

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

13 **Marlin IPTV-ES 運用仕様**
14 **ダウンロード編**

15
16 Document Version: 1.5
17 Final

18
19 Date: 3 September, 2013

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 © 2008-2013 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 本仕様の内容は予告無しに変更されることがあります。

50

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	バイトオーダー..... 5
58	2	SACに関する規定..... 6
59	2.1	メッセージパラメータ..... 6
60	2.2	SACタイムアウト..... 6
61	2.3	1つのTCP Connectionを利用可能なSACセッション..... 6
62	3	Service Protocolに関する規定..... 7
63	3.1	Get Permission Protocol (EXTRACT)..... 7
64	3.1.1	メッセージパラメータの設定..... 7
65	3.1.1.1	Get Permission Request parameters..... 7
66	3.1.1.2	Get Permission Reply parameters..... 7
67	3.1.2	メッセージパラメータの検証..... 7
68	3.1.2.1	Get Permission Request parameters..... 7
69	3.1.2.2	Get Permission Reply parameters..... 8
70	3.2	Get Permission Protocol (EXPORT)..... 8
71	3.2.1	メッセージパラメータの設定..... 8
72	3.2.1.1	Get Permission Request parameters..... 8
73	3.2.1.2	Get Permission Reply parameters..... 8
74	3.2.2	メッセージパラメータの検証..... 8
75	3.2.2.1	Get Permission Request parameters..... 8
76	3.2.2.2	Get Permission Reply parameters..... 8
77	3.3	Get Trusted Time Protocol..... 9
78	3.4	Packed Message Protocol..... 9
79	3.4.1	メッセージパラメータの設定..... 9
80	3.4.1.1	Packed Message Request parameters..... 9
81	3.4.1.2	Packed Message Reply parameters..... 10
82	3.4.2	メッセージパラメータの検証..... 10
83	3.4.2.1	Packed Message Request parameters..... 10
84	3.4.2.2	Packed Message Reply parameters..... 11
85	4	ネットワーク通信プロトコル (HTTP) に関する規定..... 12
86	5	鍵の利用に関する規定..... 13
87	5.1	再生を目的としたContentKeyの利用..... 13
88	A	Appendix (Informative)..... 14
89	A.1	SAC処理の例..... 14
90	A.1.1	状態遷移..... 14
91	A.1.2	メッセージ処理..... 17
92	(1)	Challenge message送信時の受信機処理..... 18
93	(2)	Challenge message受信時のDRMサーバ処理..... 18
94	(3)	Response & Challenge message送信時のDRMサーバ処理..... 19
95	(4)	Response & Challenge message受信時の受信機処理..... 19
96	(5)	Response & Request message送信時の受信機処理..... 19
97	(6)	Response & Request message受信時のDRMサーバ処理..... 19
98	(7)	Reply message送信時のDRMサーバ処理..... 19
99	(8)	Reply message受信時の受信機処理..... 20
100	(9)	Request message送信時の受信機処理..... 21
101	(10)	Request message受信時のDRMサーバ処理..... 21
102	(11)	Encrypted command message送信時の受信機処理..... 21
103	(12)	Encrypted command message受信時のDRMサーバ処理..... 21

104	(13)	Commandが「ACK」のEncrypted command message送信時の	
105		DRMサーバ処理.....	22
106	(14)	Encrypted command message受信時の受信機処理.....	22
107	(15)	Plain command message受信時の受信機処理.....	22
108	(16)	Plain command message送信時のDRMサーバ処理.....	22
109	(17)	Commandが「ERROR」の	
110		Encrypted command message送信時のDRMサーバ処理.....	23
111	(18)	Response & Commit message送信時の受信機処理.....	23
112	(19)	Response & Commit message受信時のDRMサーバ処理.....	23
113	A.2	TransactionFlagに関する処理の解説.....	24
114	A.2.1	TransactionFlagの記憶処理.....	24
115	A.2.2	Reply messageの受信判断処理.....	28
116	A.2.3	TransactionFlagの単独削除.....	29
117	A.3	SACとService Protocolを用いたシーケンス.....	29
118	A.3.1	再生のためのContentKey取得.....	30
119	A.3.2	ExportのためのContentKey取得.....	31
120	A.4	メッセージの例.....	32
121	A.4.1	SACのメッセージの例.....	32
122	A.4.1.1	Challenge message.....	32
123	A.4.1.2	Response & Challenge message.....	32
124	A.4.1.3	Response & Request message.....	32
125	A.4.1.4	Request message.....	33
126	A.4.1.5	Reply message.....	33
127	A.4.1.6	Plain command message.....	34
128	A.4.1.7	Encrypted command message.....	34
129	A.4.1.8	Response & Commit message.....	34
130	A.4.2	Service Protocolのメッセージの例.....	34
131	A.4.2.1	Get Permission Protocol.....	35
132	A.4.2.1.1	Get Permission Request (EXTRACT).....	35
133	A.4.2.1.2	Get Permission Reply (EXTRACT).....	35
134	A.4.2.1.3	Get Permission Request (EXPORT).....	35
135	A.4.2.1.4	Get Permission Reply (EXPORT).....	36
136	A.4.2.2	Get Trusted Time Protocol.....	36
137	A.4.2.2.1	Get TrustedTime Request.....	36
138	A.4.2.2.2	Get Trusted Time Reply.....	36
139	A.4.2.3	Packed Message Protocol.....	36
140	A.4.2.3.1	Packed Message Request.....	37
141	A.4.2.3.2	Packed Message Reply.....	37

142 **1 はじめに**

143 “Marlin IPTV End-point Service Specification” [MIPTV]では、暗号化されたコンテ
144 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
145 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
146 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、
147 本編をダウンロード編と呼ぶこととする。
148

149 **1.1 本書の規定範囲**

150 本書では、暗号を復号するためのContentKeyを“Marlin IPTV End-point Service
151 Specification” [MIPTV]の 4.2.1.2 項で規定されるActionIDが「EXTRACT with Direct
152 Key Delivery (03h)」または「EXPORT for Copy with Direct Key Delivery
153 (10h)」のGet Permission Requestで取得するコンテンツ（以下、本書では“コン
154 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
155 る追加規定項目を規定し、さらに“Marlin IPTV-ES/J Specific Compliance Rules ダ
156 ウンロード編” [IPTVCRDL]に対する詳細規定項目を規定する。
157 本書は、[IPTVCRDL]に準拠する受信機およびDRMサーバに適用する。
158
159 以下に本書の規定項目を示す。
160

