



ARIB STD-B61

デジタル放送におけるアクセス制御方式（第2世代） 及びCASプログラムのダウンロード方式

CONDITIONAL ACCESS SYSTEM (SECOND GENERATION)
AND CAS PROGRAM DOWNLOAD SYSTEM SPECIFICATIONS
FOR DIGITAL BROADCASTING

標 準 規 格

ARIB STANDARD

ARIB STD-B61 2.0版

2014年 7月31日 策 定

2025年 3月25日 2.0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、併せて無線設備、放送設備の適性品質、互換性の確保等、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（第2世代）及びCASプログラムのダウンロード方式」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。

なお、詳細については、当会ホームページ (<https://www.arib.or.jp/>) の IPR ポリシーに掲載の「標準規格に係る工業所有権の取扱いに関する基本指針」を参照のこと。

ARIB STD-B61

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	ARIB STD-B61 1.0 版について包括確認書を提出*1		
一般財団法人 NHK エンジニアリングシステム	ARIB STD-B61 1.0 版について包括確認書を提出*1		
ソニー株式会社	ARIB STD-B61 1.0 版について包括確認書を提出*1		

*1 : ARIB STD-B61 1.0 版に対して有効 (平成 26 年 7 月 24 日受付)

総合目次

まえがき

第一編 アクセス制御方式（第2世代）

第1部 スランブル方式	1
第2部 コンテンツ保護方式	57
第3部 限定受信方式	115

第二編 ダウンローダブル CAS209

改定履歴表

第一編

アクセス制御方式（第 2 世代）

第 1 部 スクランブル方式

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	1
1.3.1 準拠文書	1
1.3.2 関連文書	1
1.4 用語・略語	2
第2章 機能仕様	5
2.1 スクランプルの仕様	5
2.1.1 基本的考え方	5
2.1.2 スクランプル方式に求められる各種要件	5
2.1.3 スクランプル方式の暗号アルゴリズム	5
2.2 受信機に関わる仕様	6
2.2.1 デスクランブラ	6
2.2.2 スクランプル方式の暗号アルゴリズムの判別	6
2.2.3 メッセージ認証	6
第3章 スクランプルの技術仕様	7
3.1 MPEG-2 TS 方式におけるスクランブルサブシステム	7
3.1.1 スクランプル方式	7
3.1.2 スクランプルの手順と暗号化の基本関数	7
3.1.2.1 AES 暗号を用いたスクランブルの手順	8
3.1.2.2 Camellia 暗号を用いたスクランブルの手順	9
3.1.3 スクランプルを施す階層	10
3.1.4 スクランプル範囲	10
3.1.5 スクランプル単位	10
3.1.6 同一鍵の使用時間	10
3.1.7 CBC 初期値	10
3.2 MMT・TLV 方式におけるスクランブルサブシステム	11
3.2.1 スクランプル方式	11
3.2.2 スクランプルの手順と暗号化の基本関数	11
3.2.2.1 AES 暗号を用いたスクランブルの手順	12
3.2.2.2 Camellia 暗号を用いたスクランブルの手順	13
3.2.3 スクランプルを施す階層	13
3.2.4 スクランプル範囲	13

3.2.5 スクランブル単位.....	13
3.2.6 同一鍵の使用時間.....	13
3.2.7 メッセージ認証	14
3.2.8 スクランブル関連情報の伝送	14
3.3 スクランブルサブシステムにおける暗号アルゴリズムの詳細.....	16
3.3.1 AES 暗号	16
3.3.2 Camellia 暗号	19
第 4 章 スクランブルの技術仕様（高度地上デジタルテレビジョン放送）	23
4.1 MMT・TLV 方式におけるスクランブルサブシステム	23
4.1.1 スクランブル方式.....	23
4.1.2 スクランブルの手順と暗号化の基本関数.....	23
4.1.2.1 AES 暗号を用いたスクランブルの手順（CTR モード）	24
4.1.2.2 AES 暗号を用いたスクランブルの手順（CBC モード）	24
4.1.2.3 Camellia 暗号を用いたスクランブルの手順（CTR モード）	25
4.1.2.4 Camellia 暗号を用いたスクランブルの手順（CBC モード）	25
4.1.3 スクランブルを施す階層.....	25
4.1.4 スクランブル範囲.....	25
4.1.5 スクランブル単位.....	26
4.1.6 同一鍵の使用時間.....	26
4.1.7 メッセージ認証	26
4.1.8 スクランブル関連情報の伝送	26
4.2 スクランブルサブシステムにおける暗号アルゴリズムの詳細.....	29
4.2.1 AES 暗号（鍵長 128 ビットの場合）	29
4.2.2 AES 暗号（鍵長 192 ビットの場合）	32
4.2.3 AES 暗号（鍵長 256 ビットの場合）	35
4.2.4 Camellia 暗号（鍵長 128 ビットの場合）	38
4.2.5 Camellia 暗号（鍵長 192 ビットの場合）	42
4.2.6 Camellia 暗号（鍵長 256 ビットの場合）	46
第 5 章 受信機に関わる技術仕様.....	47
5.1 受信機の概要.....	47
5.2 スクランブル有無の判定	47
5.2.1 MPEG-2 TS 方式における TS パケットのスクランブル有無の判定	47
5.2.2 MMT・TLV 方式における MMTP パケットのスクランブル有無の判定	47
5.3 暗号アルゴリズムの判別	48
5.3.1 MPEG-2 TS 方式の場合	48

