コンテンツ流通における著作権保護技術の動向

櫻井紀彦[†] 木俵豊[††] 高嶋洋一[†]
谷口展郎[†] 難波功次[†]

ネットワークを通じたディジタル情報流通サービスへの期待が高まりつつある一方，良質なディジタルコンテンツ流通の活性化に向けて，情報提供側の意図に従った範囲での利用を可能とする社会的基盤が求められている．本論文では，著作権などをともなうディジタルコンテンツの流通・保護技術に関して，原著作者などが意図した利用条件を可能な限り守り，不正な利用を予防する保護方式（Active Safety 技術）と，不正利用を検出/立証可能とすることで間接的に不正を抑止する保護方式（Passive Safety 技術）に分類し，現在提案されているディジタルコンテンツの流通システム・技術を総括するとともに，今後の課題として，加工・再利用を含めたコンテンツライフサイクルを通した情報保護，さらにプライバシー情報や企業ノウハウ情報などの保護技術への展開を考察し，将来を展望する．

A Survey on Copyright Protection Technologies for Network Distribution of Digital Information

Norihiko Sakurai,[†] Yutaka Kidawara,[††] Yoichi Takashima,[†]
Noburou Taniguchi[†] and Koji Namba[†]

Recently, more and more information is transferred, distributed, and exchanged through the Net. It includes privileged materials such as copyrighted creations, privacy information, business intelligence, etc. that should be protected from improper use. In this paper, we present a survey on technologies to protect digital information in network distribution environment. At first, we classify them in two types: 'Passive-Safety' techniques and 'Active-Safety' ones. Active-Safety techniques are subjected to forfend illegal use of information, while Passive-Safety ones are to detect and attest it. Then we argue over the details of each class, and give closer analysis of the present research and development efforts. Finally we show some prospects about the technologies.

1. はじめに

インターネットの急速な浸透，さらにパーソナルコンピュータや携帯端末の普及により，ネットワークを通じたディジタル情報の流通をだれもが手軽に行える環境が整いつつある．これにともない，様々な人々が築いた情報の海の中から，自分の目的に合わせて情報収集するような，オープンな社会系での情報の活用が行われるようになってきた．

一方，メディア処理技術の発展にともない，写真・絵画や音楽，映像などの多種多様な資産のディジタル化が進んでいる．こうした音楽，美術品など，それ自身に経済的価値のある情報（以下ディジタルコンテンツ）をネットワークを通して売買したり，結合・加工し付加価値をつけたりすることによる新たなビジネスも形成されはじめてきた．ディジタルコンテンツは，社会的資産としてより多くの人に利用してもらうことを期待するものであるが，同時にその利用に対して，著作者は利用報酬を請求するなどの権利を持つ．したがって，ディジタルコンテンツの利用に際して，著作者の権利を守り，その意図を正しく反映する仕組みを作ることが，コンテンツ流通の活性化につながる．

また，医療・教育など各種サービスのネットワーク化の進展にともない，サービスを享受するために必要なプライバシー情報を，個人がサービス主体へネットワークを介して提供することも次第に増えてきた．こうした情報は，より適切なサービスを受けるなどサービス本来の目的に対してのみ提供されるものであり，本来の目的以外に使用されることは許されないため，保護への配慮は必要不可欠である．

† 日本電信電話株式会社 NTT サイバーソリューション研究所
NTT Cyber Solution Laboratories, NTT Corporation
†† 独立行政法人通信総合研究所
Communications Research Laboratory

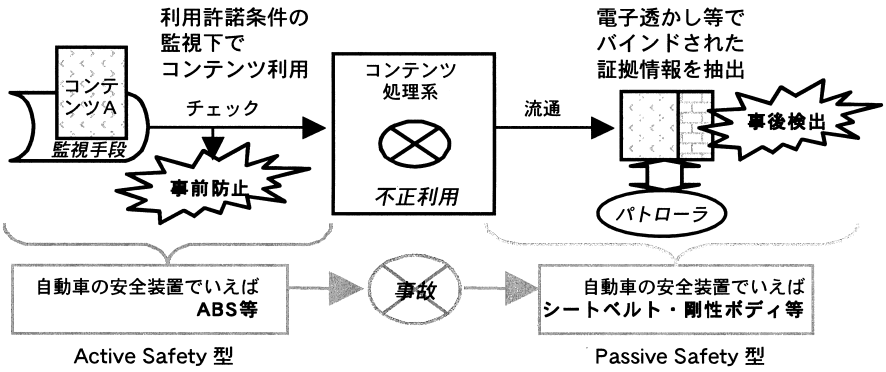

図 1 著作権保護方式のモデル
Fig. 1 Two types of copyright protection technologies.

あるいは近年，企業活動においては,「ナレッジマネジメント」などの概念に基づき，知識労働の生産性向上を目指した企業内外の情報流通の活性化が称揚されている．こうして流通する知識情報は，受け手に応じて異なる処理を行うことで様々な価値を生み出すが，企業秘密に類する情報を含むため，受信者や処理方法については発信者の意図に従う管理が求められる．

今後の情報化社会の形成においては，これら各種の情報の特質を十分考慮しつつ，その保護をつねに念頭において流通を促進するようなネットワーク基盤の形成が重要になるであろう．本論文では，上述した「ディジタルコンテンツ」「プライバシー情報」「企業の知識情報」のうち，すでにビジネスとして萌芽期から成長期に移りつつある，著作権などをともなうディジタルコンテンツの流通における保護技術に関してサーベイする．ただし，ディジタル TV など，Internet を介さない放送型システムの保護技術は対象に含まない．

本論文の構成は以下のとおりである．2 章では，保護技術を Active Safety 型技術と Passive Safety 型技術にモデル化・分類し，それぞれの特徴について述べる．3 章・4 章ではそれぞれのモデルに類する現在提案されている具体的システム・技術，その課題について考察する．5 章では，さらに個人情報や企業の知識情報を含めた将来の情報流通の課題・展望に関して考察し，まとめとする．

2. 著作権保護方式のモデル化

情報技術の進歩により，社会的資産として価値を持つディジタルコンテンツは，メディアの種類も数値文字情報から静止画像，音声，動画像へと広がり，ネットワークを用いた映画や楽曲の販売も試みられるようになった．しかしながら，ディジタル情報は複製が容易で劣化しないという特徴を持つため，一定の価値がある情報を流通する際には，不正な利用を防止し，知的所有権を保護する仕組みが不可欠である．本章では，著作物の保護技術を，事前に不正利用を防止する技術（Active Safety 型技術）と，事後に不正利用を検出/立証可能とする技術（Passive Safety 型技術）に大別してモデル化し，各々の特徴について述べる[1),2)]．

2.1 Passive Safety 型技術と Active Safety 型技術

現状提案されている著作権保護技術は，**図 1** に示すように大きく 2 つに分けることができる．

1 つは Passive Safety 型技術，つまり，不正利用の発生後の検出/識別/証明を可能にし，これにより間接的に不正利用の抑止を期待する技術である．問題発生後の安全性を追求する点で，自動車におけるシートベルトや剛性ボディにたとえられる．この技術では以下の 2 つが重要なポイントとなる．

(1) ディジタルコンテンツに，不正利用の立証を可能にする情報を，通常の利用には問題がなく，かつ簡単には取り除けないようバインドする技術．代表例として電子透かし技術があげられる．
(2) 適切な流通ポイントで，バインドされた情報を読み出し，その環境・コンテンツの利用状態から不正利用を検出する技術．代表例はパトロール機能を持つロボット（パトローラ）である．

もう 1 つは Active Safety 型技術，すなわち不正利用の発生自身を未然に防止することを目的にした技術であり，同様に自動車にたとえるとアンチロックブレーキなどに相当する．Active Safety 型技術では，

