

1
2
3
4
5
6
7
8
9
10
11
12

13 **Marlin IPTV-ES 運用仕様**
14 **VOD 編**

15
16 Document Version: 1.4
17 Final

18
19 Date: 25 April, 2012

20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43

44 **Copyright © 2007-2012 ALL RIGHTS RESERVED**
45 ソニー株式会社
46 パナソニック株式会社

47
48
49
50

本仕様の内容は予告無しに変更されることがあります。

51 目次

52

53 1 はじめに..... 4

54 1.1 本書の規定範囲 4

55 1.2 引用文書 4

56 1.3 用語の定義 5

57 1.4 略語 5

58 1.5 バイトオーダー 5

59 1.6 ビットオーダー 5

60 2 SAC に関する規定 6

61 2.1 メッセージパラメータ 6

62 2.2 SAC タイムアウト 6

63 2.3 1つの TCP Connection を利用可能な SAC セッション 6

64 2.4 Response & Commit message 6

65 3 Service Protocol に関する規定 7

66 3.1 Get Permission Protocol 7

67 3.1.1 メッセージパラメータの設定 7

68 3.1.1.1 Get Permission Request parameters 7

69 3.1.1.2 Get Permission Reply parameters 7

70 3.1.2 メッセージパラメータの検証 7

71 3.1.2.1 Get Permission Request parameters 7

72 3.1.2.2 Get Permission Reply parameters 7

73 3.2 Get Trusted Time Protocol 8

74 3.3 Packed Message Protocol 8

75 3.3.1 メッセージパラメータの設定 8

76 3.3.1.1 Packed Message Request parameters 8

77 3.3.1.2 Packed Message Reply parameters 8

78 3.3.2 メッセージパラメータの検証 8

79 3.3.2.1 Packed Message Request parameters 8

80 3.3.2.2 Packed Message Reply parameters 9

81 4 ネットワーク通信プロトコル (HTTP) に関する規定 10

82 4.1 HTTP による SAC のメッセージの伝送 10

83 4.2 HTTP ヘッダ 10

84 4.2.1 サイズ 10

85 4.2.2 メソッド 10

86 4.2.3 リクエストヘッダ 10

87 4.2.4 レスポンスヘッダ 11

88 4.3 メッセージ処理中の受信機から HTTP のリクエストを受信した時の
89 DRM サーバの処理 11

90 A Appendix (Informative) 12

91 A.1 SAC 処理の例 12

92 A.1.1 状態遷移 12

93 A.1.2 メッセージ処理 15

94 (1) Challenge message 送信時の受信機処理 16

95 (2) Challenge message 受信時の DRM サーバ処理 16

96 (3) Response & Challenge message 送信時の DRM サーバ処理 16

97 (4) Response & Challenge message 受信時の受信機処理 16

98 (5) Response & Request message 送信時の受信機処理 16

99 (6) Response & Request message 受信時の DRM サーバ処理 17

100 (7) Reply message 送信時の DRM サーバ処理 17

101 (8) Reply message 受信時の受信機処理 17

102 (9) Request message 送信時の受信機処理 17

103 (10) Request message 受信時の DRM サーバ処理 18

| | | | |
|-----|-----------|--|----|
| 104 | (11) | Encrypted command message 送信時の受信機処理..... | 18 |
| 105 | (12) | Encrypted command message 受信時の DRM サーバ処理..... | 18 |
| 106 | (13) | Command が「ACK」の Encrypted command message 送信時の | |
| 107 | | DRM サーバ処理..... | 19 |
| 108 | (14) | Encrypted command message 受信時の受信機処理..... | 19 |
| 109 | (15) | Plain command message 受信時の受信機処理..... | 19 |
| 110 | (16) | Plain command message 送信時の DRM サーバ処理..... | 19 |
| 111 | (17) | Command が「ERROR」の Encrypted command message | |
| 112 | | 送信時の DRM サーバ処理 | 19 |
| 113 | A.2 | SAC と Service Protocol を用いたシーケンス | 20 |
| 114 | A.3 | メッセージの例 | 21 |
| 115 | A.3.1 | HTTP のメッセージの例..... | 21 |
| 116 | A.3.2 | SAC のメッセージの例..... | 21 |
| 117 | A.3.2.1 | Challenge message | 22 |
| 118 | A.3.2.2 | Response & Challenge message..... | 22 |
| 119 | A.3.2.3 | Response & Request message..... | 22 |
| 120 | A.3.2.4 | Request message | 23 |
| 121 | A.3.2.5 | Reply message..... | 23 |
| 122 | A.3.2.6 | Plain command message..... | 24 |
| 123 | A.3.2.7 | Encrypted command message..... | 24 |
| 124 | A.3.3 | Service Protocol のメッセージの例..... | 25 |
| 125 | A.3.3.1 | Get Permission Protocol | 25 |
| 126 | A.3.3.1.1 | DeviceInformation | 25 |
| 127 | A.3.3.1.2 | Get Permission Request..... | 26 |
| 128 | A.3.3.1.3 | Get Permission Reply..... | 26 |
| 129 | A.3.3.1.4 | Output Control Information | 26 |
| 130 | A.3.3.2 | Get Trusted Time Protocol | 27 |
| 131 | A.3.3.2.1 | Get TrustedTime Request | 27 |
| 132 | A.3.3.2.2 | Get Trusted Time Reply | 27 |
| 133 | A.3.3.3 | Packed Message Protocol | 27 |
| 134 | A.3.3.3.1 | Packed Message Request..... | 28 |
| 135 | A.3.3.3.2 | Packed Message Reply..... | 28 |
| 136 | | | |

137 **1 はじめに**

138 “Marlin IPTV End-point Service Specification” [MIPTV]では、暗号化されたコンテ
139 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
140 している。Simple Key Delivery 方式は、様々なサービスへの適用が考えられるが、
141 最も典型的なコンテンツ配信形態としては、コンテンツがストリーム伝送される
142 VOD サービスが想定されるため、本編を VOD 編と呼ぶこととする。
143

144 **1.1 本書の規定範囲**

145 本書では、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
146 ActionID が「EXTRACT with Simple Key Delivery (01h)」の Get Permission
147 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
148 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する。
149 本書は、“Marlin IPTV-ES/J Specific Compliance Rules VOD 編” [IPTVCRVOD]に
150 準拠する受信機および DRM サーバに適用する。
151

