Marlin IPTV-ES 運用仕様
ダウンロード編

Document Version: 1.5
Final

Date: 3 September, 2013

本仕様の内容は予告無しに変更されることがあります。

目次

1 はじめに

“Marlin IPTV End-point Service Specification” [MIPTV]では、暗号化されたコンテンツを復号するための鍵を受信機が取得するための複数のKey Delivery方式を規定している。Direct Key Delivery方式は、様々なサービスへの適用が考えられるが、最も典型的なコンテンツ配信形態としては、ダウンロードサービスが想定されるため、本編をダウンロード編と呼ぶこととする。

1.1 本書の規定範囲

本書では、暗号を復号するためのContentKeyを“Marlin IPTV End-point Service Specification” [MIPTV]の 4.2.1.2 項で規定されるActionIDが「EXTRACT with Direct Key Delivery（03h）」または「EXPORT for Copy with Direct Key Delivery（10h）」のGet Permission Requestで取得するコンテンツ（以下、本書では“コンテンツ”と記す）の利用に関し、[MIPTV]に対する詳細規定項目と、[MIPTV]に対する追加規定項目を規定し、さらに“Marlin IPTV-ES/J Specific Compliance Rules ダウンロード編” [IPTVCRDL]に対する詳細規定項目を規定する。
本書は、[IPTVCRDL]に準拠する受信機およびDRMサーバに適用する。

以下に本書の規定項目を示す。

- [MIPTV]に対する詳細規定項目
  - SACに関する規定（[MIPTV], 4.1 節 Secure Authenticated Channel (SAC)Protocol）
    - メッセージパラメータ
    - SAC タイムアウト
    - 1 つの TCP Connection を利用可能な SAC セッション
  - Service Protocolに関する規定（[MIPTV], 4.2 節Marlin IPTV-ES Service Protocols over SACに関する規定）
    - メッセージパラメータの設定
    - メッセージパラメータの検証

- [MIPTV]に対する追加規定項目
  - ネットワーク通信プロトコル（HTTP）に関する規定
    - HTTP による SAC のメッセージの伝送
    - HTTP ヘッダ

- [IPTVCRDL]に対する詳細規定項目
  - 鍵の利用に関する規定

1.2 引用文書

[IPTVCRDL]	“Marlin IPTV-ES/J Specific Compliance Rules ダウンロード編”, Version 1.6
[IPTVESVOD]	“Marlin IPTV-ES 運用仕様 VOD 編”,Version 1.4
[MIPTV]	“Marlin IPTV End-point Service Specification”, Version 1.0.2

1.3 用語の定義

本書で用いる用語を以下のように定義する。

用語	定義
SAC 確立	受信機と DRM サーバとの間で相互認証とセッション鍵の共有を行うこと。
SAC 終了	SAC で用いたメッセージパラメータとセッション鍵を利用できないようにし、SAC で用いた TCP Connection を切断すること。
コンテンツ	暗号を復号するためのContentKeyを[MIPTV]の 4.2.1.2 項で規定されるActionIDが「EXTRACT with Direct Key Delivery（03h）」または「EXPORT for Copy with Direct Key Delivery（10h）」のGet Permission Requestで取得するコンテンツ。
不揮発性記憶領域	電源を切っても記憶したデータが消えない領域のこと。無停電電源装置などの障害対策が行われている機器の揮発性記憶領域も含む。

本書で用いる用語と[MIPTV]の用語との対応を以下に示す。

本書	[MIPTV]
DRM サーバ	Marlin IPTV-ES Server
受信機	Marlin IPTV-ES Device

1.4 バイトオーダー

本書で定義されるプロトコルの多バイト数値のバイトオーダーは“Big Endian”である。

2 SACに関する規定

本章では IPTV-ES SAC の運用を規定する。

2.1 メッセージパラメータ

メッセージパラメータに関する規定は、[IPTVESVOD], 2.1 節と同等である。

2.2 SACタイムアウト

SACタイムアウトに関する規定は、[IPTVESVOD], 2.2 節と同等である。

2.3 1 つのTCP Connectionを利用可能なSACセッション

1 つのTCP Connectionを利用可能なSACセッションに関する規定は、[IPTVESVOD], 2.3 節と同等である。

3 Service Protocolに関する規定

本章では、IPTV-ES Service Protocol の運用を規定する。
なお、メッセージパラメータに設定する UsageRuleReference、メッセージ送信先の DRM サーバの URI を受信機が取得する方法について、本書では規定しない。

3.1 Get Permission Protocol (EXTRACT)

[MIPTV], 4.2 節で規定されるGet Permission Protocolにおいて、ActionIDが「EXTRACT with Direct Key Delivery（03h）」のGet Permission Requestを用いて、ContentKeyを取得する場合について、本節では、メッセージパラメータの設定とメッセージパラメータの検証について規定する。

3.1.1 メッセージパラメータの設定

受信機と DRM サーバは、以下の規定に従い、メッセージパラメータを設定する。

3.1.1.1 Get Permission Request parameters

受信機は、[MIPTV], 4.2.1.2 項および以下の規定に従い、Get Permission Requestのメッセージパラメータを設定する。

- UsageRuleReference
  - 事前に取得した UsageRuleReference を設定する。

3.1.1.2 Get Permission Reply parameters

DRMサーバは、[MIPTV], 4.2.1.3 項および 4.2.1.6 項の規定に従い、Get Permission Replyのメッセージパラメータを設定する。

3.1.2 メッセージパラメータの検証

受信機と DRM サーバは、メッセージ受信時に以下の規定に従いメッセージパラメータを検証する。

3.1.2.1 Get Permission Request parameters

DRMサーバは、[MIPTV], 4.2.4.1 項および以下の規定に従い、Get Permission Requestのメッセージパラメータを検証する。

- ActionID
  - ActionID が「EXTRACT with Direct Key Delivery（03h）」の Get Permission Request に対応する DRM サーバは、ActionID が、以下に示す値の場合には検証失敗としない。
    - EXTRACT with Direct Key Delivery（03h）

3.1.2.2 Get Permission Reply parameters

受信機は、[MIPTV], 4.2.4.2 項および 4.2.4.5 項の規定に従い、Get Permission Reply のメッセージパラメータを検証する。

3.2 Get Permission Protocol (EXPORT)

[MIPTV], 4.2 節で規定されるGet Permission Protocolにおいて、ActionIDが「EXPORT for Copy with Direct Key Delivery（10h）」のGet Permission Requestを用いて、ContentKeyを取得する場合について、本節では、メッセージパラメータの設定とメッセージパラメータの検証について規定する。

3.2.1 メッセージパラメータの設定

受信機と DRM サーバは、以下の規定に従いメッセージパラメータを設定する。

3.2.1.1 Get Permission Request parameters

受信機は、[MIPTV], 4.2.1.2 項および以下の規定に従い、Get Permission Requestのメッセージパラメータを設定する。

- UsageRuleReference
  - 事前に取得した UsageRuleReference を設定する。

3.2.1.2 Get Permission Reply parameters

DRMサーバは、[MIPTV], 4.2.1.3 項および 4.2.1.7 項の規定に従い、Get Permission Replyのメッセージパラメータを設定する。

3.2.2 メッセージパラメータの検証

受信機と DRM サーバは、メッセージ受信時に以下の規定に従い、メッセージパラメータを検証する。

3.2.2.1 Get Permission Request parameters

DRMサーバは、[MIPTV], 4.2.4.1 項および以下の規定に従い、Get Permission Requestのメッセージパラメータを検証する。

- ActionID
  - ActionID が「EXPORT for Copy with Direct Key Delivery（10h）」の Get Permission Request に対応する DRM サーバは、ActionID が以下に示す値の場合には検証失敗としない。
    - ✧ EXPORT for Copy with Direct Key Delivery（10h）

3.2.2.2 Get Permission Reply parameters

受信機は、[MIPTV], 4.2.4.2 項、4.2.4.6 項の規定に従い、Get Permission Replyのメッセージパラメータを検証する。

3.3 Get Trusted Time Protocol

[MIPTV], 4.2.2 項で規定されるGet Trusted Time Protocolは、Datetimeの取得に用いる。
受信機は、[MIPTV], 4.2.2.2 項の規定に従い、Get Trusted Time Requestのメッセージパラメータを設定する。また、受信機は、[MIPTV], 4.2.4.10 項の規定に従い、Get Trusted Time Replyのメッセージパラメータを検証する。
DRMサーバは、[MIPTV], 4.2.4.9 項の規定に従い、Get Trusted Time Requestのメッセージパラメータを検証する。また、DRMサーバは、[MIPTV], 4.2.2.3 項の規定に従い、Get Trusted Time Replyのメッセージパラメータを設定する。

3.4 Packed Message Protocol

[MIPTV], 4.2.3 項で規定されるPacked Message Protocolは、以下を同時取得する場合に用いる。

- EXTRACT と EXPORT の ContentKey。
- EXTRACT の ContentKey と Datetime。
- EXPORT の ContentKey と Datetime。
- EXTRACT および EXPORT の ContentKey と Datetime。