5.3.2 MMT・TLV 方式の場合	48
5.4 MMT・TLV 方式におけるスクランブル対象レイヤーの判別	48
5.5 MMT・TLV 方式におけるメッセージ認証方式の判別	48
5.6 デスクランブルのための受信処理.....	48
5.6.1 MPEG-2 TS 方式におけるデスクランブルのための受信処理の例	48
5.6.2 MMT・TLV 方式におけるデスクランブルのための受信処理の例	49
5.6.2.1 デスクランブルのための受信処理	49
5.6.2.2 カウンタ初期値の生成	50
5.7 メッセージ認証に関する受信処理.....	51
5.8 同時に処理可能な PID 数／アセット数	52
解説 1 第 2 世代のアクセス制御方式におけるスクランブルサブシステム	53
1 MPEG-2 TS 方式におけるスクランブルサブシステム	53
2 MMT・TLV 方式におけるスクランブルサブシステム	53
3 暗号アルゴリズム	53
4 CTR モードのカウンタ初期値の運用	53
5 メッセージ認証の考え方	54
6 暗号アルゴリズムに関する留意事項	54
解説 2 スクリブル方式に関する運用について	55

第2部 コンテンツ保護方式

第2部 目次

第1章 一般事項	57
1.1 目的	57
1.2 適用範囲	57
1.3 参照文書	57
1.3.1 準拠文書	57
1.3.2 関連文書	57
1.4 用語・略語	58
第2章 機能仕様	61
2.1 関連情報の仕様	61
2.1.1 基本的考え方	61
2.1.2 コンテンツ保護方式に求められる各種要件	61
2.1.3 総合的機能	62
2.1.4 放送サービスの形態	62
2.1.4.1 対応するデジタル放送のサービス形態	62
2.1.4.2 各メディア間の整合性	63
2.1.5 EMM の伝送	63
2.1.6 ECM の伝送	63
2.1.7 セキュリティ機能	63
2.1.7.1 関連情報の暗号化	63
2.2 受信機に関わる仕様	64
2.2.1 ID	64
2.2.2 基本ユーザ入力と表示	64
2.2.3 番組の選択視聴	64
2.2.4 デスクランブラ	64
2.2.5 ECM の受信	64
2.2.6 EMM の受信	65
2.2.7 耐タンパ性	65
第3章 受信時の制御方式（コンテンツ保護方式）	67
3.1 関連情報サブシステム	67
3.1.1 システムの基本原理	67
3.1.2 本コンテンツ保護方式の構成	68
3.1.3 関連情報の種類	68
3.1.4 関連情報の形式	69
3.1.5 関連情報の暗号化方式	69

