5

光ディスク著作権保護標準化から見たMPEG-21

The Comparison of the Content Protection Standards, MPEG-21 and AACS

伊藤　聡 （株）東芝 研究開発センター
加藤　拓 （株）東芝 研究開発センター

現在用いられている最新の光ディスクメディアの著作権保護規格とMPEG標準を比較し，両者の差異と接点について検討を行い，今後の標準化が目指すべき方向について考察する．

AACS保護規格化の枠組み

AACSの目的と規格化の経緯

2006年に登場したHD DVDビデオやBlu-ray Disc（BD）ビデオで採用されているコンテンツ保護方式であるAdvanced Access Content System（AACS）[1), 2)]では，単純にディジタルコンテンツを暗号化するだけでなく，コンテンツ保護のためにさまざまな技術が採用されている．このように一般消費者が利用するエンターテイメントコンテンツを保護する仕組みは，1996年に登場したDVDビデオにおいて採用されたContent Scramble System（CSS）が最初である．

DVDビデオでは一般ユーザによるカジュアルコピーを防ぐことを目的としてCSSが策定されたが，その後のPCの能力向上により，CSSで採用された鍵長40ビットのスクランブル方式は，一般的なPCでも短時間で使用されている鍵が探索可能となり，コンテンツ保護方式として十分な強度を有しているとは言えない状況に置かれている．

その後に登場したDVDオーディオや記録型メディアのDVD-R/RW/RAMディスクで利用されているコンテンツ保護方式であるContent Protection for Prerecorded Media（CPPM）やContent Protection for Recordable Media（CPRM）では，鍵長を増やすことや暗号アルゴリズムの見直しだけでなく，機器に秘匿されたデバイス鍵が漏れてしまった場合の対策として不正機器（露呈デバイス鍵）の無効化機能を実現するためのMedia Key Block（MKB）やコンテンツが不正に再生されることを防止するための手段として電子透かし（Watermark）も採用されている．

その後ディジタル放送の開始などによって高画質（High Definition）ビデオコンテンツの普及が始まるにつれ，新たなコンテンツ保護方式が必要となってきている．そこで，高画質放送コンテンツの記録や，放送より高画質なビデオコンテンツを提供可能なビデオパッケージメディアにおいてコンテンツ提供者の要求を十分に満たすコンテンツ保護方式としてAACSの利用が始まっている．

以下の節では，HD DVDビデオを例に取りながらAACSで採用されている技術を説明する．

AACSにおけるコンテンツ保護のスキーム

AACSは広く使われることを想定して，フォーマットやメディアなどの内容に合わせて複数の仕様書を用意している：

- **Introduction and Common Cryptographic Elements**
  すべての保護方式の基本となる暗号関連のアルゴリズム，不正機器無効化のためのMKB仕様やPCバス上の保護方式を規定
- **Pre-recorded Video Book**
  パッケージメディア用のコンテンツの正当性を確認するためのコンテンツ証明書，再生機器ごとに再生データを分けるためのシーケンス鍵方式やコンテンツの暗号化方式などを規定
- **Recordable Video Book**
  記録メディアに放送コンテンツを記録する際の保護方式を規定

このほかには，HD DVDやBDといった個々のフォーマット，パッケージ用や記録用といった用途ごとに，AACSを適用させる際に必要な詳細な事項を規定した仕様書が用意されている．そのほかにも，パッケージメデ

ィアや映画館で上映されているコンテンツの不正コピー対策として電子透かしの採用が予定されている．

実際に AACS を採用した HD DVD 機器を製造しようとした場合，機器製造業者は AACS 技術ライセンスを管理している AACS Licensing Administrator（AACS LA）と契約した上で，上記仕様書に従ってコンテンツ保護技術を実装しなければならないが，実装に当たっては遵守規定と強靭性規定に従う必要がある．

遵守規定や強靭性規定には，機器がコンテンツを扱う際の機器内部での処理方法，入出力やコピー／ムーブ時のルール，さらに AACS LA からライセンスされるデバイス鍵などの秘密情報やコンテンツ暗号化／復号処理時に求められる中間データの取り扱いルールなどが規定されている．機器の実装がこれらのルールに違反していた場合，AACS 技術を用いて保護されたコンテンツを取り扱えなくするための機器無効化が実施されるだけでなく，違反内容によっては多大な損害賠償金が課せられる可能性もある．

