

ICカード ファイル設計の手引き

Ver.1.0

2017年3月22日

JBMIA カード及びカードシステム部会

標準化分科会

本書は、IC カードのファイル設計の参考例として、JICSAP1.1 に準拠したICカード(以下 JICSAP カード)を想定し解説する。

1. IC カードのファイル構成

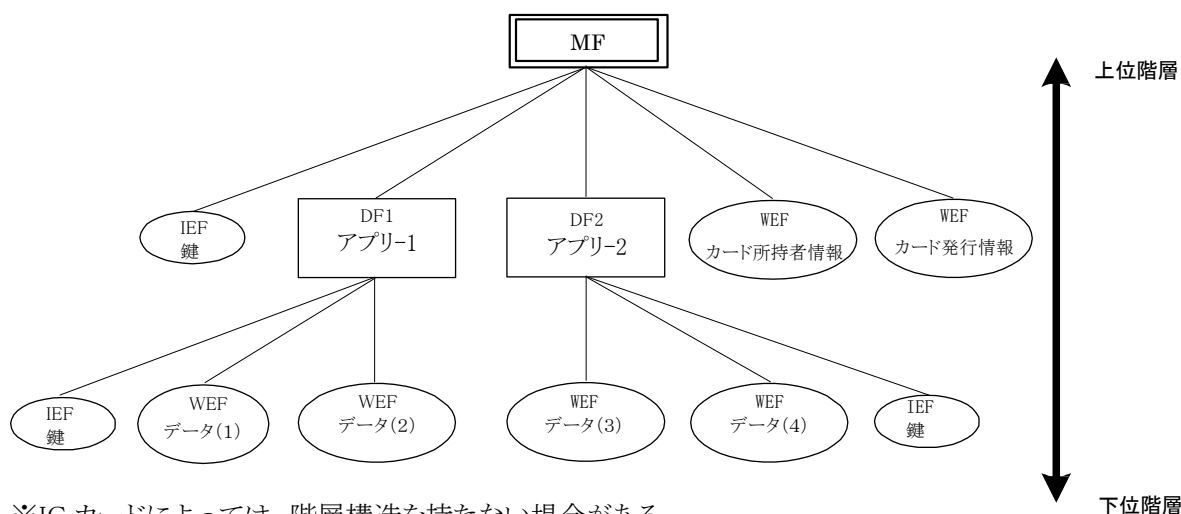
JICSAP カードは、次のファイルで構成される。

- (1) MF: Master File (主ファイル)
 - 特別な DF (専用ファイル)
 - ファイル構造の根幹となる
- (2) DF: Dedicated File (専用ファイル)
 - DF の下位の EF や DF をグループ化するファイル
 - サービス単位、アプリケーション単位等で適切にグループ化することが重要 (JICSAP V1.1 では、DF の階層が2レベルまでサポートされているため、MF 直下の DF のさらに下位に、DF を置くことが可能)
- (3) EF: Elementary File (基礎ファイル)
 - 様々なデータを格納するファイルのことで、大別すると、IEF (内部基礎ファイル) と WEF (作業用基礎ファイル) に分けられる
 - WEF には、一般的なデータが格納される
 - WEF は、データの格納方法として4つのタイプがあり、IC カードが扱うデータによって使い分けができる
 - IEF には、セキュリティのための鍵データが格納される
 - IEF には、照合キーと認証キーの2種類がある

※国際規格においては、アプリケーションの指定を「アプリケーション識別子(AID)」で行い、その内の5バイトが「アプリケーション提供者識別子(RID)」となっている。

※他のシステムとの重複を避けるために、JIS X 6320-5「アプリケーション提供者の登録」により RIDの登録ができる。

【ファイル構成例】



※IC カードによっては、階層構造を持たない場合がある。

2. ファイルの種類

WEF には、①固定長順編成、②可変長順編成、③固定長循環順編成、④透過型の 4 タイプがある。

①固定長順編成ファイル

- レコードファイル
- プログラム作成が容易であり、アクセス速度も一般に速い
- データメモリの使用効率が悪い

②可変長順編成ファイル

- レコードファイル
- ①、③と比べて、データメモリの使用効率が低い
- データを格納する領域のアドレス計算等の制御が複雑になる

③固定長循環順編成ファイル

- レコードファイル
- データ数が、設定した上限値を超えると、最旧データは最新データに置き換えられる
- 直近の取引履歴等を扱うのに適している

④透過型ファイル

- バイナリファイル
- データメモリの使用効率が最も高い
- 多種のデータ群を扱うのに適している

3. アトリビュートの設定

JICSAP カードは、アトリビュートの設定により IC カードに対してアクセスする際の諸条件を設定することができる。IC カードのセキュリティを確保するために、ファイル(EF)ごとに読み書きを制限することができる。

