Vol.2010-AVM-71 No.11
2010/12/2

# ISDB-Tmm におけるコンテンツ保護とアクセス制御技術

石井 晋司　内田 良隆†　森住 俊美†　松井 龍也
伊藤 宏一　桑野 秀豪　阿久津 明人　関野 公彦‡

NTT サイバーソリューション研究所 〒239-0847 神奈川県横須賀市光の丘 1-1
†マルチメディア放送 〒100-6104 東京都千代田区永田町 2-11-1 山王パークタワー4F
‡NTT ドコモ サービス&ソリューション開発部〒239-8536 神奈川県横須賀市光の丘 3-6
E-mail: { ishii.ishinji, matsui.tatsuya, ito.kouichi, kuwano.hidetaka, akutsu.akihito}@lab.ntt.co.jp †
{ uchida, morizumi } @mmbi.co.jp,　‡ sekino@nttdocomo.co.jp

**あらまし**　2012 年にマルチメディア放送のサービスが開始される予定である．マルチメディア放送サービスは，リアルタイム型サービスと蓄積型サービスが予定されている．これを実現する技術は，ISDB-Tmm である．本稿は ISDB-Tmm のコンテンツセキュリティ技術であるコンテンツ保護とアクセス制御の技術的背景を解説する．

**キーワード**　ISDB-Tmm，リアルタイム型放送，蓄積型放送，CAS，DRM，アクセス制御，コンテンツ保護，RMPI

# Contents protection and access control technology for ISDB-Tmm

Shinji ISHII Yoshitaka UCHIDA†　Toshiharu MORIZUMI†　Tatsuya MATSUI
Kouichi ITO Hidetaka KUWANO Akihito AKUTSU and Kimihiko SEKINO‡

NTT Cyber Solution Labs.　1-1 Hikarinooka Yokosuka-shi, Kanagawa 239-0847 Japan
† Multimadia Broadcasting, Inc. 2-11-1 Nagatacho, Chiyoda-ku, Tokyo, 100-6104 Japan
‡ NTT docomo Service & Solution Development Dept. 3-6 Hikarino-oka Yokosuka-shi, Kanagawa 239-8536 Japan
E-mail: { ishii.ishinji, matsui.tatsuya, ito.kouichi, kuwano.hidetaka, akutsu.akihito}@lab.ntt.co.jp †
{ uchida, morizumi } @mmbi.co.jp,　‡ sekino@nttdocomo.co.jp

**Abstract**　The multimedia broadcasting services is scheduled to start in 2012. The broadcasting services have real-time service and download service. The technological architecture of the broadcasting services is called “ISDB-Tmm.” This paper describes technical background of the contents protection and the access control which are contents security technologies of the ISDB-Tmm.

**Keyword**　ISDB-Tmm. Broadcast, Download, CAS, DRM, PMPI

## 1. はじめに

健全なコンテンツ流通ビジネスには，コンテンツが正しい利用範囲で利用されることを確保することが重要である．この要件を実現するコンテンツセキュリティ技術として，コンテンツ保護技術とアクセス制御がある．

本稿では，マルチメディア放送技術方式の ISDB-Tmm[1],[2]として予定されるサービスであるリアルタイム型サービスと蓄積型サービスをコンテンツの健全な流通を技術的に支えるためのコンテンツセキュリティ技術のあり方を示す．

## 2. マルチメディア放送のセキュリティ技術

マルチメディア放送のコンテンツ流通ビジネスには，図 1 に示すように，コンテンツホルダー，放送事業者，放送網，通信網，受信者の携帯電話型受信機が関連する．これらのエンティティではコンテンツの流通過程において，予め定められた範囲でコンテンツが利用され，コンテンツ制作と利用に係るマネーフローが成立することが不可欠である．さらに，有料放送の場合には，視聴契約を締結している受信者の受信機のみが利用できるように制御することが必要である．これらを実現するためのコンテンツセキュリティ技術と

