



ARIB TR-B27

サーバ型放送

DIGITAL BROADCASTING SYSTEM BASED ON HOME SERVER

技術資料

ARIB TECHNICAL REPORT

ARIB TR-B27 1.1版 (第二分冊)

2006年 9月28日 策 定

2022年10月 6日 1.1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。

「技術資料」は、国が定める技術基準と民間の任意基準を取りまとめて策定される標準規格を踏まえて、無線設備、放送設備の適性品質、互換性の確保等を図るため、当該設備に関する測定法、解説、運用上の留意事項等を具体的に定めたものであり、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。

本技術資料は、国の定める技術基準とサーバー型放送に関する標準規格を踏まえて、放送と通信が連携して新しいコンテンツ提供環境を構築するサーバー型放送を運用するために、サーバー型放送運用規定策定プロジェクト（サーバーP）で2003年9月から2006年2月にかけて検討された技術要件をまとめたものである。

本技術資料が、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。

総合目次

第零編	サーバー型放送の基本概念と共通事項	第一分冊
第一編	(欠番)	第一分冊
第二編	サーバー型放送受信機機能	第一分冊
第三編	サーバー型放送データ放送運用方法	第一分冊
第四編	サーバー型放送 PSI/SI 運用方法	第一分冊
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	第二分冊
第六編	サーバー型放送通信運用方法	第三分冊
第七編	サーバー型放送送出運用方法	第三分冊
第八編	サーバー型放送コンテンツ保護方法	第三分冊
第九編	(欠番)	第三分冊
第十編	サーバー型放送メタデータ運用方法	第三分冊

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

目 次

第 1 章 一般事項	1
1.1 はじめに	1
1.2 引用文書	1
1.2.1 準拠文書	1
1.2.2 関連文書	1
1.3 用語	2
第 2 章 サーバー型放送におけるアクセス制御方式	11
2.1 サーバー型放送におけるアクセス制御方式	11
2.2 アクセス制御方式の概要	12
2.2.1 システムリファレンスモデル	12
2.2.1.1 サーバー型放送における CAS の構成要素	12
2.2.1.2 サーバー型放送における CAS のインタフェース	14
2.2.2 セキュリティの確保が必要なインタフェースについて	15
2.3 ライセンスモデル	15
2.3.1 ライセンスの定義	15
2.3.2 ライセンスの種類	15
2.3.3 ライセンスの伝送	16
2.3.4 CAS カード・受信機におけるライセンスの蓄積管理	17
2.3.5 運用可能なサービスとライセンスの伝送形態	19
2.3.6 ライセンスの構成要素	20
2.3.6.1 個別ライセンス	20
2.3.6.2 単一サービスメインライセンス	21
2.3.6.3 単一サービスサブライセンス	21
2.3.6.4 ティアビット形式メインライセンス	22
2.3.6.5 ティアビット形式サブライセンス	22
2.3.6.6 コンテンツの利用条件 (RMPI)	23
2.3.7 レンダラ利用条件	24
2.3.7.1 再生時レンダラ利用条件	24
2.3.7.2 書き出し時レンダラ利用条件	25
2.3.8 受信機保存ライセンス	25
2.3.8.1 受信機保存個別ライセンスフォーマット	26
2.3.8.2 受信機保存サブライセンスフォーマット (単一サービスサブライセンス)	27
2.3.8.3 受信機保存サブライセンスフォーマット (ティアビット形式サブライセンス)	28
2.3.8.4 受信機保存ライセンスの利用条件 (RMPI) フォーマット	29