例えば、各EFに対して、誰がどの端末から何が出来るかを指定することができる。以下にアトリビュートの設定の事例をご紹介します。

(1) ユーザキー、ノードキー

ユーザキーは、カード発行者やカード所持者などが使用する鍵として設定する。またノードキーは、IC カードシステムにおける端末が IC カードにアクセスするときに使用する鍵として設定する。

(2) セキュリティ属性

セキュリティ属性は、下の表に示すように、ファイル種別(DF、WEF、IEF)に応じて設定できる。ファイル種別には各々、アクセス種別として3つのレベル(L1、L2、L3)がある。

■DF に対しては、当該 DF の配下の EF へのアクセスを不可能にするための DF 閉塞系と、それを解除するための閉塞解除系、および DF を新規に生成するための創成系の3レベルである。

■WEF に対しては、当該 WEF からデータを読み出す読出し系、新規にデータを書き込む書込み系、および既に書き込まれているデータを書き換える書換え系の3レベルである。

■IEF に対しては、鍵を新規に設定する設定系、既に設定されている鍵を変更する変更系、および不正な鍵照合を所定回数以上行って閉塞されてしまった鍵の閉塞を解除する閉塞解除系の3レベルである。

	L1	L2	L3
DF	閉塞系	閉塞解除系	創成系
WEF	読出し系	書込み系	書換え系
IEF	設定系	変更系	閉塞解除系

(3) 鍵の種類

IC カードは次の3種類の鍵をサポートしている。

JICSAP カードで使用される鍵は、IEF のファイルで設定され、それぞれの役割、セキュリティレベルが選択できる。

① 照合キー

- パスワードなど鍵データをそのままやりとりして照合する鍵

② 内部認証キー

- 外部装置がカードの正当性を確認するための鍵
- セキュアメッセージングが可能

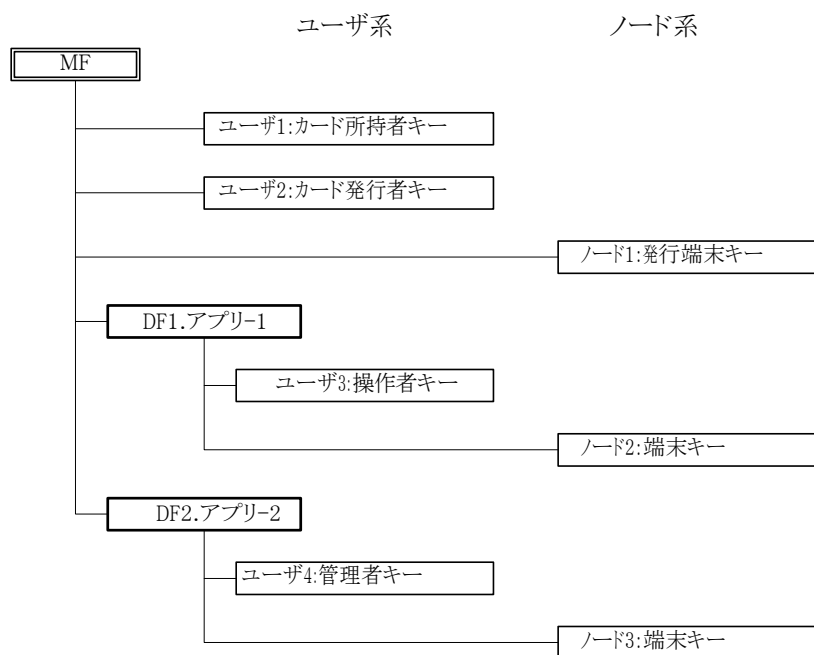
③ 外部認証キー

- カードが外部装置の正当性を確認するための鍵
- セキュアメッセージングが可能

(4) 鍵の組み合わせ論理

ICカードにアクセスするために必要な鍵の組合せを AND 条件や OR 条件で設定できる。
また、アクセス種別ごとに設定することができる。

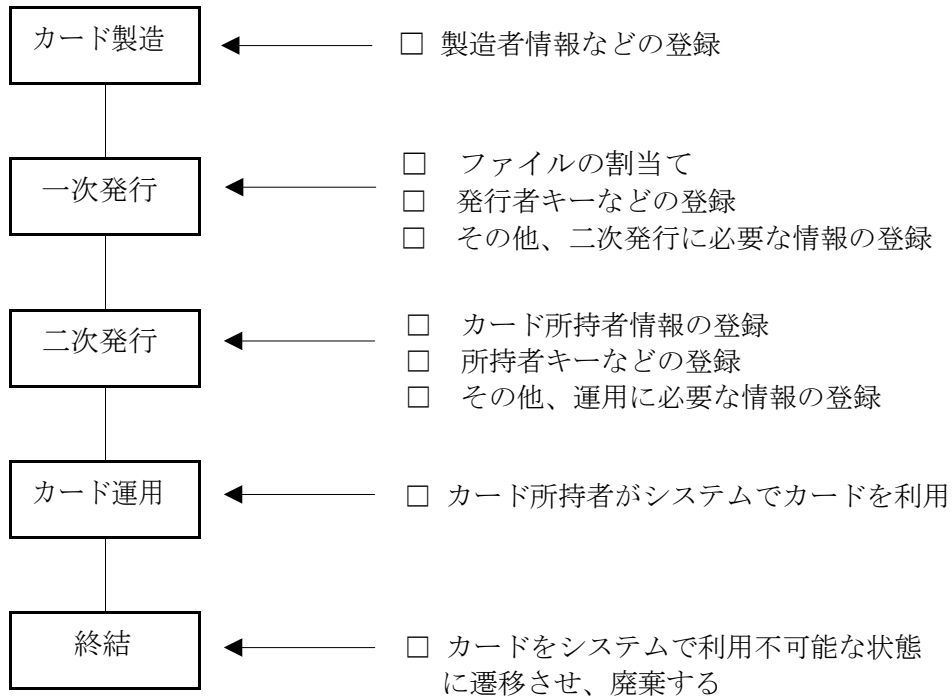
ユーザキーとノードキーの関係(例)



※例えば、「DF1」のファイルを創生するために、「ユーザー2」と「ノード1」の鍵が必要(AND)、「DF2」に設定された WEF にデータを書き込むために、「ノード1」か「ノード3」の鍵が必要(OR)などの設定ができる。