AACS LA とライセンス契約を締結することにより，機器製造業者は個々の機器に必要な秘密情報であるデバイス鍵などを，メディア製造業者は AACS 保護記録に必要な MKB などを受け取ることができるようになる．これらのライセンスデータは，物理的にもセキュリティが厳密に管理された鍵発行機関が AACS LA からの委託を受けて発行している．

AACS 技術仕様の概要

AACS 仕様書では，すでに述べたように共通な仕様として暗号アルゴリズムや不正機器無効化のための MKB，PC バス上の保護方式などを規定している [3), 5)]．

コンテンツや鍵情報の暗号化には鍵長 128 ビットの AES（Advanced Encryption Standard）が，データの正当性を示すためのディジタル署名やバス認証に使われる鍵共有には位数 160 ビットの楕円曲線上の暗号アルゴリズムが採用されている．コンテンツ暗号化／復号に必要なすべての鍵は，個々の機器が持つ秘密鍵（デバイス鍵）を使って MKB を処理しなければ復号できないようになっている．不正に利用されているデバイス鍵では暗号化／復号に必要な正しい鍵を導出できないような MKB を使用してコンテンツを暗号化することにより，不正機器では正しい復号ができなくなることで不正機器の無効化が実現されている．

PC 上のソフトウェアがドライブから AACS 技術を用いて保護されたデータを読み出す際に必要なドライブ認証に楕円曲線上の公開鍵暗号アルゴリズムである ECDSA（Elliptic Curve Digital Signature Algorithm）と ECDH（Elliptic Curve Diffie-Hellman）を採用することで，相互に接続された相手の正当性を検証している．ドライブとソフトウェア機器には AACS LA からライセンスされたドライブ証明書あるいはホスト証明書と呼ばれる個別の公開鍵証明書が割り当てられる．

AACS 保護技術を HD DVD ビデオに適用した場合には，以下のような機能が実現される．

- **階層的な鍵管理**：デバイス鍵を使用して実際にコンテンツを暗号化するためのコンテンツ鍵を導出するためには複数の処理が必要となる
- **ハードウェア機器とソフトウェア機器の分離**：ハードウェア機器で使用されるデバイス鍵をそのままソフトウェア機器に使用しても正しい復号処理が行えない
- **不正機器の無効化**：不正に利用されているデバイス鍵が発見された場合，当該デバイス鍵は無効化される．ただし，ソフトウェア機器用のデバイス鍵は不正の有無にかかわらず有効期間を過ぎると無効化される
- **再生機器同定**：人間が知覚できない程度の違いを加えた複数のコンテンツを用意し，再生機器ごとに再生できるコンテンツを変えることで，再生されたコンテンツから再生機器を特定する
- **不正コンテンツの無効化**：AACS 技術を用いて保護されているにもかかわらず，コンテンツ証明書によって正当性の確認できないコンテンツの再生を禁止する
- **コンテンツ暗号化**：AES で暗号化される
- **PC システム向けのバス認証**：PC 用 AACS 対応ソフトウェアとドライブが相互に正当性を確認する
- **ネットワークダウンロードコンテンツの保護**：追加で提供されるコンテンツもメディア上のコンテンツと同様に保護される
- **サーバを利用した HD DVD ビデオから他メディアへのコピー許可（Managed Copy）**：オリジナルディスクを 1 枚ずつ管理するために ROM ディスクにも固有 ID（Prerecorded Media Serial Number：PMSN）を記録する

AACS 遵守規定による入出力制御

すでに述べたように AACS LA は遵守規定によってコンテンツデータの入出力を規定しているが，入出力コンテンツの制御情報はコンテンツごとに利用ルール（Usage Rules）によって指定される [3)]．

現在の仕様では，Encryption Plus Non-assertion（EPN）を含むコピー制御情報（Copy Control Information：CCI），アナログコピー制御信号，アナログ画質制限フラグおよびアナログ出力制限フラグといった出力制御情報をコンテンツとともに記録することができる．

