



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 1.3版

|             |         |
|-------------|---------|
| 平成26年 7月31日 | 策 定     |
| 平成27年 3月17日 | 1. 1 改定 |
| 平成27年12月 3日 | 1. 2 改定 |
| 平成29年 3月24日 | 1. 3 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。

## 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 ..... | 33 |
| 第3部 限定受信方式 .....    | 91 |

第二編 ダウンローダブル CAS .....185

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 受信機に関わる技術仕様 .....                            | 23 |
| 4.1 受信機の概要 .....                                 | 23 |
| 4.2 スクランブル有無の判定 .....                            | 23 |
| 4.2.1 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 ..... | 23 |
| 4.2.2 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 ..... | 23 |
| 4.3 暗号アルゴリズムの判別 .....                            | 24 |
| 4.3.1 MPEG-2 TS 方式の場合 .....                      | 24 |
| 4.3.2 MMT・TLV 方式の場合 .....                        | 24 |
| 4.4 MMT・TLV 方式におけるスクランブル対象レイヤーの判別 .....          | 24 |
| 4.5 MMT・TLV 方式におけるメッセージ認証方式の判別 .....             | 24 |
| 4.6 デスクランブルのための受信処理 .....                        | 24 |
| 4.6.1 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 .....    | 24 |
| 4.6.2 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 .....      | 25 |
| 4.6.2.1 デスクランブルのための受信処理 .....                    | 25 |
| 4.6.2.2 カウンタ初期値の生成 .....                         | 26 |
| 4.7 メッセージ認証に関する受信処理 .....                        | 27 |
| 解説1 .....                                        | 29 |
| 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の解説 .....         | 29 |
| 1.1 MPEG-2 TS 方式におけるスクランブルサブシステム .....           | 29 |
| 1.2 MMT・TLV 方式におけるスクランブルサブシステム .....             | 29 |
| 1.3 暗号アルゴリズム .....                               | 29 |
| 1.4 CTR モードのカウンタ初期値の運用 .....                     | 29 |
| 1.5 メッセージ認証の考え方 .....                            | 30 |
| 1.6 暗号アルゴリズムに関する留意事項 .....                       | 30 |
| 解説2 .....                                        | 31 |
| 1 スクランブル方式に関する運用について .....                       | 31 |