4. IC カードのライフサイクル

IC カードのライフサイクルは、一般に下図のようになる。



※一般に、IC カードを製造し出荷される段階では一次発行済みの状態になっている。

イニシャライズの状態と呼ぶこともある。

※一般に、二次発行はカード発行者が実施する。二次発行済みの状態をパーソナライズの状態と呼ぶこともある。

【参考資料】

参考資料1. ファイル構成・ファイル構造の設定例

種別	EF-ID	名称
MF	DF	3F00 MF
鍵	0011	カード所持者キー
鍵	0012	カード発行者キー
鍵	0013	発行端末キー
L	0001	カード所持者情報
L	0002	カード発行情報
L	001E	WEF:カード識別子
L	2F11	WEF:IC 製造者識別子

種別	EF-ID	名称
DF1	DF	ポイント情報 PointDF
鍵	0014	店員キー
鍵	0015	店舗端末キー
L	0003	ポイント残高
C	0004	購入履歴

種別	EF-ID	名称
DF2	DF	行政情報 administrationDF
鍵	0016	行政担当者キー
鍵	0017	行政端末キー
L	0005	住民基本情報
T	0006	予備情報エリア

種別凡例	T:Transparent	透過型(バイナリ)ファイル
	C:Cyclic	固定長循環順編成ファイル
	L:Linear	固定長順編成ファイル
	規定値	JICSAP で設定が必要な WEF (規定値有り、設計不要)

参考資料2. メモリフォーマットの設定例

(サンプル)

MF	DF-ID	DF名	項目		DF構成	DF	2ケ	セキュリティ ティ属性	アクセス権(ユーザ, P)							アクセス権(ノード, N)							備考				
			項目	サイズ					論理	1	2	3	4	5	6	7	論理	1	2	3	4	5		6	7		
			DF名長	0					閉塞系	OR	●	—	—	—	—	—	—	—	—	—	—	—		—	—	—	
	3F 00	MF	DF名長	0	DF構成	DF	2ケ	閉塞系	OR	—	●	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	
			DFサイズ	—		IEF	3ケ	閉塞解除系	OR	—	●	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	
					WEF		4ケ	創生系	OR	—	●	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	

