

セキュアデジタルシネマコンテンツ伝送の考察

小池真由美*1 小暮拓世*2 藤井寛*1,3 曾根原登*1

*1 国立情報学研究所 *2 東京大学先端科学技術研究センター *3 日本電信電話 (株)

数あるセキュアコンテンツ伝送方式の中でデジタルシネマコンテンツは固有の課題を抱えている。2 K / 4 K レベルの 2 時間動画をファイル化してネットワーク転送する事は、経済性や信頼性の面であまり得策ではなく、ストリーム型やそれに準じた配信方式が当面多用されると思われる。一方、配給会社のセキュリティー政策の違いや上映シアターの端末等の多様性を考慮すれば、端末では、共通プラットフォーム的な DRM の相互運用性を確保することが要求されよう。本稿では、デジタルシネマの配信を考慮したセキュアコンテンツ配信についての DRM 標準方式の実装検証とそこから浮上した技術課題について考察する。

Some Consideration on Delivery of Secure Digital Cinema Content

Mayumi Koike*1 Takuyo Kogure*2 Hiroshi Fujii*1,3 Noboru Sonehara*1

*1 National Institute of Informatics *2 University of Tokyo, RCAST *3 NTT

ISO/IEC, MPEG-2 system standard consist from stream configuration including MPEG-2 IPMP part. MPEG-2 system stream can transfer Digital Cinema Content securely by using MPEG-2 system IPMP function where PSI(Program Specific Information) portion. Originally this PSI can use for broadcast contents carriage however this PSI also can map IPMP standard for secure interoperable compatible DRM system. This paper describe the implementation study of this high level standard actually on the practical terminal and through this feasible study try to find out the necessary middle layer standard interface for practical application. Actual amendment proposal will be necessary for this purpose.

1. 序論

映画コンテンツのデジタル化は映画製作の現場に革新をもたらし、映像音声のデジタル化は、特撮やアニメ分野の創造性を拡大、コンテンツの高度化と創作工程の効率化をもたらした。一方、MPEG-2 圧縮符号化技術は、2 Kコンテンツの圧縮伝送を可能なレベルまでに進歩し、映画コンテンツの大衆化は目前に迫りつつあるのが現状である。しかしながら 4 Kレベルコンテンツの普及はこれからであり、2K を中心とした様々な配信の可能性が検討されているのが現状である。

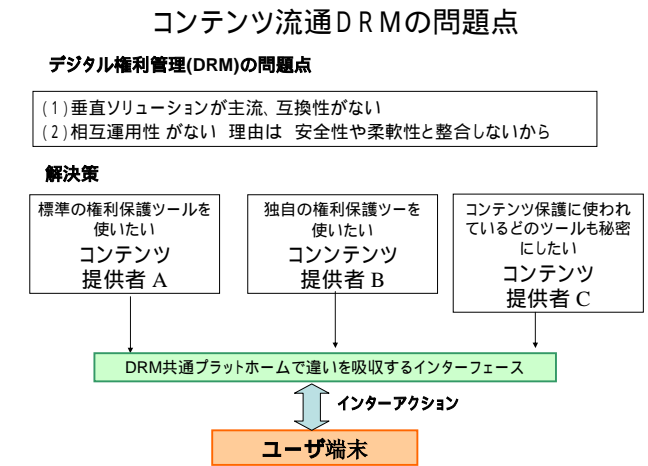
一方、デジタル放送分野で盛んになりつつある高画質コンテンツ配信は、デジタル HD 方式として世界の多くの地域で実用になりつつあり、関連機器の整備も進んで、システムトータルとして配信と視聴の環境が整いつつある。

一般に、映画コンテンツは、制作費が多額で、収益性を確保するには、多くの観衆に劇場に足を運んでもらう必要があり、上映の前に、コンテンツが流出する事は是が非でも避けなければならない。さもないと ビジネスモデルは崩壊する。そこで、映画配給会社は、DRM 技術の導入が必須であり、各配給会社は独自の DRM 技術を導入、コンテンツの配信のセキュアな環境保持を進めているのが現状であり、この分野のビジネスは、垂直統合型で推移してきている。

一方、それを支える DRM(Digital Rights Management)技術は ISO/IEC,JTC-1 や ITU-T の場を中心に標準化検討作業が進み、共通 DRM 方式としてハイレベル標準 MPEG-2 IPMP/MPEG-4IPMP の標準化が完了し参照ソフトの公表も行われたが、2005 年 2 月現在、共通 DRM プラットホームとしての実装例は報告されていない。この原因として考えられるのは、この DRM 標準が、いわゆるハイレベル標準であり、具体的な実装に近い技術課題に踏みこむのを避けた結果とも言えよう。何故ならば、DRM 技術そのものがシステムビジネスになるのではなく、コンテンツ配信システムの一部に組み込まれ、ビジネス戦略の武器、又は障害になって、コンテンツ関連ビジネスに大きな影響を及ぼす事が明らかになりつつある現状がある。

