地上デジタルテレビジョン放送運用規定

OPERATIONAL GUIDELINES FOR
DIGITAL TERRESTRIAL TELEVISION BROADCASTING

技　術　資　料

ARIB TECHNICAL REPORT

ARIB TR-B14　6.11版
（第五分冊）

2002年 1月24日　策　　定
2024年10月29日　６．１１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、放送設備の適正品質、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る。

本技術資料は、地上デジタルテレビジョン放送の放送局での運用及び地上デジタルテレビジョン放送受信機の機能仕様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

第五編

地上デジタルテレビジョン放送
限定受信方式運用規定
及び受信機仕様

目　　次

【第一部】　限定受信方式（CAS）運用規定及び受信機仕様

1　はじめに

1.1　まえがき

地上デジタルテレビジョン放送受信機に対する限定受信方式に関する仕様は電波産業会標準規格「デジタル放送におけるアクセス制御方式」第1部　受信時の制御方式（限定受信方式）（以下、ARIB STD-B25 第1部）で規定される。

本編は、ARIB STD-B25 第1部を基に、それを補足する形で運用上の送出運用規定と受信機仕様に対する要求仕様について規定した。したがって、本編に記載されていない事項に関してはARIB STD-B25第1部を参照願いたい。

地上デジタルテレビジョン放送の限定受信方式ついては、放送開始予定時点で予定されていないものについては、BSデジタル放送の限定受信方式から一部仕様を制限するという考え方に基づき、本編は記述されている。特に、電話回線を必要とするPPV機能に関しては、実サービス開始時において、視聴履歴の収集手段についても最適な運用規定とすべきとの考えから、将来追加規定として運用していく考えとした。したがって、放送サービスの実運用計画にあわせ、速やかに本規定を改定整備することを留意されたい。

無料番組のコンテンツ保護を目的としたスクランブル方式としての利用について、放送開始当初はARIB STD-B25 第1部準拠の限定受信方式の利用を想定している。将来、別の方式によるコンテンツ保護を目的としたスクランブル方式の導入や、将来の新サービスにおける新たな限定受信方式の導入など、複数の限定受信方式が運用された場合に、放送開始当初の受信機で誤動作を起こさないよう、予め複数限定受信方式の運用についても触れている。

1.2　目的

本編はARIB STD-B25 第1部に基づいて、地上デジタルテレビジョン放送受信機におけるCAS機能を搭載する際に考慮すべき受信機に対する要求仕様や、運用情報について記載したものである。

1.3　適用範囲

本規格書は、地上デジタルテレビジョン放送のARIB STD-B25 第1部に準拠した限定受信システム（CAS）方式における送出運用規定および、受信機仕様について適用する。

2　引用文書

(1)　電気通信技術審議会　諮問第 17 号答申書
(2)　電気通信技術審議会　諮問第 74 号答申書
(3)　平成 23 年総務省令第 87 号
(4)　平成 23 年総務省告示第 298 号
(5)　平成 26 年総務省告示第 233 号
(6)　平成 26 年総務省告示第 235 号
(7)　「デジタル放送に使用する番組配列情報」標準規格　ARIB STD-B10
(8)　「デジタル放送用受信装置」標準規格　ARIB STD-B21
(9)　「デジタル放送におけるアクセス制御方式」標準規格　ARIB STD-B25 第 1 部
(10)　「BS/広帯域 CS デジタル放送運用規定」標準規格　ARIB TR-B15

3　用語

本規定で用いる用語を以下のように定義する。

ARIB	Association of Radio Industries and Business： 一般社団法人電波産業会 放送事業者、電気通信事業者、機器製造者（メーカー）が参画する国内の電波利用に関する技術を標準規格化する団体。
CA system	Conditional Access system：限定受信方式。サービス（編成チャンネル）やイベント（番組）の視聴を制御するシステム。
CAT	Conditional Access Table：限定受信テーブル。有料放送を構成する関連情報のうち個別情報を伝送する TS パケットのパケット ID（識別子）を指定。
component	コンポーネント。映像、音声、文字、各種データなど、イベント（番組）を構成する要素。
descriptor	様々な情報を載せるためテーブル内に配置される記述領域、記述子。
ECM	Entitlement Control Message：番組情報（番組に関する情報とデスクランブルのための鍵など）および制御情報からなる共通情報。
EIT	Event Information Table：イベント情報テーブル。番組名、放送日時、番組内容など、番組に関する情報が記載される。 地上デジタルテレビジョン放送では、固定受信機での表示を目的とした H-EIT、移動受信機での表示を目的とした M-EIT、部分受信機での表示を目的とした L-EIT を運用する。
EMM	Entitlement Management Message：加入者毎の契約情報および共通情報の暗号を解くためのワーク鍵を含む個別情報。
EMM メッセージ	EMM で伝送される個別、共通メッセージ
ES	Elementary Stream：基本ストリーム。PES パケット中の、符号化された映像、音声、独立データに相当する。1 つの ES は同一のストリーム ID を持つ PES パケットにより伝送される。
event	イベント。ニュース、ドラマなど、同一サービス（編成チャンネル）内で開始・終了時刻の決まったストリームの集合。
PID	Packet Identifier：パケット ID（識別子）。13 ビットのストリーム識別情報で、該当パケットの個別ストリームの属性を示す。
PMT	Program Map Table：番組を構成する各符号化信号を伝送する TS パケットのパケット ID および有料放送の関連情報のうち共通情報を伝送する TS パケットのパケット ID を指定する。
PPV	Pay Per View：ペイパービュー。個々の番組や番組グループについて、視聴形態に応じて料金を徴収する有料放送。
SDT	Service Description Table：サービス記述テーブル。編成チャンネル名、放送事業者名など、編成チャンネルに関する情報を記載。
CA 代替サービス	視聴者がスクランブルチャンネルを選局したとき、非契約等の条件の場合に放送事業者が運営している視聴者への「ご案内チャンネル」に誘導するサービス。
コンテンツ保護を伴う無料番組	コンテンツの権利保護を目的とし、顧客管理を伴わず、放送波において安全にコンテンツの送信を行う無料番組。

権利保護を伴う無料番組	部分受信階層において、コンテンツの権利保護を目的とした放送波の暗号化を行わずに、デジタルコピー制御記述子およびコンテント利用記述子によってコピー制御を行う無料番組。
メール	IC カード毎に送られる EMM メッセージの内、受信機へ記憶するメッセージで、ユーザー操作などにより任意に呼び出せるメッセージ。
限定受信放送	限定受信方式記述子を利用した放送。限定受信放送には、有料番組、EMM メッセージを利用した放送、コンテンツ保護を伴う無料番組がある。
自動表示メッセージ	IC カード毎に送られる EMM メッセージの内、IC カードへ記憶するメッセージ（蓄積受信機能を有する受信機で受信した信号を再生する場合を含む）で、番組受信中に同時に表示するメッセージ。
商品企画	搭載される機能や動作が受信機または商品に依存するもの。
蓄積機能	記録した機器でのみ再生可能な記録再生機能。
無料番組	非課金対象の番組。SDT、EIT に記述された free_CA_mode=0 の番組。
有料番組	課金対象の番組。SDT、EIT に記述された free_CA_mode=1 の番組。
コンテンツ保護方式	コンテンツの権利保護を目的とし、暗号化等によりコンテンツの改ざんおよび不正コピー等を防止する技術。

4　送出運用規定

4.1　限定受信放送

- 限定受信方式記述子を利用した放送である。
- 限定受信放送には、有料番組、EMM メッセージを利用した放送、コンテンツ保護を伴う無料番組がある。

4.2　課金単位（課金対象ES）

- 課金単位は有効な ECM 毎である。
- 地上デジタルテレビジョン放送においては、ECM は PMT の第 1 ループにただ一つのみ配置される。すなわち、ES（コンポーネント）毎の課金は行わない。

4.3　ノンスクランブル／スクランブル

4.3.1　概要

- 受信側でのコンポーネントのスクランブルモードの判定は、TS パケットヘッダ中の transport_scrambling_control フィールドを参照する。地上デジタルテレビジョン放送において、free_CA_mode に関しては、有料か無料かの判定目的だけとし、スクランブル、ノンスクランブルの判定を有料・無料の判定に用いてはならない。
- コンポーネントが課金対象である場合にも、常にスクランブルされるとは限らない。運用上ノンスクランブル挿入が必要な場合を本編 4.10.4　ECM の適用の変更に記載する。

4.3.2　字幕、文字スーパーの運用

- デフォルト ES 群が PMT 第 1 ループに有効な ECM_PID が記載されている場合、すなわち通常のスクランブル状態では、字幕、および文字スーパーのコンポーネントをスクランブルする場合は、必ずデフォルト ES 群と同じ ECM _PID とする。
- デフォルト ES 群がスクランブル状態であっても、字幕、文字スーパーのコンポーネントをノンスクランブルで運用することが可能である。この場合、必ず当該ノンスクランブルコンポーネントに対して PMT 第２ループに無効な ECM_PID = 0x1FFF を記載する。
- デフォルト ES 群がノンスクランブルの場合は、字幕、文字スーパーコンポーネントのいずれもノンスクランブルで運用する。

4.4　無料番組、有料番組

4.4.1　無料番組／有料番組

4.4.1.1　定義

- 無料番組とは、その番組を構成するデフォルト ES 群が非課金のもの、有料番組は課金対象のものをいう。
- デフォルト ES 群はサービスタイプ毎に定義される。

例：デジタル TV サービスの場合

デフォルト ES 群＝デフォルト映像 ES とデフォルト音声 ES

表 4-1　デフォルト ES 群

service_type	内容	デフォルト ES 群
0x01	デジタル TV サービス	映像、音声
0xC0	データサービス	データ(エントリコンポーネント)
0xA1	臨時映像サービス	映像、音声
0xA3	臨時データサービス	データ(エントリコンポーネント)
0xA4	エンジニアリングサービス	規定せず*1
0xAA	ブックマーク一覧データサービス	データ(エントリコンポーネント)

＊1：　エンジニアリングサービスは視聴目的で選択されるサービスではないため限定受信方式としてのデフォルトES群としての規定は行わない。

4.4.1.2　運用

(1)　無料番組

- 全ての ES を非課金とする。
- SDT または EIT において free_CA_mode=0 で運用を行う。

(2)　有料番組

- 有効な ECM は PMT の第 1 ループにただ一つのみ配置され、コンポーネント毎の課金は行わない。
- SDT または EIT において free_CA_mode=1 で運用を行う。
- デフォルト ES 群以外の ES において、ノンスクランブル運用を行う場合は、PMT の第 2 ループに ECM_PID=0x1FFF を配置する。
- 有料放送事業者が加入者向けに一時的あるいは番組単位で非課金の放送を行う場合であっても有料番組として扱い free_CA_mode=1 で運用する。
- コンポーネントタグ値が 0x85 の音声 ES を、部分受信階層においてノンスクランブルで運用する場合、部分受信階層以外で運用する有料番組では、デフォルト音声 ES として運用しない。

4.4.2　コンテンツ保護を伴う無料番組

4.4.2.1　定義

- コンテンツ保護目的のため、放送波において安全にコンテンツの送信を行うため非課金のスクランブル番組である。
- ARIB STD-B25 第 1 部準拠の限定受信方式における「スクランブル有り無料番組」の機能を利用する。
- コンテンツ保護を伴う無料番組においては、受信機で、ECM の非暗号部に記載された事業体識別の値により、コンテンツ保護を伴う無料番組であることが認識されるように、4.4.2.2　運用　で規定する事業体識別が使用される。

- 部分受信階層においては、コピー制御を伴う無料番組においてはノンスクランブルで運用し、部分受信階層以外のスクランブルされたコンテンツ保護を伴う無料番組と区別するため、権利保護を伴う無料番組と称する。

4.4.2.2 運用

- ECM は必ず伝送する。また、PMT の第 1 ループに本書　第八編で規定する権利保護共通の事業体識別による有効な ECM を示す PID が 1 個のみ配置される。本書　第八編に関連記載があるので、参照のこと。
- コンテンツ保護を伴う無料番組においては CA 契約情報記述子を配置する必要はない。
- コンテンツ保護を伴う無料番組においては、基本的にはスクランブル放送の鍵明け目的の EMM の送出を必要としないが、Kw 更新のために EMM 送出することが可能である。
- EMM メッセージの運用を行う場合は、本編 4.11 EMM に準じる。
- コンテンツ保護を伴う無料番組において、事業体識別は当該番組の運用において共通の値が用いられるため、EMM を送出する場合は、EMM メッセージや通電制御など受信機で事業体識別毎に管理を行っているため、問題がおきないように全運用事業者の合意を得た後、慎重に運用を行うこと。
- デフォルト ES 群以外の ES においてノンスクランブル運用を行う場合は PMT の第 2 ループに ECM_PID=0x1FFF を配置する。ただし、コンポーネントタグ値 0x85 の音声 ES をデフォルト音声 ES として運用する番組（部分受信階層以外）においては、当該 ES がノンスクランブルであるため、PMT 第 2 ループにおいて当該 ES に対し ECM_PID = 0x1FFF を配置する。
- 有料放送事業者が一時的あるいは番組単位でコンテンツ保護を伴う無料番組の運用を行う場合がある。
- 部分受信階層における権利保護を伴う無料番組においては ECM は伝送しない。ただし、権利保護を伴う無料番組以外の限定受信サービスに関してはこの限りではない。

4.4.3 有料番組・無料番組・コンテンツ保護を伴う無料番組の運用上の組み合わせ

- 表 4-2 に有料番組、無料番組、およびコンテンツ保護を伴う番組の運用についての運用条件の一覧を示す。　また表 4-3 にデフォルト ES 群とデフォルト ES 群以外でのスクランブル／ノンスクランブルの運用可能な組み合わせについて示す。

表 4-2　有料番組、無料番組、コンテンツ保護を伴う無料番組、および権利保護を伴う無料番組の運用

No		1	2	3	4
番組種別		無料番組	コンテンツ保護を伴う無料番組（部分受信階層以外）	有料番組	権利保護を伴う無料番組（部分受信階層のみ）
有料/無料番組の区分		無料	無料	有料	無料
有料付加ＥＳ		×	×	×	×
Free_CA_mode		0	0	1	0
コンテンツ保護対象	ﾃﾞﾌｫﾙﾄ ES 群	非対象	保護対象可	保護対象可	保護対象可
	ﾃﾞﾌｫﾙﾄ以外 ES	非対象	保護対象可	保護対象可	保護対象可
ＴＳパケットヘッダ *4	ﾃﾞﾌｫﾙﾄ ES 群	00	10,11 *1	10,11	00
	ﾃﾞﾌｫﾙﾄ以外 ES	00	10,11 *2	10,11 *2	00
課金対象	ﾃﾞﾌｫﾙﾄ ES 群	非課金	非課金	課金可	非課金
	ﾃﾞﾌｫﾙﾄ以外 ES	非課金	非課金	課金可	非課金
ECM 送出		不要	必要	必要	不要
EMM 送出		送出可（EMM ﾒｯｾｰｼﾞ）	送出可 *3	必要	不要
使用する事業体識別	ﾃﾞﾌｫﾙﾄ ES 群	－	権利保護共用 ID	事業体固有 ID	－
	ﾃﾞﾌｫﾙﾄ以外 ES	－	PMT 1st ﾙｰﾌﾟのみ有効な ECM 配置	PMT 1st ﾙｰﾌﾟのみ有効な ECM 配置	－

*1：　コンテンツ保護を伴う無料番組において、デフォルトES群であっても、コンポーネントタグ値が0x85のESについてはノンスクランブルで運用され、PMT 第2ループに無効なECM_PID=0x1FFFを配置する。

*2 ：　コンテンツ保護を伴う無料番組、および有料番組において、デフォルトES群以外でノンスクランブル運用を行う場合は、コンポーネントタグ値が0x30～0x3Fの字幕、文字スーパーのES、デフォルトES群以外の0x40～0x7Fのデータコンポーネント、およびコンポーネントタグ値 0x84、0x86のAAC音声ESである。
また、この際にはPMT 第2ループに無効なECM_PID=0x1FFFを配置する。

*3 ：　コンテンツ保護を伴う無料番組においてもEMMメッセージを伝送する場合がある。また、Kw更新目的等でEMM送出が可能である。

*4 ：　TSパケットヘッダ中のtransport_scrambling_controlフィールド。

表 4-3　スクランブル／ノンスクランブルの運用可能な組み合わせ

		デフォルトＥＳ群			
		無料番組	コンテンツ保護を伴う無料番組*2 （部分受信階層以外）	有料番組	権利保護を伴う無料番組 (部分受信階層のみ)
デフォルトＥＳ群以外	ノンスクランブル *1	○ 1st：なし 2nd：なし	○ 1st：権利保護共用 2nd：PID=0x1FFF	○ 1st：固有事業体 2nd：PID=0x1FFF	○ 1st：なし 2nd：なし
	コンテンツ保護のためのスクランブル	×	○ 1st：権利保護共用 2nd：なし	×	×
	有料番組のためのスクランブル	×	×	○ 1st：固有事業体 2nd：なし	×
	存在しない（2nd ループなし）	○ 1st：なし	○ 1st：権利保護共用	○ 1st：固有事業体	○ 1st：なし

*1：デフォルトES群以外でノンスクランブル運用が可能なのはコンポーネントタグが0x30～0x3Fの字幕、文字スーパーのES、デフォルトES群以外の0x40～0x7Fおよびコンポーネントタグ値 0x84、0x86のAAC音声ESのコンポーネントに限定される。

*2：コンテンツ保護を伴う無料番組において、デフォルトES群であっても、コンポーネントタグ値が0x85のESについてはノンスクランブルで運用され、PMT 第2ループに無効なECM_PID=0x1FFFを配置する。

－ 表 4-3 における語句の解説

・○：運用可能、　×：運用禁止（運用制限）

・PMT の第 1 ループ（1st）、第 2 ループ（2nd）に配置する限定受信方式記述子の内容を示す。

1) なし　　：限定受信方式記述子を配置しない。

2) PID=0x1FFF　：限定受信方式記述子を配置し、無効な ECM をポイントする。ECM ストリームは存在しない。

3) 権利保護共用：限定受信方式記述子を配置し、権利保護共用の事業体識別の ECM をポイントする。

4) 固有事業体　：限定受信方式記述子を配置し、有料事業者固有の事業体識別の ECM をポイントする。

4.5　階層伝送時における限定受信サービスの運用

4.5.1　伝送階層と限定受信サービス関連情報の伝送

- CAT は強階層で伝送される。
- ECM は PMT が記述される階層と同一階層、またはより強い階層で伝送される。

表 4-4　部分受信階層伝送時における限定受信サービスに関連する情報の伝送

ﾊﾟﾀｰﾝ	使用階層	セグメント数	CAS に関連する情報		
			CAT	EMM	ECM
(1)	A	13	○	○	○
(2)	A	13	○	○	○
(3)	A	1（部分受信）	○	△	△
	B	12	×	○	○
(4)	A	8～2	○	○	○
	B	5～11	×	×	○
(5)	A	1（部分受信）	○	△	△
	B	12	×	○	○
(6)	A	1（部分受信）	○	△	△
	B	7～1	×	○	○
	C	5～11	×	×	○

表中、○：送出可能、×：送出しないもの、△：有料放送を行う場合に送出可能

- 表 4-4 におけるパターンは本書　運用概要 表 2 のパターンと同じ意味である。

4.5.2　部分受信階層における限定受信サービス

- 部分受信階層においては、コンテンツ保護目的のスクランブル放送は行わない。
- 将来、限定受信方式で有料放送を行う可能性がある。この場合 PMT に限定受信方式記述子を記載する。(A.9 に関連記載がある)
- 部分受信階層における有料放送運用は、運用開始時に改めて規定するものとし、必ずしも、本編で規定する ARIB　STD-B25 第一部準拠方式の限定受信方式で運用するとは限らない。

4.6　パレンタルレートの設定

- パレンタルコントロールの運用は行わない。

4.7　PPVの運用

- 地上デジタルテレビジョン放送では放送開始時点において、PPV 運用は行わない。
- PPV を運用開始する場合は、本運用規定を改定するともに、EIT または SDT に CA 契約情報記述子を正しく配置する。受信機では、番組予約時において、本記述子の IC カー

ド応答により PPV サービスか否かが認識される。つまり、放送開始時点で PPV 非対応の受信機においては、IC カード応答により当該番組が PPV であることが認識され、非対応のメッセージなどの処理が行われることを想定している。

4.8 限定受信方式記述子

4.8.1 機能

- CAT に記載された場合は EMM を伝送する TS パケット ID を特定する。
- CAT に複数の限定受信方式記述子が記述される場合がある。
- PMT に記載された場合は ECM を伝送する TS パケット ID を特定する。
- PMT に複数の限定受信方式記述子が記載される場合がある。

4.8.2 運用

- CAT に限定受信方式記述子を同一 CA_system_id で運用する場合は 1 度のみの記載とする。
- CAT に当該 TS 内で EMM を送出する CA_system_id の数の限定受信方式記述子を記載する。
- PMT に当該番組で運用される CA_system_id の数の限定受信方式記述子を記載する。
- 番組内のコンポーネントにスクランブル ES とノンスクランブル ES とが混在する場合には、PMT における限定受信方式記述子の配置を以下のように定める。
    1) 限定受信方式記述子を PMT の第 1 ループに配置する場合、番組内のすべてのコンポーネントに対し当該 ECM が適用される。
    2) 限定受信方式記述子を PMT の第 2 ループには配置しない。(PPV 運用制限の間) ただし、デフォルト ES 群以外でノンスクランブル運用する場合に限り無効な ECM_PID=0x1FFF を配置する場合がある。
    3) 複数の限定受信方式記述子を記載する場合は、第 1 ループ、第 2 ループに記載される限定受信方式記述子の数、記載される CA_system_id は同一である。この場合も第 2 ループに記載される限定受信方式記述子の ECM PID は当該 ES がノンスクランブルを意味する無効な値の場合のみである。
- PMT に限定受信方式記述子を記載する場合、private_data_byte 領域に記載するデータは先頭 1 バイトを受信機においては無視される。これは、BS デジタル放送におけるパレンタルレートの運用との整合を取るためである。(2 バイト目以降は当面運用しない)
- CAT に限定受信方式記述子を記載する場合、private_data 領域の先頭 1 バイトには EMM 伝送識別を記載する。詳細については、本書　4.11.1.1　を参照のこと。

－ 同一 TS 内において、複数の限定受信方式が運用される場合においても、EMM 伝送方式は、TS 内でただ 1 つの方式で伝送される。つまり、TS 内で異なる EMM 伝送識別で運用されることはない。

4.9 CATの送出

4.9.1 伝送されるTS PID

－ 平成 26 年総務省告示第 233 号記載の「PID の割り当て」の通り。（0x0001）

4.9.2 データ構造

－ 平成 26 年総務省告示第 233 号記載の「CAT の構成」の通り。

4.9.3 伝送される記述子とその構成

－ CAT にて伝送される記述子は限定受信方式記述子、および CA サービス記述子とし、限定受信方式記述子の構成は、平成 26 年総務省告示第 233 号記載の「限定受信方式記述子の構成」の通りとする。CA サービス記述子の構成は本書第四編を参照のこと。

－ CA_system_id は本書第七編を参照のこと。

4.9.4 送出頻度

－ CAT の送出頻度は第四編による。

4.9.5 更新頻度

－ EMM を伝送する PID が変更される場合、自動表示メッセージのサービスが変更される場合、CAT も更新される。ここで自動表示メッセージのサービスが変更される場合とは、自動表示メッセージのサービス自身を行うか行わないかを意味する。

－ 通常の運用では、更新頻度は 1 回／日以下とする。

4.10 ECM

4.10.1 ECMの特定

－ PMT の第 1 ループに限定受信方式記述子が記載される場合に ECM の伝送される TS パケットの PID が特定される。

－ 限定受信方式記述子の限定受信 PID が 0x1FFF のときに限り、当該 ECM は伝送されることはない。

4.10.2 ECMのデータ構造

4.10.2.1　セクション形式

－　平成 26 年総務省告示第 233 号記載の拡張セクション形式で伝送され、テーブル識別子の値は 0x82 のみを使用し、0x83 は使用しない。また「テーブル識別子拡張」は使用しない。

4.10.2.2　ECM本体

－　ECM セクション内の ECM 本体のデータ構造については、ARIB STD-B25 第 1 部 3.2.3 ECM を参照。

4.10.3 ECMの適用

－　限定受信方式記述子が PMT の第 1 ループに記載された場合には放送番組要素を伝送する ES すべてに当該 ECM が適用される。本来、第 2 ループに記載された場合には当該 ES のみ適用されるが、地上デジタルテレビジョン放送においては、放送開始時点、PPV 運用制限とするため、PMT の第 1 ループにのみ有効な ECM PID が記述される。

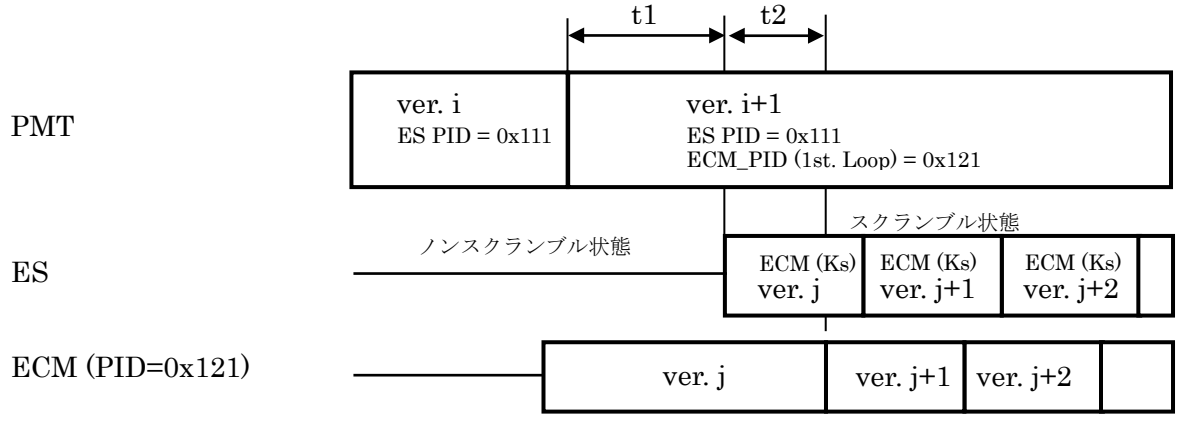
－　ECM_PID（限定受信 PID）として、0x1FFF が使用されたときは当該 ES がスクランブル処理されていないことを示し、実際に PID=0x1FFF の ECM が伝送されることもない。

4.10.4 ECMの適用の変更

本編 A.4.3 に関連記載がある。

4.10.4.1　スクランブルの開始

－　ノンスクランブル放送（または放送番組要素を伝送する ES）がスクランブル放送（または放送番組要素を伝送する ES）に切り替わる場合の放送信号の変化は以下の通り。



1)　当該 ES がノンスクランブル状態で送出された状態で、ECM が送出される。

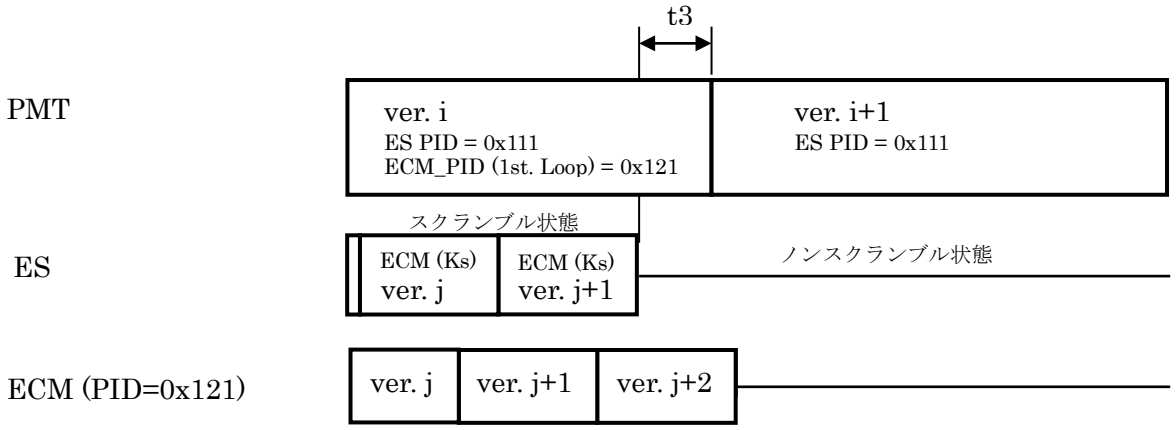
2) ECM が送出された後、PMT の第 1 ループに ECM と当該 ES（群）の関連が記載され送出される。（PMT の更新）
3) PMT 更新の t1 秒後、当該 ES（群）にスクランブルが開始される。
4) スクランブル開始後、t2 秒後に、最初の ECM 更新が発生する。
   t1= 2，0<t2

ECMの更新に関しては
4.10.5.2　更新・再送周期
4.10.5.3　ECMの更新とスクランブル鍵の変更

に準ずる。

4.10.4.2　スクランブルの終了

－　スクランブル放送（または放送番組要素を伝送する ES）がノンスクランブル放送（または放送番組要素を伝送する ES）に切り替わる場合の放送信号の変化は以下の通り。

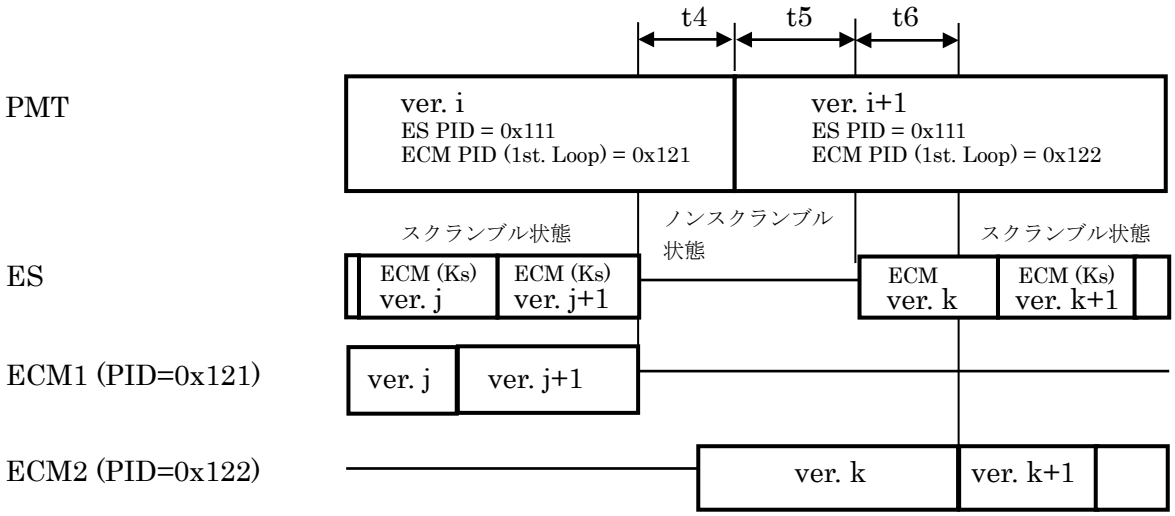


1) 当該 ES（群）へのスクランブル動作が停止する。
2) t3 秒後，PMT の第 1 ループに ECM と当該 ES（群）との関連が削除され、送出される。（PMT の更新）
   t3=1

4.10.4.3　放送番組要素を伝送するESとECMとの関係の変更

(1)　ECM_PID の変更を伴う場合

－　限定受信記述子が PMT の第 1 ループに記載されている場合に、放送番組要素を伝送する ES と既に PMT で記載されている ECM_PID との関係を変更する場合で、ECM_PID の変更が伴う場合には、以下のようなスクランブル状態からノンスクランブル状態への遷移手順を経ることとする。



1)　すべての ES がノンスクランブル状態で送出される。

2)　新しい ECM が送出される。

3)　1)から t4 秒後、PMT が更新される

4)　PMT の更新から t5 秒後，ES にスクランブルが開始される。

5)　ES にスクランブルが開始されてから t6 秒後、最初の ECM の更新が行われる。

t4=1、t5= 2、0<t6

ECMの更新に関しては本編の

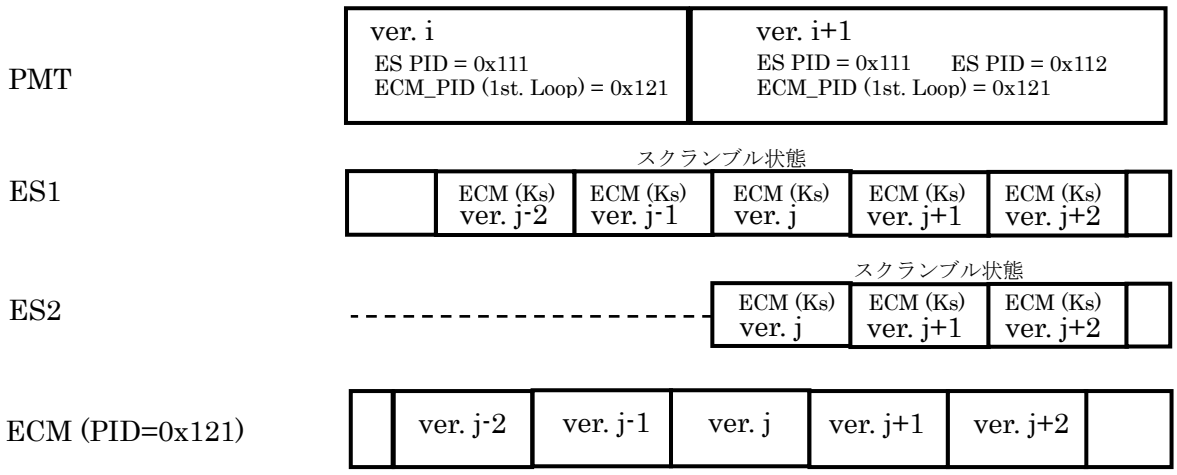
4.10.5.2　更新・再送周期

4.10.5.3　ECMの更新とスクランブル鍵の変更

に準ずる。

(2)　ECM_PID の変更を伴わない場合

- 限定受信記述子が PMT の第 1 ループに記載されている場合に、放送番組要素を伝送する ES と既に PMT で記載されている ECM_PID との関係を変更する場合で、ECM_PID の変更を伴わない場合には、スクランブル状態からノンスクランブル状態への遷移などの特別な送出手順を行う必要がない。
- 例として、新規 ES が追加される場合の放送信号の変化を以下に示す。



4.10.5 ECMの更新・再送

- ECM が適用される ES のスクランブル鍵が変更される場合には、スクランブル鍵の変更に先だって ECM が更新される。ECM の更新は拡張セクション形式のバージョン番号の変更により通知される。

4.10.5.1　スクランブル鍵の変更

- ECM が適用される ES に施されるスクランブルの鍵（Ks）の変更は、当該 ES ヘッダ内のトランスポートスクランブル制御フラグを用いて行われる。スクランブル鍵の変更に伴って、常にトランスポートスクランブル制御フラグは変更される。偶数鍵から奇数鍵、奇数鍵から偶数鍵の順に変更され、同一鍵が続けて変更されることはない。

4.10.5.2　更新・再送周期

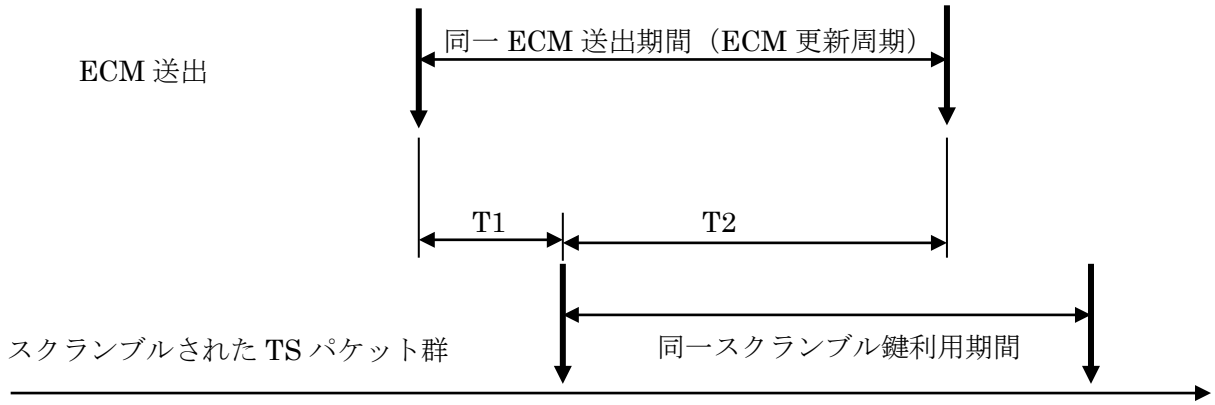
- ARIB STD-B25 第 1 部　参考 2　4.別表を参照。
- 下記に ECM の更新・再送周期の推奨値を記載する。本編 A.4 に関連記載がある。

表 4-5　ECM 更新周期、再送周期の推奨値

	部分受信階層以外	部分受信階層
ECM 更新周期	2 s	TBD
ECM 再送周期	100ms	TBD

4.10.5.3　ECMの更新とスクランブル鍵の変更

－　単一で ECM が適用された場合の ECM の更新とスクランブル鍵の変更を下図に示す。



1600ms<T1、0<T2、T 1 ＋T2>2000ms

－　複数の TS パケットに ECM が適用される場合には各パケットに対して T1、T2 ともに最小のものを適用する。

4.10.6 その他

4.10.6.1　ECMとスクランブル

- PMT の第一、第 2 ループに限定受信方式記述子が記載されていない場合は、放送番組要素を伝送する ES 群すべてがスクランブル伝送されていないことを示す。
- 逆に PMT の第一、第 2 ループに限定受信方式記述子が記載されていても、サービスを構成するすべてのコンポーネントがスクランブルされない運用も実施される。（スクランブル放送からノンスクランブル放送への遷移状態等の考慮。）
- 但し、ECM_PID=0x1FFF と関連づけられた ES にスクランブルが行われることはない。

4.10.6.2　ECMの途絶

(1) ECM の途絶の検出

各 ECM は 4.10.5.2　更新・再送周期　記載の条件で PMT に記載のある場合は再送されているので受信機は ECM が規定時間以内に受信できない場合に ECM の途絶を検出することができる。（2 秒以内）

(2) ECM の途絶時の受信機動作

番組選択時に ECM の途絶を検出した受信機は、IC カードの有無に係わらず放送番組を構成する TS パケットのヘッダ部のトランスポートスクランブル制御フラグを参照した動作を行う。

4.11　EMM

4.11.1 EMMの送出仕様

4.11.1.1　EMMストリームの指定方法

2種類のEMM伝送方式を規定する。

(1) 伝送形式の識別手段

- TypeA、TypeB の伝送形式は、CAT に記載された限定受信方式記述子の private_data_byte 領域先頭 1 バイトに記述される。

表 4-6　CAT に記載した限定受信方式記述子の private_data_byte の先頭 1 バイト

値	意味
0x00	未定義
0x01	Type A
0x02	Type B
0x03～FF	将来使用のためのリザーブ

- CAT に記載された限定受信方式記述子の private_data_byte の 1 バイト目に EMM 伝送形式の識別情報が必ず記述される。
- CAT に記載された限定受信方式記述子の private_data_byte の 1 バイト目に有効な EMM 伝送形式の識別情報値が記述されていない場合はあくまで例外処置のため、受信機での EMM 取得は保証されず、一切取得しない場合もあり得る。
- 本書　解説 A.3.5 に関連記載がある。

4.11.1.2　部分受信階層以外でのEMM送出仕様

(1)　TypeA の送出仕様

- CAT に記載された限定受信方式記述子の private_data_byte 領域の先頭 1 バイトに、必ず TypeA を指定する。
- EMM セクションのヘッダ構成は平成 26 年総務省告示 第 233 号に基づく。
- EMM セクション内の EMM 本体の構成は、ARIB STD-B25 第 1 部 第 3 章 3.2.4 項 EMM を参照のこと。
- EMM セクションはマルチセクションでは送出しない。
- EMM の伝送頻度は以下の通りとする。
  EMM セクションと EMM 個別メッセージセクションの両者を併せて送出頻度を定める。
  送出頻度は、本編 4.11.3 EMM 送出頻度による。
- 受信機は、EMM セクションのバージョン番号を参照しない。
- EMM の送出順序は、本編 4.11.4 EMM 送出順序による。
- グループ ID の運用は行わない。

(2)　TypeB の送出仕様

- CAT に記載された限定受信方式記述子の private_data_byte 領域の先頭 1 バイトに、必ず TypeB を指定する。
- 1EMM セクションに含まれる EMM 本体は 1 つ、即ち 1 カード ID のみの情報とする。セクションには、セクションヘッダ、1 つの EMM 本体、セクション CRC のみ含まれる。
- 1TS パケットには複数の EMM セクションの設定を可能とする。
  EMM フィルタリングの対象となる情報（セクションヘッダの 8 バイトとカード ID の 6 バイトの計 14 バイト）は複数の TS パケットに跨がらない。
- マルチセクションで 1TS パケットに埋め込まれるセクションの最大数は、本書　第四編 （マルチセクション伝送）にあるように最大 10 個である。
- 同一カード ID に伝送される EMM の伝送間隔は既定の 1 秒以上を遵守する。つまり、1 TS パケット内に複数 EMM が存在しても、該当する EMM は最大 1 個が保証される。

－ グループ ID とグローバル ID の運用は行わない。

4.11.1.3 部分受信階層でのEMM送出仕様（T.B.D.）

4.11.2 EMMメッセージの送出仕様

(1) TypeAの送出仕様

－ EMM メッセージセクション内の EMM 個別メッセージ本体の構成は、ARIB STD-B25 第 1 部 第 3 章 3.2.5.2 項 EMM 個別メッセージを参照のこと。

－ EMM メッセージセクション内の EMM 共通メッセージ本体の構成は、ARIB STD-B25 第 1 部を参照のこと。

－ EMM メッセージはマルチセクションでは送出しない。

－ EMM 個別メッセージの送出頻度は本編 4.11.3 EMM 送出頻度による。

－ EMM 共通メッセージの送出頻度は本編 4.11.3 EMM 送出頻度による。

－ EMM 共通メッセージのメッセージ本体の領域が 0 バイトの場合、自動表示消去種別が「0x02」の場合に、そのメッセージ、およびメッセージ用画枠含め表示しないこと。（緊急対応。この場合受信機はメッセージを表示しない）

－ 受信機は目的の EMM メッセージセクションのバージョン番号を参照し、メッセージの表示中に EMM 共通メッセージの内容の更新や表示の消去に備えるものとする。

－ 受信機は、EMM の個別メッセージセクションのバージョン番号を参照しない。

－ EMM 個別メッセージの送出順序は、本編 4.11.4 EMM 送出順序による。

－ 部分受信階層においては、EMM メッセージの送出は行わない。

－ グループ ID の運用は行わない。

(2) TypeBの送出仕様

－ 1EMM 個別メッセージセクションに含まれる EMM 個別メッセージ本体は 1 つ、即ち 1 カード ID のみの情報とする。セクションには、セクションヘッダ、1 つの EMM 個別メッセージ本体、セクション CRC のみ含まれる。

－ 1TS パケットには複数の EMM 個別メッセージセクションの設定を可能とする。

－ EMM 個別メッセージのフィルタリングの対象となる情報（セクションヘッダの 8 バイトとカード ID の 6 バイトの計 14 バイト）は複数の TS パケットに跨がらない。

－ マルチセクションで 1TS パケットに埋め込まれるセクションの最大数は、本書第四編 （マルチセクション伝送）にあるように最大 10 個である。

－ 同一カード ID に伝送される EMM 個別メッセージセクションの伝送間隔は既定の 1 秒以上を遵守する。つまり、 1 TS パケット内に複数の EMM 個別メッセージセクションが存在しても、該当する EMM 個別メッセージセクションは最大 1 個が保証される。

－ グループ ID とグローバル ID の運用は行わない。

4.11.3 EMM送出頻度

4.11.3.1　部分受信階層以外でのEMM送出頻度

（a）　EMM セクションおよび EMM 個別メッセージセクションの送出頻度

(1)　TypeA

－　地上デジタルテレビジョン放送においては、EMM は全て番組用 TS で送り、専用 TS では送らない。本編 A.3 に関連記載がある。

－　EMM セクションおよび EMM 個別メッセージセクションの TS パケットレベルの送出頻度については、基本的な考え方は第四編に準ずる。（ここでいう第四編に準ずる基本的な考え方とは、EMM の送出頻度を EMM セクションと EMM セクションの間隔で規定するのではなく、PSI/SI の運用規定にあわせて EMM セクションの伝送密度で規定することを意味する）

－　EMM セクションおよび EMM メッセージセクションを伝送する場合、当該 PID の TS パケットを、32ms 単位に 1.28kB±100%の範囲で送出する。EMM セクションおよび EMM メッセージセクションを伝送する TS パケットは、同一 PID で任意の 1 秒間あたり、320kbit を超えて伝送しない。

（上記における 320kbit において、1 つの EMM セクションおよび EMM メッセージセクションのデータ量は 4kB とみなすものとする。）

(2)　TypeB

－　番組 TS、専用 TS（特定トラポン）に関わらず、EMM セクションおよび EMM 個別メッセージセクションを伝送する場合、当該 PID の TS パケットを、32ms 単位に 8.0kB±100%の範囲で送出する。EMM セクション及び EMM メッセージセクションを伝送する TS パケットは、同一 PID で任意の 1 秒間あたり、2.0Mbit を超えて伝送しない。（上記における 2.0Mbit において、1 つの EMM セクションおよび EMM 個別メッセージセクションのデータ量は 4kB とみなすものとする。）

(b)　EMM 共通メッセージセクションの送出頻度

－　TypeA、TypeB 共に特定の定型文番号（Table ID Extension）を持つ EMM 共通メッセージセクションの送出頻度は、200ms 当たり最大 1 セクションとする。

4.11.3.2　部分受信階層でのEMM送出頻度（T.B.D.）

4.11.4 EMM送出順序

(1)　TypeA

－　EMM と EMM 個別メッセージは、1 セクションに複数個の情報が詰め込まれて伝送される。

受信機でのフィルタリング処理を容易にするために、同一セクション内に詰め込む

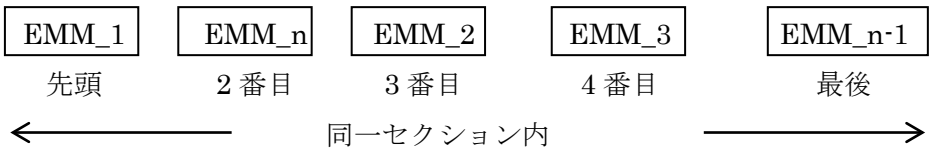
EMM の配置順序に次のような運用制限を設ける。EMM 個別メッセージについても同様とする。

1)先頭の EMM は、そのセクション内に含まれる最小のカード ID の EMM とする。

2)2 番目の EMM は、そのセクション内に含まれる最大のカード ID の EMM とする。

3)3 番目以降の EMM は、残りの EMM をカード ID 順（昇順）にソーティングして配置する。

- 1 セクション内にｎ個の EMM があり、カード ID の小さい順に EMM_1，EMM_2，…，EMM_n であるとすると、次のような順序で配置される。



- 受信機は、先頭 2 つの EMM を調べるだけで、自分宛の EMM がそのセクション内に含まれる可能性があるかないかを確定できる。さらに含まれる可能性がある場合でも、前から順番に見てゆき、自分の ID より大きくなった時点で自分宛 EMM は含まれないと確定できる。自分宛 EMM が含まれないと確定した時点でセクション全体を廃棄でき、セクション内の最後の EMM まで比較する必要はない。

(2) TypeB

- 一つの IC カード宛てに送出される EMM 及び EMM 個別メッセージは 1 セクションに 1 個のみである。

4.12 EMMメッセージにおけるメッセージコード

4.12.1 フォーマット番号

- フォーマット番号は 0x01 を定義する。以下の項はフォーマット番号 0x01 におけるメッセージコードのフォーマットについて定義する。
- ARIB または本編で定義されたフォーマット以外のフォーマット番号を受信した場合は、受信機はそのメッセージコードを破棄し、受信したこと自体を無視する。

4.12.2 フォーマット番号0x01における、EMM共通メッセージのメッセージコード本体フォーマット

- メッセージコード本体が存在する場合、その 1 バイト目を「推奨表示位置」とする（本編 4.12.6　自動表示メッセージの推奨表示位置参照)。「推奨表示位置」は、自動表示メッセージ（IC カード蓄積メッセージ）において、その表示位置を指定する。メール（IRD 蓄積メッセージ）においては無効とし、受信機は無視する。
  推奨表示位置の意味は本編 4.12.6　自動表示メッセージの推奨表示位置に詳細を規定する。
- 2 バイト目以降、NULL の前の文字までを本体とする。（本体に NULL を入れることはできない）
- 差分情報で指定されるバイト列を挿入するポイントに挿入子 0x1A を記述する。
- 挿入子 0x1A は共通メッセージの中に複数個あっても良いが、個別メッセージのメッセージコードとマージした結果、メールについては 800 バイト、自動表示メッセージについては 400 バイトを超えないものとする。
- EMM 個別メッセージでポイントされる定型文番号を持つ EMM 共通メッセージのメッセージコードは、EMM 個別メッセージのメッセージコードと同一の文字符号でなければならない。

4.12.3 差分フォーマット番号0x01におけるEMM個別メッセージの差分情報フォーマット

- 差分情報として挿入したい文字列を指定する。
- 1 バイト目から NULL の前の文字までを本体とする。（差分情報として NULL は指定できない。）

4.12.4 差分情報の使用例

以下に、フォーマット番号0x01の場合の例を示す。

1) メッセージ本体（EMM 共通メッセージ）
   ：ご加入有り難うございます。0x1A 様は本日より、
   地上スペシャルパッケージをご覧になれます。
2) 差分情報（EMM 個別メッセージ）
   ：田中
3) 生成されるメッセージ
   ：ご加入有り難うございます。田中様は本日より、
   地上スペシャルパッケージをご覧になれます。

4.12.5 文字符号

- フォーマット番号 0x01 で使用できる文字及び制御コードは、以下のものを使用する。
  1) 第四編の第 1 部 4　文字列の符号化で定義される文字符号及び制御符号

2) 挿入子 0x1A

4.12.6 自動表示メッセージの推奨表示位置

- 自動表示メッセージの表示位置や画枠等についてのガイドラインを示す。

  EMM 共通メッセージセクションにおけるメッセージコード本体の先頭１バイトを「推奨表示位置」とし、次のように定める。

  上位４ビットを横方向の推奨表示位置（0100:左、0010:中、0001:右）、下位４ビットを縦方向の推奨表示位置（0100:上、0010:中、0001:下）とする。

  メッセージは受信機のローカルのダイヤログとし、上記バイトは推奨値とし、表示画素レベルでの厳密性は問わないものとする。

- 画枠に関しては、以下のような運用が望ましい。

  1) 受信機側では 18 文字（全角にて）×最大８行相当の画枠を用いる。

  2) 送出側のデータ作成では、最大 18×8 行を前提として、改行・SPACE を適宜挿入して全体のレイアウトを取るものとする。したがって送出側では、共通メッセージと個別メッセージをマージしたメッセージコードの中に全角 144 文字以上の表示文字データを含めてはならない。

  3) 受信側では改行の数と１行あたりの最大文字数により自動表示メッセージの画枠を最適化するものとする。

  4) 画枠を文字数・行数によって最適化する場合、本編自動表示メッセージの推奨表示位置の（0100:左、0010:中、0001:右）、（0100:上、0010:中、0001:下）は以下のことを意味する。

     左：画面内で、自動表示メッセージの画枠を左寄せで配置する

     右：画面内で、自動表示メッセージの画枠を右寄せで配置する

     上：画面内で、自動表示メッセージの画枠を上寄せで配置する

     下：画面内で、自動表示メッセージの画枠を下寄せで配置する

     中：画面内で、自動表示メッセージの画枠を中央に配置する

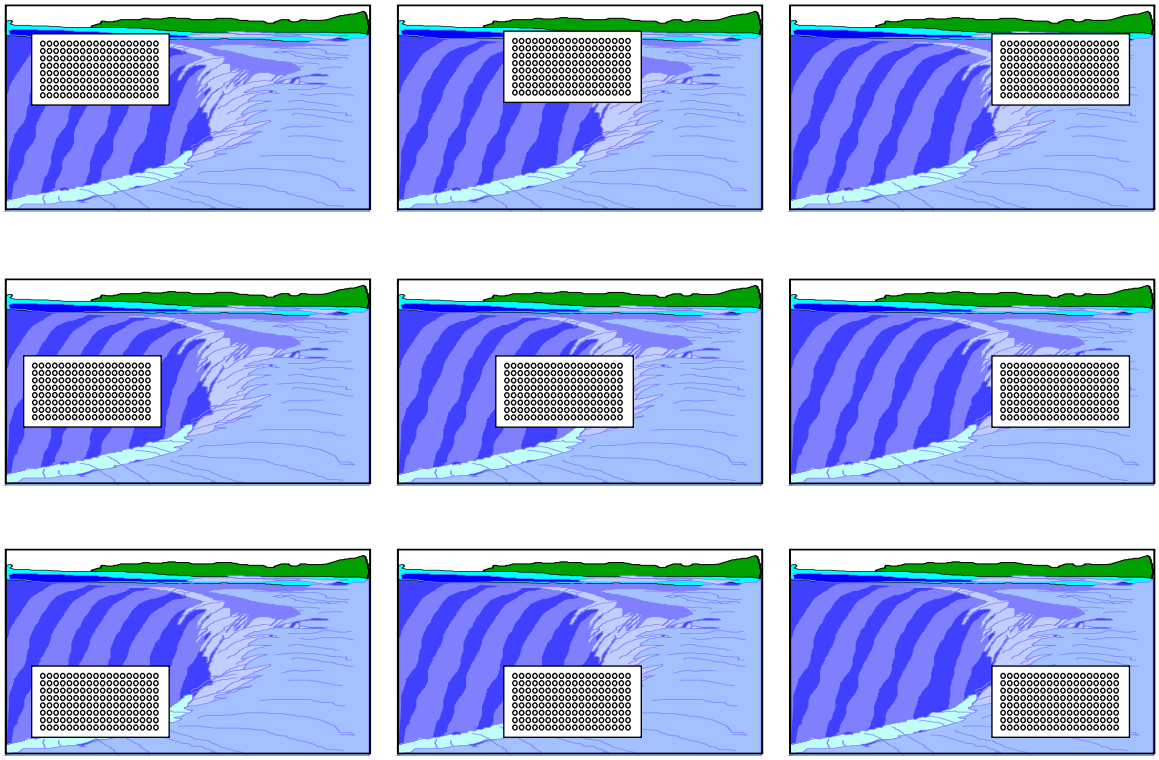
  5)送出側では最終文字の後に、改行をつけない。

  6)画枠内の上下左右の余白やデザイン等については受信機の任意とする。

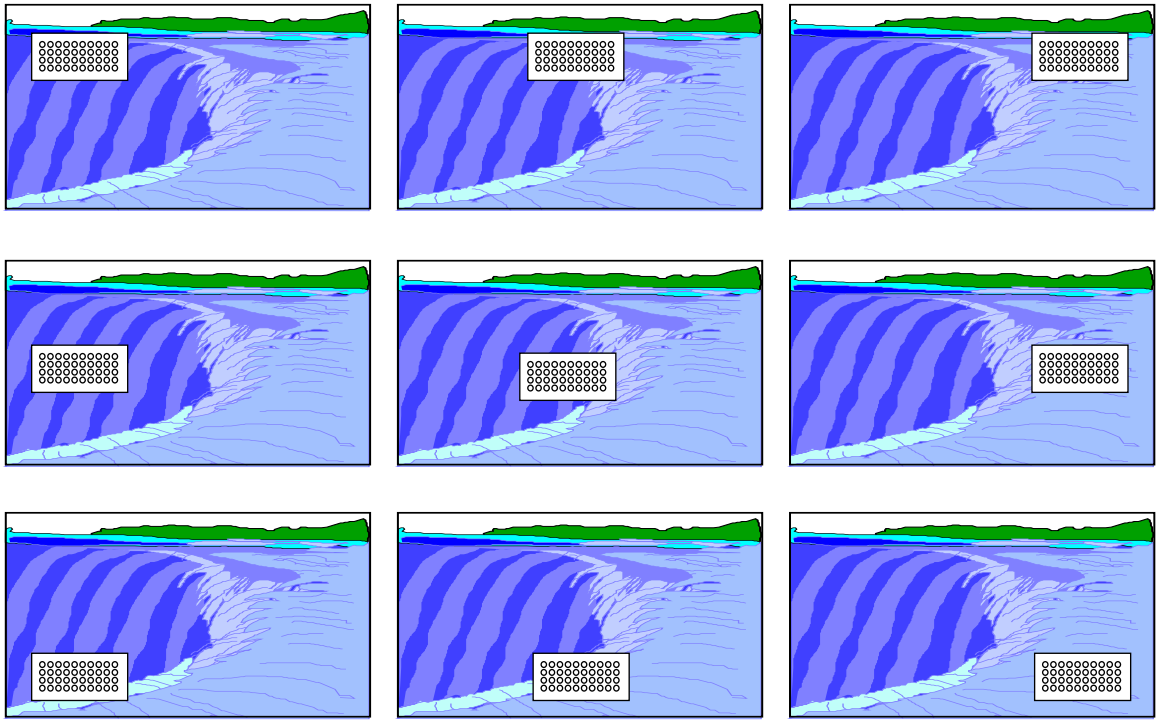
  7)受信側ではメッセージのページ送り表示はしない。

●表示のイメージについて

［最大（1 行 18 文字、8 行）画枠の例］



［画枠を最適化した場合の例］



4.13 CA契約情報記述子

- CA 契約情報記述子の運用にあたっては、本書第四編を参照のこと。
- PPV は地上デジタルテレビジョン放送開始時点では運用制限事項であるため、CA 契約情報記述子の「料金名称」は受信機において無視される。
- PPV を運用開始する場合は、本運用規定改定の後、SDT または EIT に CA 契約情報記述子を正しく配置すること。受信機は CA 契約情報記述子のカードレスポンスにより当該番組が PPV であることが認識される。
- フラット／ティアなどの契約番組に使用する CA 契約情報記述子の「料金名称」は使用しない。

4.14 メッセージID

4.14.1 運用

- メッセージ ID の再利用について規定する
- 事業体が同時に送信できるメッセージ（メール数） N 通*

事業体のメッセージ ID 再利用期間 M 日以上

事業体の 1 メッセージ送信期間 L 日以内

*メッセージ（メール）は送信開始時刻の古いメッセージ（メール）から送信を順次終了することを受信側では想定。

N=7、M＝30、L＝14

4.14.2 送信動作例

- 代表的な送信例を以下に示す。

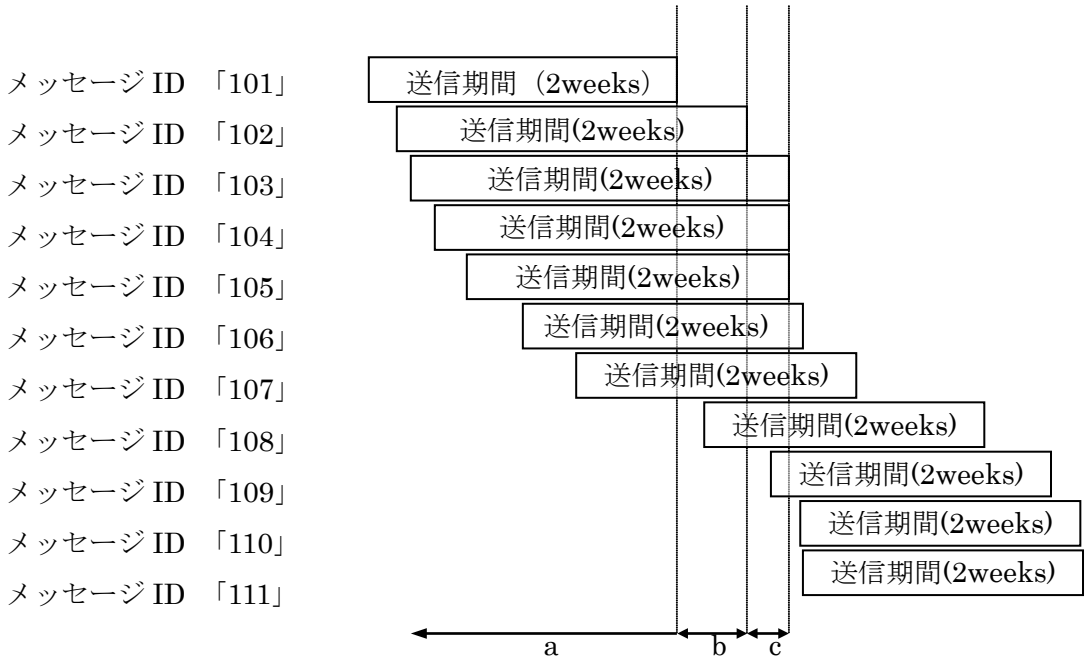
(1) 送信例 1（同一メッセージ ID）

メッセージ ID 「104」 送信期間

メッセージ ID 「104」 送信期間

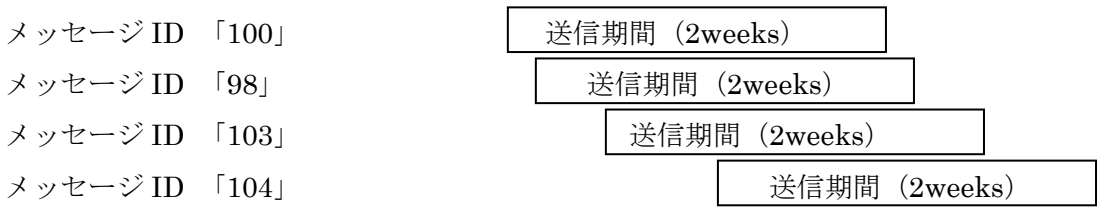
30 日以上

(2) 送信例 2（最も一般的な例）



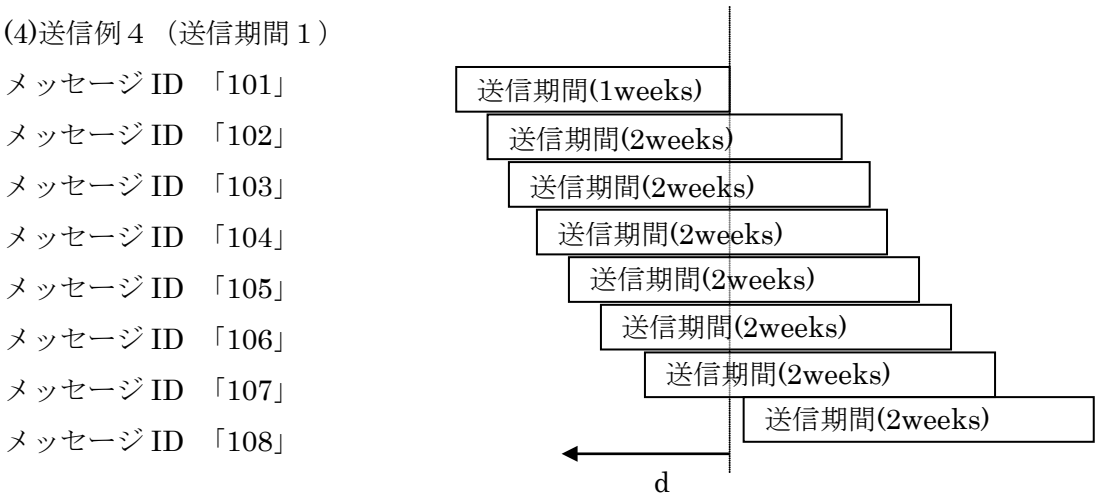
a、b、c どの領域でも送信されるメッセージ（メール）は 7 通以内

(3) 送信例 3（メッセージ ID の増加性）



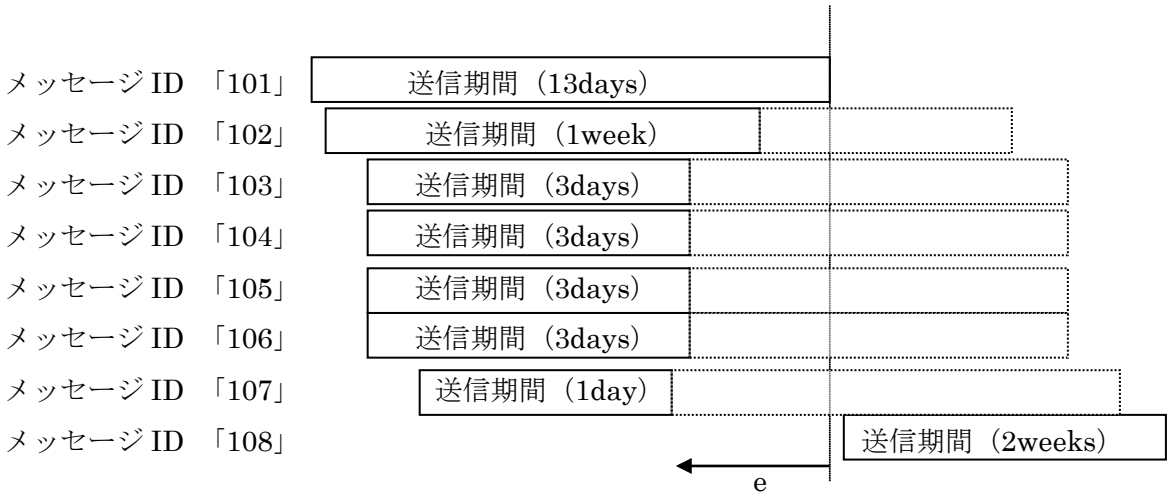
メッセージ ID の単調増加性は確保されない。（メッセージ ID で新旧のメッセージ（メール）の判断はできない。）

(4)送信例４（送信期間１）



メッセージ ID「101」は例えば１週間の送信期間で運用される。当然、d の時間領域でメッセージ ID「108」（８通目のメッセージ/メール）は送信できない。（同時送信メール数７通のルール）

(5)送信例５（送信期間２）



－ メッセージ ID「102」、「103」、「104」、「105」、「106」、「107」についてはメッセージ ID「101」の送信期間内で送信終了することは可能。ただし、受信機側では送信の終了を判定できないので、e の時間領域でメッセージ ID「108」を送信することはできない。（メッセージ（メール）は送信開始時刻の古いメッセージ（メール）から送信を順次終了することを受信側では想定ルール）