本節では、メッセージパラメータの設定とメッセージパラメータの検証について規定する。

3.4.1 メッセージパラメータの設定

受信機と DRM サーバは、以下の規定に従い、メッセージパラメータを設定する。

3.4.1.1 Packed Message Request parameters

受信機は、[MIPTV], 4.2.3.2 項および以下の規定に従い、Packed Message Request のメッセージパラメータを設定する。

- RequestMessageBoxList
  - 表 3-1に示す順番にメッセージを格納する。

表 3-1　RequestMessageBoxList に格納可能な RequestMessage の組み合わせ

RequestMessage の個数（NumberOfRequestMessageBoxes の値）	1 番目の RequestMessage	2 番目の RequestMessage	3 番目の RequestMessage
2	Get Permission Request（EXTRACT with Direct Key Delivery（03h））	Get Permission Request（EXPORT for Copy with Direct Key Delivery（10h））	
2	Get Permission Request（EXTRACT with Direct Key Delivery（03h））	Get Trusted Time Request	
2	Get Permission Request（EXPORT for Copy with Direct Key Delivery（10h））	Get Trusted Time Request	
3	Get Permission Request（EXTRACT with Direct Key Delivery（03h））	Get Permission Request（EXPORT for Copy with Direct Key Delivery（10h））	Get Trusted Time Request

3.4.1.2 Packed Message Reply parameters

DRMサーバは、[MIPTV], 4.2.3.3 項の規定に従い、Packed Message Replyのメッセージパラメータを設定する。

3.4.2 メッセージパラメータの検証

受信機と DRM サーバは、メッセージ受信時に以下の規定に従いメッセージパラメータを検証する。

3.4.2.1 Packed Message Request parameters

DRMサーバは、[MIPTV], 4.2.4.11 項および以下の規定に従い、Packed Message Requestのメッセージパラメータを検証する。

- RequestMessageBoxList
  - RequestMessageBoxList に ActionID が「EXTRACT with Direct Key Delivery（03h）」または「EXPORT for Copy with Direct Key Delivery（10h）」の Get Permission Request の RequestMessage が 1 以上格納されている場合、かつ、RequestMessage の組み合わせが、
  - 表 3-1以外の組み合わせの場合には検証失敗とし、Packed Message Reply parameterのStatusを「Message format error（8009h）」とする。

3.4.2.2 Packed Message Reply parameters

受信機は、[MIPTV], 4.2.4.12 項の規定に従い、Packed Message Replyのメッセージパラメータを検証する。

4 ネットワーク通信プロトコル（HTTP）に関する規定

ネットワーク通信プロトコル（HTTP）に関する規定は、[IPTVESVOD], 4 章と同等である。

5 鍵の利用に関する規定

本章では、[IPTVCRDL], 4 章で規定される鍵の利用に関する運用を規定する。

5.1 再生を目的としたContentKeyの利用

本書では、[IPTVCRDL], 4.1.1 項で規定される合理的な期間を 4 時間とする。

A Appendix（Informative）

A.1 SAC処理の例

本節では、ActionID が「EXPORT for Copy with Direct Key Delivery（10h）」の Get Permission Protocol に対応した受信機と DRM サーバの SAC 処理の例を示す。

A.1.1 状態遷移

SAC処理に関わる受信機の状態遷移を表A-1に、DRMサーバの状態遷移を表A-2に示す。
SAC を行う 1 対の受信機と DRM サーバは、状態遷移表に従って状態を遷移する。
表A-1のTransactionFlagは、Response & Challenge messageの送信元のDRMサーバの識別情報と対応付けて記憶したTransactionFlagである。
本書の規定外となる状態とイベントの組み合わせは、表中“ー”で示す。
なお、本書に規定されていないが、表A-1に受信機のSACタイムアウトを記述した。

表A-1　受信機の状態遷移表

		受信機の状態							
		①SAC 開始前	②Challenge message 送信後のメッセージ受信待ち	③Response & Request message 送信後のメッセージ受信待ち		④Request message 送信後のメッセージ受信待ち		⑤Encrypted command message 送信後のメッセージ受信待ち	⑥Response & Commit message 送信後のメッセージ受信待ち
				送信する Request がある	送信する Request がない	送信する Request がある	送信する Request がない		
SAC 開始指示		A.1.2項(1)の処理を実行して、②に移る	―	―	―	―	―	―	―
メッセージ受信イベント	Response & Challenge message 受信	―	A.1.2項(4)の処理を実行する • メッセージ検証に成功した場合は、TransactionFlag を記憶していなければ③に移り、TransactionFlag を記憶していれば⑥に移る • メッセージ検証に失敗した場合は①に移る	①に移る	①に移る	①に移る	①に移る	①に移る	①に移る

	Reply message 受信	—	①に移る	A.1.2項(8)の処理を実行する • メッセージ検証に成功し、[MIPTV], 4.1.4.10.1項の第2項目に該当する場合※は①に、それ以外の場合は④に移る • メッセージ検証に失敗した場合は①に移る	A.1.2項(8)の処理を実行する • メッセージ検証に成功し、[MIPTV], 4.1.4.10.1項の第2項目に該当する場合※は①に、それ以外の場合は⑤に移る • メッセージ検証に失敗した場合は①に移る	A.1.2項(8)の処理を実行する • メッセージ検証に成功し、[MIPTV], 4.1.4.10.1項の第2項目に該当する場合※は①に、それ以外の場合は④に移る • メッセージ検証に失敗した場合は①に移る	A.1.2項(8)の処理を実行する • メッセージ検証に成功し、[MIPTV], 4.1.4.10.1項の第2項目に該当する場合※は①に、それ以外の場合は⑤に移る • メッセージ検証に失敗した場合は①に移る	①に移る	①に移る
	Encrypted command message 受信	—	①に移る	①に移る	①に移る	A.1.2項(14)の処理を実行して、①に移る	A.1.2項(14)の処理を実行して、①に移る	A.1.2項(14)の処理を実行して、①に移る	A.1.2項(14)の処理を実行して、①に移る
	Plain command message 受信	—	A.1.2項(15)の処理を実行して、①に移る	A.1.2項(15)の処理を実行して、①に移る	A.1.2項(15)の処理を実行して、①に移る	①に移る	①に移る	①に移る	A.1.2項(15)の処理を実行して、①に移る
	[MIPTV], 4.1.4.1項の Message header 検証に失敗（PayloadType が上記のメッセージの場合を除く）	—	①に移る	①に移る	①に移る	①に移る	①に移る	①に移る	①に移る
SAC タイムアウト		—	①に移る	①に移る	①に移る	①に移る	①に移る	①に移る	①に移る

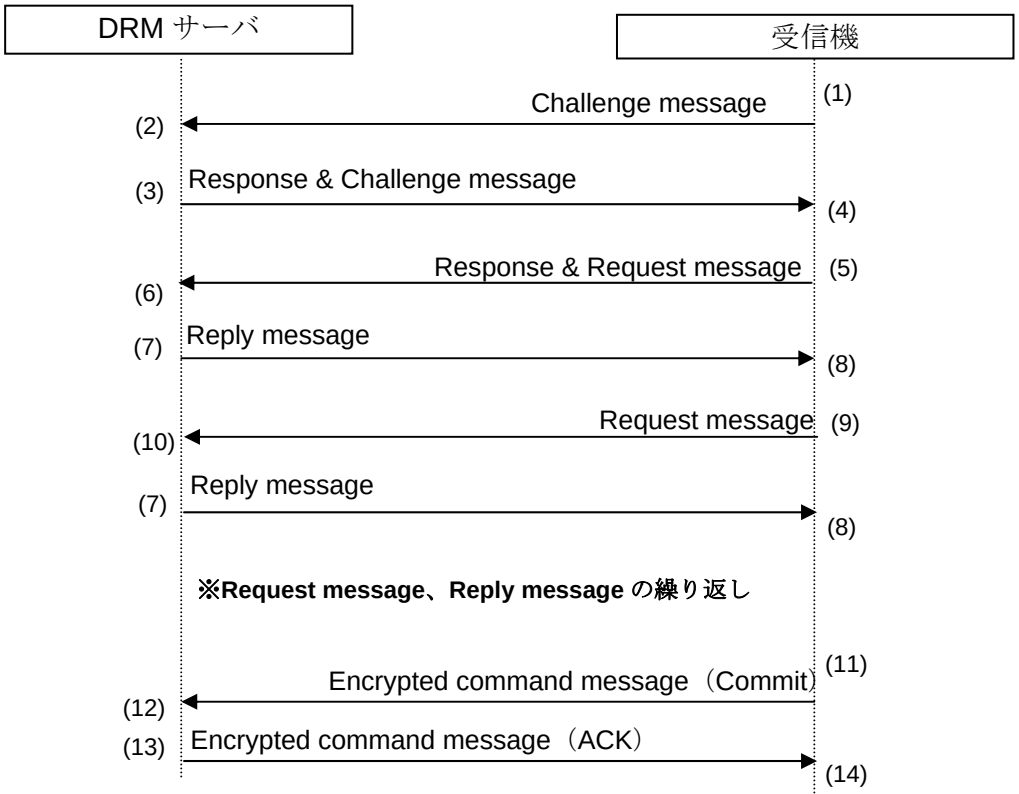
366 * Service Protocolの検証失敗により発生する状態遷移
367

