



# デジタル放送におけるアクセス制御方式

CONDITIONAL ACCESS SYSTEM SPECIFICATIONS  
FOR DIGITAL BROADCASTING

## 標準規格

ARIB STANDARD

### ARIB STD-B25 6.7版

1999年10月26日	策	定
2000年 3月29日	1. 1	改定
2000年 7月25日	1. 2	改定
2000年10月12日	1. 3	改定
2001年 3月27日	2. 0	改定
2001年 5月31日	3. 0	改定
2002年 7月25日	3. 1	改定
2003年 2月 6日	4. 0	改定
2003年 6月 5日	4. 1	改定
2006年 5月29日	4. 2	改定
2007年 3月14日	5. 0	改定
2009年 3月18日	5. 1	改定
2011年 3月28日	6. 0	改定
2012年 7月 3日	6. 1	改定
2012年 9月25日	6. 2	改定
2013年12月10日	6. 3	改定
2014年 7月31日	6. 4	改定
2015年 3月17日	6. 5	改定
2018年 4月12日	6. 6	改定
2019年 1月21日	6. 7	改定

一般社団法人 電 波 産 業 会

Association of Radio Industries and Businesses



## ま え が き

一般社団法人電波産業会は、無線機器製造者、電気通信事業者、放送機器製造者、放送事業者及び利用者の参加を得て、各種の電波利用システムに関する無線設備の標準的な仕様等の基本的な要件を「標準規格」として策定している。

「標準規格」は、周波数の有効利用及び他の利用者との混信の回避を図る目的から定められる国の技術基準と、併せて放送設備、無線設備の適性品質、互換性の確保等、放送機器製造者、放送事業者、無線機器製造者、電気通信事業者及び利用者の利便を図る目的から策定される民間の任意基準を取りまとめて策定される民間の規格である。

本標準規格は、「デジタル放送におけるアクセス制御方式」について策定されたもので、策定段階における公正性及び透明性を確保するため、内外無差別に広く無線機器製造者、電気通信事業者、放送機器製造者、放送事業者及び利用者の利害関係者の参加を得た当会の規格会議の総意により策定されたものである。

本標準規格が、無線機器製造者、電気通信事業者、放送機器製造者、放送事業者及び利用者に積極的に活用されることを希望する。

### 注意：

本標準規格では、本標準規格に係わる必須の工業所有権に関して特別の記述は行われていないが、当該必須の工業所有権の権利所有者は、「本標準規格に係わる工業所有権である別表 1 及び別表 2 に掲げる権利は、別表 1 及び別表 2 に掲げる者の保有するところのものであるが、本標準規格を使用する者に対し、別表 1 の場合には一切の権利主張をせず、無条件で当該別表 1 に掲げる権利の実施を許諾し、別表 2 の場合には適切な条件の下に、非排他的かつ無差別に当該別表 2 に掲げる権利の実施を許諾する。ただし、本標準規格を使用する者が本標準規格で規定する内容の全部又は一部が対象となる必須の工業所有権を所有し、かつ、その権利を主張した場合、その者についてはこの限りではない。」旨表明している。

別表 1

(第一号選択)

(なし)

別表 2

(第二号選択)