3.1.6 ECM.....	70
3.1.6.1 ECM の基本構成.....	70
3.1.6.2 ECM-F0 のデータ構成.....	71
3.1.6.3 ECM-F1 のデータ構成.....	73
3.1.6.4 ECM 内の記述子.....	76
3.1.7 EMM.....	76
3.1.7.1 EMM の基本構成.....	76
3.1.7.2 EMM のデータ構成.....	78
3.1.7.3 EMM 内の記述子.....	81
3.1.8 関連情報の伝送方法.....	87
3.1.8.1 ECM（番組情報）.....	87
3.1.8.2 EMM（個別情報）.....	87
第4章 受信機に関わる技術仕様.....	89
4.1 受信機の概要.....	89
4.2 同時に処理可能なスクランブル鍵の数.....	89
4.3（欠番）.....	89
4.4 本コンテンツ保護方式の実装.....	89
4.5 記憶データ.....	89
4.5.1 記憶データの区分.....	90
4.5.2 共通データ.....	90
4.5.3 局個別データ.....	91
4.6 本コンテンツ保護方式に関する受信機処理.....	94
4.6.1 ECM の処理.....	94
4.6.1.1 ECM 処理の流れ.....	96
4.6.1.2 RMP 事業体識別の判定処理.....	99
4.6.1.3 プロトコル番号処理.....	99
4.6.1.4 ワーク鍵無効フラグの判定処理.....	99
4.6.1.5 ワーク鍵識別の判定処理.....	99
4.6.1.6 ワーク鍵の選択処理.....	99
4.6.1.7 ECM 復号処理.....	100
4.6.1.8 改ざん検出鍵の算出処理.....	100
4.6.1.9 改ざん検出処理.....	100
4.6.2 デスクランブル処理.....	100
4.6.3 EMM の処理.....	100
4.6.3.1 EMM 処理の流れ.....	102

4.6.3.2 デバイス ID とデバイス鍵の算出処理	103
4.6.3.3 デバイス ID のフィルタリング処理	104
4.6.3.4 RMP 事業体識別判定処理	105
4.6.3.5 更新番号処理	105
4.6.3.6 プロトコル番号処理	105
4.6.3.7 EMM 復号処理	106
4.6.3.8 改ざん検出鍵の算出処理	106
4.6.3.9 改ざん検出処理	106
4.6.3.10 更新番号記憶処理	106
4.6.3.11 EMM 本体の処理	106
解説 1 本コンテンツ保護方式の運用概要	109
1 基本的な運用	109
1.1 運用管理	109
1.2 ECM, EMM の伝送	109
1.3 受信機	109
1.4 別表	109
2 受信機における特定の鍵の無効化運用	110
2.1 鍵の無効化の目的	110
2.2 デバイス ID/デバイス鍵更新	110
2.3 鍵の無効化の基本的な実行	110
3 受信機メーカーに供与される情報の例	111
4 受信機メーカーが提出する情報の例	112
解説 2 デバイス ID とデバイス鍵の世代更新	113

第3部 限定受信方式

第3部 目次

第1章 一般事項	115
1.1 目的	115
1.2 適用範囲	115
1.3 参照文書	115
1.3.1 準拠文書	115
1.3.2 関連文書	116
1.4 用語・略語	116
第2章 機能仕様	119
2.1 基本的な考え方	119
2.2 放送サービスの形態	120
2.2.1 対応するデジタル放送のサービス形態	120
2.2.2 各メディア間の整合性	120
2.2.3 有料放送サービス	120
2.2.3.1 料金設定方式	120
2.2.3.2 契約形態	121
2.2.3.3 プレビュー	121
2.2.4 無料放送サービス	121
2.2.5 その他のサービス	121
2.3 伝送に関わる仕様	121
2.3.1 EMM の伝送	121
2.3.2 ECM の伝送	122
2.3.3 通信経由での視聴ライセンスの伝送	122
2.4 セキュリティ機能	122
2.4.1 関連情報の暗号化	122
2.4.1.1 方式	122
2.4.1.2 管理機能	122
2.4.2 スクランブル鍵の暗号化	122
2.4.3 セキュリティの継続的な維持改善	122
2.5 耐タンパ性	122
2.6 受信機に関わる仕様	122
2.6.1 基本ユーザ入力と表示	122
2.6.2 番組の選択視聴	122
2.6.3 デスクランブラ	123
2.6.4 ECM 受信	123

