

原議保存期間	5年(平成37年3月31日まで)
有効期間	一種(平成37年3月31日まで)

警視庁交通部長
各道府県警察本部長 殿
各方面本部長
(参考送付先)

警察庁丁運発第70号
平成31年4月3日
警察庁交通局運転免許課長

各管区警察局広域調整担当部長

運転免許証及び運転免許証作成システム等の仕様の改正について

見出しのことについては、「運転免許証及び運転免許証作成システム等の仕様の改正について」（平成28年7月15日付け警察庁丁運発第89号。以下「旧通達」という。）により示しているところ、下記のとおり改正を行い、「運転免許証及び運転免許証作成システム等仕様書（仕様書バージョン番号:008）」（以下「仕様書V8」という。）を別添のとおり策定したので、事務処理上遺漏のないようにされたい。

なお、本通達は、元号を改める政令（平成31年政令第143号）の施行の日から実施することとし、旧通達は、本通達の実施をもって廃止する。

記

1 改正理由

元号を改める政令（平成31年政令第143号）が公布されたことに伴い、所要の改正を行った。

2 改正内容

別紙のとおり。

運転免許証及び運転免許証作成システム等仕様書
(仕様書バージョン番号：008)

- 1 参照規格、略語・用語及び定義・・・・・・・・・・別紙 1
- 2 運転免許証の仕様・・・・・・・・・・別紙 2
(外形寸法、電氣的仕様及び論理ファイル等)
- 3 運転免許証（追記権限等）・・・・・・・・・・別紙 3
及び免許証追記装置の仕様
- 4 運転免許証作成システムの仕様・・・・・・・・・・別紙 4
- 5 運転免許証の仕様・・・・・・・・・・別紙 5
(物理的構造、物理的特性等)
- 6 運転免許証等の様式・・・・・・・・・・別紙 6

警察庁交通局運転免許課

参照規格、略語・用語及び定義

- 1 参照規格
以下の諸規格を参照する。

JIS X 0201	7ビット及び8ビットの情報交換用符号化文字集合
JIS X 0208	7ビット及び8ビットの2バイト情報交換用符号化漢字集合
JIS X 6301: 1998	識別カード-物理的特性
JIS X 6305-6: 2001	識別カードの試験方法 - 第6部:外部端子なしICカード - 近接型
JIS X 6306: 1995	外部端子付きICカード - 共通コマンド
JIS X 6307: 1998	外部端子付きICカード - 共通データ要素
JIS X 6308: 1999	外部端子付きICカード - 第5部:アプリケーション識別子のための付番システム及び登録手続
JIS X 6322-2: 2001	外部端子なしICカード - 近接型 - 第2部:電力伝送及び信号インターフェイス
JIS X 6322-3: 2001	外部端子なしICカード - 近接型 - 第3部 初期化及び衝突防止
JIS X 6322-4: 2002	外部端子なしICカード - 近接型 - 第4部 伝送プロトコル
ISO/IEC 7810: 1995	Identification cards - Physical characteristics
ISO/IEC 7816-4: 1995	Information technology - Identification cards - Integrated circuits card(s) with contacts - Part 4: Interindustry commands for interchange
ISO/IEC 7816-5: 1994	Information technology - Identification cards - Integrated circuits card(s) with contacts - Part 5: Numbering system and registration procedure for application identifiers
ISO/IEC 7816-6: 1996	Information technology - Identification cards - Integrated circuits card(s) with contacts - Part 6: Industry data elements
ISO/IEC 10373-6: 2001	Identification cards - Test methods - Part 6: Proximity cards
ISO/IEC 14443-2: 2000	Identification cards - Contactless integrated circuit(s) card(s) Proximity cards - Part 2: Radio frequency power and signal interface
ISO/IEC 14443-3: 2001	Identification cards - Contactless integrated circuit(s) card(s) Proximity cards - Part 3: Initialization and anti-collision
ISO/IEC 14443-4: 2001	Identification cards - Contactless integrated circuit(s) card(s) Proximity cards - Part 4: Transmission protocol
ISO/IEC 15444-1: 2000	Information technology - JPEG2000 image coding system - Part 1: Core coding system
ISO/IEC 15444-1 AMENDMENT 1: 2000	Information technology - JPEG2000 image coding system - Part 1: Core coding system AMENDMENT 1: Code stream restrictions
ISO/IEC 18013-1	Personal Identification - ISO Compliant Driving Licence - part 1: Physical Characteristics and Basic Data Set
ISO/IEC 18013-2	Personal Identification - ISO Compliant Driving Licence - part 2: Machine Readable Technologies
ITU-T Recommendation T.6: 1988	Facsimile Coding Schemes and Coding Control Functions for Group 4 Facsimile Apparatus
FIPS PUB 46-3	DATA ENCRYPTION STANDARD (DES) U. S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology
FIPS PUB 180-2	SECURE HASH STANDARD U. S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology
PKCS #1 Version 1.5	RSA Cryptography Standard RSA Security Inc.

2 略語・用語及び定義（概要）

以下の略語・用語及び定義（概要）を使用する。

略 語	用 語	定 義（ 概 要 ）
	“0”～“9”及び“A”～“F”	16進数
	b “00000000”～b “11111111”	2進数
0201		JIS X 0201 (8ビット符号化文字集合を使用する)
0208		JIS X 0208
ADC	Application Data Coding, type B	応用データ符号化(B型)(JIS X 6322-3)
AFI	Application Family Identifier card preselection criteria by application, type B	カードの応用分野識別子(B型) (JIS X 6322-3)
AID	Application IDentifier	アプリケーション識別子(JIS X 6308)
ATTRIB	PICC selection command, type B	PICC の選択コマンド(B型)(JIS X 6322-3)
BER	Basic Encoding Rules	基本符号化規則
	BitMap	文字を白と黒のドット集合を使って表現した もの
BINARY	BINARY file	TXT以外のファイル形式
CID	Card IDentifier	カード識別子(JIS X 6322-4)
DES	Data Encryption Standard	米国で標準化されたデータ暗号化規格 (FIPS PUB 46-3)
DF	Dedicated File	専用ファイル(JIS X 6306)
DPIN	Default PIN	デフォルトPIN
EF	Elementary File	基礎ファイル(JIS X 6306)
HEX	HEXadecimal notation	16進法
ID	IDentifier	識別子
IEF	Internal Elementary File	内部基礎ファイル(JIS X 6306)
JPEG2000	Joint Photographic Experts Group 2000	ウェーブレット変換による画像圧縮方式 (ISO/IEC 15444-1)
L	Length	長さ(JIS X 6306)
MF	Master File	主ファイル(JIS X 6306)
MMR	Modified Modified Read code	ITU-T Recommendation T.6で規定された符号 化方式
PCD	Proximity Coupling Device	近接型カード結合装置(JIS X 6322-3)
PICC	Proximity Card	近接型カード(JIS X 6322-3)
PIN	Personal Identification Number	個人識別番号(JIS X 6306) (暗証番号)
PIX	Proprietary application Identifier eXtension	個別アプリケーション識別拡張子 (JIS X 6308)
RFU	Reserved for Future Use	将来利用のために留保(JIS X 6306)
RID	Registered application provider IDentifier	登録アプリケーション提供者識別子 (JIS X 6308)
SHA-256	Secure Hash Algorithm-256	米国で標準化された256ビット長のハッシュ アルゴリズム(FIPS PUB 180-2)
T	Tag	タグ(見出し)(JIS X 6306)
TLV	Tag-Length-Value	タグ(見出し)・長さ・値(JIS X 6306)
TXT	TeXT file	文字コードと限られた制御コードのみからな るファイル
WEF	Working Elementary File	作業用基礎ファイル(JIS X 6306)
(YY)YYMMDD		年月日
	RSA公開鍵暗号方式	RSA SECURITY Inc. が開示する公開鍵暗号方