152 以下に本書の規定項目を示す。

- 153
- 154 ● [MIPTV]に対する詳細規定項目
 - 155 ➤ SAC に関する規定 ([MIPTV], 4.1 節 Secure Authenticated Channel (SAC)
 - 156 Protocol)
 - 157 ☆ メッセージパラメータ
 - 158 ☆ SAC タイムアウト
 - 159 ☆ 1つの TCP Connection を利用可能な SAC セッション
 - 160 ☆ Response & Commit message
 - 161 ➤ Service Protocol に関する規定 ([MIPTV], 4.2 節 Marlin IPTV-ES Service
 - 162 Protocols over SAC に関する規定)
 - 163 ☆ メッセージパラメータの設定
 - 164 ☆ メッセージパラメータの検証
- 165 ● [MIPTV]に対する追加規定項目
 - 166 ➤ ネットワーク通信プロトコル (HTTP) に関する規定
 - 167 ☆ HTTP による SAC のメッセージの伝送
 - 168 ☆ HTTP ヘッダ
- 169

170 **1.2 引用文書**

| | |
|-------------|---|
| [IPTVCRVOD] | “Marlin IPTV-ES/J Specific Compliance Rules VOD 編” , Version 1.4 |
| [MIPTV] | “Marlin IPTV End-point Service Specification” , Version 1.0.2 |
| [RFC2109] | HTTP State Management Mechanism |
| [RFC2616] | Hypertext Transfer Protocol – HTTP/1.1 |

171
172
173
174

175 **1.3 用語の定義**

176 本書で用いる用語を以下のように定義する。

177

| 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 Simple Key Delivery (01h)」の Get Permission Request で取得するコンテンツ。 |

178

179 本書で用いる用語と[MIPTV]の用語との対応を以下に示す。

180

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

181

182 **1.4 略語**

183 本書で用いる略語を以下に示す。

184

| 略語 | 正式名称 |
|-----|----------------------|
| MSB | Most Significant Bit |

185

186 **1.5 バイトオーダー**

187 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
188 ある。

189

190 **1.6 ビットオーダー**

191 本書で定義されるプロトコルのビットオーダーは“MSB First”である。

192

193 2 SAC に関する規定

194 本章では IPTV-ES SAC の運用を規定する。

195

196 2.1 メッセージパラメータ

197 [MIPTV], 4.1.3 項で規定されるプロトコルのメッセージパラメータの運用を以下に示
198 す。

199

200 ● SenderID

201 ․ 受信機は、DRM サーバの SenderID としていかなる値を受信しても、
202 「NULL value (00h)」を受信したものとして処理する。

203 ● SequenceNumber

204 ․ 受信機は Request message 送信時に SequenceNumber が $(2^{24}-3)$ 以
205 上になる場合には、[MIPTV], 4.1.4.10.1 項に従い、SAC を終了する。

206 ● TransactionFlag

207 ․ DRM サーバと受信機は、Encrypted command message の TransactionFlag
208 を検証しない。

209 ● Status

210 ․ DRM サーバは、Plain command message の Status として「Certificate
211 issuer mismatch (8005h)」を運用しない。

212 ● SinkCertificate

213 ․ 受信機が送信する SinkCertificate は certificate chain を含む PKIPath とする。

214 ● SourceCertificate

215 ․ DRM サーバが送信する SourceCertificate は certificate chain を含む
216 PKIPath とする。

217

218 2.2 SAC タイムアウト

219 DRM サーバは、メッセージ送信後に 10 秒間はタイムアウトせずにメッセージ受信
220 待ちを行う。

221 DRM サーバはタイムアウト後に[MIPTV], 4.1.4.10.2 項に従い SAC を終了する。

222

223 2.3 1 つの TCP Connection を利用可能な SAC セッション

224 1 つの TCP Connection を利用可能な SAC セッションは 1 つとする。従って、受信
225 機と DRM サーバは、SAC を終了した時、速やかに TCP Connection を切断する。

226

227 2.4 Response & Commit message

228 Response & Commit message は運用しない。

229

230 **3 Service Protocol に関する規定**

231 本章では IPTV-ES Service Protocol の運用を規定する。
232 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
233 の DRM サーバの URI を受信機が取得する方法については、本書では規定しない。
234

235 **3.1 Get Permission Protocol**

236 [MIPTV], 4.2 節で規定される Get Permission Protocol は ContentKey 取得に用いる。
237 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
238 定する。
239

240 **3.1.1 メッセージパラメータの設定**

241 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。
242

243 **3.1.1.1 Get Permission Request parameters**

244 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
245 メッセージパラメータを設定する。
246

- 247 ● UsageRuleReference
- 248 ‣ 事前に取得した UsageRuleReference を設定する。
- 249

250 **3.1.1.2 Get Permission Reply parameters**

251 DRM サーバは、[MIPTV], 4.2.1.3 項、4.2.1.4 項および以下の規定に従い、Get
252 Permission Reply のメッセージパラメータを設定する。
253

- 254 ● Status
- 255 ‣ 本書 3.1.2.1 項を参照のこと。

256 **3.1.2 メッセージパラメータの検証**

257 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
258 メータを検証する。
259

260 **3.1.2.1 Get Permission Request parameters**

261 DRM サーバは、[MIPTV], 4.2.4.1 項および以下の規定に従い、Get Permission
262 Request のメッセージパラメータを検証する。
263

- 264 ● ActionID
- 265 ‣ ActionID が以下に示す値の場合には、検証失敗としない。
- 266 ‣ EXTRACT with Simple Key Delivery (01h)
- 267

268 **3.1.2.2 Get Permission Reply parameters**

269 受信機は、[MIPTV], 4.2.4.2 および 4.2.4.3 項の規定に従い、Get Permission Reply
270 のメッセージパラメータを検証する。

271 **3.2 Get Trusted Time Protocol**

272 [MIPTV], 4.2.2 項で規定される Get Trusted Time Protocol は Datetime 取得に用いる。
273 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
274 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
275 Trusted Time Reply のメッセージパラメータを検証する。
276 DRM サーバは、[MIPTV], 4.2.4.9 項の規定に従い、Get Trusted Time Request のメ
277 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
278 に従い、Get Trusted Time Reply のメッセージパラメータを設定する。
279

280 **3.3 Packed Message Protocol**

281 [MIPTV], 4.2.3 項で規定される Packed Message は ContentKey と Datetime の同時
282 取得に用いる。
283 本節では、メッセージパラメータとメッセージパラメータの検証について規定する。
284

285 **3.3.1 メッセージパラメータの設定**

286 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。
287

288 **3.3.1.1 Packed Message Request parameters**

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

- 291
- 292 ● RequestMessageBoxList
- 293 > 表 3-1 に示す順番にメッセージを格納する。
- 294

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

| 1 番目の RequestMessage | 2 番目の RequestMessage |
|--|--------------------------|
| Get Permission Request (EXTRACT with Simple Key Delivery (01h)) | Get Trusted Time Request |

