TREND

デジタルコンテンツ保護の現状と課題

Current Status of Digital Content Protection and Related Issues

山田　尚志　　**河原　潤一**

■ YAMADA Hisashi　　■ KAWAHARA Junichi

インターネットの普及に伴い，コンテンツ保護が大きな課題になりつつある。コンテンツ保護は著作権者の権利を守るということだけではなく，適切な保護なしでは，インターネット上での新しいサービスやビジネスができないことがしだいにはっきりしつつある。技術的には，保護のレベルそのものを強くすることは可能ではあるが，それにより使用者が不便を感じるようでは本末転倒である。

一方で，インターネット上ではすべての情報は無料という誤った常識が形成され始めており，これに対して，コンテンツは著作権者に対価を払って正しく利用しなければならないと認識してもらうことが重要である。そして，楽しくコンテンツを利用するために，コンテンツ保護が果たす正当な役割を認識してもらう必要がある。

社会が大きく変わるときには法律も後追いになり，新しい秩序ができるまでは混乱が続くのが常である。現在はその混乱期であり，技術，法律，啓蒙（けいもう）活動を通してコンテンツ保護を認識してもらうとともに，技術的に納得性のあるシステムの導入が課題である。

The worldwide expansion of the Internet has created many issues to be solved from the content protection perspective. Content protection is necessary not only to properly protect the rights of content owners but also to do business via the Internet. Technologies for content protection are well developed and can realize a sufficiently strong protection system. Causing inconvenience to users by content protection, however, would be like putting the cart before the horse. On the other hand, there is an expanding view that information via the Internet is or should be free of charge.

In this connection, it is important for a general perception to be established that content should always be enjoyed and consumed correctly by paying a reasonable fee to content owners, otherwise business via the Internet will never become a reality. Significant changes in a social system are always accompanied by chaos and confusion among the public. Moreover, legislation is not prepared in time for rapid change. We are now in such a period of chaos, and need to introduce reasonable technical solutions for the future.

インターネットの普及とコンテンツ保護

コンテンツということばが一般化したのは，ここ数年ではないかと思われる。それだけ，ビジネスにおけるコンテンツの重要性が認識されてきたと言える。それに伴い，違法コピーなどコンテンツに関係するビジネスを脅かす存在も顕在化し，これに対する保護が問題となってきている。

インターネットにおけるウィルスが問題化しているが，まったく同じ時期に，ファイル交換などのコンテンツに対する脅威が問題化してきたのは，それだけインターネットが普及して身近なものになったことと軌を同じくしている。マルチメディア時代においては，コンテンツの保護と適正な利用環境の実現が必須であり，一般利用者，機器製造者，コンテンツの権利保持者の3者が平等に恩恵を受けるような環境の実現が，コンテンツ保護の最終目標である。

コンテンツ保護

DVDは，1996年11月に市場に導入されたが，実質的な導入は97年である。この後，**図1**に示すように，今まで登場したメディアフォーマットの中ではもっとも速い成長を示し，2003年のDVD機器の市場規模は6～7千万台，そして2004年には1億台の大台を超えるものと予想されており，かつパソコン（PC）でも同じ程度の市場が期待できる。

DVDに対しては，量産メディアでは初めてコンテンツ保護の技術が導入された。このときは，暗号技術の輸出規制などの問題で鍵の長さも40ビットと制限され，システムとしては十分な強さにできなかったため，後に問題が発生した。

コンテンツの保護と消費者の権利との関係の調整はもっとも重要である。もともとコンテンツは，消費者が使用し又は楽しむために生み出されたものであり，消費者のもとに配信されて初めて役にたつと言える。しかし，このコピーが無制限に行われた場合，コンテンツの権利保持者が正当な収入を得ることができず，コンテンツの再生産がで