2.6.5 EMM 受信、EMM メッセージ受信	123
2.6.6 通電制御機能	123
2.6.7 自動表示メッセージ	123
2.6.8 メール表示	123
2.6.9 CAS モジュール情報表示 (ID 表示)	123
2.6.10 番組予約	123
2.6.11 エラー表示	124
2.6.12 通信からの視聴ライセンス取得機能	124
第3章 関連情報の技術仕様	125
3.1 関連情報サブシステムの基本原理	125
3.2 関連情報の種類	126
3.3 ECM	126
3.3.1 ECM の基本構成	126
3.3.2 ECM セクション構造の詳細	127
3.3.2.1 ECM における固定部	127
3.3.2.2 ECM における可変部の例	128
3.3.2.3 改ざん検出	128
3.4 EMM	129
3.4.1 EMM の基本構成	129
3.4.2 EMM セクション構造の詳細	130
3.4.2.1 EMM における固定部	130
3.4.2.2 EMM における可変部の例	131
3.4.2.3 改ざん検出	131
3.5 EMM メッセージ情報	132
3.5.1 EMM 共通メッセージ	132
3.5.1.1 EMM 共通メッセージの基本構成	132
3.5.1.2 EMM 共通メッセージ セクション構造	133
3.5.1.3 EMM 共通メッセージセクション詳細	134
3.5.2 EMM 個別メッセージ	137
3.5.2.1 EMM 個別メッセージの基本構成	137
3.5.2.2 EMM 個別メッセージセクション構造	139
3.5.2.3 EMM 個別メッセージセクション詳細	140
第4章 送出運用に関わる技術仕様	143
4.1 関連情報の送出方法	143
4.1.1 ECM (番組情報、制御情報)	143

4.1.2 EMM（個別情報）	143
4.1.2.1 EMM の送出	143
4.1.2.2 EMM 送出順序	143
4.2 SI との関連	143
4.2.1 契約確認情報	143
4.2.2 EMM メッセージ関連	147
第5章 受信機に関わる技術仕様	149
5.1 限定受信処理	149
5.1.1 デスクランブラ	149
5.1.2 ECM 受信	149
5.1.3 EMM 受信、EMM メッセージ受信	149
5.2 通電制御機能	150
5.3 EMM メッセージ表示機能	150
5.3.1 自動表示メッセージ	150
5.3.2 メール表示	151
5.3.2.1 メール一覧表示	151
5.3.2.2 メール詳細表示	151
5.4 ユーザインタフェース	152
5.4.1 CAS モジュール情報表示（ID 表示）	152
5.4.2 番組予約機能	152
5.4.3 パスワード消去機能	152
5.4.4 エラー表示	152
5.4.4.1 正常な CAS モジュールを認識できない場合	153
5.4.4.2 CAS モジュールでの契約判定等で視聴できない場合	153
5.4.4.3 CAS モジュールに何らかのエラーが発生した場合	153
5.4.5 データコンテンツ表示機能	153
5.5 スクロンブル鍵の暗号化機能	153
5.6 通信による視聴ライセンスの取得	153
5.7 同時に処理可能なスクロンブル鍵の数	153
第6章 CA インタフェースに関わる技術仕様	155
6.1 CAS モジュールインタフェース	155
6.1.1 CAS モジュールの形状、物理仕様	155
6.1.2 端子の位置と形状	155
6.1.3 電気信号及びプロトコル	155
6.1.3.1 VCC 端子	155

6.1.3.2 CLK 端子	155
6.1.3.3 ATR (AnswerToReset)	156
6.1.3.4 プロトコル形式選択 (PPS)	158
6.1.3.5 伝送プロトコル形式	158
6.1.3.6 プロトコル制御	161
6.2 コマンド／レスポンス仕様	165
6.2.1 コマンド APDU	165
6.2.1.1 CLA	165
6.2.1.2 INS	166
6.2.1.3 P1、P2	166
6.2.1.4 Lc、Le	166
6.2.2 レスポンス APDU	166
6.2.2.1 SW1, SW2	166
6.2.2.2 レスポンスの Data フィールドの詳細構成	166
6.3 コマンド／レスポンス詳細	167
6.3.1 初期設定条件コマンド	168
6.3.1.1 機能概要	168
6.3.1.2 コマンド	168
6.3.1.3 レスポンス	168
6.3.2 ECM 受信コマンド	169
6.3.2.1 機能概要	169
6.3.2.2 コマンド	169
6.3.2.3 レスポンス	169
6.3.3 EMM 受信コマンド	170
6.3.3.1 機能概要	170
6.3.3.2 コマンド	170
6.3.3.3 レスポンス	170
6.3.4 契約確認コマンド	171
6.3.4.1 機能概要	171
6.3.4.2 コマンド	171
6.3.4.3 レスポンス	171
6.3.5 EMM 個別メッセージ受信コマンド	172
6.3.5.1 機能概要	172
6.3.5.2 コマンド	172
6.3.5.3 レスポンス	172