		式(PKCS #1 Version 1.5)
	実施細則	「警察情報管理システムによる運転者管理業務実施細則の改正について(通達)」(平成31年1月30日付け警察庁丁運発第26号、丁情管発第48号)
	応用データ	PICCCに搭載した応用をPCDに伝える情報(JIS X 6322-3)
	外字	JIS X 0208に規定されていない文字であり、かつ、DF1/EF03 又は DF1/EF05 において定義された文字
	欠字	JIS X 0201、JIS X 0208及び外字以外の文字
	公開鍵	秘密鍵とペアになった公開鍵暗号方式の鍵。本仕様書においては、電子署名の真正性検証に用いる鍵をいう。
	照会番号	都道府県警察の免許台帳の整理番号
	セキュアメッセージング	通信されるデータを暗号によって保護すること。
	電子署名	記録データに改変が行われていないかどうか検証するために格納するBINARYデータ
	デリミタ	データの項目を区切る記号。
	バイト	バイトは、b1~b8と表記された8ビットのデータで構成される。b8を最上位ビット(MSB)、b1を最下位ビット(LSB)とする。(JIS X 6322-3)
	ハッシュアルゴリズム	一方向性の特徴をもったデータ圧縮アルゴリズム
	パディング	データの長さをそろえるため、未使用部分を特定のコードで埋めること。
	秘密鍵	公開鍵とペアになった公開鍵暗号方式の鍵。本仕様書においては、運転免許証に電子署名を行う際に用いる鍵をいう。

運転免許証の仕様（外形寸法、電氣的仕様及び論理ファイル等）

1 外形寸法

JIS X 6301 (ISO/IEC 7810) ID-1型に準拠すること。

2 電氣的仕様

(1) 電力伝送及び信号インタフェース

JIS X 6322-2 B型 (ISO/IEC 14443-2 Type B) に準拠すること。

(2) 初期化及び衝突防止

JIS X 6322-3 B型 (ISO/IEC 14443-3 Type B) に準拠すること。設定値等は以下のとおり。

ア AFI (1 バイト) = “00”

イ ADC (2 ビット) = b “00”

ウ 応用データ (4 バイト) = “00000000”

エ ATTRIB コマンドの形式 (上位階層の情報) : 0 バイト

オ ATTRIB コマンドに対する応答 (上位階層応答) : 0 バイト

(3) 伝送プロトコル

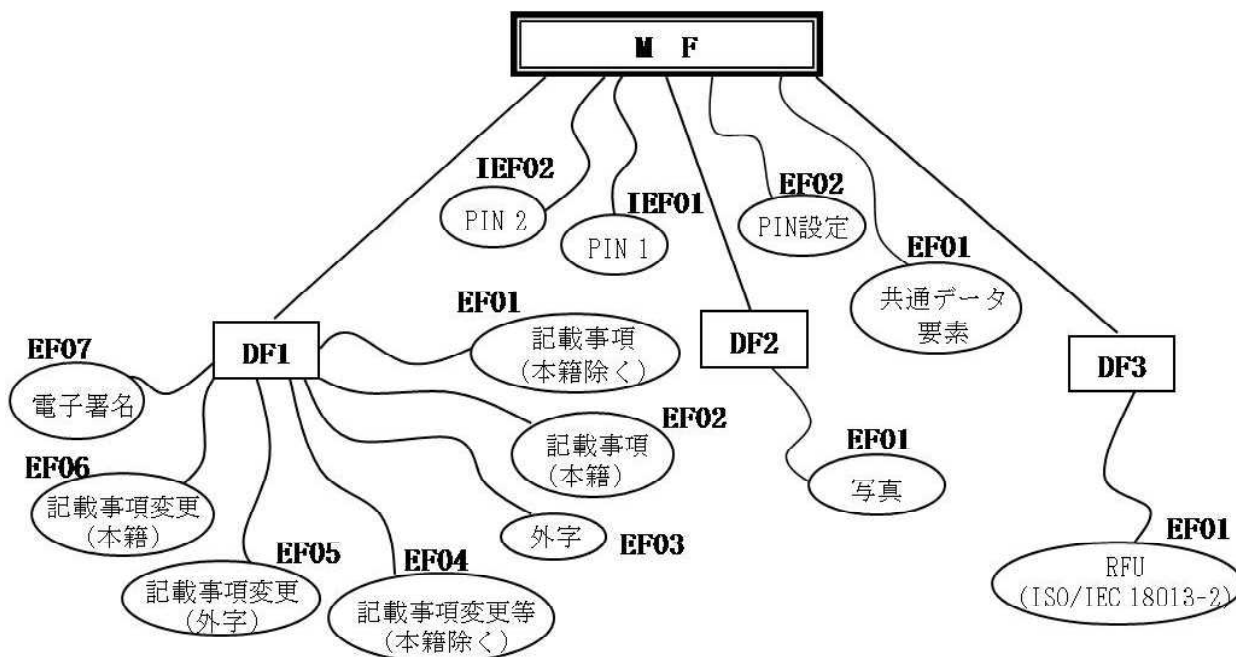
JIS X 6322-4 B型 (ISO/IEC 14443-4 Type B) に準拠すること。

(4) カード識別子 (CID)

CID を実装すること。

3 論理ファイル

(1) 論理ファイル構成図



(2) ファイル構成・内容、基本符号化規則 等

ア ファイル構成

MF/DF	EF	EF 識別子	EF種別	ファイル内容	ファイル容量 (バイト)	備 考
MF	EF01	“2F01”	WEF透過	共通データ要素	17	HEX
	EF02	“000A”	WEF透過	暗証番号(PIN)設定	3	
	IEF01	“0001”	IEF	暗証番号1(PIN 1)	6	格納方法(基本符号化規則)はBER-TLV(3(2)ウ参照)以外も可
	IEF02	“0002”	IEF	暗証番号2(PIN 2)	6	
DF1	EF01	“0001”	WEF透過	記載事項 (本籍除く)	880(注)	TXT
	EF02	“0002”	WEF透過	記載事項(本籍)	82	TXT
	EF03	“0003”	WEF透過	外字	264	BINARY
	EF04	“0004”	WEF透過	記載事項変更等 (本籍除く)	640	TXT
	EF05	“0005”	WEF透過	記載事項変更(外字)	663	BINARY
	EF06	“0006”	WEF透過	記載事項変更(本籍)	256	TXT
	EF07	“0007”	WEF透過	電子署名	578	TXT, BINARY
DF2	EF01	“0001”	WEF透過	写真	2005	BINARY/ JPEG2000
DF3	EF01	“0001”	WEF透過	RFU (ISO/IEC 18013-2)	512	TXT

注 RFUを含む。

イ アプリケーション識別子(AID)(注1)

D F	A I D	
	R I D	P I X
DF1	“A0 00 00 02 31”	“01 00 00 00 00 00 00 00 00 00 00” (注2)
DF2	“A0 00 00 02 31”	“02 00 00 00 00 00 00 00 00 00 00” (注2)
DF3	“A0 00 00 02 48”	“03 00 00 00 00 00 00 00 00 00 00” (注2)

