

CASについて

JCTEA STD-001-2.3

デジタル有線テレビジョン放送「限定受信方式」 (2012年5月改定)

第1章	目的	1
第2章	適用範囲	1
第3章	準拠	1
第4章	用語・略語	1
第5章	機能仕様	2
5.1	スクランブル及び関連情報の仕様	2
5.2	受信機に関わる仕様	2
第6章	スクランブル及び関連情報の技術仕様	3
6.1	スクランブルサブシステム	3
6.2	関連情報サブシステム	3
第7章	受信機に関わる技術仕様	4
7.1	受信機の概要	4
7.2	ユーザインタフェース	4
7.3	CAインタフェース	4
7.4	EMM受信機能（受信の効率化）	5
7.5	通信機能	5
7.6	EMMメッセージ表示	6
7.7	SIとの関連	6
7.8	スクランブル有無の判定	6
7.9	同時に処理可能なスクランブル鍵の数	6
7.10	同時に処理可能なPID数	6
参考文献		7

限定受信方式の標準規格JCTEA STD-001 (ARIB STD-B25との比較)

ARIB STD-B25 6.1版 アクセス制御方式 (限定受信方式)

第1部 受信時の制御方式(限定受信方式)		
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
1.4	用語・略語	2
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
2.2	受信機に関わる仕様	10
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
3.2	関連情報サブシステム	21
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
4.3	CA インタフェース	64
4.4	EMM 受信機能(受信の効率化)	109
4.5	通信機能	109
4.6	EMM メッセージ表示	141
4.7	SI との関連	143
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
第6章	関連情報ECM-S 及びEMM-S を使用するCAS-R 方式	151
第2部 再生時の制御方式(限定再生方式)		
第1章	一般事項	263
第2章	ストリーム型コンテンツのアクセス制御方式	267
第3章	ファイル型コンテンツのアクセス制御方式	297
第3部 受信時の制御方式(コンテンツ保護方式)		
第1章	一般事項	335
第2章	機能仕様	339
第3章	スクランブル及び関連情報の技術仕様	345
第4章	受信機に関わる技術仕様	387

JCTEA STD-001-2.3 限定受信方式

(ARIB STD-B25 6.1版 第1部のXXを適用する)

第1章	目的	1
第2章	適用範囲	1
第3章	準拠	1
第4章	用語・略語	1
第5章	機能仕様	2
5.1	スクランブル及び関連情報の仕様	2
5.2	受信機に関わる仕様	2
第6章	スクランブル及び関連情報の技術仕様	3
6.1	スクランブルサブシステム	3
6.2	関連情報サブシステム	3
第7章	受信機に関わる技術仕様	4
7.1	受信機の概要	4
7.2	ユーザインタフェース	4
7.3	CAインタフェース	4
7.4	EMM受信機能(受信の効率化)	5
7.5	通信機能	5
7.6	EMMメッセージ表示	6
7.7	SIとの関連	6
7.8	スクランブル有無の判定	6
7.9	同時に処理可能なスクランブル鍵の数	6
7.10	同時に処理可能なPID数	6
参考文献		7