295

296 **3.3.1.2 Packed Message Reply parameters**

297 DRM サーバは、[MIPTV], 4.2.3.3 項の規定に従い、Packed Message Reply のメッセ
298 ージパラメータを設定する。
299

300 **3.3.2 メッセージパラメータの検証**

301 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
302 ータを検証する。
303

304 **3.3.2.1 Packed Message Request parameters**

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

- 307 ● RequestMessageBoxList
- 308 ➤ RequestMessageBoxList に ActionID が「EXTRACT with Simple Key
- 309 Delivery (01h)」の Get Permission Request の RequestMessage が 1 以上
- 310 格納されている場合、かつ、RequestMessageBoxList に格納された
- 311 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
- 312 証失敗とし、Packed Message Reply Parameter の Status を「Message
- 313 format error (8009h)」とする。
- 314

315 3.3.2.2 Packed Message Reply parameters

- 316 受信機は、[MIPTV], 4.2.4.12 項の規定に従い、Packed Message Reply のメッセー
- 317 ジパラメータを検証する。
- 318

319 4 ネットワーク通信プロトコル (HTTP) に関する規定

320 本章では、SAC のメッセージの伝送に用いるネットワーク通信プロトコル
321 (HTTP) の運用を規定する。

322 ネットワーク通信プロトコルは、[RFC2616]で規定される HTTP/1.1 および
323 [RFC2109]で規定される Cookie に準拠し、以下に示す運用とする。Cookie は SAC
324 のセッションを識別するために用いる。なお、Cookie と Set-Cookie における
325 attribute のうち、設定および解釈を必須とするのは NAME のみとする。
326

327 4.1 HTTP による SAC のメッセージの伝送

328 HTTP メッセージには SAC のメッセージを 1 個のみ格納して送信する。
329

330 4.2 HTTP ヘッダ

331 本節では、必須となる HTTP ヘッダについて規定する。
332 以下に示す HTTP ヘッダ以外は実装依存であり、受信しても解釈しなくてよい。
333

334 4.2.1 サイズ

335 受信機と DRM サーバは、以下に示す規定に従う。
336 なお、本項におけるヘッダとは、HTTP ヘッダを含む HTTP メッセージにおける
337 start-line から空行までを示す。
338

- 339 ● ヘッダ 1 行のサイズ
 - 340 ▶ 受信機と DRM サーバは、ヘッダ 1 行 (CR+LF を含む) のサイズの上限は
 - 341 256byte とし、それを超える場合は、複数行に分割する。
 - 342 ▶ 受信機と DRM サーバは、1 行が 256byte を超えるヘッダを含むメッセージ
 - 343 は受信できなくてもよい。
- 344 ● ヘッダ全体のサイズ
 - 345 ▶ 受信機と DRM サーバは、ヘッダ全体のサイズが 4096byte を超えるメッセ
 - 346 ージを受信できなくてもよい。但し、プロキシにより 1Kbyte 程度のヘッダ
 - 347 が付加されても受信できるように、5Kbyte 程度のヘッダは受信できるよう
 - 348 受信機の実装は考慮されるべきである。
 - 349 ▶ DRM サーバは、送信するレスポンスヘッダ全体のサイズが 4096byte を超
 - 350 えないようにすべきである。但し、受信したリクエストヘッダに表 4-1 に記
 - 351 載されている以外のヘッダ項目が設定されている場合は、送信するレスポ
 - 352 ンスヘッダ全体のサイズが 4096byte を超えてもよい。
353

354 4.2.2 メソッド

355 受信機は、メソッドとして POST のみ運用する。
356

357 4.2.3 リクエストヘッダ

358 DRM サーバは、リクエストヘッダとして表 4-1 に記載されたもののみ解釈を必須と
359 する。受信機は、表 4-1 の運用に従う。

表 4-1 解釈を必須とする HTTP リクエストヘッダ

| ヘッダ | | 運用 |
|---------|----------------|--|
| Request | Cookie | 受信機は、SAC を終了する場合に Cookie を削除する。 受信機は、Challenge message 以外を送信する場合は Set-Cookie で指定された Cookie をつけて、Challenge message 送信時には Cookie をつけない。 |
| | Host | |
| General | Connection | Close のみ運用し、受信機のリクエストヘッダの設定処理において、HTTP のリクエストを送信する際に HTTP のレスポンス受信後に TCP connection を切断することが確定している場合には必ず用いる。 |
| Entity | Content-Length | |
| | Content-Type | Application/octet-stream のみ運用する。 |

360

361 **4.2.4 レスポンスヘッダ**

362 受信機は、レスポンスヘッダとして表 4-2 に記載されたもののみ解釈を必須とする。

363 DRM サーバは表 4-2 の運用に従う。

364 なお、DRM サーバは HTTP のリクエストが正常である場合はステータスコードとし

365 て「200 OK」のみを送信する。受信機は、ステータスコードとして「200 OK」以

366 外はエラーとする。なお、HTTP がエラーの場合でも、SAC は終了しなくてよい。

367

表 4-2 解釈を必須とする HTTP レスポンスヘッダ

| ヘッダ | | 運用 |
|----------|----------------|---|
| Response | Set-Cookie | Set-Cookie の値は SAC のセッションを識別可能な情報を格納する。 Cookie の最大数は 1 個とする。 Set-Cookie は複数行に分割しない。 |
| General | Cache-Control | No-cache のみ運用する。 |
| | Connection | Close のみ運用し、TCP connection 切断時には必ず用いる。 |
| Entity | Content-Length | |
| | Content-Type | Application/octet-stream のみ運用する。 |

368

369 **4.3 メッセージ処理中の受信機から HTTP のリクエストを受信し**
370 **た時の DRM サーバの処理**

371 受信したメッセージ処理中に、メッセージを送信した受信機から HTTP のリクエ

372 トを受信した場合、DRM サーバは [MIPTV], 4.1 節に規定する SAC の処理は行わず

373 に、ステータスコードが「200 OK」以外の HTTP レスポンスを送信する。

374

375 **A Appendix (Informative)**

376 **A.1 SAC 処理の例**

377 **A.1.1 状態遷移**

378 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
379 に示す。

380 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。
381 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 “-” で示す。なお、本
382 書に規定されていないが、表 A-1 に受信機の状態遷移を記述した。

383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423

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 |
| | | | | 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 ③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 |
| | 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 した場合は 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 した場合は 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 した場合は 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 した場合は 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 |
| | 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 |
| | 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 |
| | [MIPTV], 4.1.4.1 項 の Message header 検 証に失敗 (Payload Type 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 |
| 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 |