そのほか，将来的にコンテンツの取り扱いをより詳細に規定した利用ルールも定義できるようになっている．

	AACS	MEPG-21 等
識別情報の定義	・Volume ID ・Media ID ・Content ID ・PMSN など	・ディジタルアイテム（DI）の ID の要件（Part3：DII） ・ID 発行機関リスト（Part3：DII） ・DI の断片化と識別（Part18：FIDS）
データフォーマット	・コンテンツ保護に関するデータフォーマットは詳細に規定 ・コンテンツ自体は DVD Forum で規定	・DI の構造記述の枠組み（Part2：DID） ・ファイルフォーマット（Part9） ・バイナリフォーマット（Part16）
コンテンツ保護	・保護方式 ・暗号アルゴリズム指定 ・署名アルゴリズム指定 ・不正機器の無効化 ・ホスト／ドライブ無効化 ・コンテンツ無効化（CRL，SKB，電子透かし等）	・保護範囲の指定方法（Part4：IPMP Component） ・保護方式に関する情報記述（Part4：IPMP Component） ・電子透かしのガイドライン（Part11）
利用制御	・コピーコントロール情報（CCI） ・Managed Copy ・Title Usage File（TUF）	・汎用的な利用権記述（Part5：REL, Part6：RDD） ・Domain 管理プロトコル (ISO/IEC 29116-1 の一部)
ユビキタス対応	―	・端末適応化（Part7：DIA） ・イベントレポート（Part15：ER）
API	・標準 API	・API 標準化（Part10：DIP） ・Middle Ware（MPEG-E：M3W）
実効性の担保	・Robustness Rule ・Compliance Rule	・Conformance（Part14） ・テストベッド（Part12） ・Reference Soft（Part8）
	・KGF 運営 ・サーバ運営 ・アフターケア（ハッキング対応等）	・パテント管理（MPEG-LA）

表 -1　AACS と MPEG-21 等の標準化項目の比較

AACS 規格と MEPG-21 規格の比較

◘規格化項目の対比

AACS 標準と MEPG-21 標準等の標準化項目等について比較を行った結果を**表 -1** に示す．なお，厳密な対比は困難であるため，かなり抽象的なレベルでの比較となっている．

◘比較結果に関する考察

表 -1 に基づくと，それぞれの活動内容は以下のような特徴があると考えられる．

AACS

- 応用・目的，想定している脅威が具体的で明確．
- 実装する上での必要なコンポーネントは決めている．
- 実効性を保つための技術だけではなく，運用・契約面の仕組みも決めている．

MPEG-21

- DRM の相互運用性を考慮した汎用的な枠組みを規定
- 重要度の高いコンポーネントはあるが網羅的でなく，具体性に欠ける．
- 特許管理の仕組みがあるが，制度上，技術的標準化に活動が限定されており，実効性を維持するための仕組みが不十分である．

AACS と MEPG-21 REL の接点

前述のとおり，両者を比較すると全体としてかなりの差異があることが分かった．ただし，利用制御の項目では両者の接点となり得る部分も存在している．

◘ AACS TUF の構成

HD DVD 等の次世代光ディスクでは，ネットワーク接続により多様な利用サービス形態を可能とする枠組みが準備されている．そして AACS 規格ではこれらの利用を制御する TUF（Title Usage File）と呼ぶ枠組みが規定されている [4]．

図 -1 に HD DVD における TUF の構造を示す．TUF では，

AudioVideo Object 等のコンテンツ部品に対してそれぞれの利用ルールを Usage Rule Set（以下，URS と呼ぶ）で記述することができ，各 URS には 4 種類の利用ルールが格納できる．そのうちの 1 つは利用条件を自由に記述できる REL フィールドとして定義されている．

この REL フィールドに MPEG-21 REL によるライセンス記述を行うことにより，コンテンツ部品単位で多様な利用条件を簡潔な文法でユーザに理解しやすい形式で記述を行うことができ，利用条件の効率的で意図通りの設定が可能となる．