(1) ディジタルコンテンツにその利用許諾条件や利用管理プログラムをどうバインドするか，
(2) その条件を確実にかつ安全に執行する環境をいかに形成するか，

が重要なポイントになる．

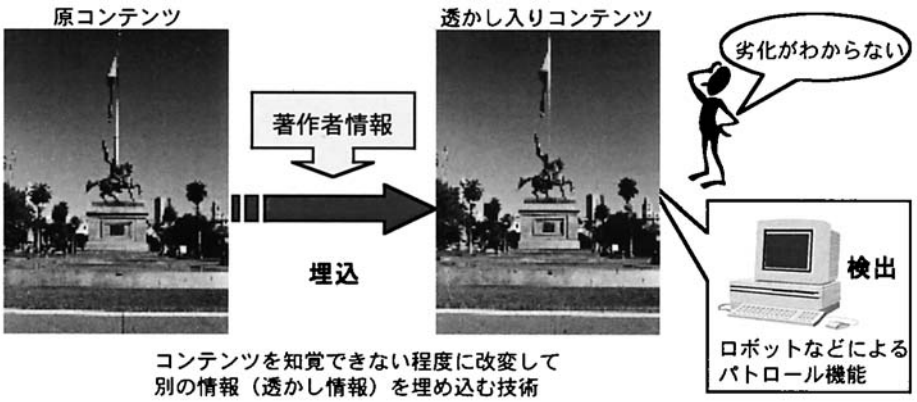

図 2 Passive Safety 型技術の例（電子透かし技術と検出技術）
Fig. 2 Insertion and detection of digital watermark.

これら 2 つの技術は競合するものではなく補完しあうものであり，組み合わせることでより優れた著作権保護システムの実現が期待できる．

3. Passive Safety 型技術

本章では Passive Safety 型技術の概要と効果について具体的なシステムの例をあげて論じる．

Passive Safety 型技術は，ディジタルコンテンツの不正利用を事後に検出/証明する技術である．不正利用の発生自体を防ぐことはできないが，検出/証明による損害の回復を可能とするとともに，こうした損害賠償のおそれがあることを潜在的な不正利用者に知らしめることで，結果的に不正利用の抑止も期待できる．

たとえば，ディジタルコンテンツにそれを識別する ID 情報を埋め込み，その正当な配布先を ID 管理データベースに登録しておく．不正かどうか不明なコンテンツが発見されたときは，埋め込まれた ID 情報を読み取り，それを ID 管理データベースに照会すれば，正しい配布先の情報が得られる．これを発見された場所と比較すると，不正コピーかどうかが判断できる．**図 2** にこのシステムのイメージを示す．

このようなシステムにおいて重要なポイントは以下の 2 つである．

(1) 不正利用を証拠立てる情報をいかに強力にディジタルコンテンツにバインドするか．
(2) ネットワーク上で流通している大量の情報の中から，いかに網羅的にディジタルコンテンツの不正利用を検出するか．

ディジタルコンテンツへの証拠情報のバインドには，コンテンツの切り取り・変形などの加工に対する耐性が求められるため，一般に電子透かし技術が用いられる．電子透かし技術の中には，いったん光学的コピーなどでアナログ情報に変換された後の再度のディジタル化に対しても効力を発揮する強力なものもある．

一方，不正利用の検出については，ネットワーク巡回ロボットによるパトロールなどの技術が用いられる．こうした自動検出を行う場合は，インターオペラビリティを確保するために，バインドする証拠情報の表現形式が標準化されていることが望ましい．この点に関しては，コンテンツ ID フォーラム[3]などにおいて，標準化の取り組みが精力的に進められている．

3.1 証拠情報のバインド ～電子透かし技術

不正利用を証拠立てるためには，コンテンツから ID 情報などの証拠情報が正しく得られることが必要である．コンテンツのヘッダ領域やコメント領域などに ID を記述するという方法も考えられるが，不正利用者がカット&ペーストで，コンテンツを入手することなども想定されるので，そうした領域に埋め込まれた情報がいつまでも残っているとは限らないし，また残っていても内容が書き換えられている可能性もある．そこで利用されるのが電子透かしである．

電子透かしとは，画像，映像，音声といったディジタルコンテンツに，人間に知覚されないように，別の情報（透かし情報）を埋め込む技術である[4)~7)]．電子透かしなら，コンテンツそのものに ID 情報が埋め込まれ，しかも部分切り取りなどの編集を施されたコンテンツであっても埋め込まれた ID を取り出すことも可能になる．

もちろん，電子透かしといえども限界はある．たとえば，静止画から 1 ピクセルだけ切り出したものから電子透かしを読み取ることはできない．また，電子透かしの読み取り装置を持っていれば，検出されないように元の透かし入りコンテンツに編集を施すことは比較的容易である．

そこで電子透かしでは，編集などの攻撃を受けてもどの程度透かしが残るかという耐性が重要になる．透かしの耐性とコンテンツの品質にはトレードオフの関係があるので，どの程度の品質まで透かしが残る必要があるかを事前に決めておく必要がある[12)〜15)]．

一般的な電子透かし技術の例としては，IBM のデータハイディング[16)]，サンモアテックの Syscop[17)]，エム研の Acuaporta[18)]などがあげられる．

静止画に対する電子透かしとしては Digimarc[19)]のものが有名で，Adobe 社の Photoshop Ver. 5.0 以降にも組み込まれている．また，ISO IEC/JTC1/SC29/WG1（JPEG）においても，JPEG2000 の規格に電子透かしが盛り込まれている．

動画に対する電子透かしについては，まず蓄積メディアである DVD のコピー制御（2 ビット）を透かし情報として埋めこむことが検討された．DVD フォーラムの下部組織である，CPTWG（Copy Protection Technical Working Group）で DVD のコピー制御方法とその電子透かし方法について検討され，GALAXY[20)]陣営，Millennium[21)]陣営の合意が得られている．一方，ネットワークを流れる動画ストリームへの電子透かしについては，ISO IEC/JTC1/SC29/WG11（MPEG）などで検討中だが，現時点では何も決まっていない．

音楽情報に対する電子透かしについては，SDMI（Secure Digital Music Initiative）で，Phase I, Phase II にわたる電子透かしの検討が行われた．Phase I では Verance 社の電子透かし技術が採用されたが，その次の仕様である Phase II の電子透かしは，これを破ったとする研究者が現れる騒ぎもあり，現在のところまだ定まっていない．日本では，JASRAC において STEP2000 と呼ばれる電子透かしコンテストが行われ，IBM，JVC，MarkAny[22)]などの技術が認定されている．

これ以外のテキストや文書などのメディアに対する電子透かしについては，研究は行われているものの，まだ実用的なものは出てきていない．

3.2 不正利用の検出〜パトロール技術

オンライン/オフラインに存在する大量の情報の中から，不正に複製・利用されているディジタルコンテンツを，人手で探すのはもはや不可能といっても過言ではない．そこで，人手ではなくネットワークを自動巡回するロボットなどを利用して不正コンテンツを探し出してくる方法が考えられている[8),9)]．

しかし，ロボットを利用する方法はネットワークへの負担も大きく，リンクをたどって巡回するという性質から，独立したリンクのないサイトの不正利用コンテンツは見つけられないという問題点もある．

そこで，松井らは利用者から告発するタイプのシステムの提案をしている[10),11)]．このシステムは，ネットワークへの負荷も少なく，リンクの張られていないコンテンツにもたどりつくことができるが，利用者が少ないコンテンツは見逃すということ，利用者が不正かどうかチェックするための動機付けが必要ということ，利用者のプライバシーがセンタへ洩れるということなどの短所もあり，いまだに実用化はされていない．

ロボット型，利用者協力型は独立に動作できるものであるから，各々独立にサービスをすることも可能である．さらに効率の良い方法が考えられる可能性もあり，今後の成果が期待される．

他方，冗長度の低いコンテンツに対しては，電子透かしを利用せず，全文比較という手段で不正コンテンツを見つけ出してくる手法も研究されている．コンテンツそのものの全体あるいは一部について，同じものであるかどうかを比較して探すという方法である．たとえば，アクティブ探索法[23)]を用いた音楽放送の高速マッチングが提案されており，CM が正しく放送されているかどうかなどに利用されている．

