原議保存期間	5年(令和12年3月31日まで)
有 効 期 間	一種(令和12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）
各管区警察局広域調整担当部長

警察庁丁運発第145号
令 和 6 年 7 月 19 日
警察庁交通局運転免許課長

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」（令和４年８月30日付け警察庁丁運発第187号）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:010）」（以下「仕様書Ｖ１０」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。

本通達は令和４年４月27日に交付された道路交通法の一部を改正する法律（令和４年法律第32号。以下「改正法」という。）の施行後の仕様について策定したものであるため、改正法の施行前については、前記通達を参照すること。

なお、改正法の施行をもって前記通達は廃止する。

記

１　改正理由

改正法において、運転免許に係る情報の個人番号カードへの記録に関する規程が整備されたことから、運転免許証作成システム等のインタフェースの変更等に対応させるため、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：010）

警察庁交通局運転免許課

別紙１

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。

規　　格	定　義（概　要）
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)
AES	Advanced Encryption Standard	米国で標準化されたデータ暗号化規格 (FIPS 197)
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)
ELF-AID	Executable and Linking Format － Application IDentifier	カードAPのバイナリファイルを管理するAID （ICカード内部で管理されるAID）
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	ウエ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)」(令和５年８月23日付け警察庁丁運発第123号、丁技企発第709号)
	インスタンス-AID	記録データの読出し時にSELECT FILEコマンドを使用するときのAID
	応用データ	PICC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
	実行モジュール-AID	ELF-AIDの中にあるプログラムの開始点を指すAID
	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。
	特定署名用電子証明書記録情報	デジタル社会の形成を図るための関係法律の整備に関する法律（令和３年法律第37号）による改正後の電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成14年法律第153号）第18条第３項に規定する特定署名用電子証明書記録情報をいう。
	個人番号カード	行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）第２条第７項に規定する個人番号カードをいう。
	署名用電子証明書	電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成14年法律

		第153号）第３条第１項に規定する署名用電子証明書をいう。
	特定免許情報	道路交通法の一部を改正する法律（令和４年法律第32号）による改正後の法第95条の２第２項に規定する特定免許情報をいう。
	免許情報記録	道路交通法の一部を改正する法律（令和４年法律第32号）による改正後の法第95条の２第２項第１号に規定する免許情報記録をいう。
	運転経歴情報	道路交通法の一部を改正する法律（令和４年法律第32号）による改正後の法第105条の２第３項に規定する運転経歴情報をいう。
	免許情報記録個人番号カード	道路交通法の一部を改正する法律（令和４年法律第32号）による改正後の法第95条の２第４項に規定する免許情報記録個人番号カードをいう。
	運転経歴情報記録個人番号カード	道路交通法の一部を改正する法律（令和４年法律第32号）による改正後の法第105条の２第３項に規定する運転経歴情報が記録された個人番号カードをいう。

別紙２

運転免許証の仕様（外形寸法、電気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。

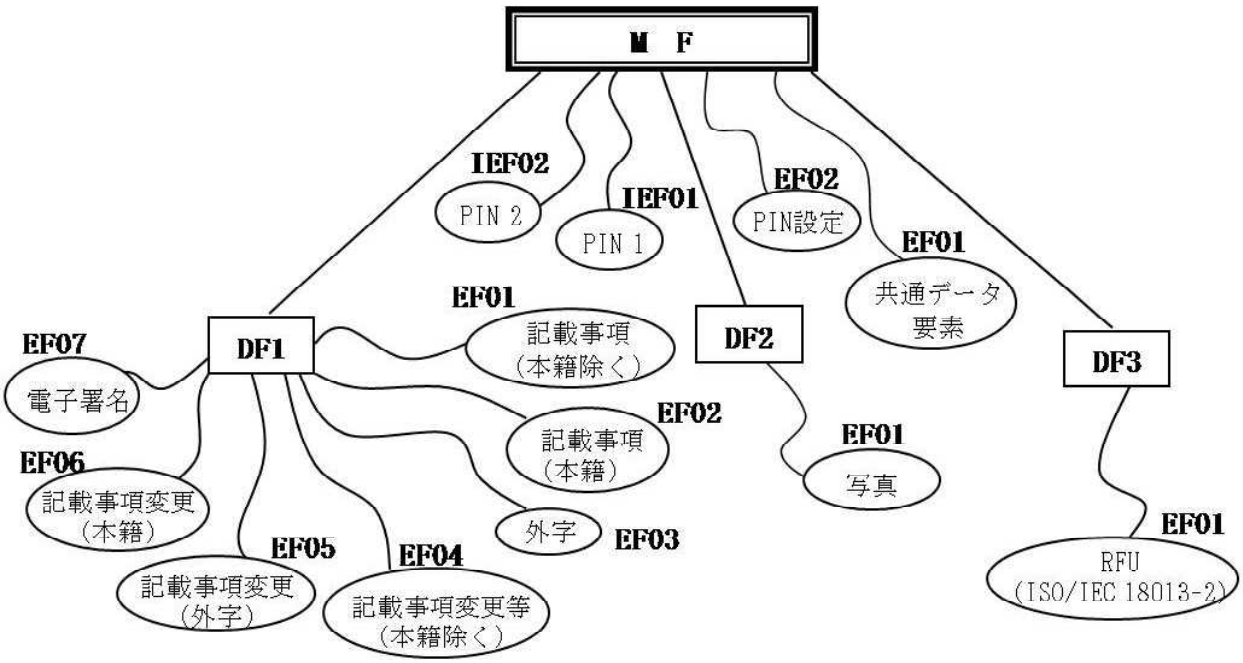
２　電気的仕様
(1)　電力伝送及び信号インタフェース
JIS X 6322-2 Ｂ型(ISO/IEC 14443-2 Type B)に準拠すること。