- 161 ● [MIPTV]に対する詳細規定項目
 - 162 ➤ SACに関する規定 ([MIPTV], 4.1 節 Secure Authenticated Channel
163 (SAC)Protocol)
 - 164 ☆ メッセージパラメータ
 - 165 ☆ SAC タイムアウト
 - 166 ☆ 1つの TCP Connection を利用可能な SAC セッション
 - 167 ➤ Service Protocolに関する規定 ([MIPTV], 4.2 節Marlin IPTV-ES Service
168 Protocols over SACに関する規定)
 - 169 ☆ メッセージパラメータの設定
 - 170 ☆ メッセージパラメータの検証
- 171
- 172 ● [MIPTV]に対する追加規定項目
 - 173 ➤ ネットワーク通信プロトコル (HTTP) に関する規定
 - 174 ☆ HTTP による SAC のメッセージの伝送
 - 175 ☆ HTTP ヘッダ
- 176
- 177 ● [IPTVCRDL]に対する詳細規定項目
 - 178 ➤ 鍵の利用に関する規定
- 179

180 **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

182 **1.3 用語の定義**

183 本書で用いる用語を以下のように定義する。

184

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。

185

186 本書で用いる用語と[MIPTV]の用語との対応を以下に示す。

187

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

188

189 **1.4 バイトオーダー**

190 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
191 ある。

192 **2 SACに関する規定**

193 本章では IPTV-ES SAC の運用を規定する。

194

195 **2.1 メッセージパラメータ**

196 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。

197

198 **2.2 SACタイムアウト**

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

200

201 **2.3 1つのTCP Connectionを利用可能なSACセッション**

202 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],

203 2.3 節と同等である。

204

205 **3 Service Protocolに関する規定**

206 本章では、IPTV-ES Service Protocol の運用を規定する。
207 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
208 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。
209

210 **3.1 Get Permission Protocol (EXTRACT)**

211 [MIPTV], 4.2 節で規定される Get Permission Protocol において、ActionID が
212 「EXTRACT with Direct Key Delivery (03h)」の Get Permission Request を用いて、
213 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
214 ッセージパラメータの検証について規定する。
215

216 **3.1.1 メッセージパラメータの設定**

217 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。
218

219 **3.1.1.1 Get Permission Request parameters**

220 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
221 メッセージパラメータを設定する。
222

- 223 ● UsageRuleReference
- 224 ▶ 事前に取得した UsageRuleReference を設定する。
225

226 **3.1.1.2 Get Permission Reply parameters**

227 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
228 Reply のメッセージパラメータを設定する。
229

230 **3.1.2 メッセージパラメータの検証**

231 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
232 ータを検証する。
233

234 **3.1.2.1 Get Permission Request parameters**

235 DRMサーバは、[MIPTV], 4.2.4.1 項および以下の規定に従い、Get Permission
236 Request のメッセージパラメータを検証する。
237

- 238 ● ActionID
- 239 ▶ ActionID が「EXTRACT with Direct Key Delivery (03h)」の Get
240 Permission Request に対応する DRM サーバは、ActionID が、以下に示す
241 値の場合には検証失敗としない。
242 ☆ EXTRACT with Direct Key Delivery (03h)
243

244 **3.1.2.2 Get Permission Reply parameters**

245 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
246 のメッセージパラメータを検証する。
247

248 **3.2 Get Permission Protocol (EXPORT)**

249 [MIPTV], 4.2 節で規定されるGet Permission Protocolにおいて、ActionIDが
250 「EXPORT for Copy with Direct Key Delivery (10h)」のGet Permission Requestを
251 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
252 設定とメッセージパラメータの検証について規定する。
253

254 **3.2.1 メッセージパラメータの設定**

255 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。
256

257 **3.2.1.1 Get Permission Request parameters**

258 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
259 メッセージパラメータを設定する。
260

261 ● UsageRuleReference

262 ‣ 事前に取得した UsageRuleReference を設定する。
263

264 **3.2.1.2 Get Permission Reply parameters**

265 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
266 Replyのメッセージパラメータを設定する。
267

268 **3.2.2 メッセージパラメータの検証**

269 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
270 メータを検証する。
271

272 **3.2.2.1 Get Permission Request parameters**

273 DRMサーバは、[MIPTV], 4.2.4.1 項および以下の規定に従い、Get Permission
274 Requestのメッセージパラメータを検証する。
275

276 ● ActionID

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

280 † EXPORT for Copy with Direct Key Delivery (10h)
281

282 **3.2.2.2 Get Permission Reply parameters**

283 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
284 ャッセージパラメータを検証する。
285

286 **3.3 Get Trusted Time Protocol**

287 [MIPTV], 4.2.2 項で規定される Get Trusted Time Protocol は、Datetime の取得に用い
288 る。

289 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
290 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
291 Trusted Time Reply のメッセージパラメータを検証する。

292 DRM サーバは、[MIPTV], 4.2.4.9 項の規定に従い、Get Trusted Time Request のメッ
293 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
294 い、Get Trusted Time Reply のメッセージパラメータを設定する。
295

296 **3.4 Packed Message Protocol**

297 [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
298 合に用いる。
299

- 300 ● EXTRACT と EXPORT の ContentKey。
- 301 ● EXTRACT の ContentKey と Datetime。
- 302 ● EXPORT の ContentKey と Datetime。
- 303 ● EXTRACT および EXPORT の ContentKey と Datetime。

304

305 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
306 定する。
307

308 **3.4.1 メッセージパラメータの設定**

309 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。
310

311 **3.4.1.1 Packed Message Request parameters**

312 受信機は、[MIPTV], 4.2.3.2 項および以下の規定に従い、Packed Message Request
313 のメッセージパラメータを設定する。
314

314

- 315 ● RequestMessageBoxList

316 ➤ 表 3-1 に示す順番にメッセージを格納する。
317

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

318

319 **3.4.1.2 Packed Message Reply parameters**

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

322

323 **3.4.2 メッセージパラメータの検証**

324 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
325 ータを検証する。

326

327 **3.4.2.1 Packed Message Request parameters**

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

330

- 331 ● RequestMessageBoxList
332 ➤ RequestMessageBoxList に ActionID が「EXTRACT with Direct Key
333 Delivery (03h)」または「EXPORT for Copy with Direct Key Delivery
334 (10h)」の Get Permission Request の RequestMessage が 1 以上格納さ
335 れている場合、かつ、RequestMessage の組み合わせが、
336 ➤ 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
337 parameterのStatusを「Message format error (8009h)」とする。
338