しての仕組みが，ビジネスコンテンツ保護（プロテクション）とアクセス制御（コントロール）である．

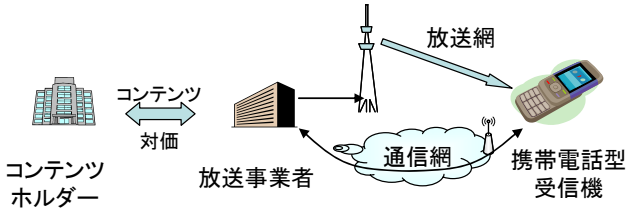


図 1　ビジネス形態モデル図

表 1　マルチメディア放送に係わるコンテンツ保護に関する技術

| | リアルタイム型放送サービス | 蓄積型放送サービス | 技術ポイント |
|---|---|---|---|
| 即時視聴 | チャネルに選局後出来るだけ早く出画すること | 蓄積完了後に復号し，視聴するため，即時視聴要件は無い | リアルタイム型では復号する鍵がコンテンツに同期して配信されていること |
| 同報性 | 非常に多くの視聴者が同時視聴する | 視聴可能な権利の取得は受信者毎に行う | |
| 保存 | 不要（タイムシフト視聴は私的録画の範疇） | 利用許可範囲内で，何時でも，何処でも利用可能 | 許可されていないコンテンツの蓄積や外部出力されないこと |
| 最小販売単位 | チャネル毎の番組単位 | チャネル毎の番組単位コンテンツ単位 | |

## 2.1. マルチメディア放送サービスの概要

マルチメディア放送サービスは，大別するとリアルタイム型放送サービス，蓄積型放送サービスが提供される予定である．サービスに応じてコンテンツを健全に利用されることをコンテンツ保護とアクセス制御技術も 2 つのサービスの特徴に応じてそれぞれの技術要件を表 1 にまとめる．

## 2.2. ISDB の告示，規格

狭帯域 CS デジタル放送が開始され，その後，ISDB（Integrated Services Digital Broadcasting、統合デジタル放送サービス）は 2000 年に BS で開始された以降広帯域 CS として ISDB-S，地上デジタルとして ISDB-T が開始され，固定受信を主とする基幹放送のデジタル放送が開始された．

ISDB-Tmm は従来のデジタル放送同様に総務省において「携帯端末向けマルチメディア放送方式の技術的条件」として技術的な議論が行われてきた．2010 年 4 月には告示[3]が改定され，スクランブル方式は 64 ビットブロック暗号 Multi2 に，128 ビットブロック暗号の AES, Camellia が加えられた．放送事業者が 3 つの暗号方式から選択実装することができる．今後，主要な技術規格が，委託放送事業者の決定に合わせて技術規格団体の電波産業会(ARIB)にて策定される予定である，

現行デジタル放送である地上デジタル放送とマルチメディア放送のコンテンツセキュリティに係わる技術標準等を表 2 に示す．

現在のデジタル放送は，一時期蓄積型放送が行われたことを除くと基本的にはリアルタイムで視聴することを前提とした放送である．受信契約をした受信機のみが再生できる仕組みであるアクセス制御（CAS: Conditional Access Systems）技術は ARIB STD-B25 にて規定されている．マルチメディア放送方式は，ISDB-T のアーキテクチャを同じ踏襲していることから，ARIB STD-B25 を基本として，必要な機能を拡充することで

表 2　コンテンツの暗号化方式概要

| | | マルチメディア放送 | 現行放送(ISDB-T) | IPTV（参考） |
|---|---|---|---|---|
| リアルタイム型 | スクランブル方式 | 時変鍵（数秒～数十秒）MPEG2-TS パケット単位 *2<br>総務省・告示第 40 号[3] | | (IPTV は MPEG2-TTS)<br>総務省指定なし |
| | スクランブルアルゴリズム | 規格化団体　電波産業会(ARIB) | | 民間仕様化団体 IPTV ﾌｫｰﾗﾑ |
| | | 64 ビットブロック暗号 Multi2<br>128 ビットブロック暗号 AES, Camellia | Multi2 | 事業者が独自に定める（放送の同時再送信は放送事業者間との合意）<br>多くは AES,など |
| 蓄積型 *1 | エンクリプト方式 | 主にコンテンツ毎　通常ファイル単位<br>総務省指定なし | 該当サービス運用なし | (IPTV は VOD を含む)<br>総務省指定なし |
| | エンクリプトアルゴリズム | 規格化団体　電波産業会(ARIB) | | 民間仕様化団体 IPTV ﾌｫｰﾗﾑ |
| | | 現時点では未定（ARIB STD-B25 を想定） | ARIB STD-B25[4]<br>DES 相当以上を推奨 | AES |
| ITU 国際標準化状況 | | 直接的ではないが BT.1306 System C[5] にて ARIB STD-B25 参照可能 | | X.1191[6]にて概要・要件を記載 |

*1: IPTV は VOD を含む　*2: IPTV はタイムスタンプ付き TS

実現できると考えられる.

