

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
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
45
46
47
48
49
50

Marlin IPTV-ES 運用仕様
IP マルチキャスト編

Document Version: 1.8
Final
Date: 30 September, 2015

Copyright © 2007-2015 ALL RIGHTS RESERVED
ソニー株式会社
パナソニック株式会社

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 Contents

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..... 5
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..... 6
59	1.6	ビットオーダー..... 6
60	2	SAC に関する規定..... 7
61	3	Service Protocol および ECM に関する規定..... 8
62	3.1	Get Permission Protocol..... 8
63	3.1.1	メッセージパラメータの設定..... 8
64	3.1.1.1	Get Permission Request parameters..... 8
65	3.1.1.2	Get Permission Reply parameters..... 9
66	3.1.2	メッセージパラメータの検証..... 9
67	3.1.2.1	Get Permission Request parameters..... 9
68	3.1.2.2	Get Permission Reply parameters..... 10
69	3.1.3	UsageRuleReference の設定..... 11
70	3.1.4	受信機における「WorkKey・SubscriptionTierBits・ExtractInfo」の
71		取得に関する処理..... 12
72	3.1.5	DRM サーバにおける「WorkKey・SubscriptionTierBits・ExtractInfo」の
73		送信に関する処理..... 12
74	3.2	Get Trusted Time Protocol..... 13
75	3.3	Packed Message Protocol..... 13
76	3.3.1	メッセージパラメータの設定..... 13
77	3.3.1.1	Packed Message Request parameters..... 13
78	3.3.1.2	Packed Message Reply parameters..... 15
79	3.3.2	メッセージパラメータの検証..... 15
80	3.3.2.1	Packed Message Request parameters..... 15
81	3.3.2.2	Packed Message Reply parameters..... 15
82	3.4	ECM に関する規定..... 15
83	3.4.1	CA_descriptor および ECM の送出..... 16
84	3.4.1.1	CA_descriptor の送出..... 16
85	3.4.1.2	ECM の送出..... 16
86	4	ネットワーク通信プロトコル (HTTP) に関する規定..... 17
87	A	Appendix (Informative)..... 18
88	A.1	コンテンツの利用シーケンス..... 18
89	A.1.1	「WorkKey・SubscriptionTierBits・ExtractInfo」の取得処理..... 18
90	A.1.1.1	ティアビット..... 19
91	A.1.1.2	WorkKeyManagementID..... 19
92	A.1.1.3	WorkKey (odd/even)..... 19
93	A.1.1.4	受信機における「WorkKey・SubscriptionTierBits・ExtractInfo」の管理..... 20
94	A.1.1.5	RenderingObligation による EXTRACT・RECORD・EXPORT..... 20
95	A.1.1.6	Packed Message Protocol による
96		「WorkKey・SubscriptionTierBits・ExtractInfo」の取得..... 20
97	A.1.2	コンテンツ受信時の ECM 処理..... 21
98	A.1.3	「WorkKey・SubscriptionTierBits・ExtractInfo」の更新処理..... 21
99	A.1.3.1	更新の有無と更新開始日時オフセット..... 21
100	A.1.3.2	「WorkKey・SubscriptionTierBits・ExtractInfo」の更新..... 21
101	A.2	WorkKeyID および UsageRuleReference の運用例..... 22
102	A.2.1	ティアビット・WorkKeyID・UsageRuleReference の関係..... 22
103	A.2.1.1	WorkKeyID とティアビットとの関係..... 22
104	A.2.1.2	UsageRuleReference と WorkKeyID との関係..... 22

105	A.2.1.3	ティアビットと WorkKeyID・UsageRuleReference の値との関係の例..	23
106	A.2.2	WorkKey を更新する運用における WorkKeyID と UsageRuleReference との	
107		関係の例.....	23
108	A.3	「WorkKey・SubscriptionTierBits・ExtractInfo」の更新運用の例.....	24
109	A.4	メッセージの例.....	35
110	A.4.1	Service Protocol のメッセージ例.....	35
111	A.4.1.1	Get Permission Protocol	35
112	A.4.1.1.1	Get Permission Request message	35
113	A.4.1.1.2	Get Permission Reply message.....	36
114	A.4.1.2	Get Trusted Time Protocol	36
115	A.4.1.3	Packed Message Protocol	36
116	A.4.1.1.3	Packed Message Request message	37
117	A.4.1.1.4	Packed Message Reply message.....	37
118			

119 1 はじめに

120 “Marlin IPTV End-point Service Specification” [MIPTV]では、暗号化されたコンテ
121 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
122 している。Indirect Key Delivery 方式は、様々なサービスへの適用が考えられるが、
123 最も典型的なコンテンツ配信形態としては、IP マルチキャストサービスが想定され
124 るため、本編を IP マルチキャスト編と呼ぶこととする。
125

126 1.1 本書の規定範囲

127 本書では、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
128 「EXTRACT with Indirect Key Delivery (02h)」の Get Permission Request と
129 [MIPTV], 6.1.2 項で規定される ECM で取得するコンテンツ（以下、本書では“コン
130 テンツ”と記す）の利用に関し、[MIPTV]に対する詳細規定項目と追加規定項目とを
131 規定する。

132 本書は、“Marlin IPTV-ES/J Specific Compliance Rules IP マルチキャスト編”
133 [IPTVCRMC]に準拠する Marlin IPTV-ES Device、Marlin IPTV-ES Server（以下、本
134 書ではそれぞれ“受信機”、“DRM サーバ”と記す）、および、ECM を送出する
135 サービス事業者に適用する。

136

137 以下に、本書の規定項目を示す。

138

139 ● [MIPTV]に対する詳細規定項目

140 ➤ SAC に関する規定 ([MIPTV], 4.1 節 Secure Authenticated Channel (SAC) 141 Protocol)

142 ☆ メッセージパラメータ

143 ☆ SAC タイムアウト

144 ☆ 1 つの TCP Connection を利用可能な SAC セッション

145 ☆ Response & Commit message

146

147 ➤ Service Protocol に関する規定 ([MIPTV], 4.2 節 Marlin IPTV-ES Service 148 Protocol over SAC に関する規定)

149 ☆ メッセージパラメータの設定

150 ☆ メッセージパラメータの検証

151 ☆ UsageRuleReference の設定

152 ☆ 受信機における WorkKey・WorkKeyID・PrivateData・

153 SubscriptionTierBits・ExtractInfo の取得に関する処理

154 ☆ DRM サーバにおける WorkKey・WorkKeyID・PrivateData・

155 SubscriptionTierBits・ExtractInfo の送信に関する処理

156

157 ➤ ECM に関する規定 ([MIPTV], 6.1.2 項 ECM format)

158 ☆ CA_descriptor および ECM の送出

159

160 ● [MIPTV]に対する追加規定項目

161 ➤ ネットワーク通信プロトコル (HTTP) に関する規定

162 ☆ HTTP による SAC のメッセージの伝送

163 ☆ HTTP ヘッダ

164

165 **1.2 引用文書**

[IPTVCRMC]	“Marlin IPTV-ES/J Specific Compliance Rules IP マルチキャスト編”, Version 1.8
[IPTVESVOD]	“Marlin IPTV-ES 運用仕様 VOD 編”, Version 1.4
[MIPTV]	“Marlin IPTV End-point Service Specification”, Version 1.0.2
[MP2S]	ISO/IEC 13818-1 “Information technology – Generic coding of moving pictures and associated audio information: Systems” Second edition 2000-12-01

166

167 **1.3 用語の定義**

168 本書で用いる用語を以下に定義する。

169

用語	定義
CA_descriptor	[MP2S], 2.6.16 項で規定される CA_descriptor。
更新開始日時オフセット	WorkKey・WorkKeyID・PrivateData・SubscriptionTierBits・ExtractInfo を更新する運用における、更新の開始日時（更新開始日時）の NotAfter からのオフセット時間（単位は分）。更新開始日時オフセットは、PrivateData ([MIPTV], 4.2.1.5 項で規定される StatusExtension の PrivateData) で指定する。
コンテンツ	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。

170

171 本書で用いる用語と[MIPTV]の用語との対応を以下に示す。

172

本書	[MIPTV]
DRM サーバ	Marlin IPTV-ES Server
受信機	Marlin IPTV-ES Device
チャンネル	Channel
ティアビット	Tier Bits

173

174 **1.4 略語**

175 本書で用いる略語を以下に示す。

176

略語	正式名称
LSB	Least Significant Bit
MSB	Most Significant Bit

177

178 **1.5 バイトオーダー**

179 本書で規定す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
180 ある。
181

182 **1.6 ビットオーダー**

183 本書で規定するプロトコルのビットオーダーは、“MSB First”である。
184

185 **2 SAC に関する規定**

186 Marlin IPTV-ES SAC の運用は、[IPTVESVOD], 2 章と同等である。

187

188 **3 Service Protocol および ECM に関する規定**

189 本章では、Marlin IPTV-ES Service Protocol および ECM の運用を規定する。
190 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
191 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。
192

193 **3.1 Get Permission Protocol**

194 [MIPTV], 4.2 節で規定される Get Permission Protocol は、WorkKey・WorkKeyID・
195 PrivateData・SubscriptionTierBits・ExtractInfo の取得に用いる。以降、Get
196 Permission Protocol で取得する一組の WorkKey・WorkKeyID・PrivateData・
197 SubscriptionTierBits・ExtractInfo を示す場合、かぎかっこを付与して「WorkKey・
198 SubscriptionTierBits・ExtractInfo」などと表記する。
199 本節では、以下の項目を規定する。

- 200
- 201 ● メッセージパラメータの設定
- 202 ● メッセージパラメータの検証
- 203 ● UsageRuleReference の設定
- 204 ● 受信機における「WorkKey・SubscriptionTierBits・ExtractInfo」の取得に関する
205 処理
- 206 ● DRM サーバにおける「WorkKey・SubscriptionTierBits・ExtractInfo」の送信に
207 関する処理
- 208

209 なお、DRM サーバは、同時期に一对となる 2 つの WorkKey (odd) と WorkKey
210 (even) とを常に発行する運用をおこなうこととする。よって、受信機は、
211 「WorkKey・SubscriptionTierBits・ExtractInfo」を取得する場合、一对となる 2 つ
212 の WorkKey (odd) と WorkKey (even) とを取得することとする。
213 以降、2 つの Get Permission Reply で同時期に取得する同一 ServiceProviderID・同
214 一 WorkKeyManagementID の WorkKey (odd) と WorkKey (even) の組、または、
215 Packed Message Reply で同時に取得する同一 ServiceProviderID・同一
216 WorkKeyManagementID の WorkKey (odd) と WorkKey (even) の組を示す場合、
217 “一对の” という表記を加え、“一对の WorkKey”、“一对の WorkKey (odd) と
218 WorkKey (even)”などと表記する。
219

220 **3.1.1 メッセージパラメータの設定**

221 受信機および 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
222 る。
223

224 **3.1.1.1 Get Permission Request parameters**

225 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
226 メッセージパラメータを設定する。

- 227
- 228 ● UsageRuleReference
 - 229 ➤ 事前に取得する UsageRuleReference を設定する。UsageRuleReference の
230 規定については、3.1.3 項を参照のこと。
 - 231

232 3.1.1.2 Get Permission Reply parameters

233 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
234 Permission Reply のメッセージパラメータを設定する。

235

- 236 ● Status

- 237 > 3.1.2.1 項を参照のこと。

- 238 ● WorkKeyID

- 239 > 同一 ServiceProviderID かつ同一 WorkKeyManagementID の WorkKey に関
240 し、同時期に発行する一対の WorkKey (odd) と WorkKey (even) の
241 WorkKeyVersion には連続した値を設定する。WorkKeyVersion が 255
242 (FFh) と 0 (00h) とである場合は、連続した値とみなす
243 なお、WorkKeyID の運用例については、A.2 節を参照のこと。

