

# 著作権管理技術とICタグ

審査第四部情報処理 審査官

原 秀人

審査第四部画像処理 審査官

梅本 達雄

## はじめに

近年、ブロードバンドや携帯電話の普及により、ネットワーク環境は社会基盤としてなくてはならないものとなってきています。ネットワーク環境の整備は、電子メールやWWWなどの人間同士のコミュニケーションに大きな変化をもたらしましたが、流通にも大きな影響を与えはじめています。

例えば、あらゆる商品にICタグをつけ、商品にリーダを近づけるだけでその商品の個々の情報をネットワークからアクセスできるシステムや、オンライン音楽サービスに代表されるデジタルコンテンツのオンライン販売はすでに現実のものとなってきています。

今回は、このICタグと、デジタルコンテンツの流通には欠かせない著作権管理技術について、ご紹介させていただきます。

## 1. ICタグとは

ICタグとは、無線を用いてその物品を識別するために物品に付される装置のことで、RFID、電子タグなどとも呼ばれています。

多くのICタグは、無線回路と識別子を記録するROM等で構成されるICチップとアンテナを接合したインレットと呼ばれるシート状の小片の形をしていますが、ICチップにアンテナを内蔵する種類のタグの中には紙にすきこ

めるほど小さく薄いものも存在します。

商品にコードを付すものとして現在バーコードがひろく利用されていますが、ICタグは、バーコードと比べて記録できる情報量が多く、商品コードだけでなく商品ひとつひとつを識別するコードを記録することができます。さらに無線技術を利用するため、商品に密着させなくともタグ情報が読みとれるという特徴もあります。そのためICタグが安価になると、より効率的で細かい流通管理が実現できると期待されています。

また、近年食品の安全性に対して消費者の関心が高まっているおり、ICタグを利用することによって、原材料や流通経路の把握が可能になると期待されています（食品トレーサビリティ）。

## 2. ICタグの歴史

民生用のICタグが登場したのは1980年中頃だといわれています。初期のICタグは主に半導体の製造技術の問題から、消費電力の小さい高周波回路を持ったICチップの設計・製造ができなかったため、100k~150kHzといった低い周波数帯を用いていました。

1990年代の後半になると、UHF帯（860M~960MHz）やGHz帯といった高周波用のICタグが登場してきました。特にUHF帯は通信距離の長さなどから、流通過程への応用が期待されています。

最近になってICタグが注目されているのは、2つの大きな要因があると考えられます。

ひとつは、ICタグの製造コストと大きさが劇的に小さくなったことです。

初期のICタグは非接触ICカードから派生したものであったため、サイズやコストの面からすべての物品に付することは現実的ではなかったのですが、最近になって登場した高周波用のICタグは非常に低価格で製造可能になってきたため、ICタグをバーコードの代替としてすべての商品に付加することが現実味を帯びてきました。

米国ではタグ1つあたり5セント（約5円）で製造できればそのコストは吸収できると試算しており、既にそのめどはたつたと判断しているようです。DoD（米国防総省）や小売最大手のWal-Martが2005年1月から本格的に

運用を開始するとしており、そのための次世代ICタグの標準化作業があわただしくなっています。

もうひとつは、インターネットや携帯通信が普及したことによって、タグの情報をネットワーク上のサーバで管理でき、それを常時アクセスできるようになってきたことです。その結果、タグ自身が保持する情報はIDのみでよくなったため、タグをさらに小型化・低コスト化できるようになりました。

また、タグが付されている個々の商品の情報を消費者がいつでもどこでも参照できるようになったため、食品トレーサビリティなどの新たな応用の可能性がでてきました。

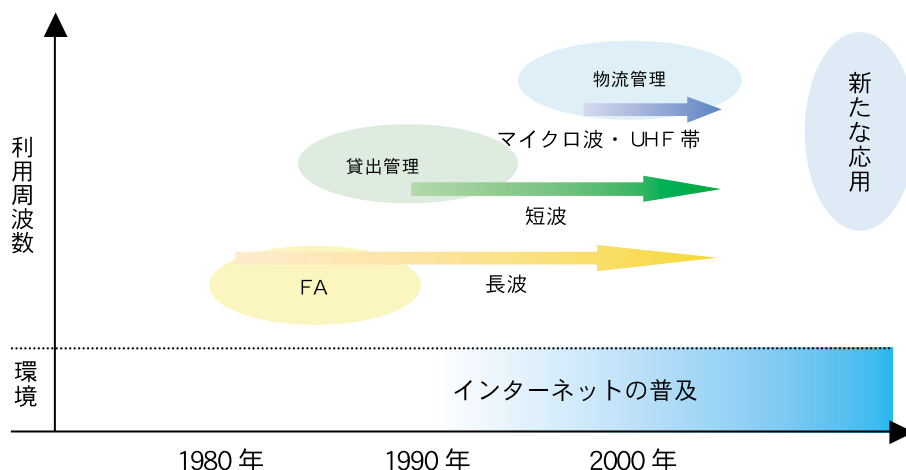


図1 ICタグの発展

### 3. ICタグの種類

ICタグは、タグへの電力供給方式、利用する周波数帯や保持するデータの種類などによって分類することができます。

#### 電力供給方式

ICタグから情報を読み取るためには、タグ内部のICチップ

を駆動させるための電力を必要としますが、ICタグはこの電力の供給方式によって、リーダ/ライターのからの電磁波より電力を得るパッシブ型、内蔵電池により通信を行うアクティブ型及び内蔵電池を有するが通信は基本的にパッシブ型と同様のセミパッシブ型に分けられます。内蔵電池を有するものは通信時以外も動作可能なため、センサーを内蔵して温度などの履歴を記録することができます。このうち、安価に製造できるパッシブ型が注目を集めています。

表 1 電源供給の方式によるタグの分類

	給電方式	
パッシブ型	アンテナ	電池を内蔵しないため小型で安価 通信距離は比較的短
セミパッシブ型	アンテナ+内蔵電池	通信中以外でも動作可能であるため、商品の温度履歴等も記録できる
アクティブ型	内蔵電池	比較的高価

### データの格納形態

ICタグをデータ格納形態で分類すると、IDのみをもつ識別子型と、賞味期限等の商品の独自情報を記録可能なデータキャリア型とに分けられます。

識別子型のICタグはIDを必ず持っており、リーダーで読

み取ったIDをサーバに問い合わせることで、IDに対応する「物」の情報にアクセスします（図2）。そのため、この形式のICタグは「ネットワーク型」とも呼ばれています。現在注目されているのもこの識別子型です。