不正利用の検出のためのパトロールは，実社会における警察の役割を担うものといえる．不正すべてを洩れなく検挙することはたしかに望ましいが，警察の検挙率が 100%ではないように，不正利用をすべて見つけ出すことは現実的には不可能に等しい．また，パトロールを強化するため，強固なセキュリティチェックを施せば，時間や要員，計算機パワーのロスにつながるので，コスト面からも限界がある．さらに，パトロールの強化は，個人の情報の監視強化に直結するため，こうしたプライバシーの問題も考慮する必要がある．

4. Active Safety 型技術

本章では Active Safety 型技術の概要と効果について具体的なシステムの例をあげて論じる．

4.1 Active Safety 型技術概論

Active Safety 型技術は，ディジタルコンテンツの不正な利用を未然に防ぐことを目的とする技術である．

著作物の不正な利用というと，真っ先にあげられるのは，いわゆる「海賊版」すなわち不正コピーの再配布の問題である．近年大きな問題となっている Napster などの P2P（Peer-to-Peer）ファイル交換システムも，そこで交換される音楽ファイルの大半が著作者の許諾のない不正コピーである点が著作者側の大きな懸念につながっている．

こうした海賊版を防ぐ方法の 1 つとして，基本的に

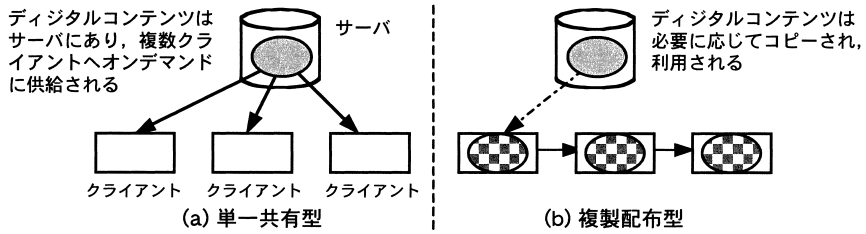

図 3 利用形態のモデル
Fig. 3 Two models of network distribution of digital information.

ディジタルコンテンツを複製しないというやり方が考えられる．ディジタルコンテンツはつねに著作者の管理下にあるサーバ上にのみ存在し，必要に応じてネットワーク経由で利用者のもとに供給されるというモデルである．1965 年 Nelson はこの考え方に基づく「transpublishing」の概念を Xanadu プロジェクトの中で提唱している[24]．また，最近の例では，Internet を介した動画や音楽のストリーミングサービスも，このモデルに基づくものの 1 つと見なせるだろう．

このような，理論的に単一のディジタルコンテンツをネットワーク経由で「共有」する，**図 3** (a) に示すモデルに基づくシステムにおいて，ディジタルコンテンツの保護に実効性を持たせるためには，

- 配送先が正しい利用者であることを認証する
- 配送経路および配送先での複製を防止する

という仕組みが必要になる．

配送先の正しさの認証については，基本は Internet における認証技術と変わりなく，この点について本論文では深く立ち入らない．RealNetworks 社の RealSystem[26]や Microsoft 社の Windows Media[27]などのストリーミングサービスシステムでは，クライアントマシンのハードウェア情報や，クライアントプログラム自身に埋め込まれた識別情報を，認証のための ID として利用しているものと考えられる．

配送経路および配送先での複製防止については，ストリーミングサービスの場合，配送経路では暗号化を，配送先では専用クライアントプログラムをサーバから制御する方法が一般的である．暗号技術の詳細については本論文のスコープ外とし，深く立ち入らない．クライアントプログラムの制御方法については，一般に，

- データストリームと並行して送受信される制御情報ストリームを通して保存の可否をクライアントプログラムに伝える，
- クライアントプログラムは，保存が許されないストリームについてはユーザインタフェースから保存の操作を選べないようにするなどして，保存が行えないようにする，

という仕組みで複製を防止する方法が考えられる．

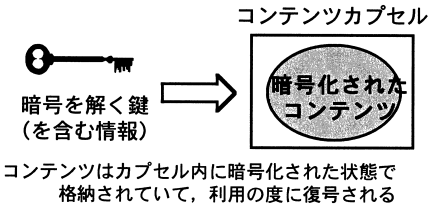

図 4 コンテンツカプセルの概念
Fig. 4 Conceptual image of a secure container.

一方，ディジタルコンテンツを不正な利用から守るもう 1 つの方法として，図 3 (b) に示すような，ディジタルコンテンツの複製自体は可能だが，仮に著作物が複製されたとしても，その利用は必ず著作者の許諾のもとで行われることを何らかのかたちで保証するやり方が考えられる．つまり，著作物の複製ではなく利用を管理するという考え方である．この考え方を一歩進めて，ディジタル情報の利用のみをメータリングし，複製および再配布についてはむしろ積極的にこれを奨励することで，ネットワークを介したディジタル情報の流通を促進する「超流通」の概念が，1983 年，森らによって示された[28),29)]．以後，その実現を目指して様々な技術の研究開発が行われている．

ディジタルコンテンツの複製ではなく利用を管理するシステムにおいては，ディジタルコンテンツあるいはその複製について，

- システム管理外で正しく扱えないようにする，
- システム管理下において，利用許諾条件の範囲内で利用者に提供する，

という仕組みが必要になってくる．

これを実現する方法として，多くのシステムでは，「コンテンツカプセル（セキュアコンテナと呼ばれることもある）」技術が利用されている．**図 4** に示すコンテンツカプセル技術の概念は，ディジタルコンテンツを鍵のかかる安全な容れ物＝コンテンツカプセルに

格納して「鍵」を掛け，鍵がないとカプセルを開けて中のディジタルコンテンツが利用できないようにすることで，ディジタルコンテンツを不正な利用から守るというものである．こうすれば，コンテンツカプセル（とその中身のディジタルコンテンツ）自体はいくら複製されても，利用のつど鍵が必要になるので，著作物の利用をつねにシステムの管理下におくよう利用者に要求することができる．

現在知られているコンテンツカプセル技術としては，InterTrust 社の MetaTrust/DigiBox[30] と IBM 社の EMMS/Cryptolope[31),32)]，Microsoft 社の WMRM（Windows Media Rights Manager）[27)]，ContentGuard 社の RightsEdge[33)]，NEC 社の RightsShell[34)]，Preview System 社の ZipLock/Vbox[35)] などの商用技術のほか，NTT 社の櫻井らの Matryoshka[55)]，通信総合研究所の木俵らの EMO（Executable Multimedia Object）[36)]，米 Cornell 大 Project Prism の FEDORA / Security Automata[43)~45)] などの研究システムがある．このほか本論文では，厳密な意味でコンテンツカプセルとはいえないが，関連技術として米 Cornell 大の Lagoze らの Warwick Framework[46),47)]，希 Forth 大の Nikolaou らによる Aurora[48),49)] なども取り上げる．

一般にコンテンツカプセル技術では，ディジタルコンテンツに鍵を掛ける仕組みとして暗号技術を利用している．実際に利用するときには，復号鍵を用いてデータを on-the-fly で復号し，それを表示/再生するというやり方である．従来は，暗号化/復号化は多くの計算機資源を必要とする処理であったため，こうしたコンテンツカプセルに高強度の暗号技術を採用することは難しかった．しかし，近年の計算機性能の急激な向上により，堅牢な暗号の on-the-fly での復号が可能になったことで，コンテンツカプセル技術はより実用性を増しつつある．

カプセル内に格納されたコンテンツの利用の際には

- 正当なプログラムへのカプセルの引き渡し
- 利用許諾条件の取得
- 利用許諾条件の解釈
- 利用許諾条件に基づくコンテンツハンドリング

という機能が求められる．

正当なプログラムへのカプセルの引き渡し：利用者がカプセル内のコンテンツを利用する場合，コンテンツカプセルを「正当な」プログラムから開く必要がある．ここで「正当な」とは，利用許諾条件を遵守し，暗号化されていない=復号されたコンテンツのカプセル外への不用意な漏出を防止するという意味である．