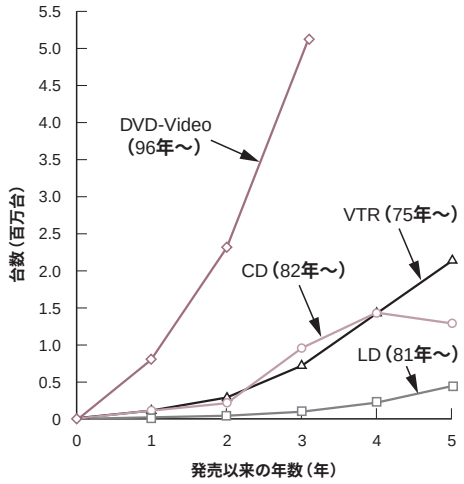

図1．DVD市場の立上り ― DVDは歴史上もっとも速い市場の立上りを示している。
DVD market

表1．WIPO著作権条約の規定
Digital Agenda of World Intellectual Property Organization (WIPO)

WIPO著作権条約		日本	米国	EU
技術的保護手段迂回規制	アクセス管理技術	不当競争防止法	著作権改正法（DMCA）	条件付きアクセス指令
	コピー管理技術	不当競争防止法 著作権法		著作権指令
私的複製の権利制限見直し		著作権法	フェアユースで判断	著作権指令
権利管理情報の改ざん規制		著作権法	DMCA	著作権指令
一般頒布権の導入		著作権法	著作権法（頒布権）	著作権指令
公衆への伝達権の創設		著作権法	著作権法（頒布権）	著作権指令

きなくなる事態も考えられる。

消費者と著作権保持者の権利主張がぶつかり合ってきたのが過去の歴史であるが，技術の進歩により，インターネットを通じて，普通の個人が一瞬で世界中にコンテンツをばらまくことが可能になった現代では，この権利関係にも新しい考え方を入れていく必要がある。特に過去には，コピーと言えばかなり物理的なイメージでのコピーであったが，デジタル時代になり，コピーの形と忠実度が変わり，いくらコピーしても質が低下しないなど，環境は大きく変わった。

この環境のもとで，法律面からだけでなく，消費者の意識をも変えていく必要がある。

著作権に関する法律の問題

97年にWIPO（World Intellectual Property Organization：世界著作権機構）の条約原案が提案され，ここでは，**表1**に示すような権利が認められた。これを受けて，各国で国内法の整備が進められている。特にインターネット時代を反映して，インターネットを通じてコンテンツを配信する権利など，今まで定義されていない権利が認められている。

現在もっとも問題となっているのは，私的複製の範囲である。法律的には，私的複製の権利は正当な範囲の使い方であれば以前から認められているが，インターネットを通じてそれをばらまくことまでは正当化されない，というのが今の解釈である。

しかし，法律の批准に際して各国の対応が異なり，国により解釈が一定していない。米国は，基本的に判例により法律の範囲を決めていく体制なので，後述するNapsterも結局は，被害が拡大して初めて対応した結果，音楽産業に対する影響は深刻なものになってしまった。これ以後，コンテンツ保護はパッケージだけの問題ではなくなり，基本的にはネットワーク社会でのコンテンツ保護の問題に発展した。

また，ネットワークでの保護の問題から，逆に，家庭内での利用に関して制限を加えずにインターネット社会での保護ができるかという問題も持ち上がっている。インターネットでは，一瞬のうちに世界中が結ばれるのであるから，家庭内といっても遠隔地の肉親も簡単に結ばれてしまう。従来の法律では，家庭内に限り適正な範囲でのコンテンツのコピーは認められているが，この家庭の概念が大きく変わってきており，法律のほうが実際の社会に合わなくなりつつある。

技術的に方法はあるが，利用者に負担を掛けずに実現するとなると，問題がかなり難しくなる。例えば，一人一人がID（IDentification）カードを持参し，これを機器に挿入することにより，家庭内の特定した人数での視聴コピーは自由に行えるようにして，かつ自動車などにもコンテンツを移して楽しめるようにするなどの提案がなされている。

