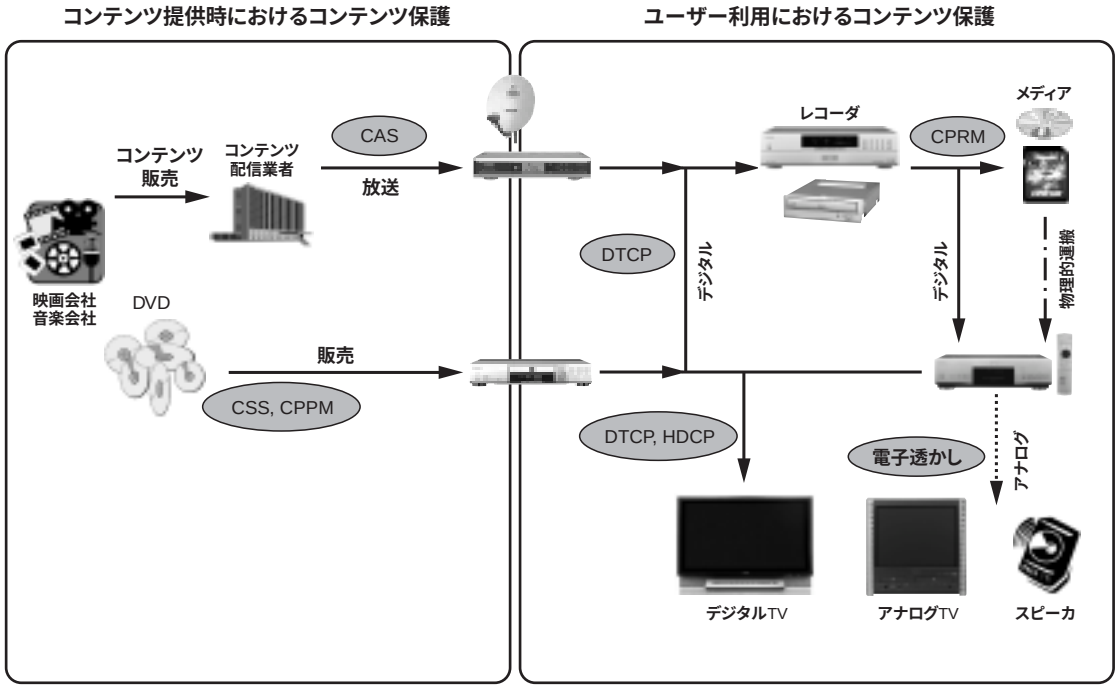

図1．コンテンツ保護技術の連携 ― コンテンツ保護においては，保護技術どうしの連携が重要である。
Content protection chain

るなど，不正な受信機を製造販売した場合にはB-CASカードの支給を停止することにより，不正受信機を取り締まることが可能である。

それに対して米国では，不正な放送受信機の製造を，技術ライセンスではなく法律で取り締まろうとする動きがある。

3.2 DVD

70年代に登場したVHSでは，コピー不可コンテンツがVHSテープに（きれいに）記録されることを防ぐために，コピーガード信号に反応するようになっている。このコピーガード信号は，コンテンツがコピー不可の場合には，DVDビデオなどのデジタル機器からのアナログ出力にも挿入されるようになっている。

96年に登場したDVD-Videoでは，CSS（Content Scramble System）[1]と呼ばれるコンテンツ保護技術が採用されている。CSSは，不正コピーを懸念する映画業界から著作権保護対策が望まれ，映画音楽業界，民生電子機器業界，及びコンピュータ業界が合意できる著作権保護技術として作成されたコンテンツ保護技術であり，現在はDVD CCA（DVD Copy Control Association）によってライセンスされている。CSSは，① 3階層の暗号鍵管理，② コンテンツスクランブル，及び③バス認証などの要素技術を備えている。

