社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2003－ EIP－21 (1)
2003／11／29

超流通の実現に向けて

吉岡 誠
有限会社 ａＩＰｉｄ（アイピッド），MMG,富士通 PST

【概要】森先生のオリジナルである超流通はその発表から２０年が経過しようとしている。パソコンの黎明期のプログラムの違法複製利用の阻止の解決がトリガだったが，あらゆる表現媒体のデジタル化が当たり前になった現在，これらの媒体を利用したあらゆるデジタル創作物の違法複製利用を阻止する技術の開発が求められている。一方創作物は，放送・通信などの経路媒体およびパッケージ媒体としてのＣＤ，経路媒体から格納するためのＨＤなどの蓄積媒体で流通されるが，違法複製利用阻止はこれらの媒体に対し適用される必要がある。本メモでは従量課金を基本とする超流通の実現に向けた，筆者の活動の歴史と提言を紹介する。

An incremental approach to implement practical Superdistribution with consistency

Makoto YOSHIOKA
aIPid Limited, MMG, Fujitsu PST

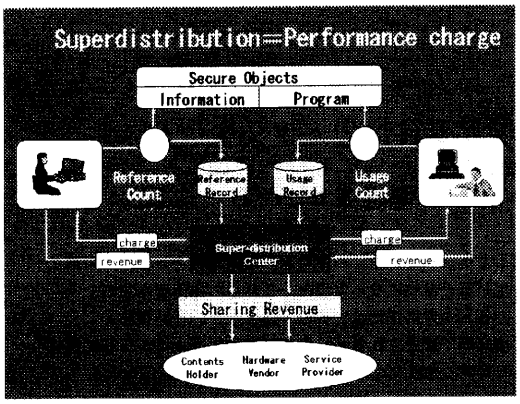
【Abstract】Superdistribution was originated around 20 years ago by emeritus professor Mori of Tsukuba University. The trigger was to solve the problem of illegal copy of software programs. Nowadays all the contents created by the creator could be expressed in digital. Therefore we should develop the technology which is applicable to all the media expressed in digital. Created contents using multiple media format is distributed to consumers through a conduit type media(broadcasting and communication) and storage container type media(like CD-ROM and rewritable storage like removable HD). The protection technology shall be applied to all the media existing in between the creator side to consumer side. This article will summarize the experience that the author has been trying to implement the Superdistribution and propose the next step.

1 はじめに

筆者はパソコンの開発，SGML の実用化の推進，光ディスクの論理形式の標準化，更には XML をベースにしたデジタルテレビの形式の標準化など，違法複製利用阻止を，常に考えざるを得ない分野の仕事をしてきた。パソコンのフロッピの時代から，プログラムの違法複製利用は盛んで，ある時，ソフトベンダの社長が，この問題をなんとか解決して欲しいと筆者にお願いにきた。この時から課題解決への挑戦が始まったが，幸いちょうどその頃森先生が電子協で SSS(Software Support System)という委員会を起こし当該テーマへの挑戦を開始したので，筆者も参加した。その後，これはより一般化した名前として，先生とブラッドコックスにより，超流通と命名されたが，その思いは，超伝導との対比で言うならば，デジタルコンテンツをフェアに流通させるためのあらゆる阻害をゼロにするということである。先生の委員会への出席と並行して，一つ一つ課題を解決しながら，超流通の実現に挑戦してきた。本文では，この経緯を紹介することにより，関連テーマに挑戦している方々に資することにしたい。更に，ｅＬｉｆｅの中の重要なテーマであるコンコンツ保護については，日本の各分野の良識を集めて，日本がリードして，その仕様を決めるための提言を述べる。

2 パソコンの視点で

1980 年代初等，パソコンは仕様がオープンであったことから，急速に普及した。そのため，違法複製利用の巣窟となった。現在でもその状況は変わらない。この問題の解決をするため，SSS 委員会に参加した。森先生には「歴史の必然としての超流通」という，有名な論文があり，タイトルもさることながら，その中身に感動した。百科事典のような有体物は，所有していることにも価値を人間は見いだしているが，これがデジタル化され，無体物となった場合には，簡単に複製が可能なので，所有していることには意味がなく，利用または参照した時にはじめて価値がでる。