2.3.8.5 受信機保存ライセンスの利用状況フォーマット	34
2.3.9 ドメイン内転送サブライセンス	34
2.3.10 ライセンスの処理概要	35
2.3.10.1 受信機側全体のライセンス処理の概要	35
2.3.10.2 CAS カード内でのライセンスの管理	37
2.3.10.3 コンテンツ利用時の CAS カードとレンドラでのライセンス処理	38
2.4 ドメインモデル	39
2.4.1 ドメインの定義及び概要	39
2.4.2 ドメインの管理及び処理の概要	40
2.4.2.1 ドメインへの CAS カードの登録	40
2.4.2.2 ドメインからの CAS カードの削除	40
2.4.2.3 ドメイン内でのサブライセンスの転送	41
2.5 アクセス制御にかかわる情報	42
2.5.1 パッケージ	42
2.5.1.1 パッケージの概要	42
2.5.1.2 パッケージの分類	43
2.5.1.3 パッケージ、シリーズ、利用単位コンテンツの関係	43
2.5.1.4 パッケージとサービス申し込み	44
2.5.1.5 パッケージを記述するグループ情報要素	45
2.5.2 ライセンス参照情報	46
2.5.2.1 ライセンス参照情報の運用想定	47
2.5.2.2 ライセンス参照情報、パッケージを記述するグループ情報要素、 番組情報要素の関係	47
2.5.3 ライセンスリンク情報 (LLI : License Link Information)	48
2.5.4 サービス申し込み済みパッケージ情報	49
2.5.5 トリックプレイ区間情報 (TSI : Trickplay Segment Information)	50
第 3 章 コンテンツの暗号化方式	51
3.1 放送コンテンツの暗号化方式	51
3.1.1 TYPE1 コンテンツのスクランブル方式	51
3.1.2 TYPE2 コンテンツのエンクリプト方式	51
3.1.2.1 エンクリプトの対象	51
3.1.2.2 リソースのエンクリプト範囲	51
3.1.2.3 コンテンツ鍵の運用	52
3.1.2.4 エンクリプトアルゴリズム	52
3.1.2.5 エンクリプト方式の指定	52
3.1.2.6 限定受信方式との併用	52

3.2 通信コンテンツの暗号化方式.....	52
3.2.1 ストリーミングのエンクリプト方式	52
3.2.1.1 エンクリプトの対象.....	52
3.2.1.2 コンテンツ鍵の運用.....	52
3.2.1.3 エンクリプトアルゴリズム	52
3.2.1.4 エンクリプト方式の指定.....	52
3.2.2 ダウンロードのエンクリプト方式.....	53
第4章 送出運用方法	55
4.1 放送送出運用方法	55
4.1.1 ライセンスの伝送方法.....	55
4.1.1.1 CAT の運用.....	55
4.1.1.2 限定再生方式記述子の運用	56
4.1.1.3 EMM の運用 (TYPE1 コンテンツ・TYPE2 コンテンツ)	57
4.1.1.4 Kc 伝送用 ECM の運用 (TYPE1 コンテンツ)	60
4.1.1.5 ECM-Kc の運用 (TYPE1 コンテンツ)	63
4.1.1.6 ACI の運用 (TYPE2 コンテンツ)	67
4.1.2 アクセス制御に関わる情報の伝送方法.....	68
4.1.2.1 ライセンス参照情報の運用	68
4.1.2.2 ライセンスリンク情報 (LLI) の運用	75
4.1.2.3 トリックプレイ区間情報 (TSI) の運用.....	78
4.1.2.4 コンテンツ情報ヘッダの運用.....	80
4.1.2.5 ACG 記述子の運用.....	81
4.1.2.6 Encrypt 記述子の運用	81
4.2 通信送出運用方法	81
4.2.1 ライセンスの伝送方法.....	81
4.2.1.1 ACI の運用.....	81
4.2.2 アクセス制御に関わる情報の伝送方法.....	81
4.2.2.1 ライセンス参照情報の運用	81
4.2.2.2 ライセンスリンク情報 (LLI) の運用	82
4.2.2.3 トリックプレイ区間情報 (TSI) の運用.....	82
第5章 受信機の技術仕様.....	83
5.1 CAS カードの機能.....	83
5.2 受信機の構成.....	84
5.2.1 IP 部.....	84
5.2.2 チューナ部.....	84
5.2.3 表示部.....	84