6.3.6 自動表示メッセージ表示情報取得コマンド	174
6.3.6.1 機能概要	174
6.3.6.2 コマンド	174
6.3.6.3 レスポンス	174
6.3.7 通電制御情報要求コマンド	175
6.3.7.1 機能概要	175
6.3.7.2 コマンド	175
6.3.7.3 レスポンス	175
6.3.8 CAS モジュール ID 情報取得コマンド	177
6.3.8.1 機能概要	177
6.3.8.2 コマンド	177
6.3.8.3 レスポンス	177
6.3.9 スクランブル鍵保護設定コマンド	178
6.3.9.1 機能概要	178
6.3.9.2 コマンド	178
6.3.9.3 レスポンス	178
6.3.10 通信データ設定コマンド	179
6.3.10.1 機能概要	179
6.3.10.2 コマンド	179
6.3.10.3 レスポンス	179
6.3.11 事業体個別データ取得コマンド	180
6.3.11.1 機能概要	180
6.3.11.2 コマンド	180
6.3.11.3 レスポンス	180
6.3.12 各パラメータ	181
6.3.12.1 INS 一覧	181
6.3.12.2 SW1/SW2 一覧	181
6.3.12.3 CAS モジュール指示一覧	182
6.3.13 リターンコード	184
6.3.13.1 コマンド共通リターンコード	184
6.3.13.2 コマンド別リターンコード	185
付録 1 CAS モジュール コマンド／レスポンス	189
1 CAS モジュール コマンド／レスポンスの動作シナリオ	189
1.1 電源 ON	190
1.2 ECM 受信（ティア）	191

1.3 EMM 受信	192
1.4 契約確認	193
1.5 EMM メッセージ受信／表示（自動表示メッセージ）	194
1.6 EMM メッセージ受信／表示（メール）	195
1.7 CAS モジュール ID 情報取得	196
解説 1 限定受信方式の概要	197
1 限定受信方式の概要	197
2 EMM メッセージ概要	198
2.1 EMM メッセージの基本的な考え方	198
2.1.1 概要	198
2.1.2 EMM 共通メッセージ	198
2.1.3 EMM 個別メッセージ	198
2.1.4 メッセージの種類	198
3 通電制御の運用	201
3.1 受信機の基本動作	201
3.1.1 受信機本体	201
3.1.2 CAS モジュール	201
3.2 契約変更 EMM の伝送運用例	202
3.2.1 基本手順	202
3.2.2 更新情報（デフォルト値の例）	202
解説 2 有料放送サービスの解説	203
1 フラット／ティア契約のサービス	203
2 CaPPV のサービス	203
参考資料 1 各 CA インタフェースに関する補足説明（T.B.D）	207
1 CAS モジュールの形状、物理仕様	207
1.1 CAS モジュールを受信機に実装する形態の場合	207
1.2 CAS モジュールが分離可能な形状である場合	207
1.2.1 端子の位置と形状	207

第二編

ダウンロードダブル CAS

第二編 目次

第1章 一般事項	209
1.1 目的	209
1.2 適用範囲	209
1.3 参照文書	209
1.3.1 関連文書	209
1.4 用語・略語	209
第2章 機能仕様	213
2.1 ダウンローダブル CAS の概要・定義	213
2.2 CAS プログラムの機能仕様	213
2.3 CAS プログラムのダウンロード方式	214
2.3.1 ダウンロードの告知	214
2.3.2 放送によるダウンロード伝送	214
2.3.2.1 DMM 及び DCM の送出機能	214
2.3.2.2 放送ダウンロードによる CAS プログラムの送出	215
2.3.3 通信によるダウンロード伝送	215
2.3.4 ダウンロードに関するセキュリティ	215
2.4 CAS 基盤に関わる仕様	215
2.4.1 CAS 基盤本体	215
2.4.2 CAS 基盤 ID と関連するセキュリティ情報	216
2.4.3 インタフェース	216
2.4.4 CAS 基盤の maker_id、model_id	216
2.4.5 伝送路暗号の復号	216
2.5 受信機本体に関わる仕様	216
2.5.1 CAS プログラムのダウンロード	216
2.5.2 ダウンロードに関する告知情報の受信処理	217
2.5.3 DCM の受信	217
2.5.4 DMM の受信	217
2.5.5 CAS プログラムの選択・起動	217
第3章 CAS プログラム	219
3.1 CAS プログラム	219
3.2 CAS プログラムの構成	219
3.2.1 CAS プログラム言語	219
3.2.2 CAS プログラムのアーキテクチャ	219
3.2.3 CAS プログラムの ID とバージョン	220