424
425
426
427
428
429

表 A-2 DRM サーバの状態遷移表

| | | DRM サーバの状態 | | |
|-------------|---|--|--|---|
| | | ⑦SAC 開始前のメッセージ受信待ち | ④Response & Challenge message 送信後のメッセージ受信待ち | ⑤Reply 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 <ul style="list-style-type: none"> メッセージ検証に成功した場合は④に移る メッセージ検証に失敗した場合は⑦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。 <ul style="list-style-type: none"> メッセージ検証に成功した場合は④に移る メッセージ検証に失敗した場合は⑦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。 <ul style="list-style-type: none"> メッセージ検証に成功した場合は④に移る メッセージ検証に失敗した場合は⑦に移る |
| | Response & Request message 受信 | ⑦に移る | A.1.2 項(6)の処理を実行する <ul style="list-style-type: none"> メッセージ検証に成功した場合は⑤に移る メッセージ検証に失敗した場合は⑦に移る | ⑦に移る |
| | Request message 受信 | ⑦に移る | ⑦に移る | A.1.2 項(10)の処理を実行する <ul style="list-style-type: none"> メッセージ検証に成功した場合は⑦に移る メッセージ検証に失敗した場合は⑦に移る |
| | Encrypted command message 受信 | ⑦に移る | ⑦に移る | A.1.2 項(12)の処理を実行して、⑦に移る |
| | [MIPTV], 4.1.4.1 項の Message header 検証に失敗 (Payload Type が上記のメッセージの場合を除く) | ⑦に移る | ⑦に移る | ⑦に移る |
| | SAC タイムアウト | — | ⑦に移る | ⑦に移る |

430

431

432 **A.1.2 メッセージ処理**

433 本項では、メッセージ送受信時に行うメッセージ処理を示す。
 434 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 と図 A-2 に示す。
 435 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
 436 いて説明する。

437
 438
 439
 440
 441
 442
 443
 444
 445
 446
 447
 448
 449
 450
 451
 452
 453
 454

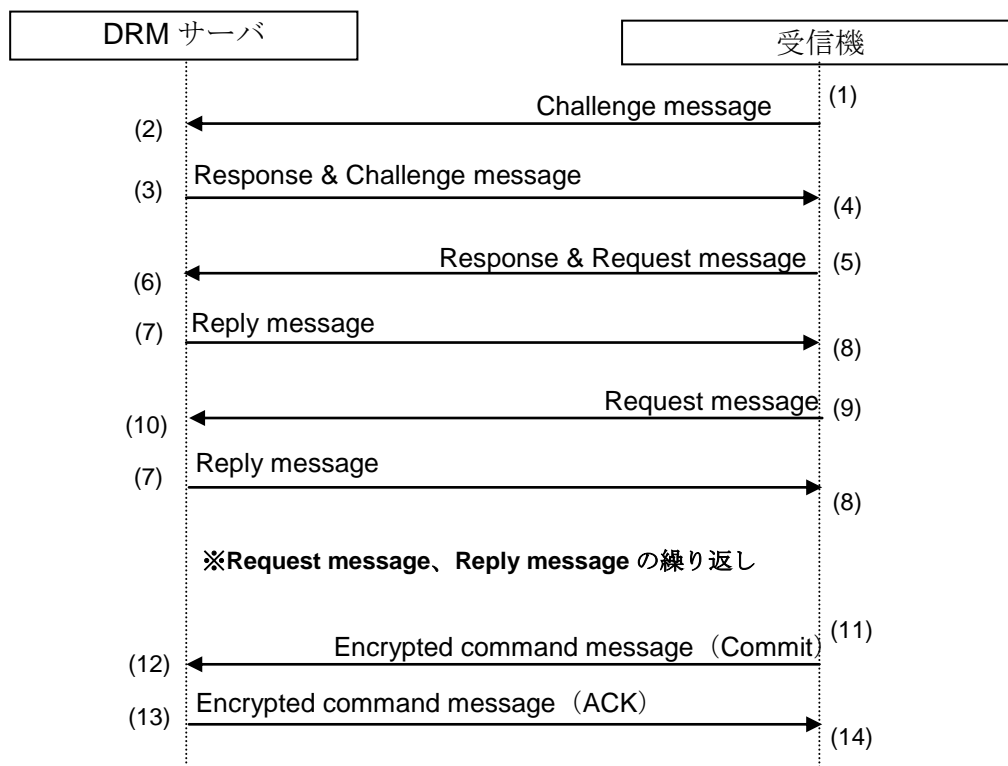


図 A-1 基本シーケンス (複数の Request を連続送信する場合)

455
 456
 457
 458
 459
 460
 461
 462
 463
 464
 465
 466
 467

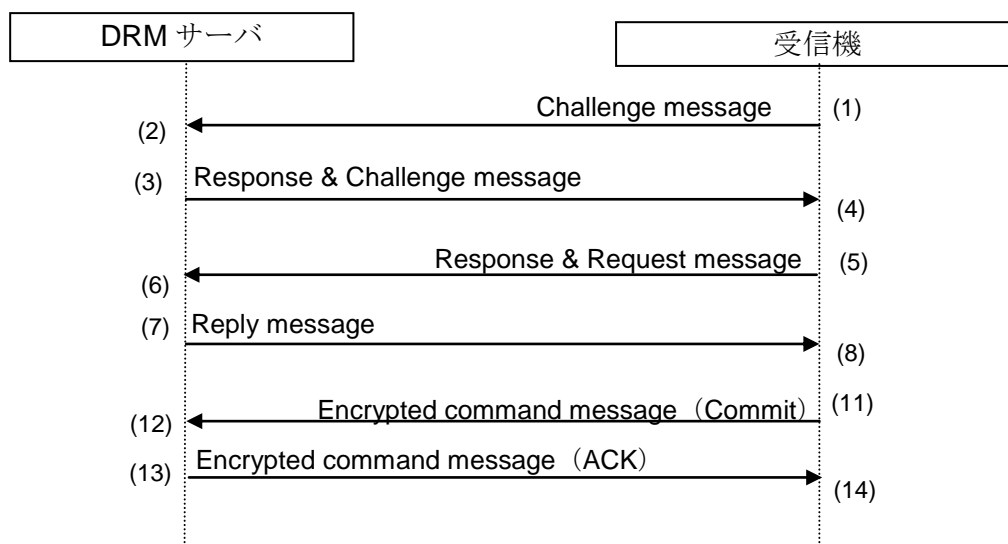


図 A-2 基本シーケンス (一つの Request のみ送信する場合)