DRM 技術の導入方法もコンテンツ配信分野やビジネスプレーヤ間で違いがある。第 1 図に DRM

システムの課題と一つの解決策を示した。



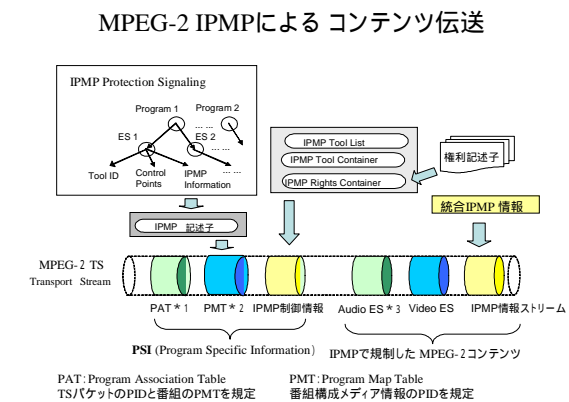
第 1 図 コンテンツ流通システム適用 DRM の課題

一般に、DRM と言った場合、DRM に使う「ツール」を指す場合と、「権利の管理」を意識する場合と、システムとしてまとまった機能、或いはビジネスモデルを指す場合とがある。

本報告は、広義の DRM として、ストリーム型コンテンツ配信に適用可能な代表的 DRM 標準として MPEG-2IPMP を取り上げ、その実装課題と、DRM 関連技術標準の課題を報告する。

2. MPEG-2 IPMP 技術

今日、デジタル放送や DVD で多用されている画像圧縮方式標準 MPEG-2 はキャリッジとして MPEG-2 システム TS(Transport Stream)を用いている。



第 2 図 MPEG-2, IPMP の TS-PSI マッピング

第 2 図は MPEG-2 TS システムストリームの PSI

(Program Specific Information) 部を用いて IPMP 情報をマッピングしその機能を図示したものである。即ち

MPEG-2 IPMP ---PSI (Program Specific Information)

MPEG-4 IPMPX---OD(Object Descriptor)

MPEG-21 IPMP---DID(Digital Item Declaration)

この中で MPEG-2IPMP は、PSI 即ち放送番組関連情報を埋め込むスペースであり、利用するのに特別の工夫を必要としない特徴がある。第 2 図に具体的なマッピングの例を示したが、ペイロードに影響しないスペースに権利制御情報を埋め込む事が可能になっている。

IPMP システムは IPMP で規定したツールにより保護システムを機能させる。この IPMP ツールは、パラメトリック・ツールとして公開或いは、識別子で区別する独自方式でも良い。更に第 2 図のように IPMP ストリームに埋め込まれダウンロードしても良いし、外部から取得しても良い。処理機能としては、IPMP ツールの要求条件が、コンテンツのストリーミングを始める前に端末に知らされる。IPMP ツールの構成と初期化情報は、IPMP 記述子又は、IPMP ストリームで運ばれる。

標準では、IPMP システムと言うより、IPMP ツールとして規格化している。それを用いる事で、認証や暗号復号、透かし処理等の IPMP 機能を実行するモジュールとしての機能構成が可能となる事による。IPMP のメッセージフレームワークはツールと端末間の API 定義の代わりとして抽象化する機能であり、制御グラフは保護システムの構造をグラフ構造で記述するフレームワークである。ツールの構成と初期化情報は、IPMP 記述子又は、IPMP ストリームで運ばれる。制御の実際は異なるツールがシステムの異なる場所で動作する様に、ツールを挿入する制御点と適用順序が IPMP 記述子の構文で定義されている。実際には、権利コンテナ、鍵コンテナ、ツール初期化データ等の各種 IPMP データが定義され、IPMP 記述子の中あるいは、IPMP ストリームの中に入れて伝送される。拡張 IPMP ストリームのシンタックスも以下のように定義されている。メッセージ・ルータ (MR) は、ビットストリームと端末と IPMP ツール間の通信をつかさどる。機器間の通信用に、メッセージ・ルータ間の通信も定義されている。