## 3. コンテンツセキュリティ機能の設計要件

### 3.1. コンテンツ保護の観点からの設計要件

コンテンツは，放送事業者がコンテンツを入手してから，放送（補完的な通信の利用を含む），放送受信した受信機に視聴・利用されて消去されるまでのすべての区間で一定以上の保護がされていることが重要である．検討されるべきコンテンツ保護の主な項目を下記に示す.

- ・コンテンツセキュリティシステム全体
  - ➢ 用いる暗号スイートの適切性
  - ➢ 鍵長などの適切性
- ・放送設備としてのセキュリティ要件
  - ➢ 入退出管理（人的側面）
  - ➢ コンテンツ保護に係わる鍵の保管管理（重要情報の管理）
- ・受信機に関するセキュリティ要件
  - ➢ セキュリティモジュールの耐タンパー性
  - ➢ コンテンツ外部出力機能に係わる安全性
- ・契約的側面
  - ➢ 受信機製造責任者に対するセキュリティ尊守事項
  - ➢ サービス利用者に対するセキュリティモジュールに対する扱いの明確化

以上の項目を中心に必要，十分なセキュリティポリシーを定めて実装,構築,製造することが重要である.

### 3.2. 開発運用コスト観点からの設計要件

一般消費者向け商用サービスに適用するセキュリティ技術に共通した最も重要な点は，費用対効果である．コンテンツ保護の観点から，コンテンツ提供者の利益損失が起こらないようには，強いセキュリティ強度をシステムが望まれる．一方，セキュリティ強度の高いシステムは，コスト負担，セキュリティ機能を実行するためのパフォーマンス低下から使い勝手の低下となり，結果的に提供サービスコストが増加する．また，すべての要件をセキュリティ技術のみで実現するのではなく，受信者とサービス提供者の契約約款等の法的な側面を合わせて利用することが，結果的に低廉で良質なサービスを提供につながる.

## 4. 技術概要

リアルタイム型放送サービスでは，放送のアクセス制御技術として用いられている CAS のスクランブル技術を適用する．蓄積型放送サービスでは，通信機能が必須であることもあり，電子商取引の技術をコンテンツビジネスから発展してきた DRM のエンクリプト技術を適用する． CAS, DRM 技術の特徴を表３に示す. スクランブルもエンクリプトともに暗号アルゴリズムは同一技術で構成可能である.

一般的な電子商取引では，守るべきデータ（売買契約情報など）に対する供給側と消費側の利害は一致している．しかしながら，通常のコンテンツ流通ビジネスでは,商品自体であるコンテンツを保護する意識は，供給側と消費側は対局に位置する．この供給側と消費側の意識の差分をコンテンツセキュリティ技術よりバランスを取る必要がある.

### 4.1. リアルタイム型放送サービス対応技術

マルチメディア放送サービスでは有料放送も想定

表３　CAS, DRM 技術の特徴

| | CAS (Conditional Access Systems)<br>限定受信システム | DRM (Digital Rights Management)*2<br>デジタル著作権管理 |
|---|---|---|
| 特長 | ・事前に契約しておくことにより、即時視聴可能⇒チャネル選局に対応<br>・片方向のみで実現可能 | ・コンテンツ視聴直前に行うことにより、多彩な販売が可能<br>・通信機能が必要 |
| 利用技術 | 限定受信技術 | ライセンス発行技術*2 |
| 視聴者認証 | 端末組み込みあるいはカードなどの ID 付きクライアントにより識別 | 相手認証機能を利用（公開鍵暗号、署名機能） |
| コンテンツ復号鍵の発行 | 暗号機能（共通鍵暗号）コンテンツに多重して送出可能（EMM） | 暗号機能（公開鍵暗号。共通鍵暗号でも実現可）（ライセンス発行） |
| 暗号･復号 | 暗号機能（共通鍵暗号）(EMM) | 暗号機能（共通鍵暗号） |
| 利用範囲 | コピー条件などシンプルな指定のみ | コンテンツの利用条件（コピー回数、外部出力、再生時間など多彩な設定が可能） |
| 利用履歴確認 | 通信を用いた事後確認型と事前確認型*1 | ライセンス発行時に把握可能なため運用不要 |
| 放送での利用 | リアルタイム型放送サービス | 蓄積型放送サービス |
| IPTV での利用 | マルチキャスト型サービス | ユニキャスト型サービス（VOD, ダウンロード） |