- 244 ● PrivateData

- 245 > 同一 ServiceProviderID かつ同一 WorkKeyManagementID の WorkKey に関
246 し、同時期に発行する一対の WorkKey (odd) と WorkKey (even) の
247 PrivateData には、送信する「WorkKey・SubscriptionTierBits・ExtractInfo」
248 の次の更新有無および次の更新における NotAfter から更新開始日時ま
249 でのオフセット時間（更新開始日時オフセット、単位は分）として、同一
250 の値を設定する。

251 なお、更新開始日時の詳細については、3.1.4 項の式(3.1)を参照のこと。

- 252 ◇ 次回の更新をおこなう場合、更新開始日時オフセットの値に 0001h (1
253 分) ~FFFFh (65535 分) を設定する。ただし、NotAfter の値が
254 0000FFFFh (更新開始日時オフセットの最大値) ~FFFFFFFEh である
255 場合のみ設定可である。

- 256 ◇ 次回の更新をおこなわない場合、更新開始日時オフセットの値に 0000h
257 を設定する。NotAfter の値が FFFFFFFFh である場合は、更新開始日時
258 オフセットの値に 0000h を設定する。

- 259 ● SubscriptionTierBits

- 260 > 同一 ServiceProviderID かつ同一 WorkKeyManagementID の WorkKey に関
261 し、同時期に発行する一対の WorkKey (odd) と WorkKey (even) の
262 SubscriptionTierBits には同一の値を設定する。

- 263 ● NotBefore/NotAfter

- 264 > 同一 ServiceProviderID かつ同一 WorkKeyManagementID の WorkKey に関
265 し、同時期に発行する一対の WorkKey (odd) と WorkKey (even) の
266 NotBefore には、同一の値を設定する。同様に、同時期に発行する一対の
267 WorkKey (odd) と WorkKey (even) の NotAfter には、同一の値を設定す
268 る。

269

270 3.1.2 メッセージパラメータの検証

271 DRM サーバおよび受信機は、以下の規定に従い、メッセージ受信時にメッセージパ
272 ラメータを検証する。

273

274 3.1.2.1 Get Permission Request parameters

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

277

278

- 279 ● ActionID
- 280 † ActionID が、以下に示す値の場合には検証失敗としない。
- 281 † EXTRACT with Indirect Key Delivery (02h)
- 282

283 3.1.2.2 Get Permission Reply parameters

284 受信機は、[MIPTV], 4.2.4.2 項、4.2.4.4 項および以下の規定に従い、Get Permission
285 Reply のメッセージパラメータを検証する。

286 受信機は、以下の検証の成功後に、一对の「WorkKey・SubscriptionTierBits・
287 ExtractInfo」を使用することとし、なお、受信機は検証に失敗した場合は、一对の
288 WorkKey として取得した 2 つの「WorkKey・SubscriptionTierBits・ExtractInfo」の
289 両方を使用しない。

290 また、受信機は保持する一对の「WorkKey・SubscriptionTierBits・ExtractInfo」と同
291 一 ServiceProviderID・同一 WorkKeyManagementID の一对の「WorkKey・
292 SubscriptionTierBits・ExtractInfo」を取得した場合、以下の検証の成功後に、
293 [MIPTV], 6.1.3 項の規定にしたがい一对の「WorkKey・SubscriptionTierBits・
294 ExtractInfo」を更新する。

- 295
- 296 ● WorkKeyID
- 297 † 一对の WorkKey (odd)・WorkKey (even) として取得した 2 つの
- 298 WorkKey が、同一 ServiceProviderID かつ同一 WorkKeyManagementID の
- 299 一对の WorkKey (odd) と WorkKey (even) であることを検証する。
- 300 したがって、取得した 2 つの WorkKeyID の値が以下の条件のいずれかに該
- 301 当する場合、検証失敗とする。
- 302 † ServiceProviderID・ReservedByte (WorkKeyID の上位 3 バイト目)・
- 303 WorkKeyManagementID のいずれかの値が異なる場合
- 304 † WorkKeyVersion の値が連続した値でない場合。ただし、2 つの
- 305 WorkKeyVersion の値が 255 (FFh) と 0 (00h) である場合は、連続し
- 306 た値とみなすこと。
- 307 † PrivateData (更新開始日時オフセット) の値が 0001h~FFFFh (更新され
- 308 る) である「WorkKey・SubscriptionTierBits・ExtractInfo」を更新する場合
- 309 において、更新前後の WorkKey (odd)・WorkKey (even) が、同一
- 310 ServiceProviderID かつ同一 WorkKeyManagementID の WorkKey であるこ
- 311 とを検証する。
- 312 したがって、更新前後の WorkKey (odd) または WorkKey (even) の
- 313 WorkKeyID の値が以下の条件に該当する場合、検証失敗とする。
- 314 † ServiceProviderID・ReservedByte・WorkKeyManagementID のいずれ
- 315 かの値が異なる場合
- 316 ● PrivateData
- 317 † 一对の WorkKey (odd)・WorkKey (even) として取得した 2 つの
- 318 WorkKey の PrivateData (更新開始日時オフセット) の値が異なる場合、検
- 319 証失敗とする。
- 320 ● SubscriptionTierBits
- 321 † 一对の WorkKey (odd)・WorkKey (even) として取得した 2 つの
- 322 WorkKey の SubscriptionTierBits の値が異なる場合、検証失敗とする。
- 323 ● NotBefore/NotAfter
- 324 † 一对の WorkKey (odd)・WorkKey (even) として取得した 2 つの
- 325 WorkKey の NotBefore の値が異なる場合、検証失敗とする。
- 326 同様に、2 つの WorkKey の NotAfter の値が異なる場合、検証失敗とする。

327 ▶ PrivateData（更新開始日時オフセット）の値が 0001h～FFFFh（更新され
328 る）である WorkKey に関して、NotAfter（単位は分）の値が 0000FFFFh
329 （更新開始日時オフセットの最大値）よりも小さい場合、または、
330 FFFFFFFFh（期限なし）である場合、検証失敗とする。
331 更新開始日時オフセットの詳細については、3.1.4 項の式(3.1)を参照のこと。
332

333 3.1.3 UsageRuleReference の設定

334 UsageRuleReference の設定は、表 3-1 に示す通りとする。
335 UsageRuleReference は、上位 6 バイトの値のみを規定し、下位 10 バイトの値は規
336 定しない。すなわち、UsageRuleReference の下位 10 バイトの値は、サービス事業
337 者の運用により任意の値を設定して良い。
338 UsageRuleReference の上位 6 バイトは、“ServiceProviderID”、
339 “ReservedByte”、“WorkKeyManagementID”、および“odd/evenID”から構成
340 される。UsageRuleReference の運用例については、A.2 節を参照のこと。
341 なお、表 3-1 のバイトインデックスの値は、UsageRuleReference の最上位バイトか
342 らの相対値である。
343 また、以降では、「WorkKey (odd)・SubscriptionTierBits・ExtractInfo」に対応す
344 る UsageRuleReference を“UsageRuleReference (odd)”、「WorkKey
345 (even)・SubscriptionTierBits・ExtractInfo」に対応する UsageRuleReference を
346 “UsageRuleReference (even)”と表記する。
347

表 3-1 UsageRuleReference の設定

バイト インデ ックス	パラメータ	パラメータの説明	パラメータ値の規定
0-1	ServiceProvider ID	・ [MIPTV], 4.2.1.5.1 項 で規定される ServiceProviderID であ る。	・ UsageRuleReference に対応 する WorkKey の ServiceProviderID と同一の値 を設定する。
2	ReservedByte	・ [MIPTV], 4.2.1.5.1 項 で規定される ReservedByte である。	・ UsageRuleReference に対応 する WorkKey の ReservedByte と同一の値 (00h) を設定す る。
3-4	WorkKey ManagementID	・ [MIPTV], 4.2.1.5.1 項 で規定される WorkKeyManagement ID である。	・ UsageRuleReference に対応 する WorkKey の WorkKeyManagementID と同一 の値を設定する。
5	odd/evenID	・ [MIPTV], 4.2.1.5.1 項 で規定される WorkKeyVersion の LSB の値である。	・ LSB に UsageRuleReference に対応する WorkKey の WorkKeyVersion の LSB と同一 の値を設定する。 ・ 上位 1 ビット目から上位 7 ビ ット目までは 0b を設定する。

3.1.4 受信機における「WorkKey・SubscriptionTierBits・ExtractInfo」の取得に関する処理

受信機は、「WorkKey・SubscriptionTierBits・ExtractInfo」の取得に関して、
[MIPTV], 4.2.4.4 項および以下の規定に従い処理をおこなう。

- 受信機は、「WorkKey・SubscriptionTierBits・ExtractInfo」の取得時には、事前に取得する UsageRuleReference (odd) ・ UsageRuleReference (even) を用いて、同一 ServiceProviderID かつ同一 WorkKeyManagementID の一対の「WorkKey (odd) ・ SubscriptionTierBits ・ ExtractInfo」と「WorkKey (even) ・ SubscriptionTierBits ・ ExtractInfo」とを取得する。
- 受信機は、取得した一対の WorkKey (odd) ・ WorkKey (even) の更新開始日時オフセット (StatusExtension の PrivateData) の値が 0001h~FFFFh (更新される) である「WorkKey・SubscriptionTierBits・ExtractInfo」の更新の制御をおこなう場合は、以下に従う。
 - 受信機は、WorkKey (odd) または WorkKey (even) の NotAfter および更新開始日時オフセットの値を用いて、式(3.1)に従い更新開始日時 (単位は分) を算出する。更新開始日時オフセットの値は、NotAfter (単位は分) から更新開始日時までのオフセット時間 (単位は分) を示す。

$$\text{(更新開始日時)} = \text{(NotAfter)} - \text{(更新開始日時オフセット)} \cdots (3.1)$$

- 受信機は、式(3.1)により算出した更新開始日時以降、DRM サーバから一対の更新された「WorkKey・SubscriptionTierBits・ExtractInfo」を取得することができる。更新開始日時以降、受信機は速やかに更新することが望ましい。
- 受信機は、取得した一対の WorkKey (odd) ・ WorkKey (even) の更新開始日時オフセットの値が 0000h (更新されない) である場合は、当該「WorkKey・SubscriptionTierBits・ExtractInfo」の更新の制御はおこなわない。

3.1.5 DRM サーバにおける「WorkKey・SubscriptionTierBits・ExtractInfo」の送信に関する処理

DRM サーバは、「WorkKey・SubscriptionTierBits・ExtractInfo」の送信に関して、以下の規定に従い処理をおこなう。

- DRM サーバは、同一 ServiceProviderID かつ同一 WorkKeyManagementID の WorkKey に関し、同時期に一対の WorkKey を発行する運用をおこなうこと。すなわち、DRM サーバは、同一 ServiceProviderID かつ同一 WorkKeyManagementID の WorkKey に関して、受信機から「WorkKey (odd) ・ SubscriptionTierBits ・ ExtractInfo」または「WorkKey (even) ・ SubscriptionTierBits ・ ExtractInfo」の要求を受信した場合、対応する「WorkKey・SubscriptionTierBits・ExtractInfo」を送信する。
 - このとき DRM サーバは、WorkKey (odd) または WorkKey (even) のいずれか一方は、WorkKey の送信時点で ECM を暗号化する WorkKey を送信する。
- サービス事業者が、ServiceProviderID および WorkKeyManagementID で特定される「WorkKey・SubscriptionTierBits・ExtractInfo」を更新する運用をおこなう場合、DRM サーバは、当該「WorkKey・SubscriptionTierBits・ExtractInfo」の