特許出願人	発明の名称	出願番号等	備考
日本放送協会	放送方式および情報記憶媒体	特願平 3-141770 特開平 4-365227 特許 3103617 号	日本
	データ放送受信システム	特願平 2-221796 特開平 4-104559 特許 3068634 号	日本
松下電器産業(株)	放送受信装置	特願平 10-098217 特開平 11-284976	日本
	放送システム、及び、受信装置からのデータ通信方法	特願平 10-253323 特開平 2000-69108	日本
	放送システムでのメッセージ伝送方法	特願平 10-313928 特開平 2000-125272	日本
	放送システムでのメッセージ伝送方法	特願平 10-316999 特開平 2000-134666	日本
	ARIB STD-B25 5.0 版について包括確認書を提出(*6)		
日本ビクター (株)	再生プロテクト方法及びプロテクト再生装置(*1)	特許 2853727 号	日本、米国、独、英、仏、韓国、インド、中国
	情報記録方法及び情報記録媒体(*1)	特許 3102416 号	日本
(株)日立製作所 (株)日立コントロールシステムズ	暗号方式(*2)	特願昭 63-103919	日本、米国
	暗号化方法及び復号化装置(*2)	特願平 9-329841	日本、米国
	暗号変換装置(*2)	特願平 9-329842	日本、米国
(株)東芝	放送受信システム(*3)	特許 2941398 号	日本
	放送受信装置および契約管理装置 (*5)	特開平 11-243536	日本、米国
	ARIB STD-B25 5.0 版について包括確認書を提出(*6)		
日本放送協会	コンテンツ送信装置、コンテンツ受信装置およびコンテンツ送信プログラム、コンテンツ受信プログラム(*4)	特願 2001-307559	日本、米国、独、英、仏
	コンテンツ利用制御送信方法、コンテンツ利用制御受信方法およびコンテンツ利用制御送信装置、コンテンツ利用制御受信装置ならびにコンテンツ利用制御送信プログラム、コンテンツ利用制御受信プログラム(*4)	特願 2001-349539	日本、米国、独、英、仏
モトローラ株式会社	ARIB STD-B25 4.0 版について包括確認書を提出(*4)		
QUALCOMM Incorporated	ARIB STD-B25 6.0 版について包括確認書を提出(*7)		

特許出願人	発明の名称	出願番号等	備考
QUALCOMM Incorporated	Apparatus and method for installing a decryption key (*8)	JP4597513	US7,203,319; BR; CN; EP; HK; IN; KR; MX
	System and method for controlling broadcast multimedia using plural wireless network connections (*8)	JP2006523386	JP; JP; US7,925,203; US2011014365 3; BR; CN; EP; HK; IL; IN; KR; MX
	Apparatus and methods for securing architectures in wireless networks (*8)	JP2009-515251	US2007019097 7; CN; EP; HK; IN; KR; KR; TW
ソニー株式会社	ARIB STD-B25 6.4 版について包括確認書を提出(*9)		
富士通 (株)	通信システムおよび通信方法 (*10)	特許第 4603570 号 特願 2007-228363 号	JP
	受信機および受信機により実行される方法(*11)	特許第 4791521 号 特願 2008-312279 号	JP
	通信システム(*12)	特許第 4791583 号 特願 2010-073798 号	JP

(\*1)1.3 版より有効 (平成 13 年 3 月 15 日提出)

(\*2)ARIB STD-B25 3.0 版改定時に ARIB STD-B20 から移行

(\*3)3.0 版より有効 (平成 13 年 5 月 21 日提出)

(\*4)4.0 版の改定部分に対して有効

(\*5)4.1 版の改定部分 (第 1 部第 6 章) に対して有効

(\*6)5.0 版の改定部分に対して有効 (平成 19 年 3 月 7 日受付)

(\*7)6.0 版の改定部分に対して有効 (平成 23 年 3 月 18 日受付)

(\*8)6.0 版の改定部分に対して有効 (平成 23 年 10 月 7 日受付)

(\*9)6.4 版の改定部分に対して有効 (平成 26 年 7 月 24 日受付)

(\*10)5.1 版の改定部分に対して有効 (2018 年 10 月 19 日受付)

(\*11)6.0 版の改定部分に対して有効 (2018 年 10 月 19 日受付)

(\*12)6.0 版の改定部分に対して有効 (2018 年 10 月 19 日受付)