IEF	EF-ID	EF内容	項目		EF種別	セキュリティ ティ属性	アクセス権(ユーザ, P)							アクセス権(ノード, N)							備考							
			項目	サイズ			論理	1	2	3	4	5	6	7	論理	1	2	3	4	5		6	7					
			キー長	4			照合 or 内部・外部認証	照合	設定系	—	—	—	—	—	—	—	—	—	—	—		—	—	—	—	—	—	—
	00 11	照合 IEF カード所持者キー	キー長	4	照合 or 内部・外部認証	照合	設定系	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	
			EFサイズ	—	キーランク(P,N-1~7)	P-1	変更系	OR	●	●	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	
					不一致上限(1~15)	3回	閉塞解除系	OR	—	●	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—		
	00 12	照合 IEF カード発行者キー	キー長	16	照合 or 内部・外部認証	照合	設定系	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—		
			EFサイズ	—	キーランク(P,N-1~7)	P-2	変更系	OR	—	●	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—		
					不一致上限(1~15)	3回	閉塞解除系	OR	—	●	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—		
	00 13	照合 IEF 発行端末キー	キー長	16	照合 or 内部・外部認証	照合	設定系	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—		
			EFサイズ	—	キーランク(P,N-1~7)	N-1	変更系	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—		
					不一致上限(1~15)	3回	閉塞解除系	OR	—	●	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—		

WEF	EF-ID	EF内容	項目		EF種別	セキュリティ ティ属性	アクセス権(ユーザ, P)							アクセス権(ノード, N)							備考						
			項目	サイズ			論理	1	2	3	4	5	6	7	論理	1	2	3	4	5		6	7				
			レコード長(TL含)	143			レコード or 透過(バイナリ)	レコード	読出し系	—	—	—	—	—	—	—	—	—	—	—		—	—	—	—	—	—
	00 01	WEF カード所持者情報	レコード長(TL含)	143	レコード or 透過(バイナリ)	レコード	読出し系	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	
			レコード数	1	リニア or サイクリック	リニア	書込み系	OR	—	●	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	
			EFサイズ	—	固定長 or 可変長	可変長	書換え系	OR	—	●	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	
	00 02	WEF カード発行情報	レコード長(TL含)	35	レコード or 透過(バイナリ)	レコード	読出し系	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	
			レコード数	1	リニア or サイクリック	リニア	書込み系	OR	—	●	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	
			EFサイズ	—	固定長 or 可変長	可変長	書換え系	OR	—	●	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	
	00 1E	WEF カード識別子	レコード長(TL含)	5	レコード or 透過(バイナリ)	レコード	読出し系	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	
			レコード数	2	リニア or サイクリック	リニア	書込み系	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	
			EFサイズ	—	固定長 or 可変長	固定長	書換え系	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	
	2F 11	WEF IC 製造者識別子	レコード長(TL含)	15	レコード or 透過(バイナリ)	レコード	読出し系	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	
			レコード数	5	リニア or サイクリック	リニア	書込み系	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	
			EFサイズ	—	固定長 or 可変長	可変長	書換え系	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	

DF1	DF-ID	DF名	項目		DF構成	DF	0ケ	2ケ	セキュリティ ティ属性	アクセス権(ユーザ, P)							アクセス権(ノード, N)							備考			
			項目	サイズ						論理	1	2	3	4	5	6	7	論理	1	2	3	4	5		6	7	
			DF名長	—						閉塞系	OR <td>—</td> <td>●</td> <td>—</td> <td>—</td> <td>—</td> <td>—</td> <td>—</td> <td>—</td> <td>—</td> <td>—</td> <td>—</td> <td>—</td> <td>—</td> <td>—</td> <td>—</td> <td>—</td> <td>—</td> <td>—</td> <td>—</td> <td>—</td> <td>—</td> <td>—</td>	—	●	—	—	—	—	—	—	—	—	—	—		—	—	—
		DFポイント情報	DF名長	—	DF構成	DF	0ケ	閉塞系	OR	—	●	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	
		PointDF	DFサイズ	—		IEF	2ケ	閉塞解除系	OR	—	●	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	
					WEF		2ケ	創生系	OR	—	●	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	

