地上デジタルテレビジョン放送 IP 再送信
Marlin IPTV-ES Specific Compliance Rules

Document Version: 1.5
Final

Date: 31 March, 2015

本仕様の内容は予告無しに変更されることがあります。

Contents

1 はじめに

1.1 本書の規定範囲

本書では、地上デジタルテレビジョン放送 IP 再送信において、コンテンツの暗号を復号するための鍵を、以下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、DRM サーバおよび受信機が満たすべき遵守規則に加え、サービス事業者が ECM を送出するにあたって遵守すべき遵守規則を規定する。

- “Marlin Trust Management Document for IPTV-ES Supplement 1: RTDB/J Support”[MTMDSUP] 2 章で規定する RTDB Client Key 及び RTDB Service Key を用いた“Marlin IPTV End-point Service Specification” [MIPTV], 4.1 項で規定される SAC において、[MIPTV], 4.2.1.2 項で規定される ActionID が「EXTRACT with Indirect Key Delivery（02h）」の Get Permission Request
- [MIPTV], 6.1.2 項で規定される ECM

特に断りがない限り、DRM サーバは、サービス向け General Compliance Rules [SRVGCR]に加えて本書の規定を遵守し、受信機は、受信機向け General Compliance Rules [CLTGCR]に加えて本書の規定を遵守すること。

以下に、本書の規定項目を示す。

- コンテンツの出力制御・蓄積装置への蓄積制御・リムーバブル記録媒体への記録制御に関する遵守規則

- 時刻に関する遵守規則
  - DRM サーバにおける時刻
  - 受信機における時刻

- 鍵の利用に関する遵守規則
  - 受信機における WorkKey の利用

- [MIPTV]の規定に関する遵守規則
  - SAC に関する遵守規則
    - ✧ TransactionFlag Management
    - ✧ メッセージパラメータの検証
  - Service Protocol に関する遵守規則
    - ✧ 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

1.2 引用文書

[ARIB-TR-B14]	“ARIB TR-B14”, 3.4 版
[CLTGCR]	“Compliance Rules for Clients Version 2.0: General Section for Audio, Visual and Audiovisual Content”, Marlin Client Agreement Exhibit A
[MIPTV]	“Marlin IPTV End-point Service Specification”, Version 1.0.2

[MTMD]	“Marlin Trust Management Document for IPTV-ES”, Version 2.0
[MTMDSUP]	“Marlin Trust Management Document for IPTV-ES Version 2.0 Supplement 1: RTDB/J Support”, Version 1.0
[RTDB]	地上デジタルテレビジョン放送 IP 再送信運用規定第八編 Version 1.3
[SRVGCR]	“Compliance Rules for Service Providers Version 2.0: General Section for Audio, Visual and Audiovisual Content”, Marlin Service Provider Agreement Exhibit A

112

113 *1.3 用語の定義*

114 本書で用いる用語を以下のように定義する。
115

用語	定義
コンテンツ	マルチキャスト伝送またはユニキャスト伝送され、暗号を復号するための鍵を[MIPTV], 4.2.1.2 項で規定される ActionID が「EXTRACT with Indirect Key Delivery（02h）」の Get Permission Request と [MIPTV], 6.1.2 項で規定される ECM で取得するコンテンツ。
蓄積装置	[MIPTV], 1.4 節で規定される Protected Storage であり、[ARIB-TR-B14], 第八編 第一部 3 章で規定される蓄積機能を有し、[ARIB-TR-B14], 第八編 第一部 6 章のコンテンツの蓄積に関する規定に準拠した受信機が、コンテンツを蓄積するための蓄積装置。
リムーバブル記録媒体	テープ、ディスク等のように、受信機から取り外すことが可能な独立した形態を持ち、かつ、他の再生機能を有する機器においても再生可能な記録媒体。

116
117 本書で用いる用語と[MIPTV]の用語との対応を以下に示す。
118

本書	[MIPTV]
受信機	Marlin IPTV-ES Device
DRM サーバ	Marlin IPTV-ES Server
出力	EXTRACT、または、DTCP への EXPORT
蓄積装置への蓄積	RECORD
リムーバブル記録媒体へのデジタル記録	DTCP 以外への EXPORT