*1 通信回線が常時利用できる場合には，視聴前の事前確認型適する
*2 多用されるが定義された用語ではない

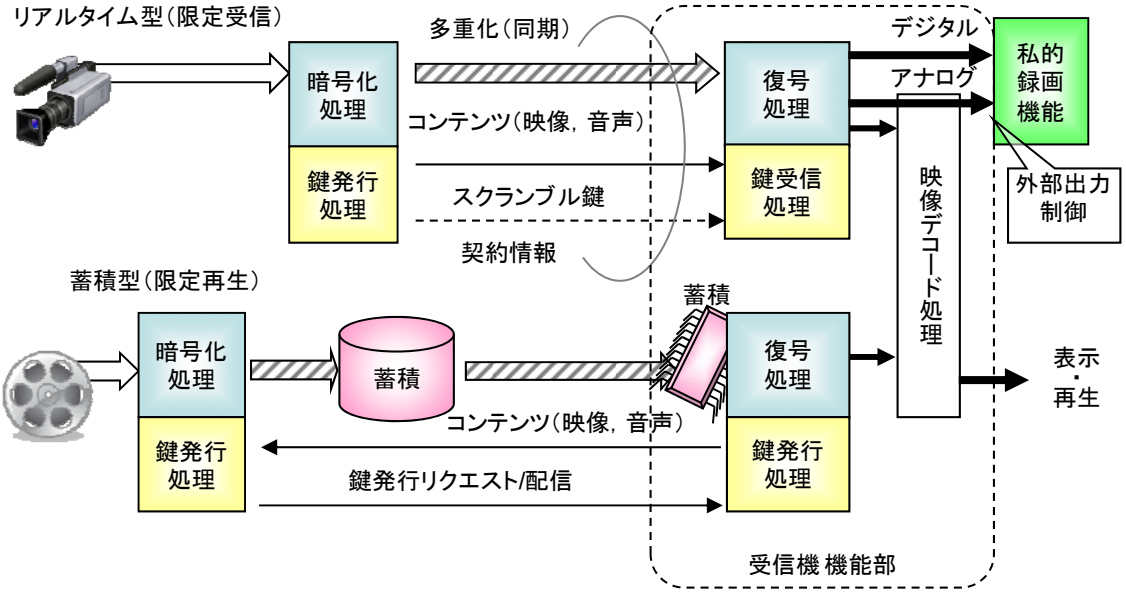


図2 アクセス制御技術とコンテンツ保護技術

上段: スクランブル方式，下段:エンクリプト方式

されるため．BS 放送や広帯域 CS 放送の有料放送で現在利用されている技術方式の標準規格である ARIB STD-B25 を基本として実現できる．ただし，受信機の形状が固定受信ではなく，携帯電話などのベースとした移動型の受信機であることから以下のような特徴に応じた実装の工夫が必要であると考えられる．

- IC カードあるいは SIM カードを中心に規格化されているが受信機実装の観点からは，物理的な形状を特定しない方式とすることが重要である
- 帯域の狭い 1 セグメントのみでの有料放送を実現するため，加入者毎の個別情報である EMM (Entitlement Management Message)の配信は主に通信機能を利用する
- 携帯電話などにも実装されているセキュリティ機能を共通化することで，受信機の低廉化を図る