468

- 469 (1) **Challenge message 送信時の受信機処理**
- 470 > Challenge message を作成する。
- 471 > DRM サーバに Challenge message を送信する。
- 472 > Challenge message 送信後のメッセージ受信待ちの状態に移る。
- 473
- 474 (2) **Challenge message 受信時の DRM サーバ処理**
- 475 > [MIPTV], 4.1.4.2 項の規定に従い、Challenge message の検証を行う。
- 476 ✧ 検証が成功した場合、(3)Response & Challenge message 送信時の
- 477 DRM サーバ処理を実行する。
- 478 ✧ 検証が失敗した場合、(16)Plain command message 送信時の DRM サー
- 479 バ処理を実行する。
- 480
- 481 (3) **Response & Challenge message 送信時の DRM サーバ処理**
- 482 > Response & Challenge message を作成する。Response & Challenge
- 483 message のメッセージパラメータに関する処理を以下に示す。
- 484 ✧ Signature : SinkRandomNumber と SourceEC-DHPhase1Value に対し
- 485 て生成する。
- 486 > 受信機にResponse & Challenge messageを送信する。
- 487 > Response & Challenge message送信後のメッセージ受信待ちの状態に移る。
- 488
- 489 (4) **Response & Challenge message 受信時の受信機処理**
- 490 > [MIPTV], 4.1.4.3項の規定に従い、Response & Challenge messageの検証を
- 491 行う。
- 492 ✧ 検証が成功した場合、(5)Response & Request message 送信時の受信
- 493 機処理を実行する。
- 494 ✧ 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。
- 495
- 496 (5) **Response & Request message 送信時の受信機処理**
- 497 > セッション鍵を生成する。
- 498 > Response & Request message を作成する。SequenceNumber、
- 499 TransactionFlag、Request、MessageDigest は生成したセッション鍵で暗
- 500 号化する。Response & Request message のメッセージパラメータに関する
- 501 処理を以下に示す。
- 502 ✧ Signature : SourceRandomNumber と SinkEC-DHPhase1Value に対し
- 503 て生成する。
- 504 ✧ SequenceNumber : 1 を Response & Request message に設定し、保
- 505 持する。
- 506 ✧ TransactionFlag : 「even (00h) 」を Response & Request message
- 507 に設定し、保持する。
- 508 ✧ Request : Service Protocol のメッセージを設定する。
- 509 ✧ MessageDigest : 暗号化前の MessageDigest を除く Response &
- 510 Request message のパラメータから生成する。
- 511 > Response & Request message 作成後に保持している SequenceNumber を
- 512 1 増加する。
- 513 > Response & Request messageをDRMサーバに送信する。

514 ➤ Response & Request message送信後のメッセージ受信待ちの状態に移る。
515

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

517 ➤ [MIPTV], 4.1.4.4 項の規定に従い、Response & Request message の検証を
518 行い、セッション鍵を生成する。
519 ✧ 検証が成功した場合、以下の処理を行い、(7)Reply message 送信時の
520 DRM サーバ処理を実行する。
521 ● SequenceNumber として、[MIPTV], 4.1.4.4 項で SequenceNumber の
522 確認に用いた値よりも 1 大きい値である 2 を保持する。
523 ● Response & Request message の TransactionFlag を保持する。
524 ● Response & Request message から Service Protocol のメッセージを
525 抽出する。
526 ✧ 検証が失敗した場合、(16)Plain command message 送信時の DRM サー
527 バ処理を実行する。
528

529 **(7) Reply message 送信時の DRM サーバ処理**

530 ➤ Reply message を作成する。SequenceNumber、
531 TransactionFlagRecordFlag、Reply、MessageDigest はセッション鍵で暗
532 号化する。Reply message のメッセージパラメータに関する処理を以下に
533 示す。
534 ✧ SequenceNumber : 保持している SequenceNumber を用いる。
535 ✧ TransactionFlagRecordFlag : 00h を設定する。
536 ✧ Reply : Service Protocol のメッセージを設定する。
537 ✧ MessageDigest : 暗号化前の MessageDigest を除く Reply message の
538 パラメータから生成する。
539 ➤ Reply message 作成後に保持している SequenceNumber を 1 増加する。
540 ➤ Reply messageを受信機に送信する。
541 ➤ Reply message送信後のメッセージ受信待ちの状態に移る。
542

543 **(8) Reply message 受信時の受信機処理**

544 ➤ [MIPTV], 4.1.4.6 項の規定に従い、Reply message の検証を行う。
545 ✧ 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
546 合は(9)の Request message 送信時の受信機処理を実行し、送信する
547 Request がない場合は(11)Encrypted command message 送信時の受信
548 機処理を実行する。
549 ● 保持している SequenceNumber を 1 増加する。
550 ● TransactionFlag の反転と保持を行う。現在、保持している
551 TransactionFlag が even (00h) の場合は「odd (01h)」を、odd
552 (01h) の場合は「even (00h)」を保持する。
553 ● Reply message から Service Protocol のメッセージを抽出する。
554 ✧ 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。
555

556 **(9) Request message 送信時の受信機処理**

557 ➤ Request message を作成する。SequenceNumber、TransactionFlag、
558 Request、MessageDigest はセッション鍵で暗号化する。Request message
559 のメッセージパラメータに関する処理を以下に示す。

- 560 ✧ SequenceNumber : 保持している SequenceNumber を用いる。
- 561 ✧ TransactionFlag : 保持している TransactionFlag を用いる。
- 562 ✧ Request : Service Protocol のメッセージを設定する。
- 563 ✧ MessageDigest : 暗号化前の MessageDigest を除く Request message
- 564 のパラメータから生成する。
- 565 ➤ Request message 作成後に保持している SequenceNumber を 1 増加する。
- 566 ➤ Request message を DRM サーバに送信する。
- 567 ➤ Request message 送信後のメッセージ受信待ちの状態に移る。
- 568

569 **(10) Request message 受信時の DRM サーバ処理**

- 570 ➤ [MIPTV], 4.1.4.5項の規定に従い、Request messageの検証を行う。
- 571 ✧ 検証が成功した場合、以下の処理を行い、(7)Reply message 送信時の
- 572 DRM サーバ処理を実行する
- 573 ● 保持している SequenceNumber を 1 増加する。
- 574 ● 保持している TransactionFlag を受信した Request message の
- 575 TransactionFlag に変更して保持する。
- 576 ● Request message から Service Protocol のメッセージを抽出する。
- 577 ✧ 検証が失敗した場合、以下の処理を行い、(17)Command が
- 578 「ERROR」の Encrypted command message 送信時の DRM サーバ処
- 579 理を実行する。
- 580 ● 保持している SequenceNumber を 1 増加する。
- 581

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

- 583 ➤ Encrypted command messageを作成する。SequenceNumber、
- 584 TransactionFlag、Command、Status、MessageDigestはセッション鍵で暗
- 585 号化する。Encrypted command messageのメッセージパラメータに関する
- 586 処理を以下に示す。
- 587 ✧ SequenceNumber : 保持している SequenceNumber を用いる。
- 588 ✧ Command : 「Commit」を設定する。
- 589 ✧ Status : 「Success (0000h)」を設定する。
- 590 ✧ MessageDigest : 暗号化前の MessageDigest を除く Encrypted
- 591 command message のパラメータから生成する。
- 592 ➤ Encrypted command message 作成後に保持している SequenceNumber を
- 593 1 増加する。
- 594 ➤ Encrypted command messageをDRMサーバに送信する。
- 595 ➤ Encrypted command message送信後のメッセージ受信待ちの状態に移る。
- 596

