情報処理最前線

ディジタルコンテンツの権利保護と流通

申　吉浩　　青沼英一
富士ゼロックス（株）

脚光を浴びるディジタルコンテンツ流通

音楽CDの流通など既存の事例にもかかわらず，最近になってにわかに「ディジタルコンテンツ流通」が脚光を浴びるようになった背景には次の2つの事由がある．

第1に，エレクトロニックコマースの進展により新たなビジネスチャンスが創造されつつあることがある．1997年にはクレジットカード会社を中心としてSET（Secure Electronic Transactions）規格[1]が制定され，インターネット上での電子決済が普及する日も遠くはないと予感させる．SET等を用いた電子決済プラットフォームの実現は，インターネットビジネスを拡大する上で従来ボトルネックとなってきた安全上の問題を一掃し，こと決済手段に関しては市場の潜在能力を飛躍的に高める．このような情勢の中で，インターネットで直接売買できる商品，すなわち，ディジタルコンテンツが21世紀のビジネスの種として注目を集めるのは自明の理である．ゲームソフトやオーディオ・ビデオなど，エンターテイメントを中心に魅力のあるディジタルコンテンツ商品の品揃えはすでに十分であることから，ディジタルコンテンツ流通の仕組みの登場が待たれている．

第2に，PCとその周辺機器，そして，インターネットの急速な普及が，ディジタルコンテンツの著作者の権利に対する大きな脅威となってきたことがある．今や，CDに記録されたデータを編集し複製することはPCさえあれば誰にでも可能であり，さらにインターネットを利用すれば海賊版データを大規模に流通させることもできる．このように，ディジタルコンテンツの著作者の権利を保護する仕組みの確立は既存の事業を守るためにも必須であり，「著作者の権利保護」を実現するディジタルコンテンツ流通システムの実現が焦眉の課題となっている．

本稿は，ディジタルコンテンツ流通システムに関して，その実現に必要な基礎的な技術の概説と，事業的な観点からの業界の動向について報告する．

著作者の権利保護を実現する技術の目的と分類

本稿では，ディジタルコンテンツ流通システムが提供すべき最優先の機能は著作者の権利保護であると捉え，「著作者の権利保護」に焦点を当てて技術の解説を行うこととする．

ディジタルコンテンツ流通における著作者の権利保護の技術は，以下の機能を提供することを目的とする．

(1) 著作者が望むユーザと望まないユーザとを識別し，前者にのみ選択的に効用を提供する．
(2) ディジタルコンテンツが再流通可能なディジタル形式で漏洩することを防止あるいは抑止する．