表2 タグが保持するデータの種類

格納形態	特徴	デメリット
識別子型	IDのみ	頻繁なサーバ問い合わせが必要
データキャリア型	ID+データ	記憶域の分、コスト高

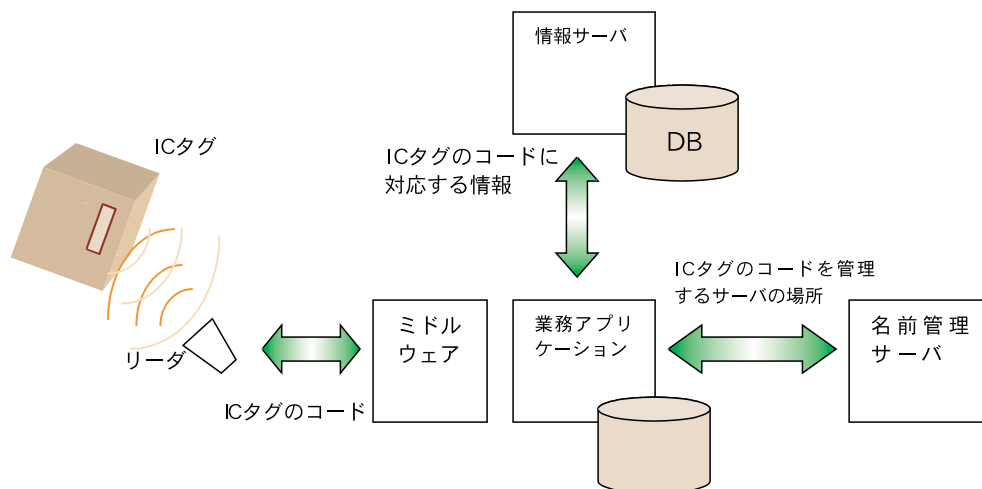


図2 ICタグを用いた「物」の情報へのアクセス（識別子型）

### 利用する周波数

ICタグは電磁波を用いて通信するため、利用できる帯域は各国の電波行政に大きく影響されます。現在利用可能な主な周波数帯の特徴を表3にまとめておきます。

#### ～135kHz帯

もっとも古くから利用されている帯域です。波長が長いので電波が回り込みやすく箱状の物品の内側にも付けられるメリットがある反面、蛍光灯などの生活ノイズに弱いというデメリットがあります。

表3 ICタグで利用される主な周波数帯

	～135kHz帯	13.56MHz帯	UHF帯	2.45GHz帯
通信距離	～1m	～80cm	3～8m	～2m
リーダーからの通信方式	電磁誘導方式	電磁誘導方式	マイクロ波方式	マイクロ波方式
他無線の干渉	なし	なし	なし	無線LAN
水分の影響	比較的小さい	比較的小さい	比較的大きい	大きい
各国の法規制	なし	なし	日本では×(950MHz帯の利用が検討)	なし
主なベンダー	Philips	Infineon Tech.	Alien Tech.	日立

#### 13.56MHz帯

世界的に規制が少なく、現在広く利用されている帯域です。電磁誘導方式により通信します。この帯域を利用するタグは通信可能距離が短いのですが、通信距離の短さは電波がもれない、ということでもあるので一概に欠点とはいえません。135kHz帯よりもタグを薄く作れるため、圖書の管理などに利用されています。この帯域は「Suica」などで知られる非接触型ICカード「FelCa」でも利用されています。

#### UHF (860-960MHz)帯

UHF以上の周波数では、電波方式により通信を行います。米国では高い出力で使うことができます。日本国内では現在携帯電話への影響が心配されるため利用できませんが、950MHz帯については将来利用可能になる予定です。通信距離が長く、2.45GHz帯に比べて電波が回り込むので読み取りが容易です。ただし、マイクロ波に比べて波長が長いので、効率よく通信するには十数cmのアンテナが必要となります。現在、Wal-Mart等で利用が検討されているのがこの帯域です。

#### 2.45GHz帯

UHF帯と異なり、現時点での日本でも利用が可能な帯域です。6cm程度のアンテナですむため、さまざまな物品にタグを付けることができます。水分に弱いこと、同じ周波数帯を利用する無線LANと干渉してしまうことが欠点です。また直進性が強いことも読み取りを困難にしています。

## 4. ICタグを支える技術

ICタグは非接触型のICカードと同じような技術の上に成り立っていますが、そのなかでもICタグに特徴的な技術としては以下のようなものがあげられます。

#### 無線インターフェイス

##### 電力供給

パッシブ型のICタグへの電力供給は、13.56MHz以下の周波数では電磁誘導方式が用いられ、それより高い周波数帯ではマイクロ波方式が用いられています。

電磁誘導方式：タグのコイルとリーダのアンテナコイルを磁束結合させてエネルギー・信号を伝達する方式です。アンテナがコイル状になっているのが特徴です。

トランスによる電力伝達と同じ原理を利用しています。電磁誘導方式は電波方式に比べてエネルギーを効率的に伝達できるので、早くから利用されてきました。磁界は距離による減衰が大きいため、高い周波数では通信距離を長くとることはできません。

マイクロ波方式：リーダからの電波エネルギーを電力にかえる方式です。電磁誘導方式より遠方まで通信できるのが特徴です。一般的なアンテナの長さは、効率良く電波を送受信するため半波長分となっています。

#### アンチコリジョン

物流管理などでICタグを利用する場合、リーダが同時に複数のタグと通信することがしばしばおこります。その際、複数のタグが同じチャンネル（通信路）を同時に利用するとコリジョン（衝突）が発生し、正しくデータが送られなくなってしまいます。アンチコリジョンの方式としては、以下のようなものがよく知られています。

Aloha：タグが送信する際に他のタグが通信していないか確認して、どのタグも通信していなければデータを送信する方式です。たまたま同時に別のタグも送信を初めてしまった場合は、しばらく待ってもう一度送信を試みます。

Binary Tree：リーダが各タグに割り当てられたIDを上から1bitずつ確認していく方式です。例えば、最初に上位1bitが'0'のタグを呼びます。該当するタグが複数ある場合は同時応答によってコリジョンが発生するので、次に上位2bitが'00'のタグを呼び、ということを繰り返していくことによって最終的に通信するタグが決めていきます。

周波数ホッピング：タグからリーダへの応答チャンネルを複数用意し、タグに割り振られたIDから得られる疑似乱数に基づいて、利用するチャンネルを一定期間毎に切り替えながらを通信する方式です。

#### 製造技術

物品一つ一つに付するICタグでは製造コストが非常に重要になります。例えばICチップをアンテナ基材に実装する方式には以下のようなものがあります。

ピックアンドブレース法：ダイシングしたICチップをロボットアームによりアンテナ基材に配置し、加圧圧着する方式で、現在のICタグ製造方法の主流です。

FSA法：米Alien Technologiesのパッシブ型タグの量産

技術Fluidic Self Assembly (FSA法)は、低コストでタグを生産する方式の一つとして注目されています。流体内で台形状のICチップを基材に流しこむことで組み立てるため、1個あたり5セントで製造可能となる、と同社では主張しています。