## 総 合 目 次

まえがき

第1部 受信時の制御方式（限定受信方式） ..... 1

第2部 再生時の制御方式（限定再生方式） ..... 239

第3部 受信時の制御方式（コンテンツ保護方式） ..... 311

第4部 セグメント連結伝送方式による地上マルチメディア放送のアクセス制御方式 ..... 411

改定履歴表





## 第 1 部

受信時の制御方式（限定受信方式）



## 第 1 部 目 次

第 1 章	一般事項	1
1.1	目的	1
1.2	適用範囲	1
1.3	参照文書	2
1.3.1	準拠文書	2
1.3.2	関連文書	2
1.4	用語・略語	3
第 2 章	機能仕様	5
2.1	スクランブル及び関連情報の仕様	5
2.1.1	総合的機能	5
2.1.2	放送サービスの形態	5
2.1.3	料金設定方式	6
2.1.4	料金収納方式	8
2.1.5	契約形態	8
2.1.6	視聴情報の収集	8
2.1.7	EMM の送信	9
2.1.8	ECM の送信	9
2.1.9	番組運行管理システム	9
2.1.10	セキュリティ機能	10
2.1.11	プレビュー	10
2.1.12	再放送課金制御	10
2.2	受信機に関わる仕様	10
2.2.1	IC カード	10
2.2.2	受信機本体	11
第 3 章	スクランブル及び関連情報の技術仕様	17
3.1	スクランブルサブシステム	17
3.1.1	スクランブル方式	17
3.1.2	スクランブルの手順	18
3.1.3	MULTI2 暗号	19
3.1.4	暗号化の基本関数	20
3.1.5	スクランブルを施す階層	21

3.1.6	スクランブルの範囲.....	21
3.1.7	スクランブルの単位.....	21
3.1.8	同一鍵の使用時間.....	21
3.2	関連情報サブシステム.....	21
3.2.1	関連情報の種類.....	21
3.2.2	関連情報の形式.....	22
3.2.3	ECM.....	22
3.2.4	EMM.....	24
3.2.5	メッセージ情報 (EMM/ECM).....	27
3.2.6	関連情報の伝送方法.....	36
第4章	受信機に関わる技術仕様.....	37
4.1	受信機の概要.....	37
4.2	ユーザインタフェース.....	37
4.2.1	仮想ユーザインタフェース.....	37
4.2.2	電源オン.....	37
4.2.3	番組視聴.....	38
4.2.4	番組予約 [オプション].....	45
4.2.5	エラー通知画面.....	51
4.2.6	自動表示メッセージ.....	53
4.2.7	CA 関連機能メインメニュー.....	53
4.2.8	PPV 購入記録表示 [オプション].....	54
4.2.9	メール表示.....	54
4.2.10	カード情報表示.....	55
4.2.11	システム設定.....	55
4.2.12	トラブル履歴表示 [オプション].....	64
4.3	CA インタフェース.....	64
4.3.1	インタフェースの機能.....	64
4.3.2	IC カードインタフェース仕様.....	65
4.3.3	コマンド/レスポンス.....	75
4.4	EMM 受信機能 (受信の効率化).....	109
4.4.1	EMM のフィルタリング.....	109
4.4.2	EMM の受信機能.....	109
4.5	通信機能.....	109
4.5.1	視聴情報収集通信における受信機動作.....	110

4.5.2	DIRD データ通信における受信機動作 .....	136
4.6	EMM メッセージ表示.....	141
4.7	SI との関連 .....	143
4.7.1	EMM 特定チャンネル伝送 .....	143
4.7.2	PPV 関連.....	143
4.7.3	EMM メッセージ受信関連 .....	145
4.8	スクランブル有無の判定.....	146
4.9	同時に処理可能なスクランブル鍵の数.....	146
4.10	同時に処理可能な PID 数.....	146
第 5 章	各メディア及び受信形態への本 CAS - R 方式の適用 .....	147
5.1	BS デジタル放送、広帯域 CS デジタル放送、地上デジタルテレビジョン放送 及び地上デジタル音声放送の固定受信への本 CAS - R 方式の適用 .....	147
5.2	地上デジタルテレビジョン放送及び地上デジタル音声放送の移動・携帯受信 への本 CAS - R 方式の適用.....	147
5.2.1	概要 .....	147
5.2.2	機能仕様.....	147
5.2.3	技術仕様.....	149