従って，電気とかガスとか水のように，利用した量に応じて課金（従量課金）こそがふさわしいとした。そうだとすると，端末側に堅牢な課金メータがいるわけで，これをどうやって実現するかが，一つの課題であった。課金メータの利用実績は，利用量とか，定期的にとか，プリペイ料金を使い切った時とかに超流通センタにアップし課金処理をして，コンテンツ制作，流通などにかかわった関係者に分配すべきとしたが，特筆すべきことは，端末側に堅牢な課金メータを実装させるとすると，当然端末メーカにはコストアップ要因になるので，端末メーカに，堅牢な課金メータを実装してもらうためのインセンティブとして収入の一部を分配すべきであると主張されたことである。

先生の委員会に出る一方，超流通の実現に向けた研究も開始した。 1977年にアラン・ケイのダイナブック関連の論文を読んで，感動を覚えた筆者は当時光ディスクの可能性にも目をつけており，将来のパソコンのイメージを描きパソコンに搭載する光ディスクをギガＲＯＭと名前を付けた。現実的には650MBのCD-ROMが登場したので，これを搭載したパソコンを超流通を実現した形で市場に登場させることを企画した。これが1989年にCD-ROMを世界で最初に搭載したHypermediaパソコンとして登場したFM-TWONSである。

FM-TOWNSでは，超流通の出発点として，従量課金までの実装はあきらめ，先ずは一度許諾を発行すれば，後はずっと利用可能なモデルを実現するために，コンテンツは暗号化をし，その暗号化キーを含んだ許諾情報を個別のTOWNS毎に一意にするために，個々のTOWNSに識別IDを装備してもらった。このようにすることで，暗号化されたコンテンツの複製は自由であるが，個別のTOWNSはそれぞれ識別IDと連動した許諾情報をもらわないとコンテンツを利用できないようにした。

残念ながら，当該システムは事業部側で実装は終わったものの，販売サイドがソフト流通の既存チャネルとコンフリクトを起こすので，実施はまかりならぬということで，市場には登場させることはできなかった。

3 SGML/光ディスクの時代

1990年代になって，情報処理の歴史的発展をレビューしながらデータプロセシングの次なる発展の場としてグループウェアを含めた通信を活用した情報および知識の共有（通有）を容易にするインフラを構築すべくSGMLの実用化に向けた活動を積極的に推進した。関心は文書処理で皆がこだわる印刷体裁よりは，文書を論理的に構造化することによる，構造情報を利用した，文書の整理，自動処理の向上，端末表示体裁定義を独立させることによる端末を利用したデータ処理アプリケーションの開発の簡易化の方に関心があった。このビジョンはXMLで完全に実現されるようになった。

一方，3.5”MOの事業化を推進していた同僚から，光ディスクの論理形式の標準化を依頼され，日本が幹事国になってISO13346を策定し，これを傘として光協会/OSTAでUDF，Secure UDFという形で標準化を進展させてきた。

ISO13346はROM/R/RAMを一つのファイル形式でカバーするが，常時寄与していたのは５人ぐらいで，一方，Ｒだけを意識したファイル形式の標準化も並行して実施されており，５０人ぐらいが参加

していた。こちらの形式は非常に汚かったので，実用にはならないのではないかと思っていた。結局は現在はUDFで全てがカバーされている。人が多く集まれば，業界に採用される標準ができるわけでは無い，やはり仕様の内容が大切であるということを体験した。

実は日本の家電はDVD-ROMはCD-ROMの形式であるISO9660の延長の形式を考えていた。これに対し，米国のIT業界が，次のようなことを言ってUDFへの流れを作った。

「ROMだけを作るなら良いが，R/RWも作るのなら，ファイル形式は再考が必要である。孫がR/RAM媒体を扱える装置で編集した結果をR/RAM媒体でROMリーダしか無い祖母のところに送付しても読めるようなファイル形式を採用すべきで，UDFを利用すれば，それが出来るではないか」

実際には物理形式の互換性も重要で-/+,R/RWと各種形式が登場，光業界は混乱をしている。

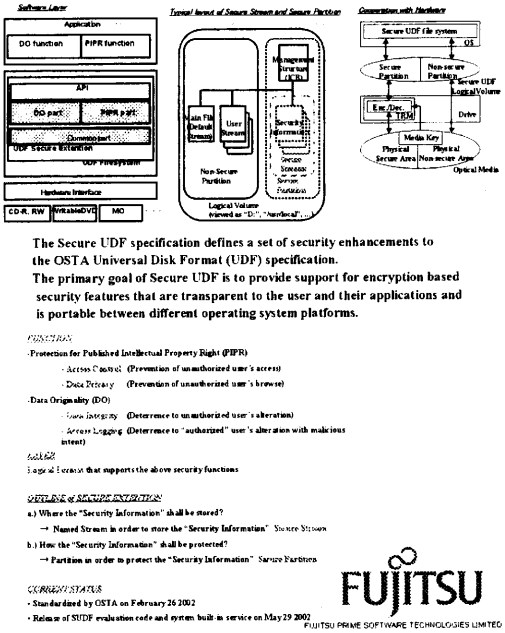
超流通の視点からは，個別の光ディスク毎に許諾情報を一意にするために，光ディスク媒体毎に一意の媒体IDを付与することをお願いした。提案してから10年ぐらい経過した現在では，ほとんどの光ディスクがなんらかの形で媒体IDが付与可能になってきた。喜ばしいことである。