そもそも，利用許諾条件を守らないプログラムによってカプセル内コンテンツの暗号が解かれてしまえば，コンテンツの保護は期待できない．また，たとえば「クリップボードへのコピー」などの編集コマンドが利用可能になっていると，いかに強力な暗号でコンテンツを保護していても，復号後のコンテンツが容易にディジタルコピーされてしまう．

逆に，カプセルが正当なプログラムから開かれるかぎり，暗号化されていないコンテンツが著作権者の意図に反してカプセル外に露出してしまうことはない．したがって，カプセル内コンテンツの暗号が解かれる際には，必ず正当なプログラムからコンテンツカプセルが開かれることを保障する仕組みが必要になる．

この仕組みの実現方法は，コンテンツカプセルの構成によって大きく 2 つに分けられる．

まず，コンテンツカプセルが，コンテンツをハンドリングするプログラムを含む構成について考える．たとえば，FEDORA/Security Automata，Matryoshka，EMO などがこれに相当する．この場合，コンテンツカプセルを開くと，まずカプセル内のプログラムが起動され，それが暗号鍵を取得して同一カプセル内のコンテンツを開くという手順になる．この場合，そもそも不正なプログラムによって暗号が解かれて原コンテンツが露出してしまう危険性は低い．

一方，コンテンツカプセルはデータのみを含み，そのハンドリングプログラムは別に存在するという構成もある．MetaTrust/DigiBox，EMMS/Cryptolope，WMRM，RightsEdge などを含め，多くのコンテンツカプセルシステムはこちらに属するものといえよう．この場合は，プログラム内包型と異なり，カプセルが必ず正当なアプリケーションから開かれるように仕向ける仕組みが別途必要になる．最も単純な方法は，カプセルファイルのデータフォーマットを秘密にし，これを解釈できるできるプログラムを，コンテンツカプセル技術の開発元のみが提供するというやり方だろう．ただ，これでは，場合によって高機能な（たとえば複数のカプセルを同時に扱える）プレイヤが欲しいというような要求に応える柔軟性に欠ける．したがって，多くのシステムでは，カプセルを扱うアプリケーションプログラム（AP）を開発するためのライブラリを提供するというかたちで，正当性とカスタマイズ，双方の要求を満たせるようにしている．さらに安全性を高めるための手段として，WMRM などのように AP の認証プロセスを持つものもある．

利用許諾条件の取得：次に，プログラムはカプセル内のコンテンツに対応する利用許諾条件をいずこから

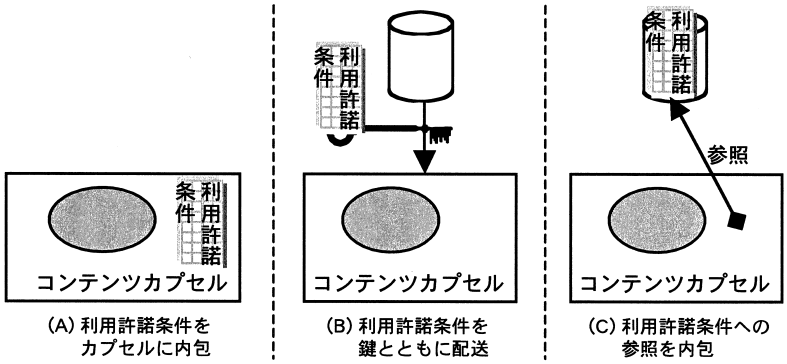

図 5 利用許諾条件のバインド方式
Fig. 5 Three typical methods to bind a content to its terms and conditions.

か取得する必要がある．コンテンツと利用許諾条件の対応づけについては，**図 5** に示すように

A） コンテンツカプセルに内包する，
B） ライセンスキーにバンドルして供給する，
C） ユニークな識別子などを用いて参照する，

などの方法が考えられる．

A) の方法は，

- 利用許諾条件自体をコンテンツカプセルによって改竄などから保護することができる，
- コンテンツとその利用許諾条件が密結合されており，コンテンツカプセルが複製される際には同時に利用許諾条件も複製されるので，コンテンツ–条件間の組合せの改竄にも強い，

という長所がある反面，密結合されているがゆえに利用許諾条件の変更などの柔軟性に欠ける．Meta-Trust/DigiBox，EMMS/Cryptolope，Matryoshka，FEDORA/Security Automata，Aurora などでこの方式が用いられている．

これに対し B) は，ライセンスキー発行ごとに利用許諾条件を設定できるため，条件設定における柔軟性が高い．しかし当然，利用許諾条件自体の保護や，ディジタルコンテンツと利用許諾条件の組合せの正しさの保証という点には難しさがある．WMRM や RightsShell などではこの方式が用いられている．

C) の方法は，A)，B) を一般化したもの，つまり「利用許諾条件は，論理的にディジタルコンテンツにバインドされていれば，物理的にはどこにあってもよい」という考え方に基づくものといえる．この方式では，ネットワーク上にあるサーバでの利用許諾条件の集中管理が可能なので，単一あるいは少数の著作権管理代行組織のもとで著作物の利用許諾処理が集中管理されている現状の著作権管理メカニズムとの親和性が非常に高い．これに基づく著作物流通体系としては，北川が 1994 年にコンセプトを発表したコピーマート[50]のほか，近年安田らによって提唱された cIDf（Content ID Forum）[51]などがあげられる．またコンテンツカプセルシステムでは，RightsEdge がこれに近い方式を採用しているものと思われる．

この 3 つの方式については，必ずしも排他的なものではなく，上に名前をあげたシステムでも，複数あるいはすべてを組み合わせて利用できるものもある．

利用許諾条件の解釈：取得された利用許諾条件は，当然ながら機械可読な形式で記述されていなくてはならない．多くのシステムでは，利用許諾条件記述は非公開の独自仕様を利用している．仕様が公開されている利用許諾条件記述言語として最もよく知られているのは，ContentGuard 社の提案する XrML（eXtensible rights Markup Language）[52]である．また cIDf では，こうした利用許諾記述を，より広い著作物のメタデータの一部として規定している．このほかメタデータ関連では，Dublin Core や MPEG などの標準化活動においても，メタデータ仕様の一部として権利記述に関する検討が行われているが，現在のところ実用レベルの仕様の公開には至っていない．

利用許諾条件に基づくコンテンツハンドリング：コンテンツの利用許諾条件を解釈し終えたら，現在のコンテンツの利用状況と比較して，それが利用許諾条件を満たせば，コンテンツ復号鍵を取得し，暗号を解いたコンテンツを利用者に供する．暗号解除後も，利用者の操作に対する監視および利用許諾条件から逸脱を防ぐ制御は継続して行われる．このプロセスにおいてキーになるのは，「安全な復号機構」「利用状況の監視機構」「利用条件の執行（enforcement）機構」の 3 つのメカニズムである．

「安全な復号機構」については，復号鍵を外部に露出させないことや，復号後のコンテンツの複製を可能

な限り防止することが求められる．復号鍵の安全性の確保については，復号鍵自体を別の鍵で暗号化するなどの措置に加えて，復号鍵および/またはそのメタ鍵を利用者機器上の永続ストレージに保存せず，コンテンツ復号の必要が生じるたびごとに著作権者の信頼できるネットワーク上の鍵管理サーバから取得するなどの方法が考えられる．また利用者機器上の永続ストレージに保存する場合でも，そのファイルを暗号化する，ユーザランドからはアクセスできない領域に保存するなど，該ストレージ領域のタンパーフリー性を確保したうえで保存する方法がある．この方法をとる場合一般に，APよりもOS，OSよりもファームウェアと，より低位な（=ハードウェアに近い）側で実現するほうが安全性は高い．また少し異なるアプローチとして，PKI/バイオメトリクス/電子署名など外部の認証機構と復号鍵（あるいはその生成に必要な情報）をバインドして，鍵の安全性を高める方法もある．