(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”

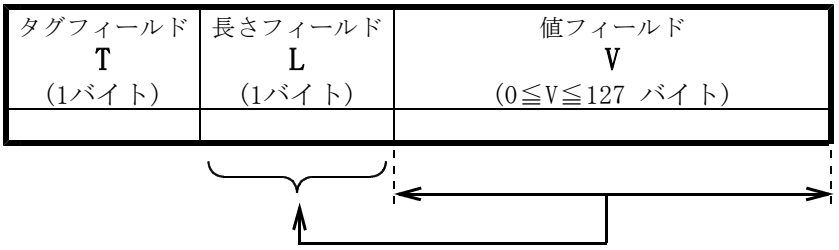
DF2:“02”

DF3:“03”　以降すべて“00”とすること。

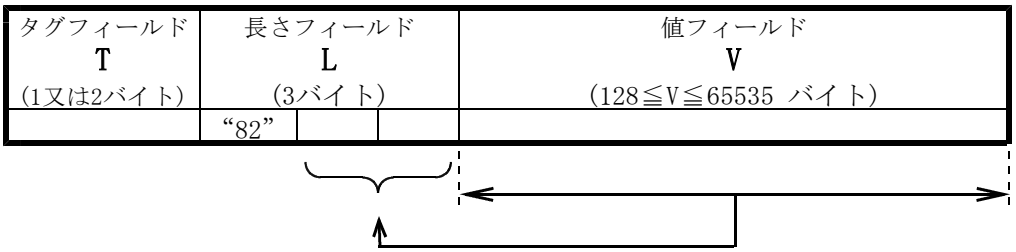
ウ　基本符号化規則

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４参照)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。	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　試行許容回数を超過した場合、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４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	
DF1	EF01	【PIN 1】 (DPIN)		
	EF02	【PIN 1 AND PIN 2】 (DPIN AND DPIN)		
	EF03	【PIN 1】 (DPIN)		
	EF04	【PIN 1】 (DPIN)		(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)
	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)000000 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)

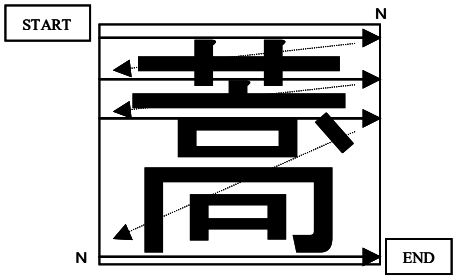
注1　128バイトを超過する場合がある。

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)YYMMDD」+「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)YYMMDD」+「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)YYMMDD」+「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)YYMMDD」+「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)YYMMDD」+「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)YYMMDD」+「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)YYMMDD」+「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)YYMMDD」+「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)YYMMDD」+「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