339 3.4.2.2 Packed Message Reply parameters

- 340 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
341 パラメータを検証する。

342 **4 ネットワーク通信プロトコル (HTTP) に関する規定**

343 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
344 である。
345

346 **5 鍵の利用に関する規定**

347 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。
348

349 **5.1 再生を目的としたContentKeyの利用**

350 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。
351

352 A Appendix (Informative)

353 A.1 SAC処理の例

354 本節では、ActionID が「EXPORT for Copy with Direct Key Delivery (10h)」の Get
355 Permission Protocol に対応した受信機と DRM サーバの SAC 処理の例を示す。
356

357 A.1.1 状態遷移

358 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
359 す。
360 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。
361 表A-1のTransactionFlagは、Response & Challenge messageの送信元のDRMサーバ
362 の識別情報と対応付けて記憶したTransactionFlagである。
363 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。
364 なお、本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。
365

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		⑤ Encrypte d comman d messag e 送信後 のメッ セージ 受信待 ち	⑥ Respons e & Comm it messag e 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、 TransactionFI ag を記憶して いなければ③ に移り、 TransactionFI ag 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		
		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⑦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
	Response & Commit message 受信	⑦に移る	A.1.2項(19)の処理を実行して、⑦に移る	⑦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)	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	

369 **A.1.2 メッセージ処理**

370 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
371 処理の典型例を示す。

372 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
373 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
374 理について説明する。

375

376

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

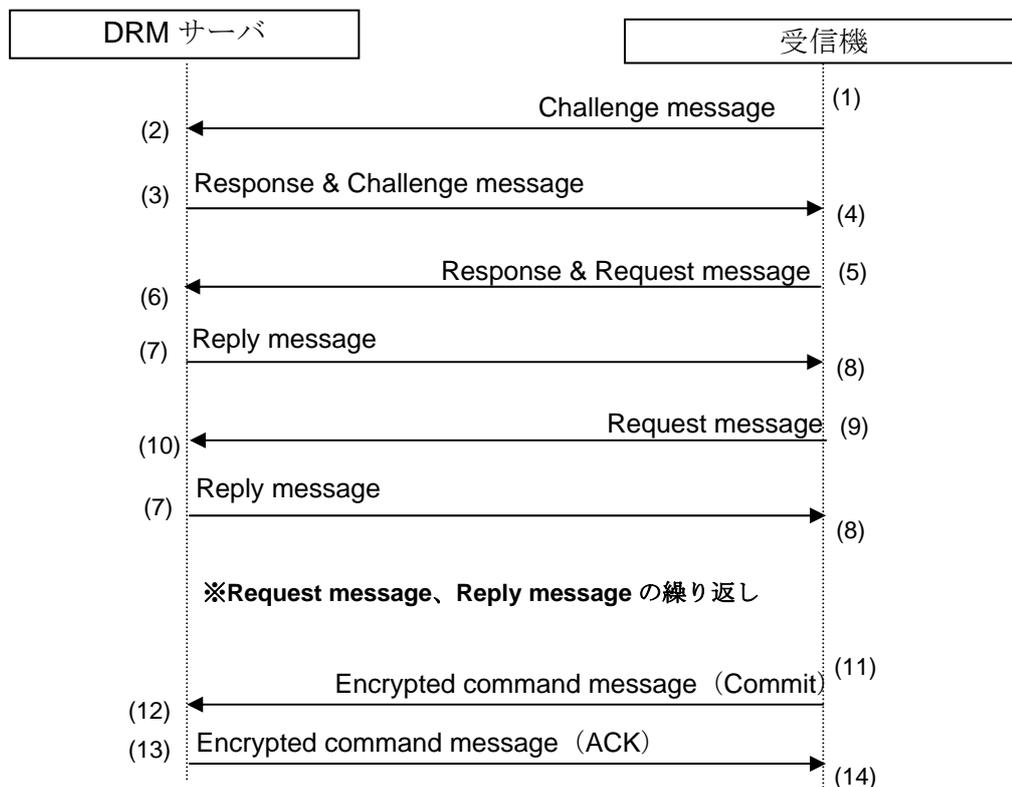


図 A-1 基本シーケンス (複数の Request を連続送信する場合)

392
393
394
395
396
397
398
399
400
401
402
403
404

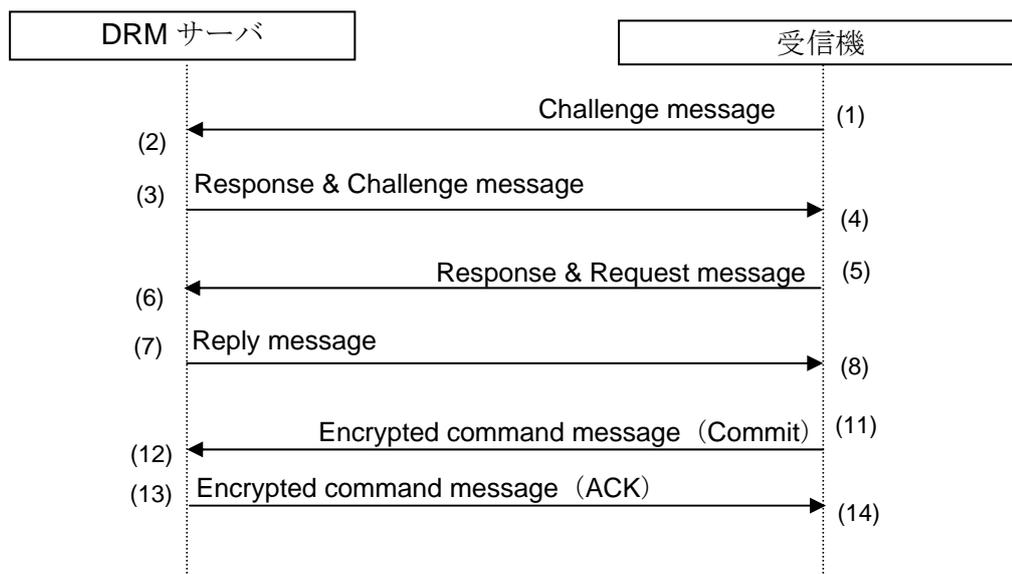


図 A-2 基本シーケンス (一つの Request のみ送信する場合)