注1 AIDはJIS X 6308(ISO/IEC 7816-5)の規定による。

注2 PIXの先頭1バイトはDF1: “01”

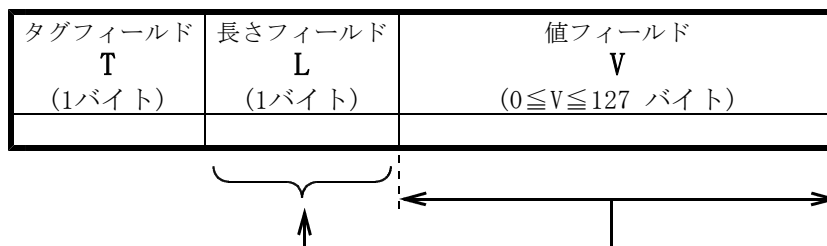
DF2: “02”

DF3: “03” 以降すべて “00” とすること。

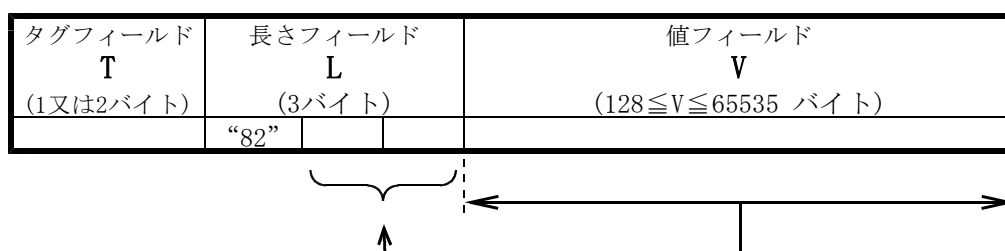
ウ 基本符号化規則

次に示す基本符号化TLV (BER-TLV) フォーマットとする。

(ア) 値フィールドが0～127バイトである場合



(イ) 値フィールドが128～65535バイトである場合



(ウ) 各フィールド

a タグフィールド

DF2/EF01を除き、1バイトで構成され、“01”～“FE”の番号をタグとして付与する。DF2/EF01についてのみ2バイトとする。

b 長さフィールド

1バイト又は3バイトで構成される。

(a) 値フィールドが0～127バイトである場合、第1バイトのb8を0とし、b7～b1で0～127の整数Lを符号化(上位先順)すること。

(b) 値フィールドが128バイト以上である場合、第1バイトには“82”を用いる(“81”は用いない)こととし、後続する2バイトで65535までの整数Lを符号化(上位先順)すること。

c 値フィールド

Lが0でないならば、連続したLバイトから構成される。

Lが0ならば、値フィールドはない。

エ 共通データ要素
格納ファイル名: MF/EF01

タグ	データ長 (バイト)	固/可 (注1)	データ内容 JIS X 6307 (ISO/IEC 7816-6)	符 号
“45”	11	固	カード発行者データ (「仕様書バージョン番号(3バイト)(注2)」+「交付年月日(4バイト)(YYYYMMDD)(注3)」+「有効期間の末日(4バイト)(YYYYMMDD)(注3)」)	0201+HEX+HEX (注6)
“46”	2	固	発行前データ (「カード製造業者識別子(1バイト)(注4)」+「暗号関数識別子(1バイト)(注5)」)	HEX+HEX(注6)

注1 データ長の固定・可変の別を示す(以下同じ。)

注2 (例) 001 → “303031”

注3 西暦とする。

(例) 2004年1月28日 → “20040128”

注4 RFUとする。当分の間“FF”とすること。

注5 「暗号関数識別子」(アルゴリズム)は“04”(Triple DES)とする。Triple DESは、DF1/EF04, DF1/EF05, DF1/EF06への追記及びDF3/EF01の書換え時に使用(別紙3参照)し、PIN(3(2)カ参照)による読み出し時の認証及びセキュアメッセージングは行わない。

注6 デリミタは使用しない。

オ 暗証番号(PIN)設定
格納ファイル名: MF/EF02

タグ	データ長 (バイト)	固/可	データ内容	符 号																											
“05”	1	固	免許保有者の希望により、 ・暗証番号(PIN)を設定する場合はb1を1 ・暗証番号(PIN)を設定しない場合はb1を0 とすること。 <table border="1" style="margin: 10px auto;"> <thead> <tr> <th>b8</th><th>b7</th><th>b6</th><th>b5</th><th>b4</th><th>b3</th><th>b2</th><th>b1</th><th>内 容</th> </tr> </thead> <tbody> <tr> <td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>1</td><td>設定する</td> </tr> <tr> <td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>設定しない</td> </tr> </tbody> </table>	b8	b7	b6	b5	b4	b3	b2	b1	内 容	0	0	0	0	0	0	0	1	設定する	0	0	0	0	0	0	0	0	設定しない	HEX
b8	b7	b6	b5	b4	b3	b2	b1	内 容																							
0	0	0	0	0	0	0	1	設定する																							
0	0	0	0	0	0	0	0	設定しない																							

カ 暗証番号、アクセス権限

(ア) 暗証番号 1 (PIN 1)

格納ファイル名: MF/IEF01

- a PIN 1は4桁の数字(JIS X 0201)とする。
- b 試行許容回数を超えた場合、PIN 1を閉塞処理すること。試行許容回数は3回とする。
- c 閉塞解除権限は各都道府県公安委員会の権限とする。詳細は別紙3で定める。
- d 交付後のPIN変更機能は実装しないこと。
- e MF/EF02の値フィールドVのb1を0とした場合は****(DPIN)を、1とした場合は免許保有者の希望する4桁の数字を記録すること。
*(ASTERISK) = “2A” (JIS X 0201)

(イ) 暗証番号 2 (PIN 2)

格納ファイル名: MF/IEF02

詳細は(ア)に同じ。

(ウ) アクセス権限

MF/DF	EF	読 出	追 記・書 換 え	備 考
MF	EF01, EF02	【FREE】 【FREE】	禁 止	(MF/EF02の値フィールドVのb1が0である場合は、PIN照合にDPINを用いる)
DF1	EF01	【PIN 1】 【DPIN】		
	EF02	【PIN 1 AND PIN 2】 【DPIN AND DPIN】		
	EF03	【PIN 1】 【DPIN】		
	EF04	【PIN 1】 【DPIN】		
	EF05	【PIN 1】 【DPIN】		
	EF06	【PIN 1 AND PIN 2】 【DPIN AND DPIN】		
	EF07	【PIN 1】 【DPIN】		
DF2	EF01	【PIN 1 AND PIN 2】 【DPIN AND DPIN】		
DF3	EF01	【PIN 1】 【DPIN】		