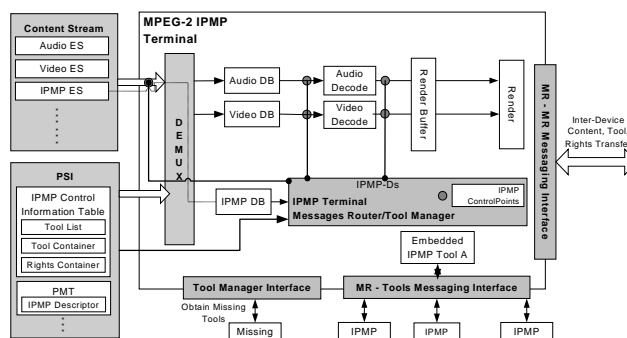
メッセージは、その構文と意味が定義されてい

る。

メッセージの配送手順も定義されている。

全ての IPMP ツールへのアクセスは端末を介して行われる。ここでは、IPMP ツール同士の直接通信は行われない。

MPEG-2 IPMP – アーキテクチャ

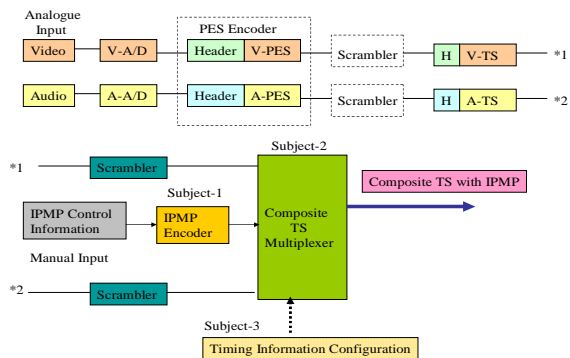


MPEG-2 IPMP Architecture

第 3 図 MPEG-2 IPMP の端末構成図

第 3 図に、MPEG-2, IPMP 標準を具体化する端末器の構成を図で示した。

MPEG-TS へのMPEG-2 IPMP 実装方法



第 4 図 MPEG-TS と IPMP 部の関連付け

3 . ソフトウェア実装

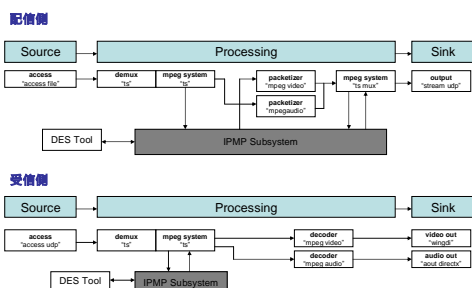
第 3 図の構成をベースに端末器、具体的には MPEG-2 ベースのストリームデコーダを構築するには IPMP ソフトウェアの実装が必要である。

そこで本研究では実装プラットフォームとして柔軟性のあるソースコード公開ソフトウェア VLC (Video LAN ' media player)を用いてその上に MPEG-2 及び IPMP をテストベッド実装し、サーバー

クライアントモデルを構築した。ここではクライアント(端末)は遠隔地にある事を意識している。実装した参照ソフトは MPEG の CVS サーバーに公開されている「IPMP4MPEG2」である。VLC プレーヤは以下のモードで動作が可能である

1. クライアントモード
2. 双方向型ストリームサーバ
3. 遠隔ストリームサーバ

VLC ベースで構成した MPEG-2IPMP プレーヤ



第 5 図 VLC プレーヤの構成

第 5 図に今回用いた VLC プレーヤの構成を示した。クライアントモードでは VLC プレーヤはプラグインホルダーにより実装される IPMP モジュールで、IPMP で保護された MPEG-2 TS を再生する。

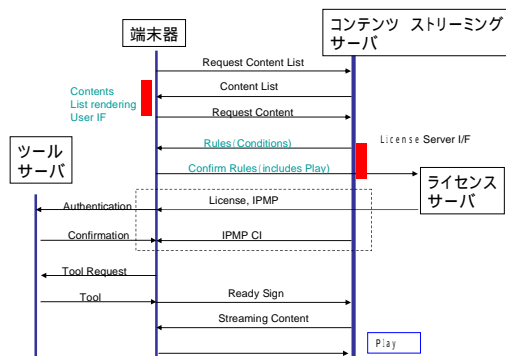
4 . ユースケースモデル

第 5 図の VLC プレーヤを用いて実際のコンテンツ配信を行うユースケースを検討した。実際にはコンテンツサーバ、ライセンスサーバ、IPMP ツールサーバ、コンテンツリスト、そして、端末から構成される仮想システムを構築した。

端末器サイドのユーザはコンテンツリストを検索して所望のコンテンツをリストから抽出し、コンテンツ取得取引確認を行ってから、コンテンツ取得のプロセスに入るが、その過程で IPMP 情報からツールリストを得て、ターミナル固有の IPMP ツールを参照し、ツール取得を実行に移す。