また復号後のコンテンツの複製防止についても，復号されたデータをキャッシュなどの目的で一時的にファイルに書き出すなどという行為を避けるのは当然として，他のプログラムによる画面のキャプチャやメモリのタンパリングなどを，OSやファームウェアを制御して可能な限り防止する手段をとることが望ましい．

利用状況の監視および利用許諾条件の執行についても同様である．たとえば，利用者環境そのものが悪意を持っている場合に備えて，これらの機構の一部を著作権者の信頼できるネットワーク上のサービスと連携しないとコンテンツを操作できないようにするという方法が考えられる．たとえば，利用許諾条件の1つとして利用期限を切るということが考えられるが，利用者環境の時計機能を利用するのではなく，信頼できるNTP（Network Time Protocol）サーバを利用して時刻を取得することで，OSの時計の巻き戻しなどにも対処できる．また，利用者機器ローカルでも，OSではなくファームウェアやハードウェアから直接時刻を取得できれば，より安全な利用期限制御を実現できる．

これまで述べてきたことから分かるように，これらの機構は，リモートもしくはローカルでもより低位レイヤで実現することが，安全性の面からは望ましい．しかし一方で「同じデータをいつでも/どこでも/いつまでも利用したい」という，データのportability（可搬性）やperpetuity（恒久性）に対する利用者の要求を実現するには，ネットワークやプラットフォームへの依存度はできるだけ低いほうがよい．これらの機構をどのレベルで実現するかは，こうした「著作者から見た安全性」と「利用者から見た利便性」を，どのようなバランスで最大化していくかという判断と密接に関係してくる．

ハードウェアレベルの著作権保護システムとしては，Sony社のMagicGate/OpenMG[53]や4C Entity のCPRM（Content Protection for Recordable Media）[54]などが様々なものがあるが，利用状況の監視や利用条件の執行などの高度な機能を組み込んだものは，今のところ知られていない．OSレベルに監視執行機能を組み込むものの代表にしてほとんど唯一の例は，WMRMであると思われる．現在最も一般的なのは，アプリケーションレベルでの実現で，MetaTrust/DigiBox，EMMS/Cryptolope，RightsEdge，RightsShellなど多数の例がある．カプセルそのものに監視執行機能を組み込むものとしては，FEDORA/Security Automata，Matryoshka，EMOなどがあげられる．

しかし，これらの区別はdistinctなものととらえるべきではない．各技術は，ハードウェアからコンテナまでの区分が明瞭ではない連続的な直線上のどこかに位置づけられるものと考えるのが適当であり，またシステムによっては複数のレベルで監視執行機能を実現するものもあるので，各レベルでの実現を排他的なものととらえるべきでもない．

4.2 Active Safety 型技術の具体例

本節では，前節で名前をあげたActive Safety型技術のうち，主要なものの特徴を簡単に紹介する．

（1）Xanadu（Nelson ほか）

Xanadu[24),25)]は，情報をネットワークを介して参照/共有するシステムの草分けの1つである．WWW（World-Wide Web）で用いられている「ハイパーテキスト」や「ハイパーリンク」という言葉は，Nelsonが用いたのが最初といわれている．

Xanaduでは，ネットワーク上の文書は，ハイパーリンクを用いて他の文書の任意の部分を参照（‘transpoint’）できる．このようにリンクによって結合された文書の集合は，‘parallel documents’と呼ばれる．Parallel documentsには，他の文書の任意の部分を自己の文書の任意の位置に埋め込む（‘transclude’）することが可能であり，これにより自由な情報の再利用をきわめて柔軟に実現するとしている．

Xanaduにおける著作権保護の仕組みは，‘transcopyright’という概念に基づいている．Transcopyrightは，transclusionに対する許諾を著作者が行うことで，著作物に関する全権利の保護と自由な情報の再利用を「摩擦なしに」両立できるという考え方で，これを実現する仕組みが‘transpublishing’と呼ばれ

る．Transpublishing システムでは，著作者が任意の transclusion に対する許諾およびその対価を設定する機能，transclusion に対する課金機能，そのためのマイクロペイメント機能などが必要になるとされているが，現在の実装にこうした機能は含まれていない．

（2）RealSystem（RealNetworks 社）

RealSystem[26]は，RealNetworks 社が提供するディジタルメディアストリーミングシステムの総称である．

RealSystem では，‘Authentication Extension’ という拡張機能を利用することで，認証ベースのメディア保護機能を提供している．認証は「ユーザ ID とパスワードの組」，もしくは「プレイヤの ID」によって行われる．これを用いて，認証された相手にのみ pay-per-view のストリーミングを提供するなどのサービスを実現している．

ストリームの暗号化については，SecureMedia 社の Encryptnite という技術を採用している．この技術は，暗号化されたストリームの任意の時点に対し，早送り/巻き戻しなどの操作が行える点に特色がある．

なお RealSystem 社は，この 6 月に，RealSystem iQ というコンテンツカプセルをサポートする技術に基づく著作権管理システム ‘RealSystem Media Commerce Suite’ を新たに発表している．

（3）WMRM（Microsoft 社）

WMRM（Windows Media Rights Manager）[27]は，Microsoft 社の Windows OS におけるディジタルメディア配信システム ‘Windows Media Technology’ において，著作権管理を担うコンポーネントである．

WMRM では，まずディジタルコンテンツを暗号化しコンテンツカプセルに格納する．サーバに置かれたコンテンツカプセルは，ストリーミングあるいはダウンロードによって利用者の手もとに配信される．利用の際には，WMRM をサポートするプレイヤ（例：Windows Media Player）はまず「ライセンス」をライセンスサーバから取得する．ライセンスには，コンテンツの暗号鍵のほか，利用条件（使用開始/終了日時，使用回数，可搬記憶メディアへの出力許可など）を含めることができる．プレイヤは利用条件をチェックし，暗号を解いてコンテンツの再生を行う．

（4）MetaTrust/DigiBox（InterTrust 社）

MetaTrust Utility[30]は InterTrust のディジタル著作権管理技術と互換性のあるシステムの総称で，DigiBox はその中核のコンテンツカプセル技術である．

MetaTrust の主要なコンポーネントは，‘DigiBox Container’，‘Usage Rules’，‘InterRights Point’，‘Transaction Authority Framework’ の 4 つである．コンテンツ提供者は，保護の対象となる情報を，その利用条件（=Usage Rules）とともに DigiBox Container に格納する．配布された DigiBox Container は，利用者デバイス上の InterRights Point が Usage Rules を満たすことを確認した場合にのみ利用できる．その一方 InterRights Point は，Transaction Authority Framework に課金などに必要な情報を送信する．

（5）EMMS/Cryptolope（IBM 社）

IBM 社の EMMS（Electronic Media Management System）[32]は，5 大音楽レーベルのネットワーク配信共同実験にも利用された，ディジタルコンテンツ流通を包括的に扱うシステムである．

EMMS では，まずコンテンツ提供者は暗号化/電子透かし処理のなされたコンテンツをコンテンツカプセルに格納してサーバに投入するとともに，低品質で暗号化されていない販促用のデータを Web 店舗などに送る．利用者が Web 店舗の販促用データを EMMS 対応プレイヤで再生し，購入のアクションをとると，プレイヤは対応するコンテンツカプセルをサーバから取得するとともに，課金情報など権利処理サーバに送る．権利処理サーバはプレイヤに対して「ライセンス」を発行するとともに，課金情報を Web 店舗やコンテンツサーバに転送して，課金処理を行う．