【MF/EF02の値フィールドVのb1が1である場合】

【MF/EF02の値フィールドVのb1が0である場合】

注 記録データの読み出しについては、5(2)流れ図(例)を参照のこと。

(エ) その他

PIN 1, PIN 2は同一番号としてもよい。

キ 記載事項（本籍除く）
格納ファイル名：DF1/EF01

タグ	最大データ長 (バイト)	固/可	データ内容	符 号
“11”	1	固	JIS X 0208 制定年番号(注1)	HEX
“12”	72	可	氏 名(注2)	0208
“13”	32	可	呼び名(カナ)(注2, 注3)	0208
“14”	32	可	通称名(注2, 注4)	0208
“15”	16	固	統一氏名(カナ)(注5)	0208
“16”	7	固	生年月日(元号(注6)YYMMDD)	0201
“17”	80	可	住 所	0208
“18”	7	固	交付年月日(元号(注6)YYMMDD)	0201
“19”	5	固	照会番号	0201
“1A”	6	可	免許証の色区分(優良・新規・その他)	0208
“1B”	7	固	有効期間の末日(元号(注6)YYMMDD)	0201
“1C”	80	可	免許の条件1(注4, 注8)	0208
“1D”	80	可	免許の条件2(注4, 注8)	0208
“1E”	80	可	免許の条件3(注4, 注8)	0208
“1F”	80	可	免許の条件4(注4, 注7, 注8)	0208
“20”	24	可	公安委員会名	0208
“21”	12	固	免許証の番号	0201
“22”	7	固	免許の年月日(二・小・原)(元号(注6)YYMMDD)(注9)	0201
“23”	7	固	免許の年月日(他)(元号(注6)YYMMDD)(注9)	0201
“24”	7	固	免許の年月日(二種)(元号(注6)YYMMDD)(注9)	0201
“25”	7	固	免許の年月日(大型)(元号(注6)YYMMDD)(注9)	0201
“26”	7	固	免許の年月日(普通)(元号(注6)YYMMDD)(注9)	0201
“27”	7	固	免許の年月日(大特)(元号(注6)YYMMDD)(注9)	0201
“28”	7	固	免許の年月日(大自二)(元号(注6)YYMMDD)(注9)	0201
“29”	7	固	免許の年月日(普自二)(元号(注6)YYMMDD)(注9)	0201
“2A”	7	固	免許の年月日(小特)(元号(注6)YYMMDD)(注9)	0201
“2B”	7	固	免許の年月日(原付)(元号(注6)YYMMDD)(注9)	0201
“2C”	7	固	免許の年月日(け引)(元号(注6)YYMMDD)(注9)	0201
“2D”	7	固	免許の年月日(大二)(元号(注6)YYMMDD)(注9)	0201
“2E”	7	固	免許の年月日(普二)(元号(注6)YYMMDD)(注9)	0201
“2F”	7	固	免許の年月日(大特二)(元号(注6)YYMMDD)(注9)	0201
“30”	7	固	免許の年月日(け引二)(元号(注6)YYMMDD)(注9)	0201
“31”	7	固	免許の年月日(中型)(元号(注6)YYMMDD)(注9)	0201
“32”	7	固	免許の年月日(中二)(元号(注6)YYMMDD)(注9)	0201
“33”	7	固	免許の年月日(準中型)(元号(注6)YYMMDD)(注9)	0201
“34”～“3F”			RFU	

注1 参照したJIS X 0208 制定年下2桁とすること。(例) JIS X 0208:1983 → “83”
ただし、JIS C 6226は、“78”とする。

注2 氏と名の間にスペース記号“2121”を挿入すること。

注3 呼び名は「実施細則」の様式1⑨に従うこと。ただし、省略記号は使用しないこと。

注4 記録しない場合は、長さフィールドLを0とすること。

注5 統一氏名は「実施細則」の様式1⑧に従うこと。

注6 明治=1, 大正=2, 昭和=3, 平成=4, 令和=5 (例) 昭和39年2月17日 → 3390217

注7 「免許の条件」が5以上の場合は、DF1/EF04の「新条件」に記録すること。

注8 「免許の条件」の内容が80バイト以上の場合は、複数のTLVに分割して記録すること。
DF1/EF04:「新条件」「備考」「予備」において同じ。

(例)「普通車はアクセル、ブレーキ及びハンドルを一本の操縦レバーで電子制御の下に操作する装置及び方向指示器等に係る操作装置が備え付けられたものに限る」

“1C”:普通車はアクセル、ブレーキ及びハンドルを一本の操縦レバーで電子制御の下に操作する

“1D”:装置及び方向指示器等に係る操作装置が備え付けられたものに限る

注9 免許種別ごとの取得年月日を記録する。保有していない免許種別には 元号(注6)0000
00 を記録、取得年月日が不明な場合は、*****を記録すること。

注10 交付時に「備考」を記録する場合は、DF1/EF04:「備考」に記録すること。

ク 記載事項（本籍）

格納ファイル名：DF1/EF02

タグ	最大データ長 (バイト)	固/可	データ内容	符 号
“41”	80	可	本 籍	0208

ケ 外字

格納ファイル名：DF1/EF03

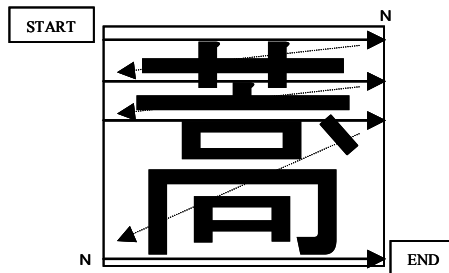
タグ	データ長 (バイト)	固/可	データ内容	符 号
“48”	128(注1)	可	「文字構成(注2)」+「外字1(BitMap MMR符号(注3))」	HEX+BINARY(注4)
“49”	128(注1)	可	「文字構成(注2)」+「外字2(BitMap MMR符号(注3))」	HEX+BINARY(注4)

注1 128バイトを超過する場合がある。

注2 「文字構成」：外字を構成するドット数とする。

(例) 50×50 : “50” 32×32 : “32”

注3 外字の走査方法は、以下のとおりとする。BitMapデータをMMR符号化すること。
(N ドット ×N ドット)



白点 : 0 (Binary)

黒点 : 1 (Binary)

パディング規則は以下のとおり。

- BitMapデータは、バイト単位となるよう下位ビットをb“0”でパディングし、MMR符号化すること。
- 「外字(BitMap MMR符号)」はバイト単位となるよう下位ビットをb“0”でパディングすること。

注4 デリミタは使用しない。

注5 3字以上の外字を有する場合又はDF1/EF03のファイル容量を超過する場合は、以降の外字は、DF1/EF05に記録すること。

コ 記載事項変更等(本籍除く)
格納ファイル名: DF1/EF04

タグ	最大データ長 (バイト)	固/可	データ内容	符 号
“50”	1	固	追記の有無(注1)	HEX
“51” ~ “5F”	25	固	「JIS X 0208 制定年番号(注2)」+「(元号)YYMM DD」+「住所地公安委員会名(注3)」(注4)	HEX+0208+0208 (注5)
“60” ~ “67”	97	可	「JIS X 0208 制定年番号(注2)」+「(元号)YYMM DD」+「新氏名」+「公安委員会名(注3)」	HEX+0208+0208+ 0208(注5)
“68” ~ “6F”	57	可	「JIS X 0208 制定年番号(注2)」+「(元号)YYMM DD」+「新呼び名」+「公安委員会名(注3)」	HEX+0208+0208+ 0208(注5)
“70” ~ “77”	105	可	「JIS X 0208 制定年番号(注2)」+「(元号)YYMM DD」+「新住所」+「公安委員会名(注3)」	HEX+0208+0208+ 0208(注5)
“78” ~ “7F”	105	可	「JIS X 0208 制定年番号(注2)」+「(元号)YYMM DD」+「新条件」+「公安委員会名(注3)」	HEX+0208+0208+ 0208(注5)
“80” ~ “87”	105	可	「JIS X 0208 制定年番号(注2)」+「(元号)YYMM DD」+「条件解除」+「公安委員会名(注3)」	HEX+0208+0208+ 0208(注5)
“88” ~ “8F”	105	可	「JIS X 0208 制定年番号(注2)」+「(元号)YYMM DD」+「備考」+「公安委員会名(注3)」	HEX+0208+0208+ 0208(注5)
“90” ~ “97”	105	可	「JIS X 0208 制定年番号(注2)」+「(元号)YYMM DD」+「予備」+「公安委員会名(注3)」(注7)	HEX+0208+0208+ 0208(注5)