405
406
407
408
409
410
411
412
413
414
415
416

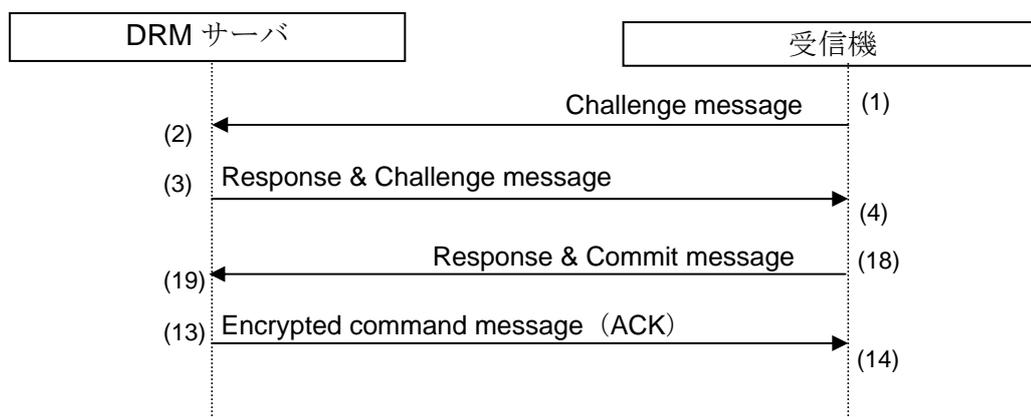


図 A-3 基本シーケンス

(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)

417
418
419
420
421
422
423
424

(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。

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

426 Response & Challenge message送信時のDRMサーバ処理は、[IPTVESVOD], A.1.2
427 項(3)と同等である。
428

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

430 ▶ [MIPTV], 4.1.4.3 項の規定に従い、Response & Challenge messageの検証
431 を行う。

432 ☆ 検証が成功した場合、以下の処理を実行する。

433 ● Response & Challenge messageの送信元のDRMサーバの識別情報
434 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
435 行する。
436

437 ● Response & Challenge messageの送信元のDRMサーバの識別情報
438 と対応付けたTransactionFlagが不揮発性記憶領域に記憶されている
439 場合、(18)Response & Commit message送信時の受信機処理を実
440 行する。

441 ☆ 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。
442

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

444 Response & Request message送信時の受信機処理は、[IPTVESVOD], A.1.2 項(5)と
445 同等である。
446

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

448 ▶ [MIPTV], 4.1.4.4 項の規定に従い、Response & Request messageの検証を
449 行い、セッション鍵を生成する。

450 ☆ 検証が成功した場合、以下の処理を行い、(7)Reply message送信時の
451 DRMサーバ処理を実行する。

452 ● Response & Request message の送信元の受信機の識別情報と対応
453 付けた TransactionFlag が不揮発性記憶領域に記憶されている場合、
454 Response & Request message の送信元の受信機に最後に送信した
455 Reply message を受信機が受信していないと判断する。

456 ● SequenceNumberとして、[MIPTV], 4.1.4.4 項でSequenceNumber
457 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。

458 ● Response & Request message の TransactionFlag を保持する。

459 ● Response & Request message から Service Protocol のメッセージ
460 を抽出する。

461 ☆ 検証が失敗した場合、(16)Plain command message送信時のDRMサー
462 バ処理を実行する。
463

464 **(7) Reply message送信時のDRMサーバ処理**

465 ▶ Reply message を作成する。Reply message のメッセージパラメータに関
466 して以下の処理を行う。

467 ☆ SequenceNumber : 保持している SequenceNumber を用いる。

468 ☆ 以下に示すように TransactionFlagRecordFlag を設定する。

469 ● [MIPTV], 4.1.3.6 項の規定に従い、EXPORTに用いるContentKeyに

- 470 ついて受信機での取得回数をカウントする場合、「record
471 (01h)」を設定する。
- 472 ● 上記以外の場合、「not to record (00h)」を設定する。
 - 473 ☆ Reply : Service Protocol のメッセージを設定する。
 - 474 ☆ MessageDigest : 暗号化前の MessageDigest を除く Reply message の
475 パラメータから生成する。
 - 476 ☆ SequenceNumber、TransactionFlagRecordFlag、Reply、
477 MessageDigest はセッション鍵で暗号化する。
 - 478 ➤ Reply message を作成後に保持している SequenceNumber を 1 増加する。
 - 479 ➤ TransactionFlag の記憶・削除を行う。
 - 480 ☆ TransactionFlagRecordFlag に「record (01h)」を設定する場合、
481 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
482 信機から受信した TransactionFlag を不揮発性記憶領域に記憶する。
 - 483 ☆ TransactionFlagRecordFlag に「not to record (00h)」を設定する場合、
484 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
485 憶領域に記憶されている TransactionFlag を削除する。
 - 486 ➤ Reply messageを受信機に送信する。
 - 487 ➤ Reply message送信後のメッセージ受信待ちの状態に移る。
 - 488

489 (8) Reply message受信時の受信機処理

- 490 ➤ [MIPTV], 4.1.4.6 項の規定に従い、Reply messageの検証を行う。
 - 491 ☆ 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
492 は(9)Request message送信時の受信機処理を実行し、送信するRequest
493 がない場合は(11)Encrypted command message送信時の受信機処理を
494 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
495 SACを終了して、SAC開始前の状態に移る。
 - 496 ● 保持している SequenceNumber を 1 増加する。
 - 497 ● TransactionFlag の反転と保持を行う。現在、保持している
498 TransactionFlag が even (00h) の場合は「odd (01h)」を、odd
499 (01h) の場合は「even (00h)」を保持する。
 - 500 ● Reply message から Service Protocol のメッセージを抽出する。
 - 501 ● [MIPTV], 4.1.4.11.1 項(2)の実行条件を満たす場合、Reply message
502 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
503 に記憶されているTransactionFlagを削除する。
 - 504 ● [MIPTV], 4.1.4.11.1 項(1)の実行条件を満たす場合、Reply message
505 の送信元のDRMサーバに最後に送信したTransactionFlagをReply
506 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
507 記憶領域に記憶する。
 - 508 ☆ 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。

510 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
511 行う。

- 512
- 513 ➤ [MIPTV], 4.1.4.11.1 項(2)の実行条件を満たす場合、Reply messageの送信
514 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
515 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
516 可の状態のContentKeyを、利用可能な状態に変更する。

517 ▶ [MIPTV], 4.1.4.11.1 項(1)の実行条件を満たす場合、TransactionFlagの記憶
518 と共に、記憶するTransactionFlagと対応付けて、Reply messageで取得し
519 たContentKeyを利用不可の状態の不揮発性記憶領域に記憶する。
520