表 A-2　DRM サーバの状態遷移表

		DRM サーバの状態		
		㋐SAC 開始前のメッセージ受信待ち	㋑Response & Challenge message 送信後のメッセージ受信待ち	㋒Reply message 送信後のメッセージ受信待ち
メッセージ受信イベント	Challenge message 受信	A.1.2項(2)の処理を実行する • メッセージ検証に成功した場合は㋑に移る • メッセージ検証に失敗した場合は㋐に移る	新たなSACとしてA.1.2項(2)の処理を実行する。Response & Challenge messageを送信したSACは終了する。 • メッセージ検証に成功した場合は㋑に移る • メッセージ検証に失敗した場合は㋐に移る	新たなSACとしてA.1.2項(2)の処理を実行する。Reply messageを送信したSACは終了する。 • メッセージ検証に成功した場合は㋑に移る • メッセージ検証に失敗した場合は㋐に移る
	Response & Request message 受信	㋐に移る	A.1.2項(6)の処理を実行する • メッセージ検証に成功した場合は㋒に移る • メッセージ検証に失敗した場合は㋐に移る	㋐に移る
	Request message 受信	㋐に移る	㋐に移る	A.1.2項(10)の処理を実行する • メッセージ検証に成功した場合は㋒に移る • メッセージ検証に失敗した場合は㋐に移る
	Encrypted command message 受信	㋐に移る	㋐に移る	A.1.2項(12)の処理を実行して、㋐に移る
	Response & Commit message 受信	㋐に移る	A.1.2項(19)の処理を実行して、㋐に移る	㋐に移る
	[MIPTV], 4.1.4.1項の Message header 検証に失敗（PayloadType が上記以外のメッセージの場合を除く）	㋐に移る	㋐に移る	㋐に移る
SAC タイムアウト		—	㋐に移る	㋐に移る

A.1.2 メッセージ処理

本項では、受信機と DRM サーバが、メッセージ送受信時に行う SAC のメッセージ処理の典型例を示す。
以降で説明するメッセージ処理の基本シーケンスについて、図A-1、図A-2、図A-3に示す。図中の()つきの番号は、各メッセージの送受信処理の種類を示す。以下、各処理について説明する。



図A-1　基本シーケンス（複数の Request を連続送信する場合）

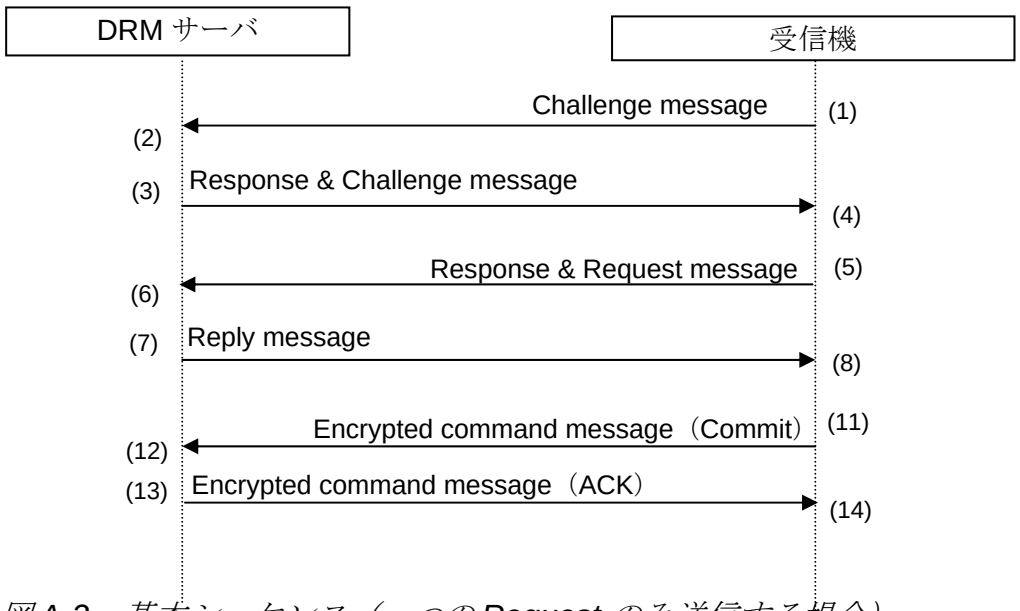


図 A-2　基本シーケンス（一つの Request のみ送信する場合）

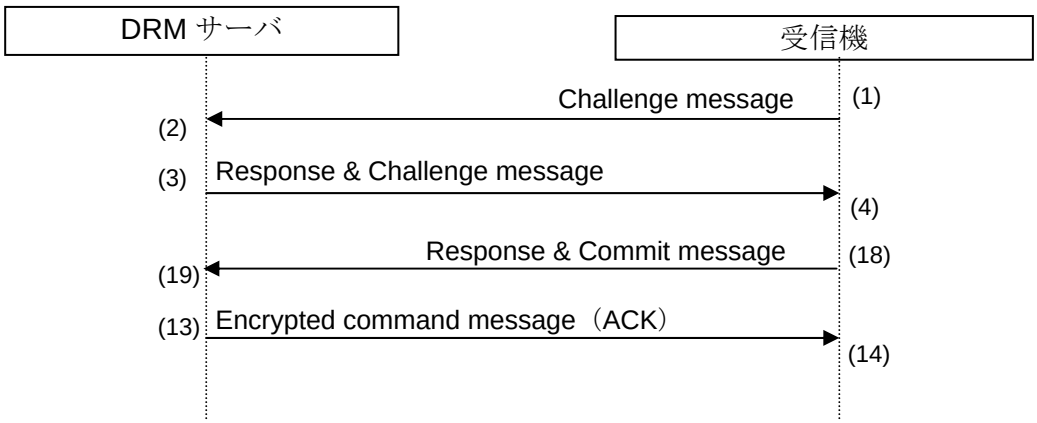


図 A-3　基本シーケンス
（受信機が Response & Challenge message の送信元の DRM サーバの識別情報と対応付けた TransactionFlag が記憶されている場合）

(1)　Challenge message送信時の受信機処理

Challenge message送信時の受信機処理は、[IPTVESVOD], A.1.2 項(1)と同等である。

(2)　Challenge message受信時のDRMサーバ処理

Challenge message受信時のDRMサーバ処理は、[IPTVESVOD], A.1.2 項(2)と同等である。

(3) Response & Challenge message送信時のDRMサーバ処理

Response & Challenge message送信時のDRMサーバ処理は、[IPTVESVOD], A.1.2 項(3)と同等である。

(4) Response & Challenge message受信時の受信機処理

- [MIPTV], 4.1.4.3 項の規定に従い、Response & Challenge messageの検証を行う。
  - 検証が成功した場合、以下の処理を実行する。
    - Response & Challenge messageの送信元のDRMサーバの識別情報と対応付けたTransactionFlagが不揮発性記憶領域に記憶されていない場合、(5)Response & Request message送信時の受信機処理を実行する。
    - Response & Challenge messageの送信元のDRMサーバの識別情報と対応付けたTransactionFlagが不揮発性記憶領域に記憶されている場合、(18)Response & Commit message送信時の受信機処理を実行する。
  - 検証が失敗した場合、SAC を終了して、SAC 開始前の状態に移る。

(5) Response & Request message送信時の受信機処理

Response & Request message送信時の受信機処理は、[IPTVESVOD], A.1.2 項(5)と同等である。

(6) Response & Request message受信時のDRMサーバ処理

- [MIPTV], 4.1.4.4 項の規定に従い、Response & Request messageの検証を行い、セッション鍵を生成する。
  - 検証が成功した場合、以下の処理を行い、(7)Reply message送信時のDRMサーバ処理を実行する。
    - Response & Request message の送信元の受信機の識別情報と対応付けた TransactionFlag が不揮発性記憶領域に記憶されている場合、Response & Request message の送信元の受信機に最後に送信した Reply message を受信機が受信していないと判断する。
    - SequenceNumberとして、[MIPTV], 4.1.4.4 項でSequenceNumberの確認に用いた値よりも 1 大きい値である 2 を保持する。
    - Response & Request message の TransactionFlag を保持する。
    - Response & Request message から Service Protocol のメッセージを抽出する。
  - 検証が失敗した場合、(16)Plain command message送信時のDRMサーバ処理を実行する。

(7) Reply message送信時のDRMサーバ処理

- Reply message を作成する。Reply message のメッセージパラメータに関して以下の処理を行う。
  - SequenceNumber：保持している SequenceNumber を用いる。
  - 以下に示すように TransactionFlagRecordFlag を設定する。
    - [MIPTV], 4.1.3.6 項の規定に従い、EXPORTに用いるContentKeyに

ついて受信機での取得回数をカウントする場合、「record（01h）」を設定する。
- 上記以外の場合、「not to record（00h）」を設定する。

✧ Reply：Service Protocol のメッセージを設定する。
✧ MessageDigest：暗号化前の MessageDigest を除く Reply message のパラメータから生成する。
✧ SequenceNumber、TransactionFlagRecordFlag、Reply、MessageDigest はセッション鍵で暗号化する。