395 受信機ごとの更新開始日時以降に当該受信機からの要求を受信した場合、少な
396 くとも NotAfter の値を更新した「WorkKey・SubscriptionTierBits・ExtractInfo」
397 を送信する。
398 ▶ DRM サーバは、3.1.4 項の式(3.1)に従い、受信機ごとの更新開始日時を算
399 出する。式(3.1)の NotAfter は、当該「WorkKey・SubscriptionTierBits・
400 ExtractInfo」に関して、当該受信機に対して最後に送信した WorkKey の
401 NotAfter の値を用いる。
402

403 **3.2 Get Trusted Time Protocol**

404 [MIPTV], 4.2.2 項で規定される Get Trusted Time Protocol は、Datetime の取得に用
405 いる。
406 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
407 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
408 Trusted Time Reply のメッセージパラメータを検証する。
409 DRM サーバは、[MIPTV], 4.2.4.9 項の規定に従い、Get Trusted Time Request のメ
410 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
411 に従い、Get Trusted Time Reply のメッセージパラメータを設定する。
412

413 **3.3 Packed Message Protocol**

414 [MIPTV], 4.2.3 項で規定される Packed Message Protocol は、以下のパラメータを同
415 時に取得する場合に用いる。

- 416
- 417 ● 1 または複数の “一対の「WorkKey (odd)・SubscriptionTierBits・ExtractInfo」
418 と「WorkKey (even)・SubscriptionTierBits・ExtractInfo」”
- 419 ● 1 または複数の “一対の「WorkKey (odd)・SubscriptionTierBits・ExtractInfo」
420 と「WorkKey (even)・SubscriptionTierBits・ExtractInfo」”
421 および Datetime
- 422

423 本節では、以下の項目を規定する。

- 424
- 425 ● メッセージパラメータの設定
- 426 ● メッセージパラメータの検証
- 427

428 **3.3.1 メッセージパラメータの設定**

429 受信機および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。
430

431 **3.3.1.1 Packed Message Request parameters**

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

- 434
- 435 ● RequestMessageBoxList
- 436 ▶ RequestMessageBoxList には、表 3-2 に示す順番で RequestMessage を格
437 納する。
- 438 ☆ RequestMessage の個数は $(2 \times N)$ 個または $(2 \times N + 1)$ 個とする。
439 ここで、N は 16 以下の自然数である。

440 (2×M-1) 番目と (2×M) 番目の RequestMessage には、同一
 441 ServiceProviderID・同一 WorkKeyManagementID の「WorkKey・
 442 SubscriptionTierBits・ExtractInfo」を取得するための Get Permission
 443 Request (UsageRuleReference の ServiceProviderID・
 444 WorkKeyManagementID が同一の値) を格納する。ここで、M は N 以
 445 下の自然数である。
 446 なお、以降、N または M を用いた RequestMessage の個数および順番
 447 の表記については「×」を省略し、(2×N) を (2N) などと記す。
 448 ☆ (2M-1) 番目の RequestMessage には「WorkKey (odd)・
 449 SubscriptionTierBits・ExtractInfo」を、(2M) 番目の
 450 RequestMessage には「WorkKey (even)・SubscriptionTierBits・
 451 ExtractInfo」を取得するための Get Permission Request を格納する。
 452 ☆ RequestMessage の個数が (2N+1) 個の場合、(2N+1) 番目の
 453 RequestMessage には Get Trusted Time Request を格納する。
 454

表 3-2 RequestMessageBoxList に格納可能な
RequestMessage の組み合わせ

Request Message の個数	1 番目の Request Message	2 番目の Request Message	...	(2M-1) 番 目 *5 の Request Message *6	(2M) 番目 *5 の Request Message *6	...	(2N+1) 番 目 *5 の Request Message
2N *5	Get Permission Request *1 ActionID : EXTRACT with Indirect Key Delivery (02h) UsageRuleRe ference : UsageRuleRe ference (odd) *3	Get Permission Request *1 ActionID : EXTRACT with Indirect Key Delivery (02h) UsageRuleRe ference : UsageRuleRe ference (even) *4	...	Get Permission Request *1 ActionID : EXTRACT with Indirect Key Delivery (02h) UsageRuleRe ference : UsageRuleRe ference (odd) *3	Get Permission Request *1 ActionID : EXTRACT with Indirect Key Delivery (02h) UsageRuleRe ference : UsageRuleRe ference (even) *4	...	
2N+1 *5	Get Permission Request *1 ActionID : EXTRACT with Indirect Key Delivery (02h) UsageRuleRe ference : UsageRuleRe ference (odd) *3	Get Permission Request *1 ActionID : EXTRACT with Indirect Key Delivery (02h) UsageRuleRe ference : UsageRuleRe ference (even) *4	...	Get Permission Request *1 ActionID : EXTRACT with Indirect Key Delivery (02h) UsageRuleRe ference : UsageRuleRe ference (odd) *3	Get Permission Request *1 ActionID : EXTRACT with Indirect Key Delivery (02h) UsageRuleRe ference : UsageRuleRe ference (even) *4	...	Get Trusted Time Request *2

455
 456 *1 : メッセージパラメータの設定については、3.1.1 項を参照のこと。

- 457 *2: メッセージパラメータの設定については、3.2 項を参照のこと。
458 *3: 「WorkKey (odd) ・ SubscriptionTierBits ・ ExtractInfo」に対応する
459 UsageRuleReference (odd/evenID の値が 01h) を示す。詳細は 3.1.3 項を参
460 照のこと。
461 *4: 「WorkKey (even) ・ SubscriptionTierBits ・ ExtractInfo」に対応する
462 UsageRuleReference (odd/evenID の値が 00h) を示す。詳細は 3.1.3 項を参
463 照のこと。
464 *5: $N \leq 16$ 、 $M \leq N$ (N 、 M はともに自然数) とする。
465 *6: $(2M-1)$ 番目と $(2M)$ 番目の RequestMessage の UsageRuleReference は、
466 同一 ServiceProviderID ・ 同一 WorkKeyManagementID とする。
467

468 3.3.1.2 Packed Message Reply parameters

469 DRM サーバは、[MIPTV], 4.2.3.3 項の規定に従い、Packed Message Reply のメッセ
470 ージパラメータを設定する。
471

472 3.3.2 メッセージパラメータの検証

473 DRM サーバおよび受信機は、以下の規定に従い、メッセージ受信時にメッセージパ
474 ラメータを検証する。
475

476 3.3.2.1 Packed Message Request parameters

477 DRM サーバは、[MIPTV], 4.2.4.11 項および以下の規定に従い、Packed Message
478 Request のメッセージパラメータを検証する。
479

- 480 ● RequestMessageBoxList
 - 481 ➤ RequestMessageBoxList に ActionID が「EXTRACT with Indirect Key
 - 482 Delivery (02h)」の Get Permission Request の RequestMessage が 1 以上
 - 483 格納されている場合、かつ、RequestMessage の組み合わせが表 3-2 の組
 - 484 合せ以外の場合には検証失敗とし、Packed Message Reply parameter の
 - 485 Status を「Message format error (8009h)」とする。
486

487 3.3.2.2 Packed Message Reply parameters

488 受信機は、[MIPTV], 4.2.4.12 項および以下の規定に従い、Packed Message Reply
489 のメッセージパラメータを検証する。
490

- 491 ● ReplyMessageBoxList
 - 492 ➤ Status が「Success (0000h)」の場合には、3.1.2.2 項にしたがい、
 - 493 ReplyMessageBoxList に格納された ReplyMessage を検証する。
 - 494 ReplyMessageBoxList に格納されたいずれかの ReplyMessage の検証に失
 - 495 敗した場合には、Packed Message Reply 全体を検証失敗とする。
496

497 3.4 ECM に関する規定

498 本節では、[MIPTV], 6.1.2 項で規定される ECM format に関する運用を規定する。
499

- 500 ● CA_descriptor および ECM の送出

501 **3.4.1 CA_descriptor および ECM の送出**

502 **3.4.1.1 CA_descriptor の送出**

- 503 ● [MP2S], 2.6.16 項で規定される CA_descriptor は、[MP2S], 2.4.4.8 項で規定され
504 る PMT の第 1 ループにのみ配置する。すなわち、ES (Elementary Stream) ご
505 と異なる ECM を適用する運用はおこなわない。
- 506 ● CA_descriptor の descriptor_tag の値は、09h とする。
- 507 ● CA_descriptor の CA_system_ID の値は TBD。
- 508

509 **3.4.1.2 ECM の送出**

- 510 ● ECM の更新
- 511 ➤ ECM の更新間隔は、10 秒以上とする。
- 512 ● ECM の再送
- 513 ➤ ECM の再送間隔は、最小 100ms ・最大 1000ms とする。推奨値は 100ms
- 514 とする。
- 515

516 **4 ネットワーク通信プロトコル (HTTP) に関する規定**

517 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
518 である。

519

520 A Appendix (Informative)

521 A.1 コンテンツの利用シーケンス

522 本節では、コンテンツの利用に関して、受信機と DRM サーバとの間、および受信
523 機とコンテンツを配信するコンテンツサーバとの間のシーケンスの概要について説
524 明する。

525
526 コンテンツの利用シーケンスは、以下に示す 3 つの処理により構成される。

- 527
- 528 ① 「WorkKey・SubscriptionTierBits・ExtractInfo」の取得処理
- 529 ② コンテンツ受信時の ECM 処理
- 530 ③ 「WorkKey・SubscriptionTierBits・ExtractInfo」の更新処理

531
532 なお、以下の処理の事前に契約処理が行われ、受信機が「WorkKey・
533 SubscriptionTierBits・ExtractInfo」の取得のための UsageRuleReference・DRM サ
534 ーバの URI を取得済みであることを前提とする。

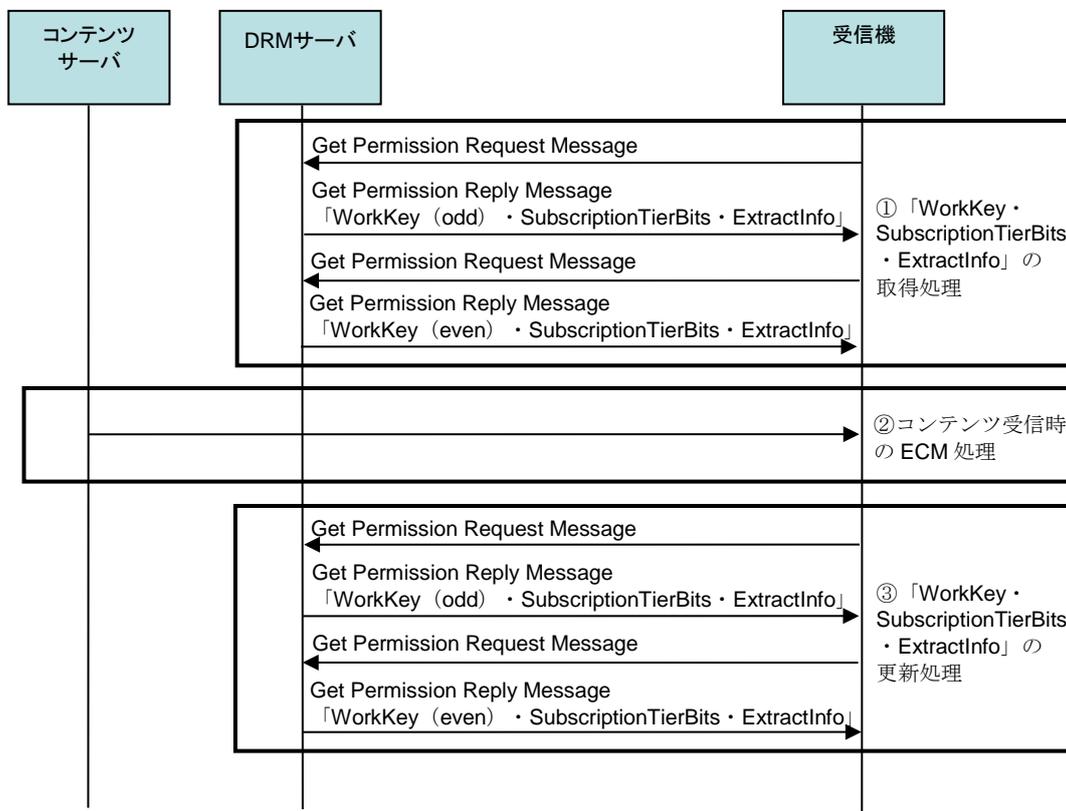


図 A-1 コンテンツの利用シーケンス

557

558 A.1.1 「WorkKey・SubscriptionTierBits・ExtractInfo」の取得処理

559 受信機は、[MIPTV], 4.1 節で規定される Secure Authenticated Channel (SAC)
560 Protocol により SAC を確立した上で、[MIPTV], 4.2.1 項で規定される Get
561 Permission Protocol により、DRM サーバから「WorkKey・SubscriptionTierBits・
562 ExtractInfo」を取得する。