Connect法：Philips Semiconductorが提唱している、ICチップを直接アンテナ基板に実装せず、あらかじめConnectと呼ばれるICチップよりも大きな金属板に張り付けておき、この金属板をアンテナ基材に実装する方法です。直接ICチップをアンテナ実装するよりも精度が要求されないため、高速に生産ができます。

### 情報システム

ICタグのシステム (RFID) は、タグやリーダ/ライタの他に、リーダが読み取ったICタグのコードから、そのコードに対応する「物」に関連するデータがどのサーバに格納されているのかを参照するためのネットワーク上の名前管理サーバ (ONS等とも呼ばれています) とコードに対応する「物」に関連する情報を管理する情報サーバ

を有しています。

名前管理サーバは、インターネットにおいてURLからホームページにあるサーバのアドレスを導き出すDNSサーバと同じような仕組みで動作しています。

一方、情報サーバは既存のデータベースに納められている商品情報を、ICタグのシステムで利用できるようにデータ変換するゲートウェイの機能を持っていることもあります。

## 5. ICタグの国際標準

ISO (国際標準化機構) では、「物」と共に使用される分野のICタグの無線インターフェイスに関する規格をISO/IEC 18000に分類しています。主な周波数帯の規格を表4に示します。

またタグのIDに関してはISO/IEC 15963で規定されています。

表4 ICタグの国際標準

規格	利用周波数帯		タグからの通信速度	備考
ISO / IEC 18000-3	13.56MHz	モード1	約26 / 6.6Kbps	ICカードの規格ISO15693にアンチコリジョンを加えたもの
		モード2	106Kbps × 8	モード1とは互換性なし
ISO / IEC 18000-4	2.45GHz	モード1	20 ~ 40Kbps	電池無
		モード2	384Kbps	電池付
ISO / IEC 18000-6	UHF	タイプA	40Kbps	電池無 / 電池付の両方をサポート EPCGlobalの規格とは互換性なし
		タイプB		

## 6. ICタグの標準化組織とその規格

ICタグの代表的な標準化団体としては、MITのAuto-ID Centerから標準化の作業を引き継いだEPCGlobalとTRONで知られる東京大学の坂村教授が中心となって活動しているユビキタスIDセンターがひろく知られています。今年に入ってから、経済産業省が「響プロジェクト」を立ち上げています。

### 5.1 EPCGlobal

EPCGlobalは、バーコードの標準化で知られるEAN InternationalとUCC (Uniform Code Council, Inc) の共同出資で2003年に設立された団体です。グローバルでユニークなEPC (Electric Product Code) を発行 / 管理するとともに、RFID、EPC、ネットワークからなるEPCネットワークの国際標準化を実施しています。

## EPCGlobalの規格

米国では、UHF(915MHz帯)の利用が可能であるため、EPCGlobalでは、通信距離が長く、無線LANとの干渉がないこの帯域を利用した規格が中心となっています。

コードは現在普及しているバーコードのEANコード(日本ではJANメーカーコード)+商品番号+シリアル

ナンバーとなっており、コードのサイズは64bitまたは96bitが基本となっています。

また、消費者のプライバシー保護に配慮して、保持している情報を無効にする機能を提供しています。

EPCGlobalではICタグ製品を以下のように分類しています。

表5 EPCGlobalのタグ製品の分類

EPC Class	定義	データ記録方式
Class 0	“リードオンリー”パッシブ型タグ	半導体製造行程で記録(RO型)
Class 1	“ライトワンス”パッシブ型タグ	一度のみ書き込み可(WORM型)
Class 2	“リライタブル”パッシブ型タグ	何度でも書き直し可能(RW型)
Class 3	セミパッシブ型タグ	
Class 4	アクティブ型タグ	
Class 5	リーダー	-

現在、UHF用に使われている無線インターフェイスは、バージョン1の「Class 0」と「Class 1」と呼ばれるものです。これらの規格には互換性がなく、同周波数帯の国際規格とも互換性がありません。そこで現在EPCGlobalでは、両方の規格のタグを読みとれる次世代規格Class1Gen2(UHFジェネレーション2とも呼ばれています)を策定して、国際規格として申請する予定です。

次世代規格の候補としては、米Matrix(現Symbol Technologies)と米Alien Technologiesが推す「Freedom案」と、米Intermec、蘭Philips Semiconductors、米TI等が推す「Global案」の2つの案が最終的に残りました。非差別かつ合理的なライセンスを主張する「Global案」陣営のIntermecが特許フリーを主張する「Freedom案」陣営のMatrixの特許侵害を訴えるなど、両陣営の対立が表面化したため、規格統一が危ぶまれましたが、その後EPCGlobalが知的財産権の問題をひとまず脇に置いたことで両陣営は歩み寄りをみせ、2004年6月に2陣営間の意見をとり入れた規格案が成立しています。

## IPポリシー

EPCGlobalでは標準化にあたって同団体への参加企業に対して、原則ロイヤリティーフリー方針を義務づけていましたが、これに対して、有力なベンダーであるIntermec等「Global案」陣営が難色を示したことから、現在、標準を確立するプロセスから知的所有権問題はいったん除かれています。

## 5.2 ユビキタスIDセンター

ユビキタスIDセンターはTRONで知られる東京大学の坂村健教授が中心となって進めているICタグ等の標準化団体です。

EPCGlobalが流通過程での商品の紛失(シュリンケージ)防止を重視しているのに対し、ユビキタスIDセンターでは食品トレーサビリティを重視しており、ICタグが高価な現段階でICタグをバーコードと置き換えることにそれほど積極的ではないようです。

## ユビキタスIDセンターの規格

ユビキタスIDセンターで用いるタグはucodeと呼ばれる128bitのコードを用いて「物」を識別します。ユビキタスIDセンターではコードの上位12bitをコード体系の識別子として管理し、残りの部分の管理は各コード体系の管理組織に任せています。

タグ(ucodeタグ)はその「物」に関する情報を格納しますが、現在では記憶容量等の制約があるため、タグにはモノを識別するIDコードを格納し、容量の範囲内で付加的な属性情報を格納しています。タグに格納できない情報を、ネットワーク上のデータベースに格納する点はEPCGlobalと同様です。