521 **(9) Request message送信時の受信機処理**

522 Request message送信時の受信機処理は、[IPTVESVOD], A.1.2 項(9)と同等である。
523

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

525 ▶ [MIPTV], 4.1.4.5項の規定に従い、Request messageの検証を行う。
526 ✧ 検証が成功した場合、以下の処理を行い、(7)Reply message送信時の
527 DRMサーバ処理を実行する。
528 ● Request message の送信元の受信機の識別情報と対応付けた
529 TransactionFlag を不揮発性記憶領域に記憶している場合、最後に
530 送信した Reply message を受信機が受信していると判断する。
531 ● 保持している SequenceNumber を 1 増加する。
532 ● 保持している TransactionFlag を受信した Request message の
533 TransactionFlag に変更して保持する。
534 ● Request message から Service Protocol のメッセージを抽出する。
535 ✧ 検証が失敗した場合、以下の処理を行い、(17)Commandが「ERROR」
536 のEncrypted command message送信時のDRMサーバ処理を実行する。
537 ● 保持している SequenceNumber を 1 増加する。
538

539 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
540 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。

541 ▶ Request message の送信元の受信機に最後に送信した ContentKey の取得
542 回数のカウントを行う。
543
544

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

546 Encrypted command message送信時の受信機処理は、[IPTVESVOD], A.1.2 項(11)と
547 同等である。
548

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

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

- 保持している SequenceNumber を 1 増加する。

563

564 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
565 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。

566

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

568

569

570 (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
571 のメッセージパラメータに関して以下の処理を行う。

572

- ◇ SequenceNumber : 保持している SequenceNumber を用いる。

573

- ◇ Command : 「ACK」を設定する。

574

- ◇ Status : 「Success (0000h)」を設定する。

575

- ◇ MessageDigest : 暗号化前の MessageDigest を除く Encrypted
576 command message のパラメータから生成する。

577

- ◇ SequenceNumber、TransactionFlag、Command、Status、
578 MessageDigest はセッション鍵で暗号化する。

579

- Encrypted command message の送信先の受信機の識別情報と対応付けて不
580 揮発性記憶領域に記憶されている TransactionFlag を削除する。

581

- Encrypted command message を受信機に送信する。

582

- SAC を終了して、SAC 開始前の状態に移る。

583

584

585 (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
586 行う。

587

- ◇ 検証が成功した場合、以下の処理を行う。

588

- [MIPTV], 4.1.4.11.1 項(2)の実行条件を満たす場合、Encrypted
589 command messageの送信元のDRMサーバの識別情報と対応付けて
590 不揮発性記憶領域に記憶されているTransactionFlagを削除する。

591

- SAC を終了して、SAC 開始前の状態に移る。

592

593

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

596

- [MIPTV], 4.1.4.11.1 項(2)の実行条件を満たす場合、Encrypted command
597 messageの送信元のDRMサーバの識別情報と対応付けられた
598 TransactionFlagの削除と共に、当該TransactionFlagと対応付けて不揮発性
599 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
600 態に変更する。

601

602

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

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

606

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

608 Plain command message送信時のDRMサーバ処理は、[IPTVESVOD], A.1.2 項(16)と
609 同等である。
610

611 **(17) Commandが「ERROR」のEncrypted command message送信時のDRMサーバ処理**
612 Commandが「ERROR」のEncrypted command message送信時のDRMサーバ処理
613 は、[IPTVESVOD], A.1.2 項(17)と同等である。
614

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

- 616 > セッション鍵を生成する。
- 617 > Response & Commit message を作成する。Response & Commit message
618 のメッセージパラメータに関して以下の処理を行う。
 - 619 ✧ Signature : SourceRandomNumber と SinkEC-DHPPhase1Value に対し
620 て生成する。
 - 621 ✧ SequenceNumber : 1 を Response & Commit message に設定する。
 - 622 ✧ TransactionFlag : Response & Commit message の送信先の DRM サー
623 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
624 TransactionFlag の値を Response & Commit message に設定する。
 - 625 ✧ MessageDigest : 暗号化前の MessageDigest を除く Response &
626 Commit message のパラメータから生成する。
 - 627 ✧ SequenceNumber、TransactionFlag、MessageDigest をセッション鍵
628 で暗号化する。
- 629 > SequenceNumber として、Response & Commit message に設定した値よ
630 りも 1 大きい値である 2 を保持する。
- 631 > Response & Commit message を DRM サーバに送信する。
- 632 > Response & Commit message 送信後のメッセージ受信待ちの状態に移る。
633

634 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、電源
635 ON 時など再度 DRM サーバの URI を取得せずに、Response & Commit message を
636 送信する SAC を実行することができる。
637

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

- 639 > [MIPTV], 4.1.4.9 項に従い、Response & Commit messageの検証を行い、
640 セッション鍵を生成する。
 - 641 ✧ 検証が成功した場合、以下の処理を行い、(13)Commandが「ACK」の
642 Encrypted command message送信時のDRMサーバ処理を実行する。
 - 643 ● Response & Commit message の送信元の受信機の識別情報と対応
644 付けた TransactionFlag を不揮発性記憶領域に記憶している場合、
645 Response & Commit message の TransactionFlag と比較して
646 Reply message の受信判断を行う。
 - 647 ◆ TransactionFlag が一致する場合は、最後に送信した Reply
648 message を受信機が受信していると判断する。
 - 649 ◆ TransactionFlag が異なる場合は、最後に送信した Reply
650 message を受信機が受信していないと判断する。
 - 651 ● SequenceNumberとして、[MIPTV], 4.1.4.9 項でSequenceNumber
652 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。

653 ☆ 検証が失敗した場合、(16)Plain command message送信時のDRMサー
654 バ処理を実行する。
655

656 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
657 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。
658

659 ▶ Response & Commit message の送信元の受信機に最後に送信した
660 ContentKey の取得回数のカウントを行う。
661

662 A.2 TransactionFlagに関する処理の解説

663 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
664 回数をサービス事業者が正しく把握できる必要がある。

665 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
666 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
667 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、
668 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
669 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。
670

- 671 ● 受信機は、Reply message の受信に失敗して、ContentKey を取得できなかった
672 場合、SAC 再開後に、記憶している TransactionFlag を DRM サーバに送信する。
- 673 ● DRM サーバは、記憶している TransactionFlag と受信した TransactionFlag が異
674 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
675 なわち受信機が ContentKey を取得できなかったと判断する。
- 676 ● 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
677 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
678 握する。
679