IEF	EF-ID	EF内容	項目		EF種別	セキュリティ属性	アクセス権(ユーザ P)							アクセス権(ノード N)							備考	
			項目	サイズ			論理	1	2	3	4	5	6	7	論理	1	2	3	4	5		6
IEF	00 14	照合 IEF 店員キー	キー長	16	照合 or 内部・外部認証 キーランク(P.N-1~7)	照合	設定系	製造時に設定済							製造時に設定済							
			EF サイズ					不一致上限(1~15)	3 回	閉塞解除系	OR	●	●	●	●	●	●	●	●	●	●	
IEF	00 15	照合 IEF 店舗端末キー	キー長	16	照合 or 内部・外部認証 キーランク(P.N-1~7)	照合	設定系	製造時に設定済							製造時に設定済							
			EF サイズ					不一致上限(1~15)	3 回	閉塞解除系	OR	●	●	●	●	●	●	●	●	●	●	

WEF	EF-ID	EF内容	項目		EF種別	セキュリティ属性	アクセス権(ユーザ P)							アクセス権(ノード N)							備考				
			項目	サイズ			論理	1	2	3	4	5	6	7	論理	1	2	3	4	5		6	7		
WEF	00 03	WEF ポイント残高	レコード長(TL 含)	8	レコード or 透過(バイナリ) レニア or サイクリック	レコード	読出し系	OR ● ● ● ● ● ● ● ●							OR ● ● ● ● ● ● ● ●										
			レコード数	1				固定長 or 可変長	固定長	書込み系	OR ● ● ● ● ● ● ● ●							OR ● ● ● ● ● ● ● ●							
			EF サイズ					固定長 or 可変長	固定長		書換え系	OR ● ● ● ● ● ● ● ●							OR ● ● ● ● ● ● ● ●						
WEF	00 04	WEF 購入履歴	レコード長(TL 含)	18	レコード or 透過(バイナリ) レニア or サイクリック	レコード	読出し系	OR ● ● ● ● ● ● ● ●							OR ● ● ● ● ● ● ● ●										
			レコード数	10				固定長 or 可変長	固定長	書込み系	OR ● ● ● ● ● ● ● ●							OR ● ● ● ● ● ● ● ●							
			EF サイズ					固定長 or 可変長	固定長		書換え系	OR ● ● ● ● ● ● ● ●							OR ● ● ● ● ● ● ● ●						

DF2	DF-ID	DF名	項目		DF構成	セキュリティ属性	アクセス権(ユーザ P)							アクセス権(ノード N)							備考				
			項目	サイズ			論理	1	2	3	4	5	6	7	論理	1	2	3	4	5		6	7		
DF2		DF 行政情報 administrationDF	DF 名長	—	DF構成	DF	0ヶ	OR ● ● ● ● ● ● ● ●							OR ● ● ● ● ● ● ● ●										
			DF サイズ	—				JEF	2ヶ	閉塞解除系	OR ● ● ● ● ● ● ● ●							OR ● ● ● ● ● ● ● ●							
								WEF	2ヶ		創生系	OR ● ● ● ● ● ● ● ●							OR ● ● ● ● ● ● ● ●						

IEF	EF-ID	EF内容	項目		EF種別	セキュリティ属性	アクセス権(ユーザ P)							アクセス権(ノード N)							備考	
			項目	サイズ			論理	1	2	3	4	5	6	7	論理	1	2	3	4	5		6
IEF	00 16	照合 IEF 行政担当者キー	キー長	16	照合 or 内部・外部認証 キーランク(P.N-1~7)	照合	設定系	製造時に設定済							製造時に設定済							
			EF サイズ					不一致上限(1~15)	3 回	閉塞解除系	OR	●	●	●	●	●	●	●	●	●	●	
IEF	00 17	照合 IEF 行政端末キー	キー長	16	照合 or 内部・外部認証 キーランク(P.N-1~7)	照合	設定系	製造時に設定済							製造時に設定済							
			EF サイズ					不一致上限(1~15)	3 回	閉塞解除系	OR	●	●	●	●	●	●	●	●	●	●	