注1 このファイルに追記する場合、初回に限り“11”を記録すること。

注2 DF1/EF01 タグ“11”に同じ。

注3 「住所地公安委員会名」及び「公安委員会名」は5字とする。

(例) 埼玉県公安委員会 → 埼玉県公安

注4 タグ“51”~“5F”は、変更後の住所地公安委員会名及び変更年月日を記録すること。
住所地公安委員会に変更がない場合は記録の必要はない。

注5 デリミタは使用しない。

注6 元号はDF1/EF01に同じ。

注7 各タグの割り当てを超えて記録する必要がある場合は、タグ“90”~“97”を使用すること。

注8 各タグは若い番号のものから使用すること。

サ 記載事項変更(外字)
格納ファイル名: DF1/EF05

タグ	データ長 (バイト)	固/可	データ内容	符 号
“A0”	1	固	追記の有無(注1)	HEX
“A1”	128(注2)	可	「文字構成(注3)」+「外字3(BitMap MMR符号)(注3)」	HEX+BINARY(注4)
“A2”	128(注2)	可	「文字構成(注3)」+「外字4(BitMap MMR符号)(注3)」	HEX+BINARY(注4)
“A3”	128(注2)	可	「文字構成(注3)」+「外字5(BitMap MMR符号)(注3)」	HEX+BINARY(注4)
“A4”	128(注2)	可	「文字構成(注3)」+「外字6(BitMap MMR符号)(注3)」	HEX+BINARY(注4)
“A5”	128(注2)	可	「文字構成(注3)」+「外字7(BitMap MMR符号)(注3)」	HEX+BINARY(注4)

注1 このファイルに追記する場合、初回に限り“11”を記録すること。

注2 128バイトを超過する場合がある。

注3 詳細はDF1/EF03 参照。

注4 デリミタは使用しない。

シ 記載事項変更（本籍）

格納ファイル名：DF1/EF06

タグ	最大データ長 (バイト)	固/可	データ内容	符 号
“AA”	1	固	追記の有無(注1)	HEX
“AB”～“AF”	105	可	「JIS X 0208 制定年番号(注2)」+「(元号)YYMM DD」+「新本籍」+「公安委員会名(注3)」	HEX+0208+0208+ 0208(注4)

注1 このファイルに追記する場合、初回に限り“11”を記録すること。

注2 DF1/EF01 タグ“11”に同じ。

注3 「公安委員会名」は5字とする。

注4 デリミタは使用しない。

注5 元号はDF1/EF01に同じ。

注6 各タグは若い番号のものから使用すること。

ス 電子署名

格納ファイル名：DF1/EF07

タグ	最大データ長 (バイト)	固/可	データ内容	符 号
“B1”	256	固	電子署名	BINARY
“B2”	16	固	シリアル番号	0201
“B3”	48	可	(RFU)	0201
“B4”	80	可	発行者名	0201
“B5”	130	可	主体者名	0201
“B6”	32	可	主体者鍵識別子	BINARY

注 電子署名のアルゴリズム等は4項「電子署名」参照のこと。

セ 写真

格納ファイル名：DF2/EF01

タグ	最大データ長 (バイト)	固/可	データ内容	符 号
“5F40”	2000	可	写真(JPEG2000)	BINARY

ソ ISO/IEC 18013-2

格納ファイル名：DF3/EF01

タグ	最大データ長 (バイト)	固/可	データ内容	符 号
RFU (ISO/IEC 18013-2)				

タ 外字及び欠字の取り扱い

(ア) 外字文字符号と外字BitMapの対応及び欠字文字符号

文字符号“FFF1”～“FFF7”及び“FFFA”は、それぞれ外字及び欠字と規定し、以下のように対応させる。

外字(欠字) 文字符号	格納ファイル名	タグ	備考
“FFF1”	DF1/EF03	“48”	外字1
“FFF2”	DF1/EF03	“49”	外字2
“FFF3”	DF1/EF05	“A1”	外字3
“FFF4”	DF1/EF05	“A2”	外字4
“FFF5”	DF1/EF05	“A3”	外字5
“FFF6”	DF1/EF05	“A4”	外字6
“FFF7”	DF1/EF05	“A5”	外字7
“FFFA”	欠 字		

(イ) 外字(欠字)記録方法(例)

氏 名 : 日 本 ● 蒿 子
 ↓ / ↓ / ↓ ↓ ↓
 文字符号 : “467C” / “4B5C” / “2121” / “FFF1” / “3B52”
 記録データ: “467C4B5C2121FFF13B52”

(ウ) 外字使用の優先順位

- 第1優先: 「本 籍」
- 第2優先: 「氏 名」
- 第3優先: 「免許の条件」
- 第4優先: 「住 所」
- 第5優先: 「通称名」

の順とする。

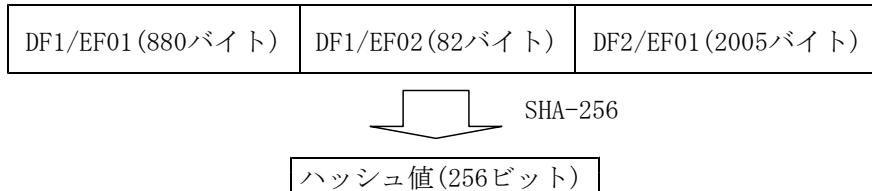
4 電子署名

(1) ハッシュアルゴリズム

SHA-256とする。

DF1/EF01, DF1/EF02 及び DF2/EF01に記録されている全データを元データとしてハッシュ値を生成すること。

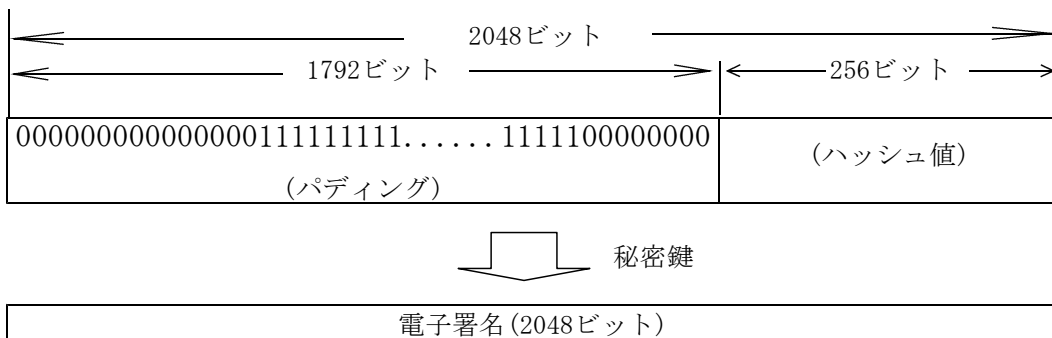
DF1/EF01, DF1/EF02 及び DF2/EF01の順序等を下図に示す。



(2) 電子署名アルゴリズム

鍵長2048ビットのRSA公開鍵暗号方式を使用し、4 (1)ハッシュ値に対して電子署名の生成を行うこと。パディング規則は、PKCS #1 Version 1.5 に準拠すること。

(参考)



パディング : 上位16ビット =b “0000 0000 0000 0001”