更に，DVD-Audioではコンテンツ保護技術としてCPPM（Content Protection for Prerecorded Media）[2]技術が採用されている。CPPMはコンテンツ提供者の要求を満たすために，① コンテンツ暗号化，② リムーバブルメディアに適した階層的鍵管理，③ バス認証，及び④ メディアによる不正機器の無効化などの技術を備えている。また，DVD-Audioではコンテンツ保護のためにオーディオ電子透かし（Audio Watermark）が採用されている。オーディオ電子透かしは，オーディオコンテンツがアナログ出力などで適切な保護が施されずに扱われた場合にも，コンテンツ管理情報を正しく伝えるために用意されている。

4 コンテンツ伝送時のコンテンツ保護

上述のように，著作権主張のされた放送コンテンツやDVDビデオコンテンツを直接扱う（最初に再生する）機器は，コンテンツ再生に必要なライセンスを受けることにより，保護されたコンテンツを再生することやコンテンツに付随するコンテンツ管理情報を正確に知ることができる。それに加えて，再生されたコンテンツを別の機器で表示・記録する場合には，再生されたコンテンツとコンテンツ管理情報を，表示・記録する機器に安全に伝える必要がある。このような場合に使われるのが，伝送路上のコンテンツ保護技術である。

4.1 DTCP

DTCP（Digital Transmission Content Protection）[3]は大きく分けて，① 認証及び鍵交換，② コンテンツ暗号化，③ コピー制御情報，④ システム リニューアビリティの四つの要素技術を備えている。

機器間におけるコンテンツの送受信では，まず互いに相手の機器を認証してコンテンツの暗号化に必要な鍵を共有し，共有された鍵を元に定期的に更新される鍵を使って暗号化されたコンテンツが伝送される。なお，1世代コピー可のコンテンツであっても，同時に大量にコピーする，あるいはコンテンツを同時に多くの場所で視聴するといった利用形態は，私的利用の範囲を超える可能性があるため，DTCPでは同じコンテンツを同時に受信できる機器の数を制限する仕組みも取り入れられている。

更に，システムの完全性の維持と不正機器の排除を目的として，機器の無効化リストの更新機能もある。リストの更新方法としては，例えばDVD-Videoディスクに無効化リストを記録しておき，当該ディスクを再生したDVDプレーヤ内の無効化リストを更新するだけでなく，DTCP経由でコンテンツを受信する機器（TVやレコーダなど）でも無効化リストを更新できるような仕組みが考えられている。この点においても，コンテンツ保護システムは，個々に独立に扱われるものではなく，互いに連携することによって成り立っていることがわかる。

DTCPは，2003年3月現在，IEEE1394（米国電気電子技術者協会規格1394），USB（Universal Serial Bus），MOST（Media Oriented System Transport）向けにライセンスが行われている。

4.2 HDCP

HDCP（High-bandwidth Digital Content Protection）[4]はDVI（Digital Visual Interface）やHDMI（High Definition Multimedia Interface）向けのコンテンツ保護技術であり，その対象をコンテンツの表示目的に限定しているところに特徴がある。つまり，HDCPで保護されたコンテンツを受信した場合には，そのコンテンツにもともとどんなコンテンツ管理情報が付けられていたかによらず，モニタへの表示目的にしか使用できない。ベースバンドコンテンツを保護対象としたHDCPは，PCのモニタのようにMPEG（Moving Picture Experts Group）などのデコーダを持たないデバイスに向いたコンテンツ保護方式である。

4.3 アナログ出力

VHSレコーダや多くのTVのように，アナログ入力しか持たないデバイスに対しては，もともとがデジタルデータであっても最終的にはアナログデータに変換して出力する必要がある。その際のビデオデータのコンテンツ保護としては，アナログコピーガード信号やCGMS-A（Copy Generation Management System - Analog）があるが，これらの信号は比較的簡単に除去されてしまう。そこで，除去が難しい方法