WEF	EF-ID	EF内容	項目		EF種別	セキュリティ属性	アクセス権(ユーザ P)							アクセス権(ノード N)							備考				
			項目	サイズ			論理	1	2	3	4	5	6	7	論理	1	2	3	4	5		6	7		
WEF	00 05	WEF 住民基本情報	レコード長(TL 含)	143	レコード or 透過(バイナリ) レニア or サイクリック	レコード	読出し系	OR ● ● ● ● ● ● ● ●							OR ● ● ● ● ● ● ● ●										
			レコード数	1				固定長 or 可変長	可変長	書込み系	OR ● ● ● ● ● ● ● ●							OR ● ● ● ● ● ● ● ●							
			EF サイズ					固定長 or 可変長	可変長		書換え系	OR ● ● ● ● ● ● ● ●							OR ● ● ● ● ● ● ● ●						
WEF	00 06	WEF 予備情報エリア	レコード長(TL 含)	202	レコード or 透過(バイナリ) レニア or サイクリック	レコード	読出し系	OR ● ● ● ● ● ● ● ●							OR ● ● ● ● ● ● ● ●										
			レコード数	1				固定長 or 可変長	可変長	書込み系	OR ● ● ● ● ● ● ● ●							OR ● ● ● ● ● ● ● ●							
			EF サイズ					固定長 or 可変長	可変長		書換え系	OR ● ● ● ● ● ● ● ●							OR ● ● ● ● ● ● ● ●						

※これはシステムを簡略化した設定例につき、実運用設計の際には十分な検討が必要。

参考資料3. 各種初期値の設定例

鍵設定初期値一覧(設定例)

MF 配下

EF-ID	EF内容	EF種別	キーランク	キーデータ(1~16Byte)	[キーデータ(16進表記)]	キー長
0011	カード所持者キー	照合キー	P-1	0000	30303030	4 Byte
0012	カード発行者キー	照合キー	P-2	1234567890ABCDEF	31323334353637383930414243444546	16 Byte
0013	発行端末機キー	照合キー	N-1	9999999999999999	3939393939393939393939393939393939	16 Byte

ポイント情報 DF 配下

EF-ID	EF内容	EF種別	キーランク	キーデータ(1~16Byte)	[キーデータ(16進表記)]	キー長
0014	店員キー	照合キー	P-3	1122334455667788	31313232333334343535363637373838	16 Byte
0015	店舗端末キー	照合キー	N-2	8877665544332211	38383737363635353434333332323131	16 Byte

行政情報 DF 配下

EF-ID	EF内容	EF種別	キーランク	キーデータ(1~16Byte)	[キーデータ(16進表記)]	キー長
0016	行政担当者キー	照合キー	P-4	1122334455667788	31313232333334343535363637373838	16 Byte
0017	行政端末キー	照合キー	N-3	8877665544332211	38383737363635353434333332323131	16 Byte

DF設定初期値一覧(設定例)

ポイント情報 DF 配下

フル DF 名(1~16Byte)	[DF名(16進表示)]	DF 名長
PointDF	506F696E744446	7Byte

行政情報 DF 配下

フル DF 名(1~16Byte)	[DF名(16進表示)]	DF 名長
administrationDF	61646D696E697374726174696F6E4446	16Byte

データ設定初期値一覧(設定例)

MF 配下

EF-ID	データ	EF種別	No. []内 16進表記、()内注釈	データ長
0001	カード所持者情報	可変長順編成	1 Tag=[] (初期入力値無し) (性別(1Byte)+生年月日(8Byte)+氏名(32Byte)+住所(80Byte) +電話番号(10Byte)+会員番号(10Byte))	141 Byte
0002	カード発行情報	可変長順編成	2 Tag=[00] 0000120010401200403310000000A1A1 (発行者コード(5Byte)+発行年月日(8Byte)+有効期限 (8Byte) +シリアル番号(8Byte)+券種(2Byte)+カードバージョン(2Byte))	33 Byte
001E	カード識別子	固定長順編成	1 Tag=[00] 030802	3 Byte
			2 Tag=[01] 00	1 Byte
2F11	IC 製造者識別子	可変長順編成	1 Tag=[45] 4A50303320	5 Byte
			2 Tag=[46] 05	1 Byte
			3 Tag=[47] 053530	3 Byte

ポイント情報 DF 配下

EF-ID	データ	EF種別	No. []内 16進表記、()内注釈	データ長
0003	ポイント情報エリア	固定長順編成	1 Tag=[00] 000000	6 Byte
0004	購入履歴	固定長循環順編成	1 Tag=[] (初期入力値無し) ~10 (年月日(8)+金額(6)+購入店舗(2))	16 Byte

行政情報 DF 配下

EF-ID	データ	EF種別	No. []内 16進表記、()内注釈	データ長
0005	住民基本情報	可変長順編成	1 Tag=[] (初期入力値無し) (性別(1Byte)+生年月日(8Byte)+氏名(32Byte)+住所(80Byte) +電話番号(10Byte)+会員番号(10Byte))	141 Byte
0006	予備情報エリア	可変長順編成	1 Tag=[] (初期入力値無し)	200 Byte