残念ながらDVD-ROMの著作権保護システムはPCで簡単にブレークされ。現在，その被害がホールダ側で問題視され始めている。暗号化技術のプロは当初からこの事態を想定していたが，ブレークされるのは予想より早かった。森先生の提案の如く，ドライブベンダ側にもマージンを落とす前提で堅牢なシステムの実装がされていればと悔やまれる。

FM-TOWNSにCD-ROMを搭載した後1993年にマッキントッシュがCD-ROMを搭載，今や光ディスクは殆どのPCに搭載されている。

このようなことから，雑誌の付録に光ディスク媒体が添付されるのは当たり前になった。この流れを利用して，超流通に挑戦したのがメディアシャトルである。メディアシャトルは定期的に発行することもあって，コンテンツにはローカルにシリアル番号を付与することにした。現在では共通認識になったコンテンツID付与の走りである。許諾情報を個別PC環境に一意にするために幅広く利用できるIDとしては，HDのシリアル番号を利用することにした。

Secure UDF



The Secure UDF specification defines a set of security enhancements to the OSTA Universal Disk Format (UDF) specification.
The primary goal of Secure UDF is to provide support for encryption based security features that are transparent to the user and their applications and is portable between different operating system platforms.

CONCERNS
- Protection for Published Intellectual Property Right (PIPR)
  - Access Control (Prevention of unauthorized user's access)
  - Data Privacy (Prevention of unauthorized user's browse)
- Data Originality (DO)
  - Data Integrity (Deterrence to unauthorized user's alteration)
  - Access Logging (Deterrence to "authorized" user's alteration with malicious intent)

SOLUTION
Logical Extension that supports the above security functions

OUTLINE of SECURE EXTENTION
a.) Where the "Security Information" shall be stored?
→ Named Stream in order to store the "Security Information" Secure Stream
b.) How the "Security Information" shall be protected?
→ Partition in order to protect the "Security Information" Secure Partition

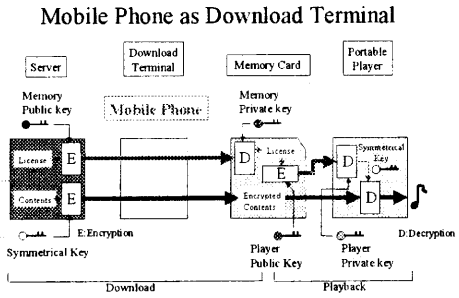
CURRENT STATUS
- Standardized by OSTA on February 26 2002
- Release of SUDF evaluation code and system built-in service on May 29 2002

FUJITSU PRIME SOFTWARE TECHNOLOGIES LIMITED

SecuerUDFの策定は，原本保証，データプライバシ保護，著作権保護，組織内データのアクセス制御などを意識して策定を開始した。DVD-ROMのブレークでも分かるとおり，ハッカにとってはフォーカスポイントが集中している場合ブレークがやりやすい。色々なレイヤが連携して保護をしているとこれをトータルにブレークするのは困難になる。ファイルシステムレベルで，重要な情報の暗号化、改竄検出が可能なように設計してある。媒体IDがあれば，論理的には，超流通を可能とするDRMが構築可能である，又機器依存の部分はドライバで吸収させることが狙いであるが，ドライブ/ドライブファーム側に一部機能を転移すればより堅牢なシ