タグには、バーコード、RFID、アクティブチップなどが含まれており、ユビキタスIDセンターでは、主にセキュリティの観点から以下のように分類しています。

表6 コピキタスIDセンターのタグの分類

Class	定義	認定された標準IDタグ
Class 0: 光学的IDタグ	光学読み取り可能なタグ(バーコード)	ミューチップ(日立)
Class 1: 下位RFIDタグ	工場焼きこみでコードの改変不能なタグ	T-Junction(凸版印刷)
Class 2: 上位RFIDタグ	簡易認証方式による同定防止プロトコルをもつタグ	
Class 5: 下位アクティブタグ	認証を通過した状態で書き込みが可能なタグ	
Class 6: 上位アクティブタグ	公開鍵暗号認証通信機能を有するタグ	Pico T-Engine

### 5.3 響プロジェクト

「響プロジェクト」は、2004年にスタートした、2年で電子タグを1個5円以下と低価格にすることを目標とした経済産業省のプロジェクトです。関連企業約100社を集めてコンソーシアムを結成し、ICチップとアンテナを低コストに実装する技術などを開発することを目標とし、現在、低価格を実現するため第三者の特許にふれない規格の可能性の調査を行っています。

公募の結果、2004年7月に日立製作所がICチップの開発から加工までの全行程の責任を持つ中核企業として採用されました。他に大日本印刷、凸版印刷、NECが協力をすることになっています。

#### 響プロジェクトの規格

響プロジェクトでは、タグのコードはEPCGlobalが規格化したEPCがデファクト・スタンダードであるとし、これを採用しています。

一方無線インターフェイスに関しては、今後日本でも認可される予定のUHF帯を利用したものを検討しています。具体的には、タグのメモリ容量は512bit以上であることやメモリの書換えが可能(10万回程度)である等の条件を満たすことが要求されています。また、EPCGlobalの次期標準規格「EPCGlobal Class1Gen2(予定)」との相互接続性も求められています。

#### 響プロジェクトのIPポリシー

響プロジェクトでは、同プロジェクトの成果及びその基礎となる知的財産権の扱いについて、

- (1) 非差別かつ合理的なライセンス料金で、他の製造企業に使用許諾すること
- (2) 電子タグ及びリーダーライターのユーザー企業にはライセンス料金を求めないこと

の2つの条件を満たす限りにおいて、実施企業に帰属させる、としています。

## 7. 主なICタグベンダー

EPCGlobal参加企業の中では、米ALIEN Technologyや2004年7月に米Symbol Technologiesに買収されたMatrixes等のベンチャー企業がよく知られています。その他、蘭Philips Semiconductorsや米Texas InstrumentsはUHF帯に限らず、幅広くICタグを製造しています。日本の企業ではミューチップを製造している日立製作所が有名です。

表7にUHFや2.45GHz帯用ICタグで現在注目されている主なベンダーを挙げます。

## 8. ICタグの課題

さまざまな面で期待されているICタグですが、いくつかの課題も指摘されています。

ひとつはコストです。将来的にはタグ一つあたり5円程度になるといわれていますが、現状ではまだまだ高価です。また、リーダーやサーバなどのインフラの置き換えにも莫大な費用がかかるといわれています。

もう一つはプライバシー問題です。商品に付いているICタグにより個人の行動が常に監視される、ということがおこる可能性があるためです。欧米ではアパレルメーカーのBenettonのように、消費者団体の不買運動がおこったため、ICタグの導入を再検討させられた例もいくつかでてきています。EPCGlobalでは商品購入時にICタグを

表7 ICタグの主なベンダー

企業名	EPCGlobalへの規格提案	特徴
ALIEN Technology (米)	Freedom案	UHF、2.45GHz帯に特化 米Gilletteや米Wal-Martと実証実験 タグの量産技術FSA法に関する特許を保有
Symbol Technologies (米)		EPCGlobal規格や独自規格「Class 0+」の製品を製造 2004年7月にMatrics (米) を買収
Intermec (米)	Global案	Matricsを特許侵害で提訴 UHF帯や2.45GHz帯のISO規格に同社の提案が採用 ISOの規格には同社の特許が最も多く関係 (65件)
Philips (蘭) TI (米)		UHF帯のISO規格に同社らの提案が採用
日立製作所		0.4mm角のミューチップ ・印刷アンテナインレットや超音波接合技術等のICタグ製造技術を保有 ・愛知万博のチケットに採用 「響プロジェクト」の中核企業
トッパン・フォームズ/FEC		複数の周波数帯に対応したMMチップを開発 マレーシア政府が採用を表明

無効化できるとしてはありますが、この問題に関してはまだ検討の余地がありそうです。

## 9. 著作権管理技術とは

最近、音楽や画像などの著作物のデジタル化が進んでいます。このようなデジタル化された著作物は何度コピーしても、どんな遠距離を送受信しても品質が劣化しないため、インターネットの普及やパソコンの高速・大容量化にともなって、著作者の許諾を得ない違法な配布・交換などが増えており、違法コピーやファイル交換ソフトを使った違法なコンテンツ交換が問題となっています。

このことは、今年の5月27日に発表された知的財産推進計画2004においても重視されていて、「映画や音楽などのファイル交換ソフトを用いた著作権侵害が横行している…状況にかんがみ、国内においても取締りを一層強化する必要がある。」としています。ファイル交換ソフトに関して話題となった事例を表8に示します。

このような著作権侵害に対抗するために、コンテンツの流通・再生に制限を加えたり違法な流通を検出したりする著作権管理技術が注目を集めています。知的財産推

進計画2004でも、「権利者がコンテンツから適切に利益の還元を受けることが可能となる技術の実用化を促進するため、2004年も引き続き、電子透かし、権利管理システム (DRM Digital Rights Management)、課金システムなどの技術開発や普及を促進するとともに、安全かつ多様な流通を実現するためのメタデータ (属性情報) フォーマットの標準化を支援する」としており、著作権管理技術の開発への期待が高まっています。