## 参考資料

参考 1 限定受信方式の解説 .....	151
1. 概要 .....	151
1.1 システムの概要 .....	151
1.2 事業・運用環境 .....	151
2. EMM メッセージ概要 .....	152
2.1 EMM メッセージの基本的な考え方 .....	152
3. 通電制御の運用 .....	155
3.1 DIRD の基本動作 .....	156
3.2 契約変更 EMM の伝送運用例 .....	157
3.3 特定ストリーム伝送 .....	158
4. グローバル ID .....	158
4.1 適用例 .....	158
4.2 留意すべき点 .....	159
5. スクランブル有無の判定 .....	160
6. PPV 番組プレビュー機能の運用事例 .....	161
7. 再放送課金制御機能の運用事例 .....	162
8. IC カード コマンド／レスポンスの動作シナリオ .....	162
8.1 カード挿入／電源 ON .....	163
8.2 グループ ID 更新 .....	164
8.3 ECM 受信（ティア） .....	164
8.4 PPV 番組購入 .....	165
8.5 EMM 受信 .....	166
8.6 契約確認 .....	167
8.7 EMM メッセージ受信／表示（自動表示メッセージ） .....	168
8.8 EMM メッセージ受信／表示（メール） .....	169
8.9 視聴情報収集センタ通信発呼（アップロードデータがある場合） .....	170
8.10 視聴情報収集センタ通信発呼（アップロードデータがない場合） .....	171
8.11 DIRD データ送信 .....	172
8.12 前払い残金確認 .....	173
8.13 カード ID 情報取得 .....	173
8.14 ユーザ発呼 .....	174
9. 相互認証システムと Ks 暗号化 .....	175

参考 2 受信機本体機能仕様の解説.....	177
1. 受信機の構成.....	177
2. 受信機の動作状態と遷移.....	179
2.1 受信機の基本状態と状態遷移.....	179
2.2 IC カードの状態と状態遷移.....	180
3. 受信機の各種機能詳細.....	181
3.1 省電力化.....	181
3.2 時刻タイマ.....	182
3.3 基本ユーザ入力と表示.....	182
3.4 デスクランブラ.....	182
3.5 IC カードの通信制御.....	183
3.6 電話モデム等と基本通信.....	186
3.7 視聴履歴情報の伝送.....	187
3.8 通電発呼制御.....	188
3.9 DIRD データの伝送.....	190
3.10 ECM の受信とデスクランブラ制御.....	191
3.11 EMM、EMM メッセージの受信.....	191
3.12 通電制御.....	195
3.13 特定チャンネル受信による EMM の受信と処理.....	197
3.14 EMM メッセージ制御.....	198
3.15 番組視聴.....	202
3.16 番組の予約.....	215
3.17 パスワードの消去.....	219
3.18 パレンタルコントロール.....	219
3.19 カード情報の表示.....	219
3.20 PPV 購入記録と表示.....	219
3.21 PPV 番組購入月額上限の制御.....	219
3.22 PPV 購入金額制限の制御.....	219
3.23 回線接続の検査.....	220
3.24 履歴表示.....	220
3.25 システム設定.....	220
3.26 リトライオーバー通知表示機能.....	220
3.27 ユーザ発呼要求機能.....	220
4. 別表.....	221
参考 3 運用について.....	223