EMMS のコンテンツカプセルとしては，明示されてはいないものの同じ IBM 社の Cryptolope 技術[31]が利用されているものと思われる．Cryptolope は，1 つのファイルの中に，（複数の）暗号化されたコンテンツ，それらのメタデータや復号鍵，契約条件，電子透かし/シグネチャ，電子公正証書などが格納された複合ファイルで，Cryptolope 対応プレイヤが，契約条件に基づくライセンスを受け取り，それに従って動作することでコンテンツの不正な利用を防止する．

（6）RightsEdge（ContentGuard 社）

ContentGuard は，もともと Xerox 社で研究開発が行われていた著作権保護技術だが，現在はスピンオフし，ContentGuard という社名のもとで，RightsEdge[33]という製品を提供している．

RightsEdge では，まず提供者がコンテンツからコンテンツカプセルと ‘Rights Label’ を生成する．Rights Label はコンテンツに許可される権利/条件，その他コンテンツに関する書誌情報などを記述したメタデータである．この Rights Label が ‘RightsEdge’ サーバに送られる一方，保護されたコンテンツはリポジトリに保管される．利用者から Web 店舗などを介してコンテンツ購入依頼があると，RightsEdge サーバは Rights Label から「ライセンス」を生成するとともに，リポ

ジトリから対応するコンテンツカプセルを取得し，利用者に届ける．最後に利用者は‘Activation’サーバからユニークな公開鍵ペアの秘密鍵を入手し，コンテンツカプセルの保護を解除して利用する．

RightsEdgeの特徴は，Rights Labelやそこから生成されるライセンスの記述に用いられる権利記述言語XrML（eXtensible Rights Markup Language）[52]である．現在のところ，XrMLは，その機能と完成度の高さから，この種の権利記述言語の標準リファレンスモデルとしての地位を固めつつある．

（7）Warwick Framework（Lagozeほか）

Warwick Framework[46),47)]は，Dublin Coreなどにおけるメタデータ記述を分析した結果生まれた，複数の「メタデータセット」をまとめて扱うためのフレームワークである．

メタデータセットとは，Dublin Core，MARCなど異なる仕様で記述されたそれぞれのメタデータを指す．Warwickではこのメタデータセットを‘package’，同一のコンテンツに対する複数のpackageを1つにまとめたものを‘container’と呼び，この2つを基本コンポーネントとしている．Containerは永続的なものであっても一時的なものであってもよく，利用者はcontainerに対してグローバルなURIを用いてアクセスする．Containerの中身であるpackageは，実データである‘metadata set’，他のpackageへの間接参照である‘indirect’，package自身が複数のpackageを内包する‘container’の3つに分類される．

Warwickが単なるメタデータフレームワークと異なるのは，そのメタデータセットの1つとして，コンテンツに対する‘terms and conditions’，つまり利用許諾条件を強く意識し，ほぼ既定値として扱う点にある．だが，その記述仕様や監視執行機能の実装は提供されず，次に述べるFEDORAに引き継がれた．

（8）FEDORA/Security Automata（Cornell大Project Prism）

Cornell大学のProject Prism[43)〜45)]は，米国の電子図書館研究プロジェクトの一環として，信頼性が高く安全なディジタルコンテンツの格納/アクセスを，オープンなアーキテクチャで実現することを目指すプロジェクトである．FEDORA（Flexible and Extensible Digital Object and Repository Architecture）はそのセキュリティシステムに相当し，Warwickをベースに，これを実体化しつつ洗練したものとなっている．Security AutomataはFEDORAにおけるコンテンツカプセルの進化形である．

FEDORAのコンテンツカプセル‘DigitalObject’は，複数のコンテンツデータを不透明なバイト列としてカプセル化したもの（‘Structural Kernel’）と，それに意味を与えたり操作したりするためのインタフェース（‘Disseminator’）から構成されるものとして概念化されている．実際にはStructural Kernelは，‘DataStream’と呼ばれるコンテンツバイト列だけでなく，それらに対する共通の操作をまとめたPrimitive Disseminatorという基本インタフェースを含んでいて，DataStreamに対する操作はこれを介して行われる．一方，拡張インタフェースである通常のDisseminatorは，コンテナ外のリモートメソッドへの参照であってもよい．DigitalObjectにおける利用許諾条件の執行では，このリモートDisseminatorでの処理が例にあげられている．

Security Automataは，このDigitalObjectの進化したもので，‘PSlang’という言語を用いて記述した利用許諾条件を，コンパイル後のプログラム自体に‘program rewriter’というツールを用いて組み込むことにより，監視執行の確実な実施を行うというものである．現在のところ，Javaバイトコード用とx86機械語用のprogram rewriterが提供されている．

（9）Aurora（Nikolaouほか）

Aurora[48),49)]はCORBAやWWW，Javaの環境を用いたカプセルフレームワークである．

Auroraの基本思想は，“Distributed Objects + Open Scripts = Network-Centric Applications”，すなわち，サービスを提供するソフトウェアをAuroraのオブジェクト指向設計に則ってコンポーネント化し，そのコンポーネントをHERMESというスクリプト言語で制御することで，アプリケーションを構築するというものである．HERMESはコンポーネントの状態や時間，各パラメータの状況に応じて処理を変更する機能を持っており，サービスの処理状況に応じて異なるコンポーネントオブジェクトが呼び出され，動的にサービスを構築することができる．こうしたHERMESの機能を利用し，利用条件許諾を実行時の状況に基づく条件分岐を行うスクリプトとして記述することで，ディジタルコンテンツの著作権管理に応用できるとしている．

現在までに，HERMESに基づく処理を行うためのAurora-compliantなコンポーネントの設計，ワークセッション管理サービス，リポジトリサービスを提供し，さらに各コンポーネントの処理を監視するロギングシステムが開発されている．

（10）Matryoshka（櫻井ほか）

Matryoshka[55),56)]は，ディジタルコンテンツとその

フォーマット情報，利用制約条件，コンテンツの説明などのコンテンツ関連情報と，カプセル全体の動作を統括し利用制約条件に基づきコンテンツを実際に表示・再生する機能（「コントロール」）を内包する実行ファイル形式のカプセルである．Matryoshka カプセルを実行すると，カプセル内のコントロールは，同じくカプセルに内包されているコンテンツ関連情報を読み込むとともに，実行環境をセンシングし，利用制約条件のチェックを行う．利用制約条件としては，利用者認証（端末限定），使用時間管理，使用期限管理，使用回数管理が可能になっている．条件が満たされた場合，コントロールは履歴情報の更新処理を行った後に，制約条件に基づいてコンテンツを出力する．通常，コンテンツおよびコンテンツ関連情報は暗号化処理がなされており，カプセルに内包されるコントロールのみが，必要な暗号復号化処理などの実行/コンテンツの正常な表示再生を行えるよう設計されている．このように Matryoshka カプセルは，コンテンツ自身に表現手段と利用制御機構をあわせ持つことで，どの流通過程においても，自律的にコンテンツの保護を行うことを可能にしている．

Matryoshka には，Active-X（Windows 専用）ベースの実装と，マルチプラットフォームでの動作をねらった Java による実装がある．さらに，cIDf で定義されたコンテンツ ID を Passive Safety 型の機能である電子透かしとしてコンテンツに埋め込み，またそのコンテンツの属性や特徴量などでの検索を可能とし，そのコンテンツを利用者に提供するときには，許諾された利用条件とともにカプセル化を行う統合的なコンテンツ管理システムも実用化されてきている[57]．

（11）EMO（木俵ほか）

EMO（Encapsulating Multimedia Object）[36)~42)] は，コンテンツをプログラムオブジェクト内にカプセル化してデータを隠蔽するとともに，処理メソッドに認証プロセスを付与して正規利用のみを認める，自律的な保護機能を持つコンテンツカプセルである．