しかし，今まで何の制限もなく家庭内では自由に視聴できていたはずが，IDカードを挿入しないとできないということでは，消費者に対する負担が大きいという反論もあり，必ずしも一般的な納得を得られていない。

コンテンツの消費に関する法律上の規制は，もともと家庭内には立ち入らなかったのに対して，コンテンツの消費は家庭内で行われ，家庭がインターネットを通じて世界に直接つながっているところに，現代社会の問題がある。

インターネットの問題

インターネットでは，現在，ファイル交換という違法コピーの交換システムがはびこっており大きな問題となっている。

米国において，一大学生が始めたNapsterが，インターネット上のファイル交換の最初であり，初めは，インターネット上でコンテンツを配布するもっとも安くて便利な手段として，Peer to Peer(注1)伝送という新語まで生まれるブームとなった(**図2**)。

Napsterの当初の主張は，Napsterのサーバには利用者が個人PC上に保有している音楽ファイルに関する情報のみを掲載し，音楽ファイル自体は使用者どうしがファイル交換するだけであり，この仕組み自体は，利用者が自分でコピーした音楽ファイルを友人にあげる行為と変わらない，というものであった。

コピーを作って他人にあげるという行為は合法とは言いがたいが，捕捉(ほそく)しがたく見逃されてきたという面がある。しかし，現実には，利用者が8千万人に達するとともに音楽会社の売上げが年々減少するという事態を招き，今も減少傾向は止まっていない。

Napster自体は，著作権者の許可なくコピーの頒布を可能にしたことで違法と判定された。しかし，インターネットでの音楽は無料という常識が形成されたことにより，一時ブームとなった音楽のネット配信の事業ができなくなるという事態を招いた。

米国は常に新しいビジネスモデルを求め，次々と新しいアイデアが出てくる社会として世界をリードしてきたが，コンピュータウィルスなども生み出しており，必ずしも良いことばかりではない。今後，インターネットを前提としてビジネスがどのように発展していくか，予断を許さない時代に入りつつある。

常に，新しい技術が登場するとそれに対応する社会問題が発生し，それに対応する法律の整備が行われて常識が形成され，社会の安定が確保されるのが人類の歴史である。法律による違法行為の規制，教育宣伝による常識の形成，及び技術的な保護手段の向上の三位一体の対応が必要と言えよう。

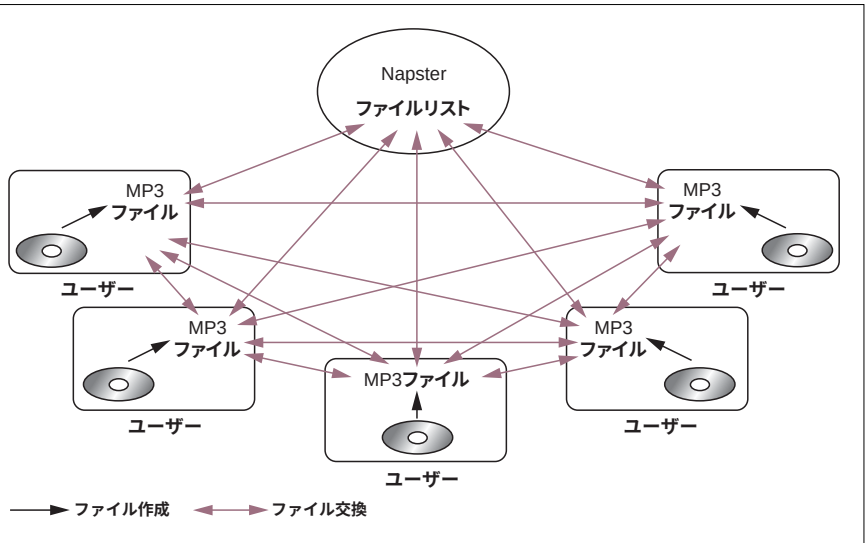

図2．Napsterにおけるファイル交換 — Peer to Peerという新語が生まれたファイル交換システム。
Peer-to-peer file exchange by Napster