このように、著作権侵害に対して、法的な保護と技術的な保護の両面から保護していく必要がありますが、ここでは、技術的保護の著作権管理技術について説明していきます。

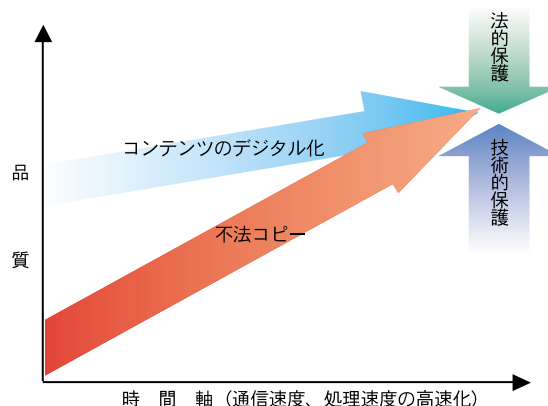


図3 コンテンツのデジタル化と不法コピー

表8 ファイル交換ソフトで著作権が問題になった事例

ファイル交換ソフト	時期	内容
Napster	1999年	Napster登場。
	2001年	米国の裁判所がNapsterの著作権侵害を認め、サービス停止。
Gnutella	2000年3月	Nullsoft社のJustin FrankelとTom Pepperにより、同社に黙って開発したもので、AOL社のWebサイトで公開されたが、同社によって24時間と経たないうちに公開停止となった。
WinMX	2001年11月28日	Photoshop等を公開したさいたま市専門学校生(20)と他1名が逮捕。
	2001年12月7日	JASRAC及びレコード会社2社からも刑事告訴。
	2002年3月26日	京都裁判所が罰金40万円の略式命令。
Winny	2004年2月26日	ネットワークセキュリティ専門企業ネットエージェントがWinnyの暗号を解明。
	2004年5月10日	Winny開発者金子勇容疑者、著作権違反幫助の疑いで逮捕。

## 10. コンテンツの種類と保護方式の比較

コンテンツの著作権は、適切に管理されると共に、その内容に基づいてコンテンツが保護される必要があります。そのための技術としては、メディアの種類、流通形態やビジネスモデル等に応じて、多種多様な技術が存在しています。

ここでは、それら技術をいくつかの観点に分けて見ていきたいと思います。

### セキュリティの程度による分類

不正利用に対するセキュリティの程度によって、2つの技術に分けることができます。1つは、利用する権利を有していなければ利用できないようにする技術で、暗号化に代表され、不正防止技術と呼ばれています。もう1つは、不正が行われたことを検出する技術で、電子透かしに代表され、不正抑止技術と呼ばれています。

### 流通形態による分類

著作権管理の方法は、流通の形態によって分類すると

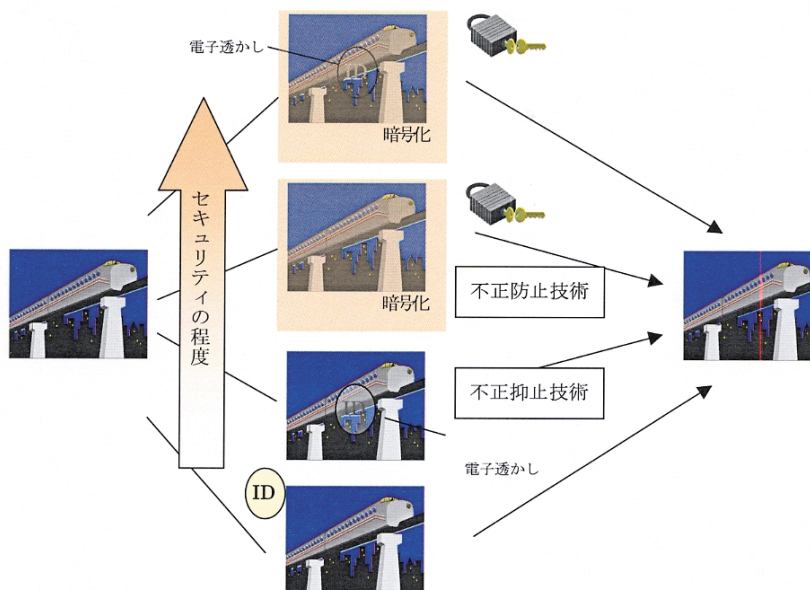


図4 セキュリティの程度による著作権保護技術の種類

表9のようになります。基本的には、ネットワークによる双方向通信が可能であるかどうかで分かります。記録メディアであればネットワークによる相互認証はあまり用いられないし、ネットワークを用いても、放送（単方向）やダウンロード方式の場合は、コンテンツを

記録してから再生制御を行うものが多いですから、記録メディアの制御と似ています。それに対してストリーミング形式は、積極的にネットワークを介して通信ができ、ネットワークを介して認証、再生、課金制御が行われます。

表9 流通形態による著作権管理方法の分類

流通形態分類		特徴
パッケージ	記録メディア	暗号化されたコンテンツと制御情報を格納。 再生機器による制御やネットワークによる認証に基づき復号。 コピー制御情報（CCI）等を電子透かし技術により埋め込む。
ネットワーク	放送	単方向伝達であり、記録メディアと同様。 デジタル放送ではICカードを受信機に挿入し、放送波の制御情報と組み合わせて認証するCAS（Conditional Access System）と呼ぶ技術が使われている。
	ダウンロード	ダウンロードする段階ではストリーミングと同様な認証が行えるが、蓄積された後は、記録メディアと同様。
	ストリーミング	利用者認証と共に利用方法に応じた課金制御や利用状況把握が可能。

## II. 基盤技術

### \* 暗号

暗号系は図5のように表わすことができます。暗号化鍵と平文を入力として暗号文を出力する暗号化処理を行

い、復号化鍵と暗号文を入力として平文を出力する復号化処理を行います。

暗号化鍵と復号化鍵が同一である暗号と共通鍵暗号と暗号化鍵と復号化鍵が異なる公開鍵暗号があります。公開鍵から秘密鍵を求めるためには非現実的な膨大な計算を要するという計算量的に困難な問題に基づいています。