EMO の特徴の 1 つに，利用者に応じて提供するサービスの内容やレベルを自律的に変更可能な点があげられる．この機能を利用することで，たとえば，3D CG データを内包するコンテナにおいて，ユーザの権利レベルに応じて表示される 3D モデルの詳細度を変更するというようなことができる．またこのような多レベルサービスを提供する際の課金方式として，EMO では，利用者の支払い範囲内でサービスを選択する課金モデル「サービスレンジ課金モデル」が提案されている．さらに，これらの機能を Web アプリケーションのコンテンツに適用した ESC（Encapsulating Synchronized Content）は，多レベルの SMIL コンテンツをカプセル化して，利用者ごとに適切な SMIL コンテンツを提供する機構を実現している．

4.3 今後の課題

前節では，ディジタルコンテンツ著作権を保護した利用形態として，ディジタルコンテンツはつねに著作者の管理下にあるサーバ上にのみ存在し，ネットワーク経由で理論的に単一のディジタルコンテンツを「共有」するモデルと，ディジタルコンテンツ自体の複製は可能だが，仮に著作物が複製されたとしても，その利用は必ず著作者の許諾のもとで行われることを何らかのかたちで保証する「複製」のモデルに大別し，具体的システムに例をもとにその特徴を述べた．

（1）利用形態および許諾条件の管理方式モデルの展望

今後ネットワークが高速かつ常時接続になり，サーバ間との通信の処理時間・コストが無視できるような理想系を考えた場合，単純にコンテンツを視聴するだけの提供型のサービスにおいては「共有」形態をとることによって，確実に著作権が管理できる安全なシステムが提供できていくと考えられる．しかし，以下の観点から「共有」形態のみでは不十分で,「複製」による利用を管理する方式が併用されていくと考える．

- 高速/常時のネットワーク接続が難しいモバイル/ユービキタス環境では，共有形態での利用制御は実質的に困難で，オフラインでも利用制御可能な自律的利用制御方式が今後も必要．
- 加工にともなう版管理まで含めたディジタルコンテンツのライフサイクル管理を考えると，まったく複製なしにこれを実現することは必ずしも妥当とはいえない．

後者については，加工プログラムが，1) 一次コンテンツのそれぞれのカプセルに設定されている加工時の条件や加工後再利用される部分に関する利用条件を継承して，2) 加工生成された二次コンテンツの利用条件をこれに加えて設定し，3) 再度カプセルとして生成することが必要である．これら一連の処理は「複製」形態を考慮した安全な処理系により行われ，その出力である二次コンテンツを再度管理するために「共有」形態のサーバを用いるようなハイブリッドな構成をとっていくのが現実的な解であろう．

（2）利用許諾条件の監視とプライバシー保護

Active Safety 型技術を利用して著作権保護を行う場合，利用状況を正確に監視しようとすればするほど，利用者のプライバシーに踏み込むことになる．たとえば利用履歴などの不用意な取得は，正当な利用者から

はプライバシー侵害と見なされる危険がある．プライバシーにかかわる情報の取得においては，次章で述べるような慎重な取扱いをしていかなければならない．

5. ま と め

本論文では，ディジタルコンテンツの流通過程における権利保護技術を，著作者の指定した利用許諾条件を管理し，可能な限り不正を未然に防止する技術（Active Safety 型）と，不正を検出/証明可能にすることによる抑止効果を狙った技術（Passive Safety 型技術）に分類し，現状の技術を総括，具体的なシステムの実例の紹介を行った．

ディジタルコンテンツのネットワークを介した流通に関しては，音楽の配信，映画の配信などをはじめ，実用化の段階に入りつつある．さらに冒頭で述べたように，今後の情報化社会においてはプライバシー情報やノウハウに類する企業の知識情報についても，適切な保護が保証された環境での流通促進が期待される．これらの情報の活用およびそのベースとなる保護技術の展望について考察を試み，まとめとする．

医療情報システム，福祉情報システムあるいは教育情報システムといった個人に密着したサービスにおいては，アクセス主体の目的を認証し，正当な場合のみプライバシー情報を提供する漏洩防止技術，あるいは被害を最小限におさえる予防技術が必須である．また，企業ノウハウ情報など，情報価値の高い知識の特定企業間共有，あるいは SOHO などにおけて個人から知識を発信するようなビジネスの形成などにおいてもやはり，利用条件や開示範囲などの制御が重要である．

これに対し，各情報に開示ポリシを記述可能とし，そのポリシを評価した結果，正しい目的として認証されたアクセス主体に対してのみ参照などを許す開示制御技術が実用化されている[58]．

開示制御によりアクセス時点での正当な参照が行われたとしても，いったん読み出されたプライバシー情報が，開示制御の及ばない範囲に転々流通することを防止することが必要となる．アクセス主体の目的を認証し，正当な場合のプライバシー情報を提供するなどの制御が可能なコンテンツカプセルなどの Active Safety 型技術は，その有効な手段となるであろう．

一方，これらの情報は，資格が与えられた者以外による加工・編集は基本的には許されない．したがって，ディジタルコンテンツ同様，不正な流通を抑止するためばかりでなく，情報自身が改竄されていないことの信頼性を高めるためにも，その情報がだれにより作成されたものであるかの特定や，改竄の検出技術などの Passive Safety 型技術が重要となる．具体的には

- 文字情報など冗長度の少ないメディアに対する電子透かし技術の展開とその検出手段
- 情報自身の原本性を保証するためのディジタル指紋技術および Active Safety 型技術との連携方式

などが，今後の課題と考えられる．

以上のように，ディジタルコンテンツの流通を中心に活発に研究開発が行われている各種の Active Safety 型技術・Passive Safety 型技術は，今後の情報化社会を支えるものと期待される．

謝辞 本論文をまとめるにあたりご指導いただいた NTT サイバースペース研究所・サイバーソリューション研究所および独立行政法人通信総合研究所の関連各位に深謝します．

参 考 文 献

1) 櫻井，瀬尾，塩野入：利用条件に基づく安全なコンテンツ提供方式，NTT 技術ジャーナル 2000 年 4 月号，pp.26–29 (2000).
2) 佐々木，吉浦：IT 革命下の著作権と違法コピー対策に関する考察，情報処理学会研究報告，CSEC-13 (2001).
3) 岸上順一：電子化知的財産とコンテンツ ID，情報処理学会研究報告，EIP 11-1, pp.1–4 (2000).
4) 中村，小川，高嶋：ディジタル画像の著作権保護のための周波数領域における電子透かし方式，1997 年暗号と情報セキュリティシンポジウム SCIS97-26A (1997).
5) 小川，中村，高嶋：DCT を用いたディジタル動画像における著作権情報埋め込み方法，1997 年暗号と情報セキュリティシンポジウム SCIS97-31G (1997).
6) 富岡，小川，中村，高嶋：音声への電子透かしパラメータの最適化について，1999 年暗号と情報セキュリティシンポジウム SCIS99-W4-2.7 (1999).
7) 松井甲子雄：電子透かしの基礎，森北出版 (1998).
8) 遠藤，小出：明るい社会を築く暗号—暗号は社会を変革する—コンテンツ配信と不正コピー防止，信学会誌，Vol.83, No.2, pp.117–121 (2000).
9) 斎藤直哉：デジタルコンテンツへの電子透かし応用—デジタルコンテンツ不正利用監視センターによる抑止効果，画像ラボ，Vol.9, No.10, pp.42–46 (1998).
10) 松井，高嶋：電子透かしの応用：一般利用者の協力に基づく海賊版データ摘発方法，1998 年暗号と情報セキュリティシンポジウム SCIS98-10.2C (1998).
11) 松井，高嶋：不正利用データ探索プロトコル，*NTT R&D*, No.6, pp.719–722 (1998).
12) 斎藤，沢戸，浦田，井上：電子透かしを用いたサ