ステムが構築可能である。

4 携帯電話/XML/デジタル放送時代



90年代後半になって，携帯電話向けにフラッシュメモリを蓄積媒体として超流通で音楽配信を実現してはどうかという提案が三洋からあった。この頃はPKIによる暗号化技術の適用が広まり始めており，これを利用して機器認証をすることにより，超流通を実現するのが一番素直ではないかということになり，コロンビア，日立などに声を掛けて検討が始まった。携帯電話はDDIポケットのPHSを対象とすることになった。これがケイタイde ミュージックである。フラッシュはMMCのセキュリティ拡張としてSecureMMCを策定し，MP3デコーダもPKIベースでの認証機構に準拠したものを策定，これらをコロンビアが設置した認証機構で認証し，配信センタは富士通が構築しサービスを実施した。許諾情報はMMCのSecureな領域に格納されており，コンテンツ鍵もPKIでやりとりしながら，最終的にはデコーダチップの中で解読されるので，非常に堅牢なシステムとなっている。ほとんど，文句も言うこともなく王道で堅牢なシステムを構築した，関係技術者には敬服を覚えた。DRMはUDAC(Universal Distribution with Access Control)-MB(Media Base)と命名した。各種媒体を利用したコンテンツの配布は自由であるが，消費者側は消費者の利用環境に応じた，許諾情報の入手が必要で，PtoP 流通で悪者にされているNapster型流通とも矛盾せず，むしろこれを歓迎するようなシステムである。UDAC-MBはPKIベースで理解しやすいことからトヨタのG-bookにも採用された。

超流通をコモディティにするためには，デジタルテレビと連携する必要性を感じていた頃，幸い総務省でMHEGに決まっていた方式をインターネットの標準であるHTMLの視点から見直す，アドホック会議が開始される旨の情報が入り，すぐ出席することを引き受けた。

マークアップ言語の歴史ではいつも体裁表示向けマークアップから論理的マークアップへの抽象化が行われ，体裁表示とマークアップ言語の独立化(TeX->LaTeX,GML->SGML,HTML->XML)が歴史的実態なので，このことを前提に提言を実施。ARIBの中にXML作業版が設置され，寄与を開始した。放送向けHTMLであるBMLはこのような経緯で策定され，実用化に至った。これを短期間で達成した日本の家電のエンジニアの頑張りには感心した。デジタルテレビの機能実装ではHTML指向のプレゼンテーションエンジンベースとJava指向のエグゼキューションエンジンベースの実装があるがどういうわけか世界全体では後者が大勢になったが，こちらのマーケットへの浸透はまだまだのようである。

携帯電話がi-mode(HTML指向)->i-Appli(Java)へと進展したのと比較し，違和感を覚えるのは筆者だけだろうか? ともあれ，デジタルテレビの仕様策定にかかわりながら，更には，ホームサーバと連携した時の許諾のあり方を検討する会議に出席しながら，テレビ業界の実態を勉強し，超流通を意識しながらどう寄与すべきかを，考えてきた。

この頃，安田先生に会う機会をいただいたが，そこでcIDfの決起合宿への参加を促され，cIDfに参加することになり，ここで，多くの識者にお会いすることができ，超流通を実現するための良識のある仲間を見いだすことが出来た。MPEG4 IPMPの標

準化の議論にも同様に参加を促され，同様の体験をした。

テレビ業界への寄与としては，テレビ放送の蓄積媒体への格納形式の策定に挑戦することにして光協会で準備をして，JEITA/IEC-TC100-TA8 のルートで PT62328 として標準化を仕掛けることにした。これは現在進行中である。現状のドキュメントは海外からも好意的に見られ，標準化にあたっては，国際的に共通の部分と各国固有部分をパーツ分けして標準化することを示唆された。

cIDf.MPEG の会議に参加している流れで電通での経験を踏まえた MMG(メロディーズ&メモリーズ グローバル)の許諾コードによる権利許諾管理のフレームワークを知ることになり，マークアップ言語の歴史もふまえ，XML の応用言語である標準化の場で討議されている XrML との関係も意識しながら，許諾コードの普及に寄与しようと考えサポートを開始した。更には JASRAC のキーマンに 2001 年の暮れにお会いすることが出来て，「志プロジェクト」を開始することになった。

やりとりは，下記のようなものである:

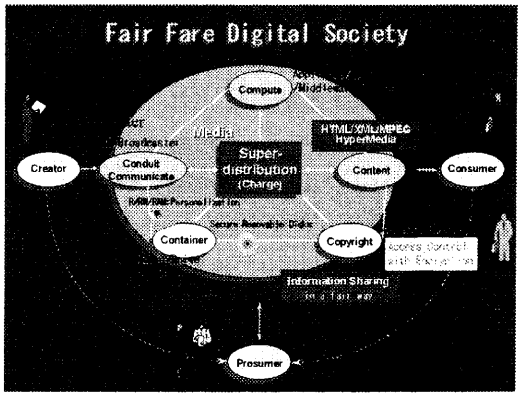
吉岡:「森先生の主張にのっとり著作権保護のために堅牢なシステムを作るハードベンダにマージンを下さいと，20 年間お願いし続けてきました」