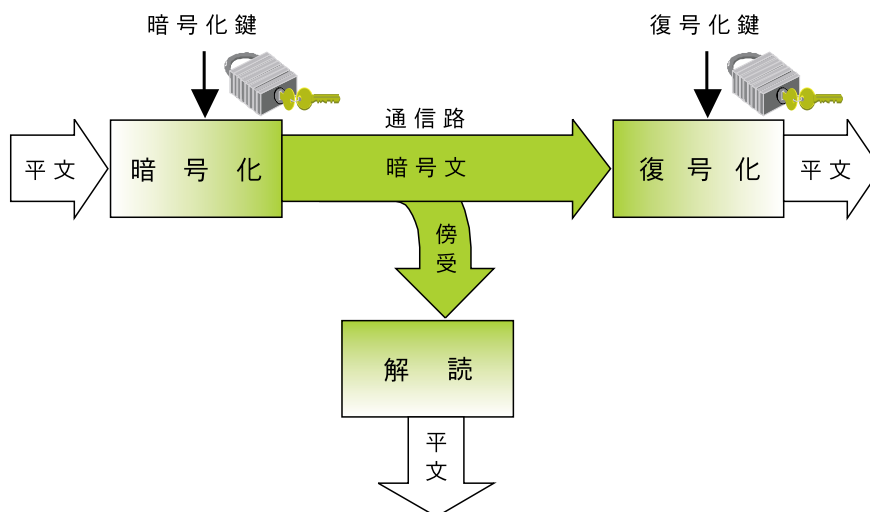


図5 暗号系

**\* 認証**

クライアントAから見てサーバBが正しいか確認しておかないと不正なクライアントを利用して不正が行われ

る危険性があります。そこで、認証が行われます。図6に、認証の例を図示しております。

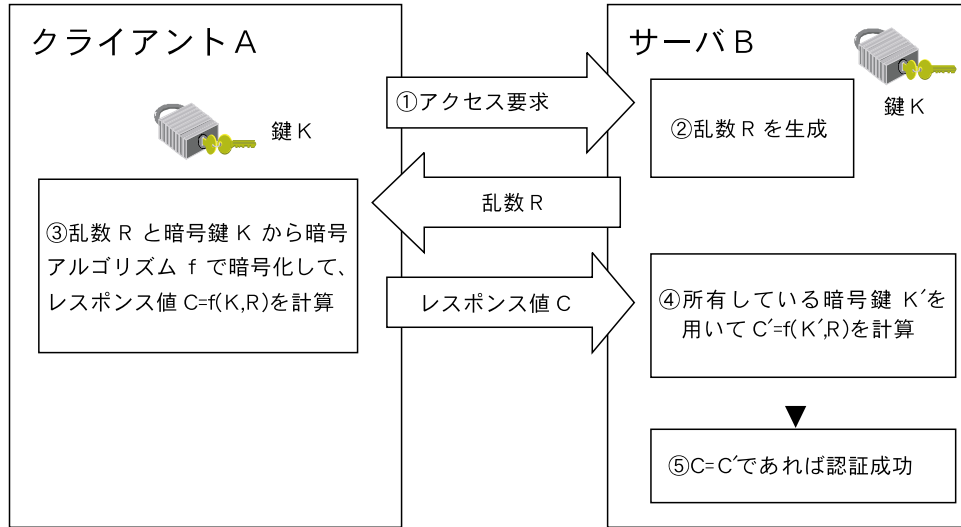


図6 認証方式の例

**\* コンテンツID**

コンテンツIDとは、音声や動画などのデジタルコンテンツ毎に付与されるユニークなIDで、これにより、著作権を判別することができます。コンテンツIDは電子透かし技術により人間には見えない/聞こえないようにコンテンツに埋め込まれます。

コンテンツID発行機関についてはまだ全世界的な統一

が取れていませんが、cIDfが標準化に向けて活動を行っています。cIDfが仕様書（第2.0版）で定めるコンテンツIDの構成を表10に示します。またコンテンツIDの階層を表11に示します。実際にコンテンツと共に流通するのは、DCDであり、ユニークコードについては、電子透かし等によりコンテンツに埋め込まれます。その他の情報は、ID管理センターで管理されることとなります。

表10 コンテンツIDの構成

項目	説明
IDセンタ管理番号 (cid/ユニークコード)	コンテンツを特定するユニークな番号 コンテンツID申請に基づき発行時に設定される
コンテンツ属性	コンテンツ内容・種別等を表す情報
権利属性	コンテンツに関わる権利の情報
権利運用属性	権利の委託・委任・譲渡に関する情報
流通属性	コンテンツ流通時に参照される情報
分配属性	
自由領域	任意の情報
システム制御	システム（ID管理センタや端末機器・ソフト）が使う情報

表11 コンテンツIDの階層

コンテンツID	ID管理センターのIPR-DBに保存される。(メタデータの全体集合) ユニークコードとコンテンツ属性、権利属性、権利運用属性、流通属性・分配属性、自由領域、システム制御情報よりなる。
DCD ( Distributed Content Descriptor )	IDセンタで管理されるコンテンツIDフルセットの内、例えばコンテンツ更新を許さない重要な項目等についてコンテンツと一緒に流通させるもの。Embedding ModelとSeparate Modelがあり前者は、DCD-EFという共通フォーマットで表現され、後者は、XML形式で表現される。
ユニークコード (IDセンター管理番号)	コンテンツID登録時にコンテンツIDセンタで付与される登録毎にユニークな番号。

\* 電子透かし

電子透かしは、画像データなどの冗長性に着目し、コンテンツに人には知覚できないデータを埋め込むことによって、著作権等の情報を認証し、不正な利用があった場合は、不正利用者を特定するような用途や不正コピーを抑制する効果が期待されています。表12に電子透かしの用途と利用方法を示します。

電子透かしは、大きく分けて、実データ(量子化誤差、

下位ビット)へ埋め込む方法、周波数変換して埋め込む方法があります。その他にも各種圧縮規格の特徴を利用して埋め込む方法、統計的偏りを生じさせる方法や、コンテンツの種類の特徴を利用した埋め込み方法が提案されています。

電子透かし技術を利用してコンテンツに対して著作権情報などを埋め込んでおくと、コンテンツに改竄が加えられた場合でも改竄を検出することができます。

表12 電子透かしの用途と利用方法

用途	情報	埋込情報の利用方法
機器制御	レコーダ/プレイヤーの制御コード (CCI: Copy Control Information)	CD, DVDなどのコピー制限、海賊版再生停止
著作権の確認	著作権情報	コンテンツに対する著作権の確認、主張
不正流通元の特定	配布先のID	不正流通(コピー)元を特定し、不当行為の停止、抑止力
流通管理	コンテンツのID	流通監視、課金、バーコード機能

\* 不正利用検出

電子透かし等の技術を用いてコンテンツにIDを埋め込み、流通させ、不正利用検出システムにより、正規配布先のURLと埋め込んだIDとの対応関係をチェックするこ

とにより不正利用を検出することができます。コンテンツ不正利用検出方式について、表13にまとめました。また、表13のコンテンツ不正利用検出方式の概略図を図7に示します。

表13 コンテンツ不正利用検出方式の種類

種類	概要	特徴
探索ロボット型	透かし読み取り機能を持つ探索ロボットにより、Webサイトのページに含まれているコンテンツ(音声・画像など)をトップダウン的に探索する。	探索キーワードを指定し範囲をある程度限定すれば探索時間は数時間。
特定ネットワーク監視型	特定ノードのゲートウェイやサーバに透かし読み取りフィルタを入れて通過するコンテンツを全てチェックする。	探索範囲を限定すれば探索制度の点では最も良い。
利用者協力型	利用者のブラウザのダウンロードモジュールに透かし読み取りツールを予めプラグインしておき、ダウンロードしたコンテンツのIDをアクセスサイトのURLをコンテンツID管理センタに通知し、チェックする。	利用者の協力が取り付けられればネットワーク負荷がなく最も良い。