5.2.4 キー入力部.....	84
5.2.5 レジデントアプリケーション.....	84
5.2.6 リモコン.....	84
5.2.7 蓄積装置.....	84
5.2.8 レンダラ.....	85
5.2.9 CAS カード / CAS インタフェース.....	85
5.2.10 入出力インタフェース.....	85
5.3 受信機・CAS カード間インタフェース.....	86
5.3.1 インタフェース概要.....	86
5.3.1.1 通信プロトコル構造.....	86
5.3.1.2 通信プロトコルの各レイヤが提供する機能.....	86
5.3.1.3 メッセージ基本構造.....	89
5.3.1.4 各レイヤのメッセージ・コマンド間の関係.....	90
5.3.2 APDU 層コマンド / レスポンス.....	91
5.3.2.1 コマンド APDU の構造.....	91
5.3.2.2 レスポンス APDU の構造.....	92
5.3.3 通信層コマンド / レスポンス.....	93
5.3.3.1 コマンド一覧.....	93
5.3.3.2 コマンドの基本構造.....	94
5.3.3.3 コマンドの詳細仕様.....	97
5.3.4 転送・制御層メッセージ.....	104
5.3.4.1 メッセージ一覧.....	104
5.3.4.2 転送・制御層の機能詳細.....	105
5.3.4.3 メッセージの詳細仕様.....	109
5.3.5 アプリケーション層メッセージ.....	117
5.3.5.1 メッセージ一覧.....	118
5.3.5.2 レジデントアプリケーション・CAS カード間のメッセージ仕様.....	120
5.3.5.3 レンダラ・CAS カード間のメッセージ仕様.....	169
5.3.5.4 パラメータ一覧.....	184
5.4 CAS カードの有効 / 無効 / 使用不可の判定.....	188
5.5 有効な限定再生方式 (CA システム ID の整合性確認).....	188
5.6 CAS カード情報の表示 (TBD).....	189
5.7 有効な CAS カードが挿入されていない場合の動作.....	189
5.8 CAS 関連のエラー分類.....	189
5.9 受信機の処理仕様.....	191
5.9.1 電源 ON・CAS カード挿入.....	191

5.9.1.1 受信機・CAS カード間インタフェースの初期設定パラメータの取得.....	191
5.9.1.2 認証暗号通信路の確立.....	193
5.9.1.3 CA システム情報の取得.....	193
5.9.1.4 通電制御情報の取得.....	194
5.9.1.5 更新制御情報の取得.....	194
5.9.2 放送コンテンツの受信・蓄積.....	195
5.9.2.1 Kc 伝送用 ECM/ACI の取得、受信機保存サブライセンスの蓄積.....	195
5.9.2.2 EMM の受信.....	197
5.9.3 通信コンテンツ（ダウンロード）の受信・蓄積.....	198
5.9.3.1 ACI の取得、受信機保存サブライセンスの蓄積.....	198
5.9.4 通信でのライセンスの取得.....	199
5.9.4.1 ティアビット形式メインライセンスの取得.....	200
5.9.4.2 単一サービスメインライセンスの取得.....	200
5.9.4.3 個別ライセンスの取得.....	201
5.9.5 ライセンスの情報取得.....	203
5.9.5.1 メインライセンスの情報取得.....	204
5.9.5.2 受信機蓄積の個別ライセンス、サブライセンスの情報取得.....	207
5.9.5.3 ストリーミング（VOD）用の個別ライセンスの情報取得.....	209
5.9.6 TYPE1 コンテンツの再生.....	211
5.9.6.1 受信機保存ライセンスの入力.....	211
5.9.6.2 TYPE1 コンテンツの再生開始.....	212
5.9.6.3 TYPE1 コンテンツの再生終了.....	215
5.9.6.4 受信機保存ライセンスの出力.....	216
5.9.7 TYPE2 コンテンツ・通信コンテンツ（ダウンロード）の再生.....	216
5.9.7.1 受信機保存ライセンスの入力.....	216
5.9.7.2 TYPE2 コンテンツ・通信コンテンツ（ダウンロード）の再生開始.....	217
5.9.7.3 TYPE2 コンテンツ・通信コンテンツ（ダウンロード）の再生終了.....	218
5.9.7.4 受信機保存ライセンスの出力.....	218
5.9.8 複数リソースで構成される TYPE2 コンテンツ・通信コンテンツ （ダウンロード）の再生.....	219
5.9.8.1 受信機保存ライセンスの入力.....	220
5.9.8.2 複数リソースで構成される TYPE2 コンテンツ・通信コンテンツ （ダウンロード）の再生開始.....	220
5.9.8.3 複数リソースで構成される TYPE2 コンテンツ・通信コンテンツ （ダウンロード）の再生終了.....	221
5.9.8.4 受信機保存ライセンスの出力.....	222
5.9.9 他の利用単位コンテンツを参照利用する TYPE2 コンテンツ・通信コンテンツ	