563 なお、Get Permission Protocol によるメッセージシーケンスは、[IPTVESVOD], A.2
564 節の ContentKey 取得シーケンスと同様である。
565

566 A.1.1.1 ティアビット

567 「WorkKey・SubscriptionTierBits・ExtractInfo」に関して、DRM サーバと受信機と
568 の間の通信回数・受信機での保持数の削減のため、サービス事業者の 1 以上のチャ
569 ネルに対して同一の WorkKey を適用する運用が想定される。そこで、受信機が有す
570 る契約に応じたチャンネルの視聴制御のため、ティアビットとよばれる 64 ビットのビ
571 ット列を用いる。ティアビットの各ビットには、各チャンネルに対する契約が対応づ
572 けられる。この対応づけは、サービス事業者の運用依存である。
573 DRM サーバは、WorkKey とともに、ティアビットのうち受信機が有する契約に対
574 応するビットを示す “SubscriptionTierBits” を受信機に送信する。一方、ECM には、
575 ティアビットのうち当該チャンネルに対する契約を示す “ChannelTierBits” が設定さ
576 れる。受信機は、SubscriptionTierBits と ChannelTierBits との照合により、受信機が
577 契約を有するチャンネルのみを視聴可とするよう制御する。受信機でのティアビット
578 による視聴制御については A.1.2 項を参照のこと。
579

580 A.1.1.2 WorkKeyManagementID

581 A.1.1.1 項で説明したティアビットを用いる運用を実現するため、サービス事業者は、
582 複数チャンネルに適用する WorkKey と、当該複数チャンネルに対する契約を対応づけた
583 ティアビットとの対応を管理する。この WorkKey およびティアビットの管理単位を
584 特定する識別子を “WorkKeyManagementID” とよぶ。WorkKeyManagementID は、
585 サービス事業者ごと (“ServiceProviderID” で識別される) に割り当てる識別子で
586 ある。
587 受信機は、ServiceProviderID および WorkKeyManagementID の単位で、DRM サー
588 バから「WorkKey・SubscriptionTierBits・ExtractInfo」を取得する。したがって、受
589 信機が取得時に指定する UsageRuleReference には、ServiceProviderID と
590 WorkKeyManagementID とが含まれる。なお、WorkKeyManagementID および
591 UsageRuleReference の運用例については、A.2 節を参照のこと。
592

593 A.1.1.3 WorkKey (odd/even)

594 コンテンツに対して、一定期間などで ECM を暗号化する WorkKey を更新する運用
595 が想定される。
596 このような運用において、WorkKey の更新時でも受信機が ECM を連続して復号し、
597 継続視聴が可能となるように、DRM サーバは同時期に一对となる 2 つの WorkKey
598 を発行する。この一对となる 2 つの WorkKey を、“WorkKey (odd)” および
599 “WorkKey (even)” とよぶ。WorkKey (odd) と WorkKey (even) は、
600 WorkKeyID に含まれる WorkKeyVersion の LSB の値 (odd/evenID) により識別でき
601 る。WorkKeyVersion の詳細については[MIPTV], 4.2.1.5.1 項を、運用例については
602 A.2 節を参照のこと。
603 また、DRM サーバは、一对の WorkKey (odd) ・ WorkKey (even) として、
604 WorkKey の送出時点で ECM を暗号化する WorkKey と、ECM を暗号化する
605 WorkKey の次回更新後の WorkKey とを送信する。
606 受信機は、2 つの Get Permission Protocol を用いて、DRM サーバから odd/even の
607 「WorkKey・SubscriptionTierBits・ExtractInfo」を個別に取得する。したがって、
608 DRM サーバが、odd/even のどちらの WorkKey を発行すればよいかを特定できるよ

609 うに、UsageRuleReference には要求する WorkKey の odd/evenID の値が設定され
610 る。
611

612 **A.1.1.4 受信機における「WorkKey・SubscriptionTierBits・ExtractInfo」の管理**

613 受信機は、ServiceProviderID・WorkKeyManagementID の単位で、取得した一对の
614 「WorkKey・SubscriptionTierBits・ExtractInfo」を管理する。受信機は
615 「WorkKey・SubscriptionTierBits・ExtractInfo」として、少なくとも WorkKey、
616 WorkKeyID、更新開始日時オフセット (PrivateData)、SubscriptionTierBits、
617 NotBefore/NotAfter を管理する。
618 [MIPTV], 4.2.4.4 項で規定される通り、受信機は、保持する WorkKey と
619 “ServiceProviderID”、“ReservedByte”、“WorkKeyManagementID”、および
620 “odd/evenID (WorkKeyVersion の LSB)” の 4 つの値が一致する WorkKey を新
621 たに取得した場合、取得した「WorkKey・SubscriptionTierBits・ExtractInfo」で、保
622 持する「WorkKey・SubscriptionTierBits・ExtractInfo」を更新する。このとき、受信
623 機は、ServiceProviderID・WorkKeyManagementID の単位での「WorkKey・
624 SubscriptionTierBits・ExtractInfo」の管理にあわせて、一对の「WorkKey・
625 SubscriptionTierBits・ExtractInfo」の単位で更新する。ただし、更新前後で値が同一
626 であるパラメータについては更新しなくても良い。
627 なお、取得した「WorkKey・SubscriptionTierBits・ExtractInfo」を不揮発性記憶領域
628 に記録するか否かについては、受信機の実装依存である。ただし、受信機は、揮発
629 性記憶領域に保持する「WorkKey・SubscriptionTierBits・ExtractInfo」の電源断など
630 による消失を防止し、DRM サーバからの再取得を不要とするため、不揮発性記憶領
631 域に記録することが望ましい。
632

633 **A.1.1.5 RenderingObligation による EXTRACT・RECORD・EXPORT**

634 受信機は、[MIPTV], 6.1.2 項で規定される ECM の RenderingObligation に基づき、
635 コンテンツの EXTRACT、RECORD、および EXPORT をおこなう。受信機は、
636 [MIPTV], 4.2.1 項で規定される RecordInfo および ExportInfo は取得しない。
637 RenderingObligation の送込に関する遵守規則、および、RenderingObligation に基づ
638 く受信機における EXTRACT・RECORD・EXPORT に関する遵守規則については、
639 [IPTVCRMC], 2 章を参照のこと。
640

641 **A.1.1.6 Packed Message Protocol による「WorkKey・SubscriptionTierBits・ 642 ExtractInfo」の取得**

643 受信機は、[MIPTV], 4.2.3 項で規定される Packed Message Protocol を用いて、1 ま
644 たは複数の“一对の「WorkKey (odd)・SubscriptionTierBits・ExtractInfo」と
645 「WorkKey (even)・SubscriptionTierBits・ExtractInfo」”とを同時に取得するこ
646 とができる。
647 また、受信機は、1 または複数の“一对の「WorkKey (odd)・
648 SubscriptionTierBits・ExtractInfo」と「WorkKey (even)・SubscriptionTierBits・
649 ExtractInfo」”とともに、Datetime を同時に取得することもできる。
650

651 A.1.2 コンテンツ受信時の ECM 処理

652 受信機は、コンテンツサーバからコンテンツを受信し、ECM を抽出する。受信機は、
653 ECM 毎に ECM の WorkKeyID で指定される WorkKey の NotBefore/NotAfter と
654 [IPTVCRMC], 3.2 節の受信機内で保持する時刻（以下、本項では“受信機内で保持
655 する時刻”と記す）とを比較し、(NotBefore) ≤ (受信機内で保持する時刻) ≤
656 (NotAfter) を満たす場合、受信機は当該 WorkKey を用いて ECM を復号する。但
657 し、NotBefore の値が FFFFFFFFh の場合は、NotBefore と受信機内で保持する時刻
658 との比較は不要である。同様に NotAfter の値が FFFFFFFFh の場合は、NotAfter と
659 受信機内で保持する時刻との比較は不要である。

660 復号した ECM の検証後、[MIPTV], 6.1.3 項の規定の通り、受信機は ECM の
661 ChannelTierBits と WorkKey の SubscriptionTierBits とを照合し、同一位置のビット
662 が共に 1b となるビットが存在する場合に視聴可と判定する。

663 受信機は、視聴可と判定した場合、ECM から抽出した ScrambleKey によりコンテ
664 ンツを復号し、ECM に設定された RenderingObligation に従った利用をおこなう。
665

666 A.1.3 「WorkKey・SubscriptionTierBits・ExtractInfo」の更新処理

667 受信機は、「WorkKey・SubscriptionTierBits・ExtractInfo」が更新される運用の場合
668 に、保持する「WorkKey・SubscriptionTierBits・ExtractInfo」の更新を制御する。
669

670 A.1.3.1 更新の有無と更新開始日時オフセット

671 DRM サーバは、送信する「WorkKey・SubscriptionTierBits・ExtractInfo」の
672 StatusExtension の PrivateData（上位 23 バイト目から上位 24 バイト目）の値によ
673 り、次回の更新の有無、および、NotAfter から次回の更新が可能となる日時（更新
674 開始日時）までのオフセット時間を受信機に通知する。この 2 バイトの値を“更新
675 開始日時オフセット”とよぶ。

676 DRM サーバは、次回の更新をおこなう場合には、送信する「WorkKey・
677 SubscriptionTierBits・ExtractInfo」の更新開始日時オフセットの値に 0001h~FFFFh
678（単位は“分”）を設定する。

679 一方、DRM サーバは、契約の解約時など、次回の更新をおこなわない場合には、更
680 新開始日時オフセットの値に 0000h を設定する。
681

682 A.1.3.2 「WorkKey・SubscriptionTierBits・ExtractInfo」の更新

683 「WorkKey・SubscriptionTierBits・ExtractInfo」が更新される運用（更新開始日時オ
684 フセットの値が 0001h~FFFFh）の場合、受信機は更新開始日時以降に更新するこ
685 とができる。更新のための「WorkKey・SubscriptionTierBits・ExtractInfo」の取得は、
686 A.1.1 項と同等である。

687 一方、DRM サーバは、更新開始日時以降に受信機から「WorkKey・
688 SubscriptionTierBits・ExtractInfo」の取得要求を受信した場合、少なくとも NotAfter
689 の値を更新した「WorkKey・SubscriptionTierBits・ExtractInfo」を送信する。