➢ Reply message を作成後に保持している SequenceNumber を 1 増加する。
➢ TransactionFlag の記憶・削除を行う。
✧ TransactionFlagRecordFlag に「record（01h）」を設定する場合、Reply message の送信先の受信機の識別情報と対応付けて、最後に受信機から受信した TransactionFlag を不揮発性記憶領域に記憶する。
✧ TransactionFlagRecordFlag に「not to record（00h）」を設定する場合、Reply message の送信先の受信機の識別情報と対応付けて不揮発性記憶領域に記憶されている TransactionFlag を削除する。
➢ Reply messageを受信機に送信する。
➢ Reply message送信後のメッセージ受信待ちの状態に移る。

(8) Reply message受信時の受信機処理

➢ [MIPTV], 4.1.4.6 項の規定に従い、Reply messageの検証を行う。
✧ 検証が成功した場合、以下の処理を行い、送信するRequestがある場合は(9)Request message送信時の受信機処理を実行し、送信するRequestがない場合は(11)Encrypted command message送信時の受信機処理を実行する。ただし、[MIPTV], 4.1.4.10.1 項の第 2 項目に該当する場合はSACを終了して、SAC開始前の状態に移る。
- 保持している SequenceNumber を 1 増加する。
- TransactionFlag の反転と保持を行う。現在、保持しているTransactionFlag が even（00h）の場合は「odd（01h）」を、odd（01h）の場合は「even（00h）」を保持する。
- Reply message から Service Protocol のメッセージを抽出する。
- [MIPTV], 4.1.4.11.1 項(2)の実行条件を満たす場合、Reply messageの送信元のDRMサーバの識別情報と対応付けて不揮発性記憶領域に記憶されているTransactionFlagを削除する。
- [MIPTV], 4.1.4.11.1 項(1)の実行条件を満たす場合、Reply messageの送信元のDRMサーバに最後に送信したTransactionFlagをReply messageの送信元のDRMサーバの識別情報と対応付けて不揮発性記憶領域に記憶する。

✧ 検証が失敗した場合、SAC を終了して、SAC 開始前の状態に移る。

なお、ContentKey に関して、Reply message の検証が成功した場合、以下の処理を行う。

➢ [MIPTV], 4.1.4.11.1 項(2)の実行条件を満たす場合、Reply messageの送信元のDRMサーバの識別情報と対応付けたTransactionFlagの削除と共に、当該TransactionFlagと対応付けて不揮発性記憶領域に記憶されている利用不可の状態のContentKeyを、利用可能な状態に変更する。

- [MIPTV], 4.1.4.11.1 項(1)の実行条件を満たす場合、TransactionFlagの記憶と共に、記憶するTransactionFlagと対応付けて、Reply messageで取得したContentKeyを利用不可の状態で不揮発性記憶領域に記憶する。

(9) Request message送信時の受信機処理

Request message送信時の受信機処理は、[IPTVESVOD], A.1.2 項(9)と同等である。

(10) Request message受信時のDRMサーバ処理

- [MIPTV], 4.1.4.5項の規定に従い、Request messageの検証を行う。
  - 検証が成功した場合、以下の処理を行い、(7)Reply message送信時のDRMサーバ処理を実行する。
    - Request message の送信元の受信機の識別情報と対応付けた TransactionFlag を不揮発性記憶領域に記憶している場合、最後に送信した Reply message を受信機が受信していると判断する。
    - 保持している SequenceNumber を 1 増加する。
    - 保持している TransactionFlag を受信した Request message の TransactionFlag に変更して保持する。
    - Request message から Service Protocol のメッセージを抽出する。
  - 検証が失敗した場合、以下の処理を行い、(17)Commandが「ERROR」のEncrypted command message送信時のDRMサーバ処理を実行する。
    - 保持している SequenceNumber を 1 増加する。

なお、サービス事業者（DRM サーバを含む）は、ContentKey に関して、最後に送信した Reply message を受信機が受信していると判断した場合、以下の処理を行う。

- Request message の送信元の受信機に最後に送信した ContentKey の取得回数のカウントを行う。

(11) Encrypted command message送信時の受信機処理

Encrypted command message送信時の受信機処理は、[IPTVESVOD], A.1.2 項(11)と同等である。

(12) Encrypted command message受信時のDRMサーバ処理

- [MIPTV], 4.1.4.8 項の規定に従い、Encrypted command messageの検証を行う。
  - 検証が成功した場合、以下の処理を行い、(13)Commandが「ACK」のEncrypted command message送信時のDRMサーバ処理を実行する。
    - Encrypted command message の送信元の受信機の識別情報と対応付けた TransactionFlag を不揮発性記憶領域に記憶している場合、最後に送信した Reply message を受信機が受信していると判断する。
    - 保持している SequenceNumber を 1 増加する。
  - 検証が失敗した場合、以下の処理を行い、(17)Command が「ERROR」のEncrypted command message送信時のDRMサーバ処理を実行する。

- 保持している SequenceNumber を 1 増加する。

なお、サービス事業者（DRM サーバを含む）は、ContentKey に関して、最後に送信した Reply message を受信機が受信していると判断した場合、以下の処理を行う。

- Encrypted command message の送信元の受信機に最後に送信した ContentKey の取得回数のカウントを行う。

(13) Commandが「ACK」のEncrypted command message送信時のDRMサーバ処理

- Encrypted command message を作成する。Encrypted command message のメッセージパラメータに関して以下の処理を行う。
  - SequenceNumber：保持している SequenceNumber を用いる。
  - Command：「ACK」を設定する。
  - Status：「Success（0000h）」を設定する。
  - MessageDigest：暗号化前の MessageDigest を除く Encrypted command message のパラメータから生成する。
  - SequenceNumber、TransactionFlag、Command、Status、MessageDigest はセッション鍵で暗号化する。
- Encrypted command message の送信先の受信機の識別情報と対応付けて不揮発性記憶領域に記憶されている TransactionFlag を削除する。
- Encrypted command message を受信機に送信する。
- SAC を終了して、SAC 開始前の状態に移る。

(14) Encrypted command message受信時の受信機処理

- [MIPTV], 4.1.4.8 項の規定に従い、Encrypted command messageの検証を行う。
  - 検証が成功した場合、以下の処理を行う。
    - [MIPTV], 4.1.4.11.1 項(2)の実行条件を満たす場合、Encrypted command messageの送信元のDRMサーバの識別情報と対応付けて不揮発性記憶領域に記憶されているTransactionFlagを削除する。
- SAC を終了して、SAC 開始前の状態に移る。

なお、ContentKey に関して、Encrypted command message の検証が成功した場合、以下の処理を行う。

- [MIPTV], 4.1.4.11.1 項(2)の実行条件を満たす場合、Encrypted command messageの送信元のDRMサーバの識別情報と対応付けられたTransactionFlagの削除と共に、当該TransactionFlagと対応付けて不揮発性記憶領域に記憶されている利用不可の状態のContentKeyを、利用可能な状態に変更する。

(15) Plain command message受信時の受信機処理

Plain command message受信時の受信機処理は、[IPTVESVOD], A.1.2 項(15)と同等である。

(16) Plain command message送信時のDRMサーバ処理

Plain command message送信時のDRMサーバ処理は、[IPTVESVOD], A.1.2 項(16)と同等である。

(17) Commandが「ERROR」のEncrypted command message送信時のDRMサーバ処理

Commandが「ERROR」のEncrypted command message送信時のDRMサーバ処理は、[IPTVESVOD], A.1.2 項(17)と同等である。

(18) Response & Commit message送信時の受信機処理

- セッション鍵を生成する。
- Response & Commit message を作成する。Response & Commit message のメッセージパラメータに関して以下の処理を行う。
  - Signature：SourceRandomNumber と SinkEC-DHPhase1Value に対して生成する。
  - SequenceNumber：1 を Response & Commit message に設定する。
  - TransactionFlag：Response & Commit message の送信先の DRM サーバの識別情報と対応付けて不揮発性記憶領域に記憶されている TransactionFlag の値を Response & Commit message に設定する。
  - MessageDigest：暗号化前の MessageDigest を除く Response & Commit message のパラメータから生成する。
  - SequenceNumber、TransactionFlag、MessageDigest をセッション鍵で暗号化する。
- SequenceNumber として、Response & Commit message に設定した値よりも 1 大きい値である 2 を保持する。
- Response & Commit message を DRM サーバに送信する。
- Response & Commit message 送信後のメッセージ受信待ちの状態に移る。

なお、受信機は、DRM サーバの URI を不揮発性記憶領域に記憶しておくと、電源 ON 時など再度 DRM サーバの URI を取得せずに、Response & Commit message を送信する SAC を実行することができる。