K:「了解です。吉岡さんのやろうとしていることは-良貨で悪貨を駆逐する-つまり意志を持って著作権上フェアな環境を作る，そのために良貨を流行らせる人にマージンを落とすということです」

ハードベンダは今までこのような言葉は貰えると思っていなかった。この言葉を貰えたなら，ボランティアベースでホールダ側からクライアント側まで，ちゃんとしたシステムが構築できるデモを TVA の淡路島会議でやろうということになり，デモとプレゼンを実施した。志は，士の心，Samurai Spirit と説明すると外人も納得した。

以上のような活動と並行して，光ディスク，フラッシュメモリの DRM が，各社各様でなかなかまとまらないこともあって，プライマリな蓄積媒体である HD に一番王道の PKI ベースの DRM 支援機能を SecureUDF，PT62328，許諾コードなどとの整合性を意識しながら，現在策定中で，これが iVDR のセキュリティ機能である。

5 業界コンセンサス作りに向けて



今までの経験を踏まえ，俯瞰図を描きながら，良識のある，水平分業を前提にした，超流通の実現に向けた許諾管理システムの構築のあり方を展望してみたい。

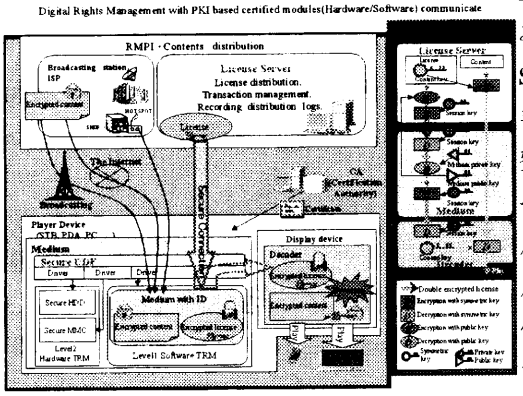
そもそも，媒体とは何であろうか。基本的には Creator(コンテンツの創作者)と Consumer(消費者)の仲介媒体と存在するもの全てを包含する。Contents の創作には創作物を表現するための表現媒体が必要でこれは，モノメディア，マルチメディア，ハイパーメディア，更にはプログラムなどがある。これら表現媒体のインターオペラビリティを確保するためには標準化が重要である。

表現媒体を利用して創作物を作成するツールとしては PC がその代表で，クライアント側で消費するのには Player が必要でこれらは Compute する

システムである。

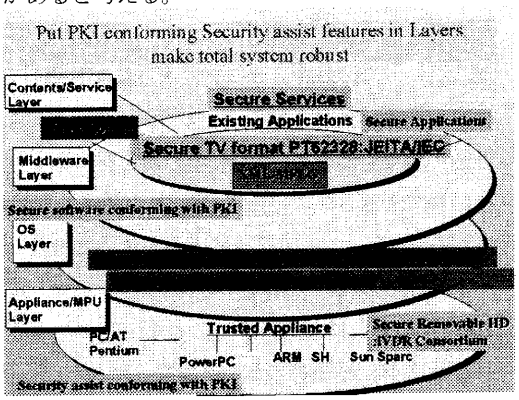
更に表現された媒体を Consumer に流通させるための Conduit(導管)として経路媒体である放送・通信媒体があり，Container としては蓄積媒体（光ディスク等）がある。

当然，Contents の Copyright 保護がフェアなデジタル社会では必須であるが，これを実現するこめには，ここで掲げた全ての媒体・ツールに一貫性を持った著作権保護機構を導入する必要がある。消費者に許諾を発行するにあたっては，セキュアなチャネルを通じて，超流通センタは消費者環境の実態を把握して，消費者とのアセスを通じて，消費者環境に対応した許諾情報を発行，消費者が当該コンテンツを consume する時には，これらの著作権保護機構を支援する関連モジュールは，PKI ベースで認証しながら，モジュール間の許諾にかかわる情報のやりとりはセキュアなセッションを通じてやりとりし，創作物の表現媒体の暗号化鍵はセキュアなデコーダで初めて解読，これもセキュアなプレゼンテーションデバイスに提示することで，システム全体の堅牢性を保証する必要がある。