ービスの現状，信学技報，Vol.97, No.565 (CQ97 70–79), pp.49–54 (1998).
13) 吉浦，今野，黒須：21 世紀を創造するマルチメディアシステム—電子透かしとその応用，日立評論，Vol.80, No.7, pp.511–516 (1998).
14) 中川，石塚，宮崎，中嶋：暗号・セキュリティ技術の現状と展望—情報セキュリティ—ディジタルコンテンツ流通技術，三菱電機技報，Vol.72, No.5, pp.424–427 (1998).
15) 山中喜義：電子透かし技術と課題について—著作権保護の切札!?，画像ラボ，Vol.9, No.7, pp.5–8 (1998).
16) IBM: http://www.trl.ibm.com/projects/s7730/Hiding/dhapp.htm
17) SYSCOP: http://www.sunmoretec.co.jp/products/syscop/index.html
18) M-ken: http://www.mken.co.jp/product/acuaporta.html
19) Digimarc: http://www.digimarc.com/about/index.shtml
20) Galaxy: http://pioneer.co.jp/press/release106-j.html
21) Millennium: http://www.macrovision.com/dvw.html
22) MarkAny: http://www.markany.co.kr/japanese/
23) 柏野，村瀬：音や映像を瞬時に探す時系列アクティブ探索法，*NTT R&D*, Vol.49, No.7, pp.407–413 (2000).
24) Nelson, T.H.: *Literary Machines*, Theodor H. Nelson (1981).
25) Nelson, T.H.: A File Structure for the Complex, the Changing and the indeterminate, *Proc. ACM National Conference* (1965).
26) RealSystem: http://www.realnetworks.com/realsystem/
27) Windows Media Rights Manager: http://www.microsoft.com/windows/windowsmedia/en/wm7/drm.asp
28) 森 亮一：ソフトウェア・サービスについて，JECC ジャーナル，No.3, pp.16–26 (1983).
29) Mori, R. and Kawahara, M.: Superdistribution: The Concept and Architecture, *Trans. IEICE*, Vol.E73, No.7, pp.1133–1146 (1990).
30) MetaTrust Utility: http://www.intertrust.com/main/metatrust/index.html
31) Cryptolope: http://www.ibm.com/software/cryptolope/
32) EMMS: http://www.ibm.com/software/emms/
33) RightsEdge (ContentGuard): http://www.contentguard.com/
34) RightsShell: http://www.digigacha.com/setumei/index.html
35) ZipLock: http://www.previewsystems.com/products/ziplock/
36) Kidawara, Y., Tanaka, K. and Uehara, K.: Encapsulating Multimedia Contents and A Copyright Protection Mechanism into Distributed Objects, *Proc. 8th International Conference on Database and Expert systems Applications* (*DEXA'97*), pp.293–302 (1997).
37) 木俵，田中，上原：版権管理のための Java による画像データカプセル化，情報処理学会研究報告，DBS 111-11, pp.73–80 (1997).
38) 木俵，杉山，田中：多レベル複合オブジェクトに基づく 3D デジタルコンテンツの課金モデルと版権管理，信学会論文誌，D-I, pp.201–210 (Jan. 1999).
39) 木俵，川口，角谷，田中：同期化コンテンツ制作・配信システムの開発と高速ネットワーク環境における配信実験，情報処理学会論文誌：データベース，Vol.42, No.SIG 8(TOD 10), pp.156–170 (2001).
40) 木俵，川口，角谷，田中：同期化コンテンツの動的生成管理と広告情報表示のための課金モデル，信学会データ工学ワークショップ (2000).
41) 杉山，田島，木俵，田中：集合デジタルコンテンツのサービスに基づく価値評価，信学会データ工学ワークショップ (2000).
42) 杉山，木俵，田中：3D デジタルコンテンツのサービスレベル制御，情報処理学会研究報告，DBS-116(2), pp.367–374 (1998).
43) Lagoze, C. and Kenney, A.R.: The Prism Project: Vision and Focus, Project Prism Working Paper (2000). http://www.cs.cornell.edu/prism/Publications/WorkingPapers/Visions.htm
44) Lagoze, C. and The Cornell Digital Library Research Group: Architectures and Policies for Distributed Digital Libraries. DLW17 (2000). http://www.cs.cornell.edu/lagoze/papers/DLW17/cdlrg.htm
45) Payette, S. and Lagoze, C.: Flexible and Extensible Digital Object and Repository Architecture (FEDORA), *Proc. 2nd European Conference on Research and Advanced Technology for Digital Libraries*, pp.41–59 (1999).
46) Lagoze, C., Lynch, C.A. and Daniel, R.: The Warwick Framework: A Container Architecture for Aggregating Sets of Metadata, Cornell Computer Science Technical Report TR96-1593 (1996).
47) Daniel, R. and Lagoze, C.: Distributed Active Relationships in the Warwick Framework, *Proc. IEEE Metadata Conf., Bethesda* (1997). http://computer.org/conferen/proceed/meta97/papers/rdaniel/rdaniel.pdf

48) Marazakis, M., Papadakis, D. and Nikolaou, C.: Aurora: An Architecture for Dynamic and Adaptive Work Sessions in Open Environments, *Proc. International Conference on Database and Expert Systems Applications* (*DEXA'98*), Springer-Verlag LNCS Series. (1998).
49) Marazakis, M., Papadakis, D. and Nikolaou, C.: The Aurora Architecture for Developing Network-Centric Applications by Dynamic Composition of Services, TR97-0213, Institute of Computer Science, FORTH (1997).
50) 北川善太郎：マルチメディアと著作権—コピー・マート：著作権市場論，信学会誌，Vol.77, No.9, pp.933–935 (1994).
51) Content ID Forum: http://www.cidf.org/
52) XrML: http://www.xrml.org/
53) MagicGate/OpenMG: http://www.openmg.com/
54) CPRM: http://www.4centity.com/tech/cprm/
55) 谷口，森賀，久松，櫻井：マルチメディア情報ベースとその格納単位 Matryoshka，情報処理学会 DICOMO シンポジウム，pp.207–212 (1999).
56) 阿部，谷口，塩野入：Java を用いた動画配信カプセルの実装，情報処理学会 DPS ワークショップ，pp.229–234 (2000).
57) 西岡，大竹，瀬尾：コンテンツ流通情報管理機構の実現，情報処理学会研究報告，DPS 102-14, pp79-84 (2001).
58) 山本，寺西，梅本：医療情報システムにおける情報開示制御方式，情報処理学会研究報告，DPS 100-4, pp.19–24 (2000).

(平成 13 年 6 月 25 日受付)
(平成 13 年 9 月 27 日採録)

（担当編集委員　安達 淳）

櫻井　紀彦（正会員）

1979 年早稲田大学理工学部電気工学科卒業．同年日本電信電話公社（現 NTT）入社．ファイル記憶階層アーキテクチャ，マルチメディアデータベース，コンテンツ流通管理・保護システムの研究開発に従事．電子情報通信学会，映像情報メディア学会各会員．

木俵　豊（正会員）

1988 年神戸大学工学部計測工学科卒業．1990 年同大学大学院工学研究科修士課程修了．同年（株）神戸製鋼所入社．製鉄所生産管理データベース，コンテンツ流通管理システムの研究開発に従事．1999 年神戸大学大学院自然科学研究科博士課程修了．工学博士．2001 年独立行政法人通信総合研究所入所．次世代インターネットに関する研究開発に従事．IEEE Computer Society，システム制御情報学会等各会員．

高嶋　洋一（正会員）

1985 年横浜国立大学工学部情報工学科卒業．1987 年同大学大学院博士課程前期電子情報工学専攻修了．1990 年同大学院博士課程後期修了．同年 NTT 入社．画像符号化，情報セキュリティに関する研究開発を経て，現在，著作権保護システムに関する研究開発に従事．電子情報通信学会会員，情報理論とその応用学会会員．

谷口　展郎（正会員）

1968 年生．1992 年東京大学工学部機械工学科卒業．1994 年同大学大学院工学系研究科機械工学専攻修士課程修了．同年 NTT 入社．以来，画像検索システムネットワーク情報流通システム等の研究開発に従事．

難波　功次

1997 年大阪大学工学部電子工学科卒業．1999 年同大学大学院電子工学専攻修士課程修了．同年 NTT 入社．以来，コンテンツ保護システムの研究開発に従事．