(ダウンロード)の再生.....	222
5.9.9.1 受信機保存ライセンスの入力	223
5.9.9.2 他の利用単位コンテンツを参照利用する TYPE2 コンテンツ・通信コンテンツ (ダウンロード)の再生開始.....	224
5.9.9.3 他の利用単位コンテンツを参照利用する TYPE2 コンテンツ・通信コンテンツ (ダウンロード)の再生終了.....	224
5.9.9.4 受信機保存ライセンスの出力	225
5.9.10 通信コンテンツ(ストリーミング(VOD))の再生.....	225
5.9.10.1 通信コンテンツ(ストリーミング(VOD))の再生開始	226
5.9.10.2 通信コンテンツ(ストリーミング(VOD))の再生終了	227
5.9.11 正当なセグメンテーションメタデータの識別	228
5.9.11.1 デジタル署名が付与されたセグメンテーションメタデータの識別.....	228
5.9.11.2 ユーザメタデータの識別.....	234
5.9.11.3 ユーザメタデータの作成.....	235
5.9.11.4 ドメイン固有情報の取得.....	236
5.9.12 TYPE1 コンテンツの書き出し.....	237
5.9.12.1 受信機保存ライセンスの入力	237
5.9.12.2 TYPE1 コンテンツの書き出し開始	237
5.9.12.3 TYPE1 コンテンツの書き出し終了	239
5.9.12.4 受信機保存ライセンスの出力	240
5.9.13 TYPE2 コンテンツ・通信コンテンツ(ダウンロード)の書き出し.....	240
5.9.13.1 受信機保存ライセンスの入力	240
5.9.13.2 TYPE2 コンテンツ・通信コンテンツ(ダウンロード)の書き出し開始.....	241
5.9.13.3 TYPE2 コンテンツ・通信コンテンツ(ダウンロード)の書き出し終了.....	242
5.9.13.4 受信機保存ライセンスの出力	242
5.9.14 TYPE1 コンテンツのトランスコード・リエンクリプト.....	242
5.9.14.1 受信機保存ライセンスの入力	243
5.9.14.2 TYPE1 コンテンツのトランスコード・リエンクリプト開始.....	243
5.9.14.3 TYPE1 コンテンツのトランスコード・リエンクリプト終了.....	245
5.9.14.4 受信機保存ライセンスの出力	245
5.9.15 TYPE2 コンテンツ・通信コンテンツ(ダウンロード)のトランスコード・ リエンクリプト	246
5.9.15.1 受信機保存ライセンスの入力	246
5.9.15.2 TYPE2 コンテンツ・通信コンテンツ(ダウンロード)の トランスコード・リエンクリプト開始	246
5.9.15.3 TYPE2 コンテンツ・通信コンテンツ(ダウンロード)の トランスコード・リエンクリプト終了	247