1. 運用形態.....	223
2. 鍵管理.....	223
2.1 ID/Kmi 等管理.....	223
2.2 CA モジュールの管理.....	223
2.3 暗号化.....	223
2.4 システムパラメータの管理.....	223
3. 視聴情報の収集.....	223
3.1 視聴情報の暗号化.....	224
3.2 ネットワークプロトコルに対する前提条件.....	224
3.3 高速モデム・携帯電話/PHS (PIAFS) 用データ通信機能の利用に関して.....	225
4. 顧客管理.....	225
4.1 フラット/ティア課金への対応.....	225
4.2 PPV 課金への対応.....	226
5. カスタマセンタ.....	226
5.1 問い合わせ応答.....	226
5.2 Call Ahead PPV 申し込み受付.....	226
5.3 オンライン EMM の送出手を、顧客管理システムに指示する。.....	226
6. 課金徴収.....	226
6.1 事業者統合の課金.....	226
6.2 事業者単位の課金.....	226
7. CAS 認証システム.....	226
8. EMM の送信.....	227
9. ECM の送出頻度.....	229
10. 番組運行管理システム.....	229
参考 4 CA インタフェースに関する補足説明.....	231
1. VCC 端子 (第 4 章 4.3.2.3 の(1)).....	231
2. Vpp 端子 (第 4 章 4.3.2.3 の(2)).....	231
3. CLK 端子 (第 4 章 4.3.2.3 の(3)).....	231
4. ATR(AnswerToReset) (第 4 章 4.3.2.3 の(4)).....	232
4.1 ATR 送出データ (第 4 章 4.3.2.3 の(4-4)).....	232
5. 伝送プロトコル形式 (第 4 章 4.3.2.3 の(6)).....	234
5.1 サブフィールドのコーディング方式 (第 4 章 4.3.2.3 の(6-3)).....	234
6. プロトコル制御 (第 4 章 4.3.2.3 の(7)).....	235
6.1 チェイニング (第 4 章 4.3.2.3 の(7-2)).....	235
6.2 IFSD の変更 (第 4 章 4.3.2.3 の(7-3)).....	235



6.3	RESYNC (第4章 4.3.2.3 の(7-4))	235
6.4	ABORT (第4章 4.3.2.3 の(7-5))	235
6.5	エラー回復 (第4章 4.3.2.3 の(7-6))	235
7.	コマンド/レスポンスの「コマンド APDU」(第4章 4.3.3.1 の(1)) のうちの項目	236
参考5	各種識別情報の運用例	237
1.	各種識別情報の関係	237
2.	代表的な識別情報の発番運用に関する考え方	238
2.1	限定受信方式識別	238
2.2	プロトコル番号	238
2.3	事業者識別	238

## 第 2 部

再生時の制御方式（限定再生方式）



## 第 2 部 目 次

第 1 章	一般事項	239
1.1	目的	239
1.2	適用範囲	239
1.3	参照文書	239
1.3.1	準拠文書	239
1.3.2	関連文書	240
1.4	用語・略語	240
第 2 章	ストリーム型コンテンツのアクセス制御方式	243
2.1	一般事項	243
2.2	機能仕様	243
2.2.1	スクランブル及び関連情報の仕様	243
2.3	スクランブル及び関連情報の技術仕様	248
2.3.1	スクランブルサブシステム	248
2.3.2	ストリーム型アクセス制御方式の関連情報サブシステム	251
2.4	ストリーム型アクセス制御簡易方式	272
第 3 章	ファイル型コンテンツのアクセス制御方式	273
3.1	一般事項	273
3.2	機能仕様	273
3.2.1	エンクリプト及び関連情報の仕様	273
3.2.2	放送サービスの形態	273
3.3	エンクリプト方式	276
3.3.1	エンクリプトの対象	276
3.3.2	エンクリプトの単位	276
3.3.3	エンクリプトアルゴリズム	276
3.3.4	エンクリプトの識別	276
3.4	関連情報サブシステム	277
3.4.1	関連情報の種類	277
3.4.2	ACI	277
3.4.3	EMM	278
3.4.4	ACI の位置指定	279
3.4.5	EMM の伝送位置指定	285