日 / 本 / ● / 外字1 / 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。

チ　旧姓を使用した氏名の取り扱い

「氏名」及び「新氏名」に旧姓を使用した氏名（以下「旧氏名」という。）を記録する場合の取扱いは、次のとおりとする。

(ｱ)　スペース記号（文字符号“2121”）は、従前のとおり、現在の氏と名の間にのみ挿入する。

(ｲ)　旧氏名は、角括弧［（文字符号“214E”）及び］（文字符号“214F”）で囲い、現氏名の後ろに続けて記録する。

(ｳ)　現氏名「日本花子」、旧氏名「東京花子」の例（●はスペース記号）

日本●花子［東京花子］

(ｴ)　(ｱ)及び(ｲ)の対応が技術的に困難である場合は、必要なシステム改修が完了するまでの間、「備考」に旧氏名を記録することとしても差し支えない。

(ｵ)　統一氏名及び呼び名は、従前のとおり現氏名に基づき記録すること。

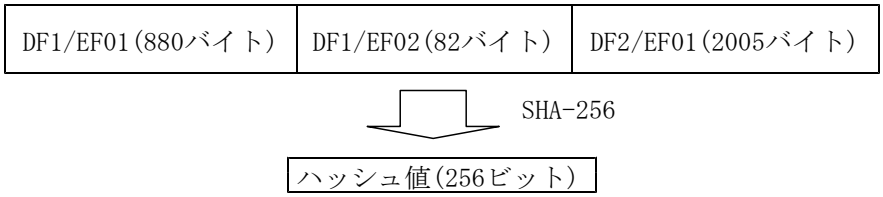
4　電子署名

(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。

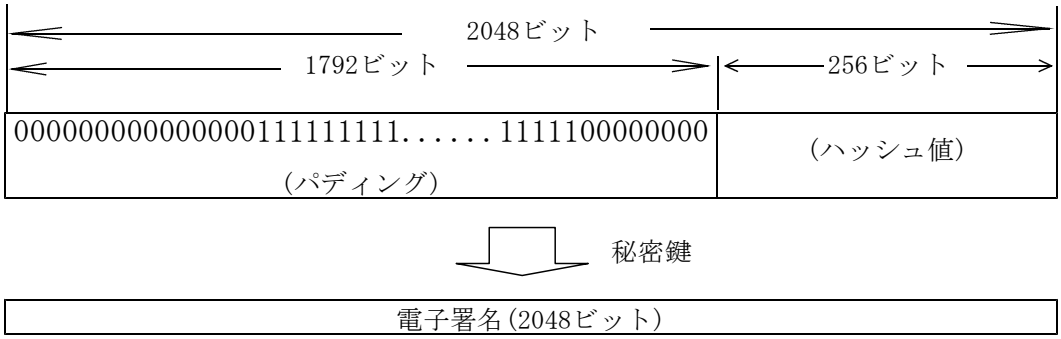
DF1/EF01, DF1/EF02 及び DF2/EF01の順序等を下図に示す。



(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)

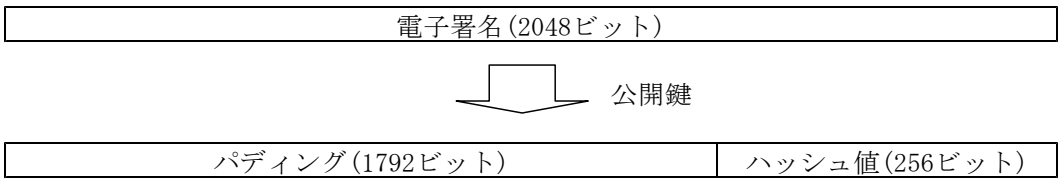


パディング：上位16ビット =b“0000 0000 0000 0001”
下位８ビット =b“0000 0000”
残りのビットはすべてb“1”