本稿では著作者の権利保護技術（機能）を以下の3つに分類することとする．

①アクセス制御技術（アクセス制御機能）
ユーザによるコンテンツへのアクセスを制御し，正当なユーザによるアクセスのみを許可する．

②コンテンツ保護技術（コンテンツ保護機能）
ユーザの利用に供されている過程において，コンテンツが漏洩することを防止する．

③追跡技術（追跡機能）

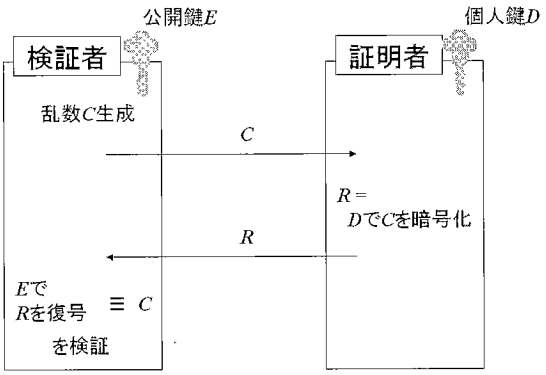


図-1　公開鍵暗号ベースの認証

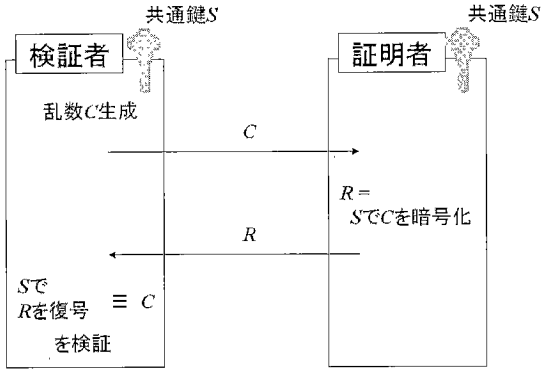


図-2　慣用暗号ベースの認証

万が一コンテンツが再流通可能な形式で漏洩した場合に備えて，追跡のための手段を提供する．

アクセス制御技術

ディジタルコンテンツ流通システムにおけるアクセス制御技術は，暗号技術の応用である認証技術と鍵配送技術とを用いて実現される．ディジタルコンテンツ流通システムでは，コンテンツの利用資格を表現する電子データ（利用資格データ）を何らかの形でユーザに発行するが，認証技術はこの利用資格データをユーザが保持していることを確実に確認するための技術である．一方，鍵配送技術は，利用資格データをユーザに安全に配達するために使われる．

■認証技術

認証技術では，検証者と呼ばれるエンティティと証明者と呼ばれるエンティティが電子的にメッセージを交換する過程で，検証者が証明者を識別する．

認証技術は，公開鍵暗号をベースとするものと，慣用暗号をベースとするものの2つに大別されるが，いずれも，「証明者は特定の秘密情報（実際には暗号の鍵）を保持し，検証者は証明者が秘密情報を保持していることを検証する」という枠組みを共有している．

公開鍵暗号を用いた認証[2]では，公開鍵（Public Key）と個人鍵（Private Key）の2つの鍵をペアとして用いる．このうち個人鍵が証明者の秘密情報であり，検証者は公開鍵を用いて検証を実行する（図-1）．

公開鍵暗号の本質的な特徴は，公開鍵に関する情報から個人鍵を算出することが事実上不可能である点にある．すなわち，認証の安全性を確保するために公開鍵を秘密にする必要はない．この特徴を利用すれば，いっさい秘密の部分を持たない検証システムの構築が可能であり，したがって，開発やインテグレーションが自由に行えるオープンなシステムを構築することが可能となる．

一方，慣用暗号はメッセージの暗号化と復号に同一の鍵を用いる暗号方式である．したがって，証明者が暗号の鍵を秘密情報として保持する一方，検証者も同一の秘密を共有する（図-2）．

公開鍵暗号の代わりに慣用暗号を用いる利点は，システムの構成を簡素化することができる点にある．ディジタルコンテンツ流通システムでは，コンテンツは暗号化されて配信されユーザが利用する時点で復号されるが，効率の観点から暗号方式としては慣用暗号が利用される．このとき，利用資格データとコンテンツを復号するための鍵とを共通とすることで，システムの簡素化を図ることができるのである．

■鍵配送技術

前節では，ディジタルコンテンツの利用資格を表現するデータとして暗号の鍵が用いられることを見たが，ここではその鍵をユーザに「安全」に配送するための技術を説明する．

古典的な鍵配送技術における「安全性」とは，鍵が通信路上で安全であることを意味する．盗聴などによって鍵が攻撃者に漏洩すると，「なりすまし」によるコンテンツの不正利用を許すこととなるからである．

通信路上での鍵の安全に対しては，鍵（利用資格データ）を暗号化して配送することで，通信路上で平文の鍵が現れることを防ぐ方法がとられる．「鍵配送センタ」を仮定して鍵を暗号化するために用いるユーザ個別の鍵を集中管理するDenning-Saccoのような方式（図-3）と，公開鍵暗号の特徴を利用することでセンタ機能を不要とする方式とがある．