(19) Response & Commit message受信時のDRMサーバ処理

- [MIPTV], 4.1.4.9 項に従い、Response & Commit messageの検証を行い、セッション鍵を生成する。
  - 検証が成功した場合、以下の処理を行い、(13)Commandが「ACK」のEncrypted command message送信時のDRMサーバ処理を実行する。
    - Response & Commit message の送信元の受信機の識別情報と対応付けた TransactionFlag を不揮発性記憶領域に記憶している場合、Response & Commit message の TransactionFlag と比較して Reply message の受信判断を行う。
      - TransactionFlag が一致する場合は、最後に送信した Reply message を受信機が受信していると判断する。
      - TransactionFlag が異なる場合は、最後に送信した Reply message を受信機が受信していないと判断する。
    - SequenceNumberとして、[MIPTV], 4.1.4.9 項でSequenceNumberの確認に用いた値よりも 1 大きい値である 2 を保持する。

- ✧ 検証が失敗した場合、(16)Plain command message送信時のDRMサーバ処理を実行する。

なお、サービス事業者（DRM サーバを含む）は、ContentKey に関して、最後に送信した Reply message を受信機が受信していると判断した場合、以下の処理を行う。

- ➢ Response & Commit message の送信元の受信機に最後に送信した ContentKey の取得回数のカウントを行う。

A.2 TransactionFlagに関する処理の解説

コンテンツを EXPORT する回数を制限する場合、受信機が ContentKey を取得した回数をサービス事業者が正しく把握できる必要がある。
この場合、受信機と DRM サーバが TransactionFlag を以下のように記憶し処理することで、DRM サーバが受信機での ContentKey の取得が確認できた場合にのみ、サービス事業者は当該受信機の ContentKey の取得回数をカウントする。したがって、通信エラーや突発的な電源断などの障害により SAC が終了し、受信機が ContentKey を未取得の場合でも、取得回数を正しく把握することができる。

- 受信機は、Reply message の受信に失敗して、ContentKey を取得できなかった場合、SAC 再開後に、記憶している TransactionFlag を DRM サーバに送信する。
- DRM サーバは、記憶している TransactionFlag と受信した TransactionFlag が異なることから、最後に送信した Reply message を受信機が受信していない、すなわち受信機が ContentKey を取得できなかったと判断する。
- サービス事業者（DRM サーバを含む）は、受信機が Reply message を受信していないため、当該受信機に送信した ContentKey を取得できなかったことを把握する。

本節では、上記を実現するために必要な TransactionFlag に関する処理の詳細を解説する。

- 障害に備えて受信機と DRM サーバが行う TransactionFlag の記憶処理。
- 障害復旧後に DRM サーバが行う Reply message の受信判断処理。

また、受信機の不揮発性記憶領域が満杯の場合や、DRM サーバでの Reply message の受信判断が不要になった場合などに、受信機と DRM サーバがそれぞれ単独で TransactionFlag を削除する処理についても解説する。

A.2.1 TransactionFlagの記憶処理

本項では、受信機と DRM サーバの不揮発性記憶領域への TransactionFlag の記憶処理の流れと不揮発性記憶領域の記憶状態を解説する。

A.2.1.1TransactionFlag の記憶処理の流れ

受信機と DRM サーバの TransactionFlag の記憶処理の流れを示す。

- 受信機は、TransactionFlag に Te を設定した Response & Request message を送信した後、Request message を送信する際に、Te→To→Te→・・・の順で反転した値を TransactionFlag に設定する。

- DRM サーバは、受信機における取得回数をカウントする ContentKey を Reply message で送信する場合、その送信前に受信機から受信した TransactionFlag を不揮発性記憶領域に記憶して、Reply message の TransactionFlagRecordFlag を「record（01h）」に設定する。
- 受信機は、Reply message の TransactionFlagRecordFlag が「record（01h）」であることから、最後に送信した TransactionFlag を記憶し、Reply message で受信した ContentKey を利用不可の状態で不揮発性記憶領域に記憶する。なお、EXTRACT では取得回数をカウントする ContentKey が送信されないため、TransactionFlagRecordFlag の値によらず、この処理は不要である。
- DRM サーバは、上記の Reply message を送信後に Request message または Command が「Commit」の Encrypted command message を受信し、検証に成功した時、受信機が上記の Reply message を受信したと判断する。
- DRM サーバは、Reply message の受信を判断して次の Reply message または Command が「ACK」の Encrypted command message を送信する時、不揮発性記憶領域の TransactionFlag の削除または更新を行う。
- 受信機は、次の Reply message または Command が「ACK」の Encrypted command message を受信し、検証に成功した時、不揮発性記憶領域の TransactionFlag の削除と ContentKey の利用可能な状態への状態変更を行う。Reply message の TransactionFlagRecordFlag が「record（01h）」の場合、さらに第 3 項目と同等に TransactionFlag と ContentKey の記憶を行う。受信機はさらに、上記で不揮発性記憶領域に記憶した利用不可の ContentKey の状態変更も行う。

A.2.1.2不揮発性記憶領域の記憶状態

不揮発性記憶領域の記憶状態として、不揮発性記憶領域への処理が完了した時の記憶状態と、不揮発性記憶領域への処理が完了する前に突発的な電源断などの障害により SAC が終了した受信機における次回 SAC 開始前の不揮発性記憶領域の記憶状態を、具体的な SAC 処理のシーケンスをもとに示す。

まず、DRMサーバがReply messageを複数回送信するSAC処理のシーケンスを例に、受信機とDRMサーバの不揮発性記憶領域の記憶状態を図A-4に示す。

図A-4のSAC処理のシーケンスは、[MIPTV], 4.1.4.11 項のTransactionFlagに関する処理に規定されている実行条件のパターンを全て含んでいる。

図A-4における受信機とDRMサーバの不揮発性記憶領域への処理を表A-3に示す。

表A-3の④の受信機の不揮発性記憶領域への処理は、[MIPTV], 4.1.4.11.1 項(2)のTransactionFlagの削除処理と[MIPTV], 4.1.4.11.1 項(1)のTransactionFlagの記憶処理を同時に行う、すなわち、更新処理として実行する場合を示す。

図A-4の表記を以下に示す。

- ①から⑧は表A-3に示している不揮発性記憶領域への処理を行うタイミング。
- （ ）の中は、TransactionFlag の値。
- [ ]の中は、ContentKey と TransactionFlagRecordFlag の値。
- K1 から Kn は ContentKey の値。
- 状態 S0 から状態 Sn+1 は、DRM サーバの不揮発性記憶領域の記憶状態。
- 状態C0 から状態Cn+1 は、受信機の不揮発性記憶領域の記憶状態。表A-3の処理で状態が変化しないパラメータは表記を省略し、状態が変化するパラメータのみ表記。
- 状態 S0 から状態 Sn+1 と状態 C0 から状態 Cn+1 の TF は、TransactionFlag を意味する。