(注1)　集中的に処理を行うサーバを設置するのではなく，各ネットワーククライアントが持つ資源(ディスク，プリンタなど)をお互いに共有するようにしたネットワークの形態。
(注2)　Macrovisionは，米国Macrovision Corporationの商標。

DVDのコンテンツ保護

DVDのコンテンツ保護の議論は，96年3月に米国で形成されたCPTWG(Copy Protection Technical Working Group)で始まった。DVDの規格がほぼ決まった段階で，コンテンツ保護をどうするかという議論が，ハリウッドのスタジオから成る映画業界，日本メーカー主体の民生機器業界，及び米国メーカー主体のPC/IT(情報技術)業界の3業界の間で始まった。

各業界ともに，DVDが次世代のパッケージメデイアとして大きく成長すると予想しており，議論は大きく分かれた。最初は，Macrovision(注2)とCGMS(Copy Generation Management System)でよいと言っていた映画業界も，IT業界の反対で徐々に問題を認識し，最終的には，暗号によるスクランブルが歴史上初めて量産機器に導入された。

このときのIT業界の対応は，MacrovisionやCGMSのチェックをフレームごとに行うのは負担が重すぎるというものであったが，最終的に本格的なコンテンツ保護が導入されるとかえって負担が増えることになってしまったのは皮肉と言える。しかし，これにより著作権に関する認識が深まり，インターネットに対する対応も議論の対象になったと言える。

この議論の過程で，コンテンツ保護に対する認識は大きな変化を遂げ，Napsterの登場などもあり，現在はネットワーク社会でのコンテンツ保護が主題になっている。

DVDでは，96年6月にCPTWGにおいて，最初のDVD-Video用のコンテンツ保護が松下電器産業(株)と東芝からCSS(Content Scramble System)として提案され，これが規格化された。

基本的な考え方は，ライセンスにより，秘密鍵を機器製造業者に供給して，この鍵によりDVDディスク上に記録されたコンテンツの暗号を解くというものである。残念ながら，99年に，まったく保

護を怠ったPCでの再生用ソフトウェアが出て，それを見つけたノルウェーの1少年により破られてしまった。このときは，戦略技術の輸出制限により鍵の長さは40ビットに制限されていたために，十分な強度がなかったことも一因である。

しかし，この後で導入されたDVD-Audio用のCPPM（Content Protection for Prerecorded Media）と，DVD-RAM/R（Recordable）/RW（Rewritable），SDカードなどの記録メディア用のCPRM（Content Protection for Recordable Media）では，鍵の長さは56ビットになるとともに，MKB（Media Key Block）の技術が導入され，破られたキーは使用不能にする技術が取り入れられている。

現在のCPUの進歩は，3年で4倍のペースで続いており，3年たつごとに2ビットずつ弱くなる計算であるが，15年はもつと言える。ただ，今後の傾向としては56ビットでは十分でないので，100ビット以上欲しいというのが常識になりつつある。

伝送ライン上のコンテンツ保護

伝送ライン上のコンテンツ保護は，CPTWGのサブグループとして，DTDG（Digital Transmission Discussion Group）が形成されたことに始まり，現在DTCP（Digital Transmission Content Protection）の規格ができて，IEEE1394（米国電気電子技術者協会規格1394），USB（Universal Serial Bus），MOST（Media Oriented System Transport）などのインタフェースに適用され，使われるようになっている。

DTCPはネットワーク上のコンテンツ保護としては最初のものであり，公開鍵を用いた相互認証や，時変鍵の採用など新しい技術が盛り込まれている。一方で，ベースバンド信号の1対1接続の保護として，Intel社がライセンスしているHDCP（High-bandwidth Digital Content Protection）があり，これはDVI（Digital Visual Interface），HDMI（High Definition Multimedia Interface）などに適用されている。一般に，コンテンツ保護の規格は，DVD-Videoなどの規格が別にありそれにかぶせる形で独立に形成されライセンスされてきた。