3.3 CAS プログラムの伝送パッケージフォーマット及び保護	220
3.4 関連情報の受信に必要な ID 及び鍵情報	220
第 4 章 ダウンロード方式	221
4.1 CAS プログラムのダウンロード方式の基本原理	221
4.2 CAS プログラムのダウンロードの告知情報	222
4.2.1 SDTT・MH-SDTT による告知	222
4.2.2 SDTT・MH-SDTT のパラメータ	222
4.3 CAS プログラム本体のセキュリティ	223
4.4 CAS プログラムの放送ダウンロード	223
4.4.1 放送ダウンロードの伝送方式	223
4.4.1.1 MPEG2-TS 方式の場合	223
4.4.1.2 MMT・TLV 方式の場合	223
4.4.2 CAS プログラムの伝送路暗号	223
4.4.3 放送ダウンロードに関わる関連情報	224
4.4.4 DCM	224
4.4.4.1 DCM の基本構成	224
4.4.4.2 DCM の詳細	225
4.4.5 DMM	226
4.4.5.1 DMM の基本構成	226
4.4.5.2 DMM の詳細	227
4.4.6 DCM、DMM の伝送方法	229
4.4.6.1 DCM（制御情報）	229
4.4.6.2 DMM（個別情報）	229
4.4.6.3 関連情報の送出期間	229
4.4.7 DCM、DMM の指定方法	229
4.4.7.1 DCM、DMM の指定情報（MPEG-2 TS 方式の場合）	229
4.4.7.2 DCM、DMM の指定情報（MMT・TLV 方式の場合）	230
4.5 CAS プログラムの通信ダウンロード	231
4.6 CAS プログラムの起動情報	231
4.6.1 CAS プログラムの起動情報（MPEG-2 TS 方式の場合）	231
4.6.2 CAS プログラムの起動情報（MMT・TLV 方式の場合）	233
第 5 章 受信機本体に関わる仕様	237
5.1 受信機の概要	237
5.2 CAS プログラムのダウンロード機能	237
5.2.1 告知情報の処理	237

5.2.2 CAS プログラムの放送ダウンロード処理 (MPEG-2 TS 方式の場合)	237
5.2.2.1 DCM の受信処理	238
5.2.2.2 DMM の受信処理	238
5.2.2.3 DCM 及び DMM の暗号復号処理	239
5.2.2.4 ダウンロードコンテンツの伝送路暗号復号処理	239
5.2.3 CAS プログラムの放送ダウンロード処理 (MMT・TLV 方式の場合)	240
5.2.3.1 DCM の受信処理	240
5.2.3.2 DMM の受信処理	240
5.2.3.3 DCM 及び DMM の暗号復号処理	240
5.2.3.4 ダウンロードコンテンツの伝送路暗号復号処理	240
5.2.4 CAS プログラムの通信ダウンロード処理	240
5.3 CAS プログラムの起動機能	241
5.3.1 CAS プログラムの起動と受信機本体の処理概要	241
5.3.2 CAS プログラムの起動手順	242
5.3.3 CAS プログラムの決定方法の詳細	243
5.4 受信機本体のレジデント機能	245
5.4.1 CAS 基盤 ID の表示、CAS プログラム ID の表示などのレジデント機能	245
5.4.2 手動ダウンロード機能	245
5.4.3 CAS プログラムの動作に必要なレジデント機能	246
第 6 章 CAS 基盤	247
6.1 CAS 基盤と受信機間のインタフェース	247
6.2 CAS プログラムと CAS 基盤間のインタフェース	247
6.3 CAS 基盤の実装形式	247
6.4 CAS 基盤が保持する CAS プログラムの数及び世代数	247
解説 1 ダウンローダブル CAS	249
1 全体概要	249
2 システム構成	249
3 CAS プログラム本体の暗号化と電子署名等による改ざん検出の考え方	250
4 CAS プログラムの伝送路暗号	250
5 受信機側の処理と実装	250
6 通信利用とセキュリティ	251
7 ECM/EMM と DCM/DMM の比較	252
8 CAS 基盤の実装について	253
9 CAS プログラムのバージョンと起動制御について	253
10 CA_system_ID の扱いについて	253