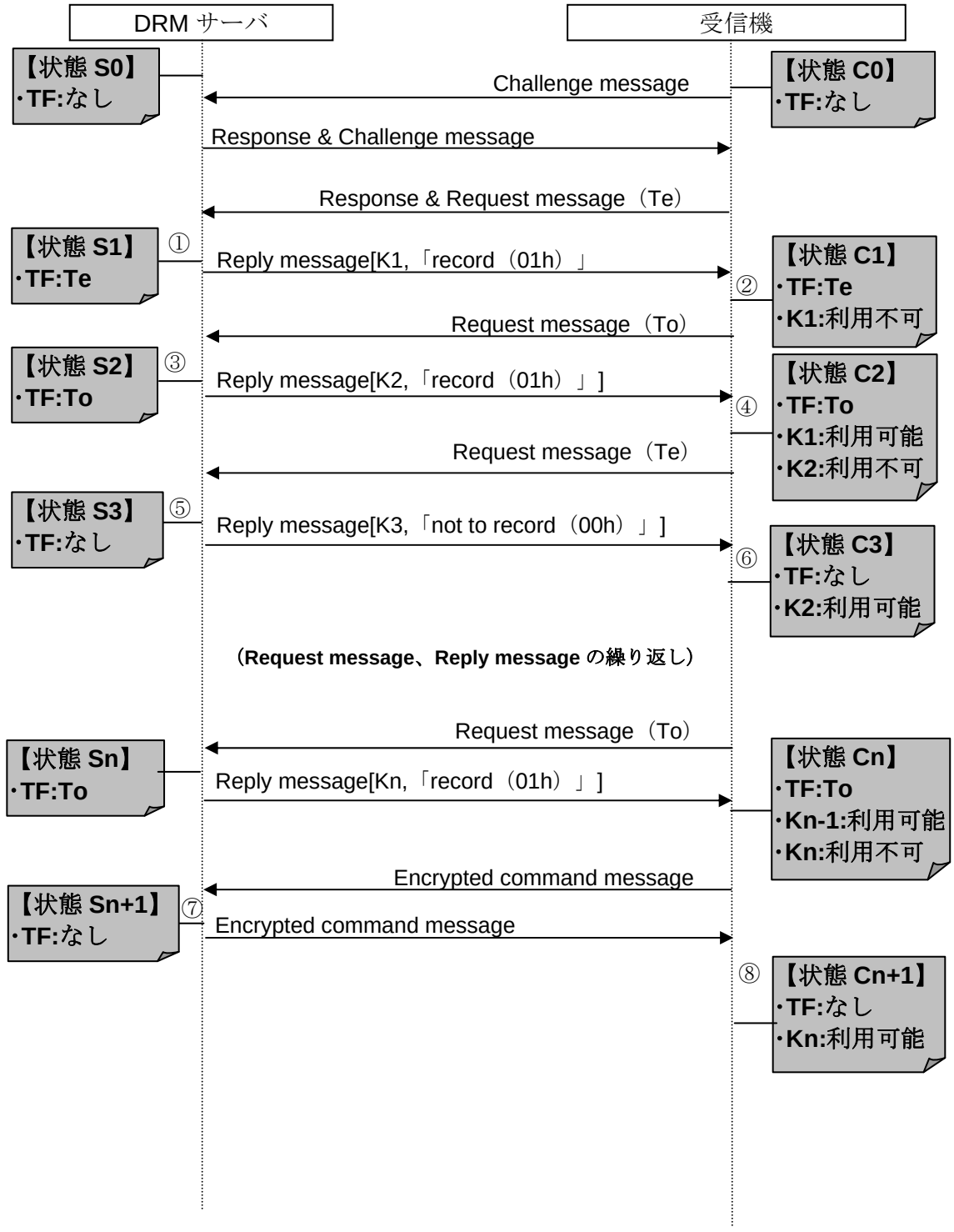


図 A-4　受信機と DRM サーバの不揮発性記憶領域の記憶状態

表 A-3　受信機と DRM サーバの不揮発性記憶領域への処理

図A-4で不揮発性記憶領域への処理を行うタイミング		DRM サーバが送信し受信機が受信するメッセージ	不揮発性記憶領域への処理		
			Ⅰ.受信機と DRM サーバが行う Transaction Flag に関する処理	受信機が行う ContentKey に関する処理	
DRM サーバ	受信機			Ⅱ.記憶処理	Ⅲ.状態変更処理
①	②	Reply message	Te を記憶	K1 を利用不可の状態で記憶	なし
③	④		To に更新	K2 を利用不可の状態で記憶	K1 を利用可能な状態に変更
⑤	⑥		To を削除	なし	K2 を利用可能な状態に変更
⑦	⑧	Encrypted command message			Kn を利用可能な状態に変更

次に、図A-4のSAC処理のシーケンスを例に、表A-3の「不揮発性記憶領域への処理」のいずれかが完了する前に、突発的な電源断などの障害によりSACが終了した場合の、次回SAC開始前の受信機の不揮発性記憶領域の記憶状態を示す。
障害によりSACが終了した受信機の不揮発性記憶領域への処理と記憶状態を表A-4に示す。表A-4の「不揮発性記憶領域への処理で変化したパラメータに対する処理」と表A-3の「不揮発性記憶領域への処理」のⅠからⅢの番号は対応づいている。受信機は、不揮発性記憶領域への処理が完了する前にSACが終了した場合、表A-3の「不揮発性記憶領域への処理」のⅠからⅢのうち完了した処理について、表A-4の「不揮発性記憶領域への処理で変化したパラメータに対する処理」を行い、次回SAC開始までに不揮発性記憶領域を表A-4の「左記の処理を行った後の不揮発性記憶領域の記憶状態」の状態にする。

表 A-4　障害により SAC が終了した受信機の
不揮発性記憶領域への処理と記憶状態

図A-4で受信機が不揮発性記憶領域への処理を行うタイミング	不揮発性記憶領域への処理が完了する前に SAC が終了した場合			
	不揮発性記憶領域への処理で変化したパラメータに対する処理			左記の処理を行った後の不揮発性記憶領域の記憶状態
	表A-3のⅠのみを完了した場合	表A-3のⅡのみを完了した場合	表A-3のⅢのみを完了した場合	
②	Te を削除	K1 を削除	なし	状態 C0
④	Te に戻す	K2 を削除	K1 を利用不可の状態に戻す	状態 C1
⑥	To を復元	なし	K2 を利用不可の状態に戻す	状態 C2
⑧			Kn を利用不可の状態に戻す	状態 Cn

A.2.2 Reply messageの受信判断処理

本項では、[MIPTV], 4.1.4.11.2 項(3)のReply messageの受信判断処理で、Response & Commit messageの受信時にDRMサーバが行うTransactionFlagの一致判定を解説する。

受信機と DRM サーバの不揮発性記憶領域に記憶されている TransactionFlag と受信機における Reply message の受信状態の関係を以下に示す。

- DRM サーバが送信した Reply message を受信機が受信する前に SAC が終了した場合、受信機と DRM サーバが不揮発性記憶領域に記憶している TransactionFlag は異なる。
  - 例：図A-4でContentKeyがK2 のReply messageを送信中にSACが終了した場合の状態S2 と状態C1。
- DRM サーバが送信した Reply message を受信機が受信した後に SAC が終了した場合、受信機と DRM サーバが不揮発性記憶領域に記憶している TransactionFlag は一致する。
  - 例：図A-4でContentKeyがK2 のReply messageを受信後、Request messageを送信中にSACが終了した場合の状態S2 と状態C2。

以上のことから、DRM サーバは、不揮発性記憶領域に記憶している TransactionFlag と Response & Commit message の TransactionFlag が異なる場合、受信機が Reply message を受信していないと判断して、一致する場合は受信機が Reply message を受信していると判断する。

A.2.3 TransactionFlagの単独削除

本項では、受信機と DRM サーバが行う TransactionFlag の単独削除について示す。

A.2.3.1受信機における単独削除

事業者がサービスの終了により DRM サーバの運用を終了すると、受信機は、DRM サーバとの通信による TransactionFlag の削除ができなくなり、不揮発性記憶領域が満杯になる可能性がある。この場合、TransactionFlag の記憶を必要とする新たな ContentKey の取得ができなくなる。
このような場合、受信機は、不揮発性記憶領域の TransactionFlag を単独削除することで、新たな ContentKey を取得することができるようになる。
受信機は、TransactionFlag を単独削除する際に、DRM サーバがサービス終了により運用を終了したことをユーザが確認できるようにメッセージ表示を行う。この時、ユーザが確認する事業者を特定できるように、受信機は、TransactionFlag と対応付けて DRM サーバを運用する事業者名などを記憶することが望ましい。
ユーザは表示されたメッセージを元に判断し、TransactionFlag を削除する。
TransactionFlag を削除すると、対応付けた ContentKey は利用可能な状態に変更できなくなる。

なお、受信機は、DRM サーバの運用の終了ではなく、障害などによる DRM サーバの一時的な停止でも、不揮発性記憶領域が満杯になり ContentKey が取得できなくなる可能性がある。この場合に TransactionFlag を単独削除すると、以下の理由により ContentKey を再取得できなくなることがあるため、削除しないことが望ましい。

- 受信機が Reply message を受信したと DRM サーバが判断した場合は、サービス事業者（DRM サーバを含む）では、ContentKey の取得回数のカウントが終了しているため。
- ContentKey の取得に期限を設ける運用で、その期限を過ぎた場合、DRM サーバが ContentKey の送信を終了するため。

A.2.3.2DRM サーバにおける単独削除

DRM サーバは、受信機における Reply message の受信判断が不要になった場合、Reply message の送信時に記憶した TransactionFlag を単独削除することができる。
Reply message の受信判断が不要になるのは、Reply message で送信した ContentKey の取得回数のカウントが不要になった場合であり、例えば ContentKey の取得に期限を設ける運用で、その期限を過ぎた場合などである。

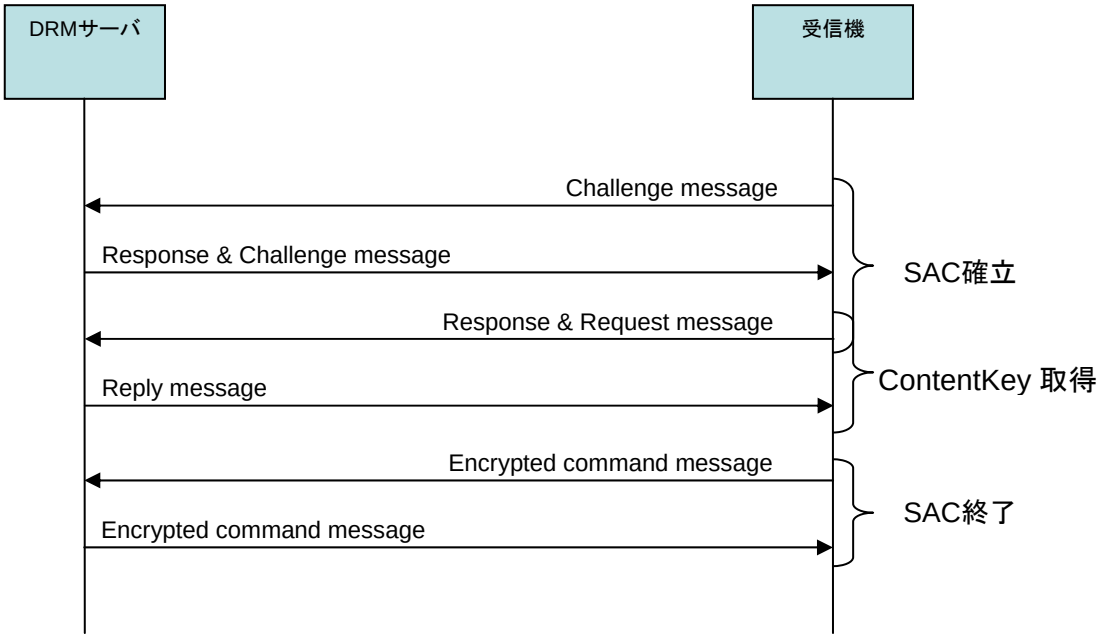
なお、DRM サーバが TransactionFlag を単独削除した後でも、TransactionFlag を記憶している受信機は、DRM サーバとの通信で、TransactionFlag と対応付けて記憶している ContentKey を利用可能な状態に変更し、当該 ContentKey を用いてコンテンツを利用することができる。