690 「WorkKey・SubscriptionTierBits・ExtractInfo」の更新に関して、DRM サーバ・受
691 信機の実装は以下の事項が考慮されることが望ましい。
692

- 693 ● DRM サーバ
 - 694 ➤ 受信機が短期間に繰り返し更新しないように、DRM サーバが更新後の
695 NotAfter に設定する値は、（「WorkKey・SubscriptionTierBits・ExtractInfo」

- 696 の送信日時) + (更新開始日時オフセット) よりも大きな値とすることが
697 望ましい。
- 698 • 受信機
 - 699 ▶ NotAfter と更新開始日時オフセットとに基づいて更新するか否かについては、
700 受信機の実装依存であるが、更新された場合に継続して視聴できるように
701 するため、受信機は更新開始日時以降、速やかに更新することが望ましい。
 - 702 ▶ DRM サーバと受信機とで保持する時刻に誤差が生じている場合などは、
703 DRM サーバが NotAfter を更新する前に、受信機が更新のために
704 「WorkKey・SubscriptionTierBits・ExtractInfo」を取得してしまう場合が考
705 えられる。このような場合、受信機は短期間に繰り返し更新しないように、
706 間隔をあけて再度更新するなどの制御をおこなうことが望ましい。
 - 707

708 **A.2 WorkKeyID および UsageRuleReference の運用例**

709 本節では、WorkKeyID および UsageRuleReference の運用例を示す。
710

711 **A.2.1 ティアビット・WorkKeyID・UsageRuleReference の関係**

712 サービス事業者が運用するティアビット、WorkKeyID、および
713 UsageRuleReference の関係について説明する。
714

715 **A.2.1.1 WorkKeyID とティアビットとの関係**

716 WorkKeyID は、“ServiceProviderID”、“ReservedByte”、
717 “WorkKeyManagementID”、および“WorkKeyVersion”から構成される。
718 WorkKeyID のうち、DRM サーバおよび受信機における WorkKey の管理単位となる
719 ID が、ServiceProviderID および WorkKeyManagementID である。サービス事業者
720 は、64 ビットからなるティアビットを管理し、当該ティアビットに対して
721 WorkKeyManagementID を対応づける。したがって、サービス事業者は、64 ビット
722 からなるティアビットを運用する個数分だけ、WorkKeyManagementID を管理する。
723 たとえば、サービス事業者が 64 ビットからなるティアビットを 1 個用いる運用をお
724 こなう場合、当該サービス事業者は 1 つの WorkKeyManagementID を管理する。ま
725 た、64 ビットからなるティアビットを 2 個用いて、64 を超える契約を当該 2 個の
726 ティアビットに対応づける運用をおこなう場合、サービス事業者は 2 つの
727 WorkKeyManagementID を管理する。
728 また、DRM サーバは、同一 ServiceProviderID・同一 WorkKeyManagementID の
729 WorkKey について、WorkKey 自体を更新する場合に限り、WorkKeyVersion を更新
730 する。すなわち、SubscriptionTierBits または ExtractInfo の値を更新する場合であっ
731 ても、WorkKey 自体を更新しない限り、WorkKeyVersion は更新しない。
732 WorkKeyID の概要については A.1.1.2 項および A.1.1.3 項を、詳細については
733 [MIPTV], 4.2.1.5.1 項を参照のこと。
734

735 **A.2.1.2 UsageRuleReference と WorkKeyID との関係**

736 UsageRuleReference は、“ServiceProviderID”、“ReservedByte”、
737 “WorkKeyManagementID”、および“odd/evenID”から構成される。

738 ServiceProviderID・WorkKeyManagementID には、UsageRuleReference に対応する
739 WorkKey の ServiceProviderID・WorkKeyManagementID と同一の値が設定され
740 る。
741 また、odd/evenID には、UsageRuleReference に対応する WorkKey の
742 WorkKeyVersion の LSB と同一の値が設定される。
743

744 **A.2.1.3 ティアビットと WorkKeyID・UsageRuleReference の値との関係の例**

745 サービス事業者が運用するティアビットと、WorkKeyID・UsageRuleReference の
746 値との関係の例を、表 A-1 に示す。
747 ただし、WorkKeyID および UsageRuleReference の ReservedByte は固定値である
748 ので、表 A-1 では記載を省略する。
749 また、3.1.3 項で規定する通り、UsageRuleReference の下位 10 バイトの値はサー
750 ビス事業者の運用依存であるため、表 A-1 では上位 6 バイトの値のみを記載する。
751

表 A-1 サービス事業者が運用するティアビットと
WorkKeyID・UsageRuleReference の値との関係の例

サービス事業者	サービス事業者が運用するティアビット		WorkKeyID の値 : 16 進表記			UsageRuleReference の値 : 16 進表記		
			ServiceProviderID	WorkKeyManagementID	WorkKeyVersion	ServiceProviderID	WorkKeyManagementID	odd/evenID
サービス事業者 1	1 個 (*1)	一つ目のティアビット	0001	0001	01, 03, ...(odd)	0001	0001	01(odd)
					02, 04, ...(even)			00(even)
サービス事業者 2	2 個 (*2)	一つ目のティアビット	0002	0001	01, 03, ...(odd)	0002	0001	01(odd)
					02, 04, ...(even)			00(even)
	二つ目のティアビット	0002	01, 03, ...(odd)	0002	0002	01(odd)		
			02, 04, ...(even)			00(even)		

752
753 *1 : 64 ビットからなるティアビットを 1 個用いる運用をおこなうサービス事業者の
754 例である。
755 *2 : 64 ビットからなるティアビットを 2 個用いて、64 を超える契約を当該 2 個の
756 ティアビットに対応づける運用をおこなうサービス事業者の例である。

757 **A.2.2 WorkKey を更新する運用における WorkKeyID と**
758 **UsageRuleReference との関係の例**

759 DRM サーバは、ServiceProviderID・WorkKeyManagementID ごとに WorkKey のバ
760 ージョン (WorkKeyVersion) を管理する。DRM サーバは、受信機から WorkKey を
761 要求された場合、一対の WorkKey (odd)・WorkKey (even) として、WorkKey の
762 送信時点で ECM を暗号化する WorkKey と、ECM を暗号化する WorkKey の次回更
763 新後の WorkKey とを送信する。よって、DRM サーバは、ServiceProviderID・
764 WorkKeyManagementID ごとに少なくとも一対の WorkKeyVersion を管理する。
765

766 WorkKey を更新する運用において、ECM を暗号化する WorkKey の WorkKeyID の
767 値、Get Permission Protocol で DRM サーバから送信する WorkKey の WorkKeyID
768 の値、Get Permission Protocol で WorkKey を要求する際の UsageRuleReference の
769 値の関係の例を、表 A-2 に示す。
770

771 表 A-2 において、Get Permission Protocol で送信する WorkKey の WorkKeyVersion
 772 は、ECM を暗号化する WorkKey の更新以降に送信する値を示すものである。DRM
 773 サーバは、ECM を暗号化する WorkKey の更新後、Get Permission Protocol で送信
 774 する一対の WorkKey (odd) ・ WorkKey (even) も速やかに更新する。
 775
 776 なお、A.2.1.3 項の表 A-1 と同様に、表 A-2 において WorkKeyID および
 777 UsageRuleReference の ReservedByte は記載を省略する。また、
 778 UsageRuleReference の下位 10 バイトの値についても、同様に記載を省略する。
 779

表 A-2 WorkKey を更新する運用における
WorkKeyID と UsageRuleReference との値の関係の例

ECM を暗号化する WorkKey の更新 (*1)	ECM を暗号化する WorkKey の WorkKeyID の値 : 16 進表記			Get Permission Protocol で送信する WorkKey の WorkKeyID の値 : 16 進表記			UsageRuleReference の値 : 16 進表記			
	ServiceProviderID	WorkKeyManagementID	WorkKeyVersion	ServiceProviderID	WorkKeyManagementID	WorkKeyVersion	ServiceProviderID	WorkKeyManagementID	odd/even ID	
運用開始	0001	0001	01(odd)	0001	0001	01(odd)	0001	0001	01(odd)	
1 回目の更新後			02(even)			02(even)			03(odd)	00(even)
			2 回目の更新後			03(odd)			03(odd)	04(even)
...					
254 回目の更新後			FF(odd)			FF(odd)			00(even)	01(odd)
			255 回目の更新後			00(even)			01(odd)	00(even)

780
 781 *1 : 256 回目以降の更新では、表 A-2 における“運用開始～255 回目の更新後”の
 782 繰り返しとなる。
 783

784 **A.3 「WorkKey ・ SubscriptionTierBits ・ ExtractInfo」の更新運**
 785 **用の例**

786 本節では、図 A-2 を用いて「WorkKey ・ SubscriptionTierBits ・ ExtractInfo」の更新
 787 運用の例を示す。
 788 以下、図 A-2 のイベントの囲い数字、および、DRM サーバ・事業者サーバの括弧書
 789 きの数字に対応して、新規契約から解約までの DRM サーバ・事業者サーバ・受信
 790 機の処理の概要について説明する。なお、事業者サーバは、契約・解約などをおこ
 791 なるサービス事業者のポータルサーバなどである。
 792
 793 本節では、以下を前提とした更新運用の例を示す。
 794

- 795 ● 特定の ServiceProviderID・WorkKeyManagementID の「WorkKey・
- 796 SubscriptionTierBits・ExtractInfo」に関して、特定の受信機についての例を示す。
- 797 ● WorkKey の期限 (NotBefore/NotAfter) を定期的に更新する、期限延長の運用を
- 798 基本とする。したがって、更新の度に「WorkKey・SubscriptionTierBits・
- 799 ExtractInfo」の全てが更新されるとは限らないことに留意されたい。
- 800 ● 期限の更新周期は 1 年とする。DRM サーバは、受信機ごとの契約月の 1 年後に
- 801 更新をおこなうため、NotAfter を契約月の 1 年後の月末日に設定する。なお、
- 802 NotBefore には期限なし (FFFFFFFFh) を設定する。
- 803 図 A-2 に示す NotAfter の年月日の表記は、受信機が取得する WorkKey の
- 804 NotAfter の値を示し、点線の矢印は、受信機が当該 NotAfter の値を保持する期
- 805 間を示す。
- 806 ● 期限延長における更新開始日時は NotAfter の 14 日前とし、更新開始日時オフセ
- 807 ットに 14 日 (20160 分) を設定する場合の例を示す。なお、以下では、更新開
- 808 始日時から NotAfter までを“更新期間”と記す。
- 809 図 A-2 に示す更新期間の年月日の表記は、受信機が NotAfter の値と更新開始日
- 810 時オフセットとから算出する更新期間 (更新開始日時～NotAfter) を示し、点線
- 811 の矢印は、受信機が当該更新期間の値を保持する期間を示す。
- 812 ● ECM を暗号化する WorkKey の WorkKeyVersion の初期値は 1 とする。DRM サ
- 813 ーバは、図 A-2 に示す“⑦ ECM を暗号化する WorkKey の更新”において、
- 814 WorkKeyVersion を 1 から 2 に更新する。
- 815 ● 事業者サーバは、契約時や解約時などに「WorkKey・SubscriptionTierBits・
- 816 ExtractInfo」の取得のための UsageRuleReference・DRM サーバの URI (DRM
- 817 サーバ URI) を含むファイルを提供する。以下、当該ファイルを“メタファイル
- 818 ”と記す。
- 819

年	2008												2009											
月	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12
イベント				△①新規契約												△②期限延長						△③契約追加		
DRMサーバ				(2)												(3)						(5)		
事業者サーバ				(1)												(4)						(4)		
受信機				⇓												⇓	⇐					⇓		
NotAfter				2009/4/30												2010/4/30								
更新期間				2009/4/16~2009/4/30												2010/4/16~2010/4/30								