さて，ディジタルコンテンツ流通では，利用資格データである暗号の鍵を通信路上で保護するだ

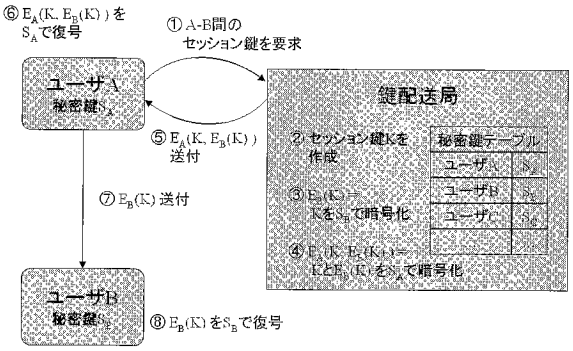


図-3　Denning-Saccoの鍵配送方式

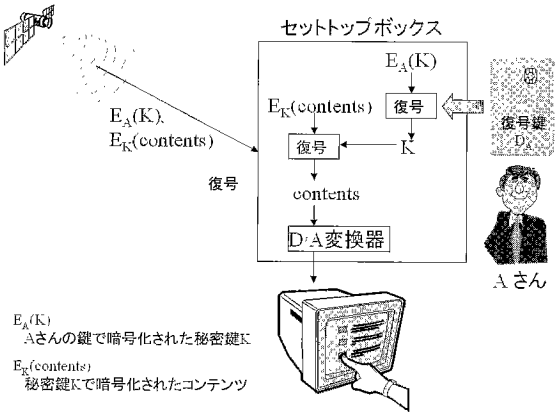


図-4　有料衛星放送における例

けでは不十分である．復号した鍵を受信者が複製することでコンテンツの不正利用が可能となるからである．ディジタルコンテンツ流通システムでは，通信路上での鍵の保護に加えて，以下の鍵保護機能を備えている必要がある．

(1) 利用資格データである鍵が受信ユーザに対しても漏洩しない．

(2) 利用資格データを復号するためにユーザ個別に設定されている鍵が，所有者であるユーザに漏洩しない．

上記の鍵保護機能をどのように実現するかについては，「安全」なハードウェアをどの程度前提とできるかによって，その答えが違ってくる．

たとえば，有料衛星放送では，セットトップボックスと呼ばれる受信機とユーザ識別のためのICカードによって，上記の鍵保護の機能を提供している例がある．コンテンツの復号鍵（利用資格データ）は暗号化されてから，衛星を経由してセットトップボックスに配信される．この鍵はセットトップボックス内で安全に復号され，使用されるが，鍵の復号にはICカード中に安全に格納されたユーザ固有の鍵が使用される（図-4）．

他方，ディジタルコンテンツの受信・再生に通常のPCのみを用いる場合は，ハードウェアによる保護機能をいっさい期待することはできない．そのため，鍵を保護する機能をソフト的に構築せざるを得ない．

「安全」なハードウェアとしては，マイクロコンピュータを内蔵したICカードがコスト的・実用的な観点から注目されており，電子マネーなどにも利用されている．端子を介した入出力を内蔵のマイクロコンピュータが管理することで，不正なアクセスを拒否する機能を有している．ハードウェアの安全性をさらに高めるためには，耐タンパ技術[3]（tamperとは改変の意味）が用いられる．耐タンパ技術は，「パッケージに孔を開ける」，「特定の端子に異常電圧・パルス信号を印加する」などの攻撃を検知して，不正行為を未然に防ぐ機能を提供する．

ソフト的に鍵保護機能を構築する際には，ソフトウェアの解析行為を困難化することを目的とする耐タンパソフトウェア技術を用いて実装を行う．耐タンパソフトウェア技術については次章で解説する．

コンテンツ保護技術

通信路上でコンテンツを保護する手段として，ディジタルコンテンツを暗号化して配信する方法はすでに広く用いられており，ディジタルコンテンツ流通システムでの前提として考えてよかろう．そこで，ここでは，ディジタルコンテンツが利用される局面での保護に焦点を当てて解説を行う．前章と同様，コンテンツ利用の保護も，安全なH/W・デバイスをどの程度仮定できるかで，方法は異なってくる．ここでは，通常のPC上で動作するソフトウェアによってディジタルコンテンツの利用が提供される，安全上最も厳しいケースに焦点を絞ることとし，ソフトウェアの保護機能を提供する耐タンパソフトウェア技術について解説する．

暗号化されたディジタルコンテンツは，必ず復号されたあとで利用に供される．暗号を解読する行為は一般に困難とされているので，攻撃者は，暗号化されたディジタルコンテンツが復号された状態あるいはその復号の過程を攻撃して平文のコンテンツを取り出すことに可能性を見出すであろう．耐タンパソフトウェア技術は，コンテンツを復号するソフトウェアプログラムや復号されたコンテンツを処理するソフトウェアプログラムを，攻撃者による解析行為から保護するための技術である．

耐タンパソフトウェア技術の特徴として以下を挙げることができる．

(1) 保護レベルを上げるに従って，特定のプロセッサ・OS・プログラミング言語に依存した技術

分類	攻撃手法（プログラム解析手法）	使用するツール	耐タンパS/W技術を用いた防御方法
静的解析	コード自体を人手で解読する	ディスアセンブラ	コードの難読化 自己コード生成（Self Code Generation）
動的解析	攻撃対象のプログラムの実行を中断し，メモリ上の情報を解析する	ソフトウェア／ハードウェアレベルでの割り込み	再暗号化／平文データの破棄
	ブレークポイント設定やステップ実行により，プログラムの動作を解析する	アプリケーション／システムレベルのデバッガ	解析行為の検知
	特殊なハードウェアを利用し，実行命令列を解析する	プロセッサエミュレータ，バスロジックアナライザ	なし