A.3 SACとService Protocolを用いたシーケンス

本節では、SAC と Service Protocol を用いたシーケンスとして、再生のための ContentKey 取得と Export のための ContentKey 取得を解説する。

A.3.1 再生のためのContentKey取得

受信機は、暗号化されたコンテンツの再生のために、DRM サーバから ContentKey と RenderingObligation の取得を行う。
取得された ContentKey には NotBefore、NotAfter が設定されているので、受信機は取得済みの ContentKey が有効な間は、コンテンツ再生に際して ContentKey 取得シーケンスを行うことなく、取得済みの ContentKey を使って、コンテンツ再生処理を開始することができる。
図A-5にDRMサーバ・受信機間のContentKey取得シーケンスを示す。



図A-5　再生のための ContentKey 取得シーケンス

ContentKey 取得シーケンスに先立ち、受信機が UsageRuleReference と DRM サーバの URI を取得・保持する。なお、UsageRuleReference や DRM サーバの URI の取得に関する仕様は本書では規定しない。

1. SAC確立：[MIPTV], 4.1 節Secure Authenticated Channel (SAC) Protocolで規定されるプロトコルにより、受信機はDRMサーバとの間で相互認証を行い、SACを確立する。
2. ContentKey取得：[MIPTV], 4.2.1 項Get Permission Protocolで規定されるプロトコルにより、受信機はContentKey取得要求を行い、DRMサーバからContentKeyとそのNotBefore、NotAfter、RenderingObligationを取得する。なお、ContentKey取得のタイミングで、1 つのService Protocolのメッセージで ContentKeyとDatetimeを同時に取得する場合、[MIPTV], 4.2.3 項Packed Message Protocolで規定されるプロトコルを用い、ContentKey取得とは別の Service Protocolのメッセージで Datetimeを取得する場合、[MIPTV], 4.2.2 項Get Trusted Time Protocolで規定されるプロトコルを用いる。
3. SAC終了：ContentKey取得後、[MIPTV], 4.1 節Secure Authenticated Channel (SAC) Protocolで規定されるプロトコルにより、DRMサーバはCommandが「ACK」のEncrypted command messageを送信した後に、受信機はCommandが「ACK」のEncrypted command messageを受信した後に、SACを終了する。

以上の ContentKey 取得シーケンスにより、受信機は ContentKey とその NotBefore、NotAfter、対応する RenderingObligation を取得する。
取得したContentKeyの扱いに関しては、[IPTVCRDL], 4.1.1 項の規定を参照のこと。
なお、再生のために必要なコンテンツのダウンロード処理は、ContentKey の取得シーケンスとは独立であり、受信機は HTTP などで取得する。ダウンロードしたコンテンツは ContentKey を利用して復号再生される。この際、RenderingObligation に従った処理を行う必要がある。また、ContentKey の利用中にその ContentKey が有効期間外となった場合には、4 時間以内に、その利用を停止すること。従って、その場合には、コンテンツの再生処理が停止される。

A.3.2 ExportのためのContentKey取得

受信機は、暗号化されたコンテンツのリムーバブル記録媒体への記録や DTCP 規定に基づく高速デジタルインタフェースへの出力のために、DRM サーバから Export のための ContentKey と ExportInfo の取得を行う。
この ContentKey と ExportInfo の取得は、Export 先の種類ごとに、Export の都度行い、Export 先の種類はリクエストメッセージの ActionParameter として提示される。
Export されるコンテンツのダウンロード処理は、ContentKey の取得処理とは独立であり、受信機は HTTP などで取得する。
図A-6にDRMサーバ・受信機間のContentKey取得シーケンスを示す。

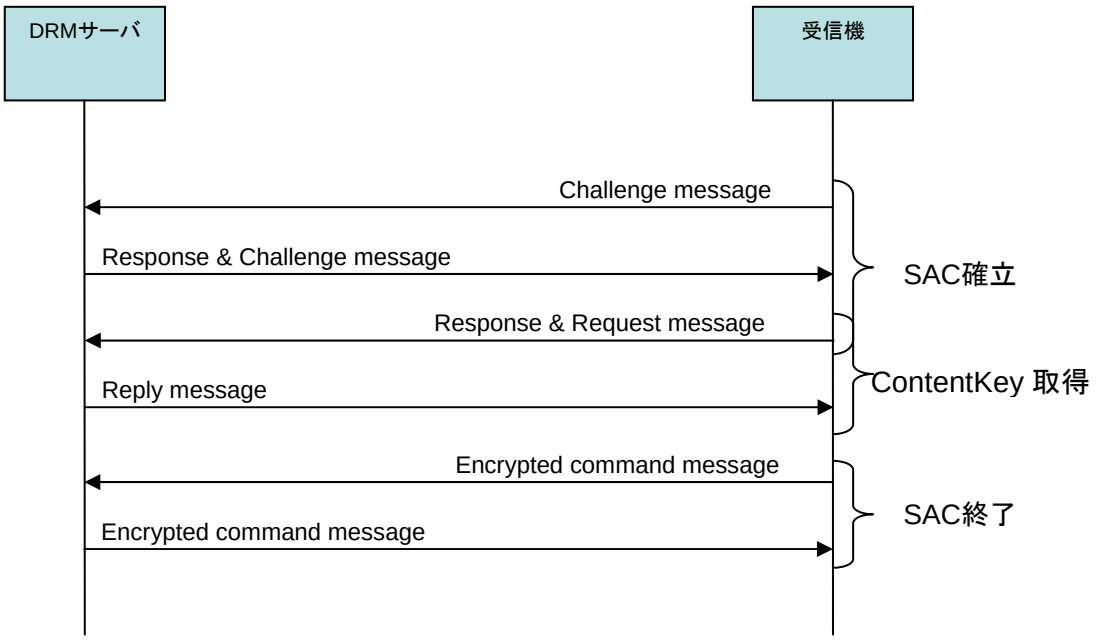


図 A-6　Export のための ContentKey 取得シーケンス

ContentKey 取得シーケンスに先立ち、受信機は UsageRuleReference と DRM サーバの URI を取得・保持する。なお、UsageRuleReference や DRM サーバの URI の取得に関する仕様は本書では規定しない。

1. SAC確立：[MIPTV], 4.1 節Secure Authenticated Channel (SAC) Protocolで規定されるプロトコルにより、受信機はDRMサーバとの間で相互認証を行い、SAC を確立する。
2. ContentKey取得：[MIPTV], 4.2.1 項Get Permission Protocolで規定されるプロトコルにより、受信機はExport先の種類を設定して、ContentKey取得要求を行う。

取得要求が許可されればDRMサーバからContentKeyとExport先のExportInfoを取得する。なお、ContentKey取得のタイミングで、1 つのService Protocolのメッセージで ContentKeyとDatetimeを同時に取得する場合、[MIPTV], 4.2.3 項 Packed Message Protocolで規定されるプロトコルを用い、ContentKey取得とは別のService Protocolのメッセージで Datetimeを取得する場合、[MIPTV], 4.2.2 項Get Trusted Time Protocolで規定されるプロトコルを用いる。

3. SAC終了：ContentKey取得後、[MIPTV], 4.1 節Secure Authenticated Channel (SAC) Protocolで規定されるプロトコルにより、DRMサーバはCommandが「ACK」のEncrypted command messageを送信した後に、受信機はCommandが「ACK」のEncrypted command messageを受信した後に、SACを終了する。

以上の ContentKey 取得シーケンスにより、受信機は ContentKey と ExportInfo を取得する。
取得したContentKeyの扱いに関しては、[IPTVCRDL], 4.1.2 項の規定を参照のこと。

なお、[MIPTV], 4.2.3 項で規定されるPacked Message Protocolを用いて、再生およびExportで用いる情報を一括して取得することができる。この時、Reply messageのTransactionFlagRecordFlagが「record（01h）」でTransactionFlagを不揮発性記憶領域に記憶する場合、Exportに用いるContentKeyを不揮発性記憶領域にTransactionFlagと対応付けて利用不可の状態で記憶する。再生に用いるContentKeyについては、TransactionFlagと対応付けて利用不可の状態で不揮発性記憶領域に記憶せず、利用してもよい。

A.4 メッセージの例

A.4.1 SACのメッセージの例

本項では SAC のメッセージの例を示す。
なお、サイズの大きいパラメータ（SinkCertificate、SourceCertificate など）と演算により生成するパラメータ（SourceEC-DHPhase1Value、Signature など）は、値の記述を省略した。また、以下の表中のハッチング部に記載されている値は暗号化前の値を示す。