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

- 598 ➤ [MIPTV], 4.1.4.8 項の規定に従い、Encrypted command message の検証を
- 599 行う。
- 600 ✧ 検証が成功した場合、以下の処理を行い、(13)Command が「ACK」の
- 601 Encrypted command message 送信時の DRM サーバ処理を実行する。
- 602 ● 保持している SequenceNumber を 1 増加する
- 603 ✧ 検証が失敗した場合、以下の処理を行い、(17)Command が
- 604 「ERROR」の Encrypted command message 送信時の DRM サーバ処
- 605 理を実行する。

- 606 ● 保持している SequenceNumber を 1 増加する
- 607

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

- 609 ➤ Encrypted command messageを作成する。SequenceNumber、
- 610 TransactionFlag、Command、Status、MessageDigestはセッション鍵で暗
- 611 号化する。Encrypted command messageのメッセージパラメータに関する
- 612 処理を以下に示す。
- 613 ☆ SequenceNumber：保持している SequenceNumber を用いる。
- 614 ☆ Command：「ACK」を設定する。
- 615 ☆ Status：「Success (0000h)」を設定する。
- 616 ☆ MessageDigest：暗号化前の MessageDigest を除く Encrypted
- 617 command message のパラメータから生成する。
- 618 ➤ Encrypted command messageを受信機に送信する。
- 619 ➤ SACを終了して、SAC開始前の状態に移る。
- 620

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

- 622 ➤ [MIPTV], 4.1.4.8項の規定に従い、Encrypted command messageの検証を行
- 623 う。
- 624 ➤ SACを終了して、SAC開始前の状態に移る。
- 625

626 **(15) Plain command message 受信時の受信機処理**

- 627 ➤ [MIPTV], 4.1.4.7 項の規定に従い、Plain command message の検証を行う。
- 628 ➤ SAC を終了して、SAC 開始前の状態に移る。
- 629

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

- 631 ➤ Plain command message を作成する。Plain command message のメッセー
- 632 ジパラメータに関する処理を以下に示す。
- 633 ☆ Command：「ERROR」を設定する。
- 634 ☆ Status：メッセージの検証で確定した Status を設定する。
- 635 ➤ Plain command messageを受信機に送信する。
- 636 ➤ SACを終了して、SAC開始前のメッセージ受信待ちの状態に移る。
- 637

638 **(17) Command が「ERROR」の Encrypted command message 送信時の DRM サーバ処**
639 **理**

- 640 ➤ Encrypted command messageを作成する。SequenceNumber、
- 641 TransactionFlag、Command、Status、MessageDigestはセッション鍵で暗
- 642 号化する。Encrypted command messageのメッセージパラメータに関する
- 643 処理を以下に示す。
- 644 ☆ SequenceNumber：保持している SequenceNumber を用いる。
- 645 ☆ Command：「ERROR」を設定する。
- 646 ☆ Status：メッセージの検証で確定した Status を設定する。
- 647 ☆ MessageDigest：暗号化前の MessageDigest を除く Encrypted
- 648 command message のパラメータから生成する。
- 649 ➤ Encrypted command messageを受信機に送信する。

650 ➤ SACを終了して、SAC開始前のメッセージ受信待ちの状態に移る。
651

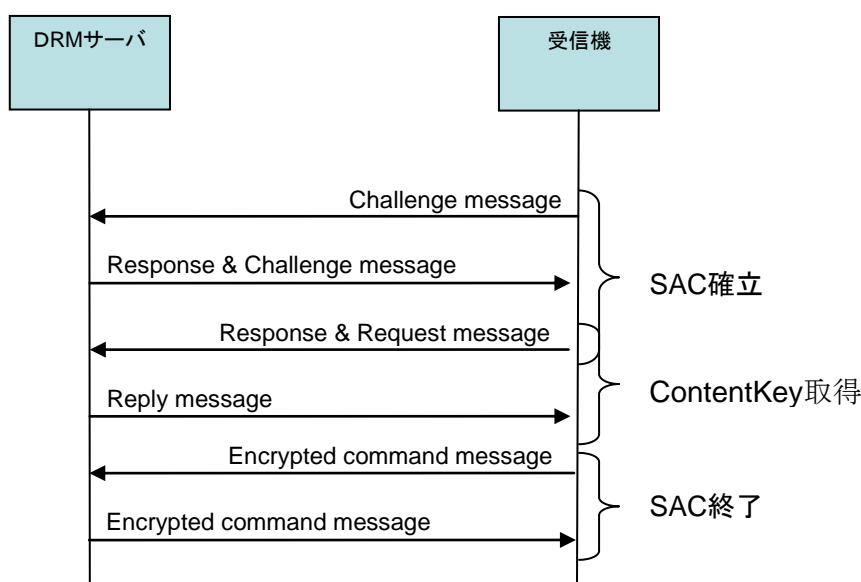
652 **A.2 SAC と Service Protocol を用いたシーケンス**

653 本節では、SAC と Service Protocol を用いたシーケンスとして、ContentKey 取得を
654 解説する。

655 図 A-3 に DRM サーバ・受信機間の ContentKey 取得シーケンスを示す。

656 なお、本 ContentKey 取得シーケンスは、ContentKey で暗号化され、ユニキャスト
657 やマルチキャストで伝送されるコンテンツを、受信時に視聴するために、都度
658 ContentKey を取得する形態への適用を想定するものである。

659
660



661

図 A-3 ContentKey 取得シーケンス

662

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

666

- 667 1. SAC 確立：[MIPTV], 4.1 節 Secure Authenticated Channel (SAC) Protocol で規
668 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、
669 SAC を確立する。
- 670 2. ContentKey 取得：[MIPTV], 4.2.1 項 Get Permission Protocol で規定されるプ
671 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
672 ContentKey と RenderingObligation を取得する。なお、ContentKey 取得と
673 Datetime を同時に取得する場合、[MIPTV], 4.2.3 項 Packed Message Protocol
674 で規定されるプロトコルを用いる。
- 675 3. SAC 終了：ContentKey 取得後、[MIPTV], 4.1 節 Secure Authenticated Channel
676 (SAC) Protocol で規定されるプロトコルにより、DRM サーバは Command が
677 ACK の Encrypted command message を送信した後に、受信機は Command が
678 ACK の Encrypted command message を受信した後に、SAC を終了する。
679

680 以上の ContentKey 取得シーケンスにより、受信機は ContentKey と対応する
681 RenderingObligation を取得する。
682 その後、受信機は、コンテンツサーバからコンテンツをストリーミングで受ける。
683 コンテンツは ContentKey で復号して再生される。この際、RenderingObligation に
684 従った処理を行う必要がある。
685 なお、受信機は取得した ContentKey、Datetime を、取得した時点で利用可能である。
686 従って、SAC 終了前に、取得済みの ContentKey、Datetime を利用してもよい。
687 また、ContentKey の扱いに関しては、[IPTVCRVOD], 4 章の規定を参照のこと。
688