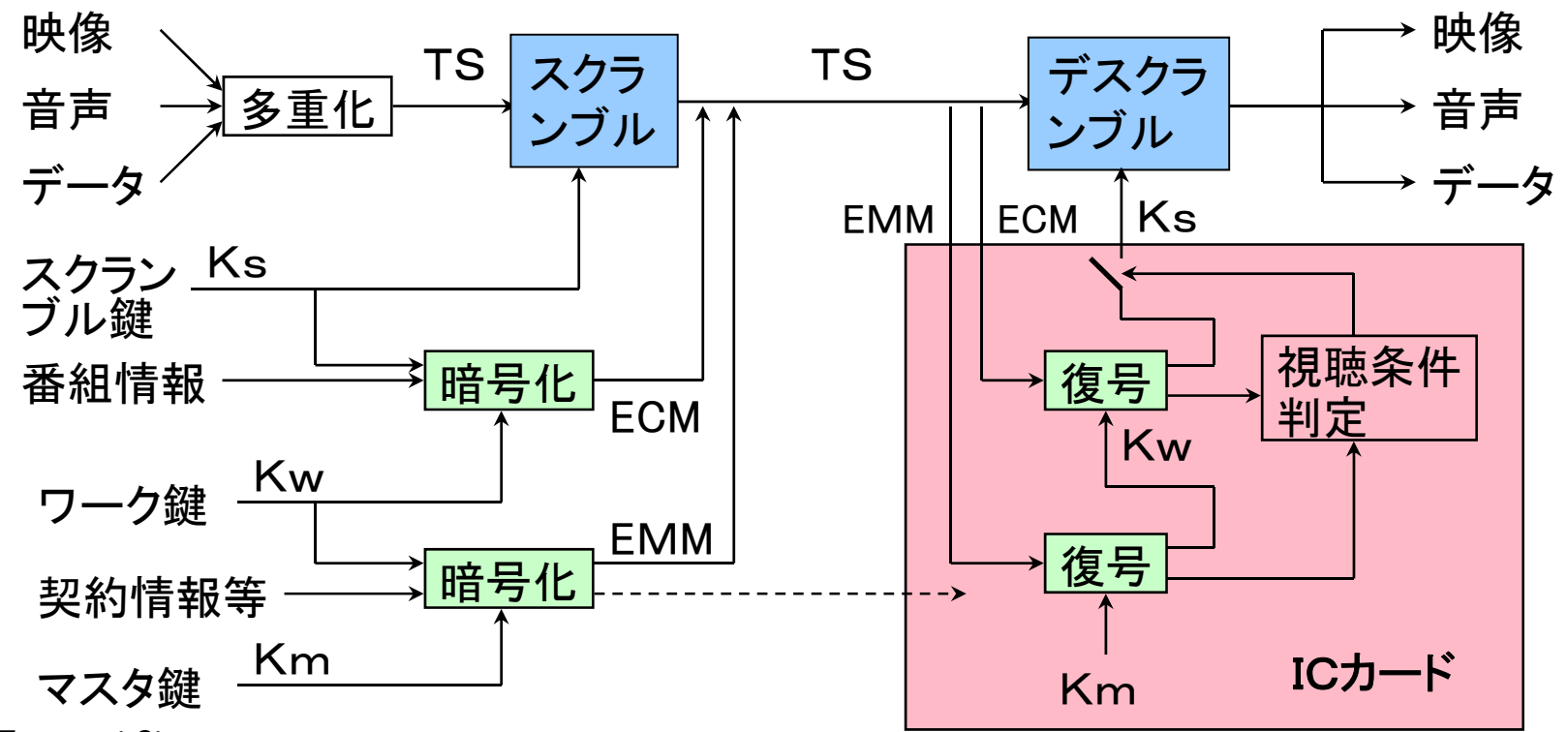
適用

地上・衛星移動体向け
(テレビや音声)
大容量蓄積機能向け
(サーバー型放送など)
受信機RMP(未運用)

JCTEAでは適用しない

本節についてはPlug-in SIM に関する記載を除きARIB STD-B25 6.1版 第1部の4.3節を適用する。

限定受信システム (JCTEA STD-001 & ARIB STD-B25)



TS: Transport Stream

ECM: Entitlement Control Message / EMM: Entitlement Management Message

Ks	スクランブル鍵	<ul style="list-style-type: none"> スクランブルのパラメータを変えて安全性を保つ ブロック暗号の鍵又はPN系列発生器の初期値 短時間 (例: 1秒程度) で更新
Kw	ワーク鍵	<ul style="list-style-type: none"> ECM (Ksと番組の属性情報) を暗号化 全受信機に共通 (例えばCHごと) 1ヶ月~1年程度で更新
Km	マスタ鍵	<ul style="list-style-type: none"> EMM (Kwと契約情報) を暗号化 各受信機 (又はセキュリティモジュール) に個別 鍵管理センターで管理

JCTEA STD-001の独自規格

JCTEA STD-001 第7章「受信機に関わる技術仕様」

7.3 CAインタフェース

本節についてはPlug-in SIM に関する記載および以下を除きARIB STD-B25 第1部の4.3節を適用する。

4.3.3.3 コマンド/レスポンスの詳細 で、(14)発呼先確認コマンドは上記参照先記載の内容に加えて、以下の内容も実施する。

a) 機能概要

- ・ICカード指示の「発呼」を受けて発行し、発呼先のIPアドレスとポート番号を得る。

b) コマンド

オフセット	フィールド	データ	長さ (byte)	値 (HEX)
+3	CLA	CLA コード	1	90
4	INS	INS コード	1	
5	P1	パラメータ 1	1	00
6	P2	パラメータ 2	1	00
7	Le	レスポンスデータ長	1	00

c) レスポンス

オフセット	フィールド	データ	長さ (byte)	値 (HEX)
+3	Data	プロトコルユニット番号	1	00
4		ユニット長	1	
5		ICカード指示	2	
7		リターンコード	2	
9		ホスト番号	8	
17		電話番号	7	*2)
24	SW1		1	
25	SW2		1	

*1)ホスト番号：運用しない

*2)電話番号：発呼先のIPアドレス&ポート番号を指定する。

IPアドレスを指定する場合は、上位1byteに0xeeを格納し、次の2byteにポート番号を、最下位4byteにIPアドレスをバイナリ値で指定する。