年	2010												2011											
月	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12
イベント				△④期限延長				△⑤契約一部解約申し込み					△⑦ECMを暗号化するWorkKeyの更新				△⑧期限延長						△⑨全解約	
DRMサーバ				(6)				(8)	(9)							(10)						(12)		
事業者サーバ				(7)				(7)	(9)							(11)						(11)		
受信機				⇓				⇓	⇓							⇓	⇐					⇓		
NotAfter				2011/4/30				2010/9/3	2011/4/30							2012/4/30						2011/10/31		
更新期間				2011/4/16~2011/4/30				2010/9/1~2010/9/3	2011/4/16~2011/4/30							2012/4/16~2012/4/30								

820
821

図 A-2 「WorkKey・SubscriptionTierBits・ExtractInfo」の更新運用の例

822
823
824
825
826
827

- ① 新規契約
- 受信機は、2008/4 に事業者サーバに新規に契約を申し込む。受信機は、事業者サーバから取得したメタファイルを用いて、DRM サーバから一対の「WorkKey・SubscriptionTierBits・ExtractInfo」を取得する。

- 828 (1) 事業者サーバからのメタファイルの取得
829 • 受信機は、事業者サーバに新規契約の要求を送信する。
830 • 事業者サーバは、受信機からの契約申し込みを受け付け、DRM サーバ
831 に契約内容を送信するなど、新規契約の受け付け処理を完了する。
832 • 受信機は、事業者サーバからメタファイルを取得し、不揮発性記憶領域
833 に記録する。
- 834 (2) DRM サーバからの「WorkKey・SubscriptionTierBits・ExtractInfo」の取得
835 • 受信機は、メタファイルで指定される UsageRuleReference (odd) を
836 設定した Get Permission Request message を作成して、メタファイル
837 の DRM サーバ URI で指定される DRM サーバに送信する。
838 • DRM サーバは、UsageRuleReference (odd) に対応する「WorkKey
839 (odd)・SubscriptionTierBits・ExtractInfo」を設定した Get
840 Permission Reply message を作成して、受信機に送信する。
841 ➢ NotAfter には、加入月の 1 年後の月末の日時 (2009/4/30) を設定
842 する。
843 ➢ 送信する「WorkKey・SubscriptionTierBits・ExtractInfo」を次回に
844 更新することを通知するため、更新開始日時オフセットの値には
845 14 日 (20160 分) を設定する。
846 ➢ WorkKey (odd) には、WorkKey の送信時点で ECM を暗号化する
847 WorkKey (WorkKeyVersion が 1) を設定する。
- 848 • 受信機は、DRM サーバから受信した Get Permission Reply message から
849 「WorkKey (odd)・SubscriptionTierBits・ExtractInfo」を取得する。
850 • 受信機は、メタファイルで指定される UsageRuleReference (even) を
851 設定した Get Permission Request message を作成して、メタファイル
852 の DRM サーバ URI で指定される DRM サーバに送信する。
853 • DRM サーバは、UsageRuleReference (even) に対応する「WorkKey
854 (even)・SubscriptionTierBits・ExtractInfo」を設定した Get
855 Permission Reply message を作成して、受信機に送信する。
856 ➢ SubscriptionTierBits・ExtractInfo には、WorkKey (odd) の
857 SubscriptionTierBits・ExtractInfo と同一の値を設定する。また、更
858 新開始日時オフセットには、WorkKey (odd) の更新開始日時オフ
859 セットと同一の値を設定する。
860 ➢ WorkKey (even) には、ECM を暗号化する WorkKey の次回更新
861 後の WorkKey (WorkKeyVersion が 2) を設定する。
- 862 • 受信機は、DRM サーバから受信した Get Permission Reply message から
863 「WorkKey (even)・SubscriptionTierBits・ExtractInfo」を取得する。
864 • 受信機は、取得した一対の「WorkKey・SubscriptionTierBits・
865 ExtractInfo」を不揮発性記憶領域に記録する。
866 • 受信機は、更新開始日時オフセットの値が 14 日 (更新される) である
867 ことから、NotAfter と更新開始日時オフセットとを用いて次回の更新期
868 間 (②の更新期間：2009/4/16～2009/4/30) を算出し、次回更新の制御
869 をおこなう。

870
871 [備考]

- 872 • DRM サーバ
873 ➢ DRM サーバは、WorkKey (odd) または WorkKey (even) のいずれかとし
874 て、WorkKey の送信時点で ECM を暗号化する WorkKey を送信する。他方
875 は、ECM を暗号化する WorkKey の次回更新後の WorkKey を送信する。

- 876 ▶ DRM サーバは、受信機が有する契約の終了日時を経過するまでは、受信機
877 に「WorkKey・SubscriptionTierBits・ExtractInfo」を送信する。送信回数は
878 制限しない。
879 ▶ DRM サーバは、更新開始日時オフセットまたは NotAfter の値を受信機ごと
880 などに異なる値とすることで、更新時の受信機からのアクセスを分散させ
881 ることができる。

882 • 受信機

- 883 ▶ メタファイルから取得した UsageRuleReference・DRM サーバ URI は、以
884 降の「WorkKey・SubscriptionTierBits・ExtractInfo」の更新時に必要となる
885 ため、受信機は不揮発性記憶領域に記録しておくことが望ましい。また、
886 この場合、受信機は新たにメタファイルを取得した場合、当該メタファイ
887 ルに含まれる DRM サーバ URI の値で、不揮発性記憶領域に記録した DRM
888 サーバ URI の値を更新することが望ましい。
889 ▶ 受信機は、同一 ServiceProviderID・同一 WorkKeyManagementID の
890 odd/even の「WorkKey・SubscriptionTierBits・ExtractInfo」を一对の組と
891 して取得する。メタファイルでは、一对の「WorkKey・
892 SubscriptionTierBits・ExtractInfo」に対応する 2 つの UsageRuleReference
893 (odd)・UsageRuleReference (even) を組として、1 組以上の
894 UsageRuleReference が指定される (1 サービス事業者が 64 ビットからな
895 るティアビットを複数個用いる運用をおこなう場合などに、2 組以上の
896 UsageRuleReference が指定される場合がある)。
897 ▶ 受信機は、更新開始日時オフセットの値が 0000h (更新されない) である
898 場合は、更新をおこなわない。
899

900 ② 期限延長

901 受信機は、②の更新期間 (2009/4/16~2009/4/30) に、期限延長された一对の
902 「WorkKey・SubscriptionTierBits・ExtractInfo」を取得する。
903

904 (3) DRM サーバからの「WorkKey・SubscriptionTierBits・ExtractInfo」の取得

- 905 • 受信機は、不揮発性記憶領域に記録したメタファイルで指定される
906 UsageRuleReference (odd) を設定した Get Permission Request
907 message を作成して、メタファイルの DRM サーバ URI で指定される
908 DRM サーバに送信する。
909 • DRM サーバは、UsageRuleReference (odd) に対応する「WorkKey
910 (odd)・SubscriptionTierBits・ExtractInfo」を設定した Get
911 Permission Reply message を作成して、受信機に送信する。
912 ▶ NotAfter には、1 年後の月末の日時 (2010/4/30) を設定する。
913 ▶ 引き続き次回に更新をおこなうことを通知するため、更新開始日時
914 オフセットの値には 14 日 (20160 分) を設定する。
915 ▶ WorkKey (odd) には、WorkKey の送信時点で ECM を暗号化する
916 WorkKey (WorkKeyVersion が 1) を設定する。
917 • 受信機は、DRM サーバから受信した Get Permission Reply message か
918 ら「WorkKey (odd)・SubscriptionTierBits・ExtractInfo」を取得する。
919 • 受信機は、メタファイルで指定される UsageRuleReference (even) を
920 設定した Get Permission Request message を作成して、メタファイ
921 ルの DRM サーバ URI で指定される DRM サーバに送信する。
922 • DRM サーバは、UsageRuleReference (even) に対応する「WorkKey
923 (even)・SubscriptionTierBits・ExtractInfo」を設定した Get
924 Permission Reply message を作成して、受信機に送信する。

- 925 ➤ SubscriptionTierBits・ExtractInfo には、WorkKey (odd) の
926 SubscriptionTierBits・ExtractInfo と同一の値を設定する。また、更
927 新開始日時オフセットには、WorkKey (odd) の更新開始日時オフ
928 セットと同一の値を設定する。
929 ➤ WorkKey (even) には、ECM を暗号化する WorkKey の次回更新
930 後の WorkKey (WorkKeyVersion が 2) を設定する。
931 ● 受信機は、DRM サーバから受信した Get Permission Reply message か
932 ら「WorkKey (even)・SubscriptionTierBits・ExtractInfo」を取得する。
933 ● 受信機は、取得した一对の「WorkKey・SubscriptionTierBits・
934 ExtractInfo」で、不揮発性記憶領域に記録した同一
935 ServiceProviderID・同一 WorkKeyManagementID の一对の
936 「WorkKey・SubscriptionTierBits・ExtractInfo」を更新する。
937 ● 受信機は、更新開始日時オフセットの値が 14 日（更新される）である
938 ことから、NotAfter と更新開始日時オフセットとを用いて次回の更新期
939 間（④の更新期間：2010/4/16～2010/4/30）を算出し、次回更新の制御
940 をおこなう。

941
942 [備考]

- 943 ● DRM サーバ
944 ➤ DRM サーバは、更新開始日時（上記では 2009/4/16）以降に受信機から
945 「WorkKey・SubscriptionTierBits・ExtractInfo」の要求を受信した場合、
946 NotAfter を更新（上記では 2010/4/30）した「WorkKey・
947 SubscriptionTierBits・ExtractInfo」を送信する。
948 ● 受信機
949 ➤ メタファイルの DRM サーバ URI が変更される場合を考慮し、受信機は、
950 期限延長時などにメタファイルを取得し、取得したメタファイルに設定さ
951 れた DRM サーバ URI の値で、不揮発性記憶領域に記録した DRM サーバ
952 URI の値を更新することが望ましい。

953
954 ③ 契約追加

955 受信機は、2009/9 に事業者サーバに契約の一部追加を申し込む。受信機は一部の契
956 約が追加された一对の「WorkKey・SubscriptionTierBits・ExtractInfo」を取得する。

957
958 (4) 事業者サーバからのメタファイルの取得

- 959 ● 受信機は、事業者サーバに対して契約の一部追加の要求を送信する。
960 ● 事業者サーバは、受信機からの契約追加の申し込みを受け付け、DRM
961 サーバに契約内容を送信するなど、契約追加の受け付け処理を完了する。
962 ● 受信機は、事業者サーバからメタファイルを取得し、受信したメタファ
963 イルで不揮発性記憶領域に記録したメタファイルを更新する。

964 (5) DRM サーバからの「WorkKey・SubscriptionTierBits・ExtractInfo」の取得

- 965 ● 受信機は、メタファイルで指定される UsageRuleReference (odd) を
966 設定した Get Permission Request message を作成して、メタファイル
967 の DRM サーバ URI で指定される DRM サーバに送信する。
968 ● DRM サーバは、UsageRuleReference (odd) に対応する「WorkKey
969 (odd)・SubscriptionTierBits・ExtractInfo」を設定した Get
970 Permission Reply message を作成して、受信機に送信する。
971 ➤ SubscriptionTierBits には、②で設定した SubscriptionTierBits のう
972 ち、追加した契約に対応するビットを 1b に変更したビット列を設
973 定する。