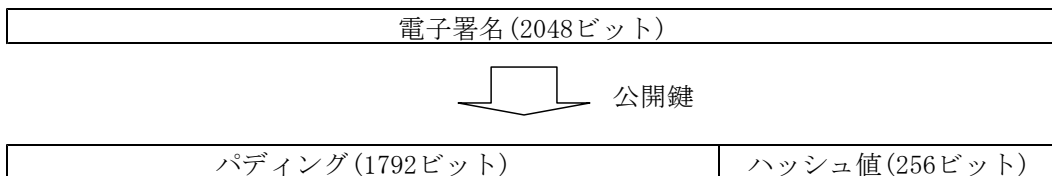
下位 8 ビット =b “0000 0000”

残りのビットはすべてb “1”

(3) 電子署名の検証

公開鍵を使用し、電子署名を復号することにより検証する。

(参考)



4 (1)及び4 (3)のハッシュ値を比較する。両者が一致しない場合は、運転免許証として正規に作成されたものでないか、DF1/EF01, DF1/EF02, DF2/EF01のいずれか又は全部について改ざんがなされた可能性がある。

5 記録データの読み出し

(1) 使用コマンド

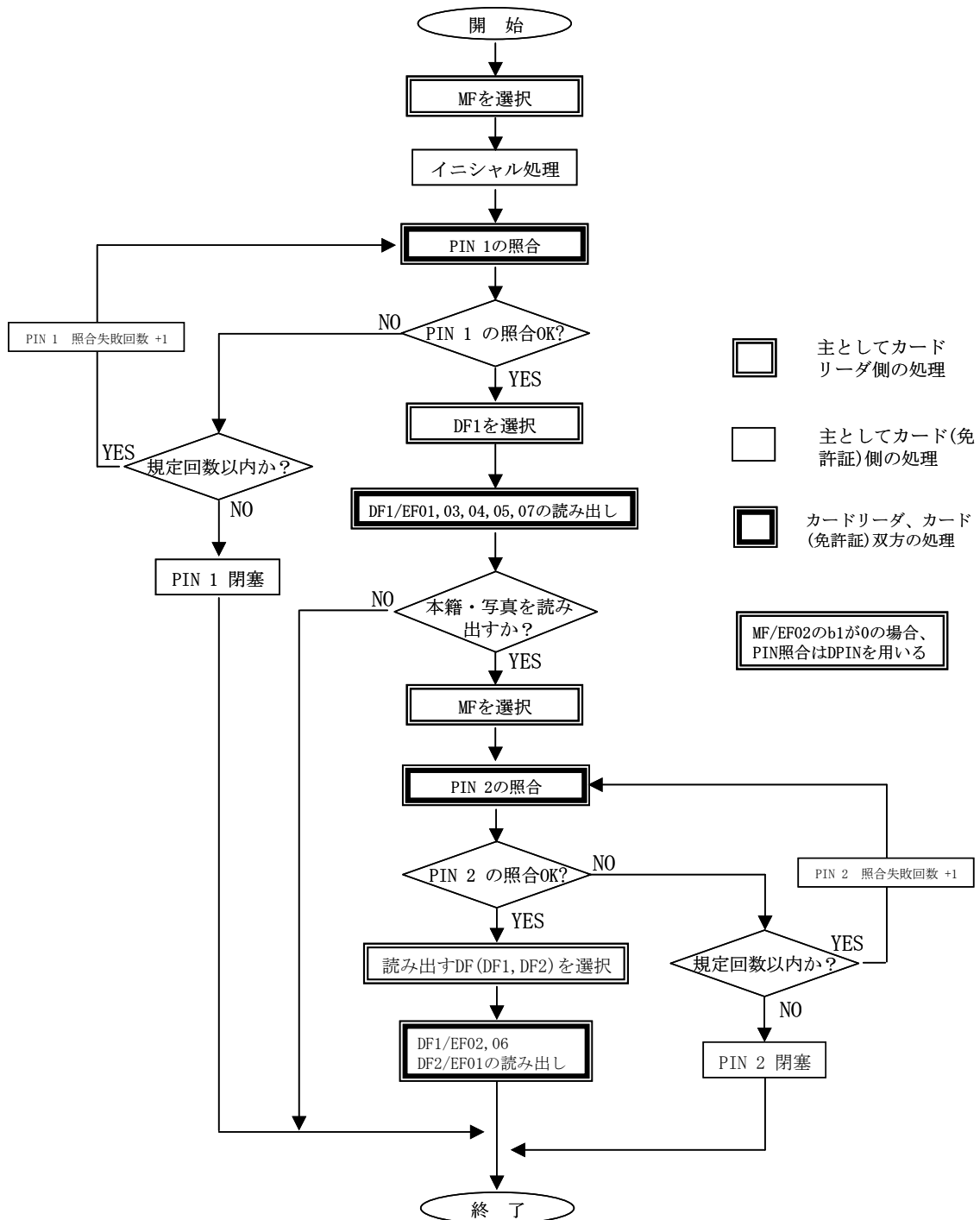
JIS X 6306 (ISO/IEC 7816-4) 規定の以下コマンドを使用する。コマンド機能仕様等を別添 2-1 に示す。

SELECT FILE コマンド

VERIFY コマンド

READ BINARY コマンド

(2) 流れ図(例)



コマンド機能仕様等

- 1 略語・用語及び定義(概要)
以下の略語・用語及び定義(概要)を使用する。

略語	用語	定義(概要)
APDU	Application Protocol Data Unit	応用プロトコルデータ単位(JIS X 6306)
CLA	CLAss Byte	クラスバイト(JIS X 6306)
FCI	File Control Information	ファイル制御情報(JIS X 6306)
INS	INStRuction byte	命令バイト(JIS X 6306)
P1-P2	Parameter byte	パラメータバイト(JIS X 6306)
SW1-SW2	Status byte	ステータスバイト(JIS X 6306)

2 ファイル構造・形式

- (1) 概要
ファイル構造は、JIS X 6306(ISO/IEC 7816-4)に基づく。
- (2) ファイルの構成と種類
ファイルの分類として、次を規定する。
専用ファイル(DF)
基礎ファイル(EF)

カード内に格納されたデータの論理構成は、次に示す専用ファイルの階層構造とする。

- DFの根幹は、主ファイル(MF)とする。
DFの階層の深さは、1レベルをサポートする。
EFは、以下の2種類の用途別ファイルが規定される。
WEF: アプリケーションが使用するデータを格納する。
IEF: 鍵データを格納する。

- (3) ファイルの選択
ファイルは、以下に述べる方法で選択可能とする。
- ア DF名による選択
DFは、指定されたAIDで符号化されたフルDF名によって選択される。このフルDF名は、免許証内で唯一である。
- イ ファイルIDによる選択
EFの選択に用いられ、2バイトで符号化したEF識別子によって選択される。
DF直下のすべてのEFは、異なる識別子を持たなければならない。全てのEFは、2バイト(“0000”～“FFFF”)で構成されたEF識別子によって選択される。特に、EF識別子が“0001”から“001E”の場合には、5ビットで符号化した1から30までの短縮EF識別子によって選択される。
- (4) ファイルポインタ
一度選択したファイルをカレントファイルとして、後続コマンドで暗黙的に選択できるように、ファイルポインタを持つ。ファイルポインタは、免許証の電氣的活性化直後にMFを指す。
- (5) 論理チャンネル
論理チャンネルはチャンネル0を使用する。