689 A.3 メッセージの例

690 A.3.1 HTTP のメッセージの例

691 本項では受信機と DRM サーバとの通信の HTTP ヘッダの例を SAC の処理毎に示す。
692 本項で示す例では、以下を想定している。

- 693 ● DRM サーバのホスト名は www.iptv.jp
- 694 ● Cookie は 000000000000000001

695 なお、Cookie を用いない場合は、以降に示す例の Set-Cookie および Cookie は不要
696 である。

697
698 受信機から Challenge message を送信する場合

```
699     POST / HTTP/1.1  
700     Host: www.iptv.jp  
701     Content-type: application/octet-stream  
702     Content- Length: 1039  
703
```

704 DRM サーバから Response & Challenge message を送信する場合

```
705     HTTP/1.1 200 OK  
706     Set-Cookie: JSESSIONID=000000000000000001  
707     Cache-Control: no-cache  
708     Content-type: application/octet-stream  
709     Content- Length: 1321  
710
```

711 受信機から Challenge message 以外のメッセージを送信する場合

```
712     POST / HTTP/1.1  
713     Host: www.iptv.jp  
714     Cookie: JSESSIONID=000000000000000001  
715     Content-type: application/octet-stream  
716     Content- Length: 236  
717
```

718 DRM サーバから Response & Challenge message 以外のメッセージを送信する場合

```
719     HTTP/1.1 200 OK  
720     Cache-Control: no-cache  
721     Content-type: application/octet-stream  
722     Content- Length: 124  
723
```

724 A.3.2 SAC のメッセージの例

725 本項では SAC のメッセージの例を示す。

726 なお、サイズの大きいパラメータ (SinkCertificate、SourceCertificate など) と演算
727 により生成するパラメータ (SourceEC-DHPhase1Value、Signature など) は、値

728 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
729 前の値を示す。

730

731 **A.3.2.1 Challenge message**

732 1001byte の SinkCertificate を格納した Challenge message の例を表 A-3 に示す。

733

表 A-3 Challenge message の例

| Byte index | パラメータ名 | 値：16 進表記 |
|------------|---------------------|------------------|
| 0-3 | ProtocolID | 49505456 (固定値) |
| 4-5 | ProtocolVersion | 0100 (固定値) |
| 6-13 | SenderID | 1001000000000000 |
| 14-15 | PayloadType | 0001 (固定値) |
| 16-19 | PayloadSize | 0000034C |
| 20-35 | SinkRandomNumber | (省略) |
| 36-37 | SinkCertificateSize | 03E9 |
| 38-1038 | SinkCertificate | (省略) |

734

735 **A.3.2.2 Response & Challenge message**

736 1171byte の SourceCertificate を格納した Response & Challenge message の例を表
737 A-4 に示す。

738

表 A-4 Response & Challenge message の例

| Byte index | パラメータ名 | 値：16 進表記 |
|------------|------------------------|------------------------|
| 0-3 | ProtocolID | 49505456 (固定値) |
| 4-5 | ProtocolVersion | 0100 (固定値) |
| 6-13 | SenderID | 0000000000000000 (固定値) |
| 14-15 | PayloadType | 0002 (固定値) |
| 16-19 | PayloadSize | 000003BC |
| 20-35 | SourceRandomNumber | (省略) |
| 36-91 | SourceEC-DHPhase1Value | (省略) |
| 92-147 | Signature | (省略) |
| 148-149 | SourceCertificateSize | 0493 |
| 150-1320 | SourceCertificate | (省略) |

739

740 **A.3.2.3 Response & Request message**

741 GetPermission Request を格納した Response & Request message の例を表 A-5 に
742 示す。

743

744

745

746

747

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 (固定値) |
| 4-5 | ProtocolVersion | 0100 (固定値) |
| 6-13 | SenderID | 1001000000000000 |
| 14-15 | PayloadType | 0003 (固定値) |
| 16-19 | PayloadSize | 000000D8 |
| 20-75 | SinkEC-DHPhase1Value | (省略) |
| 76-131 | Signature | (省略) |
| 132-135 | EncryptedDataSize | 00000064 |
| 136-138 | SequenceNumber | 000001 (固定値) |
| 139 | TransactionFlag | 00 (固定値) |
| 140-203 | Request | A.3.3.1.2 項を参照のこと |
| 204-235 | MessageDigest | (省略) |

748

749 **A.3.2.4 Request message**

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

752

表 A-6 Request message の例

| Byte index | パラメータ名 | 値 : 16 進表記 |
|------------|-------------------|-------------------|
| 0-3 | ProtocolID | 49505456 (固定値) |
| 4-5 | ProtocolVersion | 0100 (固定値) |
| 6-13 | SenderID | 1001000000000000 |
| 14-15 | PayloadType | 0004 (固定値) |
| 16-19 | PayloadSize | 00000068 |
| 20-23 | EncryptedDataSize | 00000064 |
| 24-26 | SequenceNumber | 000003 |
| 27 | TransactionFlag | 01 |
| 28-91 | Request | A.3.3.1.2 項を参照のこと |
| 92-123 | MessageDigest | (省略) |

753

754 **A.3.2.5 Reply message**

755 Get Permission Reply を格納した Reply message の例を表 A-7 に示す。

756

757

758

759

760

761

762

763

764

765

766

表 A-7 Reply message の例

| Byte index | パラメータ名 | 値：16 進表記 |
|------------|---------------------------|------------------------|
| 0-3 | ProtocolID | 49505456 (固定値) |
| 4-5 | ProtocolVersion | 0100 (固定値) |
| 6-13 | SenderID | 0000000000000000 (固定値) |
| 14-15 | PayloadType | 0005 (固定値) |
| 16-19 | PayloadSize | 0000004A |
| 20-23 | EncryptedDataSize | 00000046 |
| 24-26 | SequenceNumber | 000002 |
| 27 | TransactionFlagRecordFlag | 00 |
| 28-61 | Reply | A.3.3.1.3 項を参照のこと |
| 62-93 | MessageDigest | (省略) |

767

768 **A.3.2.6 Plain command message**

769 Status として Error other than the below を格納した Plain command message の例
770 を表 A-8 に示す。

771

表 A-8 Plain command message の例

| Byte index | パラメータ名 | 値：16 進表記 |
|------------|-----------------|------------------------|
| 0-3 | ProtocolID | 49505456 (固定値) |
| 4-5 | ProtocolVersion | 0100 (固定値) |
| 6-13 | SenderID. | 0000000000000000 (固定値) |
| 14-15 | PayloadType | 0006 (固定値) |
| 16-19 | PayloadSize | 00000004 (固定値) |
| 20-21 | Command | 0002 (固定値) |
| 22-23 | Status | 8001 |