DTCPにおいても無効化リストと呼ぶ仕組みが用意されており，迂回（うかい）機器となってしまったような機器を無効化し，排除する。

コンテンツ保護システムの構成

コンテンツ保護の技術は，基本となる暗号技術や鍵認証交換などの技術から成り立っているが，それに加えて電子透かし（Watermark）などのアナログ信号の保護がある。暗号は，DVD-VideoではCSS，CPPM/CPRMでは，C2（Cryptomeria Cipher）などの，暗号が使われた。

最近の傾向としては，公開されて安全性の保証された標準暗号に移行しつつある。暗号やコンテンツ保護の構成を公開して，なおかつ強度が保たれるような仕組みでないと使われない傾向になり，秘密は暗号化鍵だけとなっている。標準暗号としては，従来使われていたDES（Digital Encryption Standard）から，最近制定のAES（Advanced Encryption Standard）に移りつつある。鍵認証は公開鍵方式が主流であり，安全性から512ビットなどが用いられている。

更に，前述した鍵の無効化（Revoke）機能のためにMKBが導入されている。MKBは，CPPMでは約30万個の鍵がディスクに格納されているので，この鍵を破るには，56ビットに加えて多数の鍵を解読する必要があり，実効的な鍵の長さが増加している。

パッケージメディアでのコンテンツ保護の簡単化した構成例を**図3**に示す。基本的には，暗号化されたコンテンツが記録されており，暗号化されたコンテンツ鍵が同時にディスクに記録されている。機器はコンテンツの鍵を元に戻す鍵を持っており，これにより鍵を元に戻して，次にその鍵を用いてコンテンツ自体の暗号を解いて元に戻し，再生するものである。

鍵の無効化，機器の無効化を行うことにより，競争相手の企業の製品が動作しなくなるなどの事態が生じると，法律的な問題に発展することも予想される。このため現在では，企業の連合体が別組織を結成し，コンテンツ側の意見を取り入れながら，コンテンツ保護のルールなどにつき議論を行っている。また無効化なども，コンテンツ側の要求で行われるようなルールが形成されている。

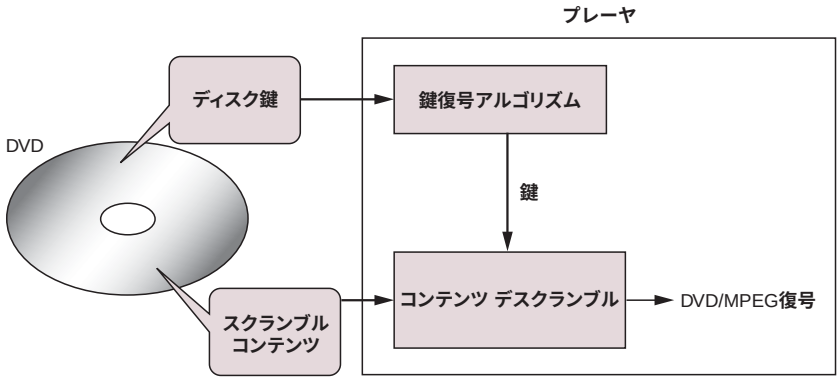

図3．パッケージメデイアのコンテンツ保護―プレーヤが秘密鍵を持ちコンテンツの暗号を解く。
Content protection for package media

■機器製造者が締結する契約（Adopter Agreement）
　■契約書本文：ライセンス条文など
　■遵守規定（Compliance Rules）：機器を作るうえで守らなければならない規定
　　●出力の規制：暗号を解いてそのまま出してはいけない，など
　　●入力の規定：セキュリティのない入力については電子透かしをチェックすること，など
　■強靭性に関する基準規定（Robustness Rules）
　　●秘密の鍵が外から見えてはいけない，など
　　●通常の方法では，セキュリティを破れないようにする，など
　■技術規格