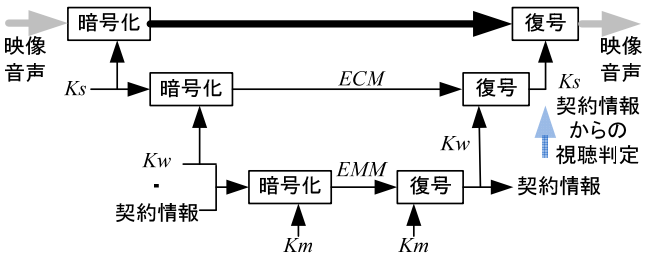


図 3　限定受信方式

図 2 の上部にリアルタイム型放送サービスを実現するシステムの概要図を示す．リアルタイム型放送サービスの限定受信方式を図 3 に示す．

現行の放送では PPV (Pay Per View)と呼ばれる番組毎の販売方法は，視聴機会を優先し，主に電話網を利用した後払い方式が運用されたことがあった．当時，受信機の電話網への接続率が低いことに課題があった．マルチメディア放送のサービス開始当初は携帯電話一体型受信機が主となる考えられることら，IPTV と同様常時利用できる通信機能を積極的に用いることができる．

## 4.2. 蓄積型放送サービス対応技術

現在の商用放送としては，蓄積型放送サービスは利用されていない．留意点としてハードディクスレコーダなどのデジタル録画機能は，受信者のタイムシフト目的の私的利用であり，放送事業者が直接的に提供するサービスではない．

すでにサーバー型放送サービスの検討結果が ARIB TR-B27[7]として技術資料にまとめれている．蓄積型放送サービスは，サーバー型放送サービスの一部の機能を具体化することにより実現できると考えられる．また，実現技術仕様としては，表 2 に参考記載した IPTV 分野のユニキャストでのサービスである VOD，ダウンロードサービスのが DRM 参考になる．

図 2 の下部に蓄積型放送サービスを実現するシステムの概要図を示す．下記に特徴を整理する．

- コンテンツ（番組）を視聴するために，鍵発行センタに鍵発行リクエストする．鍵発行条件が整っていれば，鍵発行を行う．
- 鍵発行内容には，
  ①対象コンテンツをリング付ける情報
  ②コンテンツを復号するための鍵

③利用期間，回数等のコンテンツの利用保護条件 RMPI (Right Management and Protection Information) が含まれる

## 5. セキュリティ実装技術に関する課題

デジタル放送においては，車載型の一部や有料放送を前提としない１セグ受信機を除き固定受信機が主として設計されている．今回のマルチメディア放送は有料放送を含めた移動受信機を中心に考えた本格的な放送・通信連携型サービスである．放送技術を IPTV に適用し発展してきた機能を放送・通信連携型サービスとして一体化することになる．その観点からコンテンツセキュリティ機能としても CAS, DRM の両方の機能を実装することが必要になる．

受信機としては，携帯電話として限られた容積内にコンテンツセキュリティ機能を実装することになるため様々な工夫が必要になると考えられる．

１セグ受信機のように普及させるためには，低コストでセキュリティ強度を低下させない実装技術が重要となる．

## 6. おわりに

マルチメディア放送は，総務省の省令，告示，一次答申が示された段階であり．2010 年の将来開始されための準備段階である．本稿は，現在準備が進められてるコンテンツセキュリティ機能の方向性とその背景を中心に述べた．

今後さらに，委託放送事業者の決定等具体化に合わせて，重要な技術方式が具体化すると同時に技術規格の整備とともに，今後実装形態などの詳細が検討されることなると考えられる．

## 文　献

[1] 総務省情報流通行政局：“「放送システムに関する技術的条件」のうち「携帯端末向けマルチメディア放送方式の技術的条件」”，携帯端末向けマルチメディア放送方式の技術的条件 情報通信審議会からの一部答申 (Oct.2010)

[2] ITU-R BT.1833：“Broadcasting of multimedia and data applications for mobile reception by handheld receivers”， (2010)

[3] 総務省告示第 40 号：“スクランブルの方式”，平成二十二年四月二十三日総務省告示第百七十号 (Apri.2010)

[4] ARIB STD-B25 5.1 版：“デジタル放送におけるアクセス制御方式”， (Mar. 2009)

[5] ITU-R BT.1306-4：“Error-correction, data framing, modulation and emission methods for digital terrestrial television broadcasting”，ITU-R (Sept. 2009)

[6] ITU-T X.1191：“Functional requirements and architecture for IPTV security aspects”，ITU-T (Feb. 2009)

[7] ARIB TR-B27 1.0 版：“サーバー型放送 第五編サーバー型放送アクセス制御方式運用方法及び受信機機能”， (Spet. 2006)