A.4.1.1Challenge message

Challenge messageは、[IPTVESVOD], A.3.2.1 項と同等である。

A.4.1.2Response & Challenge message

Response & Challenge messageは、[IPTVESVOD], A.3.2.2 項と同等である。

A.4.1.3Response & Request message

Get Permission Requestを格納したResponse & Request messageの例を表A-5に示す。

表A-5　Response & Request message の例

Byte index	パラメータ名	値：16 進表記
0-3	ProtocolID	49505456（固定）
4-5	ProtocolVersion	0100（固定）
6-13	SenderID	1001000000000000
14-15	PayloadType	0003（固定）
16-19	PayloadSize	000000D8
20-75	SinkEC-DHPhase1Value	（省略）
76-131	Signature	（省略）
132-135	EncryptedDataSize	00000064
136-138	SequenceNumber	000001（固定）
139	TransactionFlag	00（固定）
140-203	Request	A.4.2.1.1項を参照のこと
204-235	MessageDigest	（省略）

965

966 **A.4.1.4Request message**

967 複数のRequestを連続送信する場合のGetPermission Requestを格納した最初の
968 Request messageの例を表A-6に示す。
969

表A-6　Request message の例

Byte index	パラメータ名	値 16 進表記
0-3	ProtocolID	49505456（固定）
4-5	ProtocolVersion	0100（固定）
6-13	SenderID	1001000000000000
14-15	PayloadType	0004（固定）
16-19	PayloadSize	00000068
20-23	EncryptedDataSize	00000064
24-26	SequenceNumber	000003
27	TransactionFlag	01
28-91	Request	A.4.2.1.1項を参照のこと
92-123	MessageDigest	（省略）

970

971 **A.4.1.5Reply message**

972 ActionIDが「EXPORT for Copy with Direct Key Delivery（10h）」のGet Permission
973 Requestに対するGet Permission Replyを格納したReply messageの例を表A-7に示
974 す。
975

表 A-7　Reply message の例

Byte index	パラメータ名	値：16 進表記
0-3	ProtocolID	49505456（固定）
4-5	ProtocolVersion	0100（固定）
6-13	SenderID	0000000000000000（固定値）
14-15	PayloadType	0005（固定）
16-19	PayloadSize	00000042
20-23	EncryptedDataSize	0000003E
24-26	SequenceNumber	000002
27	TransactionFlagRecordFlag	01
28-53	Reply	A.4.2.1.4項を参照のこと
54-85	MessageDigest	（省略）

976

977 **A.4.1.6Plain command message**

978 Plain command messageは、[IPTVESVOD], A.3.2.6 項と同等である。
979

980 **A.4.1.7Encrypted command message**

981 Encrypted command messageは、[IPTVESVOD], A.3.2.7 項と同等である。
982

983 **A.4.1.8Response & Commit message**

984 Response & Commit messageの例を表A-8に示す。
985

表 A-8　Response & Commit message の例

Byte index	パラメータ名	値：16 進表記
0-3	ProtocolID	49505456（固定）
4-5	ProtocolVersion	0100（固定）
6-13	SenderID	1001000000000000
14-15	PayloadType	0008（固定）
16-19	PayloadSize	00000098（固定）
20-75	SinkEC-DHPhase1Value	（省略）
76-131	Signature	（省略）
132-135	EncryptedDataSize	00000024（固定）
136-138	SequenceNumber	000001（固定）
139	TransactionFlag	00
140-171	MessageDigest	（省略）

986

987 **A.4.2 Service Protocolのメッセージの例**

988 本項では[MIPTV], 4.2 節で規定されるService Protocolのメッセージの例を示す。
989

990 **A.4.2.1Get Permission Protocol**

991 本項では、[MIPTV], 4.2.1 項で規定されるGet Permission Protocolのメッセージ例を
992 示す。
993

994 ***A.4.2.1.1 Get Permission Request (EXTRACT)***

995 [MIPTV], 4.2.1.2 項で規定されるActionIDが「EXTRACT with Direct Key Delivery
996 （03h）」のGet Permission Requestメッセージの例を表A-9に示す。
997

表A-9 ActionID が「EXTRACT with Direct Key Delivery（03h）」のGet Permission Request メッセージの例

Byte index	パラメータ名	値：16 進表記
0-1	ProtocolVersion	0100（固定）
2-3	MessageID	0001（固定）
4-15	DeviceInformation	[IPTVESVOD], A.3.3.1.1 項参照
16-31	UsageRuleReference	全て 00
32	ActionID	03（固定）
33	ActionParameter	FF（固定）
34-35	SpecificCRID	0000（固定値）
36	PrivateDataTag	00（固定値）
37-63	PrivateData	全て 00（固定）

998

999 ***A.4.2.1.2 Get Permission Reply (EXTRACT)***

1000 [MIPTV], 4.2.1.3 項で規定されるA.4.2.1.1項のGet Permission Requestに対するGet
1001 Permission Replyメッセージの例を表A-10に示す。
1002

表A-10 表A-9のGet Permission Requestに対する Get Permission Replyメッセージの例

Byte index	パラメータ名	値：16 進表記
0-1	ProtocolVersion	0100（固定）
2-3	MessageID	0002（固定）
4-5	Status	0000
6-21	ContentKey	全て 00
22-23	ExtractInfoSize	000A（固定）
24-27	NotBefore	FFFFFFFF
28-31	NotAfter	4B3CCABD
32-33	RenderingObligation	[IPTVESVOD], A.3.3.1.4 項参照

1003

1004 ***A.4.2.1.3 Get Permission Request (EXPORT)***

1005 [MIPTV], 4.2.1.2 項で規定されるActionIDが「EXPORT for Copy with Direct Key
1006 Delivery（10h）」、ActionParameterが「Export to DTCP（00h）」のGet
1007 Permission Requestメッセージの例を表A-11に示す。

表A-11　ActionID が「EXPORT for Copy with Direct Key Delivery（10h）」のGet Permission Request メッセージの例

Byte index	パラメータ名	値：16 進表記
0-1	ProtocolVersion	0100（固定）
2-3	MessageID	0001（固定）
4-15	DeviceInformation	[IPTVESVOD], A.3.3.1.1 項参照
16-31	UsageRuleReference	全て 00
32	ActionID	10（固定）
33	ActionParameter	00
34-35	SpecificCRID	0000（固定値）
36	PrivateDataTag	00（固定値）
37-63	PrivateData	全て 00（固定）

A.4.2.1.4 Get Permission Reply (EXPORT)

[MIPTV], 4.2.1.3 項で規定されるA.4.2.1.3項のGet Permission Requestに対するGet Permission Replyメッセージの例を表A-12に示す。

表A-12　表A-11のGet Permission Requestに対する Get Permission Replyメッセージの例

Byte index	パラメータ名	値：16 進表記
0-1	ProtocolVersion	0100（固定）
2-3	MessageID	0002（固定）
4-5	Status	0000
6-21	ContentKey	全て 00
22-23	ExportInfoSize	0002
24-25	ExportInfo	3E04

A.4.2.2Get Trusted Time Protocol

本項では、[MIPTV], 4.2.2 項で規定されるGet Trusted Time Protocolのメッセージ例を示す。

A.4.2.2.1 Get TrustedTime Request

Get Trusted Time Requestは、[IPTVESVOD], A.3.3.2.1 項と同等である。

A.4.2.2.2 Get Trusted Time Reply

Get Trusted Time Replyは、[IPTVESVOD], A.3.3.2.2 項と同等である。

A.4.2.3Packed Message Protocol

本項では、[MIPTV], 4.2.3 項で規定されるPacked Message Protocolのメッセージ例を示す。

A.4.2.3.1 Packed Message Request

[MIPTV], 4.2.3.2 項で規定されるPacked Message Requestに格納するRequestがA.4.2.1.1項とA.4.2.2.1項の場合の例を表A-13に示す。

表A-13 Packed Message Request メッセージの例

Byte index	パラメータ名	値：16 進表記
0-1	ProtocolVersion	0100（固定）
2-3	MessageID	0101（固定）
4-5	NumberOfRequestMessageBoxes	0002
6-7	RequestMessageSize	0040
8-71	RequestMessage	A.4.2.1.1項参照
72-73	RequestMessageSize	0004
74-77	RequestMessage	A.4.2.2.1項参照

A.4.2.3.2 Packed Message Reply

[MIPTV], 4.2.3.3 項で規定されるPacked Message ReplyメッセージでA.4.2.3.1項に対して応答する場合の例を表A-14に示す。

表A-14 Packed Message Reply メッセージの例

Byte index	パラメータ名	値：16 進表記
0-1	ProtocolVersion	0100（固定）
2-3	MessageID	0102（固定）
4-5	Status	0000
6-7	NumberOfReplyMessageBoxes	0002
8-9	ReplyMessageSize	0022
10-43	ReplyMessage	A.4.2.1.2項参照
44-45	ReplyMessageSize	000A
46-55	ReplyMessage	A.4.2.2.2項参照