119

120 *1.4 略語*

121 本書では、以下の略語を適用する。
122

略語	正式名称
CRL	Certificate Revocation List
DRL	Device Revocation List

123

2　コンテンツの出力・蓄積装置への蓄積・リムーバブル記録媒体への記録に関する遵守規則

[MIPTV], 6.1.2 項で規定される ECM に設定する RenderingObligation に関するサービス事業者の遵守規則については、[RTDB], 4.1.2 節に従うこととする。
受信機におけるコンテンツの出力制御・蓄積装置への蓄積制御・リムーバブル記録媒体への記録制御に関する遵守規則については、[CLTGCR], 4 章及び 5 章の遵守規則に代わって、[RTDB], 5.1.2, 5.3.2, 5.4～5.9 節に従うこととする。

3 時刻に関する遵守規則

本章では、時刻に関する DRM サーバと受信機の遵守規則を規定する。

3.1 DRM サーバにおける時刻

DRM サーバは、[MIPTV], 4.2.2.3 項で規定される Get Trusted Time Reply の Datetime に設定するため、並びに、[MTMD], 6.2 節で規定される DRL の取得の要否を判断するために、合理的に正確な時刻を保持する必要がある。この目的で、その保持する時刻を、合理的に正確な時刻情報源に対して合理的な頻度で同期しなければならない。

3.2 受信機における時刻

受信機は、[MTMD], 6.1 章で規定される CRL の取得の要否を判断するため、並びに 4.1 節で規定される WorkKey の有効期間を検証するために、合理的に正確な時刻を保持しなければならない。

4 鍵の利用に関する遵守規則

本章では、鍵の利用に関する受信機の遵守規則を規定する。

4.1 受信機における WorkKey の利用

受信機は、コンテンツの暗号を復号する場合に、WorkKey の利用を開始するタイミングで、[MIPTV], 6.1.3 項の規定に従って、その WorkKey が有効期間内であるかを検証すること。有効期間外である場合には、その WorkKey を利用してはならない。

5 SAC に関する遵守規則

本章では IPTV-ES SAC に関する DRM サーバと受信機の遵守規則を規定する。なお、IPTV-ES SAC および DRM サーバの URI に対する署名検証には、[MTMDSUP] 2 章の PKI Trust Hierarchy を用いること。

5.1 TransactionFlag Management

受信機と DRM サーバは、[MIPTV], 4.1.1.1 項における TransactionFlag Management の要否について、ActionID が「EXTRACT with Indirect Key Delivery（02h）」の Get Permission Protocol では TransactionFlag Management は不要とする。

5.2 メッセージパラメータの検証

DRM サーバは、メッセージ受信時に[MIPTV], 4.1.4 項および以下に規定する検証を行うこと。

5.2.1 Challenge message

DRM サーバは、以下に示すように各パラメータの検証を行うこと。

- SinkCertificate
  - SinkCertificate に含まれる証明書が[MTMDSUP], 2 章の RTDB Peer Application Interaction CA Cert と RTDB Client Key であり、RTDB Peer Application Interaction CA Cert の Subject の value が以下の値以外の場合、検証失敗とし、受信機に通知する Status は「Authentication error（8003h）」とする。
    - “urn:marlin:clientca:rtdb-pdc-client-ca.....”

6 Service Protocol に関する遵守規則

本章では、IPTV-ES Service Protocol に関する DRM サーバと受信機の遵守規則を規定する。

6.1 Get Permission Protocol

本節では、[MIPTV], 4.2 節で規定される Get Permission Protocol メッセージパラメータ設定とその検証に関する DRM サーバと受信機の遵守規則を規定する。

6.1.1 メッセージパラメータの設定

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

6.1.1.1 Get Permission Request parameters

- ActionID
  - ActionID には、「EXTRACT with Indirect Key Delivery（02h）」を設定する。
- SpecificCRID
  - SpecificCRID には、0001h を設定する。
- PrivateDataTag
  - PrivateDataTag には、00h を設定する。

6.1.2 メッセージパラメータの検証

DRM サーバは、メッセージ受信時に[MIPTV], 4.2.4.1 項および以下に規定する検証を行うこと。

6.1.2.1 Get Permission Request parameters

DRM サーバは、以下に示すとおり、Get Permission Request のメッセージパラメータを検証すること。

- SpecificCRID
  - SpecifiCRID の値が 0001h でない場合には検証失敗とし、Get Permission Reply parameter の Status を「Error other than the below（8001h）」とする。
- PrivateDataTag
  - PrivateDataTag の値が 00h でない場合には検証失敗とし、Get Permission Reply parameter の Status を「Error other than the below（8001h）」とする。