参考 1 限定再生方式の解説 .....	287
1. 概要 .....	287
1.1 システムの概要 .....	287
1.2 アクセス制御の観点から見たサーバー型放送のサービスの分類 .....	288
1.3 サービスの例 .....	288
1.4 アクセス制御方式に求められる機能 .....	290
2. 技術的条件 .....	292
2.1 システム概要 .....	292
2.2 ストリーム型アクセス制御方式 .....	296
2.3 ACIの参照にコンテンツ情報ヘッダ及びACG記述子を用いる場合のファイル型アクセス制御方式 .....	299
2.4 ACIの参照にライセンスリンク情報を用いる場合のファイル型アクセス制御方式 .....	304
参考 2 運用について .....	307
1. ファイル型コンテンツサービスにおけるエンクリプトとスクランブルの関係 .....	307
2. 複製への対処 .....	307
2.1 スクランブル/エンクリプトが施された状態での複製 .....	307
2.2 再生時のアクセス制御が行われた後のスクランブル/エンクリプトが解かれた状態での複製 .....	307
3. エンクリプト識別の扱い .....	308
4. 共通情報について .....	308
4.1 レンタルビデオサービス .....	308
4.2 音楽配信サービス .....	309

## 第3部

受信時の制御方式  
(コンテンツ保護方式)



## 第3部 目次

第1章	一般事項	311
1.1	目的	311
1.2	適用範囲	311
1.3	参照文書	311
1.3.1	準拠文書	311
1.3.2	関連文書	311
1.4	用語・略語	312
第2章	機能仕様	315
2.1	スクランブル及び関連情報の仕様	315
2.1.1	基本的考え方	315
2.1.2	コンテンツ保護方式に求められる各種要件	315
2.1.3	総合的機能	316
2.1.4	放送サービスの形態	316
2.1.5	EMM の伝送	317
2.1.6	ECM の伝送	317
2.1.7	セキュリティ機能	317
2.2	受信機に関わる仕様	318
2.2.1	ID	318
2.2.2	基本ユーザ入力と表示	318
2.2.3	番組の選択視聴	318
2.2.4	デスクランブラ	318
2.2.5	ECM の受信	318
2.2.6	EMM の受信	319
2.2.7	耐タンパ性	319
2.2.8	権利保護情報改ざん防止機能	319
2.2.9	EMM メッセージの受信	319
2.2.10	EMM メッセージ制御	319
第3章	スクランブル及び関連情報の技術仕様	321
3.1	スクランブルサブシステム	321
3.1.1	スクランブル方式	321
3.1.2	スクランブルの手順	321
3.1.3	MULTI2 暗号	322
3.1.4	暗号化の基本関数	323
3.1.5	スクランブルを施す階層	324
3.1.6	スクランブルの範囲	324



3.1.7	スクランブルの単位.....	324
3.1.8	同一鍵の使用時間.....	324
3.1.9	システム鍵.....	324
3.1.10	CBC 初期値.....	324
3.2	関連情報サブシステム.....	325
3.2.1	システムの基本原理.....	325
3.2.2	本コンテンツ保護方式の構成.....	326
3.2.3	関連情報の種類.....	327
3.2.4	関連情報の形式.....	328
3.2.5	関連情報の暗号化方式.....	328
3.2.6	ECM.....	329
3.2.7	EMM.....	340
3.2.8	メッセージ情報 (EMM/ECM).....	350
3.2.9	関連情報の伝送方法.....	361
第4章	受信機に関わる技術仕様.....	363
4.1	受信機の概要.....	363
4.2	ユーザインタフェース.....	363
4.2.1	番組視聴画面／視聴不可通知画面.....	363
4.2.2	自動表示メッセージ.....	365
4.2.3	メール表示.....	365
4.3	スクランブル有無の判定.....	365
4.4	同時に処理可能なスクランブル鍵の数.....	366
4.5	同時に処理可能な PID 数.....	366
4.6	本コンテンツ保護方式の実装.....	366
4.7	記憶データ.....	366
4.7.1	記憶データの区分.....	366
4.7.2	共通データ.....	367
4.7.3	局個別データ.....	368
4.7.4	権利保護情報関連データ.....	370
4.7.5	メッセージ情報関連データ.....	371
4.8	本コンテンツ保護方式に関する受信機処理.....	372
4.8.1	ECM の処理.....	372
4.8.2	デスクランブル処理.....	382
4.8.3	EMM の処理.....	382
4.9	EMM メッセージに関する受信機処理.....	390
4.9.1	EMM メッセージ機能.....	390
4.9.2	SI との関連.....	392