(6) 基礎ファイルの構造・特徴

作業用基礎ファイル(WEF)は、透過構造ファイル(透過ファイル)をサポートする。
透過構造ファイル(透過ファイル)は、以下の特徴をもつ。

ア 1つのバイナリデータは、8ビット。

イ 初期値は、“FF”とする。

3 コマンド構造

メッセージ構造はJIS X 6306 (ISO/IEC 7816-4)に規定される。

コマンドAPDUはコマンド送信のためのメッセージ構造で、下図に示すコマンド基本構造を持つ。

見出し部(ヘッダ)				本体部(ボディ)		
CLA	INS	P1	P2	Lc	データフィールド	Le
(1)	(1)	(1)	(1)	(後述)	(Lcで指定)	(後述)

Lc : コマンドAPDUのデータフィールド(コマンドデータ)の長さ(バイト数)。

Le : レスポンスAPDUのデータフィールド(レスポンスデータ)の期待する最大長(バイト数)。

(1) コマンドAPDU

コマンドAPDUは、コマンドの種類により以下のように分類される。

Case 1: コマンドデータ無し、レスポンスデータ無し

ヘッダ

(4)

Case 2: コマンドデータ無し、レスポンスデータ有り

ヘッダ	ボディ
	Le

(4)

(1 or 3)

Case 3: コマンドデータ有り、レスポンスデータ無し

ヘッダ	ボディ	
	Lc	データフィールド

(4)

(1 or 3)

(Lcで指定)

Case 4: コマンドデータ有り、レスポンスデータ有り

ヘッダ	ボディ		
	Lc	データフィールド	Le

(4)

(1 or 3)

(Lcで指定)

(1 or 2)

Lc, Leは、短縮(1バイトで長さを表現)、拡張(2バイトで長さを表現)が指定できる。

拡張の場合は、ボディの最初にあるLcかLeの先頭に1バイトの“00”を追加する。

Lcが表現できる長さは、

短縮: 1~255 (“01” ~ “FF”)

拡張: 256~65535 (“0100” ~ “FFFF”)

Leが表現できる長さもLcと同様であるが、0の場合は、短縮で256、拡張で65536を表す。

拡張Lcを許すコマンドの場合、拡張Lcで1~255 (“000001” ~ “0000FF”)を表現していてもエラーとしないが、拡張Lcを許さないコマンドの場合は、エラーとなる。

(2) レスポンスAPDU

レスポンスAPDUはコマンドAPDUに対するレスポンスのメッセージ構造で、下図の構造を持つ。

レスポンスデータがない場合(コマンドAPDUのCase 1, 3の場合)

後続部(トレイラ)	
SW1	SW2
(1)	(1)

レスポンスデータがある場合(コマンドAPDUのCase 2, 4の場合)

ボディ	トレイラ	
データ	SW1	SW2
(可変)	(1)	(1)

データの長さは、コマンドAPDUのLeを超えない範囲で可変である。
ただし、プロセスが中断された場合は、トレイラのみとなる。

トレイラ	
SW1	SW2
(1)	(1)

(3) クラスバイト

コマンドAPDUのクラスバイトCLAは、ISO/IEC 7816-4に対する準拠の程度、セキュアメッセージング機能の適用の有無及び論理チャンネルの番号を表す。

下表に、本仕様で規定されるCLAの符号化規則を示す。

b8	b7	b6	b5	b4	b3	b2	b1	意味
0	0	0	0					ISO/IEC 7816-4準拠コマンド
1	0	0	0					ISO/IEC 7816-4準拠コマンド以外
				0	0			セキュアメッセージング非適用
				1	1			セキュアメッセージング適用(暗号化+認証)
						0	0	論理チャンネル0

網掛け部は規定しないことを示す(以下同じ。)

(4) コマンド一覧

下表に、本仕様で規定されるコマンドの一覧を示す。

項番	コマンド名	CLA	INS	コマンドのCase			
				1	2	3	4
1	SELECT FILE	0x	A4	○		○	○
2	VERIFY		20	○		○	
3	READ BINARY		B0		●		

表中のコマンドのCase欄にある印は、各コマンドがどのCaseで送信されてくるかを表している。その中でブロック連鎖(チェーン)が発生する場合は下記の印で表現している。

●: レスポンスにチェーンあり。

4 基本コマンド

(1) SELECT FILE コマンド

ア 定義及び適用範囲

本コマンドは、カレントファイルを設定するために使用される。
 以降のコマンドは、カレントファイルを暗黙的に参照することができる。
 DF選択後、その配下にカレントEFは存在しない。

イ 使用条件及びセキュリティ条件

本コマンドに対するレスポンスAPDUのステータスバイトが「プロセス完了」示す場合、セキュリティステータスが変化する。セキュリティ要件は、別紙2 3(2)カを参照のこと。

ウ コマンドAPDU

MFの選択

(Case 1)

CLA	INS	P1	P2
“0x”	“A4”	“00”	“00”
(1)	(1)	(1)	(1)

(Case 3)

CLA	INS	P1	P2	Lc	データフィールド
“0x”	“A4”	“00”	“00”	“02”	“3F00”
(1)	(1)	(1)	(1)	(1)	(2)

DFの選択 (FCI要求なし)

(Case 3 or 4)

CLA	INS	P1	P2	Lc	データフィールド
“0x”	“A4”				
(1)	(1)	(1)	(1)	(1)	(1~16)

EFの選択 (FCI要求なし)

(Case 3)

CLA	INS	P1	P2	Lc	データフィールド
“0x”	“A4”	“02”	“0C”	“02”	(EF-ID)
(1)	(1)	(1)	(1)	(1)	(2)

パラメタ名	長さ	意味	備考
P1	1	選択制御子	下表参照
P2	1	選択オプション	下表参照
Lc	1	DF名の長さ、又はEF識別子の長さ	
データフィールド	1~16	DF名(フルDF名)、又はEF識別子	

注 互換性のためP2の設定でFCI応答なしとする。

P1コーディング

b8	b7	b6	b5	b4	b3	b2	b1	意味
0	0	0	0	0	0	x	x	ファイルIDによる選択
						1	0	カレントDFの直下のEF(データ部=EF-ID)
						1	1	親DF(データ部なし)
0	0	0	0	0	1	0	0	DF名による直接選択(データフィールド=DF名)

P2コーディング

b8	b7	b6	b5	b4	b3	b2	b1	意味
0	0	0	0	0	0			FCIオプションテンプレート応答
0	0	0	0	1	1			FCI応答なし
						0	0	最初又は唯一のファイルを選択
						1	0	次のファイルを選択(パーシャルDF名指定可能)

エ レスポンスAPDU

SW1	SW2
-----	-----

(1) (1)

パラメタ名	長さ	意味	備考
SW1-SW2	2	ステータスバイト	

オ 特記事項

- (ア) レスポンスAPDUのステータスバイトが「プロセス中断」を示す時は、免許証内の全てのセキュリティステータスは何も変化せず保持される。
- (イ) DFの閉塞状態が通知される場合(SW1-SW2=“6283”)でも、そのファイルはカレントファイルとなる。
- (ウ) MF選択の場合、P2=“00”となるが、FCIは返さない。