680 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
681 する。
682

- 683 ● 障害に備えて受信機と DRM サーバが行う TransactionFlag の記憶処理。
- 684 ● 障害復旧後に DRM サーバが行う Reply message の受信判断処理。
685

686 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
687 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
688 TransactionFlag を削除する処理についても解説する。
689

690 A.2.1 TransactionFlagの記憶処理

691 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
692 理の流れと不揮発性記憶領域の記憶状態を解説する。
693

694 A.2.1.1 TransactionFlag の記憶処理の流れ

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

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

- 699 ● 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
700 message で送信する場合、その送信前に受信機から受信した TransactionFlag
701 を不揮発性記憶領域に記憶して、Reply message の TransactionFlagRecordFlag
702 を「record (01h)」に設定する。
- 703 ● 受信機は、Reply message の TransactionFlagRecordFlag が「record (01h)」
704 であることから、最後に送信した TransactionFlag を記憶し、Reply message で
705 受信した ContentKey を利用不可の状態でも揮発性記憶領域に記憶する。なお、
706 EXTRACT では取得回数をカウントする ContentKey が送信されないため、
707 TransactionFlagRecordFlag の値によらず、この処理は不要である。
- 708 ● DRM サーバは、上記の Reply message を送信後に Request message または
709 Command が「Commit」の Encrypted command message を受信し、検証に成
710 功した時、受信機が上記の Reply message を受信したと判断する。
- 711 ● DRM サーバは、Reply message の受信を判断して次の Reply message または
712 Command が「ACK」の Encrypted command message を送信する時、不揮発
713 性記憶領域の TransactionFlag の削除または更新を行う。
- 714 ● 受信機は、次の Reply message または Command が「ACK」の Encrypted
715 command message を受信し、検証に成功した時、不揮発性記憶領域の
716 TransactionFlag の削除と ContentKey の利用可能な状態への状態変更を行う。
717 Reply message の TransactionFlagRecordFlag が「record (01h)」の場合、さ
718 らに第 3 項目と同等に TransactionFlag と ContentKey の記憶を行う。受信機は
719 さらに、上記でも揮発性記憶領域に記憶した利用不可の ContentKey の状態変更
720 も行う。

721

722 A.2.1.2 不揮発性記憶領域の記憶状態

723 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
724 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
725 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
726 態を、具体的な SAC 処理のシーケンスをもとに示す。

727 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、
728 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。

729 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
730 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。

731 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。
732 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
733 TransactionFlagの削除処理と[MIPTV], 4.1.4.11.1 項(1)のTransactionFlagの記憶処理
734 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。

735 図A-4の表記を以下に示す。

736

- 737 ● 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。
- 738 ● () の中は、TransactionFlag の値。
- 739 ● [] の中は、ContentKey と TransactionFlagRecordFlag の値。
- 740 ● K1 から Kn は ContentKey の値。
- 741 ● 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。
- 742 ● 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
743 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
744 み表記。
- 745 ● 状態 S0 から状態 Sn+1 と状態 C0 から状態 Cn+1 の TF は、TransactionFlag を
746 意味する。

747

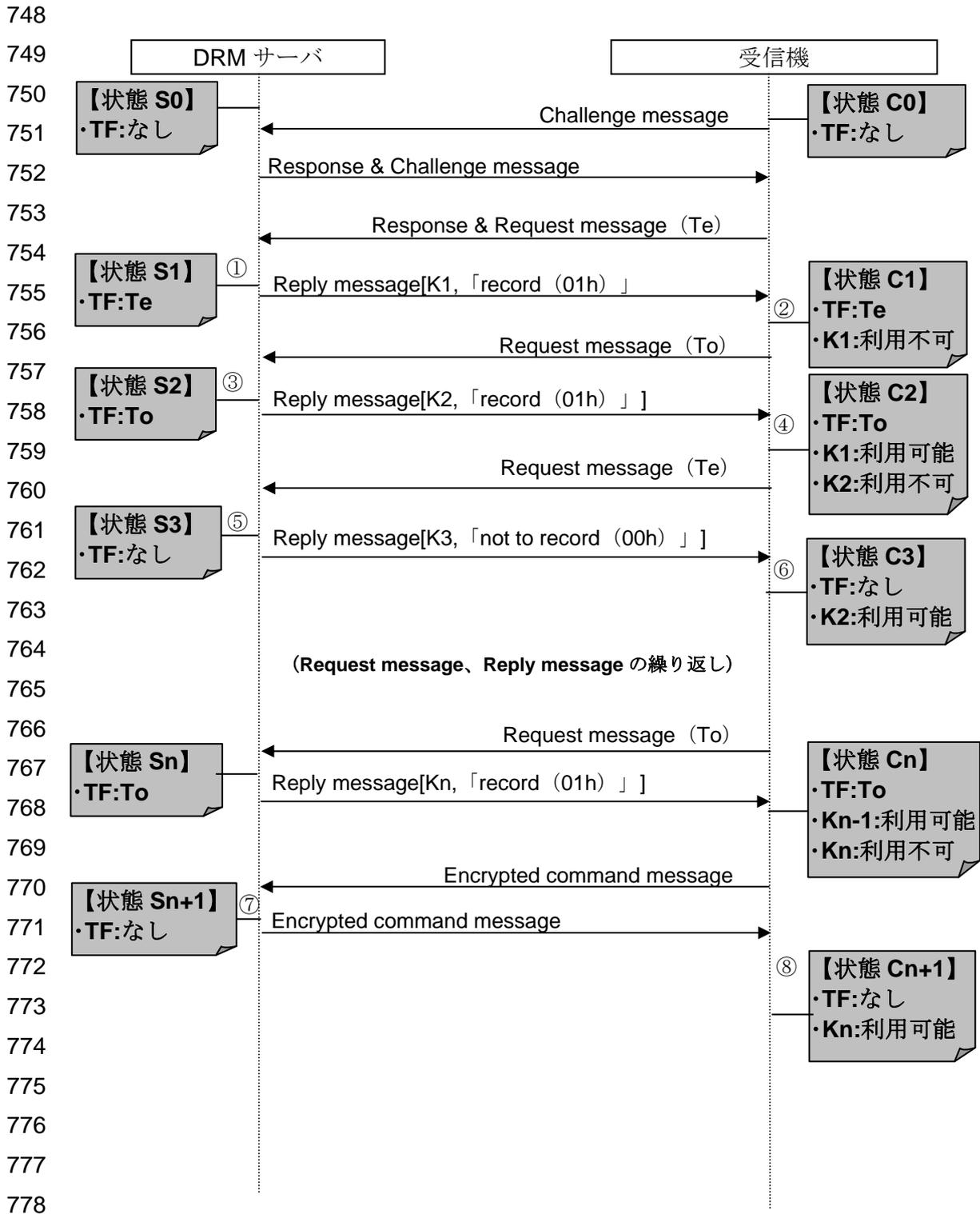


図 A-4 受信機と DRM サーバの不揮発性記憶領域の記憶状態

779

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		
DRM サーバ	受信機		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	II.記憶処理
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