- 1022 • 受信機は、DRM サーバから受信した Get Permission Reply message から「WorkKey (odd) ・ SubscriptionTierBits ・ ExtractInfo」を取得する。
- 1023
- 1024 • 受信機は、メタファイルで指定される UsageRuleReference (even) を
- 1025 設定した Get Permission Request message を作成して、メタファイル
- 1026 の DRM サーバ URI で指定される DRM サーバに送信する。
- 1027 • DRM サーバは、UsageRuleReference (even) に対応する「WorkKey
- 1028 (even) ・ SubscriptionTierBits ・ ExtractInfo」を設定した Get
- 1029 Permission Reply message を作成して、受信機に送信する。
- 1030 ➤ SubscriptionTierBits ・ ExtractInfo には、WorkKey (odd) の
- 1031 SubscriptionTierBits ・ ExtractInfo と同一の値を設定する。また、更
- 1032 新開始日時オフセットには、WorkKey (odd) の更新開始日時オフ
- 1033 セットと同一の値を設定する。
- 1034 ➤ WorkKey (even) には、ECM を暗号化する WorkKey の次回更新
- 1035 後の WorkKey (WorkKeyVersion が 2) を設定する。
- 1036 • 受信機は、DRM サーバから受信した Get Permission Reply message から「WorkKey (even) ・ SubscriptionTierBits ・ ExtractInfo」を取得する。
- 1037
- 1038 • 受信機は、取得した一対の「WorkKey ・ SubscriptionTierBits ・
- 1039 ExtractInfo」で、不揮発性記憶領域に記録した同一
- 1040 ServiceProviderID ・ 同一 WorkKeyManagementID の一対の
- 1041 「WorkKey ・ SubscriptionTierBits ・ ExtractInfo」を更新する。
- 1042 • 受信機は、更新開始日時オフセットの値が 14 日 (更新される) である
- 1043 ことから、NotAfter と更新開始日時オフセットとを用いて次回の更新期
- 1044 間 (⑧の更新期間：2011/4/16～2011/4/30) を算出し、次回更新の制御
- 1045 をおこなう。
- 1046

⑤ 契約一部解約申し込み

- 1048 受信機は、2010/8 初旬に事業者サーバに一部の契約の解約を申し込む。DRM サー
- 1049 バは、解約するチャンネルが当月末まで視聴可能となるように、SubscriptionTierBits
- 1050 は解約前と同一で、期限が来月初めに設定された一対の「WorkKey ・
- 1051 SubscriptionTierBits ・ ExtractInfo」を受信機に送信する。
- 1052 受信機は、当該「WorkKey ・ SubscriptionTierBits ・ ExtractInfo」を取得し、NotAfter
- 1053 に基づき、一部の契約が解約された一対の「WorkKey ・ SubscriptionTierBits ・
- 1054 ExtractInfo」を、来月初めに取得するための制御をおこなう。
- 1055

(7) 事業者サーバからのメタファイルの取得

- 1057 • 受信機は、事業者サーバに対して契約の一部解約の要求を送信する。
- 1058 • 事業者サーバは、受信機からの契約一部解約の申し込みを受け付け、
- 1059 DRM サーバに解約内容を送信するなど、契約一部解約の受付処理を完
- 1060 了する。
- 1061 • 受信機は、事業者サーバからメタファイルを取得し、受信したメタファ
- 1062 イルで不揮発性記憶領域に記録したメタファイルを更新する。

(8) DRM サーバからの「WorkKey ・ SubscriptionTierBits ・ ExtractInfo」の取得

- 1064 • 受信機は、メタファイルで指定される UsageRuleReference (odd) を
- 1065 設定した Get Permission Request message を作成して、メタファイル
- 1066 の DRM サーバ URI で指定される DRM サーバに送信する。
- 1067 • DRM サーバは、UsageRuleReference (odd) に対応する「WorkKey
- 1068 (odd) ・ SubscriptionTierBits ・ ExtractInfo」を設定した Get
- 1069 Permission Reply message を作成して、受信機に送信する。

- 1070 ➤ **SubscriptionTierBits** には、引き続き、③および④で設定した契約
1071 の一部解約前の **SubscriptionTierBits** を設定する。
1072 ➤ 2010/9/1 からの一部解約のための更新を指定し、かつ、更新期間
1073 を 3 日間とするため、**NotAfter** には 2010/9/3、更新開始日時オフセ
1074 ットには 3 日 (4320 分) を設定する。
1075 ➤ **WorkKey (odd)** には、**WorkKey** の送信時点で **ECM** を暗号化する
1076 **WorkKey (WorkKeyVersion が 1)** を設定する。
1077 ● 受信機は、DRM サーバから受信した **Get Permission Reply message** か
1078 ら「**WorkKey (odd) ・ SubscriptionTierBits ・ ExtractInfo**」を取得する。
1079 ● 受信機は、メタファイルで指定される **UsageRuleReference (even)** を
1080 設定した **Get Permission Request message** を作成して、メタファイル
1081 の DRM サーバ URI で指定される DRM サーバに送信する。
1082 ● DRM サーバは、**UsageRuleReference (even)** に対応する「**WorkKey**
1083 **(even) ・ SubscriptionTierBits ・ ExtractInfo**」を設定した **Get**
1084 **Permission Reply message** を作成して、受信機に送信する。
1085 ➤ **SubscriptionTierBits ・ ExtractInfo** には、**WorkKey (odd)** の
1086 **SubscriptionTierBits ・ ExtractInfo** と同一の値を設定する。また、更
1087 新開始日時オフセットには、**WorkKey (odd)** の更新開始日時オフ
1088 セットと同一の値を設定する。
1089 ➤ **WorkKey (even)** には、**ECM** を暗号化する **WorkKey** の次回更新
1090 後の **WorkKey (WorkKeyVersion が 2)** を設定する。
1091 ● 受信機は、DRM サーバから受信した **Get Permission Reply message** か
1092 ら「**WorkKey (even) ・ SubscriptionTierBits ・ ExtractInfo**」を取得する。
1093 ● 受信機は、取得した一対の「**WorkKey ・ SubscriptionTierBits ・**
1094 **ExtractInfo**」で、不揮発性記憶領域に記録した同一
1095 **ServiceProviderID ・ 同一 WorkKeyManagementID** の一対の
1096 「**WorkKey ・ SubscriptionTierBits ・ ExtractInfo**」を更新する。
1097 ● 受信機は、更新開始日時オフセットの値が 3 日 (更新される) である
1098 ことから、**NotAfter** と更新開始日時オフセットとを用いて次回の更新期
1099 間 (⑥の更新期間：2010/9/1～2010/9/3) を算出し、次回更新の制御を
1100 おこなう。

⑥ 契約一部解約

1103 受信機は、⑥の更新期間 (2010/9/1～2010/9/3) に、一部の契約が解約された一対
1104 の「**WorkKey ・ SubscriptionTierBits ・ ExtractInfo**」を取得する。

(9) DRM サーバからの「**WorkKey ・ SubscriptionTierBits ・ ExtractInfo**」の取得

- 1107 ● 受信機は、不揮発性記憶領域に記録したメタファイルで指定される
1108 **UsageRuleReference (odd)** を設定した **Get Permission Request**
1109 **message** を作成して、メタファイルの DRM サーバ URI で指定される
1110 DRM サーバに送信する。
1111 ● DRM サーバは、**UsageRuleReference (odd)** に対応する「**WorkKey**
1112 **(odd) ・ SubscriptionTierBits ・ ExtractInfo**」を設定した **Get**
1113 **Permission Reply message** を作成して、受信機に送信する。
1114 ➤ **SubscriptionTierBits** には、⑤で設定した **SubscriptionTierBits** のう
1115 ち、解約した契約に対応するビットを 0b に変更したビット列を設
1116 定する。
1117 ➤ **NotAfter** には、⑧の更新期間での期限延長を継続するため、④の期
1118 限延長で設定した **NotAfter (2011/4/30)** と同一の値を設定する。

- 1119 また、更新開始日時オフセットにも、引き続き④で設定した更新開
1120 始日時オフセット（14日）と同一の値を設定する。
- 1121 ➤ WorkKey (odd) には、WorkKey の送信時点で ECM を暗号化する
1122 WorkKey (WorkKeyVersion が 1) を設定する。
- 1123 • 受信機は、DRM サーバから受信した Get Permission Reply message か
1124 ら「WorkKey (odd) ・ SubscriptionTierBits ・ ExtractInfo」を取得する。
 - 1125 • 受信機は、メタファイルで指定される UsageRuleReference (even) を
1126 設定した Get Permission Request message を作成して、メタファイル
1127 の DRM サーバ URI で指定される DRM サーバに送信する。
 - 1128 • DRM サーバは、UsageRuleReference (even) に対応する「WorkKey
1129 (even) ・ SubscriptionTierBits ・ ExtractInfo」を設定した Get
1130 Permission Reply message を作成して、受信機に送信する。
 - 1131 ➤ SubscriptionTierBits ・ ExtractInfo には、WorkKey (odd) の
1132 SubscriptionTierBits ・ ExtractInfo と同一の値を設定する。また、更
1133 新開始日時オフセットには、WorkKey (odd) の更新開始日時オフ
1134 セットと同一の値を設定する。
 - 1135 ➤ WorkKey (even) には、ECM を暗号化する WorkKey の次回更新
1136 後の WorkKey (WorkKeyVersion が 2) を設定する。
 - 1137 • 受信機は、DRM サーバから受信した Get Permission Reply message か
1138 ら「WorkKey (even) ・ SubscriptionTierBits ・ ExtractInfo」を取得する。
 - 1139 • 受信機は、取得した一対の「WorkKey ・ SubscriptionTierBits ・
1140 ExtractInfo」で、不揮発性記憶領域に記録している同一
1141 ServiceProviderID ・ 同一 WorkKeyManagementID の一対の
1142 「WorkKey ・ SubscriptionTierBits ・ ExtractInfo」を更新する。
 - 1143 • 受信機は、更新開始日時オフセットの値が 14 日（更新される）である
1144 ことから、NotAfter と更新開始日時オフセットとを用いて次回の更新期
1145 間（⑧の更新期間：2011/4/16～2011/4/30）を算出し、次回更新の制御
1146 をおこなう。

1147
1148 [備考]

- 1149 • DRM サーバ
- 1150 ➤ DRM サーバは、「WorkKey ・ SubscriptionTierBits ・ ExtractInfo」の送信に
1151 対して、受信機から以下の SAC 層のメッセージを受信することにより、受
1152 信機での「WorkKey ・ SubscriptionTierBits ・ ExtractInfo」の更新を確認でき
1153 る。
- 1154 ☆ Command に「Commit」が設定された Encrypted command message
1155 ☆ Request message
- 1156 したがって、DRM サーバは、odd/even の一対の「WorkKey ・
1157 SubscriptionTierBits ・ ExtractInfo」の送信に対して、上記メッセージを受信
1158 することにより契約の一部解約処理を完了できる。なお、上記は Get
1159 Permission Protocol と Packed Message Protocol とで共通である。

- 1161 ⑦ ECM を暗号化する WorkKey の更新
- 1162 DRM サーバは、現在送出中の ECM を暗号化する WorkKey が更新された場合、Get
1163 Permission Protocol で受信機に送信する WorkKey を更新する。
- 1164 DRM サーバは、ECM を暗号化する WorkKey を、WorkKeyVersion が 1 の WorkKey
1165 (odd) から WorkKeyVersion が 2 の WorkKey (even) に更新する。以降、DRM サ
1166 ーバは、WorkKeyVersion が 2 の WorkKey (even) と、WorkKeyVersion が 3 の
1167 WorkKey (odd) とを受信機に送信する。

1168 [備考]