※データ長には Tag,Len 長を含めない。

参考資料4. ファイル構成・ファイル構造の設定用フォーマット

下記の網掛け部分に設定したいファイルの EFID と名称を記入する。
 ファイルの詳細は次ページ以降で記述する。

	種別	EF-ID	名称
MF	DF	3F00	MF
	L	001E	WEF:カード識別子
	L	2F11	WEF:IC 製造者識別子

	種別	EF-ID	名称
DF1	DF	—	

	種別	EF-ID	名称
DF2	DF	—	

種別凡例	T:Transparent	バイナリファイル
	C:Cyclic	循環順編成レコードファイル
	L:Linear	順編成レコードファイル
	規定値	JICSAP で設定が必要な WEF (規定値有り、設計不要)

下記の網掛け部分に記入する。

MF	DF-ID	DF名	項目		DF構成	DF	WEF	セキュリティ属性	アクセス権(ユーザ, P)							アクセス権(ノード, N)							備考		
			項目	サイズ					論理							論理									
									1	2	3	4	5	6	7	1	2	3	4	5	6	7			
	3F 00	MF	DF名長	0	DF構成	DF		閉塞系																	
			DFサイズ			EF		閉塞解除系																	
						WEF		創生系																	

IEF	EF-ID	EF内容	項目		EF種別	セキュリティ属性	アクセス権(ユーザ, P)							アクセス権(ノード, N)							備考				
			項目	サイズ			論理							論理											
							1	2	3	4	5	6	7	1	2	3	4	5	6	7					
			キー長		照合 or 内部・外部認証	設定系																			製造時に設定済
			EFサイズ		キーランク(P,N-1~7)	変更系																			製造時に設定済
					不一致上限(1~15)	閉塞解除系																			
			キー長		照合 or 内部・外部認証	設定系																			製造時に設定済
			EFサイズ		キーランク(P,N-1~7)	変更系																			製造時に設定済
					不一致上限(1~15)	閉塞解除系																			
			キー長		照合 or 内部・外部認証	設定系																			製造時に設定済
			EFサイズ		キーランク(P,N-1~7)	変更系																			製造時に設定済
					不一致上限(1~15)	閉塞解除系																			

WEF	EF-ID	EF内容	項目		EF種別	セキュリティ属性	アクセス権(ユーザ, P)							アクセス権(ノード, N)							備考				
			項目	サイズ			論理							論理											
							1	2	3	4	5	6	7	1	2	3	4	5	6	7					
			レコード長(TL倉)		レコード or 透過(バイナリ)	読出し系																			
			レコード数		リニア or サイクリック	書込み系																			
			EFサイズ		固定長 or 可変長	書換え系																			
			レコード長(TL倉)		レコード or 透過(バイナリ)	読出し系																			
			レコード数		リニア or サイクリック	書込み系																			
			EFサイズ		固定長 or 可変長	書換え系																			
	00 1E	WEF カード識別子	レコード長(TL倉)	5	レコード or 透過(バイナリ)	レコード	読出し系																		フリー
			レコード数	2	リニア or サイクリック	リニア	書込み系																		アクセス禁止
			EFサイズ		固定長 or 可変長	固定長	書換え系																		アクセス禁止
	2F 11	WEF IC 製造者識別子	レコード長(TL倉)	15	レコード or 透過(バイナリ)	レコード	読出し系																		フリー
			レコード数	5	リニア or サイクリック	リニア	書込み系																		アクセス禁止
			EFサイズ		固定長 or 可変長	可変長	書換え系																		アクセス禁止

DF1	DF-ID	DF名	項目		DF構成	DF	WEF	セキュリティ属性	アクセス権(ユーザ, P)							アクセス権(ノード, N)							備考		
			項目	サイズ					論理							論理									
									1	2	3	4	5	6	7	1	2	3	4	5	6	7			
			DF名長		DF構成	DF		閉塞系																	
			DFサイズ			EF		閉塞解除系																	
						WEF		創生系																	