表-1　攻撃手法と耐タンパソフトウェア技術を用いた防御方法

となる．

(2) 攻撃に要するコストを定量的に評価する尺度を見つけにくく，安全度を定量的に表現できない．

このように，耐タンパソフトウェア技術は，研究対象としては取り扱いにくい題材ではあるが，PCとインターネットを前提としたディジタルコンテンツ流通システム構築のためにはきわめて重要な技術となるであろう．表-1に攻撃手法と耐タンパソフトウェア技術を用いた防御方法についてまとめる．

■静的解析に対する防御

静的解析とは，取得したプログラムのコードを人手で解読する攻撃を指す．

この解析行為への対策の1つとして，①プログラムの制御構造の複雑化，②冗長コードの挿入，③命令コードの置換などにより，人間によるコードの理解を困難化する難読化技法がある．

さらに強力な防御手段としては，自己コード生成（Self Code Generation）が知られている．自己コード生成とは，次に実行すべきコードをプログラムの実行中に生成するようにプログラムを構成する手法である．暗号化したコードをプログラムの実行中に復号して実行する方法も，自己コード生成の手法に含まれる．

■動的解析に対する防御

自己コード生成などの手法で保護されたプログラムを解析するには，プログラムを実行させて解析する方法が有効となる．

最も単純な攻撃手法として，割り込みを用いたアタッチメントと呼ばれる方法がある．これは，適当なタイミングで攻撃対象のプログラムに割り込みをかけてその実行を中断し，メモリ上に展開された平文のデータやコードを取り出すことを目的とする．アタッチメントに対する対策としては，利用時に復号したデータや自己生成したコードを再暗号化あるいは破棄し，メモリ上に平文で存在する時間を最小化する方法がある．この防御を施すことにより，攻撃者は割り込みのタイミングを正確に選択しなければならず，次に述べるデバッガによるブレークポイントの設定等の手法をとらざるを得なくなる．

より高度な攻撃手法としては，アプリケーションレベル／システムレベルのデバッガを用いてプログラムの実行に干渉を行い，ブレークポイントを設定したり，実行ステップをトレースすることでプログラムの動作を解析する方法がある．この攻撃に対しては，プログラムの実行への干渉によって生じるPC中での環境変化を検知することで防御を行う．

プロセッサエミュレータ（Processor Emulator）やバスロジックアナライザ（Bus Logic Analyzer）のような特殊なハードウェアツールを利用する，より強力な攻撃に対しては，ソフトウェアによる防御方法は原理的に存在しない．ただし，これらのツールは特殊であるがゆえに高価である．また，ツールによって得られるデータにはOS・アプリケーションを問わずプロセッサによって処理されるすべての命令・データが含まれるので，攻撃目標のソフトウェアプログラムに関連するデータを抽出して解析するコストは非常に大きい．これらの理由から，通常のディジタルコンテンツを扱う場合に限り，これらのツールを利用した攻撃による危険は除外してもよいと考えられている[4]．

追跡技術

ディジタルコンテンツがPCを用いてレンダリング（印刷・演奏など）される場合，前章で説明したコンテンツ保護だけではディジタルコンテンツを完全に保護することはできない．

たとえば，ディジタルコンテンツを汎用のプリンタで印刷することを許した場合，プリンタドライバ経由で印刷データをファイルとして出力する行為を禁止する手段はない．同様に，音楽データはサウンドボードによってD/A変換されて演奏されるが，サウンドボードに入力されるべきディジタルデータが流出する可能性を排除することはで

きない．

このように，レンダリングのために生成されたディジタルデータの流出を完全に防止することは，現状のPCアーキテクチャを前提にする限り不可能である．そこで，流出したコンテンツが大量に流通することを抑止することを目的にコンテンツに著作権情報等の追跡情報を埋め込む技術として，電子透かし技術[5]が知られている．