カ ステータスバイト一覧表

ステータス		ステータスの意味	実行状態	
SW1	SW2			
“90”	“00”	正常終了	正常終了	プロセス完了
“62”	“83”	不揮発性メモリの状態は、変化していない DFが閉塞している	警告処理	
“64”	“00”	不揮発性メモリの状態は、変化していない ファイルの制御情報に異常がある	実行エラー	プロセス中断
“67”	“00”	Lc/Leが間違っている	点検エラー	
“68”	“81”	CLAの機能が提供されていない 指定された論理チャンネルの番号によるアクセス機能を提供しない	エラー	
	“82”	セキュアメッセージング機能を提供しない		
“6A”	“81”	間違ったパラメタ 機能を提供しない	エラー	
	“82”	アクセス対象ファイルが無い		
	“86”	P1-P2の値が正しくない		
	“87”	Lcの値がP1-P2に矛盾している		
“6D”	“00”	INSが提供されていない		
“6E”	“00”	クラスが提供されていない		

(2) VERIFY コマンド

ア 定義及び適用範囲

本コマンドは、外部装置から送られる照合鍵を、免許証内で照合させるために使用される。

イ 使用条件及びセキュリティ条件

コマンドは、有効な短縮EF識別子により指定したEF、あるいはカレントEFに対して実行される。

本コマンドに対するレスポンスAPDUのステータスバイトが「プロセス完了」を示す場合、指定したEFはカレントEFになる。

セキュリティステータスは、照合鍵が一致した場合、更新される。

照合失敗回数は、免許証内に記録される。

照合鍵の長さ不一致の場合も、照合失敗回数を加算する。

ウ コマンドAPDU

残りの照合許容回数の出力指定 (Case 1)

CLA	INS	P1	P2
“0x”	“20”	“00”	
(1)	(1)	(1)	(1)

照合 (Case 3)

CLA	INS	P1	P2	Lc	データフィールド
“0x”	“20”	“00”			
(1)	(1)	(1)	(1)	(1)	(1~16)

パラメタ名	長さ	意味	備考
P1	1	(特になし)	“00” 固定 (他の値はRFU)
P2	1	参照データの限定子	下表参照
Lc	1	照合鍵の長さ	別紙2 3(2)カ(ア)参照
データフィールド	1~16	照合鍵	

P2コーディング

b8	b7	b6	b5	b4	b3	b2	b1	意味	
1	0	0						固定	
			0	0	0	0	0	カレントEF指定	
			0	0	0	0	1	短縮EF識別子指定	
			~						
			1	1	1	1	0		

エ レスポンスAPDU

SW1	SW2
(1)	(1)

パラメタ名	長さ	意味	備考
SW1-SW2	2	ステータスバイト	

オ 特記事項

ボディが空の時、このコマンドは残りの照合許容回数“x”を返す(SW1-SW2=“63Cx”、既に閉塞状態にあるものについては“63C0”)。

カ ステータスバイト一覧表

ステータス		ステータスの意味	実行状態	
SW1	SW2			
“90”	“00”	正常終了	正常終了	プロセス完了
“63”		不揮発性メモリの状態は、変化している	警告処理	
	“00”	照合の不一致である		
	“Cx”	照合の不一致である[“x”によって、残りの試行可能回数を示す]		
“64”		不揮発性メモリの状態は、変化していない	実行エラー	プロセス中断
	“00”	ファイルの制御情報に異常がある。		
“65”		不揮発性メモリの状態は、変化している		
	“81”	メモリの書き込みが失敗した		
“67”	“00”	Lc/Leが間違っている	点検エラー	
“68”		CLAの機能が提供されていない		
	“81”	指定された論理チャンネルの番号によるアクセス機能を提供しない		
	“82”	セキュアメッセージング機能を提供しない		
“69”		コマンドは許可されない		
	“81”	ファイル構造と矛盾したコマンドである		
	“84”	参照されたIEFが閉塞している		
	“86”	カレントEFが無い		
“6A”		間違ったパラメタ		
	“81”	機能を提供しない		
	“82”	アクセス対象ファイルが無い		
	“86”	P1-P2の値が正しくない		
	“88”	参照された鍵が正しく設定されていない		
“6D”	“00”	INSが提供されていない		
“6E”	“00”	クラスが提供されていない		

(3) READ BINARY コマンド

ア 定義及び適用範囲

本コマンドは、透過構造のWEF内のバイナリデータを読み出すために使用される。

イ 使用条件及びセキュリティ条件

コマンドは、有効な短縮EF識別子により指定したEF、あるいはカレントEFに対して実行される。

本コマンドに対するレスポンスAPDUのステータスバイトが「プロセス完了」を示す場合、指定したEFはカレントEFになる。

DFが閉塞している場合、「プロセス中断」となる。

ウ コマンドAPDU

(Case 2)

CLA	INS	P1	P2	Le
“0x”	“B0”			
(1)	(1)	(1)	(1)	(1 or 3)

パラメタ名	長さ	意味	備考
P1-P2	2	読み出し対象短縮EF識別子及び読み出すべき最初のバイナリデータの相対アドレス	下表参照
Le	1 or 3	読み出しバイト数	

P1-P2コーディング(相対アドレス15ビット指定)

P1								P2								意味
b8	b7	b6	b5	b4	b3	b2	b1	b8	b7	b6	b5	b4	b3	b2	b1	
0																相対アドレス15ビット指定
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	相対アドレス(15ビット)
~								~								
	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

P1-P2のコーディング(相対アドレス8ビット指定)

P1								P2								意味
b8	b7	b6	b5	b4	b3	b2	b1	b8	b7	b6	b5	b4	b3	b2	b1	
1	0	0														相対アドレス8ビット指定
			0	0	0	0	0									カレントEF指定
			0	0	0	0	1									短縮EF識別子指定
~								~								
			1	1	1	1	0									相対アドレス(8ビット)
~								~								
								1	1	1	1	1	1	1	1	

エ レスポンスAPDU

(チェーンあり)

データ	SW1	SW2
(可変)	(1)	(1)

パラメタ名	長さ	意味	備考
データ	可変	読み出されたデータ	
SW1-SW2	2	ステータスバイト	

コマンドAPDUのLeが0である場合は、短縮Leでは256の範囲で、又は拡張Leでは65536の範囲で、ファイルの最後まで参照すべき全てのバイト数を読み出す。

オ ステータスバイト一覧表

ステータス		ステータスの意味	実行状態	
SW1	SW2			
“90”	“00”	正常終了	正常終了	プロセス完了
“62”	“83”	不揮発性メモリの状態は、変化していない DFが閉塞している	警告処理	
“64”	“00”	不揮発性メモリの状態は、変化していない ファイルの制御情報に異常がある	実行エラー	プロセス中断
“67”	“00”	Lc/Leが間違っている	点検エラー	
“68”	“81”	CLAの機能が提供されていない 指定された論理チャンネルの番号によるアクセス機能を提供しない		
	“82”	セキュアメッセージング機能を提供しない		
“69”	“81”	コマンドは許可されない ファイル構造と矛盾したコマンドである		
	“82”	セキュリティステータスが満足されない		
	“86”	カレントEFが無い		
“6A”	“82”	間違ったパラメタ アクセス対象ファイルが無い		
	“86”	P1-P2の値が正しくない		
“6B”	“00”	EF範囲外にオフセット指定した		
“6D”	“00”	INSが提供されていない		
“6E”	“00”	クラスが提供されていない		

運転免許証（追記権限等）及び免許証追記装置の仕様

（概要）

記載事項変更時等における追記権限及び免許証追記装置の仕様について定めている。

運転免許証作成システムの仕様

(概要)

運転免許証作成システムの構成及び仕様について定めている。

運転免許証の仕様（物理的構造、物理的特性等）

（概要）

運転免許証の物理的構造、物理的特性等の細部事項について定めている。

運転免許証等の様式

(概要)

運転免許証等の様式の細部事項について定めている。