IEF	EF-ID	EF内容	項目	サイズ	EF種別	セキュリティ属性	アクセス権(ユーザ, P)							アクセス権(ノード, N)							備考
			論理	1			2	3	4	5	6	7	論理	1	2	3	4	5	6	7	
IEF			キー長	—	照合 or 内部・外部認証	設定系	製造時に設定済							製造時に設定済							
IEF			EF サイズ	—	キーランク(P.N-1~7)	変更系															
IEF			キー長	—	照合 or 内部・外部認証	閉塞解除系	製造時に設定済							製造時に設定済							
IEF			EF サイズ	—	キーランク(P.N-1~7)	閉塞解除系															
WEF	EF-ID	EF内容	項目	サイズ	EF種別	セキュリティ属性	アクセス権(ユーザ, P)							アクセス権(ノード, N)							備考
			論理	1			2	3	4	5	6	7	論理	1	2	3	4	5	6	7	
WEF			レコード長(TL 含)	—	レコード or 透過(ハイナリ)	読出し系															
WEF			レコード数	—	リニア or サイクリック	書込み系															
WEF			EF サイズ	—	固定長 or 可変長	書換え系															
WEF			レコード長(TL 含)	—	レコード or 透過(ハイナリ)	読出し系															
WEF			レコード数	—	リニア or サイクリック	書込み系															
WEF			EF サイズ	—	固定長 or 可変長	書換え系															
DF2	DF-ID	DF名	項目	サイズ	セキュリティ属性	アクセス権(ユーザ, P)							アクセス権(ノード, N)							備考	
			論理	1		2	3	4	5	6	7	論理	1	2	3	4	5	6	7		
DF2			DF 名長	—	DF構成	閉塞系															
DF2			DF サイズ	—	IEF WEF	閉塞解除系 創生系															
IEF	EF-ID	EF内容	項目	サイズ	EF種別	セキュリティ属性	アクセス権(ユーザ, P)							アクセス権(ノード, N)							備考
			論理	1			2	3	4	5	6	7	論理	1	2	3	4	5	6	7	
IEF			キー長	—	照合 or 内部・外部認証	設定系	製造時に設定済							製造時に設定済							
IEF			EF サイズ	—	キーランク(P.N-1~7)	変更系															
IEF			キー長	—	照合 or 内部・外部認証	閉塞解除系	製造時に設定済							製造時に設定済							
IEF			EF サイズ	—	キーランク(P.N-1~7)	閉塞解除系															
WEF	EF-ID	EF内容	項目	サイズ	EF種別	セキュリティ属性	アクセス権(ユーザ, P)							アクセス権(ノード, N)							備考
			論理	1			2	3	4	5	6	7	論理	1	2	3	4	5	6	7	
WEF			レコード長(TL 含)	—	レコード or 透過(ハイナリ)	読出し系															
WEF			レコード数	—	リニア or サイクリック	書込み系															
WEF			EF サイズ	—	固定長 or 可変長	書換え系															
WEF			レコード長(TL 含)	—	レコード or 透過(ハイナリ)	読出し系															
WEF			レコード数	—	リニア or サイクリック	書込み系															
WEF			EF サイズ	—	固定長 or 可変長	書換え系															

※これはシステムを簡略化した設定例につき、実運用設計の際には十分な検討が必要。

参考資料6. 各種初期値の設定用フォーマット

鍵設定初期値一覧(設定例)

MF 配下

EF-ID	EF内容	EF種別	キーランク	キーデータ(1~16Byte)	[キーデータ(16進表記)]	キー長
						Byte
						Byte
						Byte

DF1 配下

EF-ID	EF内容	EF種別	キーランク	キーデータ(1~16Byte)	[キーデータ(16進表記)]	キー長
						Byte
						Byte

DF2 配下

EF-ID	EF内容	EF種別	キーランク	キーデータ(1~16Byte)	[キーデータ(16進表記)]	キー長
						Byte
						Byte

DF設定初期値一覧(設定例)

DF1 配下

フル DF 名(1~16Byte)	[DF名(16進表示)]	DF 名長

DF2 配下

フル DF 名(1~16Byte)	[DF名(16進表示)]	DF 名長

データ設定初期値一覧(設定例)

MF 配下

EF-ID	データ	EF種別	No.	[]内 16進表記、()内注釈	データ長
					Byte
					Byte
001E	カード識別子	固定長順編成	1	Tag=[00] 030802	3 Byte
			2	Tag=[01] 00	1 Byte
2F11	IC 製造者識別子	可変長順編成	1	Tag=[45] 4A50303320	5 Byte
			2	Tag=[46] 05	1 Byte
			3	Tag=[47] 053530	3 Byte

DF1 配下

EF-ID	データ	EF種別	No.	[]内 16進表記、()内注釈	データ長
					Byte
					Byte

DF2 配下

EF-ID	データ	EF種別	No.	[]内 16進表記、()内注釈	データ長
					Byte
					Byte

※データ長には Tag,Len 長を含めない。