772

773 **A.3.2.7 Encrypted command message**

774 Status として Error other than the below を格納した複数の Request を連続送信する
775 場合の最初の Request message に対する Encrypted command message の例を表
776 A-9 に示す。

777

778

779

780

781

782

783

784

785

786

787

788

表 A-9 Encrypted command message の例

| Byte index | パラメータ名 | 値 : 16 進表記 |
|------------|-------------------|------------------------|
| 0-3 | ProtocolID | 49505456 (固定値) |
| 4-5 | ProtocolVersion | 0100 (固定値) |
| 6-13 | SenderID. | 0000000000000000 (固定値) |
| 14-15 | PayloadType | 0007 (固定値) |
| 16-19 | PayloadSize | 0000002C (固定値) |
| 20-23 | EncryptedDataSize | 00000028 (固定値) |
| 24-26 | SequenceNumber | 000004 |
| 27 | TransactionFlag | 00 |
| 28-29 | Command | 0002 |
| 30-31 | Status | 8001 |
| 32-63 | MessageDigest | (省略) |

789

790 **A.3.3 Service Protocol のメッセージの例**

791 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。

792

793 **A.3.3.1 Get Permission Protocol**

794 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
795 を示す。

796

797 **A.3.3.1.1 DeviceInformation**

798 [MIPTV], 3.2.2 項で規定される DeviceInformation の例を表 A-10 に示す。この情報
799 は Get Permission Request メッセージに格納される。

800

表 A-10 DeviceInformation の例

| Byte index | パラメータ名 | 値 : 16 進表記 |
|------------|---|--------------|
| 0 | Marlin IPTV-ES SpecificationVersionMajor | 01 (固定値) |
| 1 | Marlin IPTV-ES SpecificationVersionMinor | 00 (固定値) |
| 2 | Capabilities | 00 (固定値) |
| 3-4 | Manufacturer | 1001 |
| 5-6 | ManufacturerModel | 0000 (固定値) |
| 7 | ManufacturerModelVersion Major | 00 (固定値) |
| 8 | ManufacturerModelVersion Minor | 00 (固定値) |
| 9-11 | Reserved | 000000 (固定値) |

801

802

803

804 **A.3.3.1.2 Get Permission Request**
 805 [MIPTV], 4.2.1.2 項で規定される Get Permission Request メッセージの例を表 A-11
 806 に示す。
 807

表 A-11 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 (固定値) |
| 2-3 | MessageID | 0001 (固定値) |
| 4-15 | DeviceInformation | A.3.3.1.1 項参照 |
| 16-31 | UsageRuleReference | 全て 00 |
| 32 | ActionID | 01 (固定値) |
| 33 | ActionParameter | FF (固定値) |
| 34-35 | SpecificCRID | 0000 (固定値) |
| 36 | PrivateDataTag | 00 (固定値) |
| 37-63 | PrivateData | 全て 00 (固定値) |

808

809 **A.3.3.1.3 Get Permission Reply**
 810 [MIPTV], 4.2.1.3 項で規定される Get Permission Reply メッセージの例を表 A-12 に
 811 示す。

表 A-12 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 (固定値) |
| 2-3 | MessageID | 0002 (固定値) |
| 4-5 | Status | 0000 |
| 6-21 | ContentKey | 全て 00 |
| 22-23 | ExtractInfoSize | 0A (固定値) |
| 24-27 | NotBefore | 00000000 (固定値) |
| 28-31 | NotAfter | 00000000 (固定値) |
| 32-33 | RenderingObligation | A.3.3.1.4 項参照 |

812

813 **A.3.3.1.4 Output Control Information**
 814 [MIPTV], 4.2.1.4.1 項で規定される RenderingObligation (Output Control Information)
 815 の例を表 A-13 に示す。
 816
 817
 818
 819
 820
 821
 822
 823
 824
 825
 826
 827

表 A-13 *RenderingObligation* の例

| Bit index | パラメータ名 | 値：2進表記 |
|-----------|-----------------------------|------------|
| 0-1 | DigitalRecordingControlData | 11 (固定値) |
| 2-3 | CopyControlType | 01 (固定値) |
| 4-5 | APSControlData | 01 |
| 6 | ImageConstraintToken | 1 (固定値) |
| 7 | RetentionMode | 0 (固定値) |
| 8-10 | RetentionState | 111 (固定値) |
| 11 | EncryptionMode | 1 (固定値) |
| 12-15 | UserDefined | 全て 0 (固定値) |

828

829 **A.3.3.2 Get Trusted Time Protocol**

830 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
831 例を示す。

832

833 **A.3.3.2.1 Get TrustedTime Request**

834 [MIPTV], 4.2.2.2 項で規定される Get Trusted Time Request メッセージの例を表
835 A-14 に示す。

836

表 A-14 *Get Trusted Time 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 (固定値) |
| 2-3 | MessageID | 0003 (固定値) |

837

838 **A.3.3.2.2 Get Trusted Time Reply**

839 [MIPTV], 4.2.2.3 で規定される Get Trusted Time Reply メッセージの例を表 A-15 に
840 示す。

841

表 A-15 *Get Trusted Time 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 (固定値) |
| 2-3 | MessageID | 0004 (固定値) |
| 4-5 | Status | 0000 |
| 6-9 | Datetime | 4B3CCABD |

842

843 **A.3.3.3 Packed Message Protocol**

844 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
845 を示す。

846

847

848

849 **A.3.3.3.1 Packed Message Request**

850 [MIPTV], 4.2.3.2 項で規定される Packed Message Request に格納する Request が
851 A.3.3.1.2 項と A.3.3.2.1 項の場合の例を表 A-16 に示す。

852

表 A-16 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 (固定値) |
| 2-3 | MessageID | 0101 (固定値) |
| 4-5 | NumberOfRequestMessageBoxes | 0002 (固定値) |
| 6-7 | RequestMessageSize | 0040 (固定値) |
| 8-71 | RequestMessage | A.3.3.1.2 項参照 |
| 72-73 | RequestMessageSize | 0004 (固定値) |
| 74-77 | RequestMessage | A.3.3.2.1 項参照 |

853

854 **A.3.3.3.2 Packed Message Reply**

855 [MIPTV], 4.2.3.3 項で規定される Packed Message Reply メッセージで A.3.3.3.1 項
856 に対して応答する場合の例を表 A-17 に示す。

857

表 A-17 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 (固定値) |
| 2-3 | MessageID | 0102 (固定値) |
| 4-5 | Status | 0000 |
| 6-7 | NumberOfReplyMessageBoxes | 0002 (固定値) |
| 8-9 | ReplyMessageSize | 0022 (固定値) |
| 10-43 | ReplyMessage | A.3.3.1.3 項参照 |
| 44-45 | ReplyMessageSize | 000A (固定値) |
| 46-55 | ReplyMessage | A.3.3.2.2 項参照 |

858