■コンテンツ配給者が締結する契約（Content Participant Agreement）
　■契約書本文：ライセンス条文など
　■遵守規定　：この規格を利用してコンテンツを保護する際のコンテンツ配給側の了解事項に関する規定，など
　■技術規格

図4．コンテンツ保護ライセンスの構成 ― 遵守規定などから構成される。
Content protection system license

コンテンツ保護ライセンスの構成

コンテンツ保護のライセンスの構成を**図4**に示す。

ライセンス契約には，機器製造者が締結する契約（Adopter Agreement）とコンテンツ配給者が締結する契約（Content Participant Agreement）の二つが存在する。

機器製造者が締結する契約は，契約書本文，それに付属する遵守規定（Compliance Rules），外部からの攻撃に対する機器の強靭（きょうじん）性に関する基準規定（Robustness Rules），及び技術規格の四つで構成されている。

一方コンテンツ配給者が締結する契約は，契約書本文，それに付属する遵守規定，及び技術規格の三つで構成されている。

契約を締結した者が守るべきルールの中でも遵守規定がもっとも重要で，例えば，機器製造者が締結する契約には，暗号化されたコンテンツを伝送ラインを通して受信し，暗号を解いたストリームをそのまま出力することを禁止する規定などが含まれている。

DVDビデオでは，従来デジタル出力が認められていなかったが，今年になり，認められる方向に討議がなされており，DTCPとHDCPからの出力が標準的に認められることが期待される。

今後の展望

コンテンツ保護が今後のインターネットビジネスに欠くことができないことは，皮肉にもNapsterの問題が起きて認識されるようになった。

今後，いかにして利用者と著作権者の権利を調整していくかが，技術問題だけではなく，法律と政策の問題ともなっているが，電子透かしの技術がまだ確定しておらず，アナログ信号を使わないわけにはいかない以上，標準的な技術の選定が大きな課題である。

将来のインターネットの世界において，コンテンツ保護の助力により，一般の消費者があまり負担を感じることなく，正常なコンテンツビジネスの環境が形成されることが望まれる。

なお，この特集で使われている主な英文用語について，次ページの**囲み記事**で解説する。

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。
DVD規格の標準化，セキュリティシステムの開発・標準化に従事。電子情報通信学会フェロー。
電気学会，映像情報メディア学会，IEEE会員。
Digital Media Network Co.

河原　潤一
KAWAHARA Junichi
デジタルメディアネットワーク社　法務担当主務。
DVDなどのセキュリティシステムの規格化に従事。
Digital Media Network Co.