第 6 図は、その場合に実行したコンテンツ取得のユースケースを実際のネットワークを用いて検証した構成である。

サーバクライアントモデルにおけるコンテンツ配信ユースケース



第 6 図 サーバクライアントモデル化したコンテンツ配信、ユースケース

5 . MPEG-2 IPMP の利点

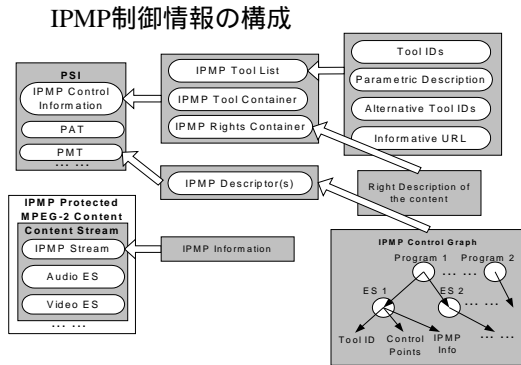
これまでの検証で抽出した MPEG-2 IPMP システムの利点は

- (1) IPMP-X の各保護機能動作は多様な用途に適用した、暗号化方式や電子透かしによる権利管理等、1 種類以上の保護機能を共存させることが可能である。
- (2) MPEG-2 IPMP は、放送モデルのみでなくコンテンツ配信モデルにも適用可能である。本システムで配信されるセキュアコンテンツは、MPEG-2 IPMP で定義された権利管理の機能より、ユーザ端末に安全に蓄積することが出来る
- (3) 本方式の他のメリットは、ホームネットワーク上の特定のコンテンツでも定義された内部デバイス間のコンテンツ転送をサポートする
- (4) 本方式は MPEG-2 TS が使われるコンテンツ伝送環境に適しているばかりでなく IP ネットワークにも適用が可能である。
- (5) コンテンツプロバイダーが「標準」「独自」「秘密」等の権利保護ツールを任意に選択出来る 相互運用性の確保が可能となる。
- (6) 端末間の互換性が確保されコンテンツプロバイダーが端末 DRM 仕様の違いを意識する事なく配信が可能になる
- (7) 端末ユーザ間のコンテンツ交換が可能になり、水平ビジネスへの広がりが期待出来る

このような利点を実現することを目標としたため、標準化作業は、開始当初から難航したが、2003年に完成した。

6. DRM 標準としての IPMP の問題

第7図は前述の MPEG System の PSI に乗せられる IPMP 制御情報の構造を拡大したものである。



第7図 IPMP 制御情報の構造図

必要なツールの一覧(IPMP Tool List)、ツールの適用場所・方法を記述した IPMP 制御グラフ(IPMP Control Graph)、必要なツールのソフトウェアモジュール(IPMP Tool Container)、コンテンツの利用条件(IPMP Rights Container)が情報として伝送される。これらはコンテンツと共に送られる IPMP ストリームを構成するので、端末側はこれを理解し、更に、コンテンツ暗号を解読する為の鍵情報などが入った IPMP 情報(IPMP Information)を理解し、実行する必要がある。これら一連の実装から、実証実験で得られた課題は以下のとおりである。

(1) 先にも述べた如く、MPEG-2IPMP はハイレベル標準設定の為に、実際にインストールするプラットフォームを特定していない。従って、実装に必要な環境設定に関しては、全て実装側の処理に任されている。

(2) 標準参照モデルとユースケースの違いがあり、ユースケースモデルの種類によってはプラグインモジュールとしての動作が確認できない。従ってモデル別に、シンタックスの変更やコマンドの追加が必要になる。

(3) コンテンツ配信のトータルから見ると IPMP 部は、その一部に過ぎないのでシステム構築の違いにより共通インターフェースを複数個用意する必要がある。

(4) PC ベースの端末器以外では、IPMP 実装にかなりの負荷がかかる。デジタルシネマコンテンツのコンシューマ機器への実装、特に、小型携帯端末では負担が重いので、今後実用レベルでの検討にはかなりの改善が必要であろう。

(5) 実証実験で確認された課題を整理し、ISO/IEC への標準改訂、追加提案を実施する。

7. 謝辞

本研究は、文部科学省 振興調整費のサポートにより実施されたものであり、本研究の機会を与えて戴きました 東京大学 安田 浩教授に感謝申し上げます。

文献

- [1] ISO/IEC JTC-1/SC29/WG11 m10848 July 2004
- [2] ISO/IEC JTC-1/SC29/WG11 m10858 July 2004
- [3] ISO/IEC JTC-1/SC29/WG11 m10974 July 2004
- [4] ISO/IEC JTC-1/SC29/WG11 m10860 July 2004
- [5] ISO/IEC JTC-1/SC29/WG11 m10862 July 2004
- [6] ISO/IEC FDIS 13818-11 Dec 2003