圧縮技術の進展，許諾のやり方の進展，消費者環境でのハード環境の進展が今後とも随時起こるとすると，許諾にかかわる関連モジュールが今後はソフト又はファームで構成されることが多くなることも，想定される。このような場合，これらのソースコードから，コンパイラ等を通じて，生成されるネーティブコード，更にはネーティブコードの実行環境も含めた安全性を，認証機構で保証する仕組み作りも重要である。

Player としての PC はその堅牢性の脆弱性がコンテンツホールダ側からは何時も問題にされ，DVD-ROM に対するブレークも PC で起こった。このため，MPU/OS ベンダがこの問題に取り組み始めたのは当然である。一方，CE(Consumer Electronics)の Player もオープンなソフトを活用し始めているので，今後は PC 同様の破綻をきたす恐れがあるので，PC 同様にこの問題に取り組む必要があると考える。



ISO のレイヤ的な視点も意識しながら全体を見てみると，消費者は，暗号化されたコンテンツを，SecureUDF の形式で蓄積媒体に何らかの経路で入手し，更に，コンテンツ ID を超流通センタに，消費者環境の情報を含め，セキュアなチャネルで PKI ベースでやりとりをして，センタとアセスをし，利用許諾を入手する。許諾情報は，SecureUDF を利用して，Secure な形で蓄積媒体に格納される。媒体に格納しておけば，可搬媒体の場合，どの Player でも Play ができるような利用許諾を発行することが可能になる。

Play 時は，Palyer ソフトが，コンテンツを構成する各表現媒体を利用した，構成要素を解読しながら，当該表現媒体をデコードするデコーダと PKI ベースで互いを認証，セキュアなチャネルで許諾情報をやりとりして，最終的にコンテンツ鍵を取り出し内容を複合して，提示媒体に提示をする。

以上のようにホールダ側の権利を王道やり方で堅牢に守ろうとすると，クライアント側のシステムには相当の負荷がかかり，コストアップにつながることは容易に想像がつく。だからこそ，森先生の主張どおり，又JASRACのキーマンの理解のように，良貨を開発するハードベンダにそれ相応のマージンを落とす必要があるのである。コンテンツホールダ側がこのことを早期に理解して，堅牢なハード開発の支援を積極的に推進するようになれば，超流通が当たり前になり，CreatorもConsumerもその仲介にいる人たちも全てがWin Winになって，コンテンツをフェアに消費する社会が登場するものと思われる。森先生の発案によるこのシステムの実現はやはり，日本の人々が主導して実現すべきであろう。幸い，どのようなシステムを作れば良いかは，大体見えてきているので，日本の関連業界が早期に良識を集めて，結束してオープンなシステムを開発すれば，このような時代の到来はそんなに遠く無いと考える。フェアなものを作るという志を関連業界の中で一つにすることが重要である。

4 まとめ

コンテンツの表現がアナログからデジタルに変化する歴史的変革期に生きた一エンジニアとして，コンテンツ消費のフェアな社会の実現に向けた本質的な提案であった，超流通の実現に向けた，筆者の20年の活動をサマライズした。どちらかというと，今までは，屍累々の仕事だったとも言える。しかし長い歴史から見れば，20年などは，ほんの一瞬である。デジタルの後はデジタルしか無い。この変化の時代の最初に生きた我々が，本質的課題は解いておくべきである。幸い，そろそろ期が熟しきたので，日本の関連業界の良識を集めれば，フェアなシステムの構築は可能な状態になったと考える。このメモがそのような動きへのトリガとなれば幸いである。

5 参考文献,URL

[1] http://sda.k.tsukuba-tech.ac.jp/SdA/

[2] 飯田尚一、飯島章夫、三輪善良、中西康浩、藤本剛一、*コンテンツ権利許諾情報管理システム「メロディーズ」&「メモリーズ」について*、2000年、電子化知的財産・社会基盤9－3

[3] 飯田尚一、中西康浩、*コンテンツ権利許諾管理ビジネスの可能性*、2002年、電子情報通信学会－信学技報

[4] 木下信幸、中西康浩、吉岡誠 許諾コードによる権利記述について、2003年、電子化知的財産・社会基盤(EIP) 20-13

[5] 吉岡　誠　「SGMLのススメ」（オーム社）

[6] 吉岡　誠　「SGMLを使いこなす」（オーム社）

[7] http://www.keitaide-music.org/index_e.html

[8] http://www.ivdr.org/index_e.html

[9] http://www.osta.org/

[10] Brad Cox "Superdistribution"- Objects as Property on the Electronic Frontier (Addison-Wesley)