この特集で使われている主な英文用語

正式名称	略　語	説　明
4C	4C	東芝，松下電器産業（株），Intel 社，IBM 社の 4 社。DVD や SD メモリカードなど記録メディア用のコンテンツ保護規格を策定した。4C Entity 社を設立して技術ライセンスを行っている。＜http://www.4centity.com/＞
5C	5C	東芝，松下電器産業（株），Intel 社，ソニー（株），（株）日立製作所の 5 社。IEEE1394 などのデジタル伝送路用のコンテンツ保護規格を策定した。DTLA（Digital Transmission Licensing Administrator）社を設立して技術ライセンスを行っている。＜http://www.dtcp.com/＞
Analog Protection System	APS	アナログ映像信号に対するコンテンツ保護システム。DVD では Macrovision 社の技術を採用している。
Conditional Access System	CAS	放送などに用いられる制限視聴方式。日本の BS デジタル放送では B-CAS 方式が使われている。
Cryptomeria Cipher	C2	CPPM，CPRM などで採用されている暗号アルゴリズム。“ 日本の杉 ”の意味で，コンテンツ保護技術の開発に貢献された故杉原氏（松下電器産業（株））にちなんで名づけられた。
Copy Control Information	CCI	コピー制御情報。コンテンツに付加されるコピー不可，1 世代コピー可などの制御情報。
Copy Generation Management System	CGMS	映像用のコピー世代制御方式。アナログ用には CGMS-A，デジタル用には CGMS-D がある。
Content Protection for Prerecorded Media	CPPM	4C が策定した記録済みメディアに対するコンテンツ保護規格。DVD-Audio のコンテンツ保護技術として採用されている。＜http://www.4centity.com/＞
Content Protection for Recordable Media	CPRM	4C が策定した記録メディアに対するコンテンツ保護規格。DVD-RAM/-R/-RW，SD メモリカードなどのコンテンツ保護技術として採用されている。
Content Scramble System	CSS	東芝と松下電器産業（株）が策定した DVD-Video 用のコンテンツ保護規格。＜http://www.dvdcca.org/＞
Copy Protection Technical Working Group	CPTWG	DVD-Video のコンテンツ保護を決めることを目的として設立され，以降コンテンツ保護技術を検討しているボランタリー組織。民生電子機器業界，IT 業界，コンテンツ業界，関連団体などの代表者が一堂に集まっている。＜http://www.cptwg.org/＞
Digital Transmission Content Protection	DTCP	5C が策定したデジタル伝送路に対するコンテンツ保護規格。現在，IEEE1394（米国電気電子技術者協会規格 1394），USB，MOST に対する規格が決まっている。ほかのデジタル伝送路への拡張も検討されている。
DVD	DVD	DVD Forum が策定した規格に基づいて作られる光ディスク。
DVD Copy Control Association	DVD CCA	DVD-Video 用の CSS 規格をライセンスする会社。＜http://www.dvdcca.org/＞
DVD Forum	DVD Forum	DVD 規格の制定及び DVD 規格の普及促進を図る組織。＜http://www.dvdforum.org/＞，＜http://www.dvdforum.gr.jp/＞
Digital Visual Interface	DVI	PC や民生用電子機器とデジタルディスプレイ間のデジタル映像信号インタフェース。Digital Display Working Group（DDWG）が策定。
High-bandwidth Digital Content Protection	HDCP	ベースバンド信号伝送用の一方向伝送インタフェースである DVI 及び HDMI 上でのコンテンツ保護規格。＜http://www.digital-cp.com/＞
High Definition Multimedia Interface	HDMI	DVI に音声信号を付け加えた民生電子機器向け規格。
Macrovision		アナログ映像信号に付加されるコピー防止信号。この技術を提供している会社の名前でもある。
Media Key Block	MKB	CPPM や CPRM で採用されている，不正機器を無効化するために行われる暗号化鍵情報。
Serial Copy Management System	SCMS	デジタルオーディオ用のコピー制御方式。CD，DAT（Digital Audio Taperecorder），MD（MiniDisc）などの登場で策定された。映像用の CGMS と同じコピー世代管理を行う。
SD Card Association	SDA	東芝，松下電器産業（株），SanDisk 社の 3 社が，次世代メモリカードとして共同開発した SD メモリカードの普及推進のために設立した組織。＜http://www.sdcard.org/＞
SD Memory Card		SD Card Association が推進する次世代メモリカード。コンテンツの著作権保護機構を備えた安全な記憶メディア。＜http://www.toshiba.co.jp/sd-life/＞
Secure Digital Music Initiative	SDMI	音楽配信のコンテンツ保護規格を決めるために作られた組織。ポータブルオーディオ機器におけるコンテンツ保護仕様を決めた。
Tamper Resistant Software	TRS	解読，改ざんの防止策を施したソフトウェア。
World Intellectual Property Organization	WIPO	世界著作権機構。＜http://www.wipo.org/＞
Watermark	WM	電子透かし。人間の感覚では検知されないような形でコンテンツの中に埋め込まれた信号。音楽用と映像用などがある。アナログ，デジタルなどコンテンツの形態にかかわらず，埋め込んだ情報を保持することが可能であるため，コンテンツ保護技術の一つとして使われる。