(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。

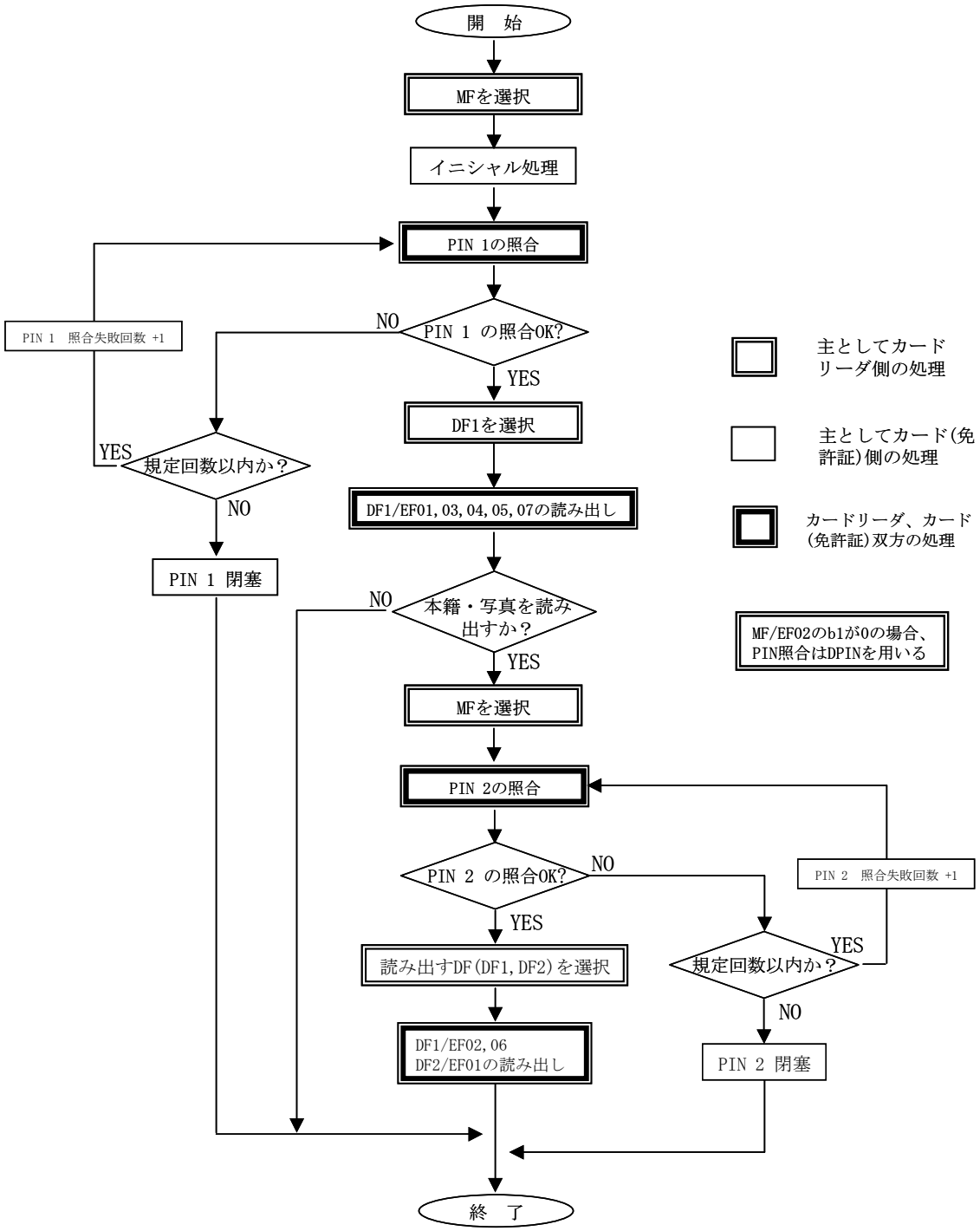
5　記録データの読み出し

(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)



別添　２－１

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、ファイルポインタを持つ。ファイルポインタは、免許証の電気的活性化直後にMFを指す。

(5)　論理チャネル
論理チャネルはチャネル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(チェイン)が発生する場合は下記の印で表現している。
●: レスポンスにチェインあり。

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。セキュリテイ要件は、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			
			正常終了	プロセス完了
“90”	“00”	正常終了		
“62”		不揮発性メモリの状態は，変化していない	警告処理	
	“83”	DFが閉塞している		
“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		
“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		
“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		
	“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									
								0	0	0	0	0	0	0	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

(チェインあり)

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の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”		不揮発性メモリの状態は，変化していない	警告処理	
	“83”	DFが閉塞している		
“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		
“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		
	“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”		間違ったパラメタ		
	“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		
“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		

別紙３

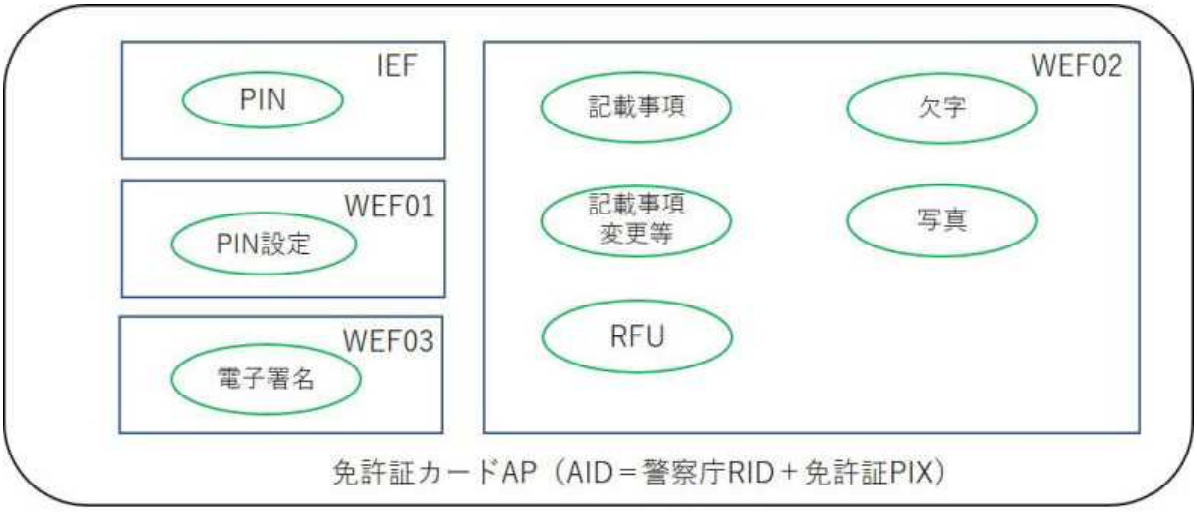
免許情報記録個人番号カードの仕様（外形