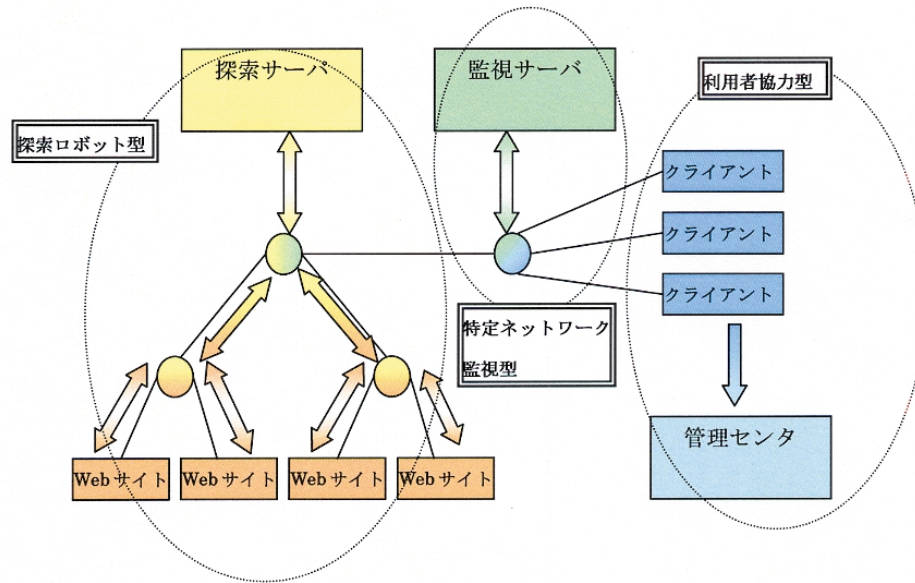


図7 コンテンツ不正利用検出方式

**\* カプセル化**

カプセル化されたコンテンツは、それ自体の複製は容易であるが正規の手続きにより復号しなければ利用できません。

図8にカプセル化コンテンツの構造を示します。

カプセル化されたコンテンツの動作は以下のように行われます。

- ①カプセル化されたコンテンツが、参照プログラムによってロードされます。
- ②参照プログラムは、カプセル内のコンテンツ制御情報を解析することにより処理手順の情報を得ます。
- ③処理手順に従い、コンテンツ管理プログラムや、コン

テンツ表現プログラムを実行します。

- ④コンテンツ管理プログラムは、コンテンツ管理情報に従い、利用条件の判断等を行います。
- ⑤コンテンツ表現プログラムでは、コンテンツ表現情報を参照してコンテンツデータを処理することによりコンテンツを再生します。

**\* 著作権管理システム**

このような各種基盤技術を用いて、著作権管理システムが構成されます。図9に、著作権管理システムの一例を示します。

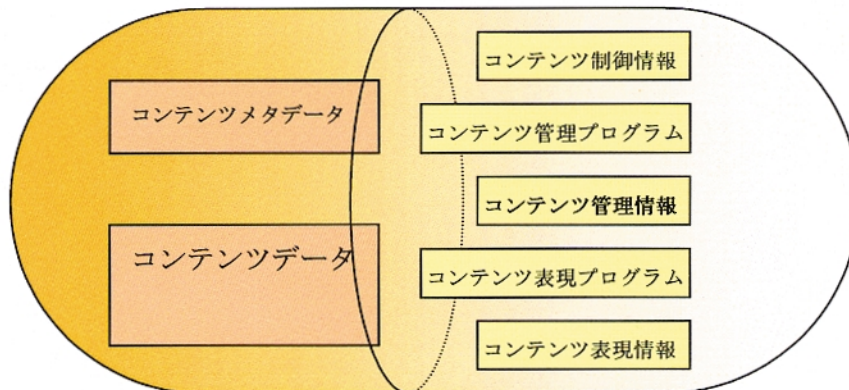


図8 カプセル化コンテンツの構造

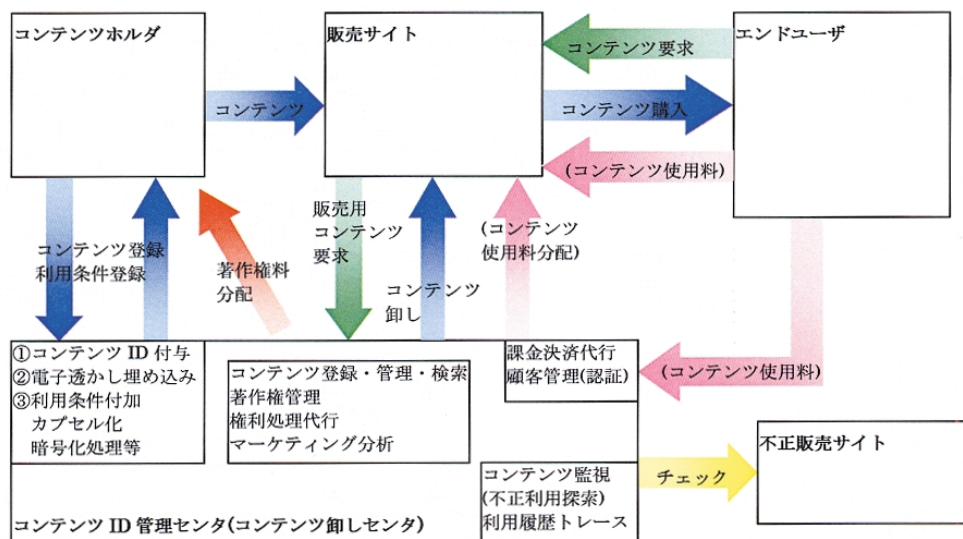


図9 著作権管理システムの例

## 12. 各メディアの著作権管理技術導入動向

コンテンツ流通業界では、各種著作権管理技術の導入が行われています。表14に著作権管理技術の実施事例を示します。

表14 著作権管理技術の実施事例

	製品	著作権管理技術	説明
デジタル放送	地上波デジタル/BS・CSデジタル放送	MULTI2暗号	信号をスクランブルする方式の一種。信号列をブロックに区切り、このブロックを鍵情報を用いて攪拌するブロック暗号方式。
		B-CASカード	暗号の復号に必要なスクランブル鍵はECM (Entitlement Control Message) から取り出す。
オーディオ	DAT/MD/DCC等	SCMS (Serial Copy Management System)	媒体のヘッダ領域に1回コピー可、コピー不可などのコピーフラグを設けてコピーの可否を判断。
	DVD-Audio	CFPM (Content Protection for Pre-recorded Media)	コンテンツ暗号化、リムーバブルメディアに適した鍵管理、パス認証、メディアによる不正機器の無効化の各技術によりなる。
ビデオ	DVD-Video	CSS (Content Scrambling System)	3階層の暗号鍵管理、コンテンツスクランブル、パス認証により行う。
	DVD-RAM/R/RWのビデオ記録フォーマット	CPRM (Content Protection for Recordable Media)	コンテンツ暗号化、リムーバブルメディアに適した鍵管理、パス認証、メディアによる不正機器の無効化の各技術によりなるが、パス認証は、CFPMとは異なる。
メモ리카ード	マジックゲート・メモリースティック	MagicGate	マジックゲート対応機器とメモリースティックの間でお互いが正式なメディア対応関係であるかを相互認証し、認証が成功した機器とマジックゲート・メモリースティック間で、記録、再生するデータの暗号化を行う。
	SDメモ리카ード	CPRM	DVDと同様。
	セキュアMMC	UDAC-MB (Universal Distribution with Access Control Media Base)	音楽配信などで入手した暗号化された音声データを、いったんセキュアマルチメディアカードに保存し、ライセンスキーを購入して再生するしくみ。携帯電話を使った音楽配信で利用されている。