ディジタルコンテンツの種別（音声・静止画像・動画像）によって，情報の埋め込み方式は異なるが，電子透かし技術は以下に述べる共通の要請を満たす必要がある．

(1) 攻撃者による電子透かしの除去は大幅な品質の低下を伴う．
(2) D/A・A/D変換，印刷・スキャン，圧縮・伸長，各種フィルタなどのデータ変換を施しても，埋め込まれた情報を取り出すことができる．
(3) ディジタルコンテンツの一部からでも埋め込まれた情報を取り出すことが可能である．

コンテンツの種類や適用領域によっては，さらに，透過性とよばれる次の性質を満たす必要がある．

(4) 情報の埋め込みによって生じる品質劣化は，人間が通常感知できないほど小さい．

一般に，これらの条件を高いレベルで満たす電子透かし技術の実現には，困難な技術開発を伴う．

たとえば，音楽データなどに追跡情報を埋め込む場合には，透過性の要求を満足することが必須となる．透過性を実現するには，人間の聴覚・視覚特性を利用し，比較的鈍感な領域に追跡情報を埋め込む手法がとられる．しかし，ある種の圧縮方式では，やはり人間の官能特性を利用してデータの間引きを行うため，追跡データが破壊されてしまう危険がある．

また，印刷された画像イメージを再びスキャンしてディジタル化する場合，現在の技術では紙面とスキャン方向との角度のずれがある一定以上大きいと，追跡データが復元されないことも知られている．

このように，現状では，耐タンパソフトウェア技術の場合と同様，電子透かし技術も対象とするディジタルコンテンツに一定の留保を設けた上で実用に供さざるを得ない．

今後の技術開発上の課題

この章では，今後ディジタルコンテンツ流通システムを発展させていく上で，筆者が重要であると考えるポイントを2点述べる．

■オープンアーキテクチャに基づくアクセス制御プラットフォームの提供

ディジタルコンテンツ流通システムを構成する3つの機能（技術）のうち，コンテンツ保護および追跡に関する機能は，ディジタルコンテンツの種別や価値などの固有の特性に依存して適用方式を変化させる必要がある．それに対し，アクセス制御機能は個別のディジタルコンテンツの特性から超越した汎用の機能として実現することが可能である．

この特徴を活用して，アクセス制御機能をコンテンツ保護や追跡の機能から分離した独立のプラットフォームとして提供すること，さらには，公開鍵暗号の利用によりオープンアーキテクチャとすることで，以下のメリットが提供される．

(1) プラットフォームの上に個別のシステムを構築することにより，システム開発および運用のコストを低減することができる．
(2) サードベンダによるシステム開発が促進され，多様性や変化に対する柔軟性が生まれる．

これらのメリットは，ビジネスとしてのディジタルコンテンツ流通を加速する原動力となる．

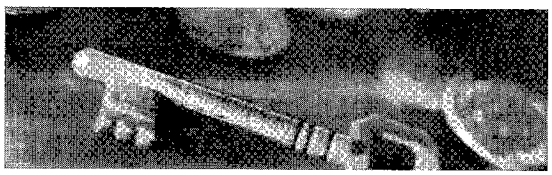
■「安全」なソフトウェアのための開発環境の提供

今後も，PCおよびインターネットがエレクトロニックコマースの基本的なインフラストラクチャを構成していくことを考えると，耐タンパ性を有する「安全」なソフトウェアの普及はきわめて重要である．そのためには，耐タンパソフトウェアの開発環境が広く提供されなければならない．

米Intel社が耐タンパソフトウェアのためのアーキテクチャを発表している[4]ほか，数社に上る企業が耐タンパソフトウェア技術を保有しているとされているが，これらはDVDドライバなど特定のソフトウェアへの適用に限定されているのが現状である．

耐タンパソフトウェアの開発環境を提供するためには，次の技術課題を解決しなければならない．

(1) 開発環境が解析されることで，耐タンパ性を破るためのヒントが与えられない．
(2) 環境に落し戸（trap door）が存在しないことが，アプリケーション開発者によって確認できる．



業界動向

この章では，ディジタルコンテンツ流通を進める上で著作者の権利保護のための技術を必須としている代表的な業態とそこでの動向について紹介する．

■出版業界と電子書籍コンソーシアム

出版社主導で，出版社・取次・書店から73社，その他印刷・通信・メーカを加えた合計130社が参加して，1998年10月に「電子書籍コンソーシアム」が設立された．衛星通信を用いて物流経費を大幅に削減し，高精細液晶からなる読書端末を普及させて新しい読書文化とニーズを創出することを狙っている．