4.9.3	個別 ID の生成 .....	392
4.9.4	EMM 個別メッセージの受信処理 .....	392
4.9.5	EMM 共通メッセージの受信処理 .....	395
参考 1	.....	399
1.	本コンテンツ保護方式の運用概要 .....	399
1.1	基本的な運用 .....	399
1.1.1	運用管理 .....	399
1.1.2	ECM, EMM の伝送 .....	399
1.1.3	受信機 .....	399
1.1.4	別表 .....	400
1.2	受信機における特定の鍵の無効化運用 .....	402
1.2.1	鍵の無効化の目的 .....	402
1.2.2	デバイス ID / デバイス鍵更新 .....	402
1.2.3	鍵の無効化の基本的な実行 .....	402
1.3	受信機メーカーに供与される情報の例 .....	403
1.4	受信機メーカーが抛出する情報の例 .....	404
参考 2	.....	405
1.	デバイス ID とデバイス鍵の世代更新 .....	405
参考 3	.....	407
1.	EMM メッセージの解説 .....	407
1.1	EMM メッセージの基本的な考え方 .....	407
1.1.1	概要 .....	407
1.1.2	EMM 共通メッセージ .....	407
1.1.3	EMM 個別メッセージ .....	408
1.1.4	自動表示メッセージ .....	408
1.1.5	個別 ID と指定 ID .....	409
1.1.6	別表 .....	409

## 第 4 部

セグメント連結伝送方式による  
地上マルチメディア放送のアクセス制御方式



## 第 4 部 目 次

第 1 章	一般事項	411
1.1	目的	411
1.2	適用範囲	411
1.3	参照文書	412
1.3.1	準拠文書	412
1.3.2	関連文書	412
1.4	用語・略語	413
第 2 章	リアルタイム型放送サービスのアクセス制御方式	415
2.1	一般事項	415
2.2	機能仕様	415
2.2.1	スクランブル及び関連情報の仕様	415
2.3	受信機に関わる仕様	419
2.3.1	アクセス制御部	419
2.3.2	受信機本体	419
2.4	スクランブル及び関連情報の技術仕様	422
2.4.1	スクランブルサブシステム	422
2.4.2	関連情報サブシステム	436
2.4.3	関連情報の伝送方法	442
第 3 章	ダウンロード型放送コンテンツのアクセス制御方式	443
3.1	一般事項	443
3.2	機能仕様	443
3.2.1	エンクリプト及び関連情報の仕様	443
3.3	エンクリプト方式	446
3.3.1	エンクリプトの対象	446
3.3.2	エンクリプトの単位	446
3.3.3	エンクリプトアルゴリズム	446
3.3.4	エンクリプトの識別	446
3.4	関連情報サブシステム	447
3.4.1	関連情報の種類	447
3.4.2	ライセンス	447
第 4 章	受信機に関わる技術仕様	449

4.1	受信機の概要.....	449
4.2	ユーザインタフェース .....	449
4.2.1	受信機機能の起動 .....	449
4.2.2	番組視聴.....	449
4.2.3	番組予約.....	450
4.2.4	エラー通知画面 .....	450
4.2.5	自動表示メッセージ.....	451
4.2.6	アクセス制御部関連機能メインメニュー .....	451
4.2.7	PPV 購入記録表示 .....	451
4.2.8	アクセス制御部情報表示.....	451
4.3	EMM 受信機能 (受信の効率化) .....	451
4.3.1	EMM のフィルタリング .....	451
4.4	通信機能.....	451
4.5	スクランブル有無の判定.....	452