5.9.15.4 受信機保存ライセンスの出力.....	248
5.9.16 ライセンスの削除.....	248
5.9.16.1 単一サービスマインライセンス・個別ライセンスの削除.....	249
5.9.16.2 受信機保存ライセンスの削除.....	249
5.9.16.3 CAS カード内の無効なライセンスの削除.....	250
5.9.17 ライセンスの更新.....	251
5.9.17.1 放送でのライセンスの更新.....	251
5.9.17.2 通信でのライセンスの更新.....	253
5.9.18 CAS カードのドメイン登録・削除.....	257
5.9.18.1 通信での CAS カードのドメインへの登録.....	257
5.9.18.2 通信での CAS カードのドメインからの削除.....	258
5.9.18.3 放送での CAS カードのドメインへの登録・ドメインからの削除.....	259
5.9.19 ドメイン内でのサブライセンスの転送.....	260
5.9.19.1 サブライセンス転送元でのドメイン内転送サブライセンスの出力.....	260
5.9.19.2 サブライセンス転送先でのドメイン内転送サブライセンスの入力.....	260
5.9.20 受信機保存ライセンスの入力・出力.....	261
5.9.20.1 受信機保存ライセンスの入力.....	261
5.9.20.2 受信機保存ライセンスの出力.....	262
5.9.21 時刻の取得.....	264
5.9.21.1 時刻管理サーバーからの時刻取得.....	264
5.9.22 OTP の取得.....	264
5.9.22.1 CAS サーバーからの OTP の取得.....	264
5.9.23 通信中断状態からの回復.....	265
5.9.23.1 通信切断情報の取得.....	265
5.9.23.2 通信中断状態の回復.....	265
5.9.24 CAS カード・接続先間のデータ転送.....	266
5.9.24.1 接続先 URI の取得と接続先との通信接続.....	267
5.9.24.2 接続先への通信接続状態の通知.....	267
5.9.24.3 CAS カードと接続先との間のデータ転送及び接続先との通信接続切断.....	268
5.9.25 CAS カード指示に対する受信機処理.....	269
5.9.25.1 通電制御情報取得指示に対する処理.....	269
5.9.25.2 更新制御情報取得指示に対する処理.....	269
5.9.25.3 機器認証指示に対する処理.....	269
5.9.25.4 通信切断情報取得指示に対する処理.....	269
5.9.25.5 カード交換指示に対する処理.....	270
5.9.25.6 ライセンス更新指示に対する処理.....	270
5.9.25.7 メモリ満杯 (CAS カード蓄積) 通知に対する処理.....	270

5.9.25.8	メモリ満杯（受信機蓄積）通知に対する処理	271
5.10	エラー時の受信機処理	272
5.10.1	受信機の電源断時のエラー処理	272
5.10.1.1	受信機保存ライセンスの出力	272
5.10.1.2	通信切断状態の回復	273
5.10.1.3	受信機保存ライセンスの再削除処理	274
5.10.2	Kc 伝送用 ECM/ACI からの受信機保存サブライセンス取得時のエラー処理	274
5.10.3	通信切断時のエラー処理	275
5.10.4	コンテンツ再生・書き出し時のエラー処理	275
5.10.5	時刻の取得時のエラー処理	275
5.11	受信機の実装基準	275
5.11.1	保護の対象	275
5.11.2	具体的な実装基準	276
5.11.2.1	全体構成	276
5.11.2.2	出力	276
5.11.2.3	ローカル暗号	276
5.11.2.4	時刻の管理	277
A	解説	279
A.1	受信機の動作シーケンス	279
A.1.1	電源 ON・CAS カード挿入	280
A.1.2	放送コンテンツの受信・蓄積	281
A.1.2.1	Kc 伝送用 ECM の取得、受信機保存サブライセンスの蓄積	281
A.1.2.2	ACI の取得、受信機保存サブライセンスの蓄積	282
A.1.2.3	EMM の受信、メインライセンスの蓄積	282
A.1.3	通信コンテンツ（ダウンロード）の受信・蓄積	283
A.1.3.1	ACI の取得、受信機保存サブライセンスの蓄積	283
A.1.4	通信でのライセンス取得	284
A.1.4.1	ティアビット形式メインライセンスの取得	284
A.1.4.2	単一サービスメインライセンスの取得	285
A.1.4.3	個別ライセンスの取得	286
A.1.5	ライセンスの情報取得	287
A.1.5.1	コンテンツ一覧表示のためのライセンスの情報取得	287
A.1.5.2	通信コンテンツ（ストリーミング（VOD））一覧表示のためのライセンスの 情報取得	288
A.1.6	TYPE1 コンテンツの再生	289
A.1.7	TYPE2 コンテンツ・通信コンテンツ（ダウンロード）の再生	290