## 13. コンピュータ業界の著作権管理技術 導入動向

コンピュータ業界でも著作権管理技術の導入が活発化しています。Apple社のサービスiTune Music StoreもDRM技術を採用しており、再生できるコンピュータの制限やCDへのコピーの制限が加えられています。また、Microsoft社も5月に新しいWindows Media DRMの機能公開をしており、セキュリティを強化しながらも、多様なデバイスに対応したシームレスなコンテンツフロー

を可能にしているそうです。

## 14. 著作権管理言語

著作権管理については、各種団体があり、デジタルコンテンツに対する著作権管理のための活動を行っています。ここでは、著作権管理言語を紹介します。表15に著作権管理言語として有名なXrMLとXMCLの概要を示します。

表15 著作権管理言語

言語	概要
EXtensible rights Markup Language (XrML)	Microsoftを中心とした著作権保護技術の標準化団体である。Xerox Management Right部門がスピノフしてできた米ContentGuard社が事務局になっている。
Extensible Media Commerce Language (XMCL)	Real Networksを中心とした著作権保護技術の標準化団体XMCL Initiativeによるデジタルコンテンツを商業利用する際に必要となる情報の共通化を目的とした記述言語。XMLベースのオープンな言語で、ビジネスのルールとなる言語を標準化することで、XMCLを利用して、コーデック、デジタル著作権管理システムや、電子商取引システムとは無関係に、コンテンツを自由に操作することができるようにすることを目指す。

## 15. 著作権管理を主な目的とする関連団体・規格

著作権管理については、上述した著作権管理言語の標準化団体以外にも各種団体があり、デジタルコンテンツに対する著作権管理のための活動を行っています。主な著作権管理のための団体を表16に示します。

表16 著作権管理を主な目的とする関連団体・規格

団体名	概要
コンテンツIDフォーラム (cDf)	主な目的はデジタルコンテンツにコピー確認をするためコンテンツにユニークなIDを挿入するコンテンツIDを標準化すること。
DOI (Digital Object Identifier)	DOIは、コンテンツに持続的に存在する識別子 (identifier) を指す。全米の書籍、雑誌出版業者の組織であるAAP (Association of American Publishers) によって1994年に開始された。
Copy Protection Technical Working Group (CPTWG)	コンテンツ事業者、IT企業、家電企業によるコピー管理技術の国際標準化検討をしている。暗号・認証・電子透かしなどの技術をサブWGで検討している。
Secure Digital Music Initiative (SDMI)	1999年2月発足。全米レコード協会 (RIAA) 主導で、音楽コンテンツの配信規格を策定する団体。電子透かしの標準化を含むPhase1仕様を発表。現在Phase2仕様を策定中。
JASRAC	利用可能な電子透かし技術の水準の設定と、水準をクリアした技術の認定作業を行ったプロジェクト (2000年、2001年にSTEP2000、STEP2001) の2回を実施。
Open eBook Forum (OeB)	電子書籍の規格を作成して維持し、その採用を促進することを目的とする団体。

## 16. 各種規格の著作権管理技術の導入状況

各種コンテンツの再生・通信の規格団体もまた、著作権管理技術の導入を進めています。各種規格の著作権管理技術の導入状況を表17に示します。

表17 各種規格の著作権管理技術の導入状況

規格・団体	状況
MPEG-21	2003年7月に、MPEGは、MPEG-21の「権利表記言語」(Rights Expression Language: REL)のパート5と「権利データディクショナリ」(Rights Data Dictionary: RDD)のパート6の完了を発表した。
MPEG-4	標準化団体 Internet Streaming Media Alliance (ISMA) が2004年3月3日、ストリーミングメディア配信に関して標準に基づく技術の採用を促進するべく、新たにコンテンツ保護仕様をリリース。
TV-Anytime	2003年10月にフェーズ1(放送を主体としたアプリケーションを想定したもの)規格がETSI (the European Telecommunications Standards Institute) の技術文書 (ETSI TS 102 822) として発行されたが、RMP (Rights Management and Protection) と呼ばれるパート5が未完成である。
DHWG (Digital Home Working Group)	2005年頃を目指してDRM/コンテンツ保護技術を明確化する予定。
UPnP	AV仕様では、DRM/コンテンツ保護技術を含む「Chapter2」をまとめているところ。
OMA (Open Mobile Alliance)	2004年2月2日 OMA DRM 2.0 Enabler Release公開。音楽やビデオクリップ、ストリーミングコンテンツへの対応を強化。
MPEG LA	2003年10月2日にデジタル著作権管理 (DRM) に対応する製品の実現に必要な特許を集めて集中管理する取り組みを発表し、DRM技術に関連する特許を提出するよう業界に呼びかけ、2004年7月20日にはDRM Reference Model 2.0を発表。

## おわりに

本稿では、特許審査第四部で重要な分野として位置づけている、ICタグと著作権管理技術について概略を説明させていただきました。

2004年度はICタグが実証実験から本格稼働へと移行する重要な時期となります。著作権管理技術についても、ネットワークによるコンテンツ流通やデジタル放送の本格的な普及を前に規格等についてさまざまな動きがでてきています。

そのため、特許審査第四部では今年度、ICタグと、著作権管理技術の1つである電子透かしを特定注目分野と位置づけて、迅速且つ的確な審査に取り組んできています。また、今年度の技術動向調査のテーマとしてICタグを選定しています。特許審査第四部では、他部との連携も視野に入れて、特許、政策及び市場などの面からも、これら技術分野の動向を注意深く追っていきたいと考えています。

### profile

原 秀人(はら ひでと)

平成8年4月入庁

平成15年10月 特許審査第四部審査調査室

平成16年10月より 現職

### profile

梅本 達雄(うめもと たつお)

平成8年4月入庁

平成15年7月 特許審査第四部審査調査室

平成16年7月より 現職