780
781
782
783
784
785
786
787
788
789
790
791
792

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

793

794 **A.2.2 Reply messageの受信判断処理**

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

798

799 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
800 機における Reply message の受信状態の関係を以下に示す。

801

802 ● 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
803 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
804 TransactionFlag は異なる。

805 ➤ 例：図A-4でContentKeyがK2 のReply messageを送信中にSACが終了した
806 場合の状態S2 と状態C1。

807 ● 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
808 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
809 TransactionFlag は一致する。

810 ➤ 例：図A-4でContentKeyがK2 のReply messageを受信後、Request
811 messageを送信中にSACが終了した場合の状態S2 と状態C2。

812

813 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
814 TransactionFlag と Response & Commit message の TransactionFlag が異なる場合、
815 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
816 Reply message を受信していると判断する。

817

818 A.2.3 TransactionFlagの単独削除

819 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。

820

821 A.2.3.1受信機における単独削除

822 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
823 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
824 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
825 ContentKey の取得ができなくなる。

826 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
827 とで、新たな ContentKey を取得することができるようになる。

828 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
829 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、
830 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
831 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。

832 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。

833 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
834 きなくなる。

835

836 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
837 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
838 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
839 ContentKey を再取得できなくなることもあるため、削除しないことが望ましい。

840

841 ● 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
842 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
843 了しているため。

844 ● 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
845 バが ContentKey の送信を終了するため。

846

847 A.2.3.2DRM サーバにおける単独削除

848 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、
849 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。
850 Reply message の受信判断が不要になるのは、Reply message で送信した
851 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
852 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。

853

854 なお、DRM サーバが TransactionFlag を単独削除した後でも、TransactionFlag を記
855 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
856 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
857 ンツを利用することができる。

858

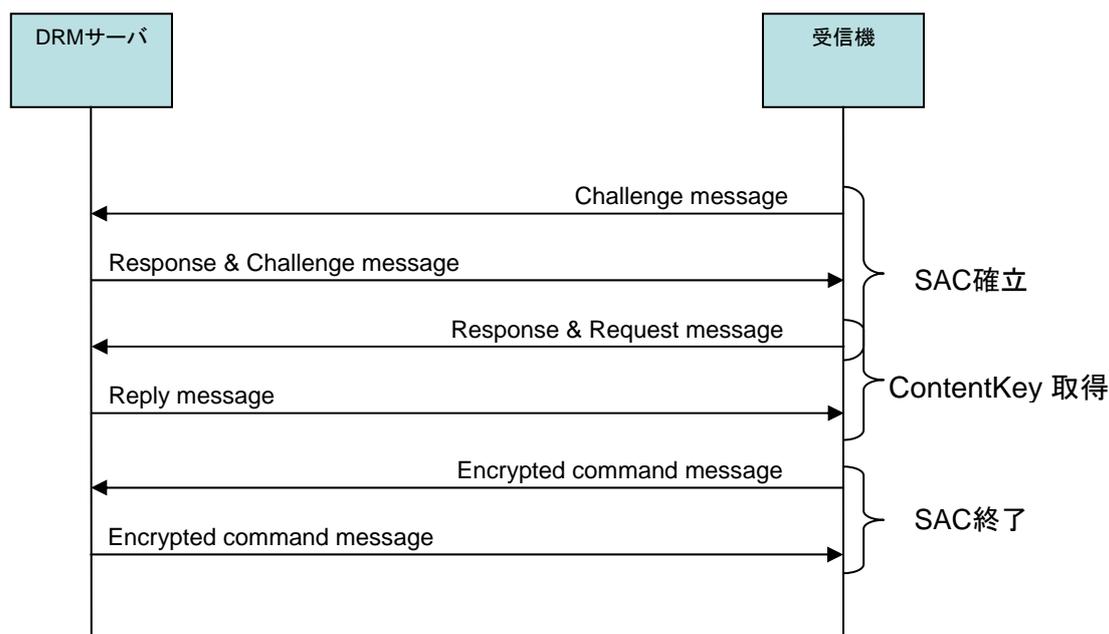
859 A.3 SACとService Protocolを用いたシーケンス

860 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
861 ContentKey 取得と Export のための ContentKey 取得を解説する。

862

863 **A.3.1 再生のためのContentKey取得**

864 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
 865 と RenderingObligation の取得を行う。
 866 取得された ContentKey には NotBefore、NotAfter が設定されているので、受信機は
 867 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
 868 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
 869 開始することができる。
 870 図A-5にDRMサーバ・受信機間のContentKey取得シーケンスを示す。
 871



872 図 A-5 再生のための ContentKey 取得シーケンス

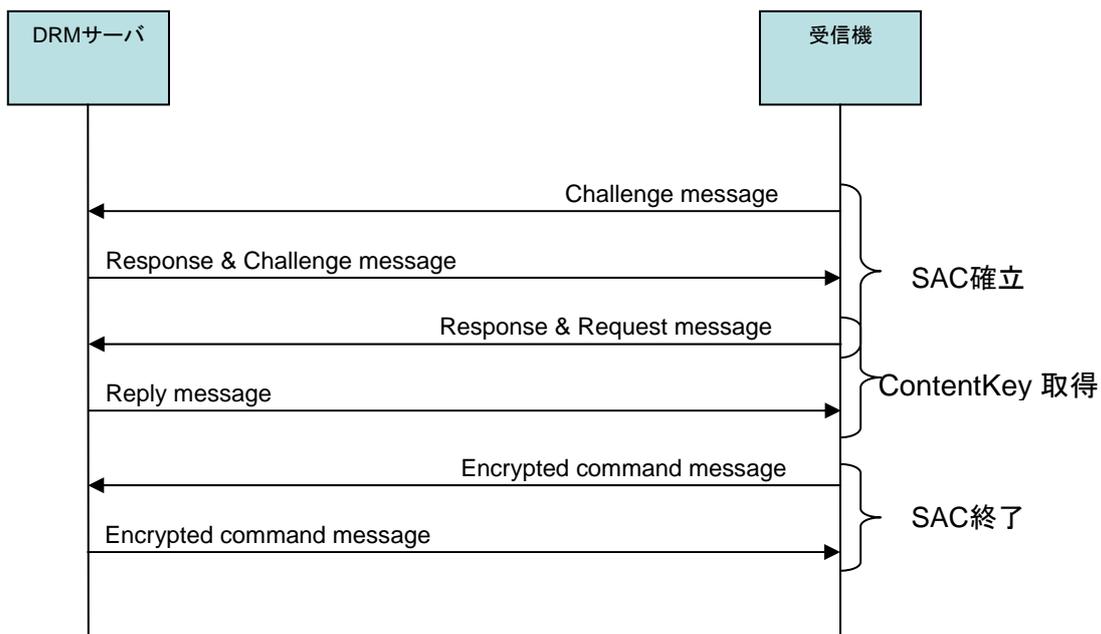
873
 874 ContentKey 取得シーケンスに先立ち、受信機が UsageRuleReference と DRM サー
 875 バの URI を取得・保持する。なお、UsageRuleReference や DRM サーバの URI の
 876 取得に関する仕様は本書では規定しない。
 877