A.1.8	複数リソースで構成される TYPE2 コンテンツ・通信コンテンツ (ダウンロード)の再生	291
A.1.9	他の利用単位コンテンツ (TYPE1 コンテンツ) を参照利用する TYPE2 コンテンツ・通信コンテンツ (ダウンロード) の再生	292
A.1.10	通信コンテンツ (ストリーミング (VOD)) の再生	293
A.1.11	正当なセグメンテーションメタデータの識別	294
A.1.11.1	ユーザメタデータの識別におけるドメイン固有情報の取得	294
A.1.12	TYPE1 コンテンツの書き出し	295
A.1.13	TYPE2 コンテンツ・通信コンテンツ (ダウンロード) の書き出し	296
A.1.14	TYPE1 コンテンツのトランスコード・リエncrypt	297
A.1.15	TYPE2 コンテンツ・通信コンテンツ (ダウンロード) のトランスコード・ リエncrypt	298
A.1.16	ライセンスの削除	299
A.1.16.1	単一サービスメインライセンス、ストリーミング (VOD) 用 ライセンスの削除	299
A.1.16.2	受信機保存ライセンスの削除	299
A.1.16.3	CAS カード内の無効なライセンスの削除	299
A.1.17	ライセンスの更新	300
A.1.17.1	放送でのメインライセンスの更新	300
A.1.17.2	放送でのサブライセンスの更新	301
A.1.17.3	通信でのティアビット形式メインライセンスの更新	302
A.1.17.4	通信での単一サービスメインライセンスの更新	303
A.1.17.5	通信でのサブライセンスの更新	304
A.1.18	CAS カードのドメイン登録・削除	305
A.1.18.1	通信での CAS カードのドメインへの登録	305
A.1.18.2	通信での CAS カードのドメインからの削除	306
A.1.18.3	放送での CAS カードのドメインへの登録・ドメインからの削除	306
A.1.19	ドメイン内でのサブライセンスの転送	307
A.1.19.1	サブライセンス転送元でのドメイン内転送サブライセンスの出力	307
A.1.19.2	サブライセンス転送先でのドメイン内転送サブライセンスの入力	307
A.1.20	受信機保存ライセンスの入力・出力	308
A.1.20.1	受信機保存ライセンスの入力	308
A.1.20.2	受信機保存ライセンスの出力	308
A.1.21	時刻の取得	309
A.1.21.1	時刻管理サーバーからの時刻取得	309
A.1.22	OTP の取得	310
A.1.22.1	CAS サーバーからの OTP の取得	310

A.1.23	通信中断状態からの回復.....	311
A.1.24	CAS カード・接続先間のデータ転送.....	312
A.2	各種シナリオにおける CAS 処理を中心としたシーケンスモデル.....	313
A.2.1	S1： TYPE2 フラット・ティア（2 階層ライセンス・通信取得）.....	313
A.2.2	S2： TYPE2 フラット・ティア（2 階層ライセンス・放送取得）.....	315
A.2.3	S3： TYPE2 フラット・ティア（1 階層ライセンス）.....	318
A.2.4	S4： TYPE1 フラット・ティア（2 階層ライセンス・放送取得）.....	320
A.2.5	S5： TYPE2 PPU（1 階層ライセンス）.....	322
A.2.6	S6: 通信ダウンロード フラット・ティア（2 階層ライセンス）.....	324
A.2.7	S7: 通信ダウンロード フラット・ティア（1 階層ライセンス）.....	325
A.2.8	S8: 通信ダウンロード PPU（1 階層ライセンス）.....	327
A.2.9	S9: VOD ストリーミング フラット・ティア（1 階層ライセンス）.....	328
A.2.10	S10: VOD ストリーミング PPU（1 階層ライセンス）.....	330