電子化した出版物を流通させる場合，特に商品価値の高い人気タイトルを取り扱う場合には，著作者の権利保護のための技術の重要性が高まる．最近ようやく，コピー防止などの不正対策技術にメドがつきつつあり，富士通（株）と（株）日立製作所の技術をそれぞれ利用した大日本印刷（株）の「BookWorld West/East Floor」や，自社の技術を用いた富士ゼロックス（株）の「インターネット有報」など，ディジタルコンテンツをインターネット上で販売する企業が出現してきている．

同コンソーシアムでも，著作権処理部会で著作権処理に係るシステムの標準化等が検討されており，電子書籍市場の確立と発展に向けて今後の進展が期待される．

■音楽業界とディジタル配信

楽曲のディジタル配信はリスナとアーティストの双方が求めている大きな流れであるが，業界の対応の遅れにより，すでに大量のMP3ファイルが全世界で無料でダウンロードされており，社会的に大きな問題となっている．

楽曲をディジタル配信するにあたっては，著作者の権利保護のための技術が不可欠であり，業界各社がそれぞれ活発な動きを見せている．特に，1999年2月には各社のプレスリリースが集中した．

レコード会社を自社系列に持つソニー（株）は，「Super MagicGate」と銘打った著作権保護技術を開発し，世界の大手レコード各社に採用を働きかける．また，米IBM社は電子透かし技術等を用いた配信システム「Electronic Music Management System」を開発し，米国の大手レコード会社5社と，ダウンロード販売実験を開始する．いずれも，今後，米国のディジタル音楽著作権保護団体（SDMI）を巻き込む形で展開していく．

一方，NTT（株）と（株）神戸製鋼所は，共同開発した携帯用音楽プレイヤ「SolidAudio」とNTT（株）の情報流通プラットフォーム「Infoket」，（株）東芝による固有の識別番号（ID）付きスマートメディアを利用した，ディジタルコンテンツ流通方式「InfoBind」を共同で開発した．また，すでに独自の暗号化や著作権管理技術を持つ米Liquid Audio社は，米Texas Instruments社と共同で，携帯用音楽プレイヤを開発すると発表した．

音楽データはコンテンツがグローバルな分だけ，世界規模での開発競争・主導権争いが起きており，その喧騒は当分収まりそうにない．

■伝統産業と京都デジタルアーカイブ推進機構

1998年8月に「京都デジタルアーカイブ推進機構」が設立されたが，同機構には伝統産業事業者・大学・研究機関など計66の個人・法人のほか，新産業の創出をもくろむ40の企業が参加した．対象となる西陣織や京友禅，京縫の業界は，和装離れの進行に加え，景気の低迷で深刻な経営状況にあり，これまで眠っていた意匠等の財産を再活用する途を模索することで活性化を目指す．

ただ，寺社や地元企業には，不正コピーの氾濫や品位のない使われ方をするのではないかという懸念があり，ディジタル化に対するアレルギーは依然として強い．美術館や博物館，カメラマンといった所有者や著作権者には電子透かし技術だけではその抑止効果は不十分とみられており，ここでもコンテンツ保護と認証のための技術の確立が強く望まれている．

同機構に参加している（財）比較法研究センターでは，著作物の流通のための法モデルとして「コピーマート」という考え方を提唱している[6]が，ディジタル著作物を公開する際の著作権問題，特に著作者人格権としての同一性保持権の取り扱いがこの場合議論となろう．同機構における，ディジタル化に伴う知的所有権に関する諸課題の研究の進展が期待される．

参考文献

1) The SETTM Standard, http://www.setco.org
2) ITU-T X.509, The Directory－Authentication Framework (1988).
3) Anderson, R.J. and Kuhn, M.G.: Tamper Resistance－A Cautionary Note, in The Second USENIX Workshop on Electronic Commerce Proceedings, pp.1-11 (Nov. 1996).
4) Aucsmith, D. and Graunke, G.: 逆解析や改変からソフトを守る, NIKKEI ELECTRONICS 1998, No.706.
5) 井上　彰: 電子透かし, 丸山学芸図書 (1997).
6) 北川善太郎他: マルチメディア時代における著作物の権利処理と流通に関する総合的研究, 総合研究開発機構 (1997).

(平成11年4月1日受付)