- 878 1. SAC確立 : [MIPTV], 4.1 節Secure Authenticated Channel (SAC) Protocolで規定
 879 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
 880 を確立する。
- 881 2. ContentKey取得 : [MIPTV], 4.2.1 項Get Permission Protocolで規定されるプロト
 882 コルにより、受信機はContentKey取得要求を行い、DRMサーバからContentKey
 883 とそのNotBefore、NotAfter、RenderingObligationを取得する。なお、
 884 ContentKey取得のタイミングで、1つのService Protocolのメッセージで
 885 ContentKeyとDatetimeを同時に取得する場合、[MIPTV], 4.2.3 項Packed
 886 Message Protocolで規定されるプロトコルを用い、ContentKey取得とは別の
 887 Service ProtocolのメッセージでDatetimeを取得する場合、[MIPTV], 4.2.2 項Get
 888 Trusted Time Protocolで規定されるプロトコルを用いる。
- 889 3. SAC終了 : ContentKey取得後、[MIPTV], 4.1 節Secure Authenticated Channel
 890 (SAC) Protocolで規定されるプロトコルにより、DRMサーバはCommandが
 891 「ACK」のEncrypted command messageを送信した後に、受信機はCommand
 892 が「ACK」のEncrypted command messageを受信した後に、SACを終了する。

893 以上の ContentKey 取得シーケンスにより、受信機は ContentKey とその NotBefore、
894 NotAfter、対応する RenderingObligation を取得する。
895 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。
896 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
897 ーケンスとは独立であり、受信機は HTTP など取得する。ダウンロードしたコン
898 テンツは ContentKey を利用して復号再生される。この際、RenderingObligation に
899 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
900 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
901 の場合には、コンテンツの再生処理が停止される。

902 A.3.2 ExportのためのContentKey取得

903 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
904 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
905 のための ContentKey と ExportInfo の取得を行う。
906 この ContentKey と ExportInfo の取得は、Export 先の種類ごとに、Export の都度行
907 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。
908 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
909 あり、受信機は HTTP など取得する。
910 図A-6にDRMサーバ・受信機間のContentKey取得シーケンスを示す。
911



912

図 A-6 Export のための ContentKey 取得シーケンス

913 ContentKey 取得シーケンスに先立ち、受信機は UsageRuleReference と DRM サー
914 バの URI を取得・保持する。なお、UsageRuleReference や DRM サーバの URI の
915 取得に関する仕様は本書では規定しない。
916

917

- 918 1. SAC確立 : [MIPTV], 4.1 節Secure Authenticated Channel (SAC) Protocolで規定
919 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
920 を確立する。
- 921 2. ContentKey取得 : [MIPTV], 4.2.1 項Get Permission Protocolで規定されるプロト
922 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。

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

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

933

934 以上のContentKey取得シーケンスにより、受信機はContentKeyとExportInfoを取
935 得する。

936 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。

937

938 なお、[MIPTV], 4.2.3 項で規定されるPacked Message Protocolを用いて、再生およ
939 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
940 のTransactionFlagRecordFlagが「record (01h)」でTransactionFlagを不揮発性記
941 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
942 TransactionFlagと対応付けて利用不可の状態に記憶する。再生に用いるContentKey
943 については、TransactionFlagと対応付けて利用不可の状態に不揮発性記憶領域に記
944 憶せず、利用してもよい。

945

946 **A.4 メッセージの例**

947

948 **A.4.1 SACのメッセージの例**

949 本項ではSACのメッセージの例を示す。

950 なお、サイズの大きいパラメータ (SinkCertificate、SourceCertificate など) と演算
951 により生成するパラメータ (SourceEC-DHPhase1Value、Signature など) は、値
952 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
953 前の値を示す。

954

955 **A.4.1.1 Challenge message**

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

957

958 **A.4.1.2 Response & Challenge message**

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

960

961 **A.4.1.3 Response & Request message**

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

964

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.4.1.4 Request 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.4.1.5 Reply 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.4.1.6 Plain command message**

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

979

980 **A.4.1.7 Encrypted command message**

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

982

983 **A.4.1.8 Response & 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.4.2.1 Get 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)

1008

1009 **A.4.2.1.4 Get Permission Reply (EXPORT)**

1010 [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
1011 Permission Replyメッセージの例を表A-12に示す。

1012

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

1013

1014 **A.4.2.2 Get Trusted Time Protocol**

1015 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
1016 を示す。

1017

1018 **A.4.2.2.1 Get TrustedTime Request**

1019 Get Trusted Time Requestは、[IPTVESVOD], A.3.3.2.1 項と同等である。

1020

1021 **A.4.2.2.2 Get Trusted Time Reply**

1022 Get Trusted Time Replyは、[IPTVESVOD], A.3.3.2.2 項と同等である。

1023

1024 **A.4.2.3 Packed Message Protocol**

1025 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
1026 を示す。

- 1027 **A.4.2.3.1 Packed Message Request**
 1028 [MIPTV], 4.2.3.2 項で規定されるPacked Message Requestに格納するRequestが
 1029 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。
 1030

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

1031

- 1032 **A.4.2.3.2 Packed Message Reply**
 1033 [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
 1034 対して応答する場合の例を表A-14に示す。
 1035

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

1036