として，電子透かし技術がある。既にDVD-Audioでは電子透かし技術が採用されており，DVD-Videoに関しても電子透かし技術導入が検討されている。

5 コンテンツ記録時のコンテンツ保護技術 CPRM

DVD-RAM/R（Recordable）/RW（ReWritable）用のビデオ記録フォーマット（Video Recording Format）には，CPRM（Content Protection for Recordable Media）[5]と呼ばれるコンテンツ保護技術が採用されいる。CPRMは3.2節で述べたCPPMと非常に類似した技術であり，① コンテンツ暗号化，② 記録用リムーバブルメディアに適した鍵管理，及び③メディアによる不正機器の無効化を実現する技術，は基本的にCPPMと同じ技術である。

SDメモリカードにおいても，同様のCPRM技術[6]が採用されている。

6 コンテンツ保護技術ライセンス

機器製造者は，暗号化されたコンテンツを復号するために必要なライセンス契約を結ぶことにより，前述のように，メディア上や伝送路上ではコンテンツの暗号化などによりコンテンツ保護が実現される。しかし，コンテンツを扱う機器内では，次の保護技術に受け渡したり表示するためにコンテンツは平文の状態となる。そのため，機器の持つ秘密鍵（デバイス鍵）などの重要な秘密が露呈したり，コンテンツに適切な保護が掛けられずに出力されることを防ぐために，コンテンツ保護には一般的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。これらには次のような規定がある。

⑴ 秘密情報の機器内秘匿要件
⑵ 規定に従った機器出力の制限（セキュアデジタル出力，非セキュア出力時の画質・音質制限など）
⑶ メディア上に書かれているコンテンツ管理情報を出力信号へ正確に反映
⑷ 保護技術の使用目的
⑸ 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
⑹ 機器の再生制御規則や出力制御規則

秘密情報が漏えいしたり機器が規定に準拠しなくなった場合など，本来意図した以外の動作をする機器（不正機器）が出てきた際には，その不正機器をコンテンツ保護システムから排除する（不正機器の無効化）手続きが取られることになる。一つの不正機器の存在は，場合により多大な被害を引き起こす可能性もあるため，適切な対処が必要となる。更に，その被害が大きい場合には，当該機器製造者のライセンスが取り消される可能性もある。

7 あとがき

ここでは，エンターテインメントコンテンツを扱う場合に考えられているコンテンツ保護の考え方と，それを実現するために必要となる保護技術の連携の重要性について述べるとともに，実際に使われているコンテンツ保護技術を紹介した。コンテンツ保護を考える場合には，技術だけでなく，それに関連する法律も重要となる。それに加えて，個々のユーザーがコンテンツ保護（コンテンツ著作権者の権利保護）を意識することも重要である。

文 献

⑴ 館林 誠，ほか．“DVD著作権保護システム”．映像情報メディア学会技術報告．画像情報記録．**21**，31，1997-5，p.15－19.
⑵ 4C Entity, LLC. "Content Protection for Prerecorded Media Specification, DVD Book", Rev.0.93, Jan. 31, 2001.
＜http://www.4centity.com/＞, (accessed 2003-4-7).
⑶ Digital Transmission Licensing Administrator. "Digital Transmission Content Protection Specification", Vol.1(Informational Version), Rev.1.2a, Feb. 25, 2002.
＜http://www.dtcp.com/＞, (accessed 2003-4-7).
⑷ Digital Content Protection, LLC. "High-bandwidth Digital Content Protection System", Rev.1.091", Apr. 22, 2003.
＜http://www.digital-cp.com/＞, (accessed 2003-4-28).
⑸ 4C Entity, LLC. "Content Protection for Recordable Media Specification, DVD Book", Rev. 0.96, Jan. 31, 2003.
＜http://www.4centity.com/＞, (accessed 2003-4-7).
⑹ 4C Entity, LLC. "Content Protection for Recordable Media Specification, SD Memory Card Book, Common part", Rev. 0.96, Jan. 10, 2002.
＜http://www.4centity.com/＞, (accessed 2003-4-7).

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 SI技術担当主務，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