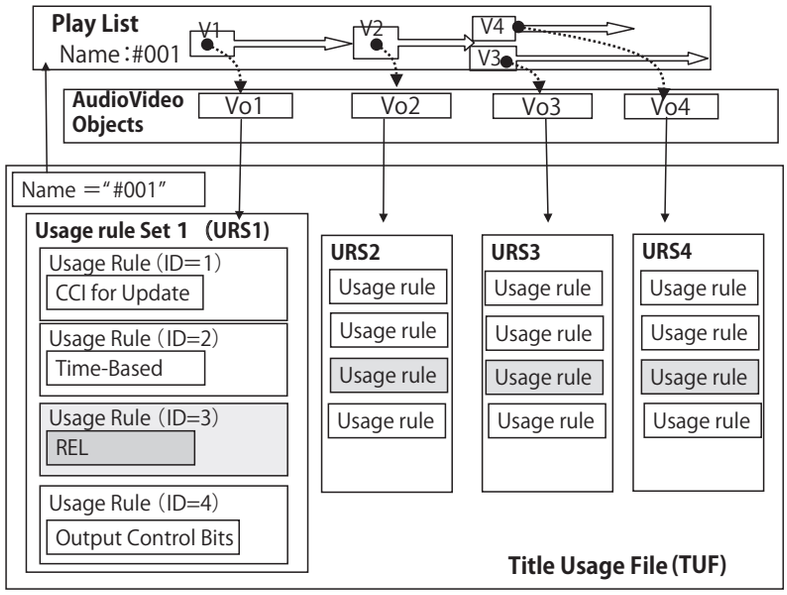

図 -1　HD DVD における TUF の構造

◘光メディア応用を志向した REL プロファイル

MPEG-21 REL は応用分野に依存しない幅広い利用を目指して設計・標準化されている．これは個別の応用を考えた場合に，冗長な部分が出てくるのと同時に，その応用に特化した部分が欠落する傾向があることを意味する．そのため，REL プロファイルと呼ばれる，必要な言語拡張をした上で，必要最小限のスキーマのサブセットを定義したものの開発・標準化が進行している．

このうち，MPEG-21 REL MAM（Mobile And optical Media）Profile は携帯端末などのモバイル機器や DVD プレーヤなどの組み込み型の機器への応用を志向したプロファイルである．このプロファイルは携帯電話におけるコンテンツ保護規格（OMA DRM Ver2.0）および AACS 規格をベースに開発され，2007 年 1 月に国際標準化が完了した．以下に MAM Profile で想定している，光ディスクでの応用例を示す．

a）劇場公開版パッケージに特典映像を記録し，ネット接続して許諾を取得して再生
b）レンタル用 HD DVD で，一定期間の経過後に高画質再生
c）出演俳優のコメントをダウンロードし本編と同期再生
d）テーマパーク内でのみ再生できるコンテンツ
e）新しい吹替音声をダウンロードし，再生
f）TV シリーズ物を全巻そろえると特典映像が再生可能
g）映像と BGM の主従を入れ替え，好きな映画音楽をお気に入りの映像を背景に再生

拡張 Element 名	Semantics	派生の基礎となる Element 名
IdentityHolder	ID で識別した利用権者	Principal
GovernedCopy	統制付き Copy 操作	Right
GoverndMove	統制付き Move 操作	Right
Enlist	新プレイリストへの参照追加	Right
Delist	新プレイリストへの参照削除	Right
ProtectedResource	暗号化コンテンツ	Resource
DrmSystem	統制付き Copy/Move 先の DRM	Condition
OutputRegulation	出力信号の品質／制限	Condition
SeekPermission	Permission の有無	Condition
StartCondition	操作の開始時点の条件	Condition
DerivationConstraint	部品再利用時の他部品との制約	Condition

表 -2　REL Multimedia Extension 1 で拡張した Element

MAM Profile のための REL スキーマ拡張 [4)]

この MAM profile で必要な拡張は Multimedia Extension 1 と呼ぶ XML スキーマで定義されている．**表 -2** に拡張した Element を示す．

スキーマサブセット設定による MAM Profile 定義

MEPG-21 REL MAM Profile では REL スキーマ全体から冗長な部分として，"*DelegationControl*" Element などを削減するとともに，主要な Element の派生となる Element を大幅に制限し，特に課金に関する条件を記述する Element はすべて対象外としている．