- 1169 • DRM サーバは、ECM を暗号化する WorkKey の更新後、Get Permission
1170 Protocol で送信する一対の WorkKey (odd) ・ WorkKey (even) も速やかに更
1171 新する。
1172 • DRM サーバが WorkKey を更新するタイミングは、サービス事業者の運用依存
1173 とする。
1174 • DRM サーバは、WorkKey 自体を定期的に更新する運用をおこなう場合、ECM
1175 を暗号化する WorkKey の更新前に、全ての受信機が更新後に ECM の暗号化に
1176 用いる WorkKey を取得できるように各受信機の更新期間を設定する。
1177

1178 ⑧ 期限延長

1179 受信機は、⑧の更新期間 (2011/4/16~2011/4/30) に、期限延長された一対の
1180 「WorkKey ・ SubscriptionTierBits ・ ExtractInfo」を取得する。
1181

1182 (10) DRM サーバからの「WorkKey ・ SubscriptionTierBits ・ ExtractInfo」
1183 の取得

- 1184 • 受信機は、不揮発性記憶領域に記録したメタファイルで指定される
1185 UsageRuleReference (odd) を設定した Get Permission Request
1186 message を作成して、メタファイルの DRM サーバ URI で指定される
1187 DRM サーバに送信する。
1188 • DRM サーバは、UsageRuleReference (odd) に対応する「WorkKey
1189 (odd) ・ SubscriptionTierBits ・ ExtractInfo」を設定した Get
1190 Permission Reply message を作成して、受信機に送信する。
1191 ➤ NotAfter には、1年後の月末の日時 (2012/4/30) を設定する。
1192 ➤ 引き続き次回に更新することを通知するため、更新開始日時オフセ
1193 ットの値には 14 日 (20160 分) を設定する。
1194 ➤ WorkKey (odd) には、ECM を暗号化する WorkKey の次回更新後
1195 の WorkKey (WorkKeyVersion が 3) を設定する。
1196 • 受信機は、DRM サーバから受信した Get Permission Reply message から
1197 「WorkKey (odd) ・ SubscriptionTierBits ・ ExtractInfo」を取得する。
1198 • 受信機は、メタファイルで指定される UsageRuleReference (even) を
1199 設定した Get Permission Request message を作成して、メタファイル
1200 の DRM サーバ URI で指定される DRM サーバに送信する。
1201 • DRM サーバは、UsageRuleReference (even) に対応する「WorkKey
1202 (even) ・ SubscriptionTierBits ・ ExtractInfo」を設定した Get
1203 Permission Reply message を作成して、受信機に送信する。
1204 ➤ SubscriptionTierBits ・ ExtractInfo には、WorkKey (odd) の
1205 SubscriptionTierBits ・ ExtractInfo と同一の値を設定する。また、更
1206 新開始日時オフセットには、WorkKey (odd) の更新開始日時オフ
1207 セットと同一の値を設定する。
1208 ➤ WorkKey (even) には、WorkKey の送信時点で ECM を暗号化す
1209 る WorkKey (WorkKeyVersion が 2) を設定する。
1210 • 受信機は、DRM サーバから受信した Get Permission Reply message から
1211 「WorkKey (even) ・ SubscriptionTierBits ・ ExtractInfo」を取得する。
1212 • 受信機は、取得した一対の「WorkKey ・ SubscriptionTierBits ・
1213 ExtractInfo」で、不揮発性記憶領域に記録した同一
1214 ServiceProviderID ・ 同一 WorkKeyManagementID の一対の
1215 「WorkKey ・ SubscriptionTierBits ・ ExtractInfo」を更新する。

- 1216 • 受信機は、更新開始日時オフセットの値が 14 日（更新される）である
1217 ことから、NotAfter と更新開始日時オフセットとを用いて次回の更新期
1218 間（2012/4/16～2012/4/30、図 A-2 に図示せず）を算出し、次回更新の
1219 制御をおこなう。

1220

1221 ⑨ 全解約

1222 受信機は、2011/10 初旬に事業者サーバに当該 WorkKey に関する全契約の解約を申
1223 し込む。受信機は、解約日を期限とした一対の「WorkKey・SubscriptionTierBits・
1224 ExtractInfo」を取得する。

1225

1226 (11) 事業者サーバからのメタファイルの取得

- 1227 • 受信機は、事業者サーバに対して全契約の解約の要求を送信する。
1228 • 事業者サーバは、受信機からの全解約申し込みを受け付け、DRM サー
1229 バに解約内容を送信するなど、全解約の受付処理を完了する。
1230 • 受信機は、事業者サーバからメタファイルを取得し、受信したメタファ
1231 イルで不揮発性記憶領域に記録したメタファイルを更新する。

1232 (12) DRM サーバからの「WorkKey・SubscriptionTierBits・ExtractInfo」

1233 の取得

- 1234 • 受信機は、メタファイルで指定される UsageRuleReference (odd) を
1235 設定した Get Permission Request message を作成して、メタファイル
1236 の DRM サーバ URI で指定される DRM サーバに送信する。
1237 • DRM サーバは、UsageRuleReference (odd) に対応する「WorkKey
1238 (odd)・SubscriptionTierBits・ExtractInfo」を設定した Get
1239 Permission Reply message を作成して、受信機に送信する。
1240 ➢ NotAfter には、解約月の月末の日時（2011/10/31）を設定する。
1241 ➢ 当該受信機の以降の更新を停止するため、更新開始日時オフセット
1242 の値には 0000h を設定する。
1243 ➢ WorkKey (odd) には、ECM を暗号化する WorkKey の次回更新後
1244 の WorkKey (WorkKeyVersion が 3) を設定する。
1245 • 受信機は、DRM サーバから受信した Get Permission Reply message か
1246 ら「WorkKey (odd)・SubscriptionTierBits・ExtractInfo」を取得する。
1247 • 受信機は、メタファイルで指定される UsageRuleReference (even) を
1248 設定した Get Permission Request message を作成して、メタファイル
1249 の DRM サーバ URI で指定される DRM サーバに送信する。
1250 • DRM サーバは、UsageRuleReference (even) に対応する「WorkKey
1251 (even)・SubscriptionTierBits・ExtractInfo」を設定した Get
1252 Permission Reply message を作成して、受信機に送信する。
1253 ➢ SubscriptionTierBits・ExtractInfo には、WorkKey (odd) の
1254 SubscriptionTierBits・ExtractInfo と同一の値を設定する。また、更
1255 新開始日時オフセットには、WorkKey (odd) の更新開始日時オフ
1256 セットと同一の値を設定する。
1257 ➢ WorkKey (even) には、WorkKey の送信時点で ECM を暗号化す
1258 る WorkKey (WorkKeyVersion が 2) を設定する。
1259 • 受信機は、DRM サーバから受信した Get Permission Reply message か
1260 ら「WorkKey (even)・SubscriptionTierBits・ExtractInfo」を取得する。
1261 • 受信機は、取得した一対の「WorkKey・SubscriptionTierBits・
1262 ExtractInfo」で、不揮発性記憶領域に記録した同一
1263 ServiceProviderID・同一 WorkKeyManagementID の一対の
1264 「WorkKey・SubscriptionTierBits・ExtractInfo」を更新する。

- 1265 • 受信機は、更新開始日時オフセットの値が 0000h（更新されない）であ
1266 ることから、次回以降の更新はおこなわない。

1267

1268 [備考]

- 1269 • DRM サーバ
- 1270 ➤ DRM サーバは、「WorkKey・SubscriptionTierBits・ExtractInfo」の送信に
1271 対して、受信機から以下の SAC 層のメッセージを受信することにより、受
1272 信機の「WorkKey・SubscriptionTierBits・ExtractInfo」の更新を確認できる。
1273 ✧ Command に「Commit」が設定された Encrypted command message
1274 ✧ Request message
1275 したがって、DRM サーバは、odd/even の一対の「WorkKey・
1276 SubscriptionTierBits・ExtractInfo」の送信に対して、上記メッセージを受信
1277 することにより解約処理を完了できる。なお、上記は Get Permission
1278 Protocol と Packed Message Protocol とで共通である。
- 1279 • 受信機
- 1280 ➤ 「WorkKey・SubscriptionTierBits・ExtractInfo」の削除は、受信機の実装依
1281 存とする。ただし、更新開始日時オフセットの値が 0000h（更新されない）
1282 である場合、NotAfter を経過した「WorkKey・SubscriptionTierBits・
1283 ExtractInfo」を削除することが望ましい。このとき、不揮発性記憶領域に記
1284 録した、対応するメタファイルも削除することが望ましい。
- 1285

1286 **A.4 メッセージの例**

1287 本節では、[MIPTV], 4.2 節で規定される IPTV-ES Service Protocol の、コンテンツの
1288 利用に関するメッセージの例を示す。

1289 なお、受信機と DRM サーバとの通信の HTTP ヘッダの例については[IPTVESVOD],
1290 A.3.1 項を、SAC のメッセージの例については[IPTVESVOD], A.3.2 項を参照のこと。
1291

1292 **A.4.1 Service Protocol のメッセージ例**

1293 **A.4.1.1 Get Permission Protocol**

1294 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
1295 を示す。

1296 **A.4.1.1.1 Get Permission Request message**

1297 [MIPTV], 4.2.1.2 項で規定される Get Permission Request message の例を、表 A-3
1298 に示す。

1299

表 A-3 Get Permission Request message の例

バイト インデックス	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	[IPTVESVOD], A.3.3.1.1 項 参照
16-31	UsageRuleReference	0001000001010000000000 0000000000
32	ActionID	02 (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)

1300

1301 **A.4.1.1.2 Get Permission Reply message**

1302 [MIPTV], 4.2.1.3 項で規定される Get Permission Reply message の例を、表 A-4 に
1303 示す。

1304

表 A-4 Get Permission Reply message の例

バイト インデックス	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	WorkKey	00112233445566778899A ABBCCDDEEFF
22-27	WorkKeyID	000100000101
28-29	PrivateData	4EC0
30-37	SubscriptionTierBits	8000000000000000
38-39	ExtractInfoSize	0A (固定値)
40-43	NotBefore	FFFFFFFF
44-47	NotAfter	4B3CCAAF
48-49	RenderingObligation	0000 (固定値)

1305

1306 **A.4.1.2 Get Trusted Time Protocol**

1307 [MIPTV], 4.2.2 項で規定される Get Trusted Time Protocol のメッセージ例について
1308 は、[IPTVESVOD], A.3.3.2 項を参照のこと。

1309

1310 **A.4.1.3 Packed Message Protocol**

1311 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
1312 を示す。

1313

1314 **A.4.1.1.3 Packed Message Request message**

1315 [MIPTV], 4.2.3.2 項で規定される Packed Message Request に格納するリクエストメ
1316 ッセージが A.4.1.1.1 項の場合の例を、表 A-5 に示す。
1317

表 A-5 Packed Message Request message の例

バイト インデックス	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	NumberOfRequest MessageBoxes	0002
6-7	RequestMessageSize	0040
8-71	RequestMessage	A.4.1.1.1 項参照
72-73	RequestMessageSize	0040
74-137	RequestMessage	A.4.1.1.1 項参照

1318

1319 **A.4.1.1.4 Packed Message Reply message**

1320 [MIPTV], 4.2.3.3 項で規定される Packed Message Reply message で、0 項に対して
1321 応答する場合の例を、表 A-6 に示す。
1322

表 A-6 Packed Message Reply message の例

バイト インデックス	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	NumberOfReply MessageBoxes	0002
8-9	ReplyMessageSize	0032
10-59	ReplyMessage	A.4.1.1.2 項参照
34-35	ReplyMessageSize	0032
36-85	ReplyMessage	A.4.1.1.2 項参照

1323