4.15 ICカードの録画制御応答

－ 有料放送のコピー制御に関しては本編 5.9 有料放送におけるコピー制御に記載する。地上デジタルテレビジョン放送開始時点では PPV 運用は制限事項であるため、受信機は、IC カードからの録画制御に関する情報を無視する。IC カードからのコピー制御に関する

指定は PPV の録画購入動作であるため、IC カード応答のコピー制御情報が有効になるのは、PPV 運用にあたり本規定改定後に運用された PPV 番組の対応からである。

4.16 CA代替サービス

4.16.1 運用単位

- CA 代替サービスの運用はサービス単位で行う。コンポーネント単位での CA 代替サービスの運用は行わない。
- CA 代替サービスの対象となるリンク元サービスは、スクランブル放送サービス（有料サービス及びコンテンツ保護を伴う無料番組）とする。

4.16.2 リンク先サービス

- リンク先サービスは、有料放送事業者との契約/未契約にかかわらず、必ず視聴できるようにする必要があるため、ノンスクランブルでの運用を必須とする。
- データ放送にリンクした CA 代替サービスを行う場合には、リンク先サービスへのデータコンポーネントの配置を必須とし、CA 代替サービス用のデータコンテンツを必ず伝送する。ただし、リンク先サービスがデータコンポーネントなしの映像サービス又は音声サービスの場合もある。
- リンク先サービスは同一 TS 内で、かつ、 1 service のみとする。

4.16.3 リンク記述子の送出運用

- CA 代替サービスを行う場合、リンク記述子を SDT に配置して送出する。リンク記述子にはリンク先サービスの情報（original_network_id, transport_stream_id, service_id 等）を記述する。
- ノンスクランブル運用しているサービスの SDT にもリンク記述子を配置することがある（スクランブル／ノンスクランブルが混在する放送において、固定的にリンク記述子を運用する場合)。この場合、ノンスクランブル放送で視聴可能であるため、リンク動作は発生しない。
- リンク先サービスに再び CA 代替サービスリンク記述子を配置する運用は禁止する。（リンク動作がループする可能性があるため）
- リンク記述子の private_data_byte の先頭 8bit は、メッセージ番号とする。2 バイト目以降にメッセージ本体を記述する。
- 移動確認メッセージに記述可能な文字数・バイト数は、80 文字かつ 160 バイト以内（メッセージ番号 8bit を含まず）とする。
- 受信機での表示枠などの想定のため、前記に加え 1 行あたりの最大文字数は全角 24 文字まで、表示行数は 6 行以下（改行のみの行を含む）とする。

- 移動確認メッセージに使用できる文字及び制御符号は本書第四編４　文字列の符号化で定義される文字符号および制御符号とする。
- 同一のメッセージ番号を、同一 TS 内で複数の service_id に対し使用する場合は、private_data_byte は、メッセージ番号 8bit のみとすることにより、メッセージ内容の送出を省略することが可能である。
- 同一 TS 内で記載されているメッセージ番号のメッセージ本体は、必ずその TS で送出すること。
- 地上デジタルテレビジョン放送においては同時に送られる移動確認メッセージの種類は、20 種類以下とし、CA 代替用メッセージ番号は 41～60（0x29～0x3C）までとする。
- 受信機内蔵メッセージを表示する場合は、private_data_byte 領域に何も記述しない。
- リンク記述子の運用にあたっては、本書第四編を参照のこと。

4.17　CA_EMM_TS記述子の運用

- 地上デジタルテレビジョン放送においては CA_EMM_TS 記述子の運用は行わない。

4.18　CAサービス記述子

4.18.1 運用

- 自動表示メッセージを運用する事業体の編成チャンネルを示し、当該メッセージの表示制御情報を記述する。
- CAT に複数の CA サービス記述子が記載される場合がある。これは、当該 TS において複数の限定受信方式が運用される場合において、CA サービス記述子で指定された CA_system_id で自動表示メッセージの運用が行われる。また、CA サービス記述子は自動表示メッセージを運用する場合、事業体毎に 1 個を配置する。したがって、CAT に記載可能な CA サービス記述子の個数は複数の限定受信方式が運用される場合、自動表示メッセージが行われる CA_system_id と事業体識別の組み合わせの数だけ記載可能である。

4.18.2 猶予期間の運用

- IC カードに事前に組みこまれている自動表示メッセージが表示されるまでの猶予期間を日単位で示す。ただし、0xFF は猶予期間が伝送されていないことを示す。（猶予期間の保留）
- 起算日は ARIB STD- B25 第 1 部 に記載される「自動表示メッセージ取得コマンド」の現在年月日とする。
- 蓄積機能を有する受信機に対して、受信し蓄積した番組に自動表示メッセージを機能させる場合には、猶予期間の最下位ビットを 0 として運用する。

－　蓄積機能を有する受信機に対して、受信し蓄積した番組に自動表示メッセージを機能させない場合には、猶予期間の最下位ビットを１として運用する。

5　受信機への要求仕様

5.1　受信機の構成

図5-1にCASに関わるハードウェア構成を示す。ここでは、あくまで仕様を説明するためのモデル構成であり、実際の構成は受信機の設計による。

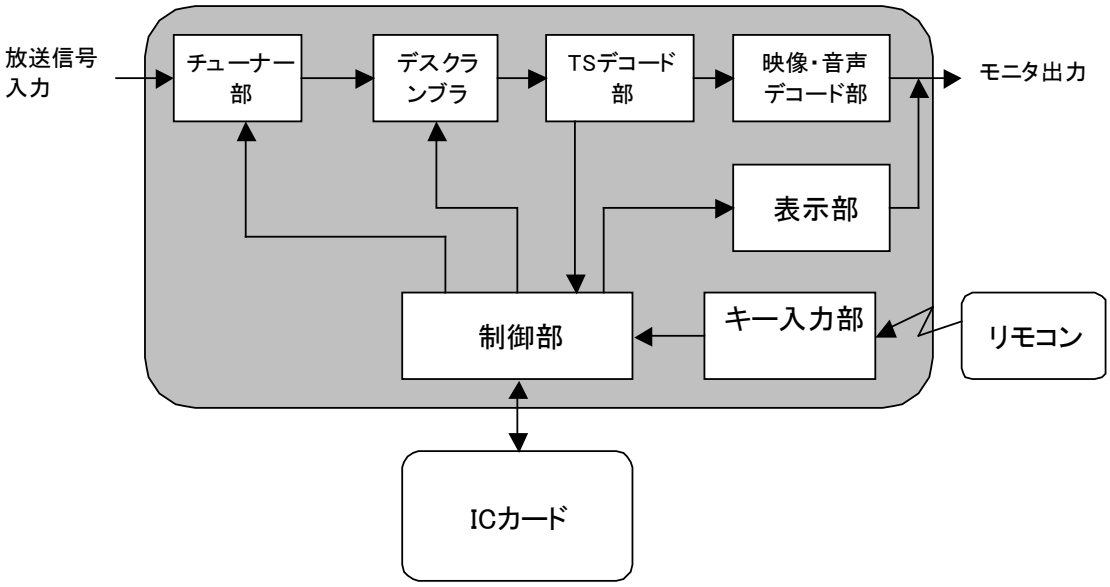


図 5-1　受信機の基本構成

(1)　チューナー部

－　制御部からの制御で放送信号の受信と選択を行い、伝送信号のパケット処理、エラー訂正処理を行う。

(2)　デスクランブラ

－　制御部からの制御で、MULTI2 方式による特定パケットのデスクランブルを行う。

－　ARIB STD-B25 第 1 部の下記を参照。

第 2 章	2.2.2.4	デスクランブラ
第 4 章	4.8	スクランブルの有無の判定
参考 2	3.4	デスクランブラ
参考 2	3.10	ECM の受信とデスクランブラ制御

(3)　TS デコード部

－　TS 多重された信号から必要なパケットを分離し、放送番組信号の選択、各種多重データ（各種 SI データ、ECM、EMM 等）の分離を行う。

(4) 映像音声デコード部

- 映像、音声のデコードを行いモニタに出力する。

(5) 表示部

- ユーザーに対するメニュー、リスト、IC カード情報、自動表示メッセージ、メール、IC カードテスト、IC カード応答時のエラー等を表示するための画面提示手段、ユーザーインタフェースを搭載する。

(6) キー入力部

- リモコンからのキー入力処理を行う。

(7) 制御部

- 受信機全体の制御を行う。特に CAS に関しては、IC カードとの通信、放送信号から分離した各種データの処理、デスクランブラの制御、時刻カウント、表示処理制御、キー入力処理がある。

(8) IC カード、低速 CA インタフェース

- 受信機に装着され、受信機の制御部と通信を行う。受信機の CAS の中核をなす処理として、受信した暗号化 EMM の復号と契約データ管理、暗号化 ECM の復号と有料番組の視聴制御処理、暗号化 EMM メッセージの復号などを行う。
- EMM 受信コマンド、EMM 個別メッセージ受信コマンドについて、自身のカード宛の EMM および EMM 個別メッセージを受信後、30 秒以内に 1 事業体あたり少なくとも 1 個は受信機から IC カードに対してコマンドの発行を行うこと。（本編解説 A.3.6 に関連記載がある。）
- 受信機は複数回のコマンド／レスポンス送受が必要なコマンド（PDU 番号を用いるもの）や通信関連コマンドによる発呼中など、送出順位の決まっているコマンドを発行している場合に ECM 受信コマンド、契約確認コマンド、カード要求コマンド、以外の番組視聴に不要なコマンドを発行してはならない。
- 本書に準拠した受信機は、プリペイドカードは運用上行わないため「前払い残金確認コマンド」を発行してはならない。プリペイドカードに関してはプリペイドカード運用に見合った時期に関連規格の改定を行うものとする。
- ARIB STD-B25 第 1 部の下記に記載される低速 CA インタフェースを搭載すること。

  第 4 章　4.3　CA インタフェース

  参考 2　3.5　IC カードの通信制御

- IC カードの問い合わせ先に関する記載が付録 B.2 にある。

5.2 ユーザーインタフェース

- ユーザーインタフェースの詳細については商品企画による。

  したがって、ARIB STD-B25「第 1 部　第 4 章　受信機に関わる技術仕様」に記載の[手順]に表示されている表示画面は、理解を深めるための一例である。

－　自動表示メッセージはスーパーインポーズ表示を行う。

5.3　メモリ

－　限定受信サービス関連で必要な NVRAM は、下記とする。

1)　メール受信用として、5.6kB 以上とする。内訳は、1 通 800 バイトのメールを 7 通以上記憶するための必要なサイズである。

2)　メッセージ ID 再利用のため 1 事業体あたり、13 個のメッセージ ID と受信時刻の記憶が必要で、32 事業体以上とする。

3)　事業体毎（最大 32 レコード）の通電制御管理やメッセージ ID 再利用のため、受信機における設計次第で追加のメモリが必要となる場合があるが、サイズや実装手段は受信機の任意とする。

－　地上デジタルテレビジョン受信機の譲渡や廃棄の際のために、NVRAM に保持される限定受信関連の個人情報に関して消去機能を持つこと。

具体的には、受信機で記憶する EMM メールの保存領域全てを消去できる機能を持つこと。本書　第二編　6.2.5.7 に関連記載がある。

5.4　省電力化

－　地上デジタルテレビジョン放送限定受信方式では、EMM の更新において省電力化を図るため、通電制御方式を採用する。EMM 通電制御の場合、最初の加入申し込み時は加入したサービス受信中に該当する EMM を受信し、それ以降の EMM 更新時期は IC カードからの応答によって、受信機が次に EMM を受信すべき時期がわかるため、それまでの期間の省エネ設計が可能となる。

－　上記の動作のため、受信機は絶対時刻をカウントする時刻タイマ機能（カレンダ機能）が必要である。詳細については下記を参照のこと。

ARIB STD-B25 第 1 部

参考 2　3.1　　省電力化

参考 2　3.2　　時刻タイマ

5.5　通電制御

5.5.1　ICカード応答等による通常の通電制御

－　本機能は EMM により指定された通電制御期間である時に、サブ電源オフ（AC オフでなくリモコンで電源をオフした状態）でスタンバイ状態となった場合には、少なくとも EMM 受信のための回路通電を行い、指定されたネットワーク及びトランスポートストリームから指定された時刻に EMM を受信するための機能である。

－　通電制御は事業体毎（最大 32 レコード）に設定され、それぞれの通電制御期間が重な

る場合は、全ての事業体について順次受信制御を行う。また、通電制御が中断された場合などでも、毎回特定の事業体に受信制御が集中しないように、全ての事業体について一様にスケジュール管理を行う。

- 通電制御期間中は EMM のみならず、EMM メッセージの取得も行うことが望ましい。
- 有料放送の申し込み時において、放送事業者が EMM 生成する場合の通電制御が行われる TS を特定するため、加入者がどの TS で受信しているかを特定する必要がある。したがって、受信機では受信している TS が特定できるよう現在視聴しているサービスのＴＳ名 10 文字を表示する機能を装備すること。ただし、EPG や番組詳細情報などの表示機能と共用してもよい。
- 通電制御情報要求コマンド／レスポンスによって指定された EMM 受信のための通電期間において、他の待機時における動作との優先順位については本編 5.5.4　待機時における動作の優先順位を参照のこと。
- 通電制御は CA_system_id 毎で管理される。受信機においては、有効な IC カードが挿入され、それ以前に挿入されていた IC カードの CA_system_id と異なる ID のカードであった場合、それ以前の CA_system_id の通電制御データはリセットして構わない。

5.5.2　CA_EMM_TS記述子による通電制御

- 地上デジタルテレビジョン放送においては、CA_EMM_TS 記述子の運用は行わない。

5.5.3　関連規格

- ARIB STD-B25 第 1 部の下記を参照

  参考 1　　4.　　通電制御の運用例

  参考 2　　3.12　通電制御

5.5.4　待機時における動作の優先順位

- 待機時における各種動作が重なった場合の優先順位は下記のとおりとする。

  1)　ユーザーによる各種予約動作（番組予約など）は最優先とする。

  2)　EMM の受信制御、ダウンロードの優先順位は受信機の任意とする。また、ダウンロードにおいて全受信機共通データの場合は、EMM の受信制御を優先とする。
- 特にダウンロードコンテンツの取得においては、取得中に予約動作（予約録画等）の開始時刻になることが予測される場合は、コンテンツの取得を行わないこと。
- 予約動作（予約録画等）が終了した時点で、EMM 取得のための通電期間である、またはダウンロードの配信スケジュールが存在する場合は、EMM またはダウンロードコンテンツの取得動作を行う。

5.6　有効な限定受信方式（ICカードと放送波におけるCA_system_idの整合性確認）

- 複数の限定受信方式が運用される場合があるが、限定受信方式の区別は CA_system_id によって行う。
- 有効な限定受信方式とは、電源オン時、または IC カードの挿入時に IC カードとの初期設定条件コマンド／レスポンスによって得られる CA_system_id と PSI/SI で送られる CA_system_id とが一致したものを有効とする。
- 複数の CA_system_id が CAT や PMT に記載されている場合でも IC カードとのコマンド／レスポンスで得られた CA_system_id と整合した値であれば、本編で定める受信機処理を行う。
- PMT における限定受信方式記述子、および SDT/EIT における CA 契約情報記述子において、IC カードとのコマンド／レスポンスによって得られる CA_system_id と整合しないサービス、または event の場合であっても誤動作を行わないように配慮し、本編　5.15 エラー通知画面　で規定するエラー表示を行うこと。ただし、SDT/EIT においては、コンテンツ保護を伴う無料番組などでは CA 契約情報記述子の記載がないか、または free_CA_mode=0 で運用されるため、放送波と IC カードとの CA_system_id が整合しない場合においても予約可能と判断される場合はエラー表示する必要はない。

5.7　有料番組の視聴制御

5.7.1　視聴処理

- 基本的な動作は、PSI/SI をもとに、選択された番組のトランスポートストリームを選択し、番組を構成するコンポーネントを選択する。
- TS パケットヘッダのスクランブル制御フラグ、アダプテーションフィールドコントロールを参照すると共に、逐次受信した ECM を IC カードに与え、その応答により視聴制御を行う。
- サービスが課金対象である場合でも、スクランブル放送とは限らない。このようなノンスクランブル放送の場合はスクランブルフラグの判定により番組を提示する。
- ECM は当該サービス内でただ 1 つのみ指定され、PMT の第 1 ループに記述される。なお、本運用規定改定後に PPV 運用が開始された場合を想定し、受信機において、PMT の第二ループに第 1 ループに記載された ECM_PID と異なる PID の ECM が記載された場合は、ES 毎別課金の運用が行われた場合とみなし、当該 ES の切り換えができない旨の表示機能など有すること。
- 地上デジタルテレビジョン放送開始時点で、PPV 運用は行わないため、受信機で PPV 機能を実装するべきではない。PPV の運用にあたっては、本運用規定改定後の運用の導入

とする。したがって、放送開始当初の PPV 機能を搭載しない受信機においては、IC カード応答で PPV 関連のリターンコードが返ってきても誤動作を行わないよう配慮すること。

- 地上デジタルテレビジョン放送開始時点において、コンポーネント（ES）毎課金の運用は、現時点では運用しないものと定めるが、将来本規格が改訂され運用される場合を配慮して、PMT 第 2 ループに有効な ECM_PID が記載された限定受信方式記述子が配置されている ES が配置された場合は、PPV 同様非対応の旨のメッセージを表示し、誤動作しないよう配慮すること。

5.7.2 関連規格

- ARIB STD-B25 第 1 部の下記を参照

  第 4 章　4.2.3　番組視聴

  参考 1　6.　スクランブル有無の判定

  参考 2　3.5　IC カードの通信制御

  参考 2　3.10　ECM の受信とデスクランブラ制御

  参考 2　3.15　番組視聴

- 本編 4.送出運用規定

5.8 コンテンツ保護を伴う無料番組、および有料番組の予約

5.8.1 機能概要

- 番組の予約は有料・無料番組の区別なく扱われるべきであり、受信機に番組予約機能が装備されている場合は有料放送もその範囲に含まれることが望ましい。
- 予約する有料番組が視聴可能かどうかは SDT または EIT から CA 契約情報記述子を利用し、IC カードに契約確認コマンド／レスポンスにより視聴の可否、視聴形態を得る。視聴形態はリターンコードによって判断可能である。
- PPV の運用は、地上デジタルテレビジョン放送開始時点では行わない。（本編 A.1.に関連記載がある。）ただし、運用開始を想定し、EIT または SDT に記載された CA 契約情報記述子のカード応答により非対応の限定受信サービス（PPV や、異なる CA_system_id のサービス）と判定された場合は、非対応である旨を表示すること。
- 番組予約において、EIT で free_CA_mode=0 の場合は無条件に予約可能とみなす。（無料番組／コンテンツ保護を伴う無料番組）ただし、コンテンツ保護を伴う無料番組の場合は CA 契約情報記述子の配置は行われないが、番組視聴のためには有効な IC カードの装着が必要であるため、予約時においても IC カード装着の有無を検出し、未装着、または無効な IC カードの場合には有効な IC カードの装着を促すメッセージなどを表示することが望ましい。
- CA 契約情報記述子がない場合で free_CA_mode が 1 の場合は予約不可とする。

- CA 契約情報記述子は SDT ではサービス全体の、EIT では番組毎の契約確認情報を定義する。この記述子が SDT、EIT ともに定義されている場合には EIT での定義が優先される。
- 予約を行う番組で当該 CA 契約情報記述子による IC カードからの応答が非契約の場合で、かつ SDT に当該サービスの CA 代替サービスを目的としたリンク記述子が記述されている場合でも、CA 代替サービスを起動しない。

5.8.2 関連規格

- ARIB STD-B25 第 1 部の下記を参照。

  第 4 章 4.2.4　番組予約

  参考 2　3.16　番組の予約

5.9 有料放送におけるコピー制御

- コピー制御方式については、本書　第八編を参照のこと。
- PSI/SI におけるコピー制御情報については第四編、第八編を参照のこと。
- 地上デジタルテレビジョン放送開始時点においては、PPV の運用は行わないため、限定受信サービスとして IC カードからの応答に関係なく、PSI/SI で指定されるコピー制御に関する制御情報により所定のコピー制御を行うこと。PPV の録画購入動作については、運用に先立ち本運用規定改定後の導入とする。

5.10 自動表示メッセージ表示

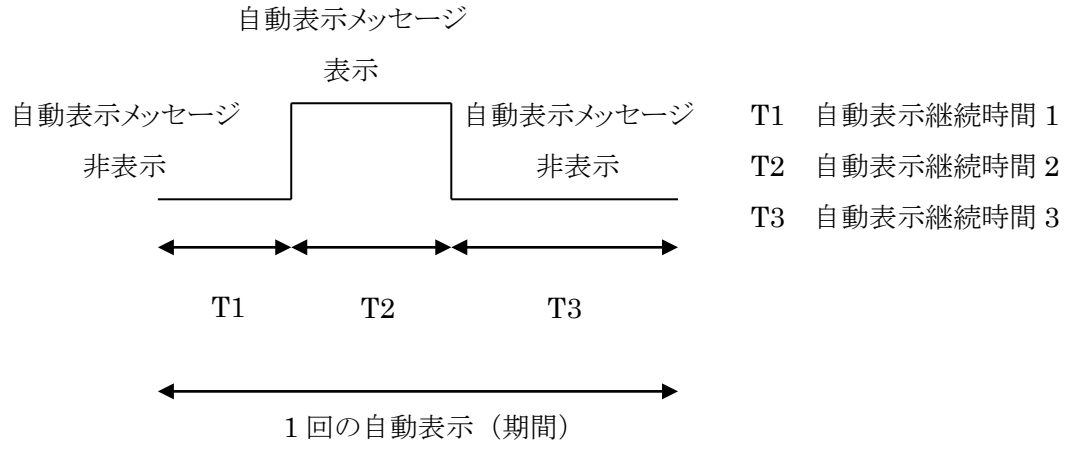
5.10.1 基本動作

- 自動表示メッセージは、各受信機に伝送される EMM 個別メッセージ（IC カード蓄積メッセージ）と、全受信機に共通に伝送される EMM 共通メッセージから得る。EMM 個別メッセージは IC カードに記憶され、EMM 共通メッセージは基本的に表示実行時に受信する。（ただし、蓄積受信機能を有する受信機で受信し蓄積した番組を再生する場合には、再生される信号に含まれる情報あるいは再生時点に当該事業体の放送波で送信されている情報を取得する。）
- 本機能が動作するのは CAT に記載された CA サービス記述子において、IC カード応答によって得られる CA_system_id と CA サービス記述子に記載の CA_system_id とが一致し、かつ選局中の service_id が記載された場合である。
- EMM メッセージでメールか自動表示メッセージかの区別は、EMM 個別メッセージセクションにおいて、メッセージ本体の非暗号化ヘッダのメッセージ制御を参照して行う。そこが「IC カード蓄積(0x01)」である場合が自動表示メッセージに該当するメッセージである。

- 自動表示メッセージの EMM 個別メッセージは、必ず暗号化されており、IC カードで復号を行い、IC カードに記憶される。受信機は装着された IC カードに、EMM 個別メッセージ受信コマンド／レスポンスを用いて、メッセージコード領域を送り、応答メッセージコードを取得する。メッセージコード領域の長さは初期設定条件コマンドで得られるメッセージ分割長よりも短く、分割せずに 1 コマンドで IC カードに送る。
- 自動表示メッセージの場合は、応答メッセージコード領域の最終部分にスタッフィングが存在することがある。受信機は、スタッフィング部分を無視する。
- 応答メッセージコード領域は以下のとおりである。

メッセージコード領域内の項目	説明	bit 数
alternation_detector	改ざんチェック	16
limit_date	有効期限	16
fixed_message_ID	メッセージ定型文番号	16
extra_ message_format_version	差分フォーマット番号	8
extra_message_length	差分情報長	16
extra_message_code	差分情報	N
stuffing	スタッフィング	M

- 受信機は、IC カードに記憶された EMM 個別メッセージ情報を番組選局時に IC カードとの自動表示メッセージ情報取得コマンド／レスポンスにより取得する。
- 受信機は 1 つの CA サービス記述子から 1 つの自動表示メッセージ情報取得コマンドを生成しなければならない。
- 受信機はまず、IC カードから得た EMM 個別メッセージ情報内からメッセージ定型文番号を取得し、対応する EMM 共通メッセージを受信する。次に、その EMM 共通メッセージ情報に EMM 個別情報メッセージ情報の内の差分情報を付加して画面に表示する。（差分情報がない場合もありうる）
- 自動表示メッセージ表示の際、受信機は EMM 共通メッセージ本体部に記載された、自動表示継続時間 1、2、3 に従い、下記のような表示動作を行う。



- 受信機は、上記の表示のオン／オフ制御を EMM 共通メッセージ本体部に記載された自動表示回数分だけ繰り返す。
- 所定の回数を繰り返した後は、表示を消去する。再び選局された場合、受信機は前記の制御を改めて実行する。
- EMM 共通メッセージセクションに記載された 3 種類の自動表示消去種別に対する受信機動作は下記のとおりとする。
  (1)0x00：消去可。前記のメッセージオン／オフ含めた表示期間中において、視聴者の操作によりメッセージを消去可能
  (2)0x01：消去不可。メッセージ表示期間中、視聴者の操作によってメッセージ消去を行ってはならない。
  (3)0x02：表示消去。自動表示メッセージの表示は行わない。自動表示メッセージ表示中の場合に「表示消去」に更新された場合は、メッセージの枠を含めて自動表示メッセージ表示を中止する。
- 視聴者操作による消去の手段は商品企画による。
- CA サービス記述子で送られた猶予期間を IC カードに伝送することにより、自動表示メッセージの表示が開始されるまでの期間が制御される。この場合は、IC カード内でスケジュール管理が行われるため、受信機はこの猶予期間に関するスケジュール管理の必要はなく、IC カードとの自動表示メッセージ情報取得コマンド／レスポンスに従えばよい。
- 自動表示メッセージについて、同一 EMM 個別メッセージの再送チェックは、EMM 個別メッセージセクションに記載されたメッセージ ID と事業体識別とを用いて、同一メッセージの再送チェックを行う。受信機には、直前に受信したメッセージ ID と事業体識別を記憶しておくなど、同一メッセージの再受信を防ぐ仕組みを搭載することが望ましい。
- EMM 共通メッセージのバージョン監視期間は、使用中の EMM 共通メッセージの表示期間（自動表示期間 1～3 の和に自動表示回数を掛けた期間）行う。ただし、自動表示メッセージ種別が 0x02（表示消去）の場合は、常時バージョン監視を行う。
- メッセージコード本体の更新が行われた場合は直ちに反映し表示する。また、更新の際の表示期間のカウントは、更新のあった時点から新たにカウント（リロード）しても、（チャンネル切り換え等による）次の表示期間からカウントしてもどちらでもよいが、できる限り後者が望ましい。
- EMM 共通メッセージのバージョン番号が更新される際に変更される項目は、メッセージコード本体（推奨表示位置情報含む）、自動表示消去種別、自動表示継続時間 1～3、自動表示回数である。

5.10.2 関連規格

詳細に関しては下記を参照のこと。

- ARIB STD-B25 第 1 部
  - 第 3 章 3.2.5　メッセージ情報（EMM/ECM）
  - 第 4 章 4.2.6　自動表示メッセージ
  - 第 4 章 4.3.3　コマンド／レスポンス
  - 第 4 章 4.6　EMM メッセージ表示 (1)自動表示メッセージ表示
  - 第 4 章 4.7.3　EMM メッセージ受信関連
  - 参考 2 3.11　EMM、EMM メッセージの受信

ただし、第1部 参考2　3.11.2 EMM，EMMメッセージの受信形態については、通電制御による受信をサポートすること。

- 本書の下記を参照のこと。
  - 4.11.2　EMM メッセージの送出仕様
  - 4.12　EMM メッセージにおけるメッセージコード
- 第四編　CA サービス記述子

5.10.3 表示について

- 通常状態での番組視聴中の自動表示メッセージ表示機能は必須とする。
- EPG やメニューなどのユーザー操作により一時的に番組映像とブレンド表示する場合のメッセージ表示については商品企画による。この場合 EPG 等の表示を見やすくするために自動表示メッセージ表示を移動するのはかまわないが、通常視聴状態に復帰した場合は、自動表示メッセージ表示も所定の表示動作に復帰すること。
- メニュー等で番組映像とブレンド表示を行わない場合は、自動表示メッセージを表示する必要はない。
- 自動表示メッセージの文字色については、商品企画によるが、必要以上に派手な色を避け、無彩色な色が望ましい。
- メッセージ用画枠についても同様に商品企画によるが、メッセージ文字が読みやすく、また、必要以上に番組の視聴に支障を与えることのないように半透明処理などを施すことが望ましい。
- 文字サイズについては、目安として SD 出力時は 18×18～20×20 ドット程度とする。HD 出力においても画面上で同程度の大きさで見えるようなサイズにて表示すること。ただし、小型画面の受信機などにおいて、EPG や受信機で表示される他のエラーメッセージ等との文字の大きさと比べて著しく小さく視認性を損なう場合は、文字サイズを必要最小限の範囲内で大きくして視認性を確保することが望ましい。

- 前記の目的で文字サイズを大きくしている場合においても、メッセージの文字が読みやすく、かつ番組映像の視認性を確保すること。
- BS デジタルとの共用受信機においては、自動表示メッセージの表示仕様（文字サイズ等）に関しては、BS デジタルでのメッセージ表示仕様に合わせることが望ましい。（表示仕様の優先順位の指定）
- 自動表示メッセージ運用状態において、他のエラーが発生した場合に、複数のメッセージ表示により視聴者に見難い表示を避けるため、自動表示メッセージはデフォルト ES 群が正常にデコードされた状態で表示されることが望ましい。
  例えばコンテンツ保護を伴う無料番組においてデフォルト ES 群がスクランブルされており、自動表示メッセージとの両方が運用されている状態で IC カード未装着のためコンテンツがデコードできない場合は、受信機で実装したカード未装着のエラーを表示し、有効な IC カード挿入後にデスクランブルされ正常にコンテンツが表示された状態になれば、本書規定に沿って自動表示メッセージが表示されることが望ましい。

5.10.4 蓄積機能内蔵受信機での、蓄積した番組を再生する場合の自動表示メッセージ表示

- ここでいう蓄積機能内蔵の定義は記録した機器でのみ再生可能な記録再生機能を持った受信機を意味する。蓄積機能に関する詳細は、本書　第八編を参照のこと。
- 自動表示メッセージを運用する放送事業者の番組を視聴する際には、蓄積機能内蔵受信機に蓄積した番組を再生して視聴する場合にも自動表示メッセージを表示する。このとき、各受信機における自動表示メッセージの表示の制御は、同受信機に装着されている IC カードに記録されている情報（番組再生時の状態）に基づいて行う。
- 蓄積機能内蔵受信機での、蓄積した番組を再生する場合において、蓄積される信号が、サービスタイプに関係なく CAT に記載された CA サービス記述子で、IC カード応答によって得られる CA_system_id と CA サービス記述子に記載の CA_system_id とが一致し、かつ該当のサービスである場合は自動表示メッセージの表示に関する制御を行う。
- 上記の機能を実現するために、自動表示メッセージを運用する放送事業者を受信信号の CAT の CA サービス記述子で確認して、その事業者の番組を記録する際には、同 CAT と同 TS に含まれる EMM 共通メッセージを含めて記録する。この場合、テーブル ID：0x85 で、かつ、table_id_extension≠0x0000（共通メッセージ）でフィルタすることが望ましいが、table_id_extension に関係なく、テーブル ID：0x85（EMM メッセージ）のみでフィルタしてもかまわない。
- 蓄積機能内蔵受信機において自動表示メッセージを運用している事業者の番組をリアルタイムで視聴する場合と、蓄積された番組を再生して視聴する場合で、自動表示メッセージを表示させるか否かを放送局側で制御できる機能を持たせる。

- 記録した番組を再生して視聴する場合、その再生信号の TS から CAT を抽出し、CA サービス記述子が含まれる場合には、猶予期間の最下位ビットを参照して、再生時にも自動表示メッセージを表示するように指定されているかどうか判断する。表示するように指定されている場合（最下位ビット＝0）は、IC カードに「自動表示メッセージ表示情報取得コマンド」を発行し、その応答に基づいて、メッセージ定型文番号を取得し、その定型文番号に対応する再生信号内の EMM 共通メッセージを取得して表示する。表示しないように指定されている場合（最下位ビット＝1）は、IC カードに「自動表示メッセージ表示情報取得コマンド」を発行することなく、メッセージ表示は行わない。
- 表示されるメッセージ文に関しては、記録した番組を再生する場合は、上記のようにデータ放送信号を記録する際に記録された EMM 共通メッセージ文を表示することを基本とするが、リアルタイムの受信機能を並行して持つ受信機では、最新のメッセージ文を表示することも可能とする。
- 再生信号の中に、EMM 及び EMM 個別メッセージが含まれる場合には、これらは無視する。

5.11 メール表示

5.11.1 基本動作

- メールは自動表示メッセージ同様、EMM 個別メッセージ（IRD 蓄積メッセージ）と EMM 共通メッセージとから構成される。
- メールは、自動表示メッセージと異なり、IC カードではなく、受信機に記憶されるメッセージである。
- EMM 個別メッセージは、暗号化する場合としない場合とがあり、EMM 個別メッセージが暗号化されている場合は IC カードで復号を行い、最終的には受信機に記憶する。
- EMM メッセージがメールか自動表示メッセージかの区別は、EMM 個別メッセージセクションにおいて、メッセージ本体の非暗号化ヘッダのメッセージ制御を参照して行う。そこが「IRD 蓄積(0x02)」である場合がメールに該当するメッセージである。
- EMM 個別メッセージが暗号化されている場合、受信機は装着された IC カードに EMM 個別メッセージ受信コマンド／レスポンスを用いて、メッセージコード領域を送り、応答メッセージコードを取得する。メッセージコード領域の長さが初期設定条件コマンドで得られたメッセージ分割長よりも長い場合は、メッセージ分割長ごとに分割しながら順番に IC カードに送る。最終のコマンドでは余った分だけ送る。

- 応答メッセージコード領域の内容は以下のとおりである。

メッセージコード領域内の項目	説明	Bit 数
Reserved	予備	16

Reserved	予備	16
fixed_message_ID	メッセージ定型文番号	16
extra_ message_format_version	差分フォーマット番号	8
extra_message_length	差分情報長	16
extra_message_code	差分情報	N
stuffing	スタッフィング	M*

＊：IRD蓄積メッセージの場合はスタッフィングは送らない（0バイト）。

分割して送った場合は、得られた応答メッセージコードを連結して使用する。
有効な差分情報は差分情報長で示される長さまでである。

- メールの場合は、定型文がある場合とない場合（メッセージ定型文番号＝0）がある。定型文がある場合、受信機はまずメッセージ定型文番号から対応する EMM 共通メッセージを受信する。次に、受信した EMM 共通メッセージ情報と、EMM 個別メッセージの差分情報を組み合わせてメール本文を合成して記憶する。
- 受信機には、少なくとも 7 個のメールを記憶する。記憶先は NVRAM とする。メールは 1 通あたり最大 800byte であるため、メール用のメモリに最小 5.6kB 確保する必要がある。記憶容量を越えるメールを受信した場合は、受信日時の古いものから消去してかまわない。
- メールは 1 通あたり、全角 400 文字以下、かつ 800byte 以下とする。表示方法（1 行あたりの表示文字数や改ページを用いた表示など）については、商品企画による。
- 受信機には、ユーザーに対する「メール受信」を意味する表示機能を装備することが望ましい。「メール受信」とは、未読のメールを記憶している場合である。
- 受信機は、EMM 個別メッセージと EMM 共通メッセージとでメールを構成し、記憶した時点でメール受信が完了したと見なし、前述の通知手段によりユーザーへ通知する。
- メールを記憶したときと異なるカード ID の IC カードが装着されても、受信機は記憶したメールを削除しない。またメールを記憶したときと異なる CA_system_id の IC カードが装着された場合も、同様に受信機は記憶したメールを削除しない。（受信機側に最新メールを 7 個以上記憶する）
- メールを記憶したときと異なるカード ID の IC カードが装着された場合、そのメールの表示処理については商品企画による。処理については下記などが想定される。
  - 例 1： カード ID の違うメールは表示しない。
  - 例 2： カード ID の違うメールは表示しないが、カード ID の異なるメールを蓄積している場合にはその旨をユーザーに知らせる。
  - 例 3： 装着されているカード ID にかかわらず、蓄積されているメールはすべて表示される。
- 既読メールをユーザー操作などで削除するかどうかは、商品企画による。
- メールについて、同一メールの再送チェックは、EMM 個別メッセージセクションに記載されたメッセージ ID と事業体識別とを用いて行う。受信機には、削除したメールを再度取得しないようにするため、内容確認後に削除したメールの識別 ID（メッセージ ID と

事業体識別）を記憶して同一メールの再受信を防ぐ仕組みなどを搭載することが望ましい。なお、受信機は、以前装着されていたICカードと異なるCA_system_idのICカードが装着された場合、記憶しているメールの識別ID（メッセージIDと事業体識別）などのメッセージID管理データをリセットしても構わない。

- 受信メールをタイトルとして使用する場合は、先頭の10文字程度以上を使用する。
- メールの表示については商品企画によるが、ユーザーが読みやすいサイズで画面中央に表示することが望ましい。
- 本書　付録　B　B.1に関連記載がある。

5.11.2 関連規格

- ARIB STD-B25 第1部の下記を参照。

  第4章　4.2.9　　メール表示

  第4章　4.6　　EMMメッセージ表示 (2)メール表示

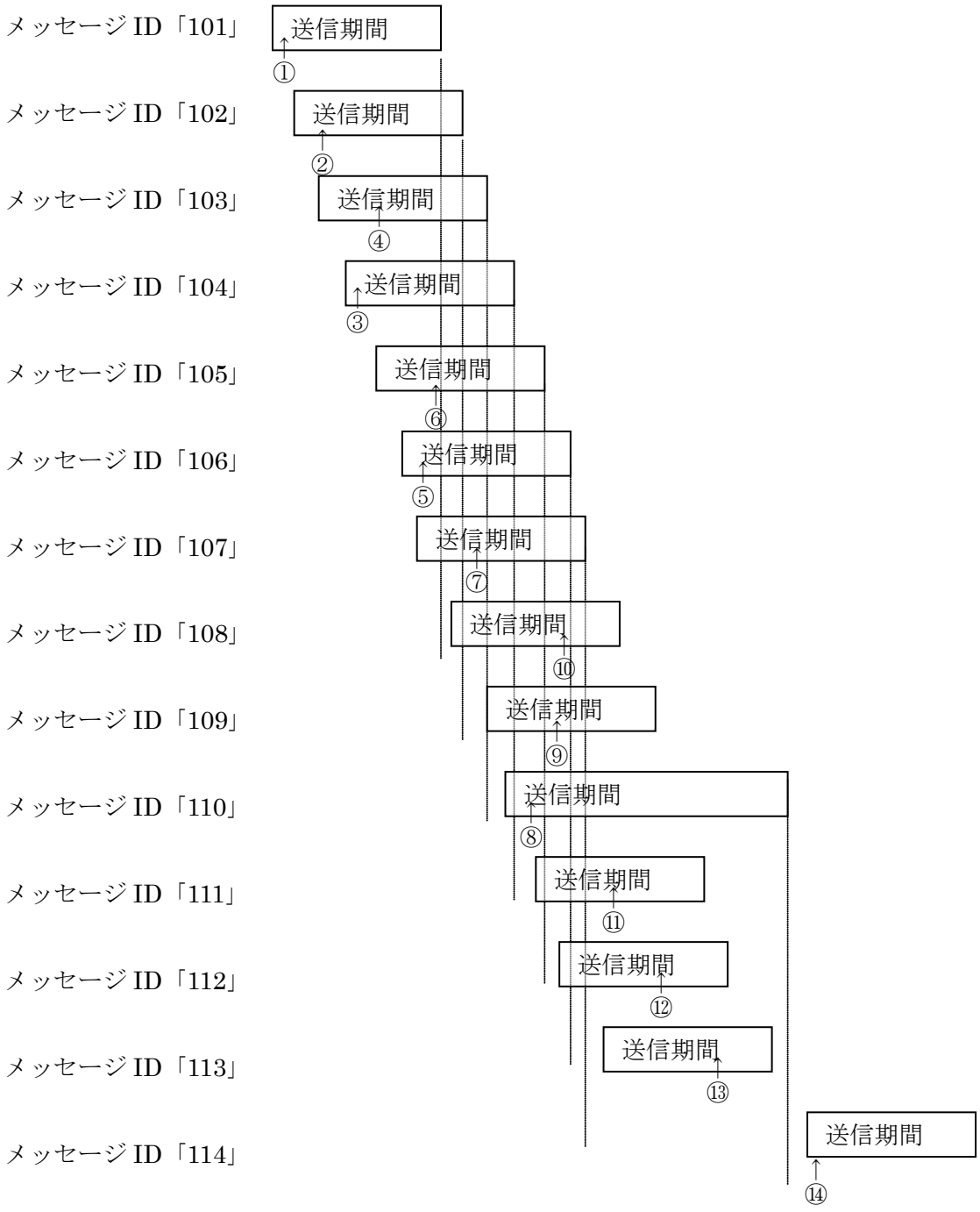
  参考2　3.11　　EMM、EMMメッセージの受信

ただし、第1部 参考2　3.11.2　EMM、EMMメッセージの受信形態において、通電制御による受信をサポートすること。

5.11.3 メッセージID処理

- 受信機はメッセージID、受信時刻を格納するエリアを事業体別に１３個用意する。
  （13個は2N-1個の領域の確保。N：事業体が同時に送信できるメッセージ数）
- 受信時刻が１４日を経過したエリアについては、送信期間終了として、内容を削除する。
- 13個のエリアの情報が全て満たされ、かつ14個目の新メッセージ（メール）を受信した場合には、一番古い時刻のエリアにメッセージID、受信時刻を上書きする。

以下に送信期間と受信機動作例を示す。


メッセージ ID「101」
送信期間
①
メッセージ ID「102」
送信期間
②
メッセージ ID「103」
送信期間
④
メッセージ ID「104」
送信期間
③
メッセージ ID「105」
送信期間
⑥
メッセージ ID「106」
送信期間
⑤
メッセージ ID「107」
送信期間
⑦
メッセージ ID「108」
送信期間
⑩
メッセージ ID「109」
送信期間
⑨
メッセージ ID「110」
送信期間
⑧
メッセージ ID「111」
送信期間
⑪
メッセージ ID「112」
送信期間
⑫
メッセージ ID「113」
送信期間
⑬
メッセージ ID「114」
送信期間
⑭

受信機動作

■　時刻①

メッセージ ID 101 受信 1 番目のエリアにメッセージ ID101 と受信時刻①を格納。

■　時刻②

メッセージ ID 102 受信 2 番目のエリアにメッセージ ID102 と受信時刻②を格納。

■　時刻③

メッセージ ID 104 受信 3 番目のエリアにメッセージ ID104 と受信時刻③を格納。

■　時刻④

メッセージ ID 103 受信 4 番目のエリアにメッセージ ID103 と受信時刻④を格納。

■　時刻⑤

メッセージ ID 106 受信 5 番目のエリアにメッセージ ID106 と受信時刻⑤を格納。

■　時刻⑥

メッセージ ID 105 受信 6 番目のエリアにメッセージ ID105 と受信時刻⑥を格納。

■　時刻⑦

メッセージ ID 107 受信 7 番目のエリアにメッセージ ID107 と受信時刻⑦を格納。

■　時刻⑧

メッセージ ID 110 受信 8 番目のエリアにメッセージ ID110 と受信時刻⑧を格納。

■　時刻⑨

メッセージ ID 109 受信 9 番目のエリアにメッセージ ID109 と受信時刻⑨を格納。

■　時刻⑩

メッセージ ID 108 受信 10 番目のエリアにメッセージ ID108 と受信時刻⑩を格納。

■　時刻⑪

メッセージ ID 111 受信 11 番目のエリアにメッセージ ID111 と受信時刻⑪を格納。

■　時刻⑫

メッセージ ID 112 受信 12 番目のエリアにメッセージ ID112 と受信時刻⑫を格納。

■　時刻⑬

メッセージ ID 113 受信 13 番目のエリアにメッセージ ID113 と受信時刻⑬を格納。

■　時刻⑭

メッセージ ID 114 受信 1 番目のエリアにメッセージ ID114 と受信時刻⑭を格納。

（時刻①が最も古い受信時刻。時刻①から⑭までの経過時間が 14 日以内の場合の動作。）

5.12　パレンタルコントロール（視聴年齢制限）

地上デジタルテレビジョン放送においては、パレンタルコントロール機能は運用しない。

5.13 ICカードの有効／無効／使用不可について

5.13.1 有効なICカード

- 有効な IC カードとは、以下の全ての条件を満たすものとする。
  (1) ARIB STD-B25 第 1 部初期設定条件コマンドで正常なレスポンス（正常終了）を得るもの。
  (2) 初期条件コマンド／レスポンスで system_management_id が 0x0301 または 0x0201 を含むもの。
  (3) 初期条件コマンド／レスポンスでカード種別が 0x01 のもの。

5.13.2 無効なICカード

- 無効な IC カードとは、本編 5.13.1 に記載の有効な IC カードの条件を満たさないものとする。
- 受信中の番組がスクランブルの場合、無効な IC カードの場合は、本編 5.15 エラー通知画面に記載のエラーメッセージを表示する。
- 受信中の番組がノンスクランブルで CAT に記載の CA サービス記述子において選局中の service_id が記載されている場合、IC カードが無効の場合は、本編 5.16 有効な IC カードが挿入されていない場合の動作に記載の動作を行う。

5.13.3 使用不可のカード

- 使用不可のカードとは無効なカードと区別するため有効な IC カードであっても故障などで使用不可となったカードを意味し、本編 5.13.1 で規定する有効な IC カードであってもリターンコードが A1FF、A102 のものとする。
- 受信中の番組がスクランブル放送の場合、使用不可の場合は、本編 5.15 エラー通知画面に記載のエラーメッセージを表示する。
- 受信中の番組がノンスクランブルで CAT に記載の CA サービス記述子において選局中の service_id が記載されている場合、使用不可のカードである場合は、本編 5.15 エラー通知画面に記載のエラーメッセージを表示する。

5.14 ICカード情報の表示

5.14.1 機能概要

- 本機能は、加入申し込みや種々の限定受信サービスについてカスタマーセンターなどに問い合わせる際に、メニュー等のユーザー操作によって IC カード情報を表示するための機能である。
- ユーザー操作により、カード識別、カード ID を表示する。

- 各々の統一名称もカード識別、カード ID とする。ユーザーインタフェースは商品企画によるが、各々の表示番号と統一名称との対応が明確になるよう配慮すること。
- グループ ID の運用は行わないため、グループ ID の表示は考慮しなくてよい。（カード識別およびカード ID は表示すること）
- IC カード情報の表示については、本編解説 A.8 に関連記載がある。

5.14.2 関連規格

ARIB STD-B25 「第 1 部　第 4 章　4.2.10 カード情報の表示」を参照。

5.15 エラー通知画面

5.15.1 機能概要

- CAS 関連におけるエラー通知には下記表に示した種類がある。
  表中において対応リターンコード、SW1/SW2 を記載しているものは、エラーメッセージにカードからのリターンコードまたは SW1/SW2 を 16 進表示で「コード：＊＊＊＊」を記載する。（＊＊＊＊は IC カードからのリターンコードまたは SW1/SW2）
- エラーメッセージは基本的に商品企画によるが、カスタマーセンターなどでの判定のため下記例を参照することとし、表示例に従うことが望ましい。また、カスタマーセンターから別途エラーメッセージ表示例が通知される場合もある。表中の表示例の空欄については商品企画による。

No	エラー分類	対応リターンコード	SW1/SW2	表示例
1	パスワード不一致			
2	IC カード未装着			例 1 注 1
3	使用不可 IC カード装着通知	A1FF, A102		例 2
4	非契約（Kw なし）	A103		例 3
5	非契約（契約外）	8901,8501,8301		例 4
6	非契約（期限切れ）	8902,8502,8302		例 5
7	非契約（視聴制限）	8903,8503,8303		例 6
8	購入期間外購入不可通知画面	8108		例 7
9	データ満杯購入不可通知画面	8109		例 8
10	通信失敗の通知	9103,9104,9105,9106		
11	IC カード交換		6400,6581	例 9
12	その他のエラー	A104,A105, A106,A107		例 10
13	無効な IC カード装着通知			例 11
14	CA_system_id の不整合			例 12

注1：ICカード未装着時におけるエラーメッセージ表示については、本編　5.16　有効なICカードが挿入されていない場合の動作を参照のこと。

注2：本表にないエラーコードの扱いについて
本表にない下記のエラーコードは、放送局や受信機の障害によって発生するエラーや、通常の運用でも発生するコード（エラー扱いしてはならないもの）である。これらは視聴者のオペレーションとは

無関係であるため、視聴者に対するエラーコード・エラーメッセージの表示は行わない。

(1)受信機の障害によるプロトコル違反と考えられるもの

（コード）SW1/SW2＝6700、6800、6A86、6D00、6E00（全て規格外コマンド）

（受信機での対応）エラーコード・エラーメッセージは表示しない

(2)予約によるPPV自動購入で発生するエラー

（コード）8141　PPV番組番号不一致（視聴不可）

4040　PPV番組番号不一致（視聴可）

（発生理由）　予約によるPPV自動購入時に、前の番組が延長されたなどの理由で、予約購入しようとする番組と実際に放送されている番組が一致していない。
視聴不可と視聴可は、放送中の番組を視聴できるか否かの状態を示す。

（受信機での対応）　受信機は、契約確認コマンドで得られる予約購入期限までの範囲で、「購入済：後払いPPV」の応答が返るまでPPV番組購入コマンドを発行してリトライする。予約購入期限を過ぎても本コードが返る場合には、リトライを中止しPPV自動購入失敗となる。
リトライ中のエラーメッセージ表示は不要。最終的に自動購入動作が失敗した場合は何らかの提示が必要と思われるが、その方法は商品企画による。

(3)該当データがないことを示すエラー

（コード）A101　該当データなし

（発生理由）　自動表示メッセージ表示情報取得コマンド、発呼日時要求コマンド、通電制御情報要求コマンドに対し、応答すべき該当データがカード内部に存在しない。
それらの情報が存在するかしないかは局の運用や個人の契約状態によって異なるため、存在しなくても決してエラーではない。

（受信機での対応）　エラーコード・エラーメッセージは表示しない

(4)その他のエラー

（コード）A1FE　その他のエラー

（発生理由）　放送局や受信機の障害による規約違反などで発生する

（受信機での対応）　エラーコード・エラーメッセージは表示しないこと。ただし、ＥＣＭ受信コマンド、ＰＰＶ番組購入コマンドなどＩＣカードからＫｓが返送されるコマンドで当該エラーコードが発生した場合を除く。
また、ICカードからＫｓが返送されるコマンドで当該エラーが発生した場合、デスクランブルエラーとなる。この場合のエラー表示に関しては商品企画マターとするが、参考例として以下に示す。

［エラー表示例］
スクランブル解除のための情報にエラーが発生しています。
ご覧のチャンネルのカスタマーセンターへご連絡ください。
コード：Ａ１ＦＥ

(5)発呼不可

（コード）11FF　発呼不可

（発生理由）　ICカード指示の「リトライオーバ通知」受けずに、受信機側から「ユーザ発呼要求コマンド」をICカードに与えた。

（受信機での対応）　エラーコード・エラーメッセージは表示しない。

例 1：IC カード未装着（スクランブル放送受信時の場合）

IC カードを正しく装着してください。

例 2： 使用不可 IC カード装着

（IC カードの有効／無効／使用不可については本編　5.13　IC カードの有効／無効／使用不可についてを参照のこと）

この IC カードは使用できません。

ご覧のチャンネルのカスタマーセンターへご連絡ください。

コード：＊＊＊＊

例 3：非契約（Kw なし）

- ケース１：IC カード応答が A103 であって、選局中の番組の限定受信方式記述子に記載の CA_system_id と ECM に記載の事業体識別が、本書　第八編に記載のコンテンツ保護のための無料番組で使用される事業体識別以外の場合（有料番組の場合）

  このチャンネルは契約されていません。

  ご覧のチャンネルのカスタマーセンターへご連絡ください。

  コード：＊＊＊＊

- ケース２：IC カード応答が A103 であって、選局中の番組の限定受信方式記述子に記載の CA_system_id と ECM に記載の事業体識別が、第八編に記載のコンテンツ保護のための無料番組で使用される値の場合（コンテンツ保護のための無料番組の場合）

  この IC カードには必要な情報がありません。

  ご覧のチャンネルのカスタマーセンターへご連絡ください。

  コード：＊＊＊＊

例 4：非契約（契約外）

このチャンネルはご覧いただけません。

ご覧のチャンネルのカスタマーセンターへご連絡ください。

コード：＊＊＊＊

例 5：非契約（期限切れ）

契約期限が切れています。

ご覧のチャンネルのカスタマーセンターへご連絡ください。

コード：＊＊＊＊

例 6：非契約（視聴制限）

このチャンネルは視聴条件により、ご覧いただけません。

ご覧のチャンネルのカスタマーセンターへご連絡ください。

コード：＊＊＊＊

例 7：購入期間外購入不可通知画面

受け付け時間を過ぎていますので購入できません。

コード：＊＊＊＊

例 8：データ満杯購入不可通知画面

電話回線を接続のうえ、ご覧のチャンネルのカスタマーセンターへご連絡ください。

コード：＊＊＊＊

例 9：IC カード交換

IC カードの交換が必要です。

ご覧のチャンネルのカスタマーセンターへご連絡ください。

コード：＊＊＊＊

例 10：その他のエラー

この IC カードは使用できません。

ご覧のチャンネルのカスタマーセンターへご連絡ください。

コード：＊＊＊＊

例 11：無効な IC カード（スクランブル放送受信の場合）

（IC カードの有効／無効／使用不可については本編　5.13　IC カードの有効／無効／使用不可についてを参照のこと）

この IC カードは使用できません。

正しい IC カードを装着してください。

コード：EC01

（例 11 におけるコードはカードリターンコードではなく、上述のエラーコードを表示する。）

例 12：　CA_system_id の不整合場合

（CA_system_id の整合性の判定については、本書 5.6 を参照のこと）

この IC カードではご覧になることができません。

ご覧のチャンネルのカスタマーセンターへご連絡ください。

コード：EC02

（例 12 におけるコードはカードリターンコードではなく、上述のエラーコードを表示する。）

5.15.2 関連規格

- ARIB STD-B25 「第 1 部　第 4 章　4.2.5 エラー通知画面」を参照。
- 統一エラーメッセージに関しては第二編を参照。

5.16　有効なICカードが挿入されていない場合の動作

5.16.1 有効なICカード未装着時のエラーメッセージ表示方法

- 選択した番組がスクランブル放送であり、受信機でカード未装着を検出した場合は、カード装着を促すメッセージを表示する。メッセージ表示については本編 5.15 エラー通知画面を参照のこと。

- 以下は、選択した番組がノンスクランブル放送の場合に、IC カードが未装着の場合、または装着された IC カードが無効な IC カードであった場合に表示が必要となるエラーメッセージ表示について述べる。
- この場合のエラーメッセージは、自動表示メッセージ表示の手法を以下のように用いて表示するものとする。

5.16.1.1 エラーメッセージを表示する条件

- IC カードが未装着の場合、または装着された IC カードが無効な IC カードの場合。
- CAT に記載された CA サービス記述子において、選局中の service_id が記載されている場合。
- 電源オン時、チャンネル変更時において表示を行う。

5.16.1.2 表示方法

- EMM 共通メッセージの取得に関して、IC カードが装着されていない場合、下記に記載したデフォルトメッセージコードの CA_system_id を用いて該当する EMM メッセージを取得すること。
- 当該のサービスにおいて、対応する EMM 個別メッセージでデフォルトメッセージを定義する。すなわち受信機は CA サービス記述子の事業体識別に対し、EMM 個別メッセージ受信コマンドを IC カードに発行し、IC カードより下記のメッセージコードを得たものとして処理する。
- デフォルトのメッセージコードは以下の通りとする。

  有効期限：0xFFFF

  メッセージ定型文番号：上位バイトを当該の事業体識別、下位バイトを 0x01

  差分フォーマット番号：0x01

  差分情報：0x00（情報なし）

  CA_system_id ：本書第七編を参照のこと
- 文字色や画枠色に付いては 本編 5.10 自動表示メッセージ表示の場合と同様に、必要以上に派手な色を使わず、番組の視聴に支障を与えないよう配慮すること。
- 表示のオン／オフ制御やその他の表示要領については、本編 5.10 自動表示メッセージ表示の場合と同様である。
- ノンスクランブル放送時において番組映像が提示可能な場合には、本エラーメッセージを視聴画面にスーパーインポーズで表示すること。

5.16.2 送信側におけるICカード未装着時のための定型文の条件

- 定型文番号 ：上位バイトを当該の事業体識別、下位バイトを 0x01

5.16.3 その他

- ARIB STD-B25 「第 1 部　第 4 章　4.2.2 電源オン」を参照。
- アナログ VTR への出力映像に本メッセージを表示するかどうかは規定しない。

5.17　システムテスト

5.17.1 ICカードテスト

- IC カードテストを行うためのユーザーインタフェースを持つこと。
- 本機能は、IC カードテストの結果を通知する。
- IC カードテストの成功は、少なくとも初期設定条件コマンドにより正常終了することとする。

5.18　CA代替サービス

5.18.1 機能概要

- 視聴者がスクランブル放送サービス（有料チャンネル及びコンテンツ保護を伴う無料番組。以下、リンク元サービス）を選局した時、以下の条件のいずれかにあてはまった場合に当該放送事業者が運営しているチャンネル（以下、リンク先サービス）に誘導する機能である。

  (1)有料放送事業者との契約が締結されていない。

  (2)選局したチャンネルを運営している有料放送事業者と契約しているが、選局したチャンネルは未契約である。
- CA 代替サービスを行うチャンネルは、SDT に配置する linkage_type=”0x03”のリンク記述子の有無によって識別される。リンク記述子が記載されている場合のみ、CA 代替サービスを起動する。
- CA 代替サービスを起動する場合は、リンク先サービスに移動するかどうか視聴者に確認を求め、視聴者が許可した場合にリンク先サービスへ移動する。
- リンク先サービスはプロモーション用の「ご案内チャンネル」であり、データ放送を利用したオンライン契約なども想定されている。
- 本機能を取扱説明書などでユーザーへ説明する場合の機能名称は「ご案内チャンネル切り換え機能」とする。

5.18.2 基本動作

－ リンク先サービスが補完データ放送付きサービスの場合の CA 代替サービス処理フローを以下に示す。なおリンク先サービスへ移動後のフロー（⑥⑦⑧）は一例である。

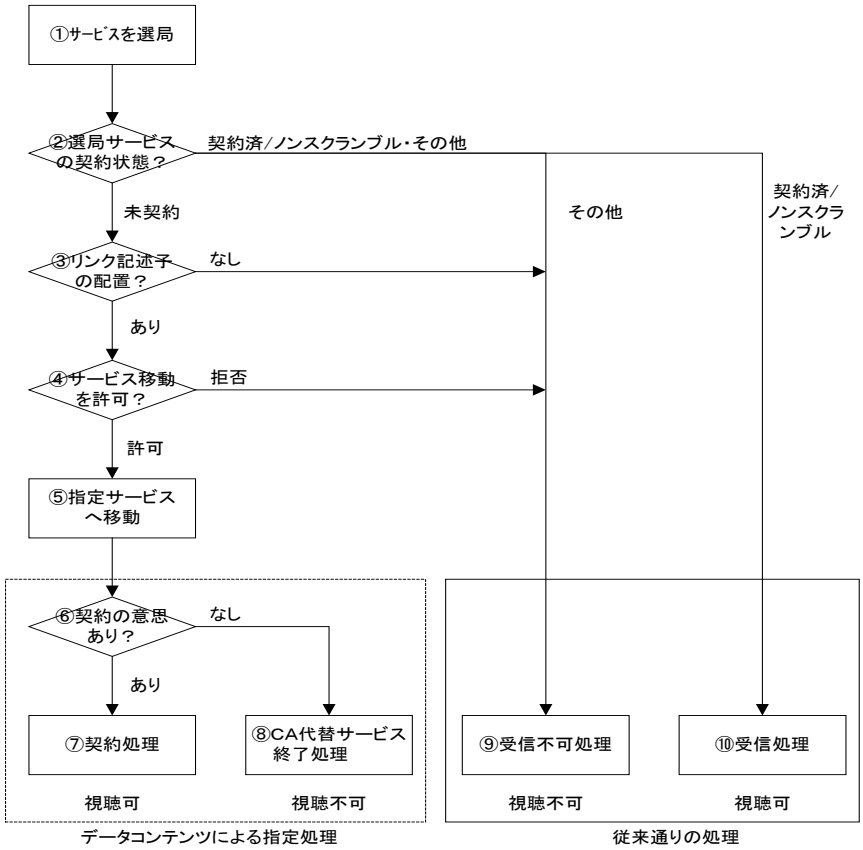


図 5-2　CA 代替サービスの処理フロー例

①視聴者が当該チャンネル（サービス）を選局する。

②通常の選局動作と同様に ECM より契約状態を確認する。

1)　未契約の場合、CA 代替サービス処理（③～）

未契約とは、受信した番組がスクランブル放送で、ECM 受信コマンドに対する IC カードからのリターンコードが次表にあてはまる場合のことをいう。

表 5-1　未契約の場合のリターンコード

リターンコード	状態詳細
A103	非契約（Kw なし）
8901	非契約（契約外；ティア）
8902	非契約（期限切れ；ティア）
8301	非契約（契約外；後払い PPV）
8302	非契約（期限切れ；後払い PPV）
8501	非契約（契約外；前払い PPV）
8502	非契約（期限切れ；前払い PPV）

IC カードが未挿入の場合や無効／使用不可のカードが挿入されている場合、当該番組の PMT に記載されている CA_system_id と IC カードからの応答で得られる CA_system_id とが一致しない場合は、未契約と判断せずに通常エラー処理を行う。

2) 契約済／ノンスクランブル・その他の場合、従来通りの受信処理（⑩）又は受信不可処理（⑨）。

③ SDT のリンク記述子配置の有無を確認する。

1) リンク記述子が配置されている場合、サービス移動意思確認処理（④）

2) リンク記述子が配置されていない場合、従来通りの受信不可処理（⑨）

注：linkage_type=0x03 のリンク記述子が CA 代替サービスを示す。

④ リンク記述子に記述されている事業者固有の移動確認メッセージ（以下、移動確認メッセージ）又は受信機内蔵メッセージを表示し、視聴者のリンク先サービスへの移動の許諾と意思確認を行う。移動確認メッセージはリンク記述子の private_data_byte に記述される。CA 代替サービスのリンク記述子の private_data_byte に記述がない場合は、受信機内蔵メッセージ（「この番組をご覧いただくには契約・登録が必要です。詳細はご案内チャンネルの中でご紹介しています。」）を表示する。

1) 視聴者がリンク先サービスへの移動を許可した場合、サービスの移動処理（⑤）

2) 視聴者がリンク先サービスへの移動を拒否した場合、従来通りの受信不可処理（⑨）

注：
－当該画面を抜ける選択肢（移動拒否）を用意する場合は、通常の未契約処理とする。
－当該画面を抜ける選択肢（移動拒否）がない場合は、その画面でステイすることも可。
（視聴者の選局動作によって当該画面から抜ける）

3) CA 代替サービスの送出側の仕様で、受信中の TS の SDT では、複数の移動確認メッセージ番号（以下、メッセージ番号）が運用される場合、メッセージ本体は少なくともその TS では１つ以上送られるが、同一メッセージ本体を省略することも可能である。その場合は、同一メッセージ番号の本体の表示を参照して表示を行うこと。例外処理として、同一 TS 内でメッセージ本体が定義されていない場合は、受信機内蔵のメッセージを表示する。

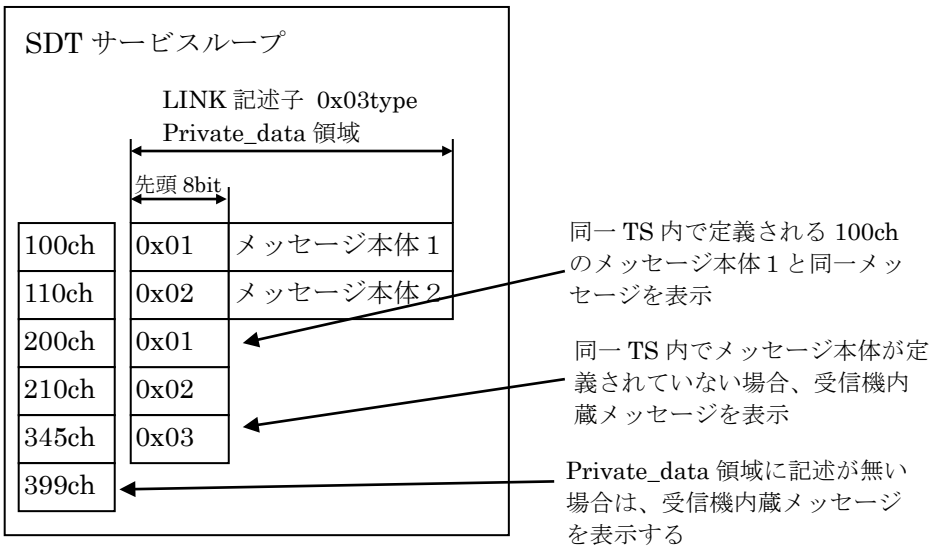
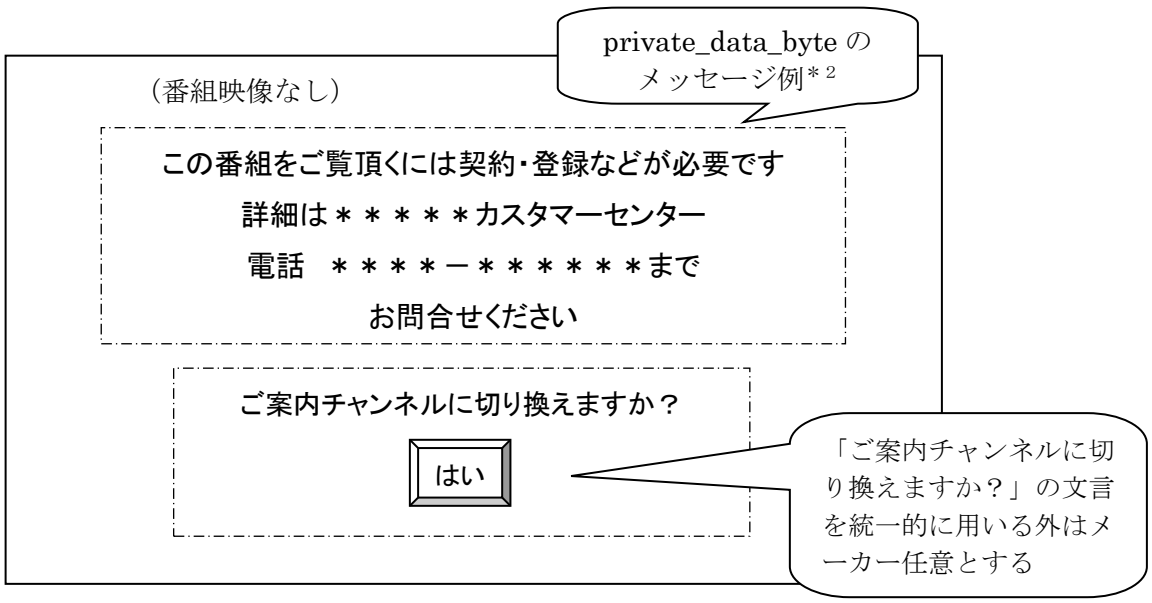


図 5-3　CA 代替サービスの運用と受信機処理の例

4)移動確認メッセージは、80 文字かつ 160 バイト以下である。また、表示仕様として 1 行あたり最大 24 文字、表示行数は 6 行以下（改行含む）を想定する。

5)リンク記述子が配置されている場合、リンク記述子の private_data 領域に記載されたメッセージ（あるいは受信機内蔵メッセージ）以外に、下記例のように移動確認の画面を表示すること。ここで表示する文面は予め受信機に内蔵され、内容は「ご案内チャンネルに切り換えますか？」とする。表示枠などの表示方法に関しては、商品企画による。

下記に移動確認画面の例を示す。



（注*1）　CA 代替サービス機能を取扱説明書などでユーザーへ説明する場合は「ご案内チャンネル切り換え機能」とする。

（注*2）　private_data_byte に記述が無い場合は「この番組をご覧いただくには契約・登録が必要です。詳細はご案内チャンネルの中でご紹介しています。」との受信機内蔵メッセージを表示。

図 5-4　CA 代替サービス*1移動確認画面の例

⑤ SDT のリンク記述子より、リンク先サービス情報を取得し、サービスを移動する。リンク記述子の original_network_id/ transport_stream_id/ service_id に従い、リンク先サービスへ移動させる。

＜データコンテンツによる指定処理の例⑥⑦⑧＞

⑥ リンク先サービスの番組内で契約の意思確認を行う。意思確認方法は有料放送事業者によって異なる。

1)契約意思がある場合、契約処理（⑦）

2)契約意思がない場合、CA 代替サービス終了処理（⑧）

⑦ 視聴者との契約処理を行う。契約処理は、データ放送等を利用したオンライン処理や契約書の送付等のオフライン処理等、有料放送事業者毎に異なる。処理終了後もリンク元サービスへは復帰しない。

⑧ CA 代替サービスの終了処理を行う。処理終了後もリンク元サービスへは復帰しない。

＜従来通りの処理⑨⑩＞

⑨ 通常の受信不可動作と同様にサービスの受信不可処理を行う。

⑩ 通常の受信動作と同様に選局サービスの受信処理を行う。

- 受信機は、視聴者がダイレクト又は EPG 又はアップダウンキーにより未契約サービスを選局した場合に CA 代替サービスを起動して移動確認画面を表示する。ただし、以下の条件にあてはまる場合は、CA 代替サービスを起動しない。

  1)視聴者が有料放送事業者と契約済である。（上記②で示した未契約以外の場合）

  2)視聴者の選局したサービスがノンスクランブルで運用されている。

  3)リンク先サービスのサービス形式種別（service_type）が受信機未対応の場合。

  4)受信機が選局対象としていないサービス(例えば受信対象としていないネットワーク内サービス等)がリンク指定されている場合

- 未契約の有料放送サービスを予約しようとした場合など、予約設定時のサービスについては CA 代替サービスを起動しない。
- SDT は PMT に比べて送信周期が長いため、SDT を受信してリンク記述子の有無を確認して移動確認画面を表示するまでに時間がかかることが予想される。そのため、当該サービスを選局後、受信機内蔵の非契約メッセージが一瞬表示された後に移動確認画面に切り替わるような動作もありうる。そうした動作が、選局する度に起こることを避けるため、受信機は SDT を RAM にキャッシュしておき、当該サービスの選局後は直ちに移動確認画面を表示することが望ましい。
- 地上デジタルテレビジョン放送においては同時に送られる CA 代替メッセージの種類は、20 種類とし、CA 代替用メッセージ番号は 41～60（0x29～0x3C）までとする。もし、この番号以外の CA 代替用メッセージ番号が送られてきた場合、受信機はそのメッセージを無効とし、受信機内蔵のメッセージを表示する。
- CA 代替サービスによりリンク先サービスに移動した後（上記の⑦又⑧）の終了処理後は、リンク元サービスに復帰せずにリンク先サービスを選局した状態のままにする。また、リンク先サービスがデータコンポーネントなしの映像サービス又は音声サービスの場合においても、リンク元サービスに復帰せずにリンク先サービスを選局した状態のままにする。視聴者の選局動作によって他へ移動する。
- 移動確認画面の表示条件が成立して一度表示した後は、ユーザーが確認動作を行うまで消去する必要はない。表示中に表示条件が不成立に変化した場合でも、自動消去する必要はなく、表示したままで構わない。ただし、その場合はリンク条件が生きており、ユーザーがリンク先へ移動許可を行えば、リンク先へ移動すること。
- リンク先サービスが補完データ付きサービスの場合に、データコンテンツ上でリンク記述子によるリンク元サービスの取得及びリンク記述子によるリンク時のリンク種別の取得

を可能とする。これらの、BML 文書に対する DOMAPI については ARIB STD-B24 を参照のこと。

5.18.3 関連規格

- ARIB STD-B10 の下記を参照

  第 2 部　　6.1　　識別子の識別と配置

  　　6.2.8　　リンク記述子

- ARIB STD-B24 の下記を参照

  第二編　　第 7 章　　手続き記述言語

- ARIB STD-B25 第 1 部の下記を参照

  第 2 章　2.2.2.15 番組の選択視聴

  第 4 章　4.2.3　　番組視聴

  参考 2　3.15　　番組視聴

5.19　字幕・文字スーパーのスクランブルと表示優先順位

5.19.1 字幕

- デフォルト ES 群がスクランブル状態における字幕の表示に関しては、基本的に受信機商品企画とする。ガイドラインとして、字幕コンポーネントのスクランブル状態に関係なく、字幕表示が有効となる場合は、デフォルト ES 群が正常にデスクランブルされた場合にのみ表示されることが望ましい。

5.19.2 文字スーパー

- デフォルト ES 群がスクランブル状態における文字スーパーの表示に関しては、基本的に受信機商品企画とする。

5.20　部分受信階層における有料放送非対応機器の動作

5.20.1 PMTで限定受信方式記述子を検出した場合の動作

- 限定受信非対応の部分受信専用受信機において、PMT 第 1 ループに限定受信方式記述子が配置された有料放送を受信した場合、非対応である旨の以下に示すエラーメッセージ（例）を表示し、誤動作等起こさないよう設計すること。ただし、PMT に限定受信方式記述子が配置された場合であってノンスクランブルで放送されている場合のコンテンツの提示については商品企画マターとする。

- 有料放送　非対応メッセージ

  ご覧の番組は有料放送で、受信できません。

  エラーコード：EC03

- 部分受信階層における有料サービスが、本編で規定する ARIB STD-B25 第一部に準拠した限定受信方式とは限らず、運用開始時点で規定されるため、部分受信階層の放送開始当初における限定受信非対応受信機においては、有料放送方式機能を搭載する必要はない。

A 解説

A.1 地上デジタルテレビジョン放送の放送開始時点の限定受信方式仕様について

A.1.1 ARIB STD-B25 第1部からの運用制限について

地上デジタルテレビジョン放送ではARIB STD-B25第1部に記載の機能から、放送開始時点において運用予定がないことから、一部の機能制限を行った。

まず、機能制限を行ったものは、PPVの運用、ES毎別課金、IRDデータ伝送機能である。これらの機能について、将来に渡って一切の運用を否定しているのではなく、運用の開始にあたっては、その時点での環境状況に合わせて最適な運用方式を導入するという観点から、運用開始前に本規定を見直し、その後に導入することとした。放送開始時点に発売される受信機では前記の制限された機能が搭載される必要はないが、新たに運用開始される時点で、誤動作を起こさないよう放送開始当初から配慮されることを目的に運用開始時のPPVの識別手段など文中に記載した。

また、運用予定が無いグループIDについては、2013年12月のTR-B14 5.4版改定において、運用は行わないこととした。グループIDの表示に関しては、本編解説A.8に関連記載がある。

A.1.2 複数限定受信方式の運用について

地上デジタルテレビジョン放送のコンテンツ保護について本書では、ARIB STD-B25第1部準拠の限定受信方式を利用した方式を規定したが、将来において、これよりもコンテンツ保護に適したコンテンツ保護専用方式が登場した場合に、それを導入できるように複数の限定受信方式を運用可能な規定とした。規定の記載にあたっては、コンテンツ保護専用方式導入時に複数の限定受信方式記述子を運用しても、放送開始当初の受信機でも誤動作をおこさないために記載する目的を主として、コンテンツ保護専用方式に関する規定は、今後の検討結果次第であるため、記載せず複数の限定受信方式記述子、CAサービス記述子がCAT、PMTに配置可能な旨を規定した。

放送開始時点で販売される受信機においては、ARIB STD-B25第1部準拠の限定受信方式のみが搭載されることが想定される。将来において、コンテンツ保護専用方式の導入が行われる場合、この受信機においてもコンテンツ保護を目的とした無料番組の視聴を可能とするため下記の運用イメージのように、ARIB STD-B25第1部準拠のECMとコンテンツ保護専用方式準拠のECMの両方で同一のKsの伝送を行う運用としなければならない。

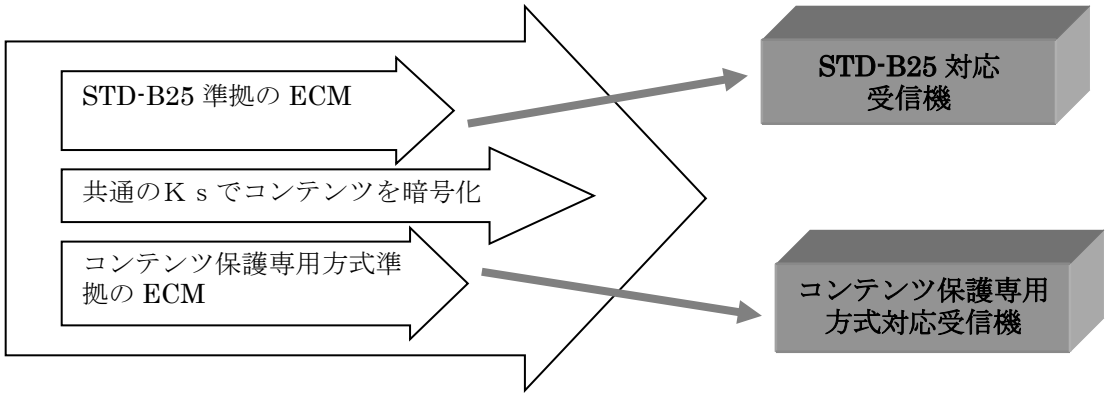


図 A-1　コンテンツ保護目的で複数の限定受信方式を運用した場合のイメージ

今回規定した複数の限定受信方式の運用の可能性は図 A-1 で示したようなコンテンツ保護目的に限定されず、例えば同一 TS 内において、番組毎や、チャンネル（service_id）毎で異なる有料のための限定受信方式運用を否定しているわけでなく、このような運用が行われた場合においても、受信機に搭載されていない限定受信方式のサービスでは、非対応である旨のメッセージを表示することで誤動作することなく処理されることを想定して規定した。

A.1.3　STD-B25 第1部準拠方式という考え方について（想定）

本書では、前述したように地上デジタルテレビジョン放送の放送開始当初において複数の限定受信方式が運用されることを想定していない。本書は、将来コンテンツ保護を伴うスクランブル放送の運用を、地上デジタルテレビジョン放送開始当初とは異なる別の方式で運用したいという機運が高まった場合に、可能な限りそれまでに流布した受信機が混乱なく使用され続けることを意図している。

ここで、放送におけるコンテンツ保護方式、限定受信方式、ARIB STD-B25第1部準拠方式、そして運用パラメータであるCA_system_idの関係を明確にしておくことは、上記の機運が発生した場合にきわめて重要であるので、本書が想定した考え方を以下に記述する。

［放送におけるコンテンツ保護方式］

コンテンツは視聴者に提示されないと意味がない性質ものであるから、受信機内では必ず平文として扱われる。したがって、この平文たるコンテンツをコンテンツ自身で保護する手段は存在せず、あくまで受信機がこれを保護するように機能することが期待される。放送におけるコンテンツ保護方式とは、このような受信機の機能の具備を法的手段に訴えることなく、技術

的手段を用いて契約的に行うことのできる方式である。したがって限定受信方式といった枠に拘束されないものである。

ここで、本編に記載する「放送におけるコンテンツ保護方式」と第八編における「記録におけるコンテンツ保護方式」との用語の使い方の違いは、コンテンツを保護するために暗号など利用してコンテンツの改ざんや不正コピー防止する技術を広義にコンテンツ保護方式として、放送波におけるコンテンツ保護方式、ここでは限定受信方式をその目的に利用しているが、「放送におけるコンテンツ保護方式」と称し、リムーバブルメディアなどに記録する際のコンテンツ保護方式を「記録におけるコンテンツ保護方式」として区別した。

［限定受信方式］

日本のデジタル放送における限定受信方式は、その基本形式が省令の形で定められている。その基本要素を列挙すると以下のとおりである

a) コンテンツはMULTI2と呼ばれる暗号方式によって、TSレベルでスクランブルされる。
b) スクランブルを解除する鍵はECMと呼ばれるテーブルで暗号化されて送出される。
c) ECMの暗号を解くための鍵はワーク鍵とよばれ、受信者別の識別子をもつEMMと呼ばれるテーブルで暗号化されて送出される。
d) 受信者別の識別子をもつEMMは、受信機内の受信者別の暗号鍵で復号される。
e) CATと呼ばれるテーブルは限定受信方式記述子をもち、この記述子は具体的な限定受信方式を示すCA_system_idとEMMが送出されるPIDを明らかにする。
f) PMTと呼ばれるテーブルも同じく限定受信方式記述子をもち、この記述子は具体的な限定受信方式を示すCA_system_id と、ECMとデスクランブルすべきES_PIDの関係を明らかにする。

限定受信方式とは上記の基本的な構成に基づくものである。

［ARIB STD-B25 第1部準拠方式］

省令に示される限定受信方式を、より具体的な方式にまとめられたものがARIB STD-B25 第1部であるが、関連情報に対する暗号方式が特定されていないこともあり、個別の限定受信方式を示すものではない。したがって限定受信方式の集合体である。しかしながらARIB規格は時代の推移によって改定されてゆくものであるから、何をもってARIB STD-B25 第1部準拠方式かをあらためて整理しておく必要がある。本書では、将来STD-B25 第1部が改定されても決して変わることのない部分は何かを以下の点であると想定した。

a) 省令が示す限定受信方式に該当する部分
b) セキュリティモジュールとして、電気的にISO7816に準拠したICカードを用いた低速インタフェース方式であること
c) ICカードのコマンド/レスポンスのうち現行の初期設定コマンドに完全準拠するもの

［CA_system_id］

個別の限定受信方式を示す識別子である。

（図A-2における限定受信方式の範囲での識別子）

上記の4つの概念と、将来導入されるかもしれない、放送におけるコンテンツ保護方式の関係を図A-2　に示す。

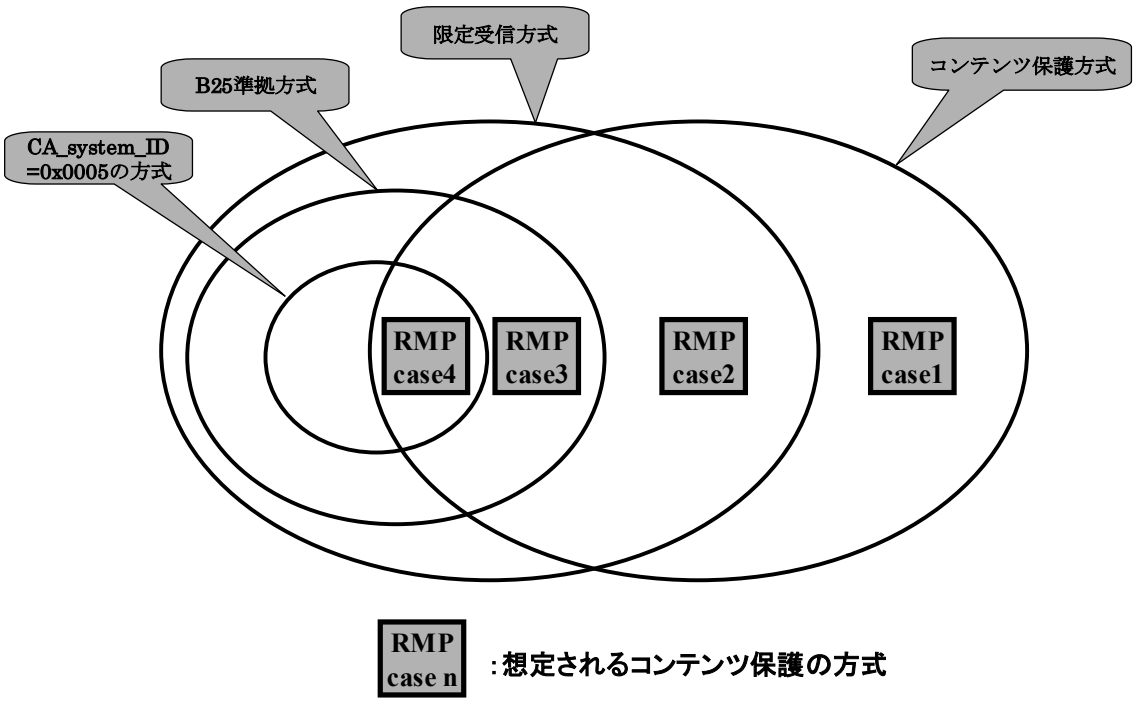


図 A-2　可能性のある放送におけるコンテンツ保護方式の位置づけ

本書では、将来策定されるかもしれない放送におけるコンテンツ保護方式を上記4つの場合に分類・想定し、各場合において、それまでに流布した受信機が可能な限り問題なく使用され続けるように、運用規格を策定した。

case1：これは、まったく未知の方式であり現時点でその備えをすることは不可能であり、また省令・ARIB規格の根本的策定を伴うものである。さらに本書の役割である限定受信方式の運用規格の範疇を超えるものである。したがって、このようなケースにおいては、それまでに流布した受信機が可能な限り問題なく使用され続けるようにするために、新たな規格の策定がその責務を負わねばならないと考える。

case2：この場合は、複数の限定受信方式が存在することになるので、その事が受信機の誤動作につながることのないように本書で規格化する。この場合はその方式の登場に際して新たな追加規格が策定されねばならない。

case3：この場合は、case2と同様に複数の限定受信方式が存在することになるので、その事が受信機の誤動作につながることのないように規格化する。本書では、この場合にはその方式の登場に際して新たな規格の策定が不要であるように配慮した。
この場合に備えて、本書ではCA_system_idの具体的な番号の指定は行っていない。

case4：この場合は、地上デジタルテレビジョン放送のコンテンツ保護の方式が、BS/広帯域CSデジタル放送におけるコンテンツ保護と同様の運用をされることを意味し、特に大きな技術的懸念要素はない。

以上、地上デジタルテレビジョン放送の限定受信方式の運用規定を策定するに当たり、将来の放送におけるコンテンツ保護方式が新たに策定されるための備えとして検討した基本的考え方を述べるものである。

A.1.4　有効なICカードについて

本項は、1.3版改定時にそれまでTBD事項であった5.13章を明確化するにあたり解説として記載した。

まず、本編では、限定受信方式を識別するものがCA_system_idであるとした。そこで、複数限定受信方式の運用にあたってCA_system_idの扱いを以下のように考えた。

受信機に有効なICカードが装着され、有効な限定受信方式であれば、CA_system_idの値に関わらず、本書に規定した限定受信放送サービスの機能が動作することが可能であるように規定した。

ここで、有効なICカードとは、STD-B25 第1部(4.0版)準拠のカードであるとした。したがってICカードの形態をなさないものは対象とせず、ARIB規格などの改定・整備とともに規定することとした。また、STD-B25 第1部準拠の考え方にあたっては、ECMを受信しカード応答でKsを正常に得られるものという考え方もあったが、ECMを受信しない電源オン時やカード装着時に有効・無効の判定が行えるように初期設定条件コマンド／レスポンスにより有効を判断する基準とした。

有効なカード条件の一つであるsystem_management_idに関しては、本来限定受信方式の内容とは無関係な値であり。有効な条件から外す考えもあったが、TR-B15との整合性を鑑み地

上デジタルテレビジョン放送でのsystem_management_idを含むもの、および、放送開始時点で運用されるCA_system_id=0x0005との整合性を加味してTR-B15に記載される0x0201を含むものを有効とした。

カード種別については、本編A.2でも述べたように例えば受信機とICカードの相互認証機能を搭載した場合、本書1.3版対応受信機との互換性がないため、そのカードではカード種別が0x01以外で運用され、受信機で互換性のないカードを判定できるように想定した。

また、有効な限定受信方式は本文で述べたように有効なICカードと放送波のCA_system_idとが一致したサービスが有効な限定受信方式として特にCA_system_idの値自身によらない規定とした。これにより上記の条件を満たしたものであれば、CA_system_id=0x0005以外の限定受信方式でも有料放送などが可能である規定である。

A.2 相互認証機能

本書1.0版において、本編5.6章には相互認証機能（TBD）を記載していた。相互認証機能は、コンテンツ保護目的で限定受信方式を使用する場合、本来の限定受信サービス目的である視聴者個人を認証する機能ではなく、コンテンツ保護では規定のエンフォースを行うため受信機を認証すべき機能であることから導入を検討していた。

相互認証については、A.1.2で述べたコンテンツ保護専用方式と同様、方式開発、契約スキームなどの整備が必須であり、放送開始時点の受信機に間に合わせるのが日程的に困難であるため、放送開始時点では、相互認証機能なしのARIB STD-B25 第1部準拠の限定受信方式搭載仕様とした。

相互認証機能についてもコンテンツ保護専用方式と併せ検討をすすめ、詳細が決定した時点で必要に応じ、運用規定の改定を行う必要がある。

本書　1.1版では、かかる事情により、本編　5.6章を相互認証機能から、複数限定受信方式運用でのための「有効な限定受信方式の判定」に変更した。

A.3 EMMについて

A.3.1 地上デジタルテレビジョン放送におけるEMM伝送TSについて

BSや広帯域CSではEMMを伝送するTSとして、各事業者の番組用TSの他に、複数の事業者で特定のTSを共有し、その特定TSをEMM伝送用の専用TSとする方法が想定されている。

地上波においては、ネットワークIDは送信マスター単位に付与され、さらに国内の全てのネットワークを受信できないことから、複数の事業者で特定のTSを共有する運用は難しい。このため地上デジタルテレビジョン放送では、EMMは全て番組用TSで送り、専用TSでは送らない運用とした。

A.3.2　部分受信階層におけるEMM送出について（T.B.D.）

A.3.3　通電制御機能のユーザーへの通知について

本限定受信方式で省電力設計が可能となるように通電制御や通電発呼制御を運用することは、既に本文で述べたとおりである。この方式では受信機が内部タイマでEMM受信を管理する必要があるため、機能を維持できるようユーザーに対して通知することが望ましい。つまり、EMM受信モード以外での待機時電力の省エネ化に努めると共に、待機時にEMM受信制御が確実に受信されるよう取扱説明書などで、ユーザーに対して

- 受信機の待機時は省エネ設計になっていること
- 限定受信サービスを受けるときには個別情報（EMM）の受信制御のため、緊急時や旅行などの長期不在時等を除き、電源はリモコンでオフすることを推奨する

など通知することが望ましい。

A.3.4　EMMメッセージ

(1)　フォーマット作成経緯

EMMメッセージのフォーマットに関しては、ARIB STD-B25 第1部で定められておらず、補足するため本編で規格化した。以下に経緯を記載する。

EMMメッセージにはメールと自動表示メッセージがあるが、表示のフォームに関しては、前者は受信機仕様で特に問題ないが、後者は画面に重畳されるメッセージであることから、表示位置を概略でも位置制御可能とするための制御コードを定義した。CAS専用でなんらかの文字を表示する為の機能を規定するのではなく、受信機が搭載する字幕などの手段の流用も検討したが、字幕とは異なり、メッセージが提示される映像フォーマットが特定できないなどの理由から、本編で記載したような概略の位置指定を行い、詳細は受信機の裁量にゆだねるという形態のフォーマット規定とした。

自動表示メッセージとしての最大文字数に関しては、ARIB STD-B25 第1部では、最大400バイトとの記載があるが、検討段階において、受信機で搭載される文字サイズの想定や、上中下左右などの位置制御が効果的に見えることなどの配慮から、文字数、行数制限を加える形で規定した。また、画枠に関しては、他の字幕などとの区別のため画枠を用い少しでも映像を見えるようにするため、画枠サイズは、伝送する1行あたりの最大文字数と行数とから、受信機側で最適化することとした。

(2)　メッセージ ID の事業体識別あたりの同時送信可能な個数（N）について

1事業体が同時に送信できるメッセージ数は、ARIB TR-B15（2.0版）ではBSデジタル放送ではN=4通、広帯域CSデジタル放送ではN=7通である。地上デジタルテレビジョン放送受信機では、これらBSデジタル放送や広帯域CSデジタル放送との共用機を想定した場合に、事業体機器別の値では、BSデジタル放送か、地上デジタルテレビジョン放送かの判定はできない

ため、数の多い数値を採用することによりこれらの共用受信機でも受信機内部での混乱がおきないように、N=7とした。

A.3.5　EMM送出仕様　TypeAとTypeBについて

・EMM送出仕様としてTypeAとTypeBの２種類が定義されている。BSデジタル放送においてはTypeAのみが使用され、広帯域CSデジタル放送と地上デジタルテレビジョン放送においては両方が使用可能である。

・TypeAはEMMの伝送効率を主眼においた伝送方法である。1セクション（最大4096バイト）に複数のEMMを詰め込んで送るため、セクション形式のオーバヘッド（ヘッダとCRC誤り検出の計12バイト）を最小にでき、伝送効率はよい。しかしながら、受信機で自分宛のEMMだけを抜き出すフィルタリング処理がソフト処理とならざるをえず、受信機にCPU負荷がかからないようにEMM伝送速度の上限は320kbit/sに制限される（番組用TSで送る場合）。

・TypeBはEMMの大容量伝送を主眼においた伝送方法である。1セクションで1EMMを送るため、TypeAに比べてセクション形式のオーバヘッドは大きくなる。（ただしマルチセクション形式が可能で、1TSパケットの中に複数のセクションを詰め込んで送ることができる。）しかし受信機はフィルタリング処理をハードウェアで行うことが可能となり、EMM伝送速度の上限は2.0Mbit/sまで上げることができる。
なお受信機のハードフィルタを前提としているが、フィルタ資源を節約するためにカードIDを一種類に絞る必要があり、グループIDの運用は禁止されている。

・EMMの大きさは契約内容やCA方式によって異なるが、例えば一律40バイトと想定して両仕様を比較すると次のような違いになる。

（TypeAの場合）

－　１セクション（4092byte）＝ヘッダ(8)＋EMM(40)×102 個＋CRC 誤り検出(4)。
オーバヘッドの割合＝12／4092＝0.29%。

－　１秒間で伝送可能な EMM 数＝約 900 個[*1]（320kbit/s の伝送時）

（TypeBの場合）

－　１セクション（52byte）＝ヘッダ(8)＋EMM(40)×1 個＋CRC 誤り検出(4)。
オーバヘッドの割合＝12／52＝23%。

－　１秒間で伝送可能な EMM 数＝約 4700 個[*2]。（2Mbit/s の伝送時）

・当初はBSデジタル放送の運用規格としてTypeAだけが標準化されていた。広帯域CSデジタル放送の規格策定にあたり、CS放送では契約変更が頻繁に発生し、大量のEMMを送る必要があるという特質を考慮して、TypeBの仕様が追加されたものである。
送るべきEMMの数、割り当て可能なEMM伝送容量などは事業者の運用によって異なるため、事業者ごと（正確にはTS単位）にTypeAとTypeBの送り方を選択できる。

注*1（TypeAの場合）
・１セクション（102EMM）の伝送に必要なTS数＝4092／184＝23個。
・最大320kbit/sを割り当てた場合に１秒間で送ることができるEMM数
＝320kbit／（188×23×8bit）×102＝943個。
注*2（TypeBの場合）
・最大2.0Mbit/sを割り当てた場合に１秒間で送ることができるEMM数
＝（2.0Mbit×184／188）／（52×8bit）＝4705個。
なお、セクションヘッダ(8)＋カードID(6)の計14バイトが複数のTSパケットに跨るマルチセクション運用は禁止されているため、実際にはもう少し少なくなる。

A.3.6　EMM関連コマンドの処理に関して

ECM関連コマンドは、デスクランブル処理を行うためKs更新周期に応じてリアルタイム処理を行う必要がある。一方、視聴者からの有料放送加入申込みや、自動表示メッセージ消去などに対応するために、ECM関連コマンドに比べ必ずしもリアルタイム処理を必要としないものの、EMM関連コマンドも速やかにICカードへの処理が行われることが前提である。

EMM関連コマンドの遅延許容時間値は、規定がなかったことによりEMM関連コマンドの処理を無制限に遅延させる可能性を排除し、受信機実装／送信側運用の自由度を確保しつつ、複数のEMMが交錯した場合を想定して設定した。したがって、意図的に受信側で遅延許容時間を消費させるといった受信機実装を全く期待していないことに留意されたい。

A.4　ECMの運用について

A.4.1　再送周期

ECMの再送周期については本編4.10.5.2　更新・再送周期に、許される最大値としては本編4.10.6.2　ECMの途絶に記載されている。

具体的には、

100ms≦ECM再送周期＜2秒

である。

ECM再送周期は「チャンネル選択時のコンテンツ提示までの時間」を定義してしまうので、短いほうが望ましい。そこで部分受信階層以外では

ECM再送周期約100ms

で運用される。（部分受信階層におけるECMの運用に関してはTBD）

ただし、受信機として、ECM再送周期を100ms～1000ms程度の範囲内を想定して設計を進めることを推奨する。

A.4.2　更新周期

ECMの更新周期に関しては、本編4.10.5 ECMの更新・再送に記載されている。ICカードの処理能力に応じたタイミングとしては、

- 1 ECM の処理に最大 800ms を想定
- 異なる ECM の更新間隔は 1000ms 以上

という前提のもと、受信機仕様を想定している。また、更新周期を 2 秒以上としたのは下記の想定である。

- 地上放送を TV 画面で見ながら地上裏番組録画が 1 枚の IC カードで処理できる。
- 同様のことが任意の地上チャンネル 2 画面同時表示も IC カードとして 1 枚で処理。

以上のことから、ECMの更新間隔が2000ms以上であれば、異なるTSにおける少なくとも任意の2つのスクランブルサービスが1枚のICカードで処理可能になる。

- また、スクランブルのセキュリティ確保の観点から更新周期に関しても標準的推奨値を記載した。

A.4.3　PMT更新時のESとECMの関係について

A.4.3.1　背景・経緯

地上デジタルテレビジョン放送では、幅広い放送事業者がスクランブル放送を行うことが予想される。このため、スクランブル放送を行うために必要とされる放送用送出システムは、有料放送の様々な課金形態に対応する高度で複雑なものより、運用のための負荷が小さく容易に導入できるようなシステムに対する要求がより重要と考え、PMT更新時のスクランブル／ノンスクランブルの状態制御を極力簡略化できるような運用規定とした。

A.4.3.2　PMT更新時に想定される放送信号の状態と受信機動作について

PMTを更新する要因を主に限定受信システムの観点から、以下のように分類して考えた。

a)　ノンスクランブル放送からスクランブル放送に切り替わる場合。
b)　スクランブル放送からノンスクランブル放送に切り替わる場合。
c)　ECM_PID が変更される場合。
d)　ES の PID が変更される場合。
e)　新規 ES が追加される場合。
f)　ES が消滅する場合。
g)　ES 数の増減、ES PID の変更、ECM_PID の変更、スクランブル有無の状態の変化などの意図がない場合。

上記項目a)～g)のうち、a)、b)については、スクランブル／ノンスクランブルの状態制御そのものが目的のため、それぞれ本編 4.10.4.1 スクランブルの開始、4.10.4.2 スクランブルの終了 の手順に従うこととした。

PMT更新の要因としてc)が含まれる場合については、ECM_PIDの切り替え前後における送出側でのスクランブル鍵の制御がスクランブル状態を継続したままでは困難であるとの認識から、本編 4.10.4.3 放送番組要素を伝送するESとECMとの関係の変更 (1) ECM_PIDの変更を伴う場合 に示したような手順に従うこととした。

PMT更新の要因としてa)～c)のいずれも含まれない場合（すなわち、d)～g)各々あるいはそれらを組み合わせた場合）については、コンポーネント課金の運用制限によりPMT更新時の受信機の処理負担が軽減されることから、受信機開発においても特別な負担が生じること無くスクランブル状態の継続に対応することが可能であると考えた。（本編 4.10.4.3 放送番組要素を伝送するESとECMとの関係の変更 (2) ECM_PIDの変更を伴わない場合参照）

一例として、HD番組からSD番組(3ch)への切り替え時に想定される放送信号と受信機動作について説明する。

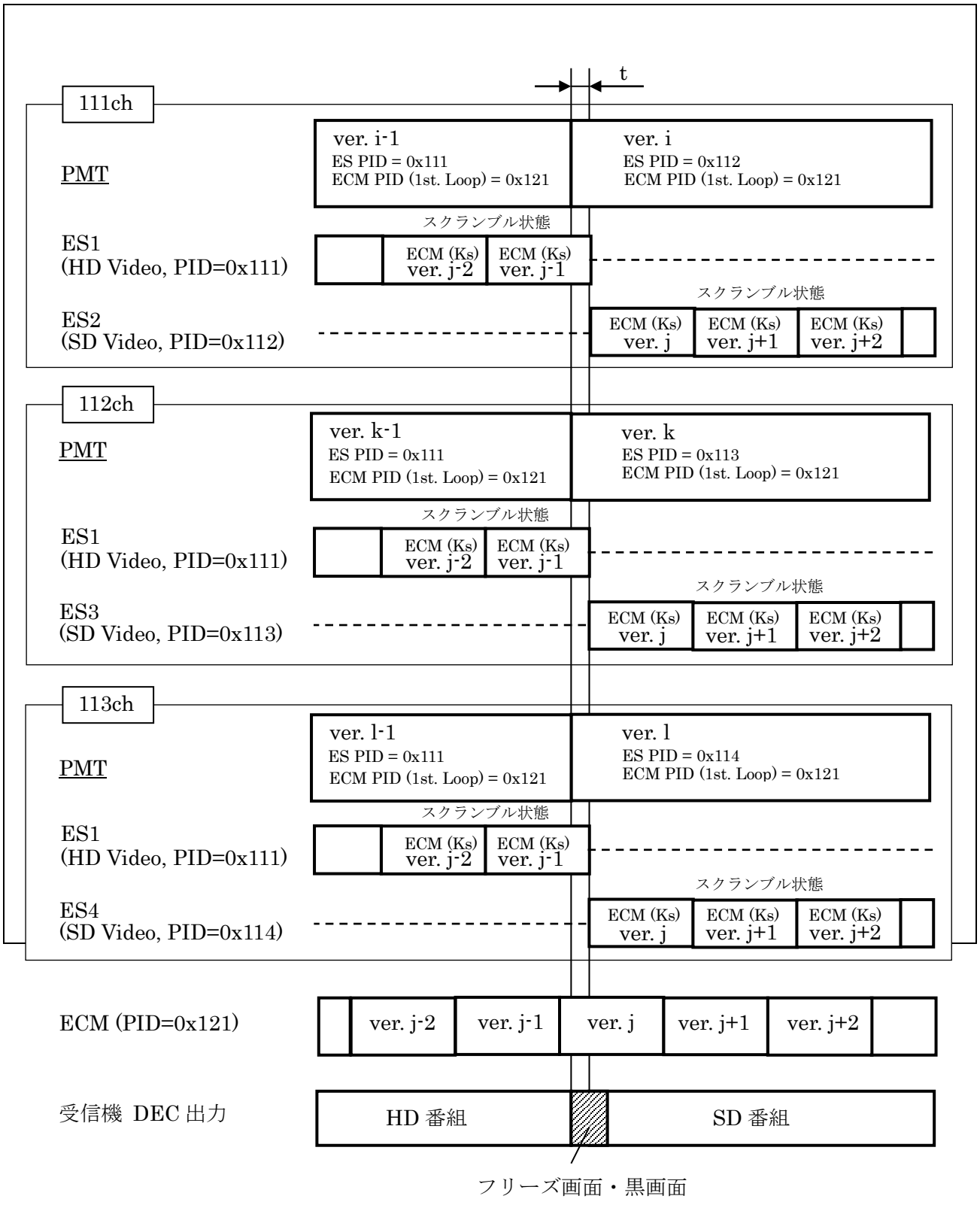


図 A-3　HD 番組から SD 番組(3ch)への切り替え時に想定される放送信号と受信機動作

図に示したようにESの切り替わるt秒前にPMTの更新が行われるとすると、受信機は、PMTの更新をトリガーにして、ESの切り替え処理を行う。このとき、ARIB STD-B20 第2部 4.3 シームレス切り替え に記載されているようにシームレス切り替え未対応受信機及びシームレス切り替え対応型受信機であってもAVデコーダーのバッファがアンダーフローになるような場合においては、スクランブル継続の有無に関わらず切り替え時に映像のフリーズまたは黒画面（ミューティング状態）が発生する場合が考えられる。従って、コンテンツ制作においては、このような場合を想定した配慮（静止画や無音区間の挿入等）を行うことが望ましい。また、PMTの更新時にスクランブル状態が継続された場合、PMTの更新によりスクランブル鍵（Ks）を再取得するような処理を行う受信機の存在も考えられる。このような受信機においては、ノンスクランブルの場合に比べてKsの再取得分だけ映像・音声のフリーズやミューティング時間が長くなることも考えられる。なお、地上デジタルテレビジョン放送では、コンポーネント課金の運用制限により同一サービス中で同時に運用されるKsは一種類だけなので、受信機がPMTの更新前のKsを保存しておくことより、PMT更新時の映像・音声のフリーズやミューティング時間に対するスクランブルの影響を抑制することも可能である。

A.5 事業体識別の運用についての想定

- 地上デジタルテレビジョン放送での事業体識別の運用に関しては、コンテンツ保護を伴う無料番組については、全国同一の事業体識別を使用する。
- 有料番組おける事業体識別は、事業体識別が有限な数であるため基本的には系列で 1 個の事業体識別で運用を行い、同一系列内の運用に関しては、その事業体識別の中でのティア運用であることを想定した。
- 複数限定受信方式の運用導入にあたり、事業体識別の値については、CA_system_id 内でユニークという想定とした。

A.6 CA代替サービスのメッセージIDについての想定

CA代替サービスはその運用目的から主に有料放送開始時点で視聴者に対して加入案内のサービスにリンクするなどの機能であり、メッセージにおいては、顧客管理センターなどの問い合わせ電話番号などが記載されることが想定される。この顧客管理センターは、事業体識別を持つ事業者単位で運用され放送事業者単位での運用ではないことを想定した。

一方、受信機においては最大32個の事業体識別が管理されるため、CA代替サービスにおけるメッセージIDについては、地上デジタルテレビジョン放送全国において20個以内で運用されることとした。（最大32個の事業体識別は、BS、広帯域CS、地上トータルで32個である）

CA代替メッセージのメッセージIDについては、前記事業体識別を持った事業者間で調整されることを想定した。

A.7　自動表示メッセージの蓄積機能内蔵受信機の対応

蓄積機能を内蔵した受信機で、蓄積・再生された信号に対して自動表示メッセージを表示するか否かを放送局側で制御する機能を持たせる理由は、当初、再生信号でメッセージを表示することは問題ないとして運用を開始したものの、将来、再生信号までにメッセージを表示することは問題であるとなった場合などに、表示しないように制御するとリアルタイムの放送でも表示できなくなる可能性があることを避けるためである。

この規定で猶予期間の最下位ビットが0として適用された場合は、猶予期間として偶数日を意味し、1の場合は奇数日が指定されることになる。例えば猶予期間が30日か31日かの差はかかる運用で大きな差がないと考え、最下位ビットの0または1で蓄積内蔵受信機でのメッセージ表示の制御という最下位ビットに二重の意味をもたせた運用となっている。したがって、蓄積機能を持たない受信機においては、表示制御に関しては関係なく、指定された猶予期間で制御される。

A.8　カードＩＤの表示について

カードＩＤの表示機能の目的は、主に有料放送や自動表示メッセージを利用したサービスなど、EMMの受信に関する視聴者からの問い合わせの際に、カスタマーセンターでカードIDの確認を行うためである。EMM受信に関する問い合わせであることから、受信機メーカーより放送局のカスタマーセンターで対応する場合が多く、各社の受信機での対応を行わなければならない。また視聴者によっては受信機に装着されているカードの位置が判らなかったり、故障を恐れて抜きたがらないなど、カードを直接確認する方法では、電話応対しきれない場合がある。

受信機機能としてのカードID表示機能のユーザーインタフェースについては、メーカーの商品企画とするが、上述のような理由から、極力視聴者から問い合わせに対して混乱を避けるため、例えば受信機のメニューの階層の浅いところで、少ないボタン操作で容易に表示できるなど、視聴者にとって表示機能操作がわかりやすいことが望ましい。

グループIDについては、今後運用を行わないことから、2013年12月のTR-B14 5.4版改定において、グループIDに関する記載を削除するとともに、グループIDの表示機能について搭載不要とした。ただし、ICカードと受信機間のカード情報取得コマンドレスポンスについては、特に変更は無い。

A.9　部分受信階層における有料放送の導入に関して

部分受信階層放送開始当初においては、有料放送の規定は行わず、運用開始時にその時点で最適な方式で運用するため放送開始から当面部分受信専用受信機においては、有料放送機能を搭載しない。そのため、将来有料放送を開始する場合は、それまでの有料非対応の部分受信専

用受信機では、有料放送を視聴する術がないためユーザーの混乱を招きかねないので、それまでの放送と同一サービスで無料と有料番組を混在した編成は極力避けるべきである。

A.10　必須・オプションに対する基本的な考え方

表 A-1　限定受信に関する受信機の必須・オプション

No	CAS を利用するサービス	受信機の仕様	部分受信階層専用受信機	部分受信階層以外の受信機
1	基本	低速 CAI/F	C	A
		ID 番号表示	C	A*3
		エラー通知	A	A
		通電制御	C	A
		デスクランブラ	C	A
		IC カードテスト	C	A
		複数 CAS 運用の識別	A	A
2	コンテンツ保護を伴う無料番組	通常視聴	C	A
		番組予約	C	B
		エラー表示	C	A
3	有料放送：フラット/ティア	契約視聴処理	C	A
		有料放送の予約	C	B
4	有料放送：ペイパービュー	PPV 視聴処理	C	C
		電話モデムの利用	C*1	C*1
		ﾘﾄﾗｲｵｰﾊﾞｰ通知機能	C	C
		ユーザー発呼要求	C	C
		電話回線導通テスト	C	C
		録画購入	C	C
		ES 毎課金	C	C
		通電発呼制御	C	C
5	CA 代替サービス		C	B
6	EMM メッセージサービス	自動表示メッセージ	C	A
		メール	C	A
		IC カード未装着メッセージ（ノンスク時自動表示メッセージを使ったもの）	C	A
		蓄積機能搭載受信機での対応	C	A
7	EMM 受信	EMM 受信	C	A
		EMM 送出タイプ	C	A
8	パレンタルコントロール	パレンタル制御	C	C
		暗証番号消去	C	C
9	IRD データ伝送	双方向サービスのデータ暗号化	C	C

A：必須、B：オプション、C：実装不可*2

*1： 電話モデムに関しては、CASとしてはPPV、IRDデータ伝送の運用制限に伴いモデム搭載は不要である。本項目はCASとして搭載が不要であり、双方向サービスの対応に関してはこの限りでなく、本書第六編に準ずる。

*2： 実装不可は下記の主旨から記載している。

本編では地上デジタルテレビジョン受信機を想定して記載しているが、「実装不可」との記載は、PPV機能のように放送開始当初は運用制限とした機能が、将来運用開始する時に、その時点で最適な規定（現在のTR-B15とは異なる新しい規定）になることを想定しているためである。

例えば、PPVの視聴履歴収集ではBSではBASIC系モデム搭載をオプションとしているが、地上では、例えば運用開始時には、TCP/IP経由ということなども想定される。もし地上のPPV機能として現行のTR-B15のまま実装した受信機が存在すれば、将来の規格策定においてレガシー受信機への対応が必要になり、最適な規格策定が出来なくなるため、あえて誤解を発生しないように実装不可と明記した。

つまり地上デジタルテレビジョン専用受信機はもとより、BSとの共用受信機においても地上デジタル受信機能として実装してはならないものとの解釈をしていただきたい。ただし、共用受信機において提示中の放送コンテンツと無関係な、BSで必要な機能の設定メニュー等（例えばパレンタル機能のパレンタルレベル（視聴最少年齢）の設定、PPVの購入限度額の設定等）を地上デジタルテレビジョン放送視聴中に提示するか否かは受信機の裁量の範囲と考えている。

以上のような考えから表A-1においては、本編にて規定していない機能でTR-B15に記載されている機能に対しても確認の意味で記載した。

*3： カード識別、カードIDの表示は必須のままとするが、グループIDの表示機能については搭載不要とする。

B　付録

B.1　地上・BS・広帯域CS共用デジタル受信機の要求仕様

地上・BS・広帯域CS共用デジタル受信機に対する第五編に関係する要求仕様は、BS／広帯域CSデジタル受信部は、TR-B15、地上デジタルテレビジョン受信部は本編に従うことを原則とする。ただし、以下の項目に関し共用受信機での要求仕様について規定する。

B.1.1　メール表示

- 共用受信機におけるメールの記憶について、少なくとも BS／広帯域 CS デジタル用、地上デジタル合わせ３１個のメールを記憶する。
- 記憶容量を超えたメールの処理については商品企画マターとする。ただし、BS/広帯域 CS デジタル放送で２４通、地上デジタルテレビジョン放送で 7 通を各々別に管理することが望ましい。

B.2　ICカードに関する問い合わせ先

(1) CA_system_id　0x0005

管理会社名	㈱ビーエス・コンディショナルアクセスシステムズ
電話	0570－000－250
URL	http://www.b-cas.co.jp

【第二部】　RMP方式運用規定及び受信機仕様

1　はじめに

1.1　まえがき

地上デジタルテレビジョン放送受信機に対する限定受信方式に関する仕様は電波産業会標準規格「デジタル放送におけるアクセス制御方式」（以下、ARIB STD-B25）で規定される。

無料番組を対象とするコンテンツ保護方式には、ARIB STD-B25 第1部　受信時の制御方式（限定受信方式）に規定する方式とARIB STD-B25 第3部　受信時の制御方式（コンテンツ保護方式）に規定する方式があるが、本編第二部はARIB STD-B25 第3部に規定する方式について、それを補足する形で運用上の送出運用規定と受信機仕様に対する要求仕様について規定した。したがって、本編第二部に記載されていない事項に関してはARIB STD-B25第3部を参照願いたい。

なお、本編第二部は、ARIB STD-B25 第3部に基づき、コンテンツ保護を伴う無料番組を対象とした方式（CA_system_id=0x000E　以下RMP方式）に関する記載である。従って、ARIB STD-B25 第1部に基づき、コンテンツ保護を伴う無料番組を対象とした方式の運用を実施する場合の記載については、本編第一部に記載されている方式（CA_system_id＝5　以下CA5方式）を参照願いたい。RMP方式とCA5方式の同時運用（サイマルクリプト運用）については、本編第二部に記載している。

1.2　目的

本編第二部はARIB STD-B25第3部に基づいて、地上デジタルテレビジョン放送受信機におけるCAS機能を搭載する際に考慮すべき受信機に対する要求仕様や、運用情報について記載したものである。

1.3　適用範囲

本規格書は、地上デジタルテレビジョン放送のARIB STD-B25第3部に準拠したRMP方式における送出運用規定および、受信機仕様について適用する。

2　引用文書

(1)　平成 26 年総務省告示第 233 号

(2)　「デジタル放送におけるアクセス制御方式」標準規格　ARIB STD-B25

3　用語

本規定で用いる用語を以下のように定義する。

ARIB	Association of Radio Industries and Business： 一般社団法人電波産業会 放送事業者、電気通信事業者、機器製造者（メーカ）が参画する国内の電波利用に関する技術を標準規格化する団体。
CA system	Conditional Access system：限定受信方式。サービス（編成チャンネル）やイベント（番組）の視聴を制御するシステム。
CAT	Conditional Access Table：EMM を伝送する TS パケットのパケット ID などを示すテーブルである。
Component	コンポーネント。映像、音声、文字、各種データなど、イベント（番組）を構成する要素。
Descriptor	様々な情報を載せるためテーブル内に配置される記述領域、記述子。
ECM	Entitlement Control Message：全受信機共通の情報を伝送するデータで、主にスクランブル放送のスクランブル鍵、番組の情報を伝送する。
EIT	Event Information Table：番組の名称、属性、放送日時、内容など、番組に関する情報のテーブルである。
EMM	Entitlement Management Message：デバイス ID 個別の情報を伝送するデータで、EMM を識別するためのデバイス ID が付加され、主に ECM を復号化するためのワーク鍵が伝送される。
EMM メッセージ	EMM で伝送される個別、共通メッセージ
ES	Elementary Stream：基本ストリーム。PES パケット中の、符号化された映像、音声、独立データに相当する。1 つの ES は同一のストリーム ID を持つ PES パケットにより伝送される。
Event	イベント。ニュース、ドラマなど、同一サービス（編成チャンネル）内で開始・終了時刻の決まったストリームの集合。
PID	Packet Identifier
PMT	Program Map Table：放送番組のストリーム（コンポーネント）情報や、ECM を伝送する TS パケットのパケット ID などを示すテーブルである。
SDT	Service Description Table：編成チャンネルの名称、放送事業者の名称など、編成チャンネルに関する情報のテーブルである。
CA 代替サービス	視聴者がスクランブルチャンネルを選局したとき、非契約等の条件の場合に放送事業者が運営している視聴者への「ご案内チャンネル」に誘導するサービス。
コンテンツ保護を伴う無料番組	コンテンツの権利保護を目的とし、顧客管理を伴わず、放送波において安全にコンテンツの送信を行う無料番組。
メール	EMM メッセージによって受信機に記憶するメッセージで、ユーザ操作などにより任意に呼び出せるメッセージ。
限定受信放送	限定受信方式記述子またはアクセス制御記述子を利用した放送。限定受信放送には、有料番組、EMM メッセージを利用した放送、コンテンツ保護を伴う無料番組がある。

自動表示メッセージ	EMM メッセージによって受信機に記憶するメッセージ（蓄積機能を有する受信機で受信した信号を再生する場合を含む）で、番組受信中に同時に表示するメッセージ。
商品企画	搭載される機能や動作が受信機または商品に依存するもの。
蓄積機能	記録した機器でのみ再生可能な記録再生機能。
無料番組	非課金対象の番組。SDT、EIT に記述された free_CA_mode=0 の番組。
有料番組	課金対象の番組。SDT、EIT に記述された free_CA_mode=1 の番組。
コンテンツ保護方式	コンテンツの権利保護を目的とし、暗号化等によりコンテンツの改ざんおよび不正コピー等を防止する技術。
RMP 事業体	コンテンツ保護方式の運用を行なう放送事業者もしくはその集合体。
デバイス ID	受信機機種、またはメーカを識別するために、受信機機種毎、または受信機メーカ毎で管理される 64 ビットの識別番号。本書では、受信機機種を識別する運用を行わないため、RMP メーカ ID と等価。
RMP メーカ ID	受信機メーカを識別するために、受信機メーカ毎に管理されるデバイス ID。
特定の鍵の無効化	運用システム内で、特定の鍵をシステムから排除すること。
デバイス ID の世代	デバイス ID、及びデバイス鍵を受信機内で更新する場合の更新状態を示し、世代番号で識別される。
権利保護情報	デジタルコピー制御記述子、およびコンテント利用記述子の総称。
サイマルクリプト運用	１つの番組に対して複数の限定受信（CAS）方式を並列運用する運用形態。種類が異なる CAS 方式の ECM や EMM を番組に付加して並列送信する。受信機は、いずれか一方の CAS 方式に対応していれば受信可能となる。
RMP 方式	無料番組を対象とするコンテンツ保護方式の中で、ARIB STD-B25 第 3 部　受信時の制御方式（コンテンツ保護方式）に基づいて本規定第五編第二部に規定する方式。
デバイス鍵更新アルゴリズム	ARIB STD-B25 第 3 部で規定される、デバイス鍵を生成するアルゴリズム。デバイス鍵更新アルゴリズムには、算術的に乱数を生成する算法だけではなく、例えば、乱数表を参照するような手法なども含まれる。

4　送出運用規定

4.1　限定受信放送

- 限定受信方式記述子またはアクセス制御記述子を利用した放送である。ARIB STD-B25 第 3 部　受信時の制御方式（コンテンツ保護方式）に基づいて本規定第五編第二部に規定する方式（以下 RMP 方式）ではアクセス制御記述子のみを利用する。
- 限定受信放送には、有料番組、EMM メッセージを利用した放送、コンテンツ保護を伴う無料番組があるが、RMP 方式では有料番組を対象としない。

4.2　ノンスクランブル／スクランブル

4.2.1　概要

- 受信側でのコンポーネントのスクランブルモードの判定は、TS パケットヘッダ中の transport_scrambling_control フィールドを参照する。地上デジタルテレビジョン放送において、free_CA_mode に関しては、有料か無料かの判定目的だけとし、スクランブル、ノンスクランブルの判定を有料・無料の判定に用いてはならない。
- コンポーネントがコンテンツ保護対象である場合にも、常にスクランブルされるとは限らない。

  運用上ノンスクランブル挿入が必要な場合を本編第二部 4.8.7　ECM の適用の変更に記載する。
- 大規模災害報道、緊急ニュースなど人命に関わる緊急事態においては、予告なくスクランブルを解除する場合がある。この場合、PSI/SI、ECM、EMM は、スクランブルが継続して掛かっているものとして送出することがある。
- 本編第二部 5.16 エラー表示に関連する記載がある。

4.2.2　字幕、文字スーパーの運用

- デフォルト ES 群を特定する PMT の第 1 ループに有効な ECM_PID が記載されている場合、すなわち通常のスクランブル状態で字幕、および文字スーパーのコンポーネントをスクランブルする場合は、必ずデフォルト ES 群と同じ ECM_PID とする。
- デフォルト ES 群がスクランブル状態であっても、字幕、文字スーパーのコンポーネントをノンスクランブルで運用することが可能である。この場合、必ず当該ノンスクランブルコンポーネントに対して PMT 第 2 ループに無効な ECM_PID = 0x1FFF を記載する。
- デフォルト ES 群がノンスクランブルの場合は、字幕、文字スーパーコンポーネントのいずれもノンスクランブルで運用する。

4.3 無料番組

4.3.1 無料番組

4.3.1.1 定義

- 無料番組とは、その番組を構成するデフォルト ES 群が非課金のものをいう。
- デフォルト ES 群はサービスタイプ毎に定義する。

例：デジタル TV サービスの場合

デフォルト ES 群＝デフォルト映像 ES とデフォルト音声 ES

表 4-1 デフォルト ES 群

service_type	内容	デフォルト ES 群
0x01	デジタル TV サービス	映像、音声
0xC0	データサービス	データ(エントリコンポーネント)
0xA1	臨時映像サービス	映像、音声
0xA3	臨時データサービス	データ(エントリコンポーネント)
0xA4	エンジニアリングサービス	規定せず*1
0xAA	ブックマーク一覧データサービス	データ(エントリコンポーネント)

＊1： エンジニアリングサービスは視聴目的で選択されるサービスではないため限定受信方式としてのデフォルトES群としての規定は行わない。

4.3.1.2 運用

- 全ての ES を非課金とする。
- SDT および EIT において free_CA_mode=0 で運用を行う。

4.3.2 コンテンツ保護を伴う無料番組

4.3.2.1 定義

- コンテンツ保護目的のため、放送波において安全にコンテンツの送信を行うための非課金のスクランブル番組である。
- コンテンツ保護を伴う無料番組において、RMP 方式では RMP 事業体識別は各 RMP 事業体固有の値を使用する。

4.3.2.2 運用

- １つの番組において、ECM は必ず伝送する。
- 番組内のコンポーネントにスクランブル ES とノンスクランブル ES とが混在する場合を考慮し、CA_system_ID フィールドに RMP 方式の識別値、CA_PID フィールドに有効な ECM_PID を記述したアクセス制御記述子の PMT への配置を以下のように定める。
    1) PMT の第 1 ループに当該アクセス制御記述子を必ず 1 つ配置する。この場合、番組内のすべてのコンポーネントに対し当該 ECM が適用される。

2) PMT の第 2 ループには当該アクセス制御記述子を配置しない。ただし、デフォルト ES 群以外でノンスクランブル運用する場合に限り、CA_system_ID フィールドに RMP 方式の識別値、CA_PID フィールドに無効な ECM_PID=0x1FFF を記述したアクセス制御記述子を配置する。

- 受信機はワーク鍵が実装されない状態で出荷されるため、コンテンツ保護を伴う無料番組を運用する放送局はスクランブルの鍵開け目的のため、EMM を必ず常に伝送する。
- 大規模災害報道、緊急ニュースなど人命に関わる緊急事態においてスクランブルが解除されていても、ECM、EMM は継続して伝送することがある。

4.3.3 無料番組・コンテンツ保護を伴う無料番組の運用上の組み合わせ

- 表 4-2 に無料番組、およびコンテンツ保護を伴う番組の運用についての運用条件の一覧を示す。 また表 4-3 にデフォルト ES 群とデフォルト ES 群以外でのスクランブル／ノンスクランブルの運用可能な組み合わせについて示す。

表 4-2 無料番組およびコンテンツ保護を伴う無料番組の運用

No		1	2
番組種別		無料番組	コンテンツ保護を伴う無料番組
有料/無料番組の区分		無料	無料
有料付加 ES		×	×
Free_CA_mode		0	0
コンテンツ保護対象	デフォルト ES 群	非対象	保護対象可
	デフォルト以外 ES	非対象	保護対象可
TS パケットヘッダ *3	デフォルト ES 群	00	10,11
	デフォルト以外 ES	00	10,11 *1
課金対象	デフォルト ES 群	非課金	非課金
	デフォルト以外 ES	非課金	非課金
ECM 送出		不要	必要
EMM 送出		不要	必要 *2
使用する RMP 事業体識別	デフォルト ES 群	－	RMP 事業体固有 ID
	デフォルト以外 ES	－	RMP 事業体固有 ID

*1： コンテンツ保護を伴う無料番組において、デフォルトES群以外でノンスクランブル運用を行う場合は、コンポーネントタグ値が0x30～0x3Fの字幕、文字スーパーのES、およびデフォルトES群以外の0x40～0x7Fのデータコンポーネントのみである。また、この際にはPMT 第2ループに無効なECM_PID=0x1FFFを配置する。

*2： コンテンツ保護を伴う無料番組においてワーク鍵設定目的等でEMM送出が必要である。

*3： TSパケットヘッダ中のtransport_scrambling_controlフィールド。

表 4-3　スクランブル／ノンスクランブルの運用可能な組み合わせ

		デフォルト ES 群	
		無料番組	コンテンツ保護を伴う無料番組
デフォルトES群以外	ノンスクランブル *4	○ 1st：なし 2nd：なし	○ 1st：固有 RMP 事業体 2nd：PID=0x1FFF
	コンテンツ保護のためのスクランブル	×	○ 1st：固有 RMP 事業体 2nd：なし
	存在しない （2nd ループなし）	○ 1st：なし	○ 1st：固有 RMP 事業体

*4：　デフォルトES群以外でノンスクランブル運用が可能なのはコンポーネントタグが0x30～0x3Fの字幕、文字スーパーのES、およびデフォルトES群以外の0x40～0x7Fのデータコンポーネントに限定される。

－ 表 4-3 における語句の解説

・○：運用可能、　×：運用禁止（運用制限）

・PMT の第 1 ループ（1st）、第 2 ループ（2nd）に配置するアクセス制御記述子の内容を示す。

1) なし　　：アクセス制御記述子を配置しない。

2) PID=0x1FFF　　：アクセス制御記述子を配置し、無効な ECM をポイントする。ECM ストリームは存在しない。

3) 固有 RMP 事業体　　：アクセス制御記述子を配置し、事業者固有の RMP 事業体識別の ECM をポイントする。

4.4 階層伝送時におけるコンテンツ保護の運用

4.4.1 伝送階層と限定受信サービス関連情報の伝送

- CAT は A 階層で必ず伝送する。
- EMM は部分受信階層を除く A 階層、または B 階層で必ず伝送する。関連する記載が本編第二部 4.9.7.2 にある。
- ECM は PMT が記述される階層と同一階層、またはより強い階層で伝送される。

表 4-4 階層伝送時におけるコンテンツ保護サービスに関連する情報の伝送

ﾊﾟﾀｰﾝ	使用階層	セグメント数		CAS に関連する情報		
				CAT	EMM	ECM
(1)	A	13	固定	○	○	○
(2)	A	13	移動	○	○	○
(3)	A	1（部分受信）	携帯	○	×	×
	B	12	固定	×	○	○
(4)	A	8～2	移動	○	○	○
	B	5～11	固定	×	×	○
(5)	A	1（部分受信）	携帯	○	×	×
	B	12	移動	×	○	○
(6)	A	1（部分受信）	携帯	○	×	×
	B	7～1	移動	×	○	○
	C	5～11	固定	×	×	○

表中、○：送出必須または送出可能なもの、×：送出しないもの

- 表 4-4 におけるパターンは本書　運用概要 表 2 のパターンと同じ意味である。

4.4.2 部分受信階層におけるコンテンツ保護

- 部分受信階層では、RMP 方式の運用は行わない。

4.5 パレンタルレートの設定

- パレンタルコントロールの運用は行わない。

4.6 アクセス制御記述子

4.6.1 機能

- CAT に記載された場合は、CA_system_id に対応した EMM を伝送する TS パケット ID を特定する。
- CAT に RMP 方式の CA_system_id と異なる CA_system_id を持つ複数のアクセス制御記述子が記載される場合がある。

- PMT に記載された場合は、CA_system_id に対応する ECM を伝送する TS パケット ID を特定する。
- PMT に RMP 方式の CA_system_id と異なる CA_system_id を持つ複数のアクセス制御記述子が記載される場合がある。

4.6.2 運用

- CAT に RMP 方式のアクセス制御記述子を 1 つのみ必ず記載する。なお、private_data_byte 領域の先頭 1 バイトには EMM 伝送識別を記載する。詳細については、本編第二部　4.9.4.1　を参照のこと。
- PMT にアクセス制御記述子を記載する場合、private_data_byte 領域に記載するデータは先頭 1 バイトを受信機においては無視される。これは、BS デジタル放送におけるパレンタルレートの運用との整合を取るためである（2 バイト目以降は当面運用しない)。
- アクセス制御記述子の transmission_type 領域（3 ビット）に記載するデータは ECM、EMM の伝送経路を示すために使用するが、当面'111'のみを運用し、それ以外の値が記述されている場合は、受信機は当該記述子を無視すること。

4.7 CATの送出

4.7.1 伝送されるTS PID

- 平成 26 年総務省告示第 233 号記載の「PID の割り当て」の通り（0x0001)。

4.7.2 データ構造

- 平成 26 年総務省告示第 233 号記載の「CAT の構成」の通り。

4.7.3 伝送される記述子とその構成

- CAT にて伝送される記述子のうち CA_system_id=0x000E 関連のものはアクセス制御記述子のみとし、アクセス制御記述子の構成は、平成 26 年総務省告示第 233 号記載の「アクセス制御記述子の構成」の通りとする。
- CA_system_id は本書第七編を参照のこと。

4.7.4 送出頻度

- CAT の送出頻度は第四編による。

4.7.5 更新頻度

- 通常の運用では、更新頻度は 1 回／日以下とする。

4.8　ECM

4.8.1　ECMの役割

- RMP 方式は、デバイス鍵・ワーク鍵およびスクランブル鍵という 3 階層の鍵を使用する。このスクランブル鍵を伝送する情報が ECM であり、コンテンツ保護ルールを遵守した受信機のみが放送コンテンツを受信して利用できるように、コンテンツはスクランブルされて放送される。ECM はこの受信機へのスクランブル鍵の伝送用として運用される。
- コンテンツ保護ルールを遵守した受信機では、ECM を受信して使用することで、放送されたコンテンツを正しくデスクランブルでき、視聴、利用が可能になる。

4.8.2　ECMの種類

- ECM にはフォームが異なる 2 種類の ECM（ECM-F0 と ECM-F1）があるが、そのうち ECM-F1 のみを運用するものとする。ECM-F1 はスクランブル鍵を伝送する主目的のほか、ワーク鍵が受信機から漏洩した場合にその漏洩元を検出する役割を持つ。

4.8.3　ECMの基本構成

- ECM は ARIB STD-B25 第 3 部 3.2.6.1　ECM の基本構成 に示すように、MPEG2 システムズのセクション形式にて伝送される。（図 4-1）
- ECM は 1 つの TS パケットに収まるように送出され、複数のセクションが 1 つの TS パケット内に混在することはない（シングルセクション）。
- ECM 本体内のリザーブビットの運用は、送信側は 0 を送り、受信側は無視するものとする。
- ECM-F1 は、ECM のプロトコル番号で識別される。
- ECM 本体は常に固定的に伝送される固定部と運用に応じて長さが増減する可変部で構成されるが、可変部は固定的に運用する。
- 改ざん検出は存在しない。
- ECM セクション全体がセクション CRC の対象となる。

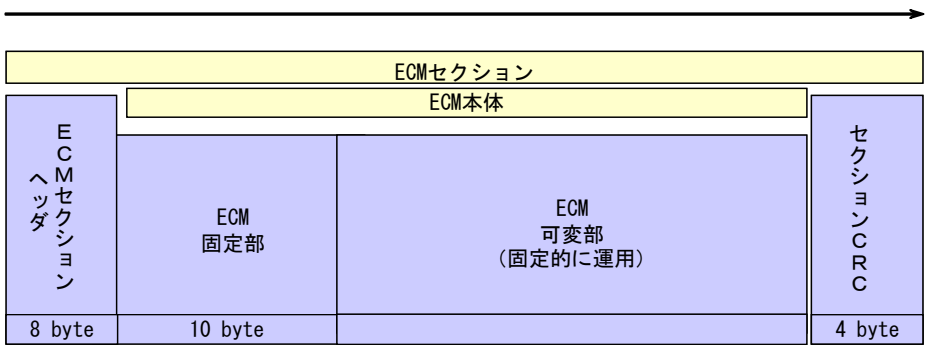


図 4-1　ECM-F1 のセクション構成

4.8.4　ECM-F1のデータ構成

- ECM-F1 は平成 26 年総務省告示第 233 号記載の拡張セクション形式で伝送され、テーブル識別子の値は 0x82 のみを使用し、0x83 は使用しない。また「テーブル識別子拡張」は使用しない。
- ECM-F1 セクションは表 4-5 に示すデータ構成である。

表 4-5　ECM-F1 セクション構成

<table>
<tr><th colspan="5">説明</th><th>byte 数</th></tr>
<tr><td rowspan="18">ECM セクション</td><td colspan="4">ECM セクションヘッダ
(テーブル識別子 0x82)</td><td>8 Byte</td></tr>
<tr><td rowspan="16">ECM-F1 本体</td><td rowspan="6"></td><td rowspan="6">固定部</td><td>プロトコル番号</td><td>1 Byte</td></tr>
<tr><td>RMP 事業体識別</td><td>2 Byte</td></tr>
<tr><td>日時</td><td>5 Byte</td></tr>
<tr><td>F1 ワーク鍵識別</td><td>1 Byte</td></tr>
<tr><td>スクランブル鍵ペア数</td><td>1 Byte</td></tr>
<tr><td rowspan="10">暗号化部</td><td rowspan="10">可変部
（固定的に運用）</td><td>スクランブル鍵 0(Odd)</td><td>8 Byte</td></tr>
<tr><td>スクランブル鍵 0(Even)</td><td>8 Byte</td></tr>
<tr><td>スクランブル鍵 1(Odd)</td><td>8 Byte</td></tr>
<tr><td>スクランブル鍵 1(Even)</td><td>8 Byte</td></tr>
<tr><td>・
・</td><td>・
・</td></tr>
<tr><td>スクランブル鍵 9(Odd)</td><td>8 Byte</td></tr>
<tr><td>スクランブル鍵 9(Even)</td><td>8 Byte</td></tr>
<tr><td colspan="4">セクション CRC</td><td>4 Byte</td></tr>
<tr><td colspan="5">合計　ECM セクション</td><td>182 Byte</td></tr>
</table>

- ECM-F1 本体は 10 バイトの固定部と 10 個のスクランブル鍵ペアからなる。スクランブル鍵部には、同一のスクランブル鍵（Odd/Even）のペアを 10 種類の異なるワーク鍵で暗号化し、スクランブル鍵 0～9（Odd/Even）に配置する。
- ECM-F1 本体は合計 170 バイト、ECM セクションは合計 182 バイトとなる。

（1）ECM-F1 における固定部

①プロトコル番号

- ECM フォームの識別と、暗号化／復号アルゴリズムのパラメータを示す。
- 上位 2 ビットで、関連情報暗号化の CBC 初期値を指定する。CBC 初期値については、関連する記載が付録 B.2.1 にある。
- 最下位ビット（bit0）で、ECM-F1 の識別を行う。

'1'： ECM-F1 であることを示す

'0'： 未定義

bit1-5 の 5 ビットについてはリザーブとする。

表 4-6　プロトコル番号

値（2 進数）	内容
00XXXXX1B	関連情報暗号化の CBC 初期値 0 を指定　ECM-F1
01XXXXX1B	関連情報暗号化の CBC 初期値 1 を指定　ECM-F1
10XXXXX1B	関連情報暗号化の CBC 初期値 2 を指定　ECM-F1
11XXXXX1B	関連情報暗号化の CBC 初期値 3 を指定　ECM-F1

②RMP 事業体識別

- 本コンテンツ保護方式を運用する RMP 事業体を識別するコードで、0x0000～0xFFFF の範囲で使用する。
- 1 トランスポートストリーム内の RMP 事業体識別は共通（1 種類）とする。

③日時

- 使用せず、リザーブとする。

④F1 ワーク鍵識別

- EMM で 2 種類の F1 ワーク鍵（Odd/Even）が設定されるが、それらの F1 ワーク鍵識別（1 バイト）と本項目（1 バイト）を比較し、一致する方の F1 ワーク鍵が本 ECM-F1 を復号するワーク鍵となる。一致するものがなければ、必要なワーク鍵がないために本 ECM-F1 を復号できないことを示す。

⑤スクランブル鍵ペア数

- 可変部で送るスクランブル鍵（Ks）のペアが何組あるかを示す。ペア数は、ECM が 1TSP に収まる 10 で運用する。

（2）ECM-F1 における可変部(固定的に運用)

ECM-F1 の可変部（固定的に運用）にはスクランブル鍵のペア（16 バイトの固定長）を 10 組配置する。記述子は配置しない。

①スクランブル鍵 0～9(Odd/Even)

- 現在と次の 2 つのスクランブル鍵（Ks）をペアで送る。
- 同一の Ks（Odd/Even）を 10 種類の異なる F1 ワーク鍵で暗号化し、スクランブル鍵 0～9 に配置して送る。
- ECM-F1 で暗号化されるのは、スクランブル鍵 0～9 の項目のみである。
- ECM-F1 の暗号化では 10 種類の F1 ワーク鍵が使用されるが、各受信機が持つ F1 ワーク鍵は 1 種類だけである。各受信機がどのスクランブル鍵を復号するかは、EMM で設定された F1Ks ポインタの値による。例えば F1Ks ポインタが 0x00 ならスクランブル鍵 0 を復号し、F1Ks ポインタが 0x09 ならスクランブル鍵 9 を復号する。

4.8.5　ECMの特定

- PMT の第 1 ループに CA_system_id＝0x000E のアクセス制御記述子が記載される場合に、RMP 方式の ECM が伝送される TS パケットの PID が特定される。
- アクセス制御記述子の限定受信 PID が 0x1FFF のときに限り、当該 ECM は伝送されることはない。

4.8.6　ECMの適用

- アクセス制御記述子が PMT の第 1 ループにのみ記載され、有効な ECM_PID が記述される。また、放送番組要素を伝送する ES すべてに当該 ECM が適用される。
- PMT の第 2 ループに ECM_PID として 0x1FFF が記述されたアクセス制御記述子が記載されたときは、当該 ES がスクランブル処理されていないことを示し、実際に PID=0x1FFF の ECM が伝送されることもない。

4.8.7　ECMの適用の変更

本編第一部 A.4.3 に関連記載がある。

4.8.7.1　スクランブルの開始

－　ノンスクランブル放送（または放送番組要素を伝送する ES）がスクランブル放送（または放送番組要素を伝送する ES）に切り替わる場合の放送信号の変化は以下の通り。

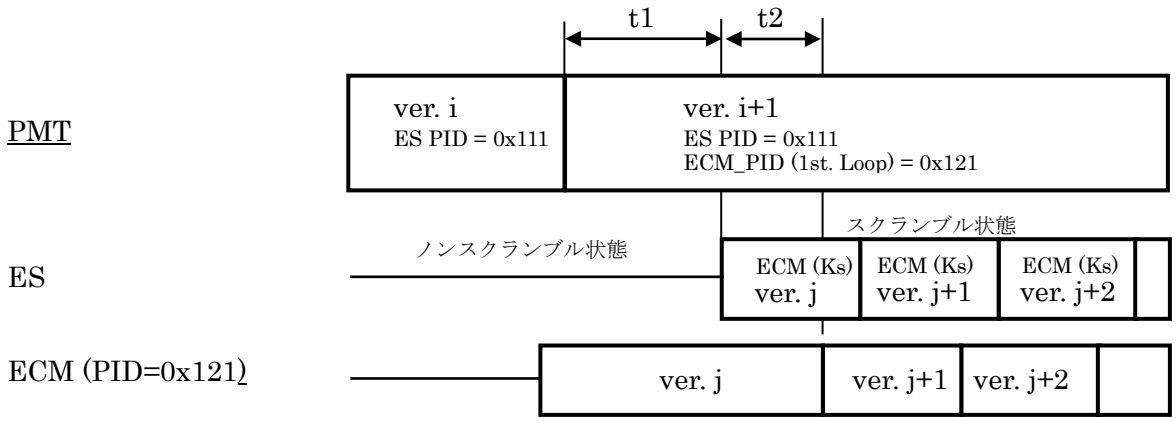


図 4-2　スクランブルの開始

1)　当該 ES がノンスクランブル状態で送出された状態で、ECM が送出される。
2)　ECM が送出された後、PMT の第 1 ループに ECM と当該 ES（群）の関連が記載され送出される。（PMT の更新）
3)　PMT 更新の t1 秒後、当該 ES（群）にスクランブルが開始される。
4)　スクランブル開始後、t2 秒後に、最初の ECM 更新が発生する。

t1= 2，0<t2

ECM の更新に関しては

4.8.8.2　更新・再送周期

4.8.8.3　ECM の更新とスクランブル鍵の変更

に準ずる。

4.8.7.2　スクランブルの終了

－　スクランブル放送（または放送番組要素を伝送する ES）がノンスクランブル放送（または放送番組要素を伝送する ES）に切り替わる場合の放送信号の変化は以下の通り。

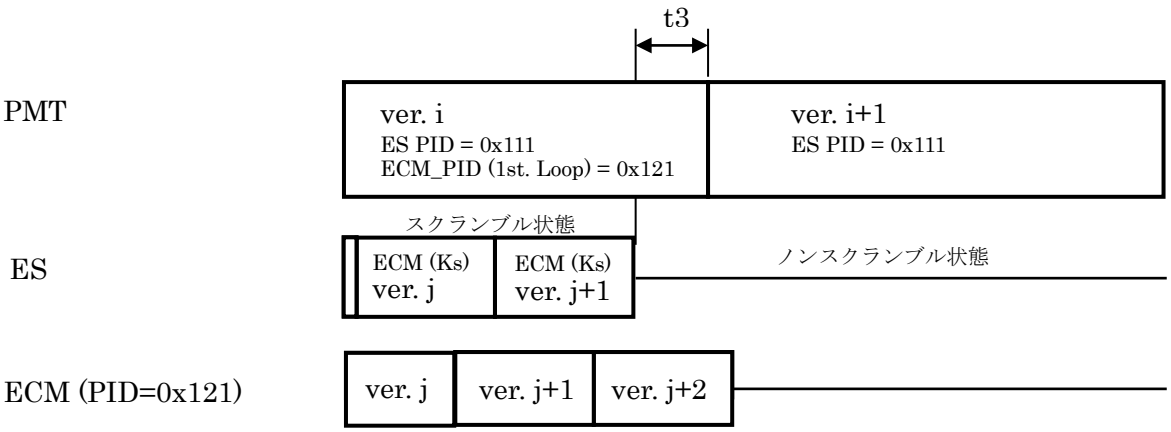


図 4-3　スクランブルの終了

1)　当該 ES（群）へのスクランブル動作が停止する。

2)　t3 秒後，PMT の第 1 ループに ECM と当該 ES（群）との関連が削除され、送出される。（PMT の更新）

t3=1

4.8.7.3　放送番組要素を伝送するESとECMとの関係の変更

(1)ECM_PID の変更を伴う場合

－　限定受信記述子が PMT の第 1 ループに記載されている場合に、放送番組要素を伝送する ES と既に PMT で記載されている ECM_PID との関係を変更する場合で、ECM_PID の変更が伴う場合には、以下のようなスクランブル状態からノンスクランブル状態への遷移手順を経ることとする。

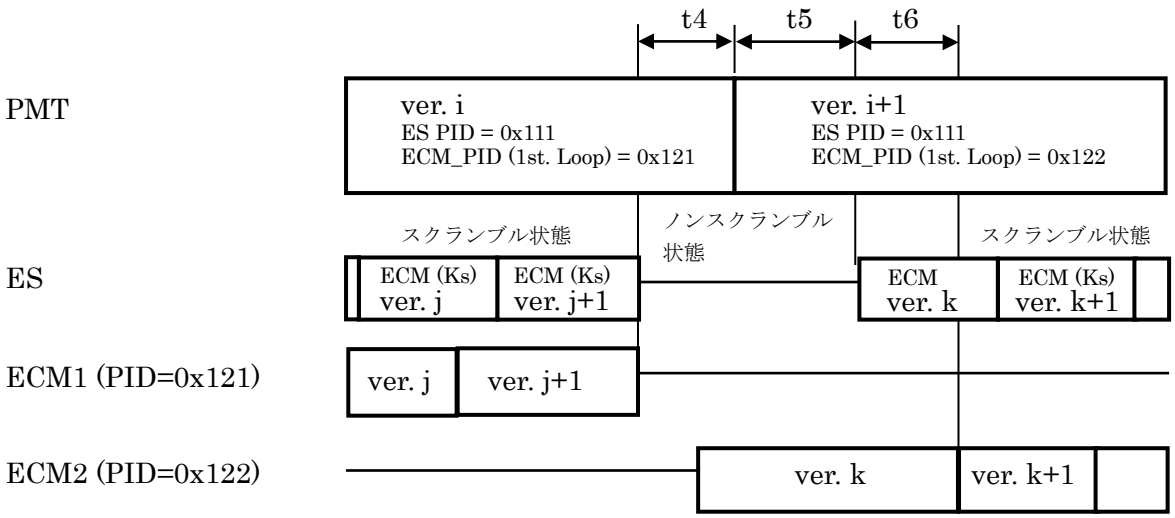


図 4-4　ECM_PID の変更を伴う場合

1)　すべての ES がノンスクランブル状態で送出される。

2)　新しい ECM が送出される。

3)　1)から t4 秒後、PMT が更新される

4)　PMT の更新から t5 秒後，ES にスクランブルが開始される。

5)　ES にスクランブルが開始されてから t6 秒後、最初の ECM の更新が行われる。

t4=1、t5= 2、0<t6

ECM の更新に関しては本編第二部の

4.8.8.2　更新・再送周期

4.8.8.3　ECM の更新とスクランブル鍵の変更

に準ずる。

(2)ECM_PID の変更を伴わない場合

- 限定受信記述子が PMT の第 1 ループに記載されている場合に、放送番組要素を伝送する ES と既に PMT で記載されている ECM_PID との関係を変更する場合で、ECM_PID の変更を伴わない場合には、スクランブル状態からノンスクランブル状態への遷移などの特別な送出手順を行う必要がない。
- 例として、新規 ES が追加される場合の放送信号の変化を以下に示す。

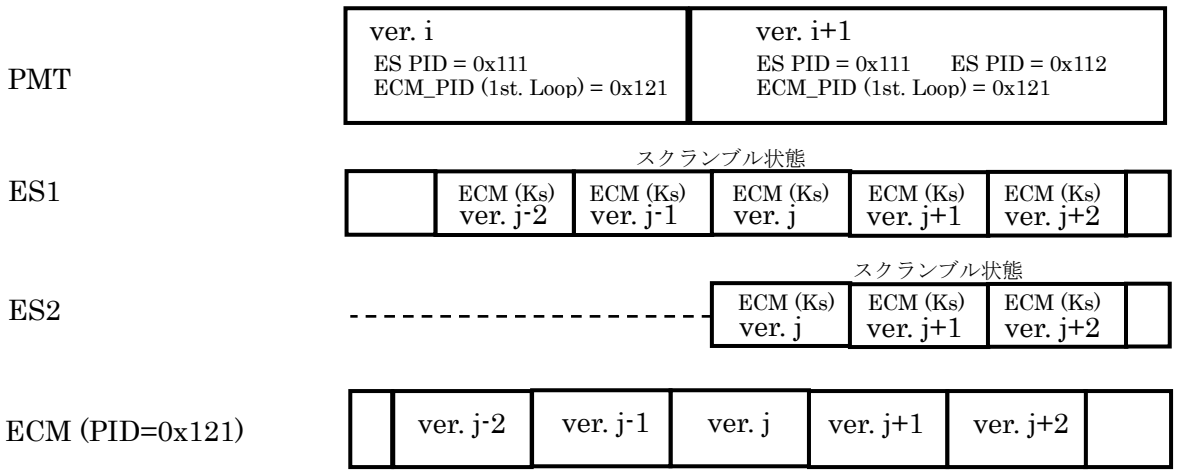


図 4-5　ECM_PID の変更を伴わない場合

4.8.7.4　ワーク鍵の更新

ワーク鍵更新によるECMの変更（ECMの暗号化鍵の変更）には、以下の3通りがある。

- 4.8.7.2 スクランブルの終了の手順にてノンスクランブル状態に移行した後に行われ、4.8.7.1 スクランブルの開始の手順にて新たな ECM が送出される。
- スクランブル制御や ECM 送出に影響を与えることなくシームレスにワーク鍵更新が行える場合は、ノンスクランブル状態に移行せずに、スクランブル状態のまま行うことも可能。
- PMT の更新を伴わないノンスクランブル状態でのワーク鍵更新を行う場合は、図 4-6 に示す手順にて実施するものとする。ES は一時的にノンスクランブルになるが、PMT は更新せず、ECM の送出も連続する。その間に ECM の変更が行われる。

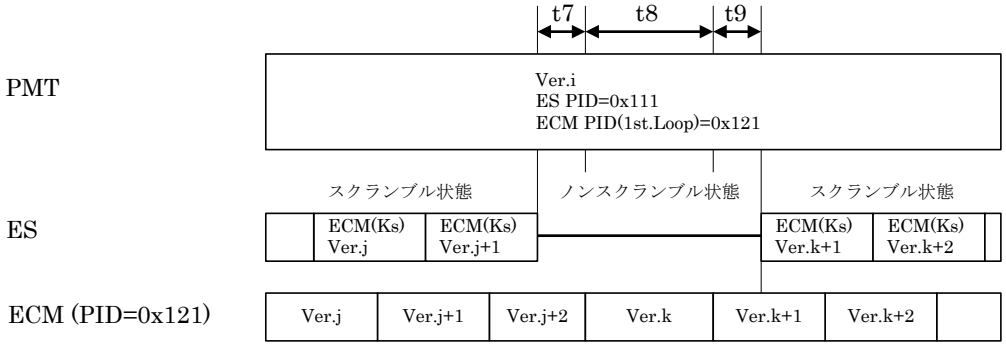


図 4-6　ワーク鍵更新の場合

1)　t7 経過後まで、もしくは、t7,t8 にて、ワーク鍵の更新を実施する

2)　 ECM の更新から 2 秒後（t9 経過後）より、ES にスクランブルが開始される。

t7≧0、t8>0、t9=2

4.8.8　ECMの更新・再送

－ ECM が適用される ES のスクランブル鍵が変更される場合には、スクランブル鍵の変更に先だって ECM が更新される。ECM の更新は拡張セクション形式のバージョン番号の変更により通知される。

4.8.8.1　スクランブル鍵の変更

－ ECM が適用される ES に施されるスクランブルの鍵（Ks）の変更は、当該 TS パケットヘッダ内のトランスポートスクランブル制御フラグを用いて行われる。スクランブル鍵の変更に伴って、常にトランスポートスクランブル制御フラグは変更される。偶数鍵から奇数鍵、奇数鍵から偶数鍵の順に変更され、同一鍵が続けて変更されることはない。

4.8.8.2　更新・再送周期

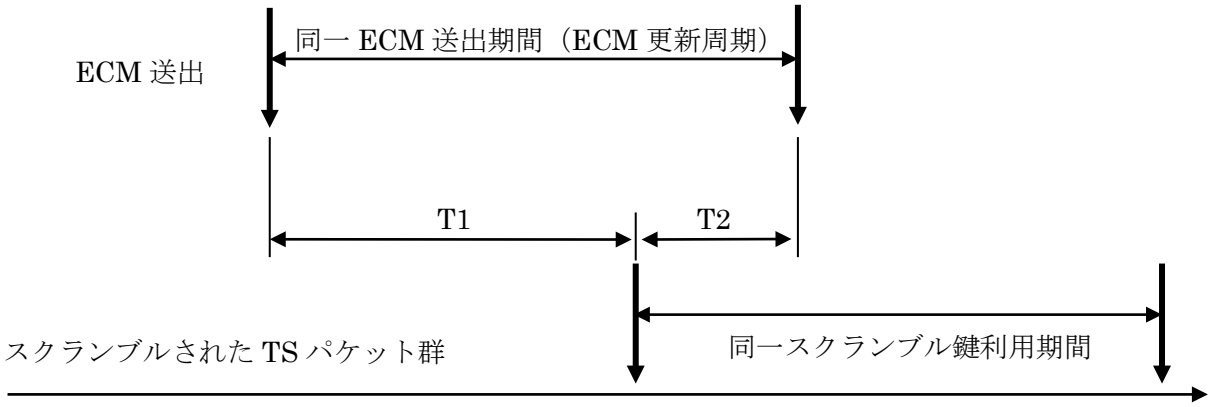
－ 下記に ECM の更新・再送周期の推奨値を記載する。本編第一部 A.4 に関連記載がある。

表 4-7　ECM 更新周期、再送周期の推奨値

	部分受信階層以外	部分受信階層
ECM 更新周期	2 s	運用しない
ECM 再送周期	100ms	運用しない

4.8.8.3　ECMの更新とスクランブル鍵の変更

－　単一で ECM が適用された場合の ECM の更新とスクランブル鍵の変更を下図に示す。



1600ms<T1、0<T2、T 1 ＋T2>2000ms

図 4-7　ECM の更新とスクランブル鍵の変更

－　複数の TS パケットに ECM が適用される場合には各パケットに対して T1、T2 ともに最小のものを適用する。

4.8.9　その他

4.8.9.1　ECMとスクランブル

- PMT の第 1、第 2 ループにアクセス制御記述子が記載されていない場合は、放送番組要素を伝送する ES 群すべてがスクランブル伝送されていないことを示す。
- 逆に PMT の第 1、第 2 ループにアクセス制御記述子が記載されていても、サービスを構成するすべてのコンポーネントがスクランブルされない運用も実施される（スクランブル放送からノンスクランブル放送への遷移状態や緊急ニュースなど人命に関わる緊急事態等の考慮)。
- 但し、ECM_PID=0x1FFF と関連づけられた ES にスクランブルが行われることはない。

4.8.9.2　ECMの途絶

(1) ECM の途絶の検出

各 ECM は 4.8.8.2 更新・再送周期 記載の条件で PMT に記載のある場合は再送されているので受信機は ECM が規定時間以内に受信できない場合に ECM の途絶を検出することができる（2 秒以内)。

(2) ECM の途絶時の受信機動作

ECM の途絶を検出した受信機は、放送番組を構成する TS パケットのヘッダ部のトランスポートスクランブル制御フラグを参照した動作を行う。

4.9 EMM

4.9.1 EMMの基本構成

- EMM は ARIB STD-B25 第 3 部 3.2.7.1 EMM の基本構成 に示すように、MPEG2 システムズのセクション形式にて伝送する。
- EMM 本体内のリザーブビットの運用は、送信側は 0 を送り、受信側は無視するものとする。

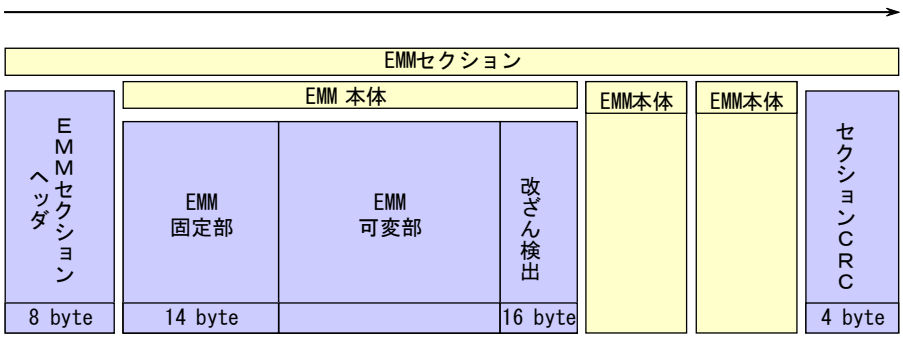


図 4-8 EMM セクション構成

4.9.2 EMMに配置する記述子

- EMM の可変部には、以下に示す記述子が配置される。
- ここで規定される記述子は、本編第二部でのみ適用される。
- ARIB STD-B25 第 3 部 3.2.7.2 表 3-12 に示される EMM 記述子のうち、
  - ワーク鍵設定記述子（tag 値＝0xF0）
  - F0 ワーク鍵設定記述子（tag 値＝0xF3）
  - ワーク鍵無効化通知記述子（tag 値＝0xF5）

  については運用しない。

表 4-8 EMM 記述子種類

記述子の種類	tag 値
デバイス鍵更新記述子	0xF1
ダミー記述子	0xF2
F1 ワーク鍵設定記述子	0xF4

4.9.3　EMMの種類

4.9.3.1　EMMの種類

(1)　ワーク鍵設定 EMM

- 初回視聴時やワーク鍵の定期更新時に送信する、ECM を復号化するために必要な情報として運用する。
- ワーク鍵設定 EMM には、F0 ワーク鍵設定 EMM と F1 ワーク鍵設定 EMM の 2 種類があるが、2 種類の ECM のうち ECM-F1 のみを運用することから、F1 ワーク鍵設定 EMM のみを運用する。F0 ワーク鍵設定 EMM は運用しない。

表 4-9　F1 ワーク鍵設定 EMM

説明				byte 数
EMM セクション	EMM セクションヘッダ			(8)
	EMM 本体 1	EMM ヘッダ	デバイス ID	8
			関連情報バイト長	1
			プロトコル番号	1
		固定部	RMP 事業体識別	2
			更新番号	2
		可変部（暗号化部）	F1 ワーク鍵設定記述子およびダミー記述子	38+N ※
		改ざん検出		16
	EMM 本体 2			
	EMM 本体 3			
	:			
	EMM 本体 n			
	CRC 誤り検出			(4)

※N はダミー記述子によって変化する

- デバイス ID については、4.9.3.2 参照のこと。
- 関連情報バイト長、プロトコル番号、RMP 事業体識別、更新番号については、STD-B25 第 3 部で規定される事項に従う。

－ STD-B25 第 3 部で規定される F1 ワーク鍵設定記述子は、表 4-10 のように運用する。

表 4-10　F1 ワーク鍵設定記述子の構成

説明	byte 数	備考
Descriptor tag	1	0xF4
Descriptor length	1	0x24
F1 ワーク鍵識別（Odd）	1	
F1Ks ポインタ（Odd）	1	
F1 ワーク鍵（Odd）	16	
F1 ワーク鍵識別（Even）	1	
F1Ks ポインタ（Even）	1	
F1 ワーク鍵（Even）	16	
合計	38	

（役割）

ECM-F1 の復号に必要な情報（F1 ワーク鍵識別、F1Ks ポインタ、F1 ワーク鍵）を伝送する。

（項目説明）

①F1 ワーク鍵識別（Odd/Even）

F1 ワーク鍵と F1Ks ポインタを識別するための情報で、0x00～0xFF の値が使用される。

②F1Ks ポインタ（Odd/Even）

送られた F1 ワーク鍵で復号すべき ECM-F1 のスクランブル鍵の番号（0～9）を示す。

③F1 ワーク鍵（Odd/Even）

ECM-F1 を復号するためのワーク鍵である。受信機は Odd/Even の 2 種類を局個別データの当該記憶領域に記憶しておく。RMP 事業体は 10 種類の F1 ワーク鍵を同時運用するが、各受信機はその内の 1 種類しか持たない。

－ ダミー記述子については、STD-B25 第 3 部で規定される構成に従う。

－ 可変部に配置されるワーク鍵設定記述子とダミー記述子は、表 4-8 に示す tag 値で識別される。配置される記述子の順番、および 1 つのダミー記述子の長さ、あるいは配置されるダミー記述子の個数は、実運用において不定であることに注意のこと。

(2) デバイス鍵更新 EMM

- デバイス鍵情報の更新処理が必要な場合に送信する情報として運用される。

表 4-11 デバイス鍵更新 EMM

説明				byte 数
EMM セクション	EMM セクションヘッダ			(8)
	EMM 本体 1	EMM ヘッダ	デバイス ID	8
			関連情報バイト長	1
			プロトコル番号	1
		固定部	RMP 事業体識別	2
			更新番号	2
		可変部（暗号化部）	デバイス鍵更新記述子およびダミー記述子	8+N ※
		改ざん検出		16
	EMM 本体 2			
	EMM 本体 3			
	:			
	EMM 本体 n			
	CRC 誤り検出			(4)

※Nはダミー記述子によって変化する

- デバイス ID については、4.9.3.2 参照のこと。
- 関連情報バイト長、プロトコル番号、RMP 事業体識別、更新番号については、STD-B25 第 3 部で規定される事項に従う。
- デバイス鍵更新記述子は、以下のような構成とする（STD-B25 第 3 部で規定のとおり）。

表 4-12 デバイス鍵更新記述子の構成

説明	byte 数	備考
Descriptor tag	1	0xF1
Descriptor length	1	0x06
ID 識別	1	0x02
世代番号	1	
デバイス鍵更新パラメータ	4	
合計	8	

（役割）

受信機に対してデバイス ID とデバイス鍵（Kd）の更新情報を伝送する。

（項目説明）

①ID 識別

更新する ID の識別番号を示す。ID 識別は、0x02（RMP メーカ ID）のみを運用する。

②世代番号

デバイス ID／デバイス鍵（Kd）の更新後の世代番号を示す。値の有効範囲は 0x01～0xFF とする。

③デバイス鍵更新パラメータ

受信機でデバイス鍵（Kd）の生成を行うためのパラメータ。

（注意事項）

デバイス鍵更新 EMM の伝送は、RMP メーカ ID について、オリジナルのデバイス ID に対してのみ伝送する。また、受信機で記憶する世代番号の初期値（デバイス ID／デバイス鍵の更新が行われていない状態）は 0x00 とする。

- ダミー記述子については、STD-B25 第 3 部で規定される構成に従う。
- 可変部に配置されるデバイス鍵更新記述子とダミー記述子は、表 4-8 に示す tag 値で識別される。配置される記述子の順番、および 1 つのダミー記述子の長さ、あるいは配置されるダミー記述子の個数は、実運用において不定であることに注意のこと。

4.9.3.2　デバイスIDの種類

- STD-B25 第 3 部で規定されるデバイス ID には、受信機メーカごとに管理される ID（RMP メーカ ID）と機種ごとに管理される ID（RMP 機種 ID）があるが、RMP メーカ ID のみを使用し、RMP 機種 ID は運用しない。
- メーカや機種を特定する受信機の識別番号。
  - ・bit63～bit61（3bit）　：RMP 機種 ID、RMP メーカ ID を識別する ID 識別で RMP 機種 ID は使用しない。
  - ・bit60～bit8 （53bit）　：機種、メーカの識別を示すデバイス ID 本体で、機種識別は使用しない。
  - ・bit7～bit0（8bit）　：世代番号（ID 本体の拡張部）

- 受信機は ID 識別（3bit）に対応するデバイス ID のデバイス ID 本体と世代番号（bit60～bit0）の一致を比較する。
- 1 セクション内で伝送する複数の EMM は同一 ID 識別とする。
- ID 識別は'010'（RMP メーカ ID に対する伝送）を使用する。デバイス ID の一部には世代番号が存在し、オリジナルのデバイス ID とデバイス鍵は世代番号＝0 であり、デバイス鍵更新記述子により世代更新が可能（最大 255 まで）。

4.9.4 EMMの送出仕様

4.9.4.1 EMMストリームの指定方法

RMP方式ではTypeA伝送形式のみの運用とする。

(1) 伝送形式の識別手段

- TypeA、TypeB の伝送形式は、CAT に記載されたアクセス制御記述子の private_data_byte 領域先頭 1 バイトに記述される。

表 4-13 CAT に記載したアクセス制御記述子の private_data_byte の先頭 1 バイト

値	意味
0x00	未定義
0x01	Type A
0x02	Type B（RMP 方式では運用しない）
0x03～FF	将来使用のためのリザーブ

- CAT に記載されたアクセス制御記述子の private_data_byte の 1 バイト目に EMM 伝送形式の識別情報が必ず記述される。
- CAT に記載されたアクセス制御記述子の private_data_byte の 1 バイト目に有効な EMM 伝送形式の識別情報値が記述されていない場合はあくまで例外処置のため、受信機での EMM 取得は保証されず、一切取得しない場合もあり得る。

4.9.4.2 EMM送出仕様

- CAT に記載されるアクセス制御記述子の private_data_byte 領域の先頭 1 バイトは、必ず TypeA を指定する。
- EMM セクションのヘッダ構成は平成 26 年総務省告示 第 233 号に基づく。
- EMM セクションはマルチセクションでは送出しない。
- 受信機は、EMM セクションのバージョン番号を参照しない。
- EMM の送出順序は、本編第二部 4.9.6 EMM 送出順序による。

4.9.5　EMM送出頻度

- 地上デジタルテレビジョン放送においては、EMM は全て番組用 TS で送り、専用 TS では送らない。本編第一部 A.3 に関連記載がある。
- EMM セクションの TS パケットレベルの送出頻度については、基本的な考え方は第四編に準ずる（ここでいう第四編に準ずる基本的な考え方とは、EMM の送出頻度を EMM セクションと EMM セクションの間隔で規定するのではなく、PSI/SI の運用規定にあわせて EMM セクションの伝送密度で規定することを意味する）。
- EMM セクションを伝送する場合、当該 PID の TS パケットを、32ms 単位に 1.28kB±100%の範囲で送出する。EMM セクションを伝送する TS パケットは、同一 PID で任意の 1 秒間あたり、320kbit を超えて伝送しない（上記における 320kbit において、1 つの EMM セクションのデータ量は 4KB とみなすものとする）。

4.9.6　EMM送出順序

- EMM は、1 セクションに複数個の情報が重畳されて伝送される。
- 受信機でのフィルタリング処理を容易にするために、同一セクション内に詰め込む EMM の配置順序に次のような運用制限を設ける。
  1) 先頭の EMM は、そのセクション内に含まれる最小のデバイス ID の EMM とする。
  2) 2 番目の EMM は、そのセクション内に含まれる最大のデバイス ID の EMM とする。
  3) 3 番目以降の EMM は、残りの EMM をデバイス ID 順（昇順）にソーティングして配置する。
- 1 セクション内に n 個の EMM があり、デバイス ID の小さい順に EMM_1，EMM_2，…，EMM_n であるとすると、次のような順序で配置される。

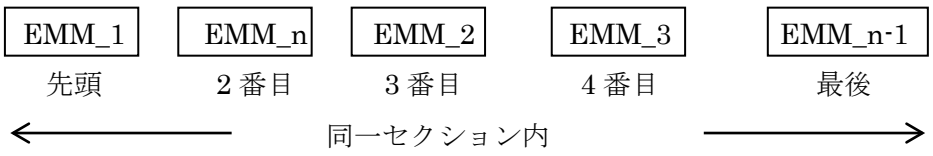


図 4-9　EMM の配置順序

- 受信機は、先頭 2 つの EMM を調べるだけで、自分宛の EMM がそのセクション内に含まれる可能性があるかないかを確定できる。さらに含まれる可能性がある場合でも、前から順番に見てゆき、自分の ID より大きくなった時点で自分宛 EMM は含まれないと確定

できる。自分宛 EMM が含まれないと確定した時点でセクション全体を廃棄でき、セクション内の最後の EMM まで比較する必要はない。

4.9.7　EMM送出の注意点

4.9.7.1　デバイス鍵更新EMM送出の制限

- デバイス鍵更新 EMM の伝送は、RMP メーカ ID について、世代番号＝0 でなければならない。すなわち、デバイス鍵更新 EMM の伝送は、オリジナルのデバイス ID に対してのみ送出可能である。一方、ワーク鍵設定 EMM は更新後の最新世代あてに送られる。よって、F1 ワーク鍵設定記述子とデバイス鍵更新記述子は別々の EMM に設定される。両 EMM が送られる場合、受信機はデバイス鍵更新 EMM を受信して世代更新し、その後に最新世代あてに送られてくるワーク鍵設定 EMM を受信することになる。

4.9.7.2　EMM常時送出

- 受信機は、地域により異なる放送局を受信するために、RMP 方式に関わるデータを放送局ごとに設定しなければならない。また、そのデータは放送局の運用に伴って更新される。受信機にそれらを全て事前設定することは不可能であり、受信機は初期スキャンや再スキャンのタイミングなどで最新データを取得する。そのために、放送局は最新のワーク鍵設定 EMM を常時送出しなければならない。
- また、デバイス鍵更新 EMM の送出により、デバイス ID とデバイス鍵の更新を行った場合には、更新実行後も、最新のデバイス鍵更新 EMM を常時送出する必要がある（在庫の受信機など、デバイス鍵更新 EMM を受信していない受信機があり得るため)。
- デバイス鍵の更新後は、対象受信機に対してデバイス鍵更新 EMM とワーク鍵設定 EMM が同時期に送出される。

4.9.7.3　EMMのPID

- CAT のアクセス制御記述子に記載する EMM_PID は送出マスター毎に固定値運用することが望ましい。受信機では、選局後、直ちに EMM の受信を開始できるようにアクセス制御記述子に記載された EMM_PID を受信機内に保持する実装が想定されるため、EMM_PID の変更は極力避けるべきである。やむを得ず EMM_PID の変更を行った場合には、変更後の EMM_PID が受信機に行き渡る相当期間をおいた後に、鍵更新運用を行うこと。

4.9.7.4　EMMの再送周期

- EMM の再送周期は、15 秒以下となるよう運用すること。
- EMM の再送周期とは、送出するすべての宛て先の EMM を一つのかたまりと見たときに、その一つのかたまりを繰り返し送出する周期である。
- 定常状態では、EMM の再送周期は、送出している EMM の内、任意のある 1 つのデバイス ID 宛ての EMM に着目したときに、そのデバイス ID 宛てに同一種類の EMM を繰り返し送出する間隔に等しい。
- 一つのデバイス ID に対して、デバイス鍵更新 EMM とワーク鍵設定 EMM を送る場合は、1 周期の中にその両方の EMM を含むものとする。なお、この場合でも、STD-B25 第 3 部参考 1 別表 2 に示される EMM の伝送条件の「同一受信機への EMM 送信最小間隔」に従い、デバイス鍵更新 EMM とワーク鍵設定 EMM の間は、1 秒以上の間隔を開けること。

4.10 鍵更新の運用

- RMP 方式のメンテナンス（セキュリティ維持)、あるいは特定の鍵の無効化を目的として、4.10.1 から 4.10.4 に示す鍵更新の運用を行う場合がある。
- 特定 RMP メーカ ID のデバイス鍵の無効化を目的とした鍵更新運用については、関連する記載が本編第二部 A.3 にある。

4.10.1 メンテナンスを目的としたワーク鍵の更新

- 定期的あるいは随時に実施されるワーク鍵の更新運用。
- 運用例：

ワーク鍵設定 EMM で送出中のワーク鍵ペア（Odd,Even）＝（A,B）に対し、ECM の暗号化に使用するワーク鍵を A から B に更新するとともに、新たなワーク鍵設定 EMM を送出し将来使用予定の新たなワーク鍵（C）を含むワーク鍵ペア（C,B）を設定する。

4.10.2 特定のワーク鍵の無効化を目的としたワーク鍵の更新

- 漏えいしたワーク鍵の無効化等を目的として実施されるワーク鍵の更新運用。
- 漏洩したワーク鍵のみを不正に使用した受信機は新たなワーク鍵を取得できないため、番組視聴ができなくなる。
- 運用例：

(1) ワーク鍵設定 EMM で送出中のワーク鍵ペア（Odd,Even）＝（A,B）に対し、ECM の暗号化に使用するワーク鍵を A から B に更新するとともに、新たなワーク鍵設定 EMM を送出し新たなワーク鍵（C）を含むワーク鍵ペア（C,B）を設定する。

(2) その後、新たなワーク鍵（C）が受信機に行き渡る相当期間をおいて、ECM の暗号化に使用するワーク鍵を B から C に更新するとともに、新たなワーク鍵設定 EMM を送出し将来使用予定の新たなワーク鍵（D）を含むワーク鍵ペア（C,D）を設定する。これにより漏えいしたワーク鍵（A および B）が無効化される。

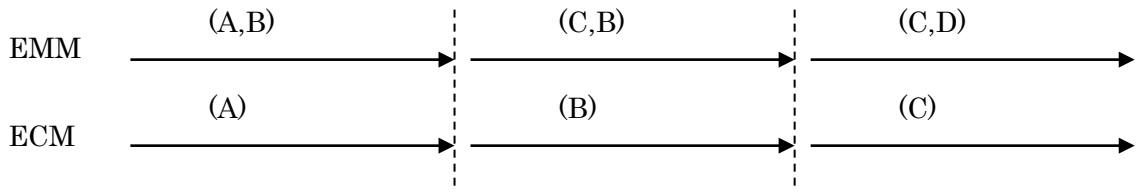


図 4-10　特定のワーク鍵の無効化を目的としたワーク鍵更新の運用フロー例

4.10.3 メンテナンスを目的としたデバイス鍵の更新

- メンテナンスを目的として実施されるデバイス鍵の更新運用。デバイス鍵の更新と同時にワーク鍵の更新を行う運用と行わない運用の両方が想定される。
- 運用例（ワーク鍵同時更新なしの場合）：

ワーク鍵設定 EMM で送出中のワーク鍵ペア（Odd,Even）＝（A,B）に対し、全てあるいは特定の RMP メーカ ID に向けたデバイス鍵更新 EMM を送出し RMP メーカ ID とデバイス鍵を更新するとともに、更新後の RMP メーカ ID に対して新たなワーク鍵設定 EMM を送出しワーク鍵ペア（A,B）を設定する。

4.10.4 特定のデバイス鍵の無効化を目的としたデバイス鍵の更新

- 漏えいした特定のデバイス鍵の無効化等を目的として実施されるデバイス鍵の更新運用。
- 漏洩元受信機からデバイス鍵更新の実行モジュール（もしくはアルゴリズム）が漏れていなければ、当該受信機メーカ（RMP メーカ ID）の受信機は視聴可能のまま、漏洩情報を不正に使用した受信機は新たなワーク鍵を取得できないため、番組視聴ができなくなる。
- 運用例（ワーク鍵同時更新なしの場合）：

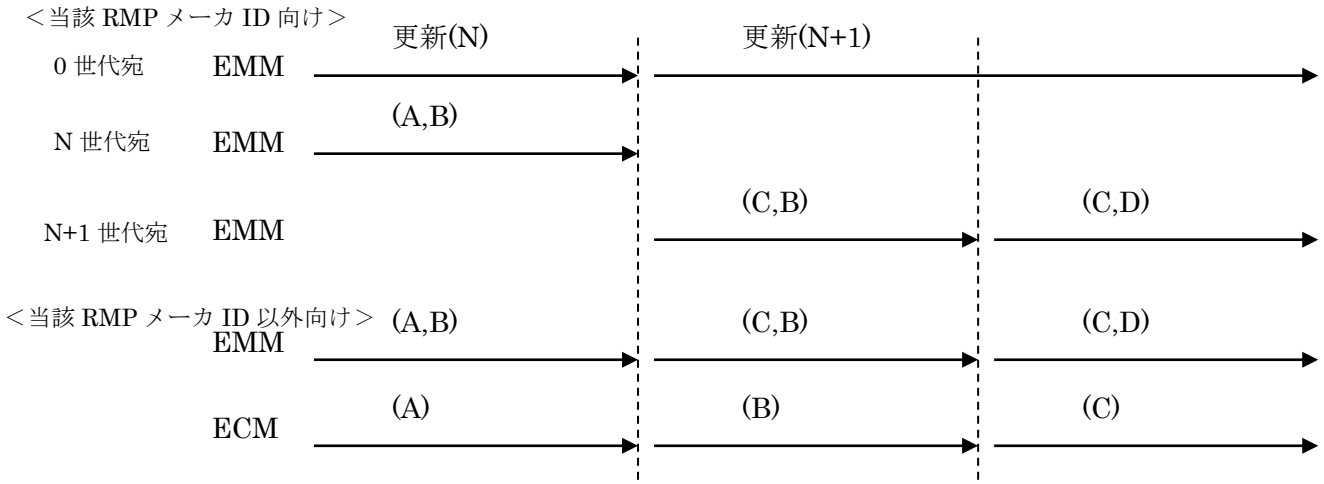
(1) ワーク鍵設定 EMM で送出中のワーク鍵ペア（Odd,Even）＝（A,B）に対して、以下の動作を同時に実施する。

①ECM の暗号化に使用するワーク鍵を A から B に更新する。

②当該 RMP メーカ ID に対してデバイス鍵更新 EMM を送出し、RMP メーカ ID とデバイス鍵を更新する。

③全ての RMP メーカ ID（当該 RMP メーカ ID は更新後のもの）に対して新たなワーク鍵設定 EMM を送出し、新たなワーク鍵（C）を含むワーク鍵ペア（C,B）を設定する。

(2) その後、新たなワーク鍵（C）が受信機に行き渡る相当期間をおいて、ECM の暗号化に使用するワーク鍵を B から C に更新するとともに、当該 RMP メーカ ID に対して新たなワーク鍵設定 EMM を送出し、将来使用予定の新たなワーク鍵（D）を含むワーク鍵（C,D）を設定する。これにより漏えいしたデバイス鍵（更新前のもの）が無効化される。



※RMP メーカ ID およびデバイス鍵を第 N 世代から第 N+1 世代へ更新する場合のフロー例

図 4-11　特定のデバイス鍵の無効化を目的としたデバイス鍵更新の運用フロー例

4.11　EMMメッセージ

－　(T.B.D)。本編第二部 解説 A.10 に関連記載がある。

4.12　CA_代替サービス

－　RMP 方式においては、CA 代替サービスの運用は行わない。

4.13　CA_EMM_TS記述子の運用

－　地上デジタルテレビジョン放送においては、EMM は全て番組用 TS で送り、専用 TS では送らないので、CA_EMM_TS 記述子の運用は行わない。

4.14 サイマルクリプト運用

- コンテンツ保護を伴う無料放送を ARIB STD-B25 第 1 部　受信時の制御方式（限定受信方式）に基づいて本規定第五編第一部に規定する方式（以下、CA5 方式）と ARIB STD-B25 第 3 部　受信時の制御方式（コンテンツ保護方式）に基づいて本規定第五編第二部に規定する方式（以下、RMP 方式）の 2 方式でサイマルクリプト運用する場合に、送出側が遵守すべき運用事項を定める。

4.14.1 ECMの送出

コンテンツ保護を伴う無料番組では ECM を次のように送出する。

- コンテンツ保護を伴う無料番組においては、サイマルクリプト運用のために、CA5 方式の ECM と RMP 方式の 2 種類の ECM を並行して送出する。
- CA5 方式の ECM と RMP 方式の ECM の両方で同一の Ks の伝送を行う。
- PMT には、CA5 方式の限定受信方式記述子と RMP 方式のアクセス制御記述子を記載すること。
- 番組内のコンポーネントにスクランブル ES とノンスクランブル ES とが混在する場合を考慮し、PMT における CA5 方式の限定受信方式記述子と RMP 方式のアクセス制御記述子の配置を以下のように定める。
  1) 限定受信方式記述子とアクセス制御記述子を PMT の第 1 ループに必ず 1 つずつ配置する。この場合、番組内のすべてのコンポーネントに対しそれぞれの ECM が適用される。
  2) 限定受信方式記述子とアクセス制御記述子を PMT の第 2 ループには配置しない。ただし、デフォルト ES 群以外でノンスクランブル運用する場合に限り、CA_PID フィールドに無効な ECM_PID=0x1FFF を記述した限定受信方式記述子とアクセス制御記述子を配置する。なお、第 2 ループに配置する CA5 方式の限定受信方式記述子と RMP 方式のアクセス制御記述子が指し示す ES は同一である。

4.14.2 EMMの送出

1TS 内でどのような種類の放送を運用するかにより、以下のように送出が変わる。

なおコンテンツ保護を伴う無料放送のための EMM は、各アクセス制御方式の運用によって送出する場合と送出しない場合がある。RMP 方式の EMM は必ず送出されるが、CA5 方式の EMM は運用によって送出しない場合がありうる。

(1) コンテンツ保護を伴う無料番組を運用する放送局の送り方

(1-1)RMP 方式の EMM だけを送る場合（CA5 方式の EMM を送らない場合）

- CAT には RMP 方式のアクセス制御記述子のみを記載して送出する。
- EMM を送出する時間帯に特に制限はなく、ノンスクランブルの時間帯も含めて、通常は常時繰り返して送出される。
- 伝送形式は TypeA とし、伝送レートは 320kbit/s 以下とする（送出頻度については 32ms 単位に 1.28kB±100%の範囲で送出する）。その他の送出仕様については、本編第二部に記載の運用事項に従う。

(1-2) CA5 方式と RMP 方式の両方の EMM を送る場合

- CAT には CA5 方式の限定受信方式記述子と RMP 方式のアクセス制御記述子を記載すること。
- 両方式の EMM は並行して送出する。それらの EMM を送出する時間帯に特に制限はなく、ノンスクランブルの時間帯も含めて、通常は常時繰り返し送出される。
- 伝送形式は TypeA とし、両方式で同一とする。
- 伝送レートは CA5 方式と RMP 方式の両方の合計で 320kbit/s 以下とする（送出頻度については、CA5 方式と RMP 方式の両方の合計が本編第一部 4.11 に記載する送出頻度を超えないものとする。すなわち、それら 2 方式の TS パケットを合わせて 32ms 単位に 1.28kB±100%の範囲で送出する）。
- その他の送出仕様については、CA5 方式の EMM は本編第一部に記載の運用事項に従い、RMP 方式の EMM は本編第二部に記載の運用事項に従うものとする。同一受信機への EMM 送信間隔を 1 秒以上とする条件などは、同一方式の EMM の中で遵守される。

(2) 運用の一例

以下に上記(1-1) RMP 方式の EMM だけを送る場合の運用の一例を示す。

（想定する運用例）

- 部分受信階層以外でコンテンツ保護を行う無料番組を運用する。CA5 方式と RMP 方式のサイマルクリプトを行うが、CA5 方式の EMM は送らない。

（上記運用例での関連情報の送り方）

- 部分受信階層以外で送るもの
  1) CA5 方式の限定受信方式記述子と RMP 方式のアクセス制御記述子を記載した PMT（部分受信階層以外用）
  2) CA5 方式の ECM
  3) RMP 方式の ECM
  4) RMP 方式の EMM
- 部分受信階層で送るもの

1)　RMP 方式のアクセス制御記述子を記載した CAT

5　受信機への要求仕様

本章ではコンテンツ保護方式の処理機能を備えた受信機への要求仕様について記述するが、各項目の処理方法については、受信機をモデル化し、その動作を記述することによって均一な仕様理解を提供することを目的とした記載としており、受信機の設計、製造を制限するものではない。さらに、フローチャートについても詳細動作や過渡的な動きよりむしろ、本来の受信機動作を中心として記載している。受信機設計／製造に関してはその点十分に留意して頂きたい。

5.1　受信機の構成

－　図 5-1 に RMP 方式に関わるハードウェア構成を示す。ここでは、あくまで仕様を説明するためのモデル構成であり、実際の構成は受信機の設計による。

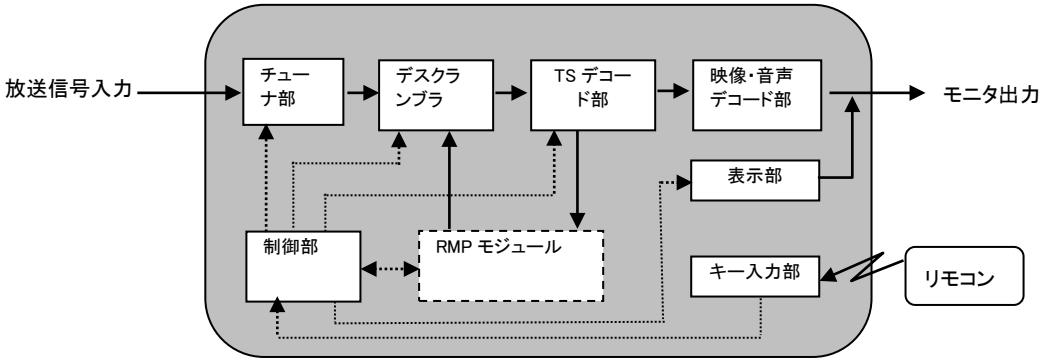


図 5-1　受信機の基本構成

(1)　チューナ部

－　制御部からの制御で放送信号の受信と選択を行い、伝送信号のパケット処理、エラー訂正処理を行う。

(2)　デスクランブラ

－　制御部からの制御で、MULTI2 方式による特定パケットのデスクランブルを行う。

－　コンポーネントのスクランブルの判定は、TS パケットヘッダ中の transport_scrambling_control フィールドにしたがうこと。

－　ARIB STD-B25 第 3 部の下記を参照。

第 2 章　　2.2.4　　デスクランブラ

(3)　TS デコード部

－　TS 多重された信号から必要なパケットを分離し、放送番組信号の選択、各種多重データ（各種 SI データ、ECM、EMM 等）の分離を行う。

(4) 映像音声デコード部

- 映像、音声のデコードを行いモニタに出力する。

(5) 表示部

- ユーザに対するデバイス ID 情報、ECM/EMM 復号化時のエラー等を表示するための画面提示手段、ユーザインタフェースを搭載する。

(6) キー入力部

- リモコンからのキー入力処理を行う。

(7) 制御部

- 受信機全体の制御を行う。

(8) RMP モジュール

- TS デコード部より出力される ECM、EMM を入力とし、ECM の暗号復号処理機能、EMM の暗号復号処理機能、デバイス鍵更新処理機能、デバイス鍵更新アルゴリズム、不揮発性メモリ機能等を有することで、デスクランブルに必要な情報をデスクランブラに出力する機能を有する RMP 方式にかかわる仮想的な機能モジュール。
- RMP モジュールは表 5-1 に示す共通データおよび表 5-2 示す局個別データを保持し、管理する機能を有する。

5.2 ユーザインタフェース

- ユーザインタフェースの詳細については商品企画による。

5.3 通電制御

5.3.1 EMMの指定による通電制御

- RMP 方式における EMM に通電制御機能はない。したがって受信機に対する要求仕様はない。

5.3.2 CA_EMM_TS記述子による通電制御

- RMP 方式では、CA_EMM_TS 記述子の運用を行わない。したがって受信機に対する要求仕様はない。

5.4 有効な限定受信方式

- 複数の限定受信方式が運用される場合があるが、限定受信方式の区別は CA_system_id によって行う。
- 本編第二部で規定する RMP 方式の CA_system_id の値は 0x000E である。

- 本編第二部で定める受信処理を行う場合、複数の CA_system_id が CAT や PMT に記載されている場合でも、本編第二部で規定する CA_system_id と整合した値であれば、有効な限定受信方式と判断する。
- PMT におけるアクセス制御記述子において、本編第二部で規定する CA_system_id と整合しないサービスであっても誤動作を行わないように配慮し、本編第二部 5.16 で規定するエラー表示を行うこと。

5.5 コンテンツ保護を伴う無料番組の予約

- コンテンツ保護を伴う無料番組の EIT の free_CA_mode は 0 である。
- free_CA_mode=0 の場合は無条件に予約可能とみなす。
- 番組視聴のためには局個別データが必要であり、局個別データがないと予約が実行できない。したがって、予約時において局個別データが記憶設定されているかを確認することが望ましい。

5.6 コンテンツ保護された番組のコピー制御

- コピー制御方式については、本書　第八編を参照のこと。
- PSI/SI におけるコピー制御情報については第四編、第八編を参照のこと。

5.7 自動表示メッセージ表示

- （T.B.D）。本編第二部 解説 A.10 に関連記載がある。

5.8 メール

- RMP 方式はメール機能を具備しない。したがって受信機に対する要求仕様はない。

5.9 パレンタルコントロール（視聴年齢制限）

- パレンタルコントロール機能は運用しない。したがって受信機に対する要求仕様はない。

5.10 CA代替サービス

- RMP 方式は CA 代替サービスを対象としない。したがって受信機に対する要求仕様はない。

5.11 字幕・文字スーパーのスクランブルと表示優先順位

5.11.1 字幕

- デフォルト ES 群がスクランブル状態における字幕の表示に関しては、基本的に受信機商品企画とする。ガイドラインとして、字幕コンポーネントのスクランブル状態に関係な

く、デフォルト ES 群が正常にデスクランブルされた場合にのみ表示されることが望ましい。

5.11.2 文字スーパー

- デフォルト ES 群がスクランブル状態における文字スーパーの表示に関しては、基本的に受信機商品企画とする。

5.12 記憶データ

- 本節では、本コンテンツ保護方式に関連する受信機に記憶するデータを規定する。本節の内容は STD-B25 第 3 部に規定されているが、ECM 等の運用が変わったので、改めて本節で規定する。
- なお、本規定は説明のための機能であり、受信機の設計を物理的に制限するものではない。

5.12.1 記憶データの区分

- 本コンテンツ保護方式に関し、不揮発性メモリに記憶するデータには、全ての放送局に共通で受信機で 1 種類管理する「共通データ」と、放送局ごとに独立して記憶管理する「局個別データ」がある。

5.12.2 共通データ

- 全放送局に共通のデータとして表 5-1 に示すデータがある。
- 表 5-1 に示す全ての共通データを、不揮発性メモリに記憶する。実装にあたっては、5.17 実装基準 を満たすこと。全ての共通データは、受信機の設計、または製造時に指定のデータを記憶し、受信機の初期化等においてクリア（消去）されないこと。

表 5-1　共通データ

項目	長さ	データ種別	備考
MULTI2 暗号（スクランブルサブシステム）のシステム鍵	32 Byte	システム全体で共通	
MULTI2 暗号（スクランブルサブシステム）の CBC 初期値	8 Byte	システム全体で共通	
関連情報暗号化の CBC 初期値 0	16 Byte	システム全体で共通	プロトコル番号の上位 2bit=00B に対応
関連情報暗号化の CBC 初期値 1	16 Byte	システム全体で共通	プロトコル番号の上位 2bit=01B に対応
関連情報暗号化の CBC 初期値 2	16 Byte	システム全体で共通	プロトコル番号の上位 2bit=10B に対応
関連情報暗号化の CBC 初期値 3	16 Byte	システム全体で共通	プロトコル番号の上位 2bit=11B に対応
オリジナルの RMP メーカ ID	8 Byte	受信機メーカごとに独自	上位 3bit は 010B 下位 1B は 0x00
RMP メーカ ID に対するオリジナルのデバイス鍵	16 Byte	受信機メーカごとに独自	
RMP メーカ ID に対する EMM の改ざん検出鍵	16 Byte	受信機メーカごとに独自	
合計	144 Byte		

5.12.3 局個別データ

- 放送局個別のデータであり、図 5-2 に示すデータを受信した放送局（ネットワーク／トランスポートストリーム）ごとに記憶管理する。
- 局個別データは、RMP 事業体識別ごとに記憶管理するのではなく、あくまでも放送局（ネットワーク／トランスポートストリーム）ごとに管理する。従って、同一の RMP 事業体識別のデータであっても、異なるトランスポートストリームであれば別々に記憶管理する必要がある。
- 異なる周波数で同一のネットワーク／トランスポートストリームを受信した場合は、いずれか 1 つの局個別データを記憶管理すればよい。

- 局個別データの組数、記憶設定方法等は、規定しない。また、例えば受信機購入時の放送局信号の受信設定方法など、受信機の商品企画、基本動作に左右されるので、具体的な記憶設定の方法については規定しない。ただし、EMM を受信して該当する放送局の局個別データを設定しないと、その放送局の番組は視聴できないので注意を要する。
- 局個別データの 1 放送局分の詳細を表 5-2 に示す。表 5-2 に示す全ての局個別データを、不揮発性メモリに記憶する。実装にあたっては、5.17 実装基準 を満たすこと。
- 全ての局個別データは、製造出荷時もしくは本書第二編 6.2.1 初期スキャン、および、本書第二編 6.2.5.7 ユーザー設定情報のクリア機能 に示す初期化時において、0 に初期化する。

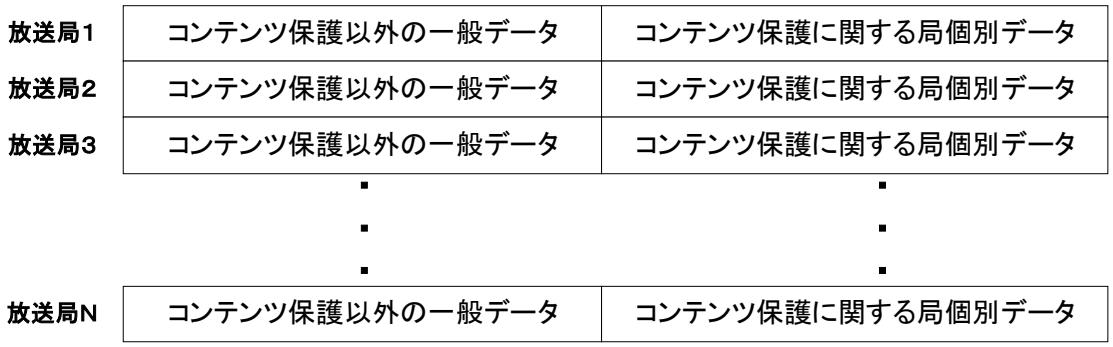


図 5-2　局個別データの記憶イメージ

表 5-2　局個別データ

項目	長さ	データ種別	備考
RMP 事業体識別	2　Byte	全ての EMM 受信時に設定	
RMP メーカ ID の世代番号	1　Byte	デバイス鍵更新記述子を含む EMM 受信時に設定	（注 1）、（注 2）
RMP メーカ ID のデバイス鍵更新パラメータ	4　Byte	デバイス鍵更新記述子を含む EMM 受信時に設定	（注 1）
更新番号	2　Byte	全ての EMM 受信時に設定	
F1 ワーク鍵識別（Odd）	1　Byte	ワーク鍵設定記述子を含む EMM 受信時に設定	
F1Ks ポインタ（Odd）	1　Byte	ワーク鍵設定記述子を含む EMM 受信時に設定	
F1 ワーク鍵(Odd)	16　Byte	ワーク鍵設定記述子を含む EMM 受信時に設定	

F1 ワーク鍵識別（Even）	1 Byte	ワーク鍵設定記述子を含む EMM 受信時に設定	
F1Ks ポインタ（Even）	1 Byte	ワーク鍵設定記述子を含む EMM 受信時に設定	
F1 ワーク鍵(Even)	16 Byte	ワーク鍵設定記述子を含む EMM 受信時に設定	
合計	45 Byte		

（注 1）

デバイス ID の世代番号、デバイス鍵更新パラメータを記憶することを示すが、この場合、EMM を受信するごと、または放送を選局するごとなどに、共通データ内のオリジナルのデバイス ID、デバイス鍵から指定された世代のデバイス ID とデバイス鍵を演算で求める必要がある。演算時間等が問題であれば、演算した結果を記憶しても良い。

（注 2）

デバイス ID の世代番号が 0 の場合、EMM によるデバイス ID の更新パラメータを受信しておらず、局個別のデバイス ID が設定されていないことを意味する。

（注 3）

表 5-2 に掲げた項目は、受信機を本コンテンツ保護方式に対応させるために必要最小限のデータであり、例えば鍵更新の際に受信不可となる時間を短縮するために EMM の PID を一時的に記憶するなど、商品企画のために受信機設計を制限するものではない。

5.13 ECMの受信処理

5.13.1 ECMの受信とデスクランブル

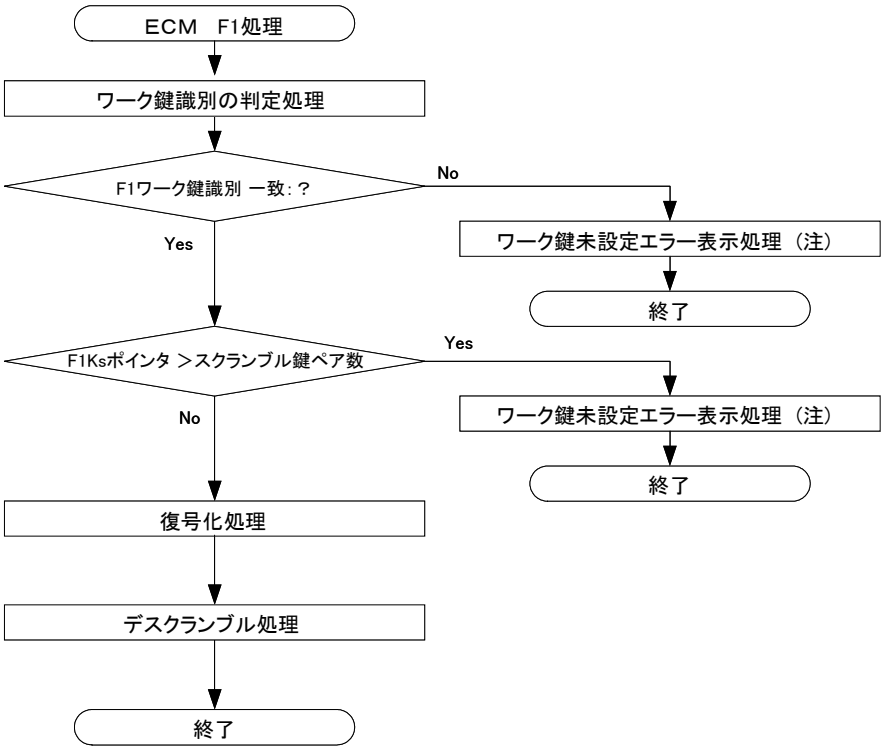
- 当該の放送局における局個別データによって ECM を処理し、デスクランブル処理する。
- すべての ES がノンスクランブル運用（緊急ニュースなど人命に関わる緊急事態）の場合は、ECM の受信の有無に関わらず、映像、音声等をデコードし提示すること。なお、すべての ES がノンスクランブル運用かどうかの判定は、表 4-3 によりデフォルト ES 群を監視すればよい。

5.13.2 ECMの受信処理とEMMの受信処理の競合

- ECM の受信処理と EMM の受信処理の競合に注意すること（注）。
- 具体的な対応例としては、ECM の受信処理時に参照する局個別データが、参照中に発生した EMM の受信処理により、書き換わってしまうことが無いように保護するなどが考えられる。
- なお、競合への対応方法は受信機商品企画による。関連する記載が 5.14.4 にある。

（注）ARIB STD-B25 第 3 部に記載の Kw 漏洩元検出のためのシステムにおいて、個別化された Kw は、一般的な 3 重鍵構造の Kw と同様に、Odd/Even 構成となっており、EMM による Kw の切り替え時の変化は Odd/Even のいずれか一方である。しかしながら、EMM による切り替え時に Ks ポインタの変更があると Odd/Even ともに変化する場合がある。その場合であっても、この ECM の受信処理と EMM の受信処理の競合に注意すれば、映像・音声等のデスクランブルができない状況にはならない。

5.13.3 ECM処理の流れ



(注)スクランブル無しの場合には、エラー表示しないこと 。

図 5-3　ECM 処理の流れ

5.14　EMMの受信処理

EMMの受信は、EMMセクションヘッダのテーブル識別によりフィルタリングして、テーブル識別0x84のEMMセクションのみを処理し、それ以外のEMMセクションは無視すること。

5.14.1 RMP方式を運用している放送局（TS）を初めて受信する場合のEMM処理

- 以下に本 EMM 処理の例を示す。なお EMM の受信タイミングを含めて、詳細は商品企画によるものとする。

- まず当該放送局の EMM を受信し、当該放送局（当該の TS）における局個別データの記憶設定を行なう必要がある。受信機は初期スキャン時などに CAT を受信し、CAT のアクセス制御記述子の記載状況により、EMM 送出の有無を判断する。EMM が送られている場合、自身宛すなわち自身に定義された RMP メーカ ID の EMM を受信する。
- 受信した自身宛の EMM がデバイス鍵更新の EMM であった場合は、更新したデバイス ID にて再度 EMM（ワーク鍵設定の EMM）を取得する。この場合、デバイス鍵更新の EMM とワーク鍵設定の EMM は、最短 1 秒の間隔で届く可能性がある為、受信機側では、デバイス鍵更新 EMM を受け取った場合、1 秒以内にデバイス鍵更新の処理を行い、ワーク鍵設定 EMM を受信する準備ができていることが望ましい。デバイス鍵更新処理に 1 秒以上かかる場合は、受信に要する時間が長くなる可能性がある。なお、本編第二部 A.8 に関連記載がある。
- ただし、局個別データの記憶設定を行なっても受信機の特定の鍵の無効化がなされた場合は、EMM を受信しても最新のワーク鍵を取得できないため番組受信できない。

5.14.2 通常時のEMM受信処理

- 受信機は本編第二部 5.14.5 で規定する処理に従い、常時 EMM を監視し、自身宛の EMM を処理しなければならない。自身宛の EMM とは、自身に定義された RMP メーカ ID の EMM のことである。
- 長期間当該 TS を受信していない場合は、当該 TS のワーク鍵の更新に追従できていない場合がありうる。その状態で当該 TS を選局した場合、最新のワーク鍵を取得して番組提示が可能になるまでに、最大で、EMM の再送周期の最大値に加えて 2 秒程度の時間を要することがある（2 秒には、デバイス鍵更新 EMM を受信してからワーク鍵設定 EMM を受信するまでの時間と、受信した EMM を処理する時間を含む)。ワーク鍵未設定に関するエラーメッセージについては、本編第二部 5.16.1 を参照のこと。なお、本編第二部 A.8 に関連記載がある。

5.14.3 RMP事業体識別が変更された場合の処理

- 当該 TS の EMM を受信して、自身宛ての EMM を受信した場合、すでに記憶設定した RMP 事業体識別と異なる RMP 事業体識別の EMM を受信する場合がある（放送局の系列の変更等)。その場合は、本編第二部 5.14.5 に従い、局個別データの初期化処理を行なわねばならない。

5.14.4 ECMの受信処理とEMMの受信処理の競合

- ECM の受信処理と EMM の受信処理の競合に注意すること。関連する記載が 5.13.2 にある。

5.14.5 EMM処理の流れ

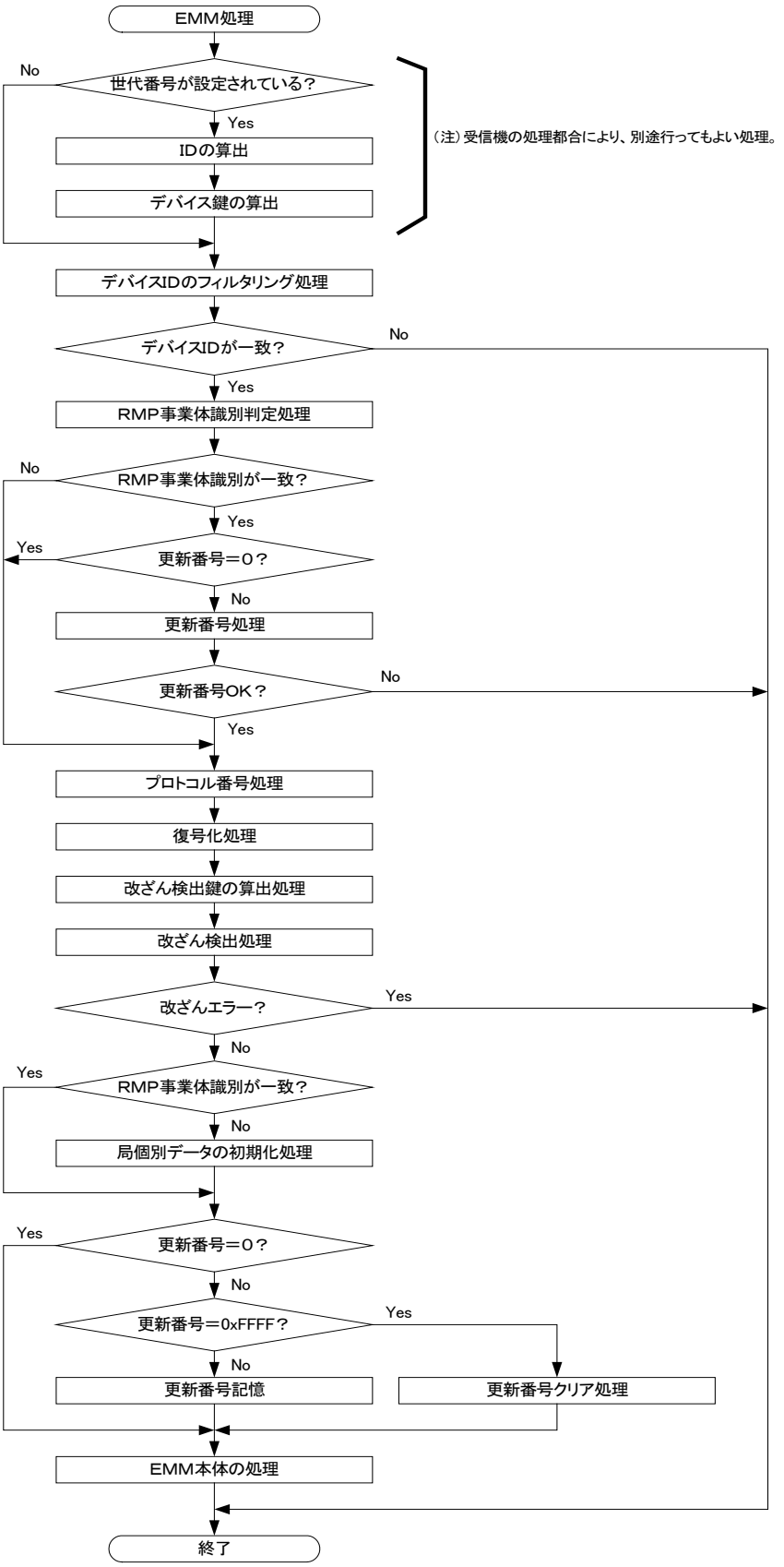


図 5-4　EMM 処理の流れ

5.14.6 デバイス鍵の更新

- デバイス鍵の更新については、ARIB STD-B25 第 3 部「4.8.3.2 デバイス ID とデバイス鍵の算出処理」を参照のこと。
- デバイス ID のフィルタリング処理について、最小で 1 種、デバイス鍵更新 EMM が伝送されデバイス ID／デバイス鍵更新が行われている場合には、最多で 2 種の ID（RMP メーカ ID）のフィルタリングを行う。
  （1）オリジナルな共通データに記憶する RMP メーカ ID
  （2）放送局毎に生成された最新世代の RMP メーカ ID（デバイス鍵更新 EMM で世代番号とデバイス鍵更新パラメータが設定されている時）
- EMM 内の ID（64bit）と、1～2 種の ID を比較し、一致した場合には EMM の処理を行い、全て一致しない場合には受信した EMM は破棄する。

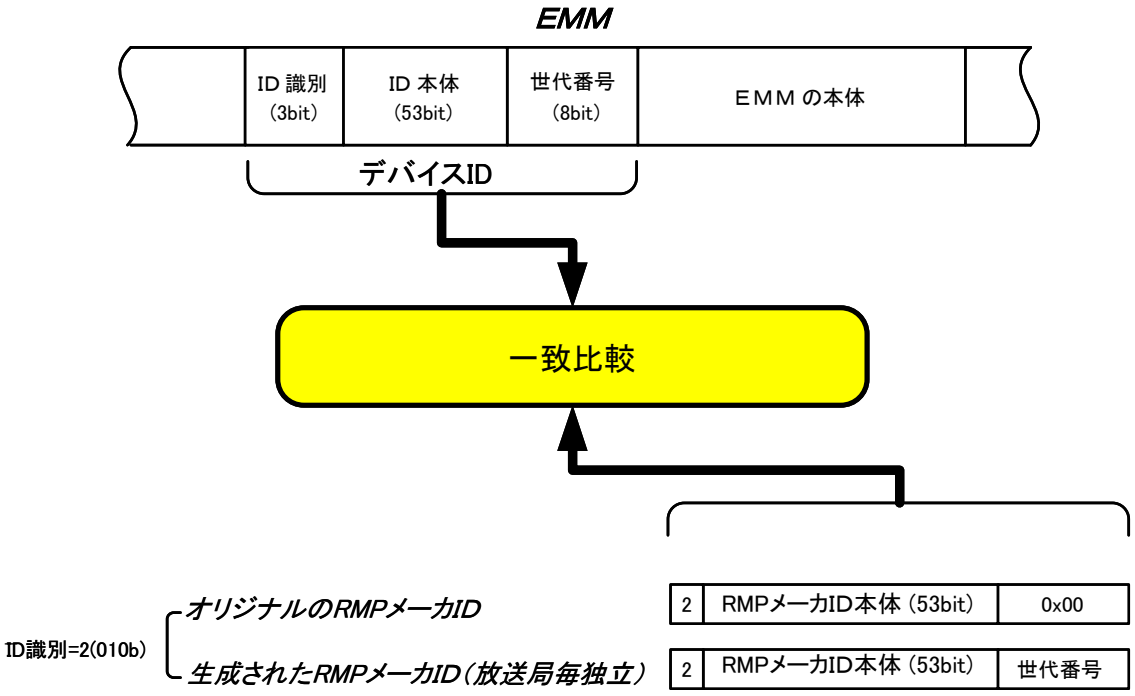


図 5-5　デバイス ID のフィルタリング

- デバイス鍵更新の実行モジュールに搭載するデバイス鍵更新アルゴリズムおよびその実装方法については受信機商品企画とする。なお、本編第二部 C 参考資料に関連記載がある。
- デバイス鍵を何世代目まで更新可能とするかは受信機商品企画とする。ただし、デバイス鍵が漏洩した場合、および、メンテナンスを目的にしたデバイス鍵更新の場合に、デバイス鍵更新機能を持つ必要があることに留意すること。

- デバイス鍵の更新は、デバイス鍵更新記述子に指定の世代番号へ更新すること。世代番号の指定は、インクリメント運用とは限らず、また減少することもあることに注意すること。

5.15 受信機のデバイスID表示

5.15.1 機能概要

- ユーザ操作により、デバイス ID を表示する。なお、関連記載が本編第二部 A.5 にある。
- デバイス ID の表示は、以下の通り 2 種行うものとする。統一名称はオリジナル RMP メーカ ID、局管理 RMP メーカ ID とする。
  1. オリジナル RMP メーカ ID（オリジナルの RMP メーカ ID）
  2. 局管理 RMP メーカ ID（局ごとに世代管理された RMP メーカ ID）

- オリジナル RMP メーカ ID は放送局に関わらず共通のデバイス ID である。
- 局管理 RMP メーカ ID は、放送局（トランスポートストリーム）ごとに異なる可能性があるデバイス ID である。もし、受信中の放送局において、局管理 RMP メーカ ID が設定されていない場合には、設定されていないことを示す表示を行う。
- デバイス ID 表示に際しては、デバイス ID（8byte）の ID 識別（3bit)、デバイス ID 本体（53bit)、世代番号（8bit）および表示用チェックコード（2byte）を、それぞれ 10 進に変換し表示を行う。それぞれの統一名称は ID 識別、デバイス ID 本体、世代番号、表示用チェックコードとする。
- 表示用チェックコードの生成方法に関しては、本編第二部 5.15.2 に記載がある。
- デバイス ID 表示のためのユーザインタフェースは商品企画によるが、各々の表示内容と統一名称との対応が明確になるように配慮すること。

5.15.2 表示方法

- 2 種のデバイス ID を、1 画面で表示する場合には、以下の順に記載するものとする。
  1. オリジナル RMP メーカ ID
  2. TS 名
  3. 局管理 RMP メーカ ID
- TS 名の表示部分は、TS 選択機能を伴うこと
- TS 選択にともなって、局管理 RMP メーカ ID の表示がその TS に対応するように更新されること。
- 2 種のデバイス ID を、複数の画面で切り替えて表示してもよい。

- 表示用チェックコードの生成は、RMP メーカ ID で、byte7-6 の 2 バイト、byte5-4 の 2 バイト、byte3-2 の 2 バイト、byte1-0 の 2 バイトの各 2 バイトを加算（桁上がりは切捨て）した結果を表示用チェックコードとする。以下の例を参照のこと。

（例）オリジナル RMP メーカ ID＝0x408B5A12CF93D500 の場合

1）0x408B＋0x5A12＋0xCF93＋0xD500＝0x23F30

2）桁上がりは切捨てし、0x3F30 を表示用チェックコードとする。

- デバイス ID（8byte）の ID 識別（3bit）、デバイス ID 本体（53bit）、世代番号（8bit）および表示用チェックコード（2byte）を、それぞれ 10 進に変換する場合、10 進に変換後の桁数は 25 桁で、内訳は、ID 識別（1 桁）、デバイス ID 本体（16 桁）、世代番号（3 桁）、表示用チェックコード（5 桁）である。
- ID 識別とデバイス ID 本体の間には区切りを入れて表示を行う。デバイス ID 本体、世代番号、表示用チェックコードを示す 24 桁には 4 桁毎に区切りを入れて表示を行う。以下の例を参照のこと。

（例）オリジナル RMP メーカ ID＝0x408B5A 12CF93D500 の場合

ID 識別＝2（010b）

デバイス ID 本体＝0153,2189,7891,1189（0x08B5A12CF93D5）

世代番号＝000（00000000b）

表示用チェックコード＝1,6176（0x3F30）

「-」の区切りを入れ、一行で表示した場合の表示例は以下の通りとなる。

2-0153-2189-7891-1189-0001-6176

5.16 エラー表示

- 視聴不可である理由を示すエラーメッセージがある。
- EMM 受信処理時に発生するエラーについては、エラー通知画面の表示は行わない。
- すべての ES がノンスクランブル運用で、以下の 5.16.1 に示すエラーが発生した場合は、エラー通知画面を表示しないこと。関連記載が本編第二部 5.13.1 および A.7 にある。

5.16.1 視聴不可である理由を示すエラー表示

- 以下に示すエラーメッセージの表示は、基本的に受信機の商品企画によるが、カスタマーセンターなどでの判定のため、次に示すエラーメッセージ例（エラーコードの表示も含む）に従うことが望ましい。なお、ワーク鍵未設定エラーについては、関連記載が本編第二部 A.8 にある。

［1-1］ワーク鍵未設定エラー

（エラーの内容）

－　伝送された ECM に対して、ワーク鍵が存在しない場合。（有効なワーク鍵を含む EMM をまだ受信していない場合で、選局してから EMM の再送周期の最大値の 2 倍の時間以下の場合）

（エラーメッセージ例）

受信制御データが設定されていません。しばらくお待ちください（最大で 30 秒かかる場合があります）。

コード：EC21

（その他）

－　本エラーにおいては、上記エラーメッセージの表示のほか、プログレスバーや残時間表示など、視聴者に対して進捗がわかるような表示を行うことも有効である。

［1-2］ワーク鍵未設定エラー

（エラーの内容）

－　伝送された ECM に対して、ワーク鍵が存在しない場合。（有効なワーク鍵を含む EMM をまだ受信していない場合で、選局してから EMM の再送周期の最大値の 2 倍の時間を超過した場合）

（エラーメッセージ例）

このチャンネルは視聴できません。ご覧のチャンネルのカスタマーセンターにお問い合わせください。

コード：EC22

［2］CA_system_id が不整合な場合のエラー

（エラーの内容）

－　PMT におけるアクセス制御記述子において、本編第二部で規定する CA_system_id と整合しない場合（本編第二部 5.4 参照）。

（エラーメッセージ例）

この受信機ではご覧になることができません。ご覧のチャンネルのカスタマーセンターへお問い合わせください。

コード：EC23

5.17　受信機におけるRMP方式の実装基準

5.17.1 保護対象

本実装基準で扱う保護の対象（保護対象）を表 5-3、表 5-4 に規定する。

表 5-3　保護対象 1

保護対象	備考
デバイス鍵更新アルゴリズム	
RMP メーカ ID に対するオリジナルデバイス鍵	STD-B25 第 3 部 表 4-2、本編第二部 B.2.1 参照
RMP メーカ ID に対するデバイス鍵	
F1 ワーク鍵(Odd/Even)	STD-B25 第 3 部 表 3-13、表 4-3 参照
F1 ワーク鍵識別(Odd/Even)	STD-B25 第 3 部 表 3-13、表 4-3 参照
F1Ks ポインタ(Odd/Even)	STD-B25 第 3 部 表 3-13、表 4-3 参照
RMP メーカ ID のデバイス鍵更新パラメータ	STD-B25 第 3 部 表 3-14、表 4-3 参照
関連情報暗号化の CBC 初期値 0～3	STD-B25 第 3 部 表 4-2、本編第二部 B.2.1 参照
RMP メーカ ID に対する EMM の改ざん検出鍵	STD-B25 第 3 部 表 4-2、本編第二部 B.2.1 参照
関連情報の改ざん検出アルゴリズム	本編第二部 B.2.1 参照
関連情報の暗号化／復号化アルゴリズム	本編第二部 B.2.1 参照

表 5-4　保護対象 2

保護対象	備考
スクランブル鍵(Odd/Even)	STD-B25 第 3 部 表 3-1、表 3-4 参照
MULTI2 暗号（スクランブルサブシステム）のシステム鍵	STD-B25 第 3 部 表 4-2、本編第二部 B.2.1 参照
MULTI2 暗号（スクランブルサブシステム）の CBC 初期値	STD-B25 第 3 部 表 4-2、本編第二部 B.2.1 参照

5.17.2 保護規定

5.17.2.1　一般事項

- 本実装基準は、5.1 受信機構成で規定する RMP モジュールのモデルおよび受信機のモデルを想定したうえで規定する。
- ハードウェア、あるいはソフトウェアでの実装にかかわらず、RMP モジュールは、同モジュールから保護の対象が基本的に漏えいすることのないように設計あるいは製造されなければならない。関連する記載が 5.17.2.2 にある。
- 前項に加え、RMP モジュールは、ハードウェア、ソフトウェアでの実装にかかわらず、RMP モジュール全体の機能が常に一体となるように実装されなければならない。5.17.3.1 (1)および 5.17.3.2 (1)に関連する記載がある。
- さらに、RMP モジュールと RMP モジュールを実装する受信機は、ハードウェア、ソフトウェアでの実装にかかわらず、機能上一体となるように実装されなければならない。5.17.3.1 (2)および 5.17.3.2 (2)に関連する記載がある。

5.17.2.2　保護対象抽出の阻止

- RMP モジュールは、表 5-3 に示す保護対象 1 の情報について、抜き取り行為が行われないように、5.17.2.3 の保護レベルに従い実装すること。
- RMP モジュールからデスクランブラに出力される表 5-4 に示す保護対象 2 については、受信機から平文のまま取り出されることがないように、5.17.2.3 の保護レベルに準じて実装することが望ましい。

5.17.2.3　保護レベル

実装基準を満足する保護レベルは、少なくとも以下に示すすべての規定を満足すること。

- 手ごろな価格で広く入手可能な汎用ツール（例えば、ドライバ、半田ごてなど)、または同様の電子ツールあるいは同様のソフトウェアツール（例えば、EEPROM リーダ・ライタ、デバッガ、逆アセンブラなど）を用いても、平文の保護対象データを得ることができないこと。
- 専門の知識を有する技術者が、プロフェッショナル用工具や装置（例えば、ロジックアナライザ、チップ分解システム、回路エミュレータなど）を用いても、平文の保護対象データを得ることが困難であること。

5.17.3 実装基準を満たす実装例

5.17.2 に規定する保護規定を満たすための実装例を、ソフトウェア実装、ハードウェア実装、およびハイブリッド実装に分けて示す。本項で示す実装例は、あくまでも実装の一例に過ぎず、たとえこの実装が行われていたとしても、実装手段によっては保護レベルを満たさないこともあることに注意すること。

5.17.3.1　ソフトウェア実装

受信機内で RMP 方式をソフトウェアによって実装する例を以下に示す。ここでいうソフトウェアとは、命令やデータからなるコンピュータプログラムコード（ただし、5.17.3.2 ハードウェア実装に組み込まれたものを除く）によって RMP 方式を実現したものをいう。

(1) RMP モジュール自体の実装例

例えば、RMP モジュールを構成するソフトウェアの全部または一部の不正な除去、置換、改変が行われた場合に、当該ソフトウェアの RMP 部分が動作しなくなるように実装することなどがあげられる。また、次に示す例などでは、セキュリティ強度の低下を招く可能性があ

るため、セキュリティ強度の低下を防ぐ実装が求められる。

- RMP モジュールの一部を受信機内の他のパーツ（モジュール）と共用すること
- RMP モジュールが解析されること

以下に実現するための具体的な実装例を示す。

- ソフトウェア自身の完全性の自己診断の実施。
- 複数のソフトウェアパーツから構成される場合は相互かつ定期的に認証管理の実施。
- 受信機内の他のルーティン、ライブラリ等から独立し、単独のメモリ管理や単独のアクセス管理の実施。
- 実装した各保護対象を隠蔽し、それらが暴かれないように設計された難読化技術、あるいは暗号化の導入。
- 管理者モード（リング 0 等）での実行を最小限にすること。

(2) RMP モジュールと RMP モジュールを実装する受信機が機能上一体となる実装

例えば、RMP モジュールを構成するソフトウェアは、不正な受信機では動作しないように実装することなどがあげられる。また、外部からの当該ソフトウェアの全部または一部の不正な除去、置換、改変等が試みられた場合に、当該受信機が使用できなくなるように実装することなどがあげられる。

以下に実現するための具体的な実装例を示す。

- 秘匿された機種固有の情報などを利用して、RMP モジュールと受信機本体との相互認証の実施。
- RMP モジュールが複数のソフトウェアパーツから構成される場合は、各ソフトウェアパーツは受信機本体との相互認証を実施。

5.17.3.2　ハードウェア実装

受信機内で RMP 方式をハードウェアによって実装する例を以下に示す。ここでいうハードウェアとは、以下の a)、b)、もしくは a)と b)とを組み合わせた方法で RMP 方式を実現した物理的な装置や部品を指す。

a)命令やデータを、装置や部品に固定的に組み込むことで RMP 方式を実現したもの

b)命令やデータを、5.17.2.3 の保護レベルを維持することでアクセスできないようにカスタマイズされた装置や部品に記憶することで RMP 方式を実現したもの

(1) RMP モジュール自体の実装例

例えば、RMP モジュールを構成するハードウェアに関しては、当該ハードウェアが分離／分解され、解析されることなどにより、セキュリティ強度の低下を招く可能性があるため、セキュリティ強度の低下を防ぐ実装が求められる。

以下に実現するための具体的な実装例を示す。

- 耐タンパ技術を用いたモノリシック IC、システム LSI など半導体回路やファームウェアへの実装。
- RMP モジュールが複数部品で構成される場合は、エポキシ等によるモールディング実装。

(2) RMP モジュールと RMP モジュールを実装する受信機が機能上一体となる実装

例えば、RMP モジュールが実装されるハードウェアは、不正な受信機では動作しないように実装することなどがあげられる。また、外部からの当該ハードウェアの全部または一部の除去、置換、改変等が試みられた場合に、当該受信機が使用できなくなるように実装することなどがあげられる。

以下に実現するための具体的な実装例を示す。

- 秘匿された機種固有の情報などを利用して、RMP モジュールと受信機本体との相互認証の実施。
- 当該ハードウェアが実装された受信機から取り外された場合に、当該ハードウェアが再利用出来ないリスクを負うような半田付け。
- 多層積層基板によるパターン設計。

5.17.3.3　ハイブリッド実装

受信機内で RMP 方式を 5.17.3.1 に示すソフトウェア実装と 5.17.3.2 に示すハードウェア実装を組み合わせて実装する場合、ソフトウェア部はソフトウェア単体での実装例に準ずるとともに、ハードウェア部はハードウェア単体での実装例に準ずる。

A　解説

A.1　複数の限定受信方式の運用に関して

コンテンツ保護方式として、ARIB STD-B25 第 1 部準拠の限定受信方式と ARIB STD-B25 第 3 部準拠のコンテンツ保護専用方式の 2 種類がある。前者の例は CA5 方式（CA_system_id＝5 の方式）であり、有料放送、EMM メッセージを利用した放送、コンテンツ保護を伴う無料放送など、様々な限定受信放送に対応する。後者の例は RMP 方式（CA_system_id= 0x000E の方式）であり、EMM メッセージを利用した放送（T.B.D.)、コンテンツ保護を伴う無料放送に対応する。

将来的には新たな第三の方式がサイマルクリプトで運用される可能性もありうるが、現時点ではそれらの機能も含めて全く不明である。本編第二部では、具体的な新方式が出てきた段階で規約を追加してゆくものとした。受信機は、そうした未知の限定受信方式の ECM と EMM は無視するようにしておき、将来に誤動作しないようにしておくものとする。

A.2　アクセス制御記述子について

限定受信方式と ECM、EMM の PID を示す記述子として、限定受信方式記述子とアクセス制御記述子の 2 つが規定されている。限定受信方式記述子は本編第一部に記載される ARIB STD-B25 第 1 部準拠の限定受信方式でのみ運用し、本編第二部に記載される ARIB STD-B25 第 3 部準拠のコンテンツ保護専用方式（RMP 方式)、および、将来的に新たな方式が運用される場合は、アクセス制御記述子を運用する。将来的に RMP 方式と新たな第三の方式がサイマルクリプトで運用される可能性もありうるが、その場合に、複数のアクセス制御記述子を運用しても、RMP 方式放送開始当初の受信機でも誤動作をおこさないことを目的として、複数のアクセス制御記述子が CAT、PMT に配置可能な旨を規定した。なお、複数のアクセス制御記述子の記載順については規定しない。いかなる順序で記載されても受信機は誤動作を起こさないことが求められる。

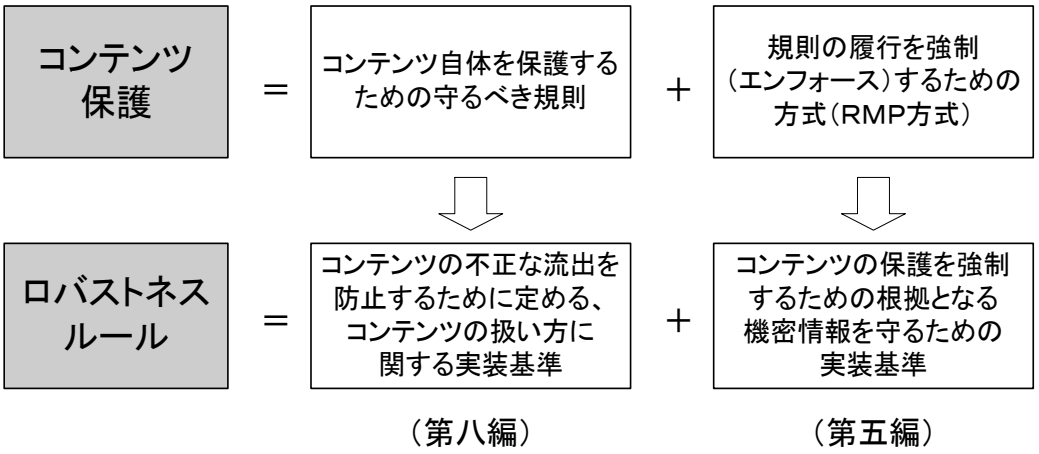
A.3　実装基準（ロバストネスルール）の扱いと特定の鍵の無効化について

コンテンツの保護においては、コンテンツ保護を強固なものにするために、守るべき機器の実装基準であるロバストネスルールの遵守が重要である。

コンテンツ保護は、コンテンツ自体を保護するための規則と、その規則の履行を強制（エンフォース）するための RMP 方式によって成り立っており、ロバストネスルールにも、コンテンツ自体の保護を強固にするための規則と、RMP 方式を守るための規則が存在する。この関係を下図に示す。

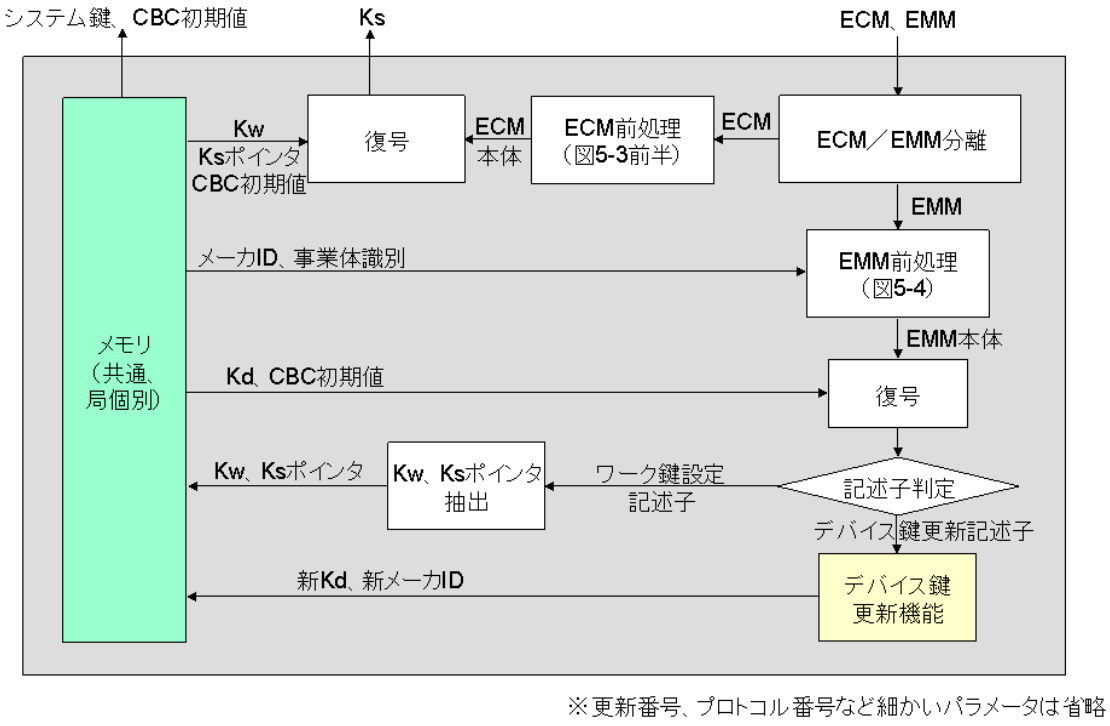
実際には、契約により本編第二部に規定の RMP 方式で使用される機密情報が提供されることと引き換えに、ロバストネスルールの遵守を強制（エンフォース）される。言い換えれば、(1)スクランブルされた番組（コンテンツ）を視聴するためには、RMP 方式で使用される機密情報が必要であり、(2)その機密情報を取得するために契約が必要、(3)その契約にはロバストネスルールの遵守が謳われている、という 3 つの要素から成り立っている構造である。

特に、本編第二部で規定される RMP 方式で使用される機密情報は、その情報が漏洩すると不正受信機の元となり、特に厳格な実装が必要となる。



受信機における RMP 方式の実装基準を規定するにあたり、ハードウェア、ソフトウェアを問わず、仮想的な「RMP モジュール」を想定した。RMP モジュール内の処理では、保護対象 1（本編第二部 5.17.1 表 5-3）に規定する機密情報が使用される。保護対象 1 は、RMP モジュール内の処理でのみ使用されるため、RMP モジュール外には平文としては、存在しないこととなる。RMP モジュールは、TS デコード部より出力される ECM、EMM を入力として、ECM の暗号復号処理機能、EMM の暗号復号処理機能、デバイス鍵更新処理機能、デバイス鍵更新アルゴリズム、不揮発性メモリ機能等を有することで、デスクランブルに必要な情報、つまり保護対象 2 をデスクランブラに出力する。「仮想的な」と規定しているのは、RMP モジュールがハードウェア、あるいは、ソフトウェアによる実装において、物理的にひとかたまりのブロックであることを求めていないためである。あくまでも、保護対象 1 を使用する処理全体の「機能」を

仮想的な RMP モジュールと表現したものである。RMP モジュールは、受信機メーカの設計・責任において実装することを前提に実装基準を作成している。実装基準が満足されていれば、たとえば、ES による更新機能など、RMP モジュールの個別機能を制限するものではない。



図A-1　RMPモジュールの機能

なお、ロバストネスルールのうちコンテンツ自体の保護を強固にするための規定は第八編で定め、RMP 方式を守るためのロバストネスルールは第五編で定めるべきという考え方に基づき、本編第二部 5.17 で定めた。

一方、万一機密情報を漏洩する受信機が出てしまい、結果として不正受信機が出回る事態になれば、特定の鍵の無効化の実施が考えられる。不正受信機については、例えばこれが蔓延する前に使用不能にする特定の鍵の無効化の運用が想定される。鍵更新の運用については、特定のワーク鍵無効化を目的としたワーク鍵更新、および、特定のデバイス鍵無効化を目的としたデバイス鍵更新運用を規定した。

鍵の無効化の基本的な実行方法としては、鍵を無効化する対象の受信機以外の受信機に対して、ワーク鍵更新の EMM を伝送し、無効化対象となる受信機に対しては、ワーク鍵を伝送しないことによってワーク鍵を無効化することとするが、正規受信機に対しては、必ず、利用可能なワーク鍵を伝送する運用を行うこととする。

A.4　保護対象の考え方

本編第二部 5.17 に、RMP 方式の実装基準（ロバストネスルール）について規定した。ここでは、保護対象を規定し、受信機器において実装上遵守すべき事項を記載した。

各保護対象は、RMP 方式として、コンテンツ保護の根幹を成す重要な機密のデータであり、このデータの流出は RMP 方式の運用・維持に重大な影響を及ぼす。RMP 方式の運用・維持を継続していくためには、各保護対象が受信機から漏洩し続けないことが基本的に重要である。例えば 1 つの保護対象が解析あるいは改ざんされた場合でも、その解析や改ざんの手順から全ての保護対象の解析や改ざん方法が推論されないような実装など、実装上の工夫が望まれる。なお、保護対象は RMP モジュール内でのみ使用される保護対象 1 と、デスクランブラ、すなわち、RMP モジュールの外で使用される保護対象 2 に分類し、それぞれに保護対象抽出の阻止について規定した。

なお、保護対象のうちデバイス鍵更新の実行モジュールおよびデバイス鍵については、実装の対象となるデータもしくは実行モジュールに関して、設計から製造過程において一貫した情報アクセス制限ルールが設定され、厳格な機密情報管理の運用が求められる。

A.5　受信機のデバイスID表示

RMP 方式では、RMP メーカ ID 単位で受信機が管理されるが、RMP メーカ ID とメーカ名とが一対一に対応するとは限らない。RMP を管理するセンタによる照会／確認等を想定し、受信機にデバイス ID 表示機能を装備することとした。

なお、RMP メーカ ID とメーカ名とが一対一に対応しない理由は、例えば以下のケースである。

1) 1 つのメーカにおいて、受信機の品種（TV、PC、車載機器、等々）ごとに RMP メーカ ID を利用することが想定される。この場合、RMP メーカ ID とメーカ名とは一対一に対応するとは限らない。
2) 委託製造の場合、販売を行うメーカ名を RMP メーカ ID とする場合があるため、委託製造メーカ名と一対一に対応するとは限らない。

A.6　受信機に必要なリソース

RMP 方式の機能は受信機ソフトウェアによる実装が可能であり、ソフトウェアによる実装時に想定される受信機に必要なリソースは以下の通りである。なお、共通データ、局個別データの詳細は本編第二部 5.12 を参照のこと。

a) ROM／不揮発性メモリ　　数百 Byte（共通データ等、実装プログラムは除く）
b) 不揮発性メモリ　　数 KByte（局個別データ等）
c) RAM　　実装プログラムに依存
d) CPU　　16 ビットマシン以上を想定
   - 2 秒毎に ECM 更新が行われても暗号復号化可能な性能であること。（暗号方式は AES 暗号相当）

A.7　エラー通知画面の扱い

非常災害時には、視聴者は生命・財産の保護のためその災害に関わる情報を要望している可能性が高く、放送継続を優先しなければならないことから、ノンスクランブルで送出する場合がある。加えて、放送設備への被災状況に応じては、臨時の放送設備から送出する場合も想定され、ECM、EMM を正常に送出することを保証することは困難である。そのため、ノンスクランブル時には ECM、EMM が正常に受信できない場合であっても、エラー通知画面を表示せずに放送を視聴できることが求められる。

本編第二部の RMP 方式ではワーク鍵等の情報を受信しながら受信機内に保持するので、ECM、EMM の受信状態によってはノンスクランブル時であってもエラー通知画面が表示される可能性があるため、あえて設計上の配慮を促す意味でこのように規定した。

A.8　EMMの受信機処理について

送出側の運用として、特定の鍵の無効化が実施された際に、デバイス鍵更新 EMM と Kw 設定 EMM の送出間隔が最短で 1 秒になりうる事が想定される。これは、デバイス鍵を更新する受信機においても受信に要する時間をなるべく短く抑える為に、EMM の送出方法を考慮した場合であるが、この場合でも受信機側がデバイス鍵更新 EMM を受信してから、新たにワーク鍵設定の EMM を受信可能になるまでの処理が 1 秒以上かかる場合等では、受信に要する時間が想定以上に長くなる可能性がある。

エラーメッセージを表示する際に、不正なメッセージが表示されることや、異なるメッセージが瞬時に切り替わって表示され、視聴者に誤解を与えることを極力防ぐ為に、ワーク鍵未設定エラーについては、その表示の切替えの目安を、EMM の再送周期の最大値の 2 倍の時間と規定している。この時間は、EMM の送出の仕方によっては、デバイス鍵更新 EMM がワーク鍵設定 EMM の後に来る可能性もあり、選局にかかる時間が最大で EMM の送出周期の 2 倍かかる可能性があるため、余裕をもってこの様な表現とした。

A.9　必須・オプションに対する基本的な考え方

表 A-1　限定受信に関する受信機の必須・オプション

No	CAS を利用するサービス	受信機の仕様	部分受信階層以外の受信機
1	基本	ID 番号表示	A
		エラー通知	A
		デスクランブラ	A
2	コンテンツ保護を伴う無料番組	通常視聴	A
		エラー表示	A
6	EMM メッセージサービス	自動表示メッセージ	T.B.D
7	EMM 受信	EMM 受信	A
		EMM 送出タイプ	A

A：必須、B：オプション、－：商品企画

A.10　自動表示メッセージの規定におけるT.B.D.について

本編第二部における自動表示メッセージの規定については、具体的な運用方法の検討に相当の期間を要することが考えられるため、その検討が終了するまで T.B.D.とする。

B　付録

B.1　RMP方式に関する問い合わせ先

(1) CA_system_id 0x000E

管理会社名　　一般社団法人　地上放送 RMP 管理センター

電話　　03-5785-1551

URL　　http://www.trmp.or.jp/

B.2　受信機メーカとの受け渡し情報

B.2.1　受信機メーカに供与される情報

受信機メーカに供与される受信機動作に必要なデータを以下に示す。

項目	内容
デバイス ID	メーカ固有の識別データである RMP メーカ ID。
RMP メーカ ID に対するオリジナルデバイス鍵	ID ごとに固有の鍵データ。
関連情報の改ざん検出鍵	EMM の改ざん検出を行うための RMP メーカ ID に対応する鍵データ。
関連情報暗号化の CBC 初期値 0～3	ECM、EMM の復号化時に使用する初期値（16Byte）であり、全部で 4 種の CBC 初期値データがある。
MULTI2 のシステム鍵と CBC 初期値	スクランブルサブシステム（MULTI2）で使用するシステム鍵と CBC 初期値のデータ。

受信機メーカに供与される技術情報を以下に示す。

項目	内容
関連情報の改ざん検出アルゴリズム	EMM の改ざん検出コードに関する技術情報。
関連情報の暗号化／復号化アルゴリズム	関連情報の暗号化／復号化アルゴリズム、ブロック暗号化／復号化手順の技術情報。

B.2.2　受信機メーカが拠出する情報

4.10.3 および 4.10.4 で規定されるデバイス鍵更新を行う場合に、受信機メーカから拠出を要するデータを以下に示す。

項目	内容
更新後のデバイス ID	更新対象となる RMP メーカ ID の更新後の値。
更新後のデバイス鍵	更新する ID に対応する更新するデバイス鍵の値。
世代番号	デバイス ID とデバイス鍵の更新を行うための世代番号。
デバイス鍵更新パラメータ	デバイス鍵更新を行うためのパラメータとなる値。

B.2.3　鍵インタフェースツール

B.2.1、B.2.2 に記載され、受信機メーカと授受されるデータ（受け渡し情報）は保護されており、受信機メーカにおいて暗号化／復号化する必要がある。このためのインタフェースツール（ソフトウェアツール）が受け渡し情報とは別に提供される。

C　参考資料　デバイス鍵更新アルゴリズムに関するガイドラインおよび実行モジュールへの実装例

本参考資料では、ARIB STD-B25 第 3 部「4.8.3.2 デバイス ID とデバイス鍵の算出処理」に規定されるデバイス鍵更新アルゴリズムの基本要件のうち、(要件 2)「新しいデバイス鍵の推定が困難であること」を満足するためのガイドラインおよび実行モジュールへの実装例を示す。本資料は上記要件を満足するための指針を参考として示すことが目的であり、必ずしも実装を制限するものではない。

C.1　新デバイス鍵の推定が困難であることに対するガイドライン

デバイス鍵更新アルゴリズムを用いて新デバイス鍵を生成するにあたって、世代間の推定を困難とするためのガイドラインを以下に示す。

C.1.1　世代間の推定が困難であることに対するガイドライン

乱数の利用が考えられる。

乱数の生成手段として、物理的手段（電気回路の雑音等）で発生させる物理乱数、算術式（プログラム等）で生成する算術乱数、あるいはその組み合わせが想定される。

※ 物理乱数を利用する場合、不規則、再現性が無い等の性質があることから、ARIB STD-B25 第 3 部「4.8.3.2 デバイス ID とデバイス鍵の算出処理」に規定されるデバイス鍵更新アルゴリズムの基本要件の（要件 1）にある「一意に更新が可能」を満足するために、生成した乱数を予め受信機に埋め込んでおく等、実装上の考慮が望まれる。

※ 算術乱数を利用する場合、以下の条件を考慮する。

- 生成した乱数列から算術式（プログラム等）と初期値の推定が困難なこと。
- 初期値として 128bit 以上のアドレス空間があること（2 の 128 乗の種類の初期値を設定可能なこと）。

C.2　デバイス鍵更新アルゴリズム（鍵更新方法）の実行モジュールへの実装例

デバイス鍵更新アルゴリズムの実行モジュールへの実装例を以下に示す。

(1) 埋め込み型

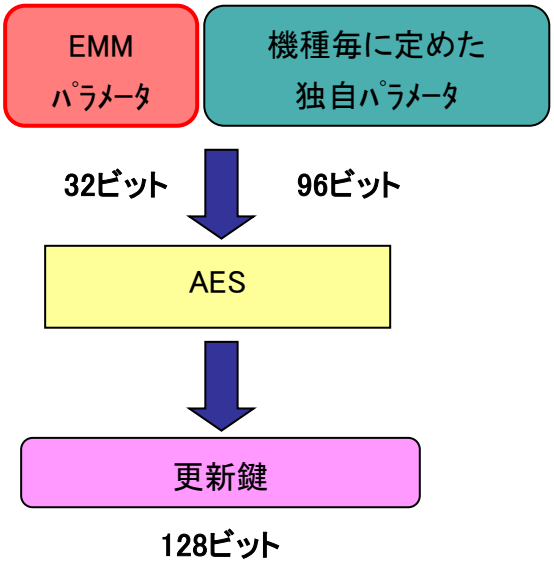
事前に乱数表を暗号化して埋め込み、デバイス鍵更新 EMM で送られる情報を元に乱数表からデータを抽出して新しいデバイス鍵とする方式。

(2) 生成型

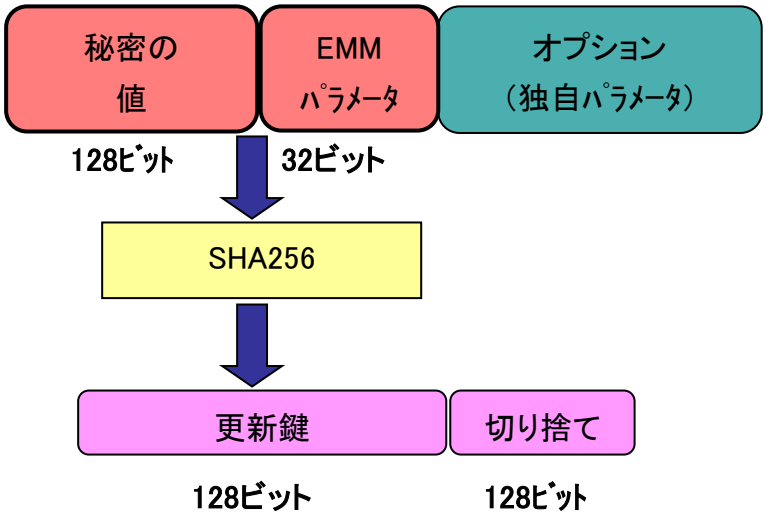
乱数を生成するプログラムを実装し、デバイス鍵更新 EMM で送られる情報を使用して新しいデバイス鍵を計算する方式。

(3) ダウンロード型

暗号化されたデバイス鍵をエンジニアリングストリーム、WWW、メディア等からダウンロードし、デバイス鍵更新 EMM をトリガとして、新しいデバイス鍵へ切り替える方式。



(a) AES 暗号（ECB モード）



(b) ハッシュ関数（SHA256）

図 C-1 デバイス鍵更新アルゴリズムの実装例（生成型）

第六編

地上デジタルテレビジョン放送
双方向通信運用規定

目　　次

1 はじめに

1.1 まえがき

地上デジタル放送における双方向データ放送サービスは、総務省令・告示、および電波産業会（以下ARIB）標準規格「デジタル放送用受信装置」(ARIB STD-B21)、「デジタル放送におけるデータ放送符号化方式と伝送方式」(ARIB STD-B24)の規定に従い行われる。しかしながら、地上デジタル放送において双方向データ放送サービスを実施するためには、細部の運用について別途規定を行う必要があり、ここに運用規定として定める。

1.2 目的

視聴者へのより良い双方向データ放送サービスの提供、および放送事業者による双方向データ放送サービスの円滑な提供のための遵守事項を規定することにより、双方向データ放送サービスの普及拡大を図ることを目的とし、本編「地上デジタル放送 双方向通信運用規定」をここに定める。

1.3 適用範囲

本規定は、地上デジタルテレビジョン放送における、固定受信機（据え置き型テレビ、STB、ポータブルテレビなど）を対象とした双方向データ放送サービスに適用する。双方向データ放送サービスに対応する固定受信機は本編のA規定を必須機能として実装することが求められる。B規定はオプション規格とする。携帯受信機（携帯端末など）については、双方向機能自体をB規定（オプション）とし、ここでは規定しない。

2　引用文書

本編の内容は以下の規格に規定される方式の地上デジタル放送における双方向通信に関する運用を定めたものである。

(1)　「デジタル放送用受信装置」標準規格　ARIB STD-B21

(2)　「デジタル放送におけるデータ放送符号化方式と伝送方式」標準規格　ARIB STD-B24

3 用語

本規定で用いる用語を以下のように定義する。

ADSL	Asymmetric Digital Subscriber Line:非対称デジタル加入者伝送方式。既存の電話線を用いて高速伝送を行う方式。
ARIB	Association of Radio Industries and Business：一般社団法人電波産業会。放送事業者、電気通信事業者、製造メーカーが参画する国内の電波利用に関する技術を標準規格化する団体。
ATコマンド	モデムを制御するためのコマンド。
BASIC系手順	データ伝送制御手順の基本的なホストと端末間用に開発された通信手順(BASIC手順)で、必要機能のみを搭載。
CATV	Cable and Tele-communication Television System：同軸ケーブル等の伝送路を通じてテレビ信号を各家庭に分配するシステム。双方向の伝送路として使用可能である。
CBCモード	Cipher Block　Chaining Mode：共通鍵暗号の暗号利用モード、暗号化結果を次の入力と排他的論理和をCBCモード(暗号利用モード)で演算した結果のIV（初期値）の値。
CRC	Cyclic Redundancy Check：巡回誤り検出符号。データの正確性を検証するための巡回型冗長チェック符号。
DNS	Domain Name Service [RFC1034, RFC1035]：ネットワーク上のホスト名とIPアドレスのマッピングをするためのサービスに使用するプロトコル。
DSU	Digital Service Unit：デジタル回線終端装置。デジタル網とデジタル通信用端末のインタフェースをとるための装置。
ECC暗号	Elliptic Curve Cryptography：楕円曲線暗号、楕円曲線上の離散対数問題を基盤とする暗号
Ethernet	LANの通信方式のひとつ。
FEC	Forward Error Correction：誤り訂正。
FTP	File Transfer Protocol [RFC959]：TCP/IP上の2つのホスト間で、ファイルの共有や転送を行うためのプロトコル。
FTTH	Fiber To The Home：通信の伝送路をユーザ宅まで光ファイバで提供するサービス。
HDLC手順	High-level Data Link Control：主にLANやインターネットでのコンピュータ間通信に利用される高信頼の伝送制御手順。
HTTP	Hypertext Transfer Protocol [RFC2616]：アプリケーション層プロトコルで、World Wide Webのデータ転送に使用されているプロトコル。
ICMP	Internet Control Message Protocol [RFC792]:プロトコルデータ転送中において発生した各種のエラーの通知や動作の確認などメッセージ送信用プロトコル。
IEC	International Electrotechnical Commission：国際電気技術委員会。
IP	Internet Protocol [RFC791]：ネットワーク層プロトコル、インターネットのアドレス機構の定義と、データの配送処理を行う。
IPCP	IP Control Protocol [RFC1332]：PPPのネットワーク層プロトコルフェーズにおいてIPを利用する際に必要な各種設定を行うプロトコル。
IPv4	現在のLAN・インターネットの基盤として使用されている国際標準プロトコル。

IPv6	IPv4の後継プロトコル。アドレス部の拡張、セキュリティ機能等を追加したプロトコル。
ISDN	Integrated Services Digital Network：サービス統合デジタル網。
ISO	International Organization for Standardization : 国際標準化機構。
ISP	Internet Service Provider：インターネット上で各種コンテンツサービスを提供する事業者。
ISP接続情報	ISPのアクセスポイント電話番号や認証プロトコル等の情報で、視聴者によって設定され受信機に保持される。
MAC	Message Authentication Code：通信文が改竄や伝送エラーなく相手に送られたことを確認するための符号。
MNP4	モデム通信用のエラー訂正方式。
MSB	Most Significant Bit：最上位ビット。
M系列	簡易な擬似乱数を生成するときに用いる比較的長い周期を持つ数字列。
NNTP	Network News Transfer Protocol [RFC977]：Internet上のNetNewsを配布、投稿、取得するために使用するアプリケーション層のプロトコル。
PDC	Personal Digital Cellular：デジタル自動車・携帯電話方式。9600bit/sのデータ通信が可能。
PDC-P	Personal Digital Cellular Paket：PDC方式のパケット交換による通信。9600bit/s～28800bit/sの通信が可能。
PHS	Personal Handy-phone System：簡易型携帯電話。
PIAFS	PHS Internet Access Forum Standard：PHSを用いたデータ通信方式32kbit/s, 64kbit/sのデータ通信プロトコル。
PIN	Personal Identification Number：個人識別番号。あるシステムへのアクセス許可を得るために秘密に事前に割り当てられた番号を用いて個人を識別／認識する。
PKCS	Public-Key Cryptography Standard：公開鍵暗号を中心とし、共通鍵暗号、ハッシュ関数、擬似乱数機能等を含めた暗号システム。
PN信号	Pseud Noise：擬似雑音。1と0がランダムに現れる性質を持った信号。デジタル信号のエネルギ拡散などに用いる。M系列が良く用いられる。
POP3	Post Office Protocol version3 [RFC1939]：メールサーバ上のスプールから電子メールの一覧や電子メール取得、削除するために使用するプロトコル。
PPP	Point to Point Protocol [RFC1661]：Point to Pointのリンク上で複数のプロトコルの転送を可能にするためのプロトコル。ダイヤルアップ接続に利用される。
PPP in HDLC-like Flaming	ppp のプロトコル上位として積み上げるためのフレーム構成。HDLC手順で用いるフレーム構成としたヘッダ・フッターの構成方法。
PSTN	Public Switched Telephone Network：公衆電話網。
RSA暗号	現在最も普及している公開鍵暗号。暗号／復号処理機能と署名／検証機能を持つ。
SMTP	Simple Mail Transfer Protocol [RFC821]：電子メール中継・配送用プロトコル。

SSL	Secure Socket Layer：ソケットレベルのセキュリティプロトコル。TCP層とアプリケーション層の中間に位置し、暗号化/復号、認証を提供する。
STD	standard：標準規格。
TA	Terminal Adapter：アナログ通信端末等をISDNへ接続できるようにプロトコル変換を行う装置。
TCP	Transmission Control Protocol [RFC793]：エンド・エンドでのトランスポート層のプロトコル、エラー検出・訂正を有するコネクション型の高信頼転送を提供する。
TCP/IPアプリケーション設定情報	TCP/IPプロトコル上で使用されるアプリケーションプロトコルに関する情報で、視聴者により設定され受信機に保持される。
TLS	Transport Layer Security：SSLをベースに標準化されたセキュリティプロトコル。特にハッシュ処理に関する変更を行っている。
Telnet	[RFC854,RFC855] TCP/IPネットワークにおいてリモートにあるサーバを端末から操作できるようにする仮想端末を提供するプロトコル。
UDP	User Datagram Protocol [RFC768]：2つのホスト間のトランスポート層プロトコル、送達確認機能はないが、プロトコルオーバーヘッドを最小にし、高伝送効率向けのサービスに適するコネクションレス型の通信。
UTC	Universal Time Coordinated：協定世界時。国際間の申し合わせにより決められた世界共通で使われている時刻。
V.22bis	ITU-T勧告が定めた2400bit/sまでの電話用全二重モデム用変調方式。
V.34	ITU-T勧告が定めた33.6kbit/sまでの電話用全二重モデム用変調方式。
V.42 bis	ITU-T勧告が定めたモデム間通信のデータ圧縮方式およびエラー訂正方式。
V.90	ITU-T勧告が定めた56Kbit/sアナログモデムの標準仕様。
X.28	モデム等を搭載した非パケット受信機をパケット交換網等に接続できるように変換する通信手順。
closedネットワーク事業者	インターネットに接続されない閉じたネットワークを運営する事業者。
reserved	未定義。符号化ビットストリームの定義に関して、将来の拡張用にISOで定義される可能性があることを示す。ARIB規格で別途定義のないビットはすべて「1」にセットする。
reserved_future_use	未定義。符号化ビットストリームの定義に関して、将来の拡張用にARIB規格で定義される可能性があることを示す。別途定義のないビットはすべて「1」にセットする。
rpchof	remainder polynomial coefficients, highest order first：多項式係数の剰余、最上位階級が先頭。
time stamp	重要な通信データに通信時刻や乱数を付加することにより、その通信データの再利用検出が可能。
uimsbf	unsigned integer, most significant bit first：最上位ビットが先頭である、符号無し整数。
アクセスポイント	受信機からの発呼を受ける通信設備。
アプリケーション情報	放送局の指定するアクセスポイント電話番号や回線種別等の情報。
エコーバック	送信側で送信文字を確認するために、モデムや通信相手が受信した文字をそのまま送り返した文字あるいはその動作を示す。

カードID	受信機に装備されるカードにあらかじめユニークに割り振られた番号、もしくは記号。
カットスルー呼	ネットワークサービスの大量呼受付サービスにおいて、受信機からの発呼の一部を予め指定したセンタに接続する呼。
カット呼	ネットワークサービスの大量呼受付サービスにおいて、受信機からの通信が発信側交換機で終端される呼。
コードインディペンデントモード	BASIC系手順でバイナリデータも伝送可能なように拡張した方法。
コピー制御	コピー世代を制御すること。 放送受信機に接続される記録機器に対して、番組その他の著作権物をコピーする時に制限を行うこと。
サービスコード（SC）	00XY等で識別される通信事業者の提供するネットワークサービスのサービス区分コード。
セキュリティレベル	取扱うデータ等に必要な機密性の程度に応じて、セキュリティの強度を段階的に定義し、運用するときに用いる指標。
セキュリティ通信関連情報	受信機に実装されたセキュリティ種別やルートCA証明書に関する情報で、受信機に保持される。
セッション鍵	セキュリティ強度の維持の観点から一セッションのみに用いる（使い捨ての）鍵。
センタ	双方向伝送サービスを提供するのに必要なホストを含めた設備。
タイムスタンプ	time stamp
タンパレジスタント	装置を取扱う者が内部のデータを読み出したり、機能を解析されないようにするために用いる物理的な覆い。
データ送信関数	BMLコンテンツに記述された命令であり、受信機とセンタ間でのデータ送信を行う関数。
デビット	利用時点で利用者の銀行口座と加盟店の銀行口座間で代金を振替える決済。即時決済。
トークン	電子投票に用いる電子的な投票券。
トラヒック	公衆網等の回線や交換設備に加わる通信量のこと。
ネゴシエーション	複数の変調方式、誤り訂正機能および再送機能を有するモデム同士の場合、両モデムが共通に有する方式、機能を探すために通信の最初行なわれる。
ネットワークサービス	受信機とセンタの間にあるネットワーク上で行うデータ集計、データの加工等の付加価値サービス。
ネットワーク代行課金	情報料課金を用いて、情報提供者に代わって通信事業者が利用者に請求する課金方式。
ハッシュ関数（メッセージダイジェスト）	大きな（場合によっては非常に大きな）領域を小さな範囲に写像する数学的関数。質のよい関数には一方向性と衝突フリーであることを同時に満たすことが必要。
バーナム暗号	送信側、受信側とが共通して持つ乱数列と通信文の排他的論理和を暗号文として送信し、受信側は同乱数列と受けとった暗号文の排他的論理和をとることにより復号する暗号方式。真の乱数を用いた場合、情報理論的に安全な暗号方式となる。
バリュー	プリペイド方式で用いられるお金や価値の情報。
プリペイドID	ネットワーク型のプリペイド決済を用いる場合、プリペイドカードに相当した利用者毎に対応付けが行なわれる識別子。
ベーシック系手順（Code Independent　Mode）	データ伝送制御手順の基本的なホストと端末間用に開発された通信手順。データ伝送の誤りを最小にするための通信手順を搭載している。

ホスト	双方向伝送サービスに必要なアクセスポイント装置やサーバ装置。
マスコーリングサービス	ネットワークサービスの一つで、大量呼受付サービスなどが含まれる。
マスター鍵	セッション鍵に対比して用いられる。セッション鍵を共有するために用いられる鍵。
メッセージダイジェスト	任意長のデータを一定の長さに要約（ダイジェスト）すること、またはその要約されたデータ。
メッセージ認証子	MAC
モール	電子的な店舗およびその集合体。
ルート証明書	公開鍵暗号を用いた認証・署名の検証に必要。信頼できる第三者機関（認証機関）の公開鍵で、この認証機関の発行した証明書に記された署名の正当性を検証するために用いられる。
ログ収集課金	データ放送利用料金を利用者毎に記録し、後日一括精算する課金方式。
一方向性	数学的な演算において逆演算をすることが不可能あるいは非常に困難な特性のこと。
回線種別	PSTN、 携帯回線、 PHSなどの通信回線の種別を示す。
拡散	デジタル信号で1または0が続いたり、一定のパターンが続くと輝線スペクトルが発生して混信妨害を与えたり、受信機でクロック再生ができなくなる。この問題を防ぐために、既知のPN信号を与えてランダムな信号としておくこと。
管理サーバ	個人情報の管理方式において、個人情報を集中して管理し、ホストからの問い合わせに対して個人情報を返す機能を有するサーバ。
簡易暗号	第三者に復号されないことが必要条件でない場合に用いる簡易的な暗号。
簡易認証	相手認証において、セキュリティ強度をあまり必要ない場合に用いられる認証手段であり、共通鍵暗号を用いて実現可能。
既知平文攻撃	既にわかっている平文を入力し暗号文生成し、その平文と暗号文から暗号化鍵を導く暗号アルゴリズムへの攻撃方法。
擬似乱数	一般的には、真の乱数を生成することは困難なため、十分長い周期性、一様性（ばらつき）を持った数字列を乱数の代用とすることが多い。
共通鍵暗号	秘密鍵暗号・対称暗号とも言う。送信者・受信者が秘密で共通して所有する共通鍵を利用して、送信側で暗号化し、受信者側で復号する。あらかじめ他の手段を利用して共通鍵を共有する必要がある。
共通情報	優先利用回線種別や外線捕捉番号等の情報で、視聴者によって設定され受信機に保持される。
検証者	署名者及びその内容が確かかどうかを検証する者。
厳密認証	公開鍵暗号を用いた認証手段。
言い逃れ	送信者本人が通信内容を送信後に否定すること。
個人情報	個人を特定するための個人の属性。氏名、住所等以外にも銀行口座番号、クレジットカード番号等が含まれる場合もある。
呼	通話の単位。
固定IP接続情報	IPアドレス等の割付けを固定的に行う形態での情報で、視聴者によって設定され受信機に保持される。

固定優先接続	通信事業者を地域通信事業者に登録することにより、その通信事業者の識別番号（00XY等）をダイヤルせずに接続される優先接続のオプションで、常時、選択された特定の通信事業者に接続される。
公開鍵暗号	非対称暗号とも言う。暗号用の鍵（公開鍵）と復号用の鍵（秘密鍵）が異なる。公開鍵を公開し、秘密鍵を秘密裏に管理することにより、共通の秘密情報がなくても暗号通信が可能。一部の公開鍵暗号（RSA暗号、ECC暗号）は、署名機能も持つ。
参加率	ある双方向データ放送サービス番組の利用者数を視聴者数で割った値。
視聴者設定情報	共通情報、ISP接続情報、固定IP接続情報、接続形態情報、TCP/IPアプリケーション設定情報からなる視聴者個々に決定すべき情報の総称。
受信機設定情報	通信関連情報、および通信デバイス情報、セキュリティ通信関連情報、共通情報、ISP接続情報、固定IP接続情報、接続形態情報、TCP/IPアプリケーション設定情報からなる受信機に設定・保持される情報の総称
収集ネットワーク	多くの受信機からのデータを集めるネットワーク。
署名	公開鍵暗号の、秘密鍵を有する者のみが生成できる演算の性質を利用して、その演算結果を電子署名とする。
商品企画	搭載される機能や動作が受信機または商品に依存するもの
衝突フリー	ハッシュ関数に必要な性質で、2つ任意の異なる入力に対して出力結果が異なる確率が十分であること。
証明書	公開鍵暗号を用いた認証・署名の検証に必要。信頼できる第三者機関（認証機関）が電子的に発行する。
上り回線	受信機からモデムなどを用いてセンタ装置に接続する回線。
情報料課金	電話回線を介して行なわれるテレホンサービス等の情報提供サービスにおいて、情報の利用者が情報提供者に支払う料金（情報料等）を通信事業者が代行するために行う課金。
接続形態情報	Ethernet接続時のIPアドレス取得に関するプロトコルで、視聴者が設定し受信機に保持される。
相手認証	通信相手を確認する必要がある場合にセキュリティ機能を利用して相手を認証する。
大量呼受付サービス	交換機の機能を利用することにより、短時間で大量呼を受け付けることができるサービス。
着信課金	通信料金を着信側が負担する課金方式。
通信デバイス情報	アクセスポイントに実装されるネットワーク終端装置と、受信機に実装されるネットワーク終端装置間で規定すべき情報で、受信機に保持される。
通信関連情報	受信機に実装された回線種別やプロトコル等の情報で、受信機に保持される。
通信事業者	電気通信サービスを提供する第１種電気通信事業者、および第2種電気通信事業者。
通信事業者識別番号	電話番号の中で通信事業者毎に指定された事業者を識別するための番号。（00XY等）
伝送モード	変調方式、誤り訂正方式の違いによる区分。

特殊番号	電話番号の中で、1から始まる短桁の番号。1XY番号。
認証機関	証明書の信頼性を保証する第三者機関。
発呼	電話をかけること。
発呼（発信）制限	アクセスポイントにおける輻輳を避けるため、受信機側で発信可能な受信機を制限すること。
発呼関数	BMLコンテンツに記述された命令であり、センタに向けて発呼するための関数。
発信遅延	アクセスポイントにおける輻輳を避けるため、受信機側で発信を任意時間だけ遅らせること。
平文	暗号化する前のデータを指し示す。
本人確認	受信機やICカードをアクセスする権限を有する人（本人）であるかを確認するための方法。パスワード（フレーズ）やPINを用いる。
無手順(TTY手順)	物理層以上の再送等の手順を定めずに行う通信。遠隔ホストとテレターミナルのテキスト通信から始まった最も簡素な通信方式。
優先利用網	受信機において複数の回線種別（PSTNや携帯電話など）の使用が可能な場合、視聴者が選択する回線種別。
予約確認番号	ネットワーク上でチケット等の購入予約をした場合に、一つの予約の解約、変更、発券、問い合わせ等を管理するために発行する予約管理の番号。
輻輳	交換機に単位時間処理能力を超える通信が集中することにより、電話がつながらなくなる現象。輻輳は電話がかからないことにより相手につながるまで繰り返し電話をかけ直す行為により増大する。

4　双方向データ放送サービスのシステム構成と接続形態

本章は、双方向サービス実現に必要な通信システム及び接続形態について解説する。

4.1　システム構成

双方向データ放送サービス形態の概念図を図4-1に示す。

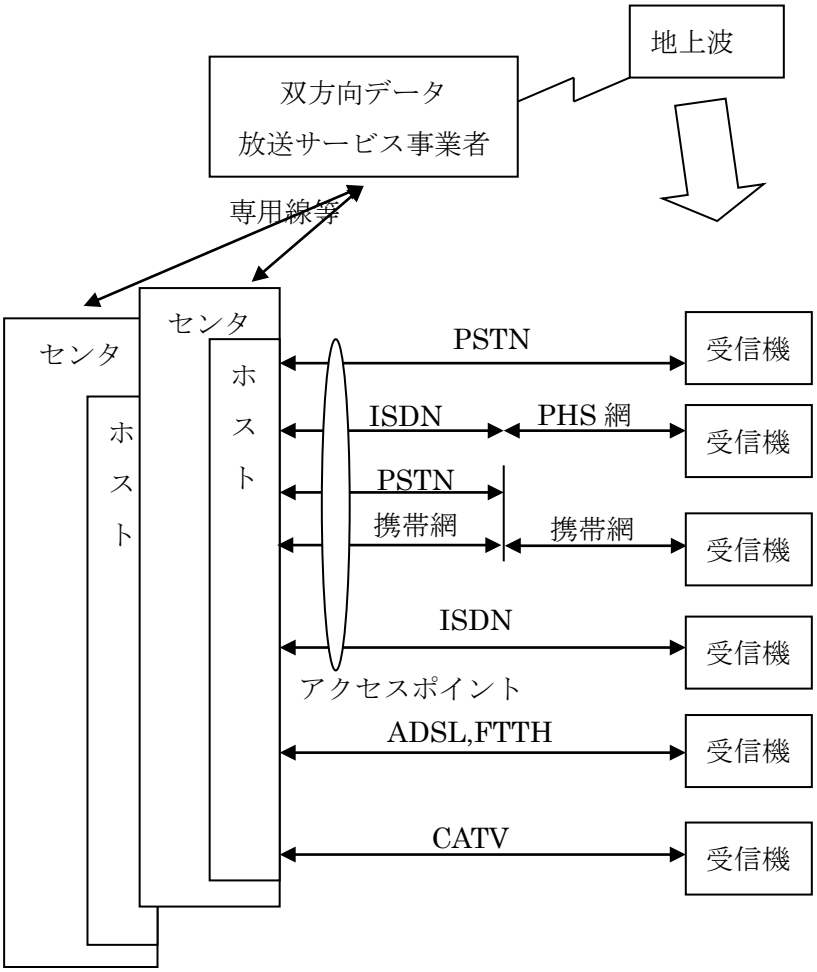


図4-1　双方向データ放送サービス形態概念図

4.2　双方向データ放送サービス事業者に関わる設備

双方向データ放送サービス事業者はセンタとの回線として必要に応じて、専用線等の通信回線を備える。回線種別は、サービス内容やデータ通信量、信頼性確保など勘案し両者間で決定される。

4.3　ホストに関わる設備

センタ内のホストは、受信機側の回線として、PSTN（PSTN、携帯使用時）、ISDN（PHS使用時）、携帯網（携帯網直接収容時）、ADSL、FTTH、CATVの中から必要に応じて回線設備を備える。ホストへの接続点であるアクセスポイントの回線数は、サービス内容やデータ通信量を勘案して決定する。また、双方向データ放送サービス事業者との間に必要に応じて通信回線を備える。

4.4　受信機の回線接続に関わる機能

受信機はPSTN、PHS網及び携帯網、ISDN、ADSL、FTTH、CATVなどの回線に接続し、センタと通信する機能を有する。

4.5　接続形態

4.5.1　直接接続

(1)　公衆網等を利用し、センタと受信機を直接接続する。

長所：　プロトコルを適切に選べば受信機の実装は軽くすることが可能。

短所：　センタがアクセスポイントを確保する必要がある。

図 4-2 に接続形態を示す。

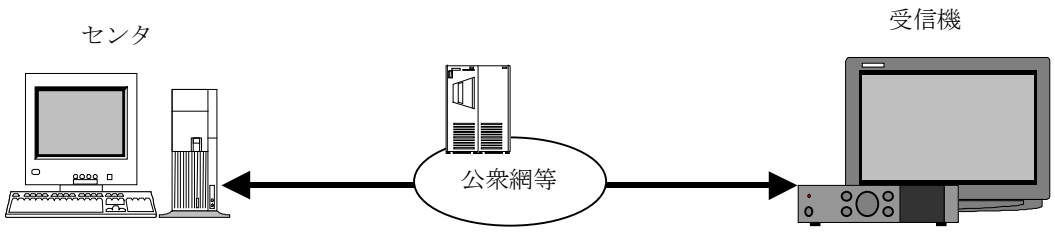


図 4-2　直接接続

(2) 公衆網等を利用し、受信機とアプリケーション毎に任意のセンタを直接接続する。

長所： プロトコルを適切に選べば受信機の実装は軽くすることが可能。
各センタがアクセスポイントを共用することができる。

短所： 複数センタが共用のアクセスポイント利用するので、アクセスポイントのスケジューリングが必要になる場合が想定される。

図 4-3 に接続形態を示す。

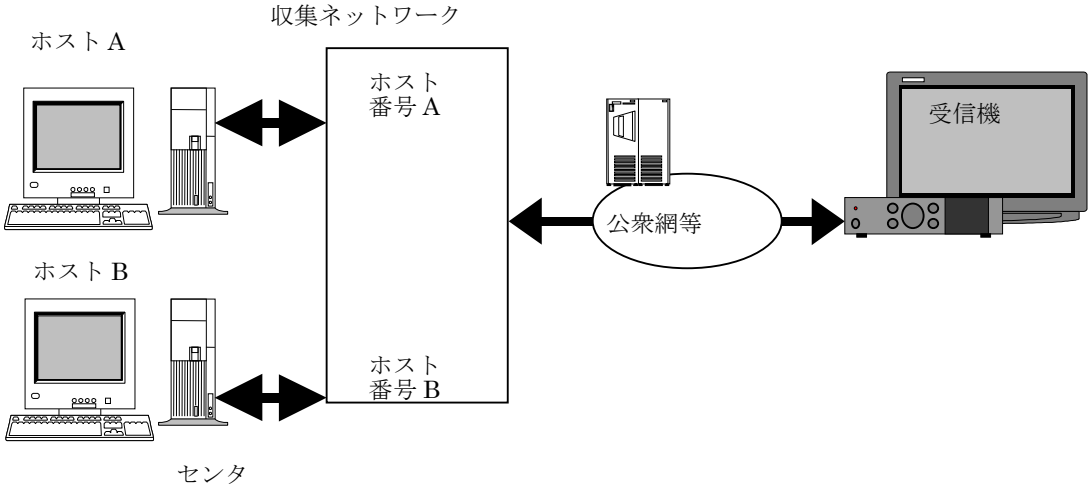


図 4-3 ホスト番号を利用した直接接続

4.5.2 ネットワークサービス

受信機とセンタ間のデータ通信において、ネットワークでデータの集計等の加工を行う。

データ加工内容は個々のサービスにより異なる。特に放送と関連したネットワークサービスとしてマスコーリングサービスがある。そのサービス中の代表的な大量呼受付サービスでは、受信機の着呼交換機で着呼数を集計処理し、センタに集計結果を逐次通知する。

長所： 受信機の実装が軽い。センタのデータ集計等の加工処理が軽くなる。

短所： あらかじめ通信事業者と契約が必要なサービスもある。

図4-4に接続形態を示す。

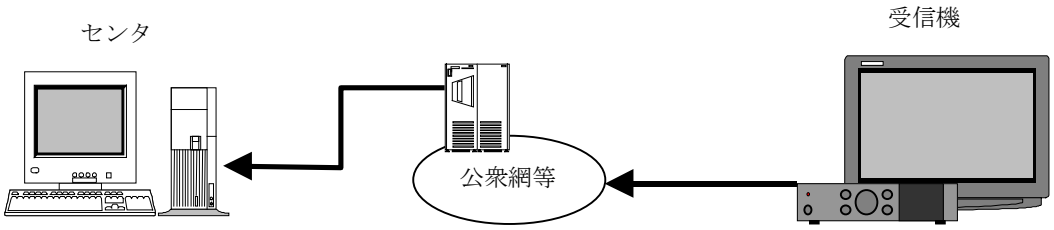


図4-4 大量呼受付サービスの接続

4.5.3　下り電波、上り回線

双方向通信のうち、リクエスト等の上り信号を公衆回線で、リクエストに対するレスポンスを電波で配信する。

長所：　大容量共通データの配信に地上波の電波を利用する場合には安価にサービスを提供可能。従来の放送・通信の何れにも無かった新たな多彩なアプリケーションが考えられる。

各受信機は、上り回線・下り回線および共通のセンタを利用することになるので、受信機間通信も可能である。

短所：　システムが複雑。上り公衆回線と下り地上波をリンクさせたプロトコルが必要である場合には大規模な開発を要する。

図 4-5 に接続形態を示す。

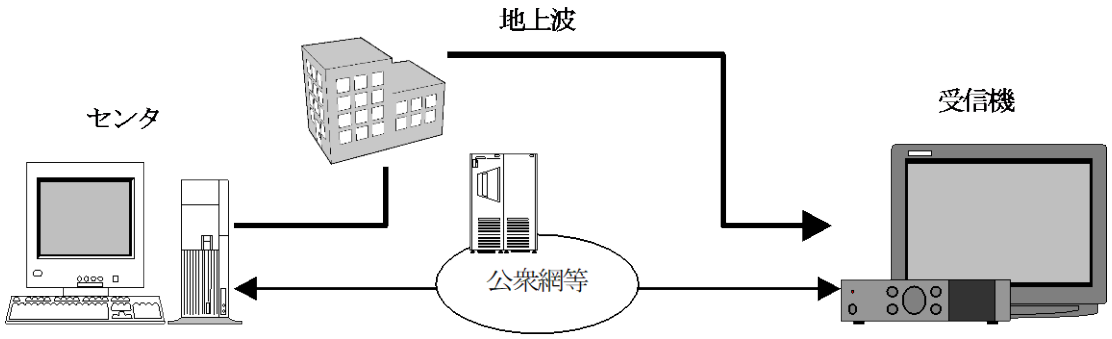


図 4-5　下り電波・上り回線を用いた接続

4.5.4　インターネット接続

受信機は、公衆網等を経由して、インターネットサービスプロバイダ（ISP）のアクセスポイントに接続される。さらに、ISPからインターネットを経由してセンタ側のISPに接続され、専用線等を経由してセンタに接続される。

長所：　全国の既存のアクセスポイントが利用可能。

短所：　受信機に TCP/IP, PPP と ISP 接続手順を実装する必要がある。視聴者は、センタからのサービスを受けるために、ISP に加入しなければならない。

図 4-6 に接続形態を示す。

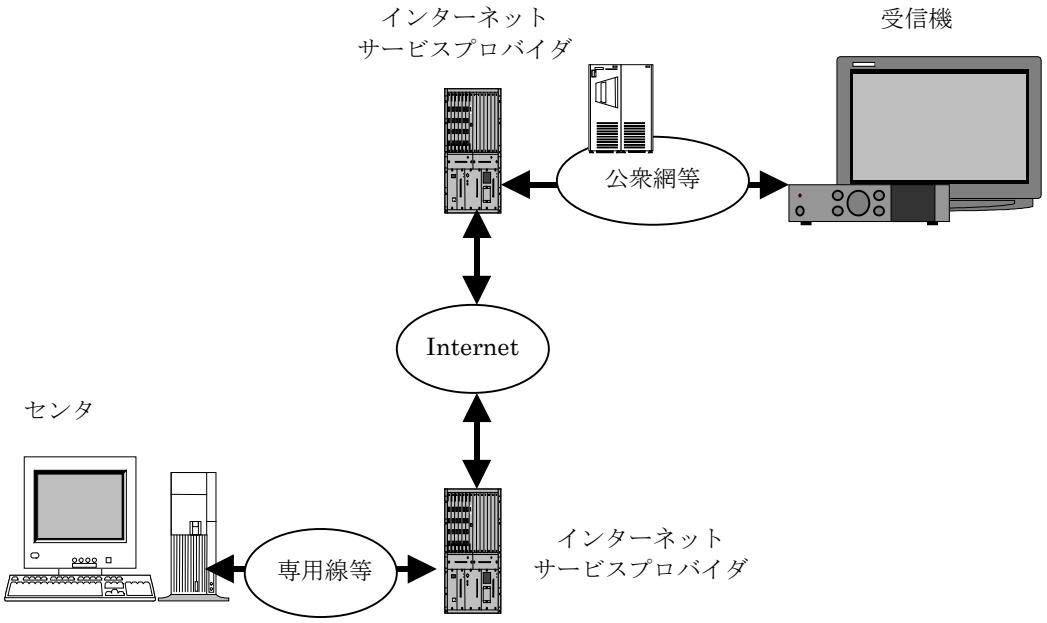


図4-6　インターネットを用いた接続

5　BASIC系通信プロトコル

5.1　双方向通信と伝送フェーズ

双方向伝送におけるPSTN、携帯網およびPHS網などの公衆網等を利用するプロトコルを図5-1に示すような、5つのフェーズに分割し、各フェーズでの通信プロトコルを5.2節で規定する。

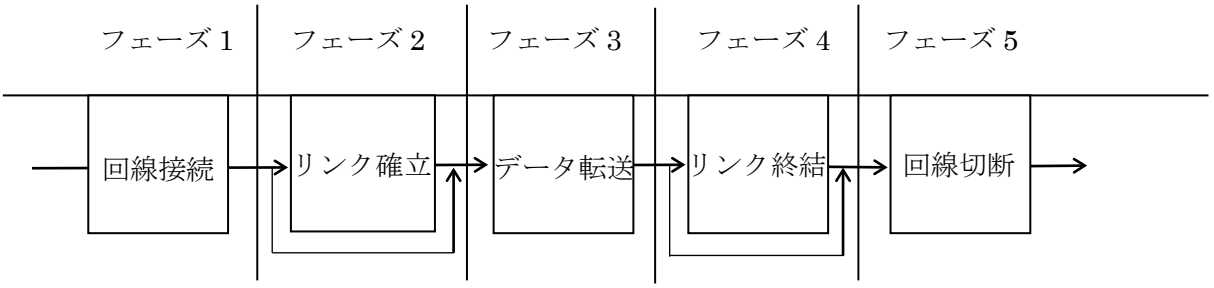


図5-1　伝送フェーズ

5.2　伝送フェーズとプロトコルスタック

5.2.1　回線接続／切断フェーズ

受信機が、公衆網等を利用してセンタとの接続／切断をするフェーズ。モデム等に対してATコマンド等を用いて回線接続／切断を行う。

5.2.2　リンク確立／終結フェーズ

リンク確立／終結フェーズは、回線接続後に受信機とセンタのデータ転送リンクを確立するため、及びデータ転送終了後受信機とセンタ間のリンクを終結するためのフェーズである。
リンク確立／終結フェーズのプロトコルスタックを表5-1に示す。なお、第６章に規定するTCP/IP通信プロトコルの実装において、PSTN用通信プロトコル以外が選択された場合には下記A規定は適用されない。

表 5-1　リンク確立／終結フェーズのプロトコルスタック

レイヤ		プロトコルスタック
データリンク層	A 規定	X.28 一部準拠手順（5.3 を参照）
物理層		
モデム　A 規定		V.22bis + MNP4
携帯電話(回線交換方式)	B 規定	PDC: 9600bit/s※
PHS	B 規定	PIAFS: 32kbit/s 以上

※携帯網内でV.22bis + MNP4に変換される場合がある

5.2.3　データ転送フェーズのプロトコル

データ転送フェーズは、リンク確立後に受信機とセンタ間でデータ通信を行うフェーズである。

BASIC系通信用プロトコルを表5-2に示す。なお、第6章に規定するTCP/IP通信プロトコルの実装において、PSTN用通信プロトコル以外が選択された場合には下記A規定は適用されない。

表 5-2　BASIC 系通信用データ転送フェーズのプロトコルスタック

レイヤ		プロトコルスタック
アプリケーション層		サービスに応じて選定
データリンク層	A 規定	BASIC 系手順 コードインディペンデントモード（詳細は 5.3 を参照）
物理層		
モデム	A 規定	V.22bis + MNP4
携帯電話(回線交換方式)	B 規定	PDC: 9600bit/s※
PHS	B 規定	PIAFS: 32kbit/s 以上

※携帯網内で V.22bis + MNP4 に変換される場合がある

5.3　BASIC系プロトコルの詳細仕様　A規定

受信機とセンタを接続する収集ネットワークを利用して双方向サービスデータの収集を行う場合の、受信機と収集ネットワークの接続及びデータ転送シーケンスを定める。なお、第6章に規定するTCP/IP通信プロトコルの実装において、PSTN用通信プロトコル以外が選択された場合には本A規定は適用されない。

双方向データ放送サービスシステムを図5-2に示す。

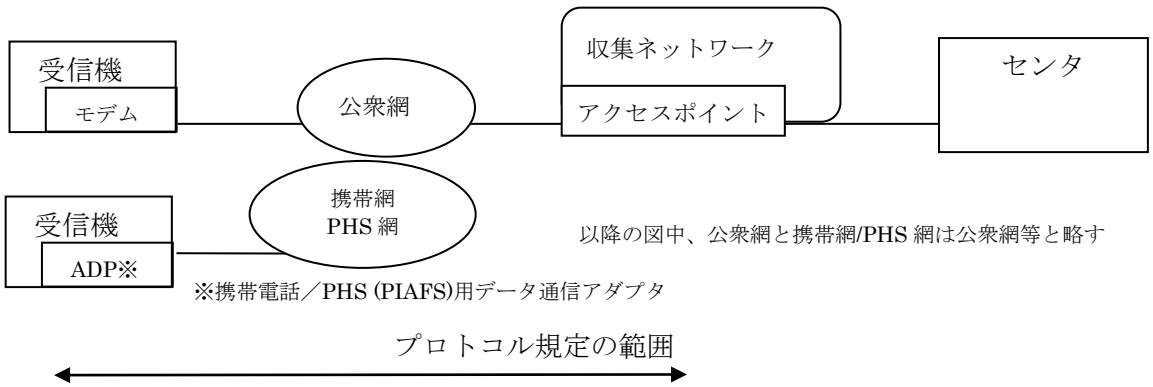


図 5-2　双方向データ放送サービスシステム

5.3.1　プロトコル条件

プロトコル条件を表5-3に示す。

表 5-3　プロトコル条件

項目	設定条件
伝送形式	ENQ、EOT による交互通信
送達確認	電文の送信毎に肯定応答、または、否定応答返送
再送制御	否定応答による再送、及び無応答時再送
最大伝送テキスト長	2048 バイト
無通信監視	タイマによる監視

5.3.2　通信条件

接続時、データ転送時及びモデムの通信条件を表5-4に示す。

表 5-4　受信機通信条件

項目	設定条件	備考
データ長（文字長）	8 ビット	接続時の通信条件
パリティ	なし	
ストップビット	1 ビット	
伝送コード体系	JIS C6220（8 単位コード）	
ローカルエコーバック	なし（リモートエコーバックあり）	
改行制御	受信機→収集ﾈｯﾄﾜｰｸ：　CR のみ送信 収集ﾈｯﾄﾜｰｸ→受信機：　CR＋LF 送信	
送信区切りコード	CR（0D H）コード	
改行コード	LF（0A H）コード	
入力訂正コード	BS（08 H）コード	
LSB/MSB(bit)	LSB First	データ転送時の通信条件
データ転送シーケンス	5.3.4 を参照	モデムの通信条件
通信方式	非同期全二重	
通信速度	5.2.3 を参照	
フロー制御	RS/CS	
MNP クラス	5.2.3 を参照	

5.3.3　接続、切断シーケンス

受信機から収集ネットワーク経由でセンタに接続するには、収集ネットワークに接続しセンタを識別するホスト番号コマンドを送出する必要がある。

(1)　接続シーケンス

a)　正常シーケンスを図 5-3 に示す。

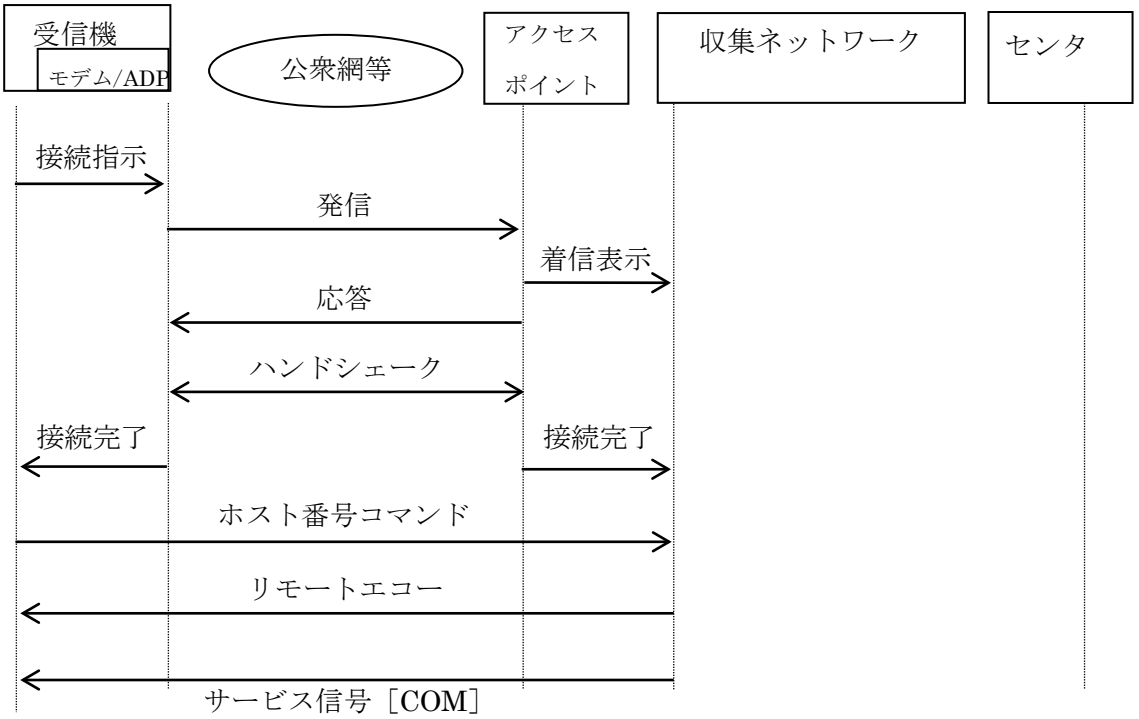


図 5-3　正常シーケンス

b)　異常シーケンス（ホスト番号コマンド誤り）を図 5-4 に示す。

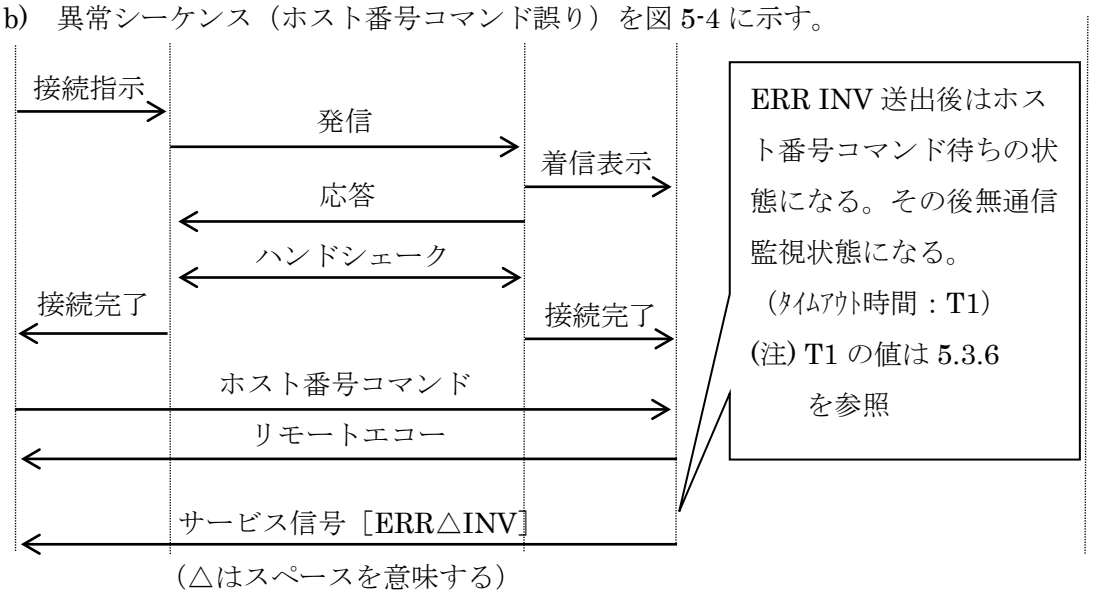


図 5-4　異常シーケンス（ホスト番号コマンド誤り）

c) 異常シーケンス（ホスト番号コマンド待ちでのセンタ側タイムアウト）を図 5-5 に示す。

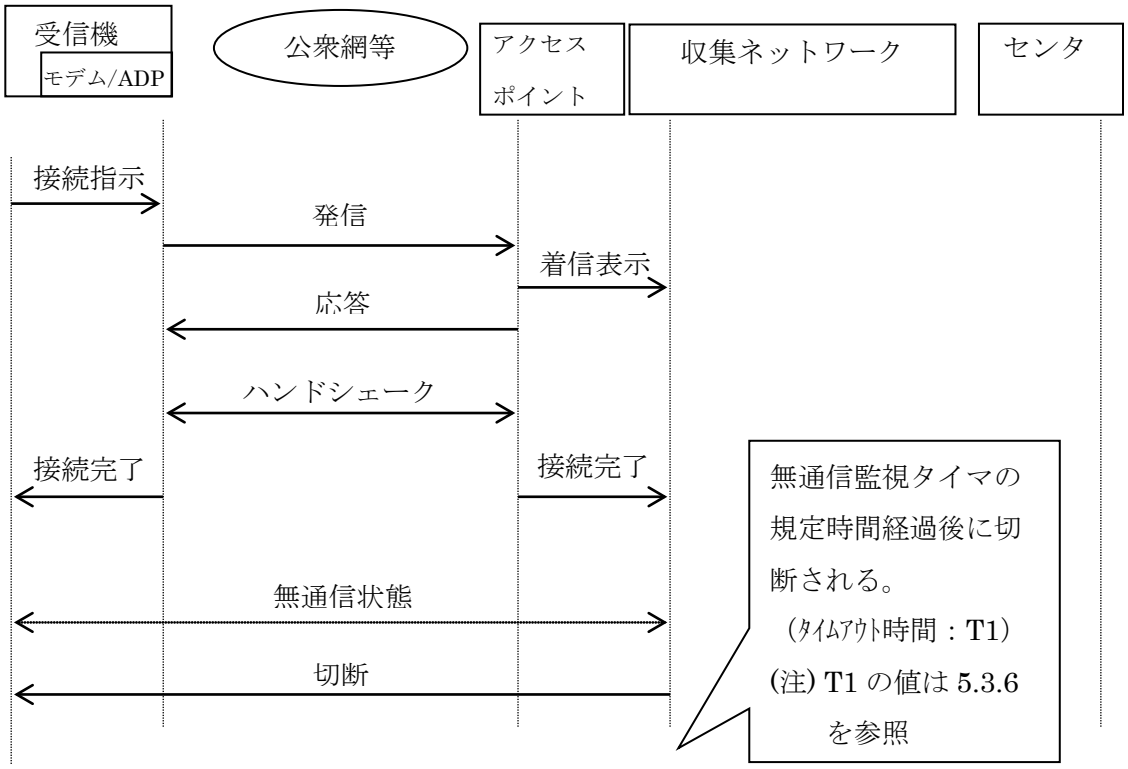


図 5-5　異常シーケンス（ホスト番号コマンド待ちでのセンタ側タイムアウト）

d) 異常シーケンス（センタの着呼拒否）を図 5-6 に示す。

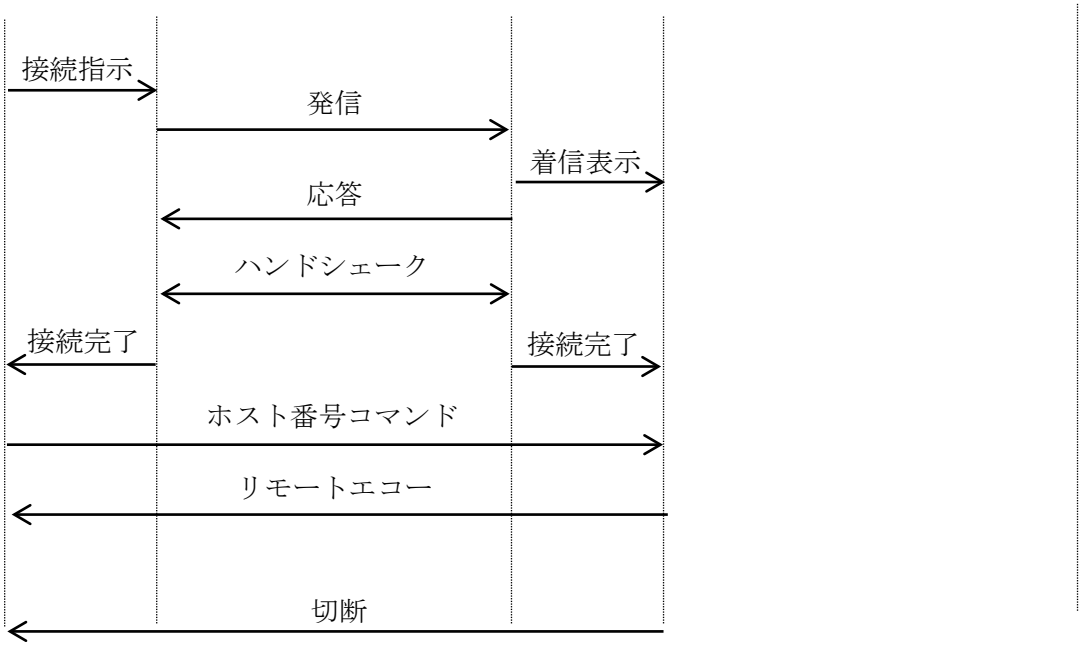


図 5-6　異常シーケンス（センタの着呼拒否）

e) 異常シーケンス（リモートエコー誤り）を図 5-7 に示す。表 5-6 リモートエコー待ちの受信機の動作を参照のこと。

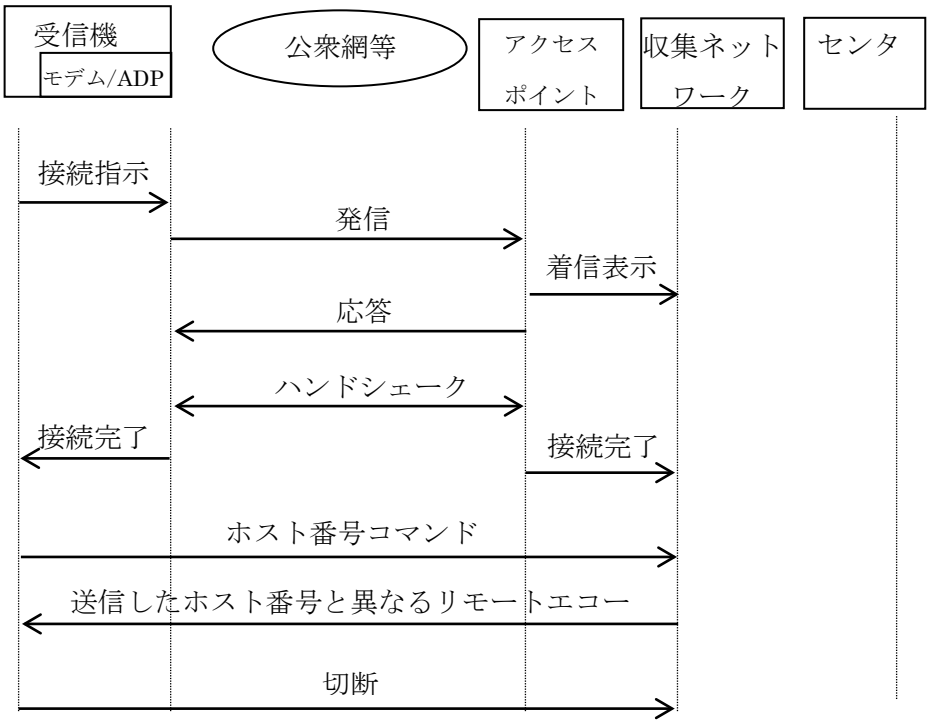


図 5-7　異常シーケンス（リモートエコー誤り）

f) 異常シーケンス（リモートエコー待ちでの受信機側タイムアウト）を図 5-8 に示す。表 5-6 リモートエコー待ちの受信機の動作を参照のこと。

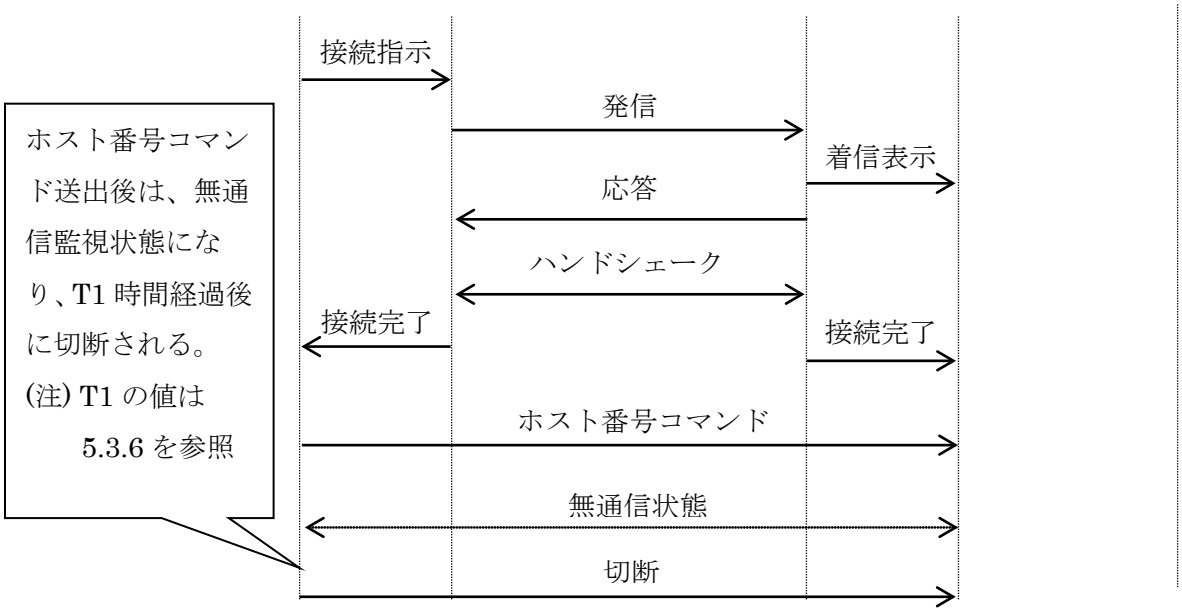


図 5-8　異常シーケンス（リモートエコー待ちでの受信機側タイムアウト）

g) 異常シーケンス（サービス信号誤り）を図 5-9 に示す。表 5-7　サービス信号待ち状態の受信機の動作を参照のこと。

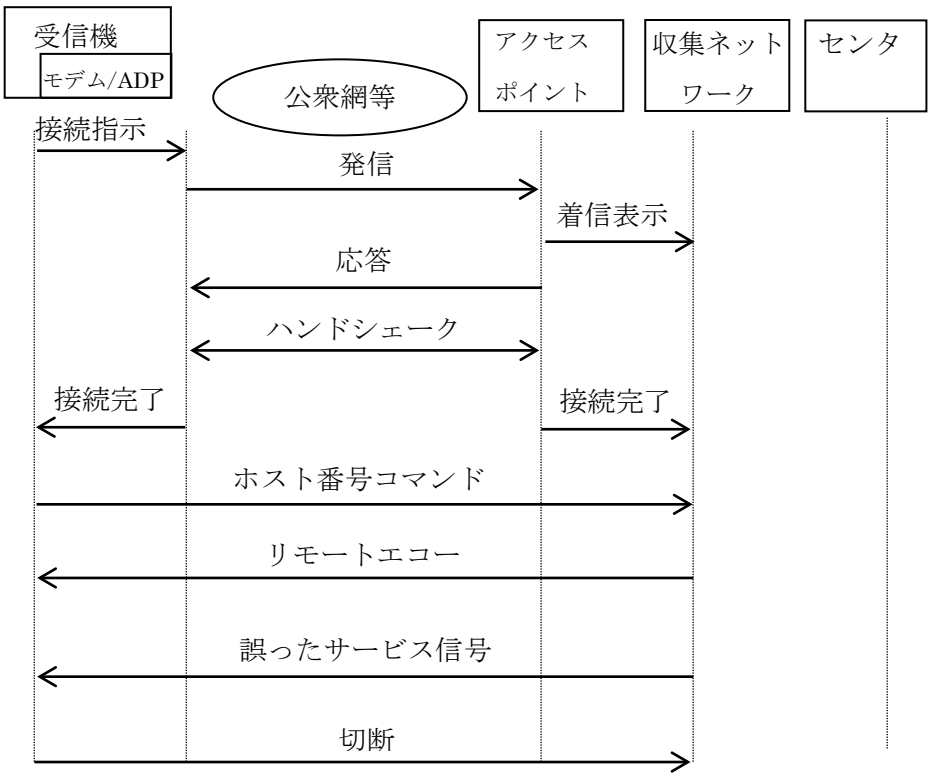


図 5-9　異常シーケンス（サービス信号誤り）

h) 異常シーケンス（サービス信号待ちでの受信機側タイムアウト）を図 5-10 に示す。表 5-7 サービス信号待ち状態の受信機の動作を参照のこと。

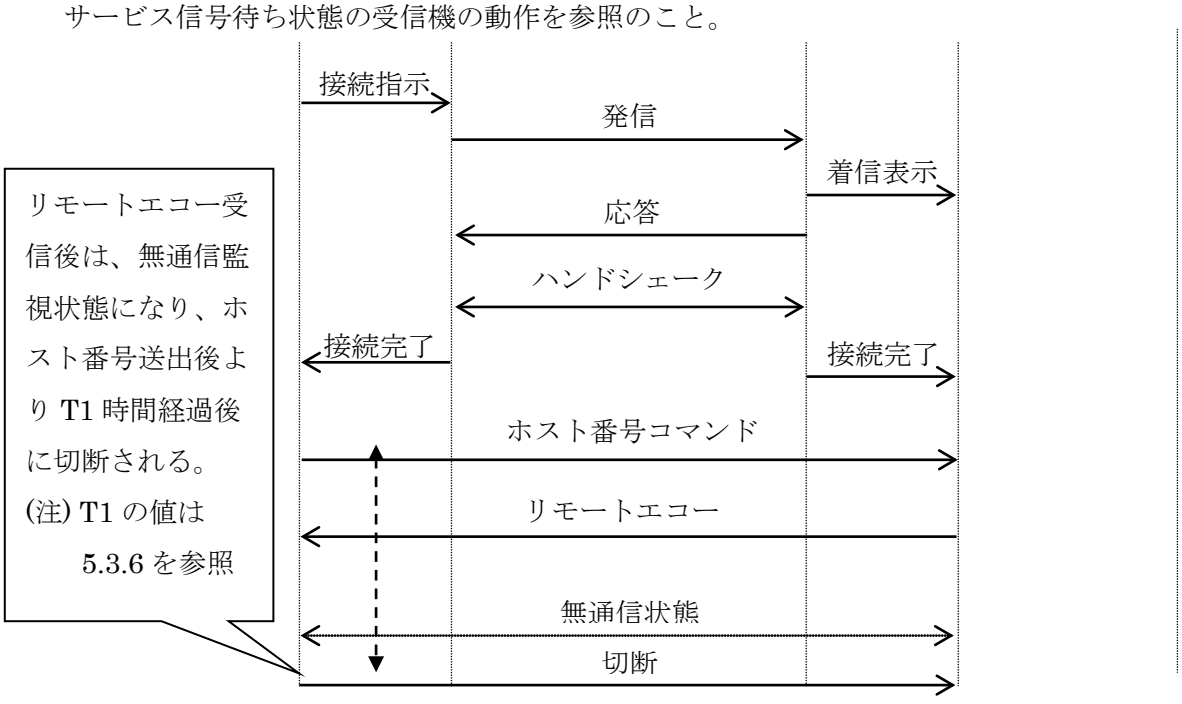


図 5-10　異常シーケンス（サービス信号待ちでの受信機側タイムアウト）

(2) 切断シーケンス

a) 受信機からの切断シーケンスを図 5-11 に示す。

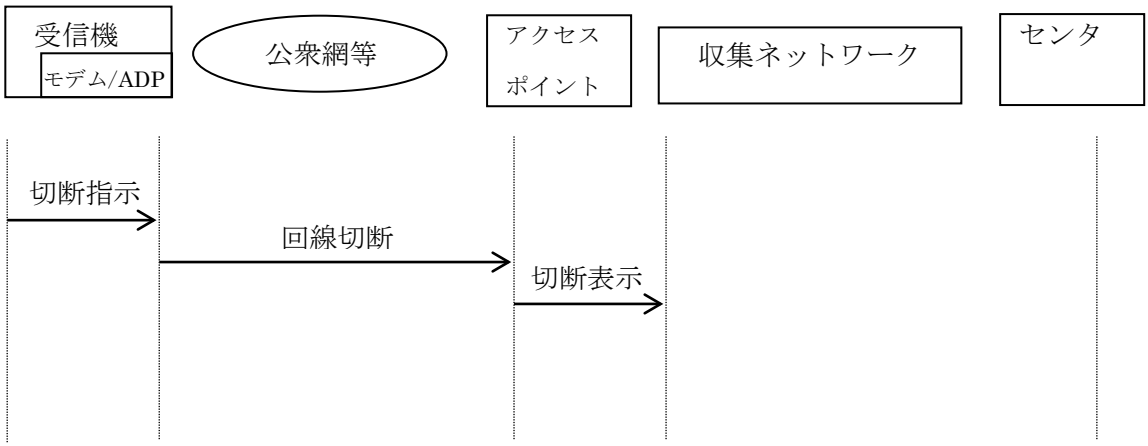


図 5-11　受信機からの切断シーケンス

b) センタからの切断シーケンスを図 5-12 に示す。

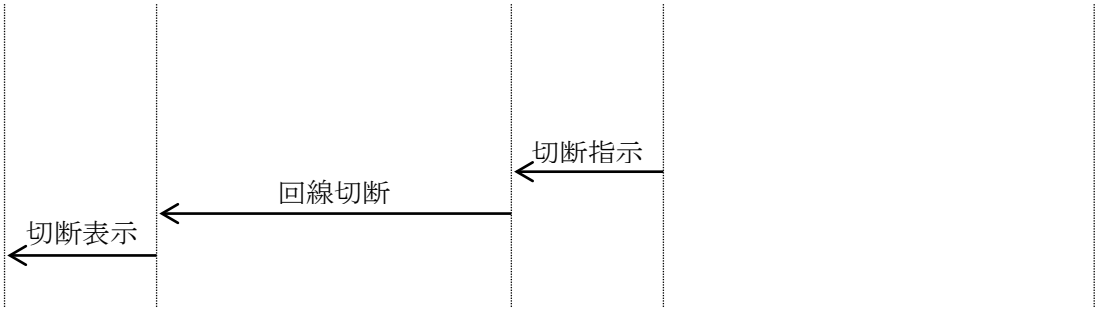


図 5-12　センタからの切断シーケンス

(3) ホスト番号コマンド及びサービス信号

ホスト番号コマンド及びサービス信号のフォーマットを表5-5に示す。

表 5-5　ホスト番号コマンド及びサービス信号のフォーマット

項目		フォーマット	記事
ホスト番号コマンド		$N_1N_2N_3N_4N_5N_6N_7N_8$ CR （エコーバックされる文字） $N_1N_2N_3N_4N_5N_6N_7N_8$ CRLF	8 桁の英数字（JIS８単位コード：0～9, A～Z, a～z）で、エコーバックされる。
サービス信号	接続完了	CR LF COM CR LF	CR：送信区切りコード LF：改行コード
	コマンドエラー	CR LF ERR△INV CR LF	△はスペースを意味する。

(4) ホスト番号コマンド送出後の受信機の動作

a) 送出したホスト番号のリモートエコー待ち状態

受信機は、ホスト番号送出後にリモートエコー受信待ち状態に遷移する。リモートエコー待ち状態の受信機の動作を表 5-6 に示す。

表 5-6　リモートエコー待ちの受信機の動作

受信信号	信号受信後の動作
送信したホスト番号と同じリモートエコー $N_1N_2N_3N_4N_5N_6N_7N_8$ CRLF を受信 （CRLF から前に遡って 8 文字分 N_1～N_8 のみ比較し、9 文字目からは無視）	サービス信号待ち状態に遷移
送信したホスト番号と異なるリモートエコー ■■■■CRLF を受信 （■■■■は、$N_1N_2N_3N_4N_5N_6N_7N_8$ を除く 0 バイト以上の任意長のコード列）	速やかに切断
ホスト番号送出後または再送後より規定時間内（受信機側のタイムアウト時間 T1 内）に CRLF を受信しない　（注１）	速やかに切断

（注1）受信機の無通信監視タイマは、ホスト番号コマンド送出後及び再送後から開始。
（T1の値は5.3.6を参照）

b) サービス信号待ち状態

受信機は、送信したホスト番号と同じリモートエコー$N_1N_2N_3N_4N_5N_6N_7N_8$ CRLFを受信後にサービス信号待ち状態に遷移する。サービス信号待ち状態の受信機の動作を表5-7に示す。

表 5-7　サービス信号待ち状態の受信機の動作

受信信号	信号受信後の動作
正しいサービス信号（接続完了）　（注 1） CRLF COM CRLF を受信	データ転送シーケンスに遷移
正しいサービス信号（コマンドエラー）（注 1） CRLF ERR△INV CRLF を受信 （△はスペース）	速やかにホスト番号コマンドを再送 再送回数は 3 回 （CRLF ERR△INV CRLF 受信 4 回で切断）
誤ったサービス信号　（注 1） CRLF COM◇ CRLF ERR○ CRLF□□□□CRLF を受信 （◇は CR 以外のコード、○はスペース以外のコード、 □□□□は COM と ERR△INV を除く 0 バイト以上の任意長のコード列）	速やかに切断
ホスト番号送出後または再送後より規定時間内(受信機側のタイムアウト時間T1内)に 正しいサービス信号を受信しない（注 2）	速やかに切断

（注1）サービス信号待ち状態に遷移してから最初のCRLFを受信するまでのデータは破棄
（注2）受信機の無通信監視タイマは、ホスト番号コマンド送出後及び再送後から開始
（T1の値は5.3.6を参照）

(5) リモートエコー

受信機からホスト番号コマンド送出時、ホスト側から受信機に対してエコーバックを行うので、受信機内でのローカルエコーバックの必要性はない。

ホスト側は受信機からホスト番号コマンドを受信しエコーバックを行ない、続いてサービス信号を送出する。

(6) ホスト側の無通信監視タイマ開始タイミング

ホスト側の無通信監視タイムアウト値T1は、回線接続完了（モデムネゴシエーション終了）時からカウントが開始され、サービス信号CRLF ERR△INV CRLF送出後に再セットされる。

5.3.4　データ転送シーケンス

(1)　電文シーケンス（例）

受信機と収集ネットワークのデータ転送シーケンスの一例を図5-13に示す。

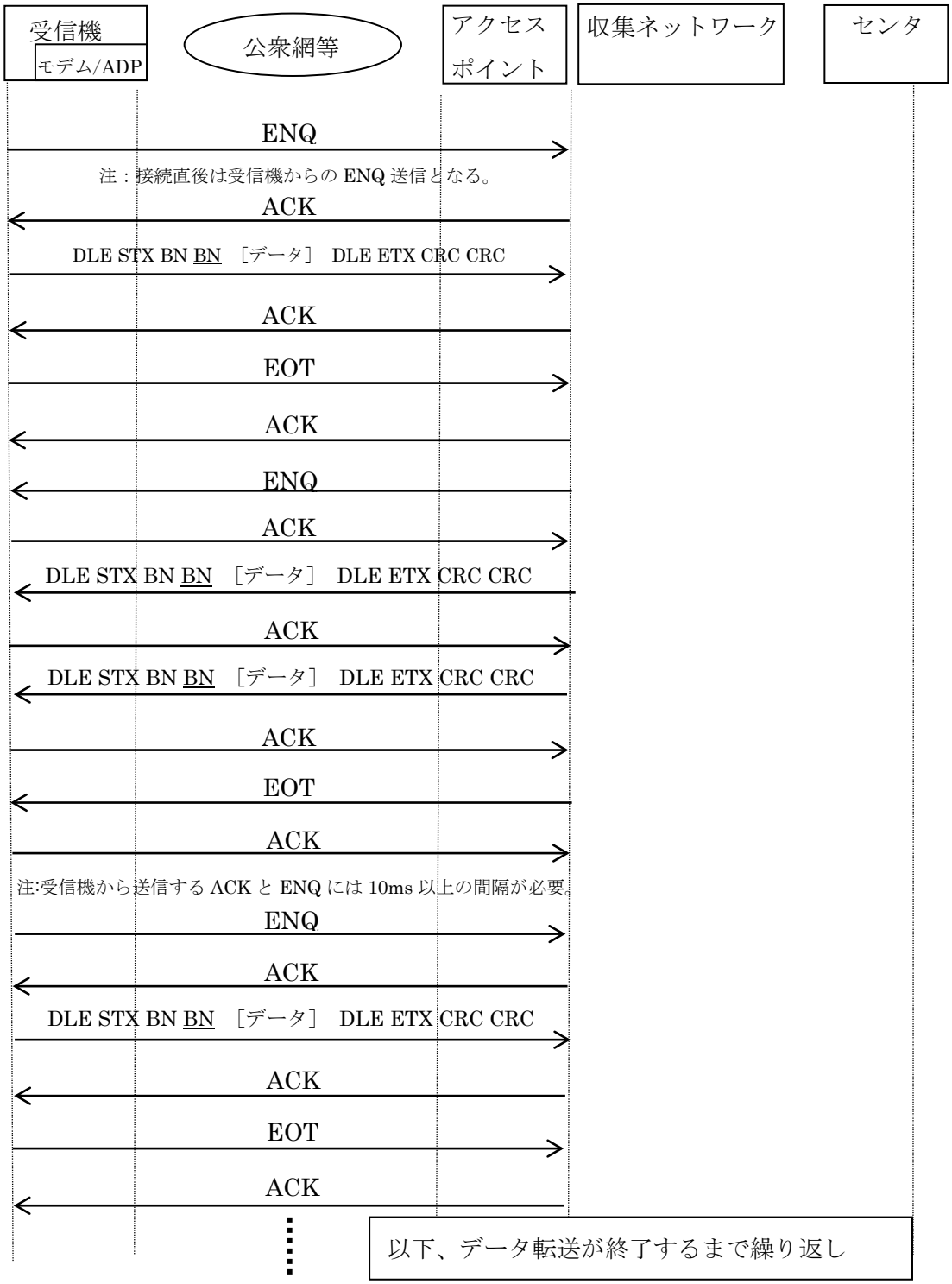
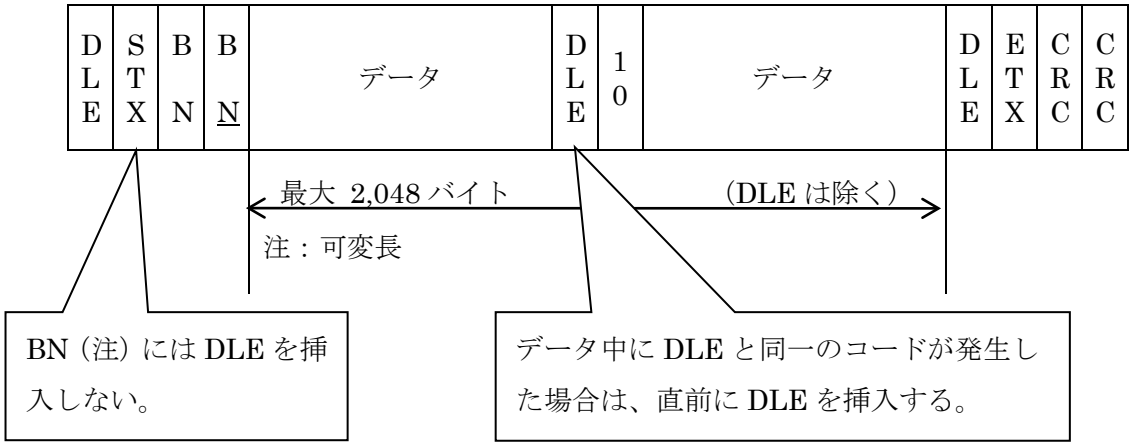


図 5-13　データ転送シーケンスの一例

(2) 電文フォーマット

a) 伝送上の電文フォーマット

伝送上の電文フォーマットを図5-14に示す。



注 BN：ブロック通番（0から255）
BN：ブロック通番（BN）の1の補数

図 5-14　伝送上の電文フォーマット

b) CRC の計算範囲

CRCの計算範囲を図5-15に示す。

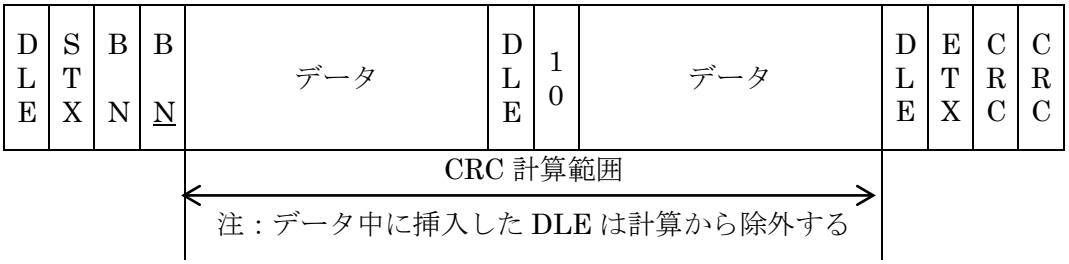


図 5-15　CRC 計算範囲

c) CRC の計算方法

CRCの計算方法には16ビットCRCを使用する。

CRC-16 計算対象のデータの、先頭バイトの最下位ビットから最後のバイトの最上位ビットまでを降べきに並べ替えた多項式にX^{16}を掛けた後、生成多項式「$X^{16}+X^{15}+X^2+1$」で割った余りになる。

CRC-16は余り（16ビット）を8ビット単位に上位、下位ビットの配列としているが、BASIC系プロトコルではセキュリティを高めるため余りの最上位ビットがCRCの最下位ビット、余りの最下位ビットがCRCの最上位ビットとなるように全ビットを降べきに並べ替える。

【計算例】

被計算データ：10_H

降べきに並べ替えたX^3にX^{16}を掛けて、
$X^{16}+X^{15}+X^2+1$で割った余りが
$X^{15}+X^5+X^4+X+1$（8033_H）となる。

8033_H(1000 0000 0011 0011)を並べ替える際に、
双方向サービスデータ収集プロトコルの場合、16 ビットを
単位として、
$CC01_H$(1100 1100 0000 0001)として CRC とする。

一般的な CRC-16 では、$01CC_H$となる。

d) ブロック通番

ブロック通番（BN）は01から始まる。この場合のブロック通番の1の補数（BN）はFE（254）となる。ブロック通番は片側から連続的にテキストを送信する場合（ENQからEOTの間）に、1ずつカウントアップしていく。ブロック通番がFF（255）に達した場合、次のブロック通番は00となる。

ブロック通番のながれを図5-16に、ブロック通番のシーケンス例を図5-17に示す。

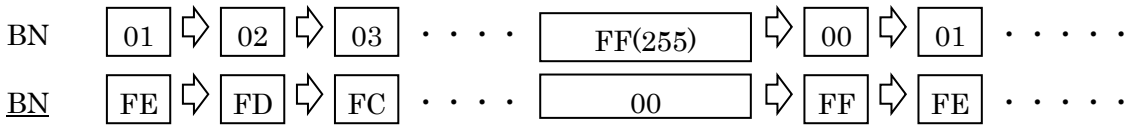


図 5-16　ブロック通番のながれ

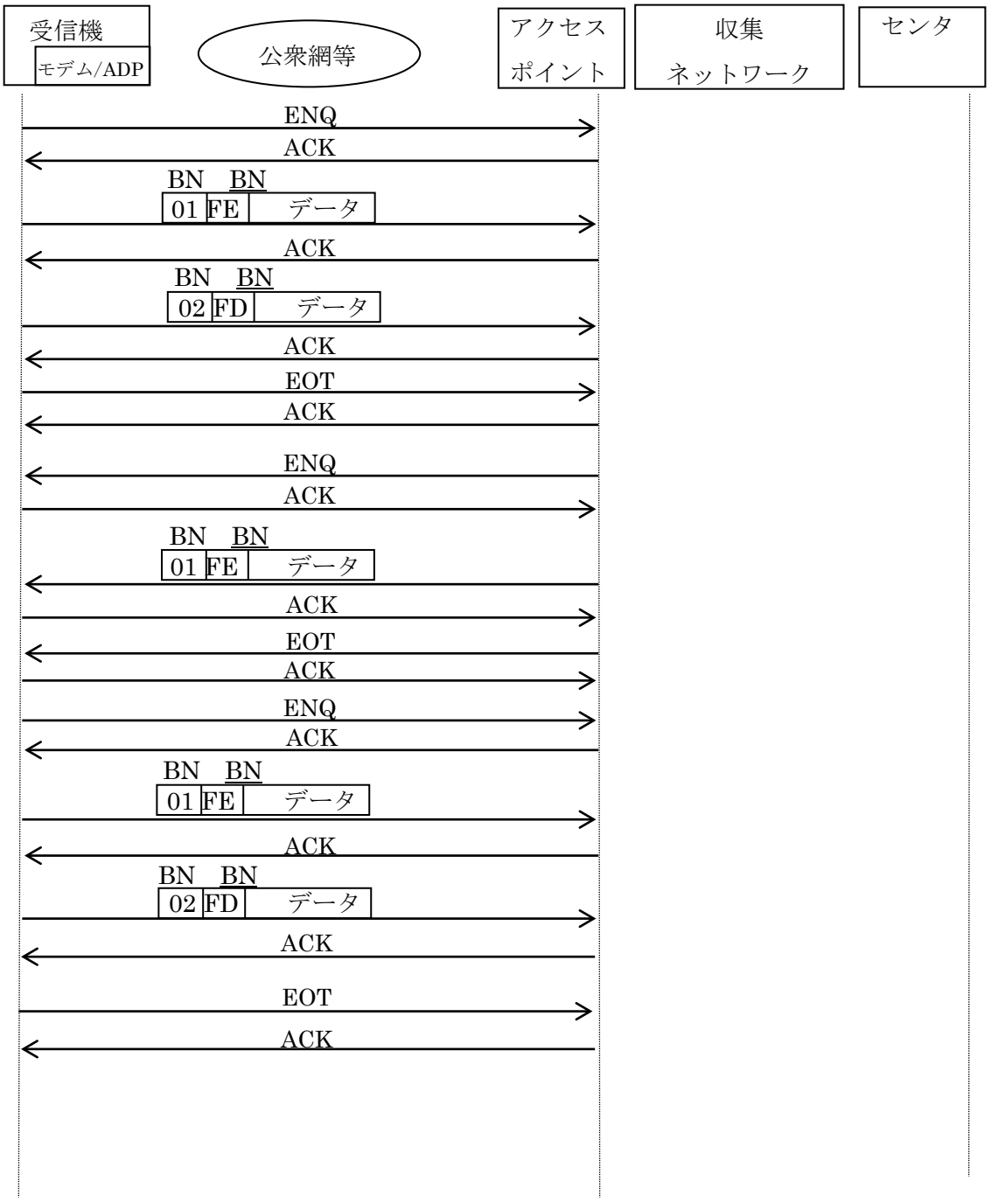


図 5-17　ブロック通番のシーケンス例

(3) 制御コードフォーマット

制御コードフォーマットを表5-8に示す。

表 5-8　制御コードフォーマット

制御符号	HEX コード	意味	記事
DLE STX	1002H	データ開始	
DLE ETX	1003H	データ終了	
ENQ	05H	回線制御権	1 バイト送受信
ACK	06H	肯定応答	同上
NAK	15H	否定応答	同上
EOT	04H	伝送終了	同上
DLE	10H	伝送制御	データ中の 10H の直前に挿入

5.3.5　状態遷移

(1)　状態遷移表

状態遷移を表5-9に示す。

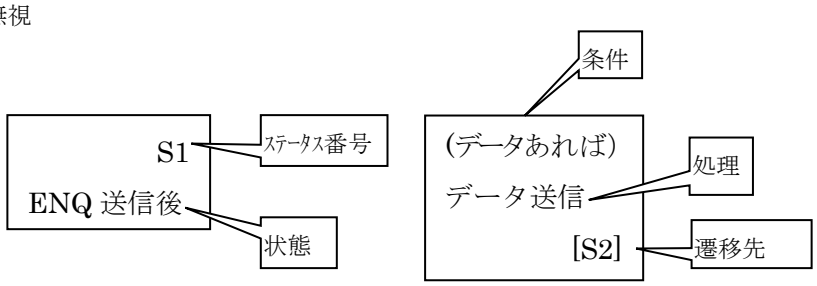
表 5-9　状態遷移

状態 / 受信コード	データ送信側				データ受信側	
	(*1)S0 ENQ 送信 [S1]	ACK 待ち			R1 ENQ 待ち	R2 ﾃﾞｰﾀ待ち
		S1 ENQ 送信後	S2 ﾃﾞｰﾀ送信後	S3 EOT 送信後		
ENQ					ACK 送信 [R2]	
ACK		データ送信 [S2]	(データあれば) データ送信 [S2] (なければ) EOT 送信 [S3]	[R1]		
NAK		ENQ 再送 [S1]	ﾃﾞｰﾀ再送 [S2]	EOT 再送 [S3]		
データ						(OK の場合) ACK 送信 [R2] (NG の場合) NAK 送信(*2) [R2] ACK 送信(*3) [R2] 切断(*4)
EOT						ACK 送信 [S0]
タイムアウト ［T2］		ENQ 再送 [S1]	ﾃﾞｰﾀ再送 [S2]	EOT 再送 [S3]	NAK 送信 [R1]	NAK 送信 [R2]
リトライアウト ［C1］		切断			切断	

(*1)　S0状態にあって、受信機から送信すべきデータがない場合には、送信すべきデータが入力されるまで、ENQの送信を保留することが望ましい。また、保留中にセンタ側のT2タイムアウト(ENQ待ち)が発生した場合、NAKを受信するが、受信機側では無視をする。

(*2)　5.3.5(2)①,③,④,⑤,⑥参照　　(*3) 5.3.5(2)②1)参照　　(*4) 5.3.5(2)②2)参照

注：空白は無視



(2) データ受信時のエラー

データ受信時のエラー（状態遷移表 R2 データ受信 NGの場合）には以下のパターンがある。

① BN と BN の関係（1 の補数）が合わない場合、NAK 送信

② BN と BN の関係は合っているが、期待値と違う場合、

1) 直前の BN と BN であった場合、当該データを破棄し ACK 送信

2) 上記以外の場合、切断

③ CRC エラーの場合、NAK 送信

④ DLE STX が無い場合、NAK 送信

⑤ DLE ETX が無い場合、NAK 送信

⑥ その他、データが規定外のフォーマットであった場合、NAK 送信

5.3.6 タイムアウト、リトライアウト値

収集ネットワークを使用する場合のタイムアウト値、リトライアウト値を表5-10に示す。

表 5-10 タイムアウト、リトライアウト値

タイムアウト値	T1	30 秒
	T2	10 秒
リトライアウト値	C1	3 回

6　TCP/IP通信プロトコル

6.1　双方向通信と伝送フェーズ

双方向伝送におけるPSTN、ISDN、携帯網およびPHS網などの公衆網等を利用するプロトコル、およびADSL、FTTH、CATVなど常時接続を利用する形態でのプロトコルを図6-1に示すような、5つのフェーズに分割し、各フェーズでの通信プロトコルを6.2節で規定する。

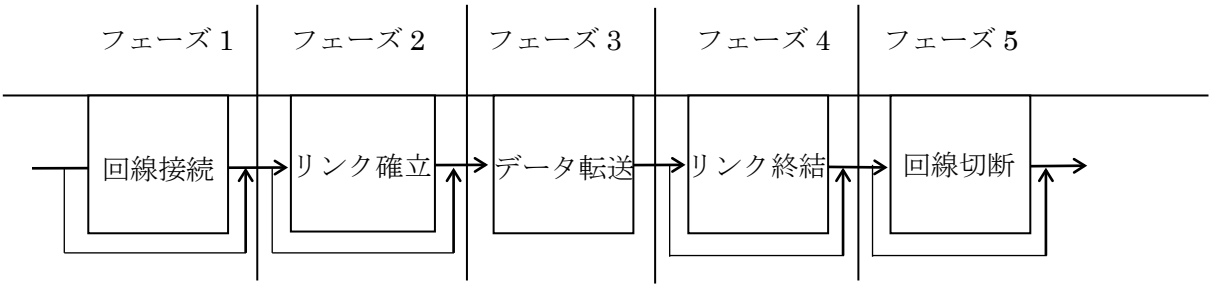


図6-1　伝送フェーズ

6.2　伝送フェーズとプロトコルスタック

6.2.1　回線接続／切断フェーズ

受信機が、公衆網等を利用してセンタとの接続／切断をするフェーズ。モデム等に対してATコマンド等を用いて回線接続／切断を行う。Ethernetを用いる形態では本フェーズはスキップされる。

6.2.2　リンク確立／リンク終結／データ転送フェーズ

リンク確立／終結フェーズは、回線接続後に受信機とセンタのデータ転送リンクを確立するため、及びデータ転送終了後受信機とセンタ間のリンクを終結するためのフェーズである。データ転送フェーズはデータリンク確立後に受信機とセンタ間でデータ転送を行うフェーズである。なお、必要なプロトコルは接続形態によって異なる。

リンク確立／終結フェーズ／データ転送のプロトコルスタックを表6-1～表6-6に示す。

(1) PSTN 用通信プロトコル

PSTN接続のプロトコルスタックを表6-1に示す。なお、本物理層に用いるモデムの通信規格V.34以上、V.42bisと併せて、第５章で規定するBASIC系プロトコルを実装すること。A規定

表 6-1 PSTN 用通信プロトコル

レイヤ	プロトコルスタック
アプリケーション層	HTTP1.1(RFC2616) ,DNS(RFC1123)A 規定, HTTP1.0(RFC1945),Telnet, FTP, NNTP, SMTP, POP3 等 B 規定の中からサービスに応じて選定
トランスポート層	TCP(RFC793) , UDP(RFC768)
ネットワーク層	IP(RFC791)/ICMP(RFC792)
データリンク層	PPP(RFC1661, 1662)/IPCP(RFC1332) PAP(RFC1334)/CHAP(RFC1994), PPP Internet Protocol Control Protocol Extensions for Name Server Addresses(RFC1877) CCP(RFC1962) B 規定
物理層	V.34 以上、V.42bis

(2) ISDN 用通信プロトコル

a) ISDN-DSU-TA 接続

ISDN-DSU-TA接続のプロトコルスタックを表6-2に示す。

表 6-2 ISDN-DSU-TA 接続用通信プロトコル

チャネル種別	B チャネル	D チャネル	
レイヤ	プロトコルスタック	プロトコルスタック	
アプリケーション層	HTTP1.1(RFC2616),DNS(RFC1123)A 規定, HTTP1.0(RFC1945), Telnet, FTP, NNTP, SMTP, POP3,等 B 規定の中からサービスに応じて選定	サービスに応じて選定	
トランスポート層	TCP(RFC793) , UDP(RFC768)		
ネットワーク層	IP(RFC791)/ICMP(RFC792)	TTC JT-Q.931	X.25(パケットレベル)※1
データリンク層	PPP(RFC1661,1662)/IPCP(RFC1332) PAP(RFC1334)/CHAP(RFC1994), PPP Internet Protocol Control Protocol Extensions for Name Server Addresses(RFC1877) CCP(RFC1962) B 規定	TTC JT-Q.921	
物理層※2	RS-232C USB		

※1： Dchパケット呼制御フェーズで使用する。

※2： TAに実装された物理インタフェースと同一規格とする。

b) ISDN-DSU-（TA 内蔵）接続

ISDN-DSU-(TA内蔵)接続のプロトコルスタックを表6-3に示す。

表 6-3　ISDN-DSU-(TA 内蔵)接続のプロトコルスタック

チャネル種別	B チャネル	D チャネル	
レイヤ	プロトコルスタック	プロトコルスタック	
アプリケーション層	HTTP1.1(RFC2616) ,DNS(RFC1123) A 規定, HTTP1.0(RFC1945) ,Telnet, FTP, NNTP, SMTP, POP3,等 B 規定の中からサービスに応じて選定	サービスに応じて選定	
トランスポート層	TCP(RFC793) , UDP(RFC768)		
ネットワーク層	IP(RFC791)/ICMP(RFC792)	TTC JT-Q.931	X.25(パケットレベル)※1
データリンク層	PPP(RFC1661,1662)/IPCP(RFC1332) PAP(RFC1334)/CHAP(RFC1994), PPP Internet Protocol Control Protocol Extensions for Name Server Addresses(RFC1877) CCP(RFC1962) B 規定	TTC JT-Q.921	
物理層	TTC JT-I.430		

※1：　Dchパケット呼制御フェーズで使用する。

(3) Ethernet 用通信プロトコル

リターン回線としてISDN,ADSL,FTTH,CATVを利用する場合。

a) ネットワーク終端装置に直接接続

ネットワーク終端装置に直接接続する際のプロトコルスタックを表6-4に示す。

表 6-4　ネットワーク終端装置に直接接続する際のプロトコルスタック

	プロトコルスタック
アプリケーション層	HTTP1.1(RFC2616) ,DNS(RFC1123) A 規定, HTTP1.0(RFC1945),Telnet, FTP, NNTP, SMTP, POP3, ,DHCP 等 B 規定の中からサービスに応じて選定
トランスポート層	TCP(RFC793) , UDP(RFC768)
ネットワーク層	IP(RFC791)/ICMP(RFC792)
データリンク層	PPP(RFC1661,1662)/PPPoE(RFC2516) /IPCP(RFC1332)　（※１） PAP(RFC1334)/CHAP(RFC1994), PPP Internet Protocol Control Protocol Extensions for Name Server Addresses(RFC1877) CCP(RFC1962) B 規定 IEEE802.2/ARP(RFC826)
物理層	IEEE802.3

※1：　常時接続サービス利用ではPPP/PPPoE/IPCPが必要

b) ルータ接続

ルータ接続する際のプロトコルスタックを表6-5に示す。

表 6-5　ルータ接続する際のプロトコルスタック

	プロトコルスタック
アプリケーション層	HTTP1.1(RFC2616) ,DNS(RFC1123) A 規定, HTTP1.0(RFC1945),Telnet, FTP, NNTP, SMTP, POP3, ,DHCP 等 B 規定の中からサービスに応じて選定
トランスポート層	TCP(RFC793) , UDP(RFC768)
ネットワーク層	IP(RFC791)/ICMP(RFC792)
データリンク層	IEEE802.2/ARP(RFC826)
物理層（※１）	IEEE802.3　（※２） IEEE802.11　（※３）

※1：　ダイヤルアップルータに具備された物理インタフェースと同一規格とする。
※2：　10BASE-T、100BASE-TX
※3：　無線LAN

(4) 携帯電話／PHS（PIAFS）を利用したデータ通信用プロトコル

携帯電話／PHS（PIAFS）を利用する際のプロトコルスタックを表6-6に示す。

表 6-6　携帯電話／PHS（PIAFS）を利用する際のプロトコルスタック

レイヤ	プロトコルスタック			
アプリケーション層	HTTP1.1(RFC2616) ,DNS(RFC1123) A 規定, HTTP 1.0(RFC1945), Telnet, FTP, NNTP, SMTP, POP3, 等 B 規定の中からサービスに応じて選定			
トランスポート層	TCP(RFC793) , UDP(RFC768)			
ネットワーク層	IP(RFC791)/ICMP(RFC792)			
データリンク層	PPP(RFC1661, 1662)/IPCP(RFC1332) PAP(RFC1334)/CHAP(RFC1994), PPP Internet Protocol Control Protocol Extensions for Name Server Addresses(RFC1877) CCP(RFC1962) B 規定 LCP Extensions(RFC1570)			
物理層（※1）	携帯電話			PHS
	PDC CDMA Cellular System	PDC-P 等（※2） CDMA Cellular System	DS CDMA, MC CDMA	PIAFS

※1　物理層はDIRD側の通信方式を表記。
携帯電話（PDC）／PHS（PIAFS）とセンターとの通信は、移動体網またはセンターでアナログ通信に変換される場合がある。
※2　携帯電話のパケット交換方式

6.2.3　物理層プロトコルの実装　A規定

物理層プロトコルの実装は、6.2.2 (1)～6.2.2(4)に規定するもののなかから1つは実装すること。なお、複数のプロトコルの実装は商品企画とする。

7　双方向通信の運用

7.1　電話番号体系とネットワーク

地上デジタルTV放送開始時期に想定されるネットワーク構成及び電話番号体系に関して解説する。

7.1.1　ネットワーク構成例

地上デジタルTV放送開始時期に想定される双方向データ放送サービスでのネットワーク構成例を図7-1に示す。

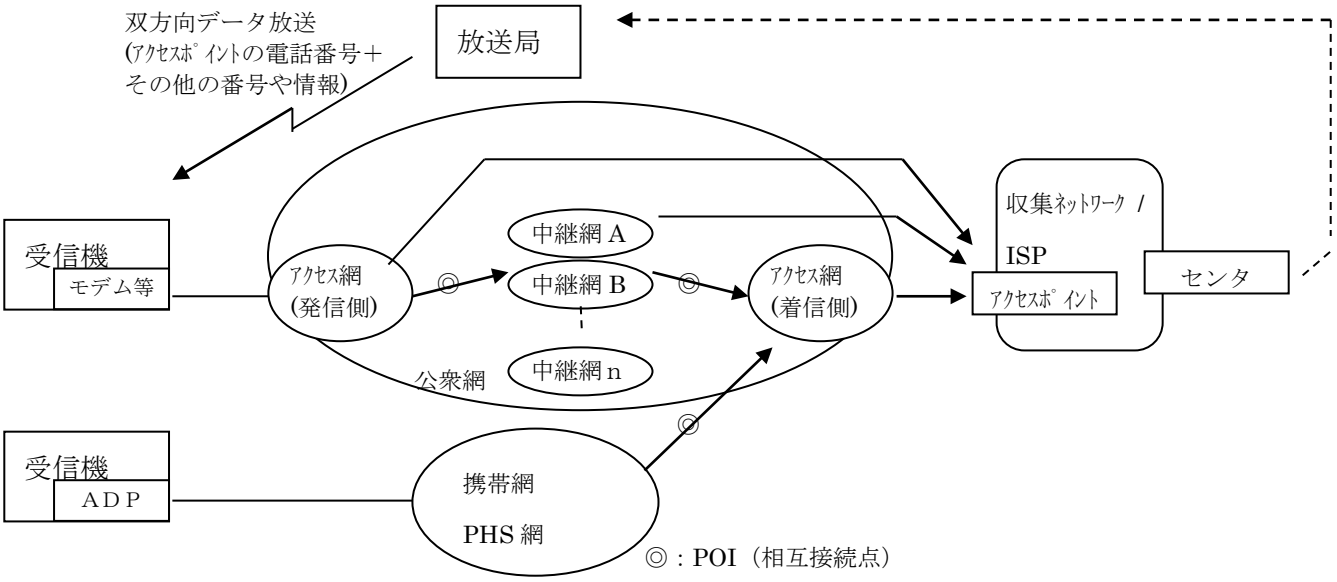


図 7-1　双方向データ放送サービスネットワーク構成例

7.1.2　電話番号体系

1999年8月25日現在の電話番号体系を表7-1に示す。なお、電話番号体系は郵政省令第82号電気通信番号規則による規定に従うものとし、将来変更される可能性がある。

表 7-1　電話番号体系

	サービス識別番号	料金負担	番号例
特殊番号	1XY	－	184, 186
			122 (※1)
通信事業者識別番号	00XY (※3)	発信側	00XY+0ABCDEFGHJ(K)
着信課金用番号	0120 (着信課金機能)	着信側	0120+DEFGHJ
	0800 (着信課金機能)	着信側	0800+DEFGHJK
	00XY+SC	着信側	00XY+SC+******** (※2)
一般番号	0ABCDEFGHJ(K)	発信側	0ABCDEFGHJ(K)
	00XY+SC	発信側	00XY+SC+******** (※2)
ネットワークサービス用番号	0180 (大量呼受付機能)	発信側	0180+ DEFGHJ
	0990 (情報料代理徴収機能)	発信側	0990+ DEFGHJ
	0570 (統一番号機能)	発信側	0570+ DEFGHJ

（※1）固定優先接続（特定事業者専用オプション）解除用番号。
（※2）SC：Service Code。00XYの事業者が提供するネットワークサービスの識別コード。料金負担方法はSCコードで識別される。
（※3）00XYで表される通信事業者識別番号は00X, 00XY, 002YZ, 002YZN1N2,0091N1N2を含む。

7.1.3　特殊番号等の発信順序と桁長

(1)　[発信番号通知番号<3>]＋[固定優先接続解除番号<3>]＋[通信事業者識別番号<7>]＋0ABCDEFGHJ(K)<10>/<11>

(2)　[発信番号通知番号<3>]＋0AB0DEFGHJ(K) <10>/<11>

(3)　[発信番号通知番号<3>]＋通信事業者識別番号<7>＋SC+********<不定>

（注意）[　　]は不要な場合がある。　< >内：99 年 9 月時点の最大桁長

7.1.4　発呼に必要な電話番号とその分類

発呼には前述の特殊番号、通信事業者識別番号の他、外線捕捉番号が必要である。ここでは、便宜的に発呼時に必要な電話番号を表7-2に分類した。この分類を用いると発呼に必要な電話番号は図7-2に示すような形式となる。

表 7-2　発呼に必要な電話番号の分類

分類名	表の分類	定義
外線捕捉番号	PBX からの外線発信番号など	外線捕捉など、各電話端末に固有な発呼に必須な番号で電話番号の先頭に付与されるもの。
特殊番号	発信番号通知番号 固定優先接続解除番号	付加サービス機能を選択するための番号。
通信事業者識別番号	通信事業者識別番号	一般電話番号に付与し、接続する通信事業者を選択するための番号。
必須電話番号*1 （電話番号）	一般電話番号 着信課金用番号 ネットワークサービス用番号	ダイヤルすると通信が確立できる必要最低限の電話番号。

*1 以下特に断りのない場合には、必須電話番号のことを電話番号と記載する。

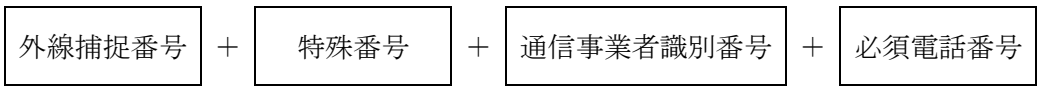


図 7-2　発呼に必要な電話番号

7.2　電話番号選択処理の流れ

双方向データ放送アプリケーション（以下アプリケーションと略す）及び受信機は、複数の電話番号から以下のフェーズを順に実行し適切な電話番号を選択し、適切な特殊番号及び通信事業者識別番号を付与し発呼する。図7-3に処理概要を示す。なお、ダイヤルアップ接続の不要な形態（ADSL、FTTH、CATV）においてはフェーズⅠ～フェーズⅢの処理は行わない。

- フェーズⅠ：接続先電話番号選択（アプリケーション機能）
  受信機に保持している通信関連情報を読出し、アプリケーション実行に必要な電話番号関連情報から、適切な唯一の電話番号を選択するフェーズ。
- フェーズⅡ：特殊番号及び通信事業者識別番号付加（受信機機能）
  フェーズⅠで唯一選択された電話番号に、視聴者設定情報に基き適切な特殊番号及び通信事業者識別番号を付加するフェーズ。
- フェーズⅢ：発呼（受信機機能）
  フェーズⅠ、フェーズⅡの処理に基き発呼するフェーズ。なお、外線捕捉番号が設定されている場合は付加する。さらに、必要に応じてホスト番号を送信する。

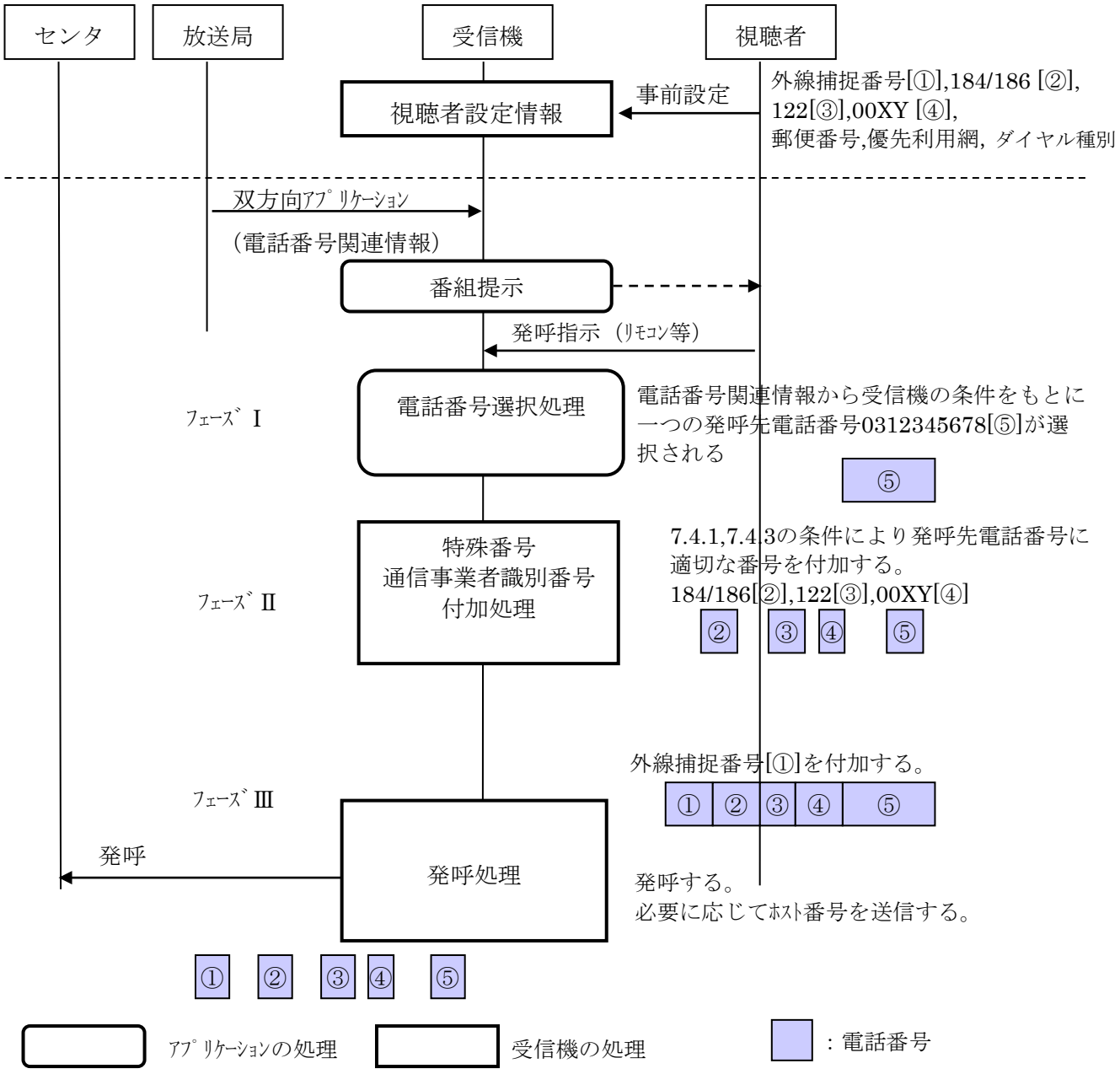


図 7-3　発呼処理の概要

7.3　放送局の運用　A規定

7.3.1　電話番号の送信条件

双方向データ放送サービスにおける電話番号の送信条件は以下の通りである。

(1)　放送局は必須電話番号のみを放送すること。

－　通信事業者識別番号(00XY 等)を付加して放送してはならない。ただし、00XY から始まる番号(00XY+SC+********)を除く。

- 固定優先接続を強制的に解除する特殊番号（122）を付加して放送してはならない。
- 視聴者の承諾を得ない場合は、発信電話番号を強制的に通知させる特殊番号（186）を付加して放送してはならない。特殊番号(186)を付加して放送する場合は、例えば、送信前に確認メッセージを表示し、BML コンテンツ上でユーザの承認動作を求める方法や受信機機能による(186)付加を求める方法など、確実な手段で承諾を得ることが望ましい。

(2) ネットワーク指定識別の運用

- 放送局は、発信者番号通知番号、および通信事業者識別番号を付与可能な電話番号には、本フラッグを ON に、受信機の番号付加機能を一時的に無効にする場合は本フラッグを OFF にして放送しなければならない。表 7-3 に現在の電話番号体系でのフラッグの運用を示す。

(3) コンテンツにおける電話番号の記述

- コンテンツで電話番号を記述する際、電話番号中に SDT（第 2 発信音）検出を必要とするときには、”,”ポーズを用いて、SDT 検出と見なす運用を行うこと。ダイヤルポーズのポーズ時間は、”,”1 つで 2～3 秒とする。

表 7-3　ネットワーク指定識別の運用

電話番号等	ネットワーク指定識別の運用
0ABCDEFGHJ(K)	On
0AB0+DEFGHJ(K)	Off
00XY+SC+*****	Off
受信機の番号付加機能を一時的に無効にする場合	Off

7.3.2　アプリケーションの機能

(1) 電話番号選択機能

受信機が保持している視聴者設定情報と通信関連情報を参照し、アプリケーションが保持している電話番号関連情報と照らし合わせて、最適な電話番号を1つ選択する機能を有すること。

(2) 発呼動作を行わない条件

アプリケーションは、以下の条件に当てはまるときは、発呼を行わない。

- 受信機の郵便番号情報を使用して電話番号を選択する場合において、受信機に郵便番号が未入力の場合。
- 受信機が有する回線等とアプリケーションが要求する回線等が異なる場合。

(3) 受信機の情報の参照

アプリケーションは、電話番号選択に必要な受信機の通信関連情報及び視聴者設定情報を参照するためのAPIを有すること。

(4) 発信者負担の双方向通信時の運用

発信課金の電話番号を用いるときなど、発信者負担の双方向通信を行う場合は、アプリケーションで承諾を得ることが望ましい。

(5)　遅延発呼時のエラー処理

遅延発呼時にビジー及びノーキャリアのエラーが発生したときには、再発呼処理、エラー処理及び必要なエラー表示をアプリケーションで行うこととする。

このとき、ノーキャリア及びビジーのエラー要因には、受信機の発呼関係の視聴者設定が誤っている可能性あるため、この点を考慮したエラー表示及びスクリプトであることが望ましい。

(6)　大量呼受付サービス時の処理

大量呼受付サービスのカットスルー接続を行うには、発呼後、交換機側の処理によりカット呼扱いになる場合があるため、アプリケーション側において、戻り値（－6）の「強制的に切断された」及び、戻り値（－8）の「回線が話中であった」が返された場合、「カット呼の成功」とみなす処理を行うこととする。

(7)　connect( )の timeout 時間の指定

connect( )を用いて発呼を行うとき、センタ応答が検出されない場合にモデムのキャリア検出タイマによる戻り値（－5）「キャリアが検出されない」の動作を保証するため、アプリケーション側においてタイムアウトとみなす時間を90000ミリ秒以上に指定することが望ましい。

(8) ユーザ ID、パスワードの提示

BMLコンテンツで発呼関数を用いて接続する場合には、ユーザID、パスワードは視聴者に表示しないこと。

(9)　ISP 接続情報の利用制限

BMLコンテンツで発呼関数を用いて接続する場合、ISP接続情報は当該BMLコンテンツ内でのみ使用し、永続的に受信機に保持しないこと。

(10) 発信者番号通知番号を BML コンテンツで付与する場合の運用

「固定優先接続解除番号」、「通信事業者識別番号」の設定がある場合には、BMLコンテンツでその「固定優先接続解除番号」、「通信事業者識別番号」を再生し、かつダイヤル数字の順序性を保証すること。ただし、通信事業者識別番号を付与不可能な電話番号の場合を除く。

(11)　BASIC 系プロトコル対応関数を用いる場合の運用

BMLコンテンツは、市場においてPSTN（モデム）を実装しBASIC系プロトコル対応の関数が実行可能な受信機と、Ethernetのみを実装した受信機などBASIC系プロトコル対応関数が実行不可能な受信機が混在することを考慮し、BASIC系プロトコル対応関数を用いる場合は、当該受信機がPSTNかどうかを判断し、PSTNを実装しない受信機に対してはその受信機が実行できるプロトコルで通信しなければならない。

(12)　自動接続機能で確立された PPP 接続回線の切断

受信機の自動接続機能で確立されたPPP接続回線をBMLコンテンツから切断関数disconnectPPP( )を用いて切断する際には、BMLコンテンツ上で視聴者の承諾を得なければならない。

7.3.3　アプリケーションが保持すべき情報

アプリケーションは以下の情報を必要に応じて保持する。

(1)　ホスト番号

アプリケーションで指定するセンタ等の識別番号。

(2)　電話番号関連情報

アプリケーションは以下の情報要素で構成される情報を必要に応じて保持すること。

a)　発信地域指定郵便番号

電話番号に発信できる地域指定のための郵便番号。

b)　電話番号

接続先の一般電話番号。

（e.g. 0ABCDEFGHJ(K), 00XY-SC******）

c)　回線種別

受信機側の回線種別を指定する。複数設定可。

（e.g.　PSTN/ 携帯回線/ PHS 回線）

d)　物理層プロトコル

受信機側の物理層プロトコルを指定する。回線種別毎に設定される。

（e.g.　V.22bis-MNP4, 32kPIAFS）

e)　データリンク・転送プロトコル

受信機とセンタ間（収集ネットワーク間）のデータリンク確立・データ転送プロトコルを指定する。

（e.g.　X.28 一部準拠-BASIC 系,TCP/IP）

f)　ネットワーク指定識別

受信機で当該電話番号に、発信者番号通知番号及び通信事業者識別番号を付与するときは ON に設定する。

(3)　ISP 接続情報

a)　ISP名

ISP の事業者名を指定する。最大 64 桁(128 バイト以下)の文字列とする。

（e.g.　地上ネット、ARIB-net）

b)　AP電話番号

放送局が指定する ISP、または closed ネットワーク事業者の提供するアクセスポイントの電話番号。複数設定可であり、選択論理は BML コンテンツに依存する。

（e.g.　0ABCDEFGHJ(K),00XY+SC******）

c)　ユーザID

放送局が指定する ISP、closed ネットワーク事業者へアクセスするためのユーザ ID を指定する。半角英数記号の組合せで使用する。最大 64 桁(64 バイト以下)の文字列とする。

（e.g.abcd1234,abcd@arib.or.jp）

d) パスワード

放送局が指定する ISP、closed ネットワーク事業者へアクセスするためのパスワードを指定する。半角英数記号の組合せで使用する。最大 32 桁(32 バイト以下)の文字列とする。

e) ヘッダ圧縮

データの転送速度を向上させるため、TCP/IP ヘッダを圧縮する場合、「使用する」とする。

f) ソフトウェア圧縮

データの転送速度を向上させるため、データ圧縮を行う場合、「圧縮する」とする。

g) DNS-IPアドレス（プライマリー）

放送局が指定する ISP、closed ネットワーク事業者の DNS サーバ（プライマリー）の IP アドレスを指定する。10 進数表記（0～255)、“.”を区切り文字とする。

(e.g. ***.***.***.***)

h) DNS-IPアドレス（セカンダリー）

放送局が指定する ISP、closed ネットワーク事業者の DNS サーバ（セカンダリー）の IP アドレスを指定する。10 進数表記（0～255)、“.”を区切り文字とする。

(e.g. ***.***.***.***)

i) 無通信切断タイマ値

発呼関数を用いて PPP 接続した回線において、一定時間パケット送受信がない場合、以下の値を参照して回線を切断する。

idleTime：1 分以上、20 分以下とする。

7.3.4 ホスト接続のための情報

(1) URI

URIの情報要素を表7-4に示す。

表 7-4 URI の情報要素

情報要素名	リテラル	備考
スキーム名	http:	
	https:	TLSまたはSSLセキュリティを利用する場合
ホスト名	英数字 記号	ＩＰアドレス直接指定は(2)を参照 RFC2396 に従う
ポート番号	数字（0～65535）	ポート番号の使用については(3)を参照
パス名	英数字 記号	RFC2396 に従う

(2) IP アドレス

IPv4ネットワークでは８bitずつ、10進数表記し（0～255）、”.”を区切り文字とする。

（例） ***. ***. ***. ***

なお、IPv6のネットワークのアドレス指定は行わないこと。

(3) ポート番号

ポート番号を用いる場合は、Assigned Number(RFC1340)の規定に従う。表7-5にポート番号の規定を示す。

表 7-5 ポート番号

ポート番号	規定
1 ～ 1023	well known port
1024 ～ 49151	IANA 登録済み port
49152 ～ 65535	IANA 動的

7.4 望ましい受信機機能

7.4.1 受信機が管理する情報 A規定

受信機は、受信機のハードの状態を示す通信関連情報と視聴者が設定する視聴者設定情報を保持する。

(1) 通信関連情報

a) 回線種別

受信機が備える回線種別の中で利用可能な回線種別を示す。複数可。

（e.g. PSTN/ 携帯回線/ PHS 回線）

b) 物理層プロトコル

受信機が備える回線種別毎に利用可能な物理層プロトコルを示す。複数可。

（e.g. V.22bis-MNP4(PSTN), 32kPIAFS(PHS), PDC(携帯)）

c) データリンク・転送プロトコル

受信機が備える受信機とセンタ（収集ネットワーク）間のデータリンク確立・データ転送プロトコルを示す。複数表示可。

（e.g. X.28 一部準拠-BASIC 系,TCP/IP）

(2) 視聴者設定情報

以下に示す情報は視聴者が受信機の持っているユーザインターフェイスを介して入力され、受信機に保持されている情報である。これらの情報は受信機の不揮発性メモリーに格納される。また、電話番号体系変更に伴う変更に対応できるよう拡張性を持っていることが望ましい。

a) 郵便番号

受信機の存在する場所の郵便番号（7 桁）を示す。

（e.g. 100-0004）

b) 優先利用回線種別

受信機に接続された回線の中から優先される一つの回線種別を示す。

（e.g. PSTN/ 携帯回線/ PHS 回線）

c) 通信事業者識別番号

視聴者が選択した通信事業者を選択するための識別番号。（現在 7 桁）

（e.g. 00X, 00XY, 002YZ, 0091N_1N_2）

d) 固定優先接続解除番号

固定優先接続を解除する番号。（現在 3 桁）

（e.g. 122 ）

e) 発信者番号通知番号

発信者の電話番号を着信者に通知するか拒否するかを設定する番号。（現在 3 桁）

（e.g. 186, 184 ）

(3) 外線捕捉番号

外線捕捉など受信機に固有な発呼に必要な番号を不揮発性メモリーに保持すること。

（e.g 0, ）

(4) ダイヤル種別

利用するPSTN回線のダイヤル種別を、不揮発性メモリーに保持すること。

（e.g Tone, 10pps, 20pps ）

7.4.2 受信機が管理する情報（TCP/IP） A規定

情報要素の内容については、STD-B21の規定による。

(1) 通信関連情報 STD-B21 11.5.7.2

セキュリティクラスの値としてCASは除く。

(2) セキュリティ通信関連情報 STD-B21 11.5.7.3

実装セキュリティ種別

表 8-6 の通りとする。

(3) 通信デバイス情報 STD-B21 11.5.7.4

6.2.3物理層プロトコルの実装で選択されたものについて実装する。

(4) 視聴者設定情報 STD-B21 11.5.7.1

- 共通情報 STD-B21 11.5.7.1(1)
- ISP 接続情報 STD-B21 11.5.7.1(2)①

以下の情報要素は、本編で規定する。

a) ISP 名

ISP名情報要素は特定のISPへの接続を前提とした受信機においては、B規定とする。

b) ユーザ ID

最大 64 桁の半角英数記号の組み合わせとする。

c) パスワード

最大 32 桁の半角英数記号の組み合わせとする。

d) ヘッダ圧縮　B 規定

e) ソフトウェア圧縮　B 規定

f) 無通信切断タイマ値

デフォルト推奨値を 180 秒とする。可変とする場合の設定可能範囲は、1 分以上、20 分以下が望ましい。以下の場合、この値の時間無通信状態であれば回線を切断する。

- 受信機の自動接続機能で PPP 接続された場合
- connectPPPWithISPParams( )実行時に、引数 idleTime の指定がない場合
- sendTextMail( )、sendMIMEMail( )を実行した場合

g) 通信事業者識別情報

setISPParams( )で指定された値を保持すること。

・固定 IP 接続情報　　STD-B21　11.5.7.1(2)②

Ethernet に対応しない受信機においては管理対象外とする。

・接続形態情報　　STD-B21　11.5.7.1(2)③

-Ethernet に対応しない受信機においては管理対象外とする。

-IP アドレス取得指定における値「PPP/PPPoE プロトコル」は B 規定とする。

参考 : PPP/PPPoE プロトコルが搭載されたルータに接続し使用される場合を考慮し、受信機への PPP/PPPoE プロトコル搭載は、B 規定とする。

・TCP/IP アプリケーション設定情報STD-B21　11.5.7.1(2)④

a) SMTP サーバ名/アドレス　B 規定

b) POP サーバ名/アドレス　B 規定

c) メールアドレス　B 規定

d) メールパスワード　B 規定

e) HTTPProxy サーバ名/アドレス　B 規定

f) HTTPProxy サーバポート番号　B 規定

g) FTPProxy サーバ名/アドレス及び FTPProxy サーバポート番号

については運用しない。

7.4.3 回線種別毎の設定条件

視聴者設定情報のなかで、実装された回線種別、および機器毎によって必要となる情報要素が異なる。回線種別毎の情報要素項目を表7-6～表7-8に示す。なお、回線種別、接続形態は

STD-B21　第11章、および解説9を参照すること。

- 視聴者設定情報の優先利用回線種別（※1）は通信関連情報の回線種別から選択されること。ただし、複数の回線種別に対応しない受信機を除く。
- 視聴者設定情報の固定優先接続解除番号（※3）は視聴者設定情報の通信事業者識別（※2）が設定されている場合のみ設定可能なこと。

表 7-6　PSTN,ISDN,携帯電話の設定条件

回線種別 / 情報要素	PSTN	ISDN				携帯電話		
	モデム	モデム	TA (Serial)	TA (ST)	ルータ	PDC	PHS	PDC-P
優先利用回線種別（※1）	○	○	○	○	○	○	○	○
通信事業者識別（※2）	○	○*1	○*1	○*1	－	－	－	－
固定優先接続解除番号（※3）	○	○*1	○*1	○*1	－	－	－	－
発信者番号通知番号	○	○*1	○*1	○*1	－	○*2	○*2	－
外線捕捉番号	○	○*1	○*1	○*1	－	－	－	－
ダイヤル種別	○	○	－	－	－	－	－	－
IP アドレス取得指定	－	－	－	－	○	－	－	－

凡例　○：設定を必要とする項目　　―：無視

*1　：　TAの機種によっては7.4.4で示す番号付加機能を持つものがあることを考慮する。

*2　：　携帯端末の設定によっては7.4.4で示す番号が付加されることを考慮する。

表 7-7　ADSL,FTTH の設定条件

回線種別 / 情報要素	ADSL				FTTH	
	ADSL モデム	ADSL モデム（非共用）	ルータ	モデム（アナログ）	ONU	ルータ
優先利用回線種別（※1）	○	○	○	○	○	○
通信事業者識別（※2）	－	－	－	○*1	－	－
固定優先接続解除番号（※3）	－	－	－	○*1	－	－
発信者番号通知番号	－	－	－	○*1	－	－
外線捕捉番号	－	－	－	○*1	－	－
ダイヤル種別	－	－	－	○	－	－
IP アドレス取得指定	○	○	○	－	－	○

凡例　○：設定を必要とする項目　　―：無視

*1　：　ADSLモデムの機種によっては7.4.4で示す番号付加機能を持つものがあることを考慮する。

表 7-8　CATV の設定条件

回線種別 / 情報要素	CATV	
	ケーブルモデム	ルータ
優先利用回線種別（※1）	○	○
通信事業者識別（※2）	－	－
固定優先接続解除番号（※3）	－	－
発信者番号通知番号	－	－
外線捕捉番号	－	－
ダイヤル種別	－	－
IP アドレス取得指定	○	○

凡例　○：設定を必要とする項目　　—：無視

7.4.4　番号付加機能　A規定

受信機は表7-9に示す条件で特殊番号及び通信事業者識別番号を付加すること。

表 7-9　　受信機の番号付加条件

回線種別	ネットワーク指定識別	発信番号通知(186/184)が設定されているとき	固定優先接続解除番号(122)が設定されているとき	通信事業者識別番号(00XY 等)が設定されているとき
PSTN(*2)	OFF	×	×	×
	ON	○	○(*1)	○
携帯回線	OFF	×	×	×
	ON	○	×	×
PHS 回線	OFF	×	×	×
	ON	○	×	×

○：付加する　×：付加しない

(*1) 固定優先接続を設定している回線を利用する場合で、固定優先接続指定をしている通信事業者以外の通信事業者識別番号を入力したときのみ、122を付与することが望ましい。

(*2) 大量呼受付サービス（vote( )関数）指定時は、ネットワーク指定識別の指定に関わらず特殊番号及び通信事業者識別番号を付加しないこと。

7.4.5　発呼機能　A規定

(1)　受信機内に保持している外線捕捉番号を付加し発呼できること。

(2)　受信機内に保持しているダイヤル種別に従い、トーン、10 パルス毎秒又は 20 パルス毎秒でダイヤル可能なこと。

(3)　受信機が付与した外線補足番号の任意の点、及び各特殊番号・通信事業者識別番号の前後に於いてダイヤルポーズ可能であること。（ポーズ時間は商品企画とする。）ダイヤルする際に、電話番号の任意の点でコンテンツで電話番号に記載される”,”に従ってダイヤルポーズできること。（ポーズ時間は、”,”1 つで 2～3 秒とする。）

注）(1)~(3)はダイヤルアップ接続時についてのみ有効である。

(4)　ISP へ未接続の状態時に BML コンテンツからデータ送信関数等が実行された場合は、予め受信機に設定してある ISP 接続情報を使用して発呼できること。

(5)　ISP へ未接続の状態時に BML コンテンツから発呼関数が実行された場合は、予め受信機に設定してある ISP 接続情報を参照して発呼できること。ただし、優先利用回線種別が Ethernet の場合を除く。

(6)　ISP へ未接続の状態時に BML コンテンツから発呼関数によって発呼できること。

(7)　受信機に複数の通信回線が接続されている場合、発呼動作は視聴者の選択した優先利用回線を使用する。ただし、優先利用回線種別が Ethernet の場合であって、PPP 接続が可能な場合においては、視聴者に承諾を得た場合に限り、当該発呼のみ発呼関数 connectPPP( )の実行を可能とする。

(8)　呼が既に確立している場合は、新たな発呼は行わない。

7.4.6　発呼禁止機能　B規定

(1)　発呼禁止状態の設定

子供等のいたずらな発呼を避けるため、受信機は発呼禁止状態を設定できることが望ましい。発呼禁止状態の設定・解除には 4 桁程度の暗証番号を必要とし、管理者以外は状態の変更ができないことが望ましい。

(2)　着呼中の受信機動作

着呼中においては、発呼しない。

7.4.7　視聴者設定情報の運用

双方向データ放送サービス以外への使用防止、および個人情報の漏洩防止の観点から、視聴者設定情報は以下の運用を行うこと。

7.4.7.1　　視聴者設定情報の保護機能　A規定

(1)　受信機機能として ISP、あるいは常時接続用ネットワーク事業者へのユーザ ID、パスワードによるアクセス認証、および視聴者設定情報設定時は、セキュリティ確保のためパスワード

は表示せず"＊"等の文字列に置換表示すること。

(2) 受信機の譲渡、廃棄時に視聴者設定情報を無効化できる機能を設けること。

7.4.7.2 視聴者設定情報の設定ユーザインタフェースのガイドライン

受信機は視聴者設定情報を入力、変更、削除するためのユーザインタフェース機能を有すること。A規定

(1) メニュー形式やヘルプ、ナビゲーションによる誘導設定などを用いて設定ミスを避けるようなユーザインタフェース機能を持つこと。B 規定

(2) 視聴者設定情報を入力時に、既に設定情報があり、受信機機能で変更をする場合は、現設定情報を表示すること。ただし、パスワードについてはセキュリティ保護の観点から表示の対象外とする。B 規定

7.4.8 発呼時表示の運用 A規定

(1) 既に接続が確立している場合及び、発呼関数を用いて接続する場合には、接続に関わるダイアログ表示は行わないこと。

(2) 未接続の状態においてデータ送信関数等の実行により発呼する場合には、接続される旨を接続先（ISP 名、電話番号等）とともに表示することが望ましい。B 規定

(3) 回線使用中は視聴者に認識可能な表示（フロントパネルの LED や OSD など）を行うこと。

(4) 発呼処理でのエラー発生時は、エラーが発生したことを視聴者に認識可能な表示（フロントパネルの LED や OSD など）を行うこと。

7.4.9 ISP接続情報の運用

(1) 事業者識別情報

視聴者設定情報のISP接続情報が設定された場合は、受信機機能によって事業者識別情報を永続的に保持すること。事業者識別情報の設定条件を表7-10に示す。

表 7-10 事業者識別情報設定条件

値（16 進表記）			定義
00	XXXX	XX	未設定状態、または受信機機能で消去されたとき設定
（1 バイト）	（2 バイト）	（1 バイト）	
8F	XXXX	XX	受信機機能で設定されたとき設定
（1 バイト）	（2 バイト）	（1 バイト）	
上記以外			左記の ID を持つ放送事業者によって設定されたとき
FF	original_network_id	broadcaster_id	
（1 バイト）	（2 バイト）	（1 バイト）	

注：Xは、don't careの意

(2) status 値

ISP接続情報が受信機機能で設定される場合、運用制限は設けない。遷移したstatus値を受信機機能にて永続的に保持すること。

(3) ispname

ispname設定方法は商品企画とする。最大64桁の文字列長（128バイト）とする。

7.4.10 登録発呼の運用

通信の集中などによって双方向通信が成功しなかった双方向呼を、コンテンツによって受信機の登録発呼領域に記録し、番組終了後も視聴者の指示によって発呼・データ送信処理を行うこと機能をもつこと。登録発呼機能における送信は、登録発呼コンテンツもしくは登録発呼機能を有する受信機アプリケーションによって行われるが、受信機アプリケーションによる登録発呼はB規定とする。詳細は、第三編 5.16「登録発呼の運用」参照のこと。

7.5 通信エラー時のガイドラインA規定

自動接続機能で正常に接続、データ送受信、切断などが行われなかった場合、エラー通知を行う。表示方法については商品企画とする。自動接続以外で検出したエラー通知、およびデータ送受信時に検出したエラー通知についてはB規定とする。

7.6　電話番号処理の詳細

フェーズⅠ～フェーズⅢにおける処理とアプリケーション情報、および視聴者設定情報、通信関連情報の詳細な関係を図7-4に示す。TCP/IPプロトコル使用時については図7-5に示す。

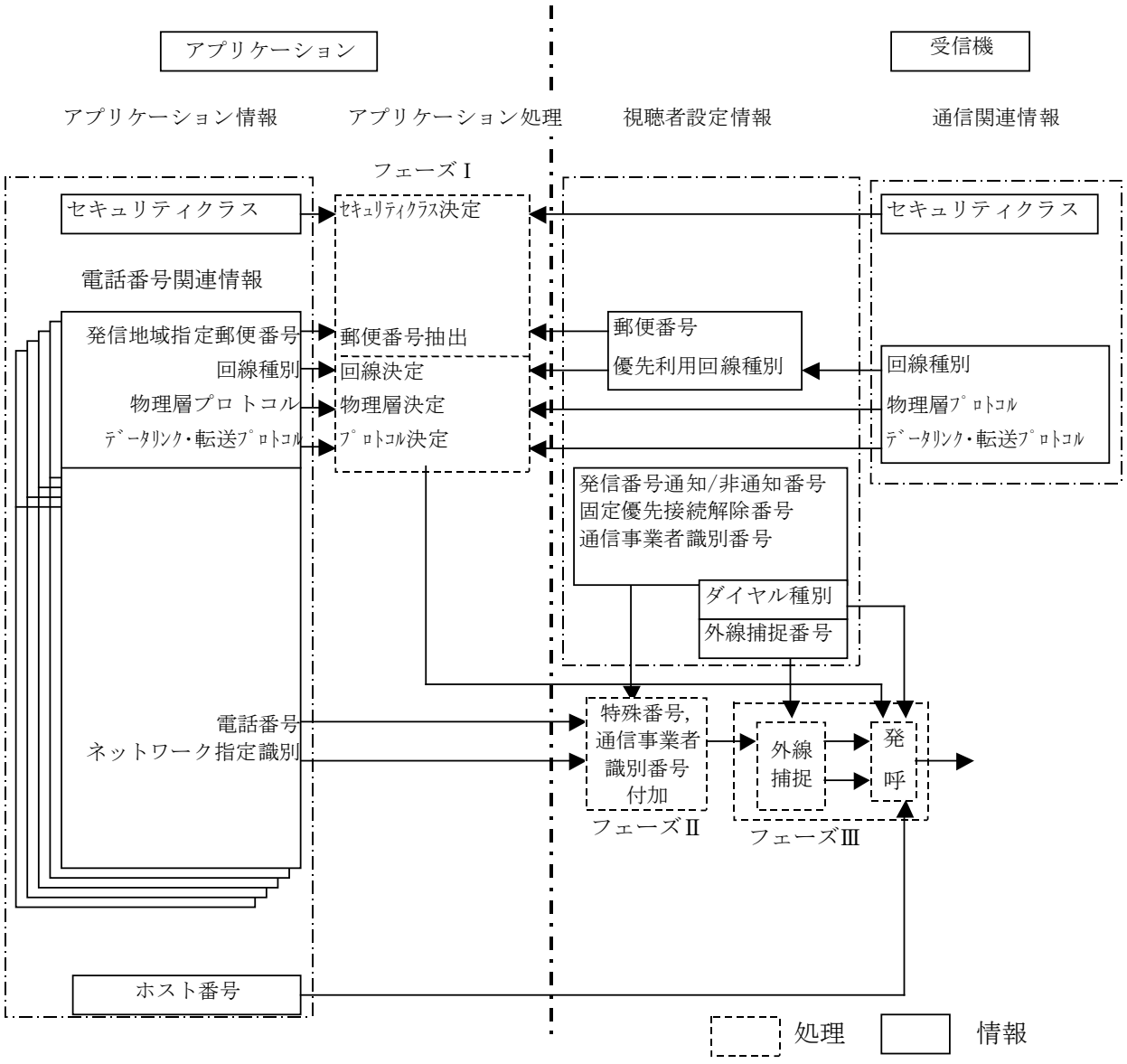


図 7-4　発呼処理の詳細

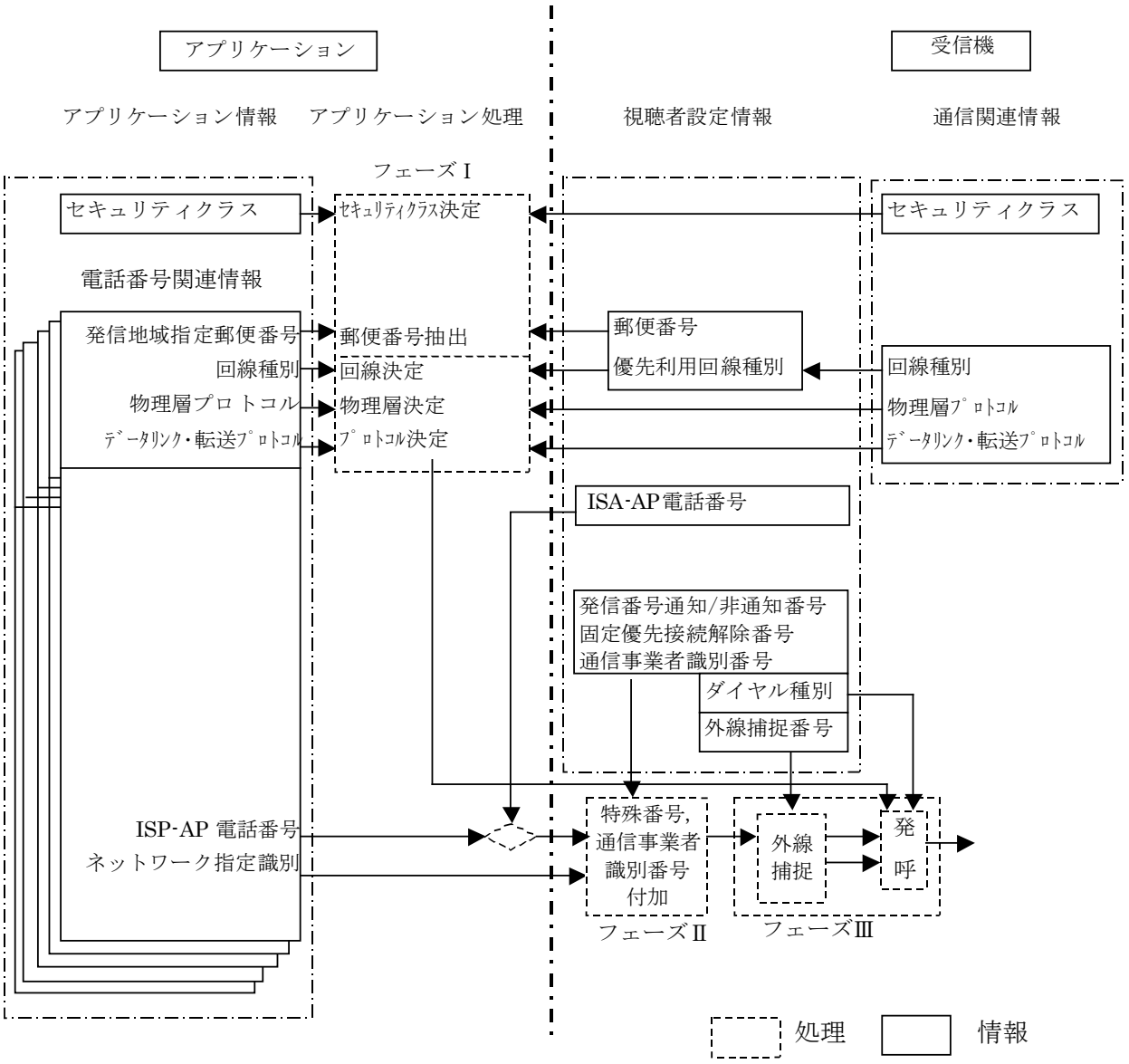

アプリケーション
受信機
アプリケーション情報
アプリケーション処理
視聴者設定情報
通信関連情報
フェーズⅠ
セキュリティクラス
ｾｷｭﾘﾃｨｸﾗｽ決定
セキュリティクラス
電話番号関連情報
発信地域指定郵便番号
回線種別
物理層プロトコル
ﾃﾞｰﾀﾘﾝｸ・転送ﾌﾟﾛﾄｺﾙ
郵便番号抽出
回線決定
物理層決定
ﾌﾟﾛﾄｺﾙ決定
郵便番号
優先利用回線種別
回線種別
物理層ﾌﾟﾛﾄｺﾙ
ﾃﾞｰﾀﾘﾝｸ・転送ﾌﾟﾛﾄｺﾙ
ISA-AP電話番号
発信番号通知/非通知番号
固定優先接続解除番号
通信事業者識別番号
ダイヤル種別
外線捕捉番号
ISP-AP 電話番号
ネットワーク指定識別
特殊番号,
通信事業者
識別番号
付加
外線
捕捉
発
呼
フェーズⅡ
フェーズⅢ
処理
情報

図 7-5 発呼処理の詳細

8　セキュリティ

8.1章にて、双方向サービスを行う上で必要になるセキュリティ機能に関する考え方を解説する。また、8.2章は、TLS1.0及びSSL3.0、またはTLS1.2を用いた公開鍵暗号システム（PKCS）による暗号化通信を行うために必要な受信機機能について規定している。

8.1　双方向サービスに必要なセキュリティ機能

双方向データ放送サービスにおいて、視聴者情報の送受信や比較的少額な決済、公平性を考慮する必要とするサービスを行う場合、セキュリティ機能を必要とする場合がある。双方向サービスをセキュリティの観点から3つのサービスクラスに分類し、それぞれのサービスクラスに必要なセキュリティ機能を表8-1に示す。

表 8-1　サービスクラスと必要なセキュリティ機能

サービスクラス	簡易サービス	標準サービス	高機能サービス
サービスの概要	決済・認証を必要としない簡易なサービス	少額な決済及び個人認証、公平性を必要とするサービス	課金されたデジタルコンテンツを配信するサービス。
対象アプリケーション例	・無記名アンケート ・資料請求	・ショッピング ・ギャンブル ・記名アンケート ・正確な意見調査	・音楽ソフト配信 ・ゲームソフト配信
セキュリティ機能			
簡易相互認証機能	－	○（レベル 1）	○（レベル 1）
情報保護機能	－	○（レベル 3）	○（レベル 3）
改竄防止機能	－	○	○
簡易署名機能	－	－	○（レベル 1）

（注 1）それぞれのセキュリティ機能の概要及びセキュリティレベルを次節以降で解説する。

8.1.1　簡易相互認証機能

表 8-2 に視聴者とセンタ側の相互簡易認証として考慮すべき項目をレベルに分類して示す。

表 8-2　相互認証レベル

セキュリティレベル		適用想定サービス	必要なモジュール
レベル 2	厳密認証 (PKCS)	インターネット系サービス	両方：公開鍵暗号、ハッシュ関数
レベル 1	保護された簡易認証	比較的低額物品購入	両方：共通鍵暗号処理、タイムスタンプ
レベル 0	保護されていない簡易認証	相手確認不要のアンケート集計等	受信機：受信機の ID

通信においてプライバシイ保護や正規視聴者であることを確認することが必要なアプリケーションを利用するときには、トランザクションの初期段階で接続した相手・接続先の確認が必要である。その手段として、相互（相手）認証機能が用いられる。相互認証機能には、公開鍵暗号を中心とした厳密認証と、何らかの制限により公開鍵が利用できない場合に代用される簡易認証との２種に大別できる。

(1) レベル 0

視聴者は、個人のプライバシイ情報やクレジットカード番号等をセンタのホストに対して送付する場合、相手が偽センタでないか確認することが望ましい。したがって、何ら保護されていない通信においては、盗聴・改竄されてもあまり差し支えない程度の情報のみに限定して送信することが望ましい。

(2) レベル 1

「通信文復元法」を利用して相互認証されることが望ましい。

センタに送る情報は、偽視聴者が、受信機のIDやパスワードを再利用することによる、成りすましをすることを防止するため、 タイムスタンプ、乱数は一方向性関数を通してから送信することが望ましい。

【通信文復元法】

図8-1に通信文復元法を利用した相手認証の方法を示す。同様に逆の方向も行うことにより、相互認証も可能である。

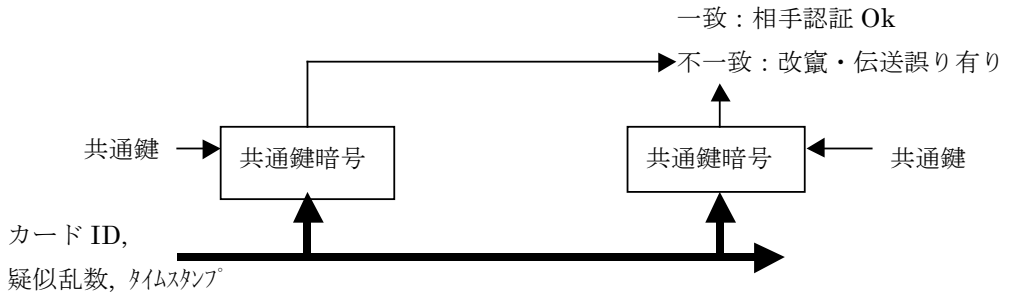


図 8-1　通信文復元法を用いた相手認証

共通鍵暗号において、送信者・受信者（検証者）が共通鍵を事前に共有している場合、その共通鍵を利用して送信側で通信文を暗号化し、その暗号文を受信者で復号したときに意味のある通信文になれば送信者を確信することができる。

(3) レベル 2

インターネットで広く使われている公開鍵暗号システム(PKCS) として知られている一連の暗号処理システムを利用する。

- 必要モジュール（レベル 1 に加えて）：公開鍵暗号処理機能、一方向性関数、証明書機能
- 必要な機関：証明書管理機関 CA（発行・参照・変更・更新・廃棄）

8.1.2　情報の保護

表8-3に情報の保護として考慮すべき項目をレベルに分類して示す。

表 8-3　情報の保護レベル

セキュリティレベル		取り扱う視聴者情報	必要なモジュール／システム
レベル 3	他ネットワークの接続	インターネット系サービスとの融合	センタ：ファイヤーウォール
レベル 2	情報アクセス権管理	顧客管理情報	センタ：アクセス管理機能
レベル 1	情報の暗号化管理	個人名と住所等	両者　：共通暗号処理機能
レベル 0	考慮なし	本人了承範囲	－

双方向データ伝送サービスでは、ショッピングのように届け先を指定するために、サービス提供者が視聴者の氏名や住所を把握する必要がある場合がある。このような双方向サービスにおいては、プライバシイ保護の観点から視聴者情報の漏洩等を防ぐために以下のことを考慮することが望ましい。

- ネットワーク上での盗聴防止
- センタ内での漏洩防止
- 外部からセンタへの進入防止。
- 必要な個人データのみを取り扱い、本人に許可なく他の用途に用いたり、譲渡したりしないこと。

(1)　レベル 0

- センタが行うことが望ましい機能及び動作

プライバシイ保護の対象となる視聴者情報を必要とするサービスは、本人の了承を得ることが望ましい。

(2)　レベル 1

- 受信機で行うことが望ましい機能及び動作

偽センタへの接続を排除するために事前に接続相手を確認すること(8.1.1(2)参照)

プライバシイ保護の対象となる視聴者情報は暗号化した後送付すること。

- センタが行うことが望ましい機能及び動作

プライバシイ保護の対象となる視聴者情報は、必要な者のみが扱うこと。

(3)　レベル 2

- センタが行うことが望ましい機能及び動作

プライバシイ保護の対象となる視聴者情報に対しては、アクセス権制御（視聴者情報等に読み出し・登録が可能者を限定するための制御）管理を行うこと。

(4)　レベル 3

- センタが行うことが望ましい機能及び動作

サービス内容の拡充にあたって、やむを得ずインターネット等の他ネットワークと接続する場合は、ファイヤーウォールを設置することにより、視聴者情報の漏洩防止に努めること。

8.1.3　改竄防止機能

通信路において、改竄があった場合には、改竄が行われたことを検出する機能を有することが望ましい。

8.1.4　署名機能

表8-4署名機能として考慮すべき項目をレベルに分類して示す。

表 8-4　署名機能レベル

セキュリティレベル		主な適用例／特徴	必要なモジュール／システム
レベル 3	デジタル署名機能	法的証拠能力が必要な情報交換	公開鍵暗号、証明書発行機関
レベル 2	共通鍵暗号の代用	共通鍵暗号	共通鍵暗号、第三者署名機関
レベル 1	簡易署名機能	一方向性関数、通信文適用法	共通鍵暗号
レベル 0	考慮なし	確認番号のメモ	不要

(1)　レベル 0

チケット予約のような場合、予約時には、受付確認書等を受信しても、受信機によっては記憶方式、出力方式が限られることが予想されるため、センタは最低限予約確認番号を発行し、手続き上のトラブルに対処できるようにすることが望ましい。ただし、予約確認番号は、センタの全面的信頼が前提となる。

(2)　レベル 1

オンラインにてショッピングをするような金銭と商品（デジタルコンテンツを含む）の取り引きがある場合、トラブルを防ぐために取り引き両者の証拠を残す必要がある。このような場合、デジタル署名を用いるのが理想であるが、デジタル署名は公開鍵暗号機能を実装しなければ実現できないので、共通鍵暗号のみを実装したシステムにも用いることができるメッセージ認証子(MAC)を利用することが望ましい。

ただし、第三者の生成した署名結果でないことは確信できるが、同じメッセージを署名受け取り者も作成できるので、センタ側の署名生成者の言い逃れに対しての効力はない。

(3)　レベル 2

センタ側の不正に対応するためには、信頼できる第三者機関のメッセージ認証子とメッセージを連結してセンタのメッセージ認証子を付加することにより実現可能である。ただし、受信機と第三者機関は共有した共通鍵を保持しつづけなければならない。

(4)　レベル 3

法的な証拠能力が必要とされるため、公開鍵暗号を利用した証明書発行機関を利用することが望ましい。

8.2　TLS、SSLの運用A規定

受信機はTLS1.0及びSSL3.0、またはTLS1.2を実装し、公開鍵暗号システム（PKCS）によって暗号化通信を行う仕組みを有すること。ルート証明書の運用方法、及び、伝送については第三編を参照すること。

※2015年10月以降に新規発売される受信機においては、TLS1.0及びSSL3.0の搭載を必須としない。

※2015年10月以降に新規発売される受信機においては、TLS1.2の搭載を必須とする。

8.2.1　ルート証明書格納モジュール運用の前提

8.2.1.1　　ルート証明書格納モジュールの管理

- 放送事業者が送出する汎用ルート証明書格納モジュール、及び、モジュール内に含まれる汎用ルート証明書自身、汎用ルート証明書識別 ID と汎用ルート証明書バージョン、汎用ルート証明書格納番号については、放送事業者等によって構成される組織（以下、証明書管理組織）によって管理されていることを前提とする。各放送事業者は、汎用ルート証明書を運用する場合は証明書管理組織の規定に従うこととする。
- 証明書管理組織は、各放送事業者が運用を希望する汎用ルート証明書を調整し、汎用ルート証明書毎にその識別 ID(root_certificate_id)とバージョン番号(root_certificate_version)を採番し、汎用ルート証明書格納番号の割当を行い、汎用ルート証明書リスト情報として管理することとする。
- 証明書管理組織は、要請があった場合に、汎用ルート証明書リスト情報を各放送事業者や受信機メーカに提供する。
- 証明書管理組織は、各放送事業者が送出すべきルート証明書格納モジュールを作成し、各放送事業者へ配布する。
- 事業者専用ルート証明書用のルート証明書モジュールについては、放送事業者によって管理されることとする。

8.2.1.2　　汎用ルート証明書の識別IDとバージョンの採番と格納番号の割当

- 汎用ルート証明書の識別 ID とバージョンは、証明書を一意に識別できるように証明書管理組織によって採番される。事業者専用ルート証明書の場合は、ルート証明書識別 ID を 0xFFFFFFFF, ルート証明書バージョンを 0xFFFFFFFF とする。
- ルート証明書 ID とバージョンが同一の汎用ルート証明書に対しては 1 つのルート証明書格納番号を割り当てる。また、同時期においては、異なる汎用ルート証明書に対して同一の汎用ルート証明書格納番号を割り当てない。
- 証明書の更新時も含め、同時期に運用する汎用ルート証明書の数は 8 以下とする。

8.2.2　汎用ルート証明書の更新

・　有効期限切れ等の理由により、汎用ルート証明書の切り替えが必要になった場合、有効期限が切れる前に移行期間を設け、汎用ルート証明書格納モジュールに新旧２つの証明書を格納して送出し、その間に順次双方向サーバ側のサーバ証明書を更新していく。汎用ルート証明書格納モジュールに格納できる汎用ルート証明書は２種類以下とする。証明書の伝送に関する詳細は第三編 2.3.1.8「ルート証明書の伝送」、を参照すること。

8.2.3　ルート証明書格納モジュールのフォーマット

ルート証明書格納モジュールに格納されるルート証明書のデータ構造には、ARIB STD-B24 第二編9.1.2「リソースのモジュールへのマッピング」の規定を用いる。ルート証明書格納番号、ルート証明書識別ID、ルート証明書バージョンをリソース名に対してマッピングすること。

リソース名の運用は以下の通りとし、拡張子は用いないで表記する。

[ルート証明書格納番号]+ ’.’+[ルート証明書識別 ID]+ ’.’+[ルート証明書バージョン]

ここで、[ルート証明書格納番号]、[ルート証明書識別ID]、[ルート証明書バージョン]は10進表記で表し、’.’で繋げる。使用する文字コードはASCIIとし、’0’～’9’, ’_’, ’A’, ‘B’, ‘.’のみ使用する。また、事業者専用ルート証明書のルート証明書格納番号は、’_A’或いは、’_B’とする。汎用ルート証明書の各番号の採り得る範囲は表8-5の通りとする。従って、リソース名の長さは可変であり、最大、2バイト+’.’+10バイト+’.’+10バイト=24バイトとなる。

例えば、ルート証明書格納番号が0x03、ルート証明書識別IDが0x0000003F 、ルート証明書バージョンが0x0000007D の場合のリソース名は以下の通り。

Ex. 3.63.125

また、事業者専用ルート証明書の場合はルート証明書識別IDが0xFFFFFFFF、ルート証明書バージョンが0xFFFFFFFF（8.2.1.2）であるので、以下のようになる。

Ex. _A.-1.-1、或いは、_B.-1.-1

num_of_resourcesの値は最大で2とする。証明書の実データはentity-bodyに格納する。

表 8-5 汎用ルート証明書格納番号と識別 ID、バージョンの範囲

	割当バイト	範囲	
		16 進表記	10 進表記
ルート証明書格納番号	2	0x0000～0x0007	0～7
ルート証明書識別 ID	4	0x00000001～ 0x7FFFFFFF	1～2147483647
ルート証明書バージョン	4	0x00000001～ 0x7FFFFFFF	1～2147483647
	合計 10		

8.2.4　受信機が実装するセキュリティ関連機能の情報

(1)暗号スイート　STD-B21 11.5.7.3

受信機は以下のCipher Suiteを搭載すること。ただし下記以外のCipher Suiteについての搭載については商品企画とする。

表 8-6 受信機でサポートする Cipher Suite 一覧

Cipher Suite	鍵交換	データ暗号	ハッシュ	備考
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA	RSA_EXPORT	DES40	SHA	※1
TLS_RSA_WITH_DES_CBC_SHA	RSA	DES	SHA	※1
TLS_RSA_WITH_3DES_EDE_CBC_SHA	RSA	Triple-DES	SHA	
SSL_RSA_EXPORT_WITH_DES40_CBC_SHA	RSA_EXPORT	DES40	SHA	※1
SSL_RSA_WITH_DES_CBC_SHA	RSA	DES	SHA	※1
SSL_RSA_WITH_3DES_EDE_CBC_SHA	RSA	Triple-DES	SHA	※1
TLS_RSA_WITH_AES_128_CBC_SHA	RSA	AES_128	SHA	※2
TLS_RSA_WITH_AES_256_CBC_SHA	RSA	AES_256	SHA	※2
TLS_RSA_WITH_AES_128_CBC_SHA256	RSA	AES_128	SHA256	※2
TLS_RSA_WITH_AES_256_CBC_SHA256	RSA	AES_256	SHA256	※2
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	DHE_RSA	Triple-DES	SHA	※2
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DHE_RSA	AES_128	SHA	※2
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DHE_RSA	AES_256	SHA	※2
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	DHE_RSA	AES_128	SHA256	※2
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	DHE_RSA	AES_256	SHA256	※2
TLS_RSA_WITH_AES_128_GCM_SHA256	RSA	AES_128	SHA256	※2
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	DHE_RSA	AES_128	SHA256	※2
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	ECDHE_ECDSA	Triple-DES	SHA	※3
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	ECDHE_ECDSA	AES_128	SHA	※3
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	ECDHE_ECDSA	AES_256	SHA	※3
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	ECDHE_RSA	Triple-DES	SHA	※3
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDHE_RSA	AES_128	SHA	※3
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDHE_RSA	AES_256	SHA	※3
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE_ECDSA	AES_128	SHA256	※3
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE_ECDSA	AES_256	SHA384	※3
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE_RSA	AES_128	SHA256	※3
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE_RSA	AES_256	SHA384	※3
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE_ECDSA	AES_128	SHA256	※3
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	ECDHE_ECDSA	AES_256	SHA384	※3
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE_RSA	AES_128	SHA256	※3
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE_RSA	AES_256	SHA384	※3

※1：TLS1.2 のみに対応する受信機では搭載を必須としない Cipher Suite

※2：TLS1.2 に対応する受信機においては搭載を必須とする Cipher Suite

※3：ECC 暗号（オプション）に対応する受信機においては搭載を必須とする Cipher Suite

(2)RSA公開鍵の鍵長

RSA公開鍵の鍵長は、2048ビットに対応することが望ましい（付録1.2参照のこと）。

(3)ECC 公開鍵の鍵長（オプション）

ECC(ECDSA)公開鍵の鍵長は、256ビットに対応すること（付録1.2参照のこと）。

8.2.5　ルート証明書およびサーバ証明書の内容・制限

(1)ルート証明書の内容

表 8-7 受信機が搭載する汎用ルート証明書

種類	数	サイズ
X.509 (ASN.1/DER 形式)	8 個	1 証明書　3KB 以下

- 8.2.4 でサポートしている暗号スイートを使用する証明書であること。
- ルート証明書の署名のハッシュ関数としては SHA-１、SHA-2 のいずれかであること。
- 日本語表記証明書が使用される。日本語の文字列は UTF8String とする。
- 拡張部の無いバージョン３証明書は運用しないこととする。
- 第三編［5.14.14.4　事業者専用ルート証明書受信時の受信機動作のガイドライン］で定義されている事業者専用ルート証明書についても上記の規定と同じものとすること。

(2)サーバ証明書、中間証明書の制限

- サーバ証明書および中間証明書は、署名のハッシュ関数として SHA-１、SHA-2 のものに限定する。

8.2.6　ルート証明書表示B規定

受信機において汎用ルート証明書が表示できる機能を有すること。表示方法については商品企画。

8.2.7　認証機能

サービスにおいて「成りすまし」を防止するため、受信機はサーバ認証をサポートする。また、クライアント認証機能は商品企画とするが、デジタル地上波サービス動作時には機能しないこととする。

8.2.8　証明書の検証項目

(1) 検証可能な証明書の枚数

WEBサーバの証明書は５階層以下とする。受信機は最低5枚の証明書を検証できること。

(2) 検証項目

・RFC3280 に準拠することとし、基本証明書フィールド及び、拡張部における KeyUsage と ExtendedKeyUsage、BasicConstraints、並びに、CommonName を検証すること。ただし、ルート証明書については署名の検証を行わなくてもよい。

・証明書の取り消し情報の検証は B 規定とする。

8.2.9　サーバ証明書取り消しリスト（CRL）の運用B規定

サーバ証明書取り消しリスト（CRL）の実装は商品企画とする。

8.2.10 証明書の参照

第三編［5.14.14.2　汎用ルート証明書の受信機への格納、5.14.14.4　事業者専用ルート証明書受信時の受信機動作ガイドライン］を参照のこと。

8.2.11 TLS及びSSLエラー時のアラート

受信機は、TLS、及び、SSLエラー発生時において、アラートメッセージを表示すること。表示方法については商品企画とするが、表8-8のようなメッセージが望ましい。また、受信機は、TLS及びSSLエラーが発生した場合は、双方向サーバに接続しないこと。

表 8-8 TLS、及び、SSL エラー時のアラートメッセージ例

	原因	メッセージ例
1	ルート証明書自体が受信機側にない場合	「受信機側にルート証明書が設定されていません。接続先の安全性が確認できない為、接続できません。」
2	ルート証明書は受信機側にあるが、接続先のサーバ証明書との検証が取れない場合	「現在設定されているルート証明書では接続先の安全性が確認できない為、接続できません。」
3	ルート証明書の有効期限切れの場合	「現在設定されているルート証明書の期限が切れています。接続先の安全性が確認できない為、接続できません。」
4	回線障害等の認証処理エラーの場合（タイムアウト処理）	「設定時間内に接続できませんでした。」
5	接続先の証明書が有効期限切れの場合	「接続先の証明書の有効期限が切れています。接続先の安全性が確認できない為、接続できません。」
6	サーバ証明書の CommonName 不一致の場合	「接続先の証明書には表示しようとしているページの名前が含まれていません。接続先の安全性が確認できない為、接続できません。」
7	受信機側で証明書を無効設定している場合	「接続先を認証する受信機のルート証明書が無効に設定されています。ルート証明書を有効にして接続しなおしてください。」
8	証明書改竄	「接続先の証明書の不正が検出された為、接続を中断します。」
9	チェーン不正などの認証エラー	「接続先の証明書設定に問題が発生している為、接続を中断します。」

9　輻輳回避

9.1　輻輳対策

双方向データ放送サービスでは、従来の電話からの通信とは異なり、番組に連動した世論調査・チケット購入等で特定のセンタへ短時間に通信が集中し、ネットワークの輻輳が発生しやすい。ネットワークが輻輳すると視聴者からの通信が完了しないなど番組の運営に支障をきたすこととなる。さらには一般電話等の他の通信にまで影響を与えるため、これを防ぐ必要がある。

9.2　放送局の輻輳対策

双方向データ放送サービスの番組制作にあたっては、視聴者からの通信が過度に集中しないように考慮する必要がある。

具体的には、双方向データ放送サービスの視聴率、参加率、通信時間、通信の受付時間等を考慮して通信数を予測し、輻輳回避の制御が必要と判断される場合は、下記の方法（組み合わせも可能）で輻輳回避を行うことが望ましい。

9.2.1　発信遅延

－　放送波を通じて送られるアプリケーション･プログラムで以下に示すような手続き関数を用いることにより、発呼時刻を個々の受信機ごとに分散させることを考慮する。

1. 乱数の発生(random( ))
2. タイマ指定(setInterval( ))
3. 登録発呼（connect( ), sendTextData( )など、BASIC 系、connectPPP( ),connectPPPWithISPParams( ),transmitTextDataOverIP( )など、TCP/IP 系送信系関数と、それをトリガとする受信機による自動発呼）

通信が集中した場合でも、受信機ごとに、ある時間だけ発信を遅延させることにより、トラヒックが分散される。発信遅延実施時のトラヒックイメージを図9-1に示す。

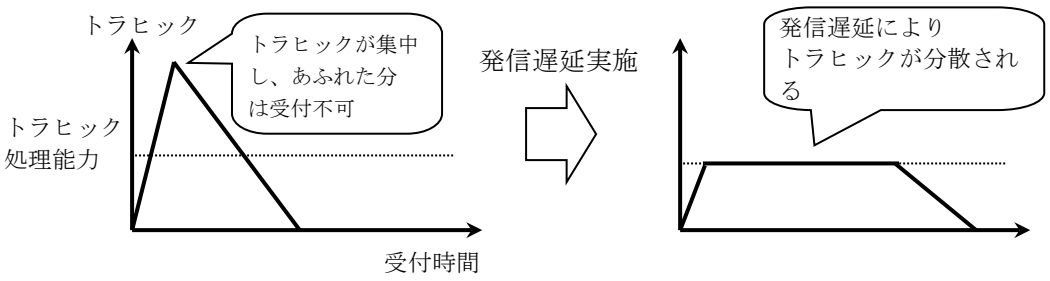


図 9-1　発信遅延実施時のトラヒックイメージ

また、主番組終了後も継続するローカルコンテンツを設定することにより、他のサービスを選局されない限り、番組終了後に発呼処理を行うことができる。

9.2.2　発信制限

－　放送波を通じて、受信機の ID の末尾制限等により、どの受信機に通信を許可するかの指示（アプリケーションプログラムレベル）を行うことを考慮する。

従来の電話による末尾制限は、視聴者の良識に負うことが前提となり、指定した電話番号以外からでも通信が可能であるが、双方向データ放送サービスでは受信機が発信制限するので、通信を制限することができる。但し、発信制限により発信できない視聴者が発生する。

発信制限実施時のトラヒックイメージを図9-2に示す。

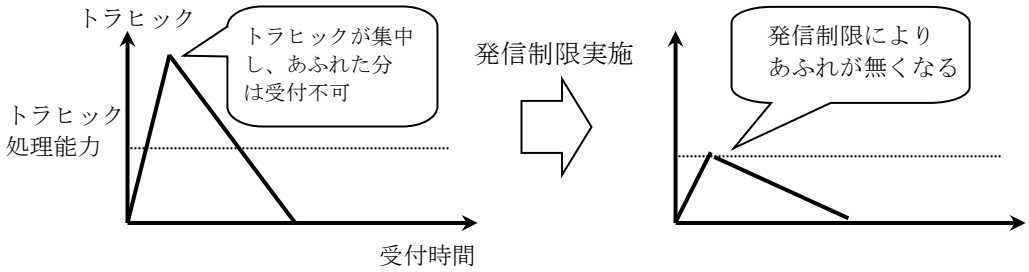


図 9-2　発信制限実施時のトラヒックイメージ

9.2.3　発信遅延・発信制限の通知　B規定

発信遅延及び発信制限の実施に当たっては、視聴者の誤解を避けるため、発信の遅延及び制限が実施されていることを放送局から通知することが望ましい。

9.2.4　ネットワークサービスの利用

短時間に通信が集中すると想定される場合には、大量呼受付サービスの利用を考慮する。

大量呼受付サービスでは、ほとんど話し中になることなく多数の呼を受け付けることができるので、電話がつながらないことによる視聴者からの苦情等を減らすことが可能となる。

9.2.5　通信事業者への事前情報提供

放送局は多数の通信が発生すると想定される場合は、事前に通信事業者に情報提供することが望ましい。

上記のような対策を講じたにもかかわらず輻輳が発生した場合は、次回番組に反映させ、通信事業者と協力して再発防止を図ることを考慮する。

9.3　通信事業者の輻輳対策

アクセスポイントの分散及び回線数については、以下のことを勘案することが望ましい。

9.3.1　アクセスポイントの分散

特定の交換機に通信が集中することによる輻輳を回避するため、受信機の地域別普及状況等を勘案したアクセスポイントの設置を考慮する。

9.3.2　アクセスポイントの回線数

アクセスポイントには、輻輳を避けるため受信機からの通信数に見合う回線数を考慮する。また受信機の普及台数の変化に伴い、適正な回線数に見直しを行う必要がある。

9.4　受信機機能　A規定

- 発信遅延を行うために必要な、乱数を発生させる機能を持つこと。
- 再発信は 3 分間に 2 回以内とする。

9.5　センタサーバの輻輳回避

センタサーバの応答遅延は、加わる要求に対するサーバのパフォーマンス不足や、ルート上の装置等のパフォーマンス不足が主な原因である。

回避するために以下の対策を行うことが望ましい。

(1) サーバの処理能力向上
(2) サーバの負荷分散
(3) キャッシュサーバの導入
(4) TLS 或いは SSL を使用している場合は TLS 或いは SSL アクセラレータの導入
(5) BML コンテンツデリバリサーバの導入（ミラーサーバへの分配）
(6) BML コンテンツのデザインを改善（長時間保留の回避）

10 異常処理

10.1 受信機の電源断時の対応　A規定

受信機は、通信中に電源断状態になった場合には、速やかに電話回線の直流回路を開放する。

11 緊急時対策

11.1 緊急時のための機能　B規定

双方向データ放送サービス実施中・予定中に、大規模災害等非常事態が発生した場合、防災等の重要通信の確保や、視聴者が緊急通信に移行するための機能を示す。

災害等緊急時の機能について表11-1に示す。

表 11-1　災害等緊急時の機能

	機　　能
放送局	・　放送波を通じて双方向データ放送サービスの中断または中止の制御が可能であることが望ましい。 ・　放送波を通じて新たな通信を行わないための制御が可能であることが望ましい。
受信機	・　放送波の制御により、新たな通信を行わないよう制御が可能なことが望ましい。

12 関連法令及び権利化状況

12.1 関係法令

双方向データ放送サービスを行う上で考慮する必要がある関係法令を以下に示す。

12.1.1 緊急時の対応に関して考慮すべき法令

(1) 電気通信事業法

・第 8 条　重要通信の確保

12.1.2 通信網の輻輳に関して考慮すべき法令

(1) 端末設備等規則

・第 11 条、第 18 条　発信の機能

付録　1　　セキュリティに関する補足説明

本章は、セキュリティ機能に関しての一般的な情報を解説する。

1.1　セキュリティ機能

1.1.1　データ暗号化

デジタルデータの暗号化には、セキュリティの強度に応じて公開鍵暗号、さらに共通鍵暗号を併用することが適切である。また、簡易なスクランブルを必要とするアプリケーションに対しては用途に注意する必要があるが、簡易暗号機能を利用することもできる。以下にそれぞれの方式の概要と特徴を解説する。

(1)　共通鍵暗号

秘密鍵暗号・対称暗号とも言う。送信者・受信者が秘密で共通して所有する共通鍵を利用して、送信側で暗号化し、受信者側で復号する。通信の両者が事前に共通鍵を何らかの手段で共有していることが必要である。

盗聴・解読された場合に視聴者側のプライバシイおよび金銭的な被害が生ずる可能性のあるデータ等には、本格的な暗号処理が必要である。一般的にはクレジットカード番号や視聴者情報を通知する必要があるアプリケーションにおいて、盗聴に対する保証がなされていない公衆網や電波・無線を用いる場合、費用対効果の観点から少なくとも 56/64 ビット共通鍵暗号が利用されている。JIS X5060 (ISO/IEC9979)に共通暗号のアルゴリズムが登録されている。これらのアルゴリズムは、暗号アルゴリズムの安全性を保証するものではないので、選択に当たっては注意を要する。

(2)　公開鍵暗号

非対称暗号とも言う。暗号用の鍵（公開鍵）と復号用の鍵（秘密鍵）が異なる。公開鍵を公開し、秘密鍵を秘密裏に管理することにより暗号通信が可能。共通鍵と比べると演算量は著しく多い。したがって、主に共通鍵暗号の共通鍵を共有するために利用される。

一部の公開鍵暗号（RSA 暗号等）は、署名機能も持つ。署名機能として利用する場合には、署名するデータに秘密鍵の演算を行い、検証者は公開鍵を用いて署名結果を検証する。

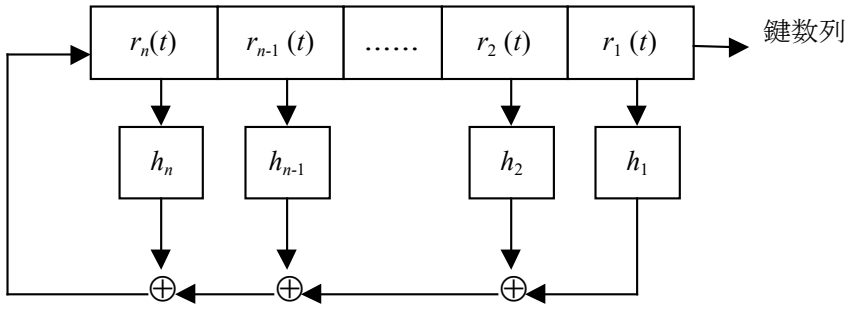
(3)　簡易暗号

簡易暗号の例としてバーナム暗号とその乱数鍵発生器に M 系列を利用する線形フィードバックシフトレジスタ方式の同期式逐次暗号がある。ただしこの方式は、線形性を有するために既知平文攻撃により解読できるので、適用に当たっては注意が必要である。

バーナム暗号は、付図 1-1 のように表現できる基本的な暗号である。

付図 1-1　バーナム型共通鍵暗号

バーナム暗号の乱数発生器として、線形フィードバックシフトレジスタの出力を利用する。



$r_i(t)$: 各桁レジスタの値　　h_i:レジスタ値を変化させる関数

付図 1-2　線形フィードバックレジスタを用いた簡易暗号器

1.1.2　その他のセキュリティに用いるモジュール

(1)　メッセージダイジェスト（ハッシュ関数）

大きな（場合によっては非常に大きな）領域を小さな範囲に写像する数学的関数。質のよいハッシュ関数には一方向性と衝突フリーであることを同時に満たすことが必要。

(2)　メッセージ認証符号

メッセージ認証子は共通鍵暗号で実現できる。共通鍵暗号の CBC モード（暗号利用モード）で演算した結果の InitialVector（初期値）の値とするのが一般的である。伝文が短い場合は、パディングをすることで対応可能である。

(3)　疑似乱数

疑似乱数と厳密な乱数を必要とする場合があるが、本章で扱う乱数は疑似乱数でも十分であると思われる。

共通鍵暗号において、完全に同一データを送付する場合、暗号化したとしても鍵と初期値が同じ場合まったく同じ結果になる。この性質を悪用して、通信路の途中で搾取した暗号化データを再利用することにより混乱させることができる。これを防ぐために、通信ごとに異なる疑似乱数などを含ませて送信し、受信側では単純な演算を施し（1 を加算する等）

返送することで上記不正に対処できる（チャレンジコード)。タイマやカウンタなどのシードに共通鍵暗号の演算をした結果を疑似乱数とすることができる。

(4) タイムスタンプ

第三者が正確な署名データ等を再利用することを防ぐために、同一署名内容であっても再現性のない署名が生成されないようにするために利用される。

(5) 簡易本人確認機能

あるデータやモジュールを利用する権利を所有しているかどうかを確認するためには、本人の確認をする必要がある。もっとも簡易な本人確認技術として PIN 認証が利用されている。

【PIN 認証】

カード所有者を確認する場合に用いる。本人が記憶できる程度の桁数があり、かつリモコンから入力できる必要があるため、数字で 4～8 桁程度が適当である。

(6) 証明書

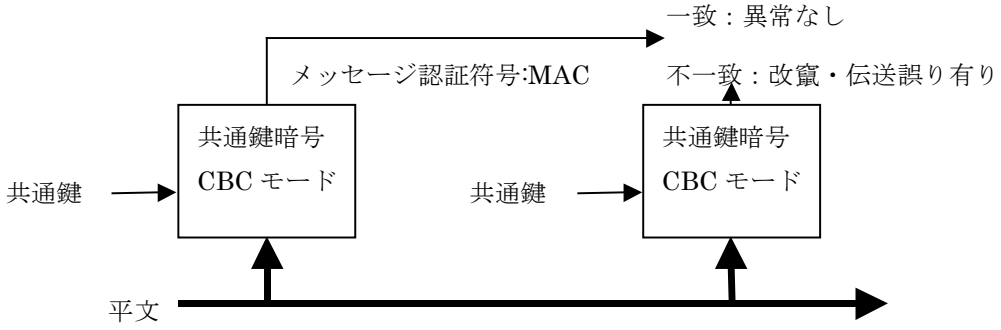
公開鍵暗号を利用して相手を認証するためには、不可欠である。証明書を発行する機関は、改竄等無く正確に証明書発行する必要があるので、署名者・検証者の両者信頼を受けている中立的な機関であることが必要である。

1.1.3 データの完全性

基本機能：共通鍵暗号機能を用いること。

メッセージ認証符号(Message Authentication Code: MAC)を代用することができる。詳細は、(JIS X 5055 [ISO/IEC9797]) を参照。

暗号通信が目的ではなく、改竄・伝送エラー等なく確実に相手に通信文を伝えるために利用される。通信文そのものの伝送と全通信文のCBCモードでの暗号を行う。通信文の暗号化終了後のIVレジスタの値をMACとして伝送する。受信者も同様な演算を行う。もし、回線上で改竄や伝送エラーがあれば、MACの値は異なるので、異常を検出できる。付図1-3にメッセージ認証符号の利用法を示す。



付図 1-3 メッセージ認証符号を利用したデータ完全性

さらに、簡便な方法としてCRCを用いることもできる。ただし、この場合データの改竄の検

出不可能。

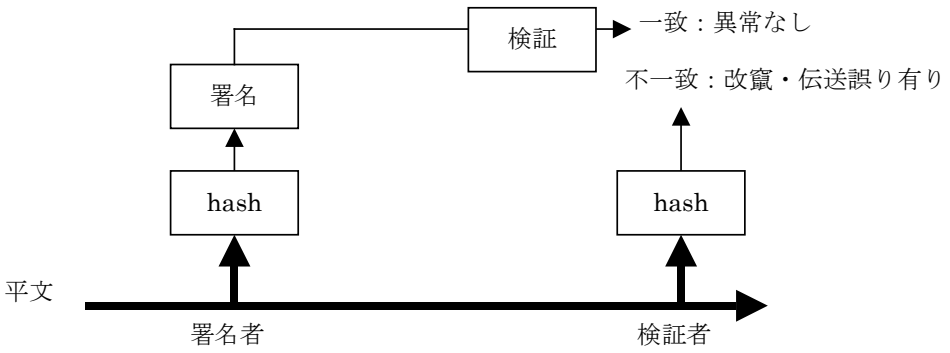
参考文献：

1　JIS X 5055 セキュリティ技術－ブロック暗号アルゴリズムによる暗号検査関数を用いるデータ完全性機能

2　ISO/IEC9797 Information technology – Security techniques – Data integrity mechanism using a cryptographic check function employing a block cipher algorithm

高機能：公開鍵暗号およびメッセージダイジェストを用いる。

送付するデータに対してメッセージダイジェスト施した後、署名を施す。メッセージダイジェストとは、ハッシュ関数(JIS X 5057 [ISO/IEC 10118])とも呼ばれ、任意の長のデータを一定長の要約（ダイジェスト）を生成するために利用される。署名は、データ長には上限がある。長いデータに対して効率的に署名をする場合、前処理としてデータに対してダイジェストを作成し、そのダイジェストに対して署名(JIS X 5056-3 [ISO/IEC 9798-3])を行う。付図1-4に公開鍵暗号およびハッシュ関数の利用法を示す。



付図 1-4　公開鍵暗号およびハッシュ関数を利用したデータ完全性

参考文献：

1　JIS X 5057-1, “セキュリティ技術　―ハッシュ関数―第 1 部 総論

2　ISO/IEC 10118-1 Information technology - Security techniques - Hash-functions –

3　JIS X 5057-2, “セキュリティ技術　―ハッシュ関数―第 2 部 n ビットブロック暗号アルゴリズムを用いるハッシュ関数”

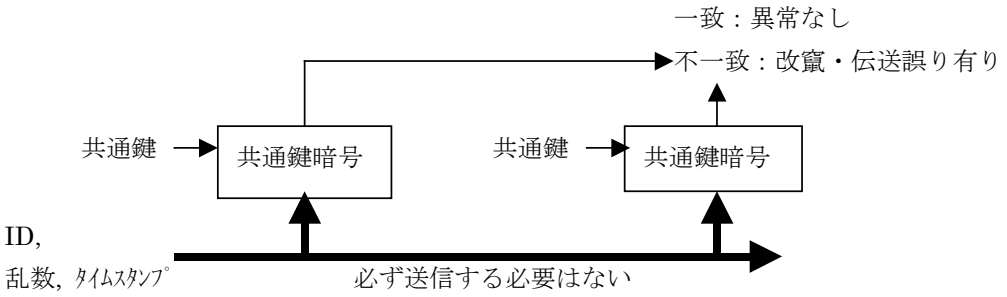
4　ISO/IEC 10118-2 Information technology - Security techniques - Hash-functions using n-bit block cipher algorithm-

5　JIS X 5056-3　セキュリティ技術　―エンティティ認証機構―　第 3 部　公開鍵アルゴリズムを用いる認証機構

6.　ISO/IEC 9798-3 Information technology - Security techniques – Entity authentication mechanisms Part.3: Entity authentication using a public key algorithm

1.1.4　相手認証

基本機能：共通鍵暗号機能を用いる（通信文復元法）付図1-5に共通鍵暗号を用いた簡易相手認証方法を示す。



付図 1-5　共通鍵暗号を利用した簡易相手認証

共通鍵暗号において、送信者・検証者が事前に共有している場合、共通鍵を利用して送信側で通信文を暗号化し、その暗号文を受信者で復号したときに意味のある通信文になれば送信者を確信することができる。

相互認証する場合、検証者は発信者が生成した乱数に1を加える等の両者事前合意の簡単な演算を施し、それを再び暗号化し送り返すことにより確認できる。（簡便な方法として、セキュリティの要求条件に応じて、ネットワークサービスの発ID通知機能等を利用することにより相手識別をすることも可能。）

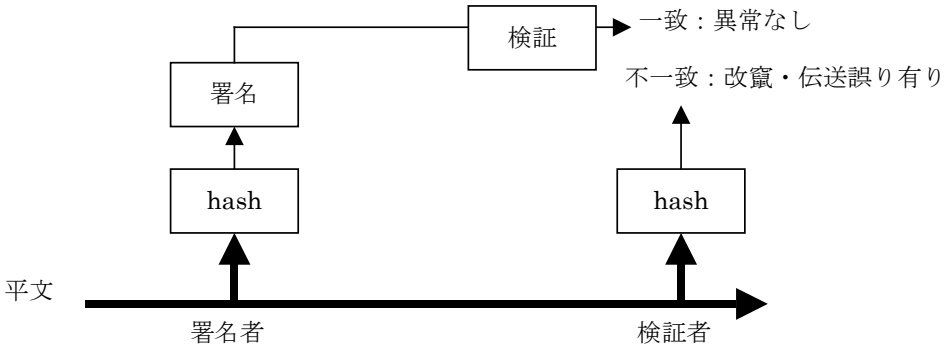
参考文献：

1 JIS X 5056-3　セキュリティ技術　―エンティティ認証機構―　第 2 部　対称暗号化アルゴリズムいる認証機構

2 ISO/IEC 9798-3 Information technology - Security techniques – Entity authentication mechanisms Part.2: Entity authentication using symmetric encipherment algorithms

高機能：公開鍵暗号機能を用いる。

公開鍵暗号における証明書発行機関が発行する証明書(X.509)の提示をもとめ、それを公開鍵暗号で検証することにより通信相手を認証する。付図1-6に公開鍵暗号を用いた相手認証の方法を示す。



付図 1-6　公開鍵暗号を利用した相手認証

（簡便な方法として、ハッシュ関数を一方向性関数として利用したX.509に記載されている簡易認証も適用可能）

参考文献：

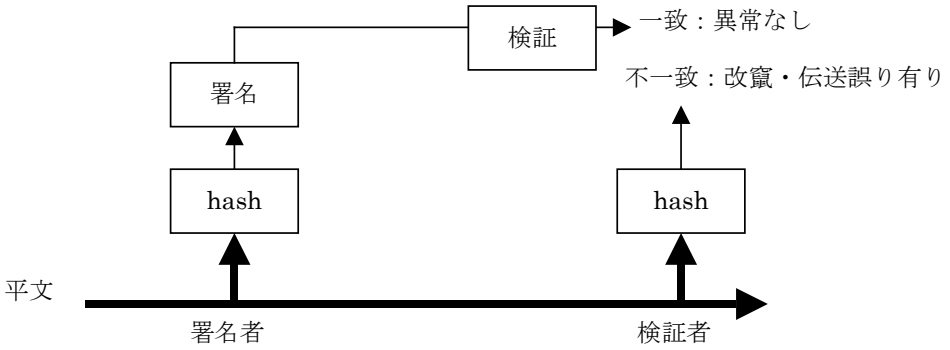
1　X.509 ディレクトリ　－認証の枠組み

1.1.5　署名

・基本機能：共通鍵暗号機能を用いる

署名するデータにて述べたメッセージ認証符号を付与することにより代用する。

高機能：メッセージダイジェスト機能および公開鍵暗号機能を用いる。付図 1-7 にメッセージ認証符号の利用法を示す。



付図 1-7　公開鍵暗号を利用した署名

送付するデータに対してメッセージダイジェストを施したのち、公開鍵暗号系の署名を施す。

1.1.6　鍵管理

鍵管理には、鍵保管法・鍵生成法・鍵更新・鍵廃棄等がある。どこか1つの項目に欠陥があってもセキュリティレベルは下がるので、どの項目も軽視できない。

鍵保管法：

公開鍵暗号の秘密鍵や共通鍵暗号の共通鍵を記憶する場所の安全性に関する。この安全性は、主に以下の項目から決まる。以下の表に参考として、セキュリティの要求条件を整理した。この例では、センタは、センタ設置場所および人的管理が厳密に行われている場合を想定している。受信機は、一般家庭を想定し、受信機に対してある程度の攻撃があると想定しているが、組織的な攻撃は考慮していない場合である。実際の運用に当たっては、セキュリティポリシーに基づき同様な考察が必要である。

公開鍵暗号の秘密鍵や共通鍵暗号のマスター鍵は、そのままの値を書き込むことはせずに、いったん別の共通鍵暗号の鍵で暗号化し、利用するときには、PINもしくはパスワード等の入力を要するのが一般的である。

付表 1-1　鍵保管場所に関する特徴

	センタ	装置（利用者）
装置を設置した場所の環境	安全性高く設定可能	攻撃を受けやすい
入退出管理	厳密管理可能	管理不可能
オペレータ教育・管理	厳密管理可能	管理不可能
物理的耐性 （tamper registrant）	中程度 他の項目により補完可能	最も重要な項目 他の項目により補完不可能
装置の筐体構造	ある程度考慮必要	非常に重要
ボード上の配線回路	同上	筐体への耐攻撃性が弱い場合考慮必要
信号端子	同上	同上
LSI 構造	同上	同上
ソフトウェアの難読性	同上	物理的耐性への耐攻撃性が弱い場合考慮必要
ファームウェア・プログラムの解析の難易度	同上	同上
メモリーへのアクセス制限	同上	同上

なお、FIPS PUB 140-2 では、4 段階にセキュリティ要求レベルを満たすべき条件を整理している。
FIPS PUB 140-2, “security requirements for cryptographic modules,”
http://www.nist.gov/itl/fipscurrent.cfm

(1)　鍵生成／鍵廃棄

共通鍵暗号の鍵は、乱数であるので比較的生成容易である。一方、公開鍵暗号は、質の良い鍵を生成するには、ある程度のプログラムと計算量を要するため、システムの構成によっては、鍵生成センタ等も必要な場合もある。RSA 暗号の鍵の生成方法の例が X.509 の付録に記載されている。

また、鍵廃棄も署名の有効性を判断する上でも大変重要である。一般には、鍵の更新・廃棄等の状況把握する機能もセンタが管理する必要がある。

(2) 鍵更新

生成した鍵を永久に安全性を保持することができる暗号アルゴリズムはなく、鍵を更新する必要がある。一般的に公開鍵暗号は、何も問題がなければ 2 年程度を有効期間としている例がある。共通鍵暗号は、公開鍵暗号と併用している場合、ほとんどの場合セッション鍵（使い捨ての鍵）としているのが普通である。

公開鍵暗号のみを利用している場合には、複数階層の鍵管理をする。最も重要となるマスター鍵は必要最小限の利用に止める必要がある。

1.2 セキュリティレベルの高度化について

一般的に、電子計算機の能力の向上および暗号解読技術の進展などにより、暗号アルゴリズムの安全性は時間の経過とともに低下するものであるが、双方向通信サービスの安全性及び信頼性を確保するためには、受信機のライフサイクル等を踏まえつつ、より安全な暗号アルゴリズムに移行することが必要となる。必要に応じてそれらの技術を取り入れることができるように、セキュリティ技術の拡張性を持たせておくことが望ましい。

米国政府で使用される暗号アルゴリズムを制定する NIST（米国標準技術研究所）では、上記の理由から定期的に採用するアルゴリズムの見直しを行っている。世界のデファクトスタンダードの暗号アルゴリズムは、そのほとんどがこの米国標準に準ずる状況である。以下の節では、この移行に関する情報を提供する。

1.2.1 RSA 公開鍵の鍵長

- NISTの勧告に準ずる形で、2013年末に証明書発効機関及び放送局のサービス提供における鍵長が1024ビットから2048ビットへ更新された。受信機の実装に当たっては、この点への留意が必要である。
- 当面の間、鍵長2048ビットのRSA公開鍵を処理できない受信機が存在する可能性がある。放送局は、サービス提供に当たり、この点への留意が必要である。

1.2.2 署名アルゴリズム

- 証明書発行機関において、今後、SHA-1アルゴリズムからSHA-2アルゴリズムへの移行が行われ、かつSHA-1アルゴリズムの証明書が発行されなくなる可能性がある。この移行が行われる時期が明確になった時点で、本規定の改定が必要となり、それに伴い、受信機の実装および放送局のサーバの運用に変更が必要となることに留意が必要である。
- また、将来においてSHA-2アルゴリズムから新規アルゴリズムへの移行が行われ、SHA-2アルゴリズムの証明書が発行されなくなる可能性がある。この移行が行われることが判明した時点で、本規定の改定が必要となる。

1.2.3 ECC 暗号

- 楕円曲線上の離散対数問題の困難性を安全の根拠とする暗号化方式であるECC暗号は、従

来のRSA暗号方式に比べて、短い鍵長で同等の安全性を実現することができる方式である。

- 但し、受信機への搭載はオプションであるため、放送局のサーバの運用については、ECC暗号に対応していない受信機に留意する必要がある。

1.2.4　データ暗号

- 将来においてデータ暗号方式として、Triple-DES、AESに代わる新規方式への移行が行われ、安全性の観点からTriple-DES、AES が運用できなくなる可能性がある。この移行が行われることが判明した時点で、本規定の改定が必要となる。

付録　2　　課金方法に関する参考情報

付録2では、データ放送事業者が課金方法を決定するときに参考となる情報を記載した。

2.1　課金方式

双方向データ放送サービスを利用する視聴者が、電子的な手段を用いて利用料金を支払う方法（課金方式）を示す。現在利用可能な主な課金方式には以下のものがある。なお、本資料で扱う用語等は経済用語を定義するものではなく、サービスイメージを説明するための便宜上のものである。

2.1.1　ネットワーク決済

(1)　ネットワーク代行課金

通信事業者の提供する代行課金サービスを利用する方式をいう。電話料金に合わせて情報料の支払いが可能である。情報料回収代行サービスなどがある。

2.1.2　カード決済

(1)　クレジット

クレジットカード利用者を対象にし、クレジット会社が利用者に代わりに支払う方式をいう。後日、クレジット会社から利用者に対して代金請求がされる。

(2)　デビット

銀行等に預金口座を持つ利用者を対象にし、利用者銀行口座から支払う方式をいう。

2.1.3　その他の決済

(1)　プリペイド

センタで管理されたバリュー（お金や価値の情報）の範囲内で支払い、残高を減算する方式をいう。

(2)　ログ収集

PPV等の課金と同様に、データ放送サービス利用料金を記録し、後日一括精算する方式をいう。

(3)　ホームバンキング

自宅から口座振込みや残高照会などができるサービスをいう。

2.2　課金方式の比較

課金方式の比較を付表2-1に示す。

付表 2-1　課金方式の比較

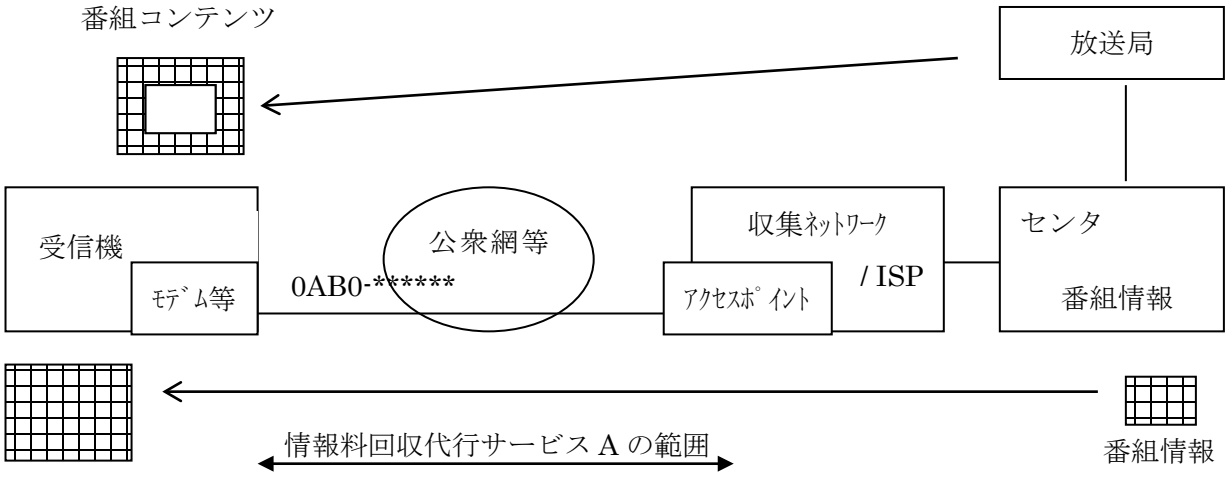
方式	ユーザ負担コスト	適用可能コンテンツ	主な適用課金領域	普及度
ネットワーク代行課金	小	物品販売以外	10 円～300 円（低額系）、1 円～1 万円（高額系）	◎
クレジット	小	物品販売、コンテンツ	数千円～数万円以上	◎
デビット	小	物品販売、コンテンツ	数千円～数万円	△
プリペイド	小	物品販売、コンテンツ	数百円～数千円	△
ログ収集	小	ストリーム系コンテンツ	数百円～数千円	◎
ホームバンキング	中	残高確認、口座振替	―	△

2.3　ネットワーク決済

ネットワーク決済のしくみは、本来情報提供者が回収すべき情報料を、通信事業者が回収業務を代行し、電話料金請求の際に合わせて回収することで実現される。情報提供者は膨大な視聴者に対し請求書の送付や管理を行うことなく、効率の良い情報提供ができる。現在提供されているサービスとして情報料回収代行サービスがある。

2.3.1　情報料回収代行サービス A

情報料回収代行サービスAの例を付図2-1に示す。



付図 2-1　情報料回収代行サービス A

(1) サービス概要

a) 放送局は情報料回収代行サービス A で提供する番組情報を、予めセンタに登録する。

b) 受信機はデータ放送、またはその他の方法で指定された情報料回収代行サービス A の番号（0AB0 - ******）に発呼する。

c) 受信機は収集ネットワークを経てセンタに接続される。

d) 受信機はサービス内容に応じて、データ放送番組情報のデータをセンタから受信する。

e) 予め設定された情報料が情報料回収代行サービス A のシステムにおいて代行回収される。

(2) 受信機に必要な機能

- 通信機能：情報料回収代行サービス A による新たなプロトコル実装は不要である。

(3) センタに必要な機能

- 番組情報配信機能

データ放送と関連する番組情報、および情報料回収代行サービス A で必要な情報（情報提供に先立ち通知する番組概要などの情報）を配信する機能。

(4) 運用上考慮すべき事項

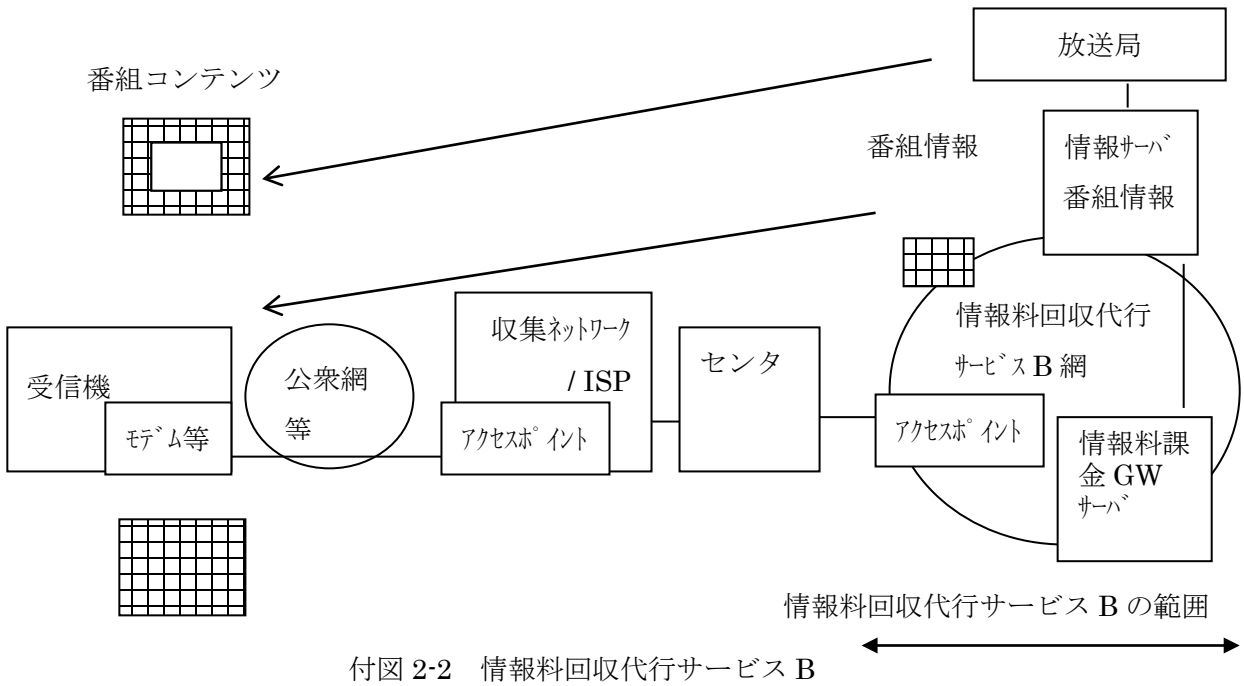
- 収集ネットワークのアクセスポイントに情報提供用回線を専用に用意する。
- PHS,携帯電話からは利用不可である。

(5) 情報料回収代行サービス A 開始までの流れ

番組企画書の審査を行い、倫理審査機関での審査完了後、情報料回収代行サービス A 契約を締結する。

2.3.2 情報料回収代行サービス B

情報料回収代行サービスBの例を付図2-2に示す。



付図 2-2 情報料回収代行サービス B

(1) サービス概要

a) 放送局は情報料回収代行サービス B で提供するデータ放送番組情報を、予め情報料回収代行サービス B 網に接続された情報サーバに登録する。

b) 受信機はデータ放送、またはその他の方法で指定された収集ネットワークのアクセスポイントに発呼する。

c) 受信機は収集ネットワークを経てセンタに接続される。

d) センタは情報料回収代行サービス B 網のアクセスポイントに接続し、ユーザ認証後、情報サーバに接続し、目的の情報（目次的なもの）を選択する。

e) 情報サーバにはセンタから、選択されたデータ放送番組情報を購入するための有料情報接続 ID,パスワードが自動入力される。

f) センタはデータ放送番組情報のデータを情報サーバより受信する。

g) センタは受信機に対してデータ放送番組情報を転送する。

h) 情報料は情報料課金 GW サーバにおいて課金される。

(2) 受信機に必要な機能

- 通信機能：情報料回収代行サービス B による新たなプロトコル実装は不要である。

(3) センタに必要な機能

- 番組情報配信機能

  情報サーバから受信したデータ放送番組情報を受信機に配信する機能。

- セキュリティ機能

  SSL3.0 以上。

(4) 情報料回収代行サービス B サービス開始までの流れ

番組企画書の審査を行い、倫理審査機関での審査完了後、情報料回収代行サービスB契約を締結する。また、SSLプロトコル利用ID（※）取得が別途必要である。

（※）SSL プロトコル利用 ID とは、SSL プロトコルを利用したセキュアな通信を行う際に必要な ID である。信頼できる第三者によって発行される。

2.4 カード決済

双方向データ放送サービスを利用するときに、クレジットカード、デビットカードを用い決済を行うものである。実際の店舗で利用する場合と同等の処理を行い、決済の安全性を確保する必要がある。

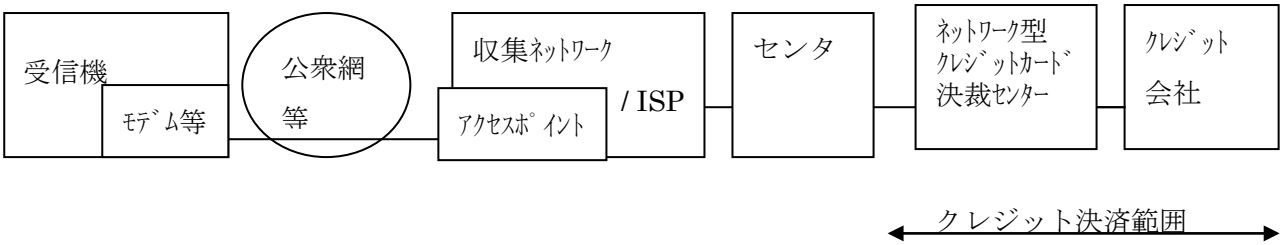
カード決済の特徴を付表2-2に示す。

付表 2-2　カード決済の特徴

	クレジットカード	デビットカード
支払い方法	後払い	同時払い
本人確認	氏名、カード番号、有効期限	口座番号、暗証番号
利用限度額	発行主体による	預金残高
専用カードリーダ・ライタ	必須ではない	必須
課題		カードリーダが受信機に必要

2.4.1 クレジットカード決済

クレジットカード決済例を付図2-3に示す。



付図 2-3　クレジットカード決済

(1) サービス概要

a) クレジットカード決済に必要なデータ（クレジットカード番号、クレジット会社名等）はセンタに予め登録する。

b) 双方向番組視聴者からの決済要求時に、センタでは視聴者とホスト側の相互認証を行う。

c) センタは、ネットワーク型クレジットカード決済センタ経由でクレジット会社に対して取り扱い金額に応じて与信照会を行う。

d) 後日、クレジット会社から視聴者に利用代金の請求がされ、視聴者の銀行口座から引き落とされる。

(2) 受信機に必要な機能

- 通信機能

クレジットカード決済で要求されるセキュリティ機能を実装する。クレジットカード決済による新たなプロトコル実装は不要である。

(3) センタに必要な機能

- クレジットカード番号等管理機能

必要に応じて予めクレジット決済に必要な情報を管理する機能。

- ネットワーク型クレジットカード決済センタに対応する機能

与信照会、照会結果受信などの機能。

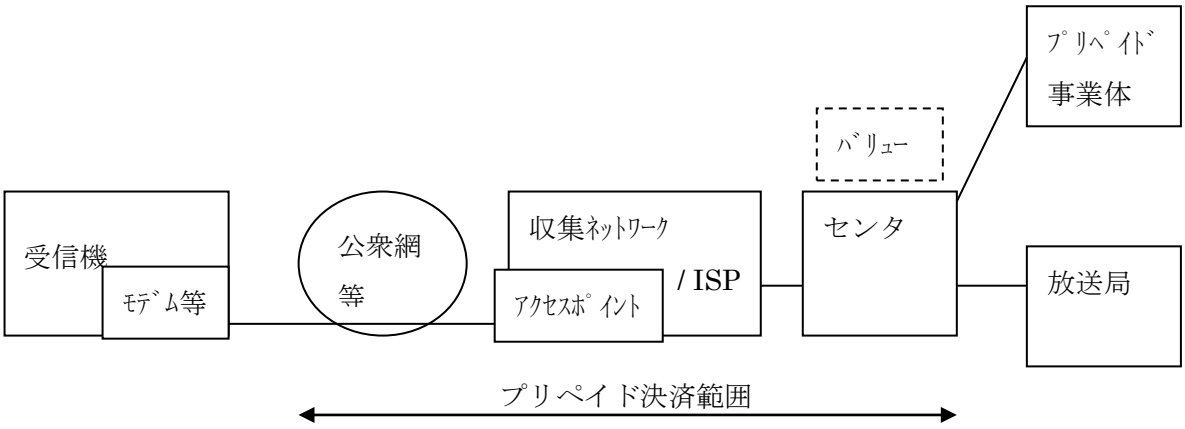
- 売上管理機能

クレジット会社の加盟店と同様に、取引の売上管理を行う機能。

2.5 その他の決済

2.5.1 プリペイド（ネットワーク型）決済

プリペイド（ネットワーク型）決済例を付図2-4に示す。



付図 2-4 プリペイド決済

(1) サービス概要

a) センタはプリペイド ID、暗証番号、バリューを管理する。

b) 双方向番組視聴者からの双方向データサービス決済要求時に、センタでは視聴者とホスト側の相互認証を行うとともに、プリペイド ID、暗証番号の入力を視聴者に要求する。

c) 視聴者からプリペイド ID、暗証番号が入力された場合、センタは現在のバリューの残高を通知する。

d) センタは、管理するバリュー残高から双方向データ放送サービス代金分を減算する。バリュー残高が 0 になった場合は、プリペイド ID を無効とする処理を行う。

e) センタは放送局とプリペイド事業体へ売上に関する情報を通知する。

f) 放送局はプリペイド事業体に代金請求を行う。

(2) 受信機に必要な機能

－ 通信機能

プリペイド（ネットワーク型）決済で要求されるセキュリティ機能。プリペイド（ネットワーク型）カード決済による新たなプロトコル実装は不要である。

(3) センタに必要な機能

－ プリペイドカード番号等管理機能

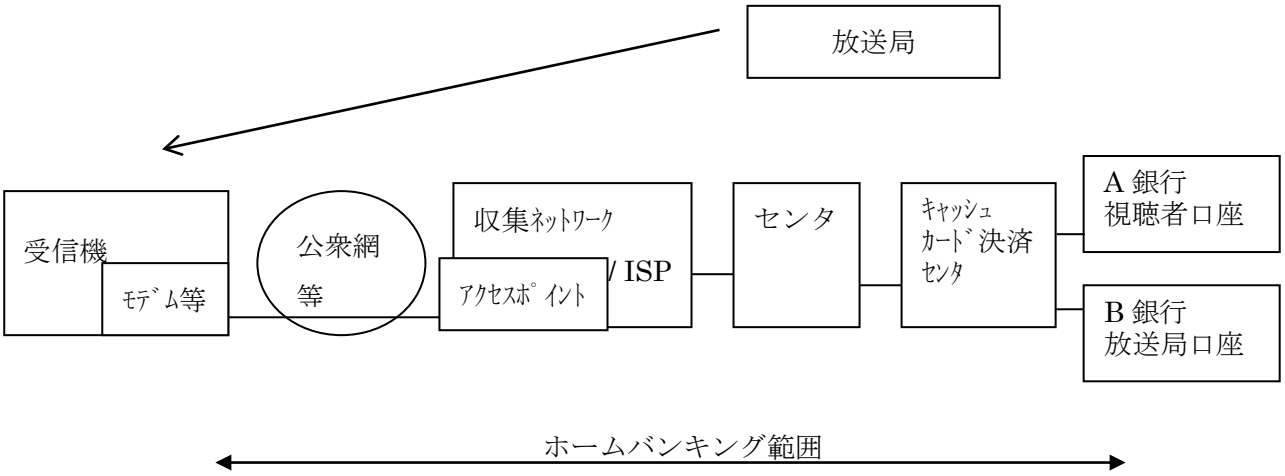
プリペイド ID、暗証番号、バリュー等の必要な情報を管理する機能。

－ 売上管理機能

販売した商品の売上に関する情報（商品コード、代金、データ放送番組名、他）を管理する機能。

2.5.2 ホームバンキング

ホームバンキング例を付図2-5に示す。



付図 2-5 ホームバンキング

(1) サービス概要

a) ホームバンキングに必要なデータ（銀行口座番号、銀行名等）を、予め必要に応じてセンタに登録する。

b) 双方向番組視聴者からのホームバンキング要求時に、センタでは視聴者とホスト側の相互認証を行う。

c) センタは、キャッシュカード決済センタ経由で視聴者口座を持つ銀行に接続を行う。

d) 視聴者の要求するホームバンキング要求に基づき、センタと視聴者口座を持つ銀行間で要求に対応した業務を行う。たとえば代金決済の場合は B 銀行口座に振込み依頼を行う。

(2) 受信機に必要な機能

- 通信機能

ホームバンキング決済で要求されるセキュリティ機能。ホームバンキング決済による新たなプロトコル実装は不要である。

(3) センタに必要な機能

- 銀行口座番号等管理機能

必要に応じて予めホームバンキングに必要な情報を管理する機能。

- キャッシュカード決済センタに対応する機能

残高照会、振込振替依頼等の業務に対応した機能。

付録　3　　輻輳に関する補足説明

3.1　輻輳とは

輻輳とは交換機に一定時間内に処理できる能力を超える通信が集中することにより、電話がつながらなくなる現象である。輻輳は電話がかからないことにより相手につながるまで繰り返し電話をかけ直す行為により増大する。

3.2　輻輳回避により得られる効果

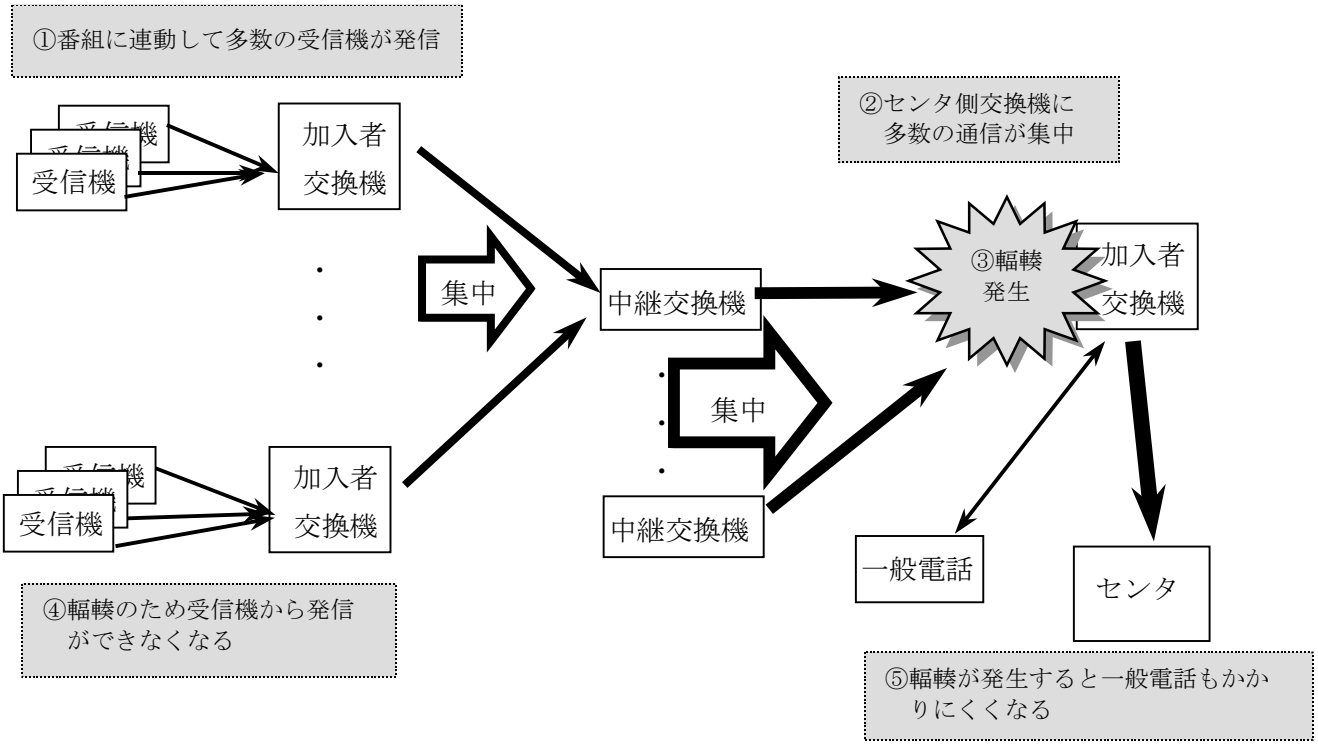
視聴者及び放送局の得られる効果を付表3-1に示す。

付表 3-1　視聴者及び放送局の得られる効果

視聴者	発信時に話中になることが少ないので、ほぼ確実に通信が可能である。従って電話がつながらないことにより、繰り返し発信する必要がない。
放送局	番組に連動して短時間に通信が集中した場合、トラヒック処理能力の限界を越えた応答データは収集できないことになるが、発信遅延等を行うことにより、結果的には効率的に多くの応答データを収集することができる。

3.3　輻輳発生のメカニズム

輻輳発生のメカニズムイメージを付図3-1に示す。



付図 3-1　輻輳発生のメカニズムイメージ

付録　4　　ネットワークサービスに関する補足説明

4.1　大量呼受付サービス

4.1.1　サービス概要

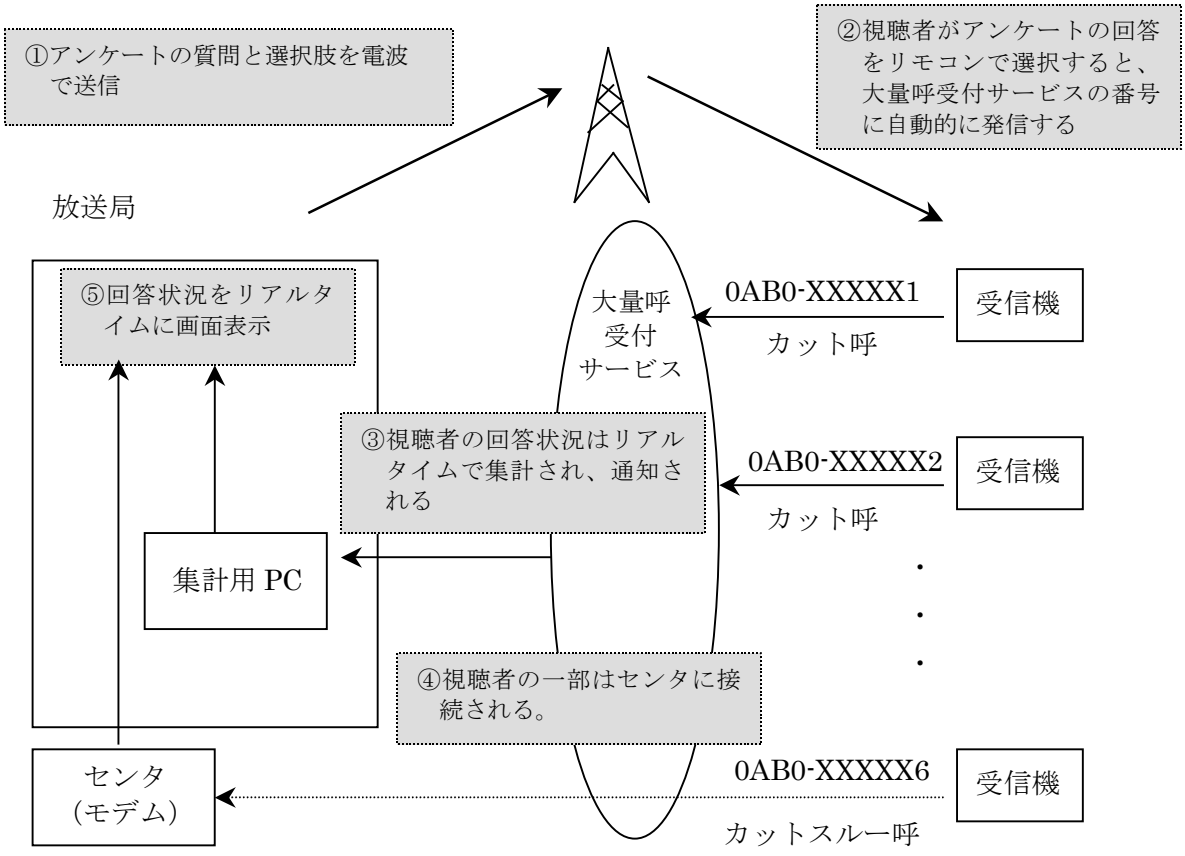
視聴者参加型の番組において、告知したサービス番号（0AB0-××××××）に対して発信された通信を自動的にカウントし、その集計結果（サービス番号ごとの合計数）を放送局にお知らせするサービス。

発信者の中から、あらかじめ設定した回線数に見合う通信を、受付用の電話回線（オペレータまたはセンタ）に接続させる「カットスルー機能」がある。

放送メディアを使った大量呼受付サービスのサービス番号数は、1番組につき最大6番号まで可能である。

4.1.2　利用例（受信機のみサービス対象）

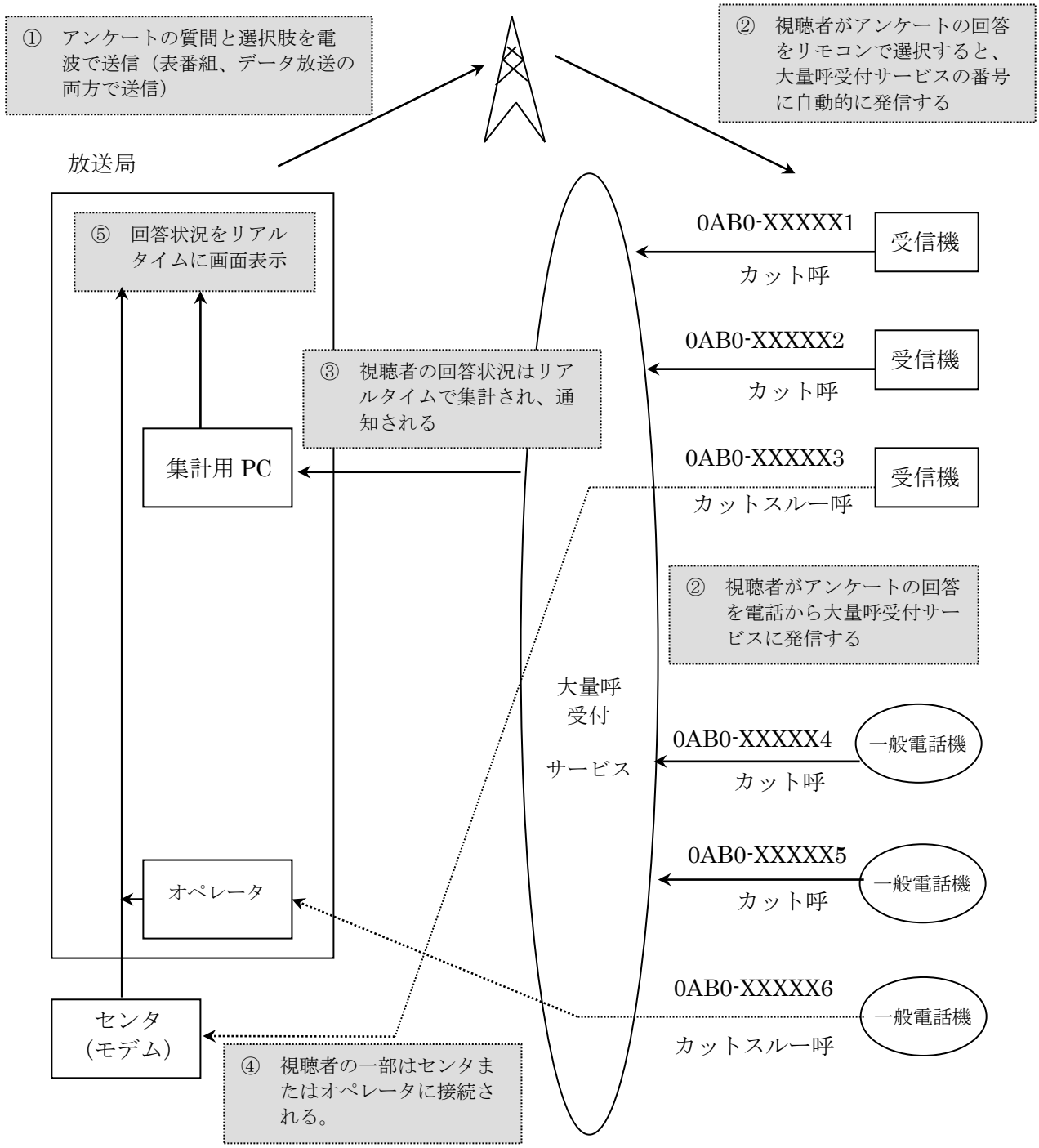
大量呼受付サービスを利用したアンケート番組のイメージを付図4-1に示す。



付図 4-1　アンケート番組イメージ（受信機のみサービス対象の場合）

4.1.3　利用例（受信機、一般電話の双方をサービス対象）

大量呼受付サービスを利用したアンケート番組のイメージを付図4-2に示す。



付図 4-2　アンケート番組イメージ（受信機、一般電話の双方がサービス対象の場合）

4.2　全国共通電話番号サービス

複数のアクセスポイントを設置した場合、アクセスポイントの電話番号を統一するため、全国共通電話番号サービスを利用した例を示す。

4.2.1　アクセスポイントの回線を着信者課金とする場合

全国共通電話番号の着信課金サービスを利用することにより、全国共通のひとつの番号にかかってきた通信を、発信地域によりあらかじめ指定したアクセスポイントに接続することが可能である。

4.2.2　アクセスポイントの回線を発信者側の課金とする場合

全国共通電話番号で発信者側に課金するサービスを利用することにより、全国共通のひとつの番号にかかってきた通信を、発信地域によりあらかじめ指定したアクセスポイントに接続することが可能である。

付録　5　　固定優先接続解除番号（122）の送出方法と接続条件

5.1　送出方法

(1)　固定優先接続を解除して通信事業者を指定

122 + 00XY + 0ABCDEFGHJ(K)

(2)　(1)で、発信者情報通知サービスの特殊番号（184、186）を併用

184（186）+ 122 + 00XY + 0ABCDEFGHJ(K)

5.2　接続条件

(1)　PSTN での発信

A　受信機から、122＋00XY＋アクセスポイントの電話番号送出時の接続条件を付表 5-1 に示す。

付表 5-1　122＋00XY＋アクセスポイントの電話番号送出時の接続条件

受信機側の回線 / ｱｸｾｽﾎﾟｲﾝﾄの電話番号例		固定優先接続の設定あり	固定優先接続の設定なし
発信側課金	0ABCDEFGHJ	○	△
着信側課金	0120+DEFGHJ	×	×
	0800+DEFGHJ	×	×
	00XY+SC+********	×	×
発信側課金	0180+ DEFGHJ	×	×
	0990+ DEFGHJ	×	×
	0570+ DEFGHJ	×	×

【凡例】○：122に続いて送出した00XY事業者に接続
△：122が不要な旨のガイダンス後、122に続いて送出した00XY事業者に接続
×：接続されない

B　122＋アクセスポイントの電話番号送出時は接続されない。

(2)　携帯電話、PHS での発信

a)　122+00XY＋アクセスポイントの電話番号送出時は接続されない。

b)　122+アクセスポイントの電話番号送出時は接続されない。

第七編

地上デジタルテレビジョン放送
送出運用規定

目　　次