これにより，XML スキーマ全体の規模が大きく削減

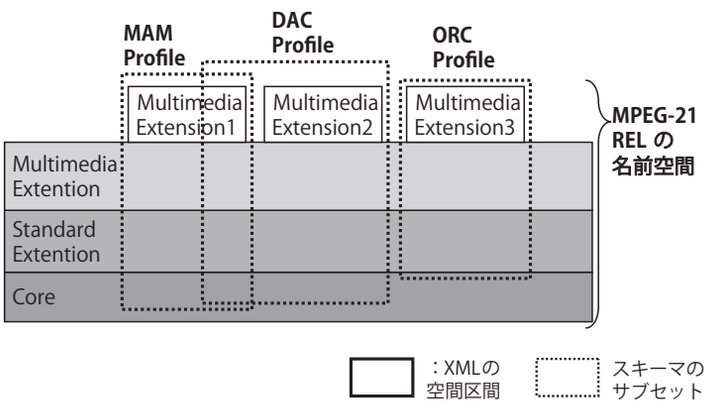

図 -2　MEPG-21 REL Profiles の位置づけ

され，対応機器の資源への負担軽減とともに利用権の処理系ソフトウェアの開発が容易となっている．

MPEG-21 標準普及への考察

コンポーネントとして独立性が高く，汎用性も高い規格についてある応用に特化したプロファイルを開発するというアプローチは，ISO，IEC などのデジュール規格が AACS などのデファクト規格との接点を作り出す 1 つの有効な方法となる可能性がある．

ここでは MPEG-21 REL 関連のほかのプロファイル標準化の活動について紹介する．

REL DAC（Dissemination And Capture）Profile

インターネット TV などを含む広い範囲のディジタル放送を対象としている．欧州系のディジタル放送規格である DVB 規格の 1 つである DVB-CPCM との互換性を意識している．このプロファイルは MAM Profile との共通部分が多いが，さらなるスキーマの拡張がなされており，それらは Multimedia Extension 2 とよばれる XML スキーマとして定義されている．2007 年 7 月の最終投票で可決となり，現在，規格書の発行手続き中である．

REL ORC（Open Release Content）Profile

ISO/IEC 23000-7：Open Release MAF（Multimedia Application Format）と呼ばれているユーザ発信型コンテンツ用フォーマット標準案に適用することを想定した REL プロファイルである．Open Release MAF はコンテンツの再利用を意識した Light-weight DRM を標榜し，Creative Commons のライセンスと同等の内容を盛り込む方向で標準化が進められている．**図 -2** に MPEG-21 REL の各プロファイルの位置づけを示す．

以上，本章では光ディスクにおける著作権保護標準化の概要を述べ，AACS 標準と MPEG-21 標準の比較検討を行い，その差異および接点についての考察を行った．

もっとも，MPEG-21 のような全体フレームワーク標準は特に技術以外の部分まで踏み込んだ枠組みを提供しないと，そのまま採用するのはまだまだ難しいと思われる．

国際標準化団体のミッションとして，今まで範囲外として扱ってきた問題に対して，今後どこまで取り組むかを改めて議論する必要もあると思われる．

参考文献

1）Advanced Access Content System（AACS）：Introduction and Common Cryptographic Elements Rev 0.91, http://www.aacsla.com/specifications/（Feb. 2006）.
2）Advanced Access Content System（AACS）：HD DVD and DVD Pre-recorded Book Rev 0.912, http://www.aacsla.com/specifications/（Apr. 2006）.
3）柏原他：図解 HD DVD ハンドブック，（株）インプレスジャパン 2007.
4）伊藤他：MPEG-21 REL におけるプロファイルの標準化，東芝レビュー 2007, Vol.62, No.7, pp.19-22 (2007).
5）加藤他：HD DVD で利用されるコンテンツ保護技術，東芝レビュー 2007, Vol.62, No.7, pp.11-14 (2007).

（平成 19 年 9 月 7 日受付）

伊藤　聡（正会員）　satoshi.ito@toshiba.co.jp

1989 年北海道大学大学院修士課程修了．同年（株）東芝入社．AI 技術，電子商取引，ディジタル著作権保護技術の研究開発に従事．1997 年計測自動制御学会論文賞．現在，研究開発センターコンピュータ・ネットワークラボラトリー主任研究員．AI 学会会員．

加藤　拓　taku.kato@toshiba.co.jp

1997 年東京大学大学院博士課程修了．同年（株）東芝入社．情報セキュリティ技術およびコンテンツ保護技術の研究開発に従事．現在，研究開発センターコンピュータ・ネットワークラボラトリー主任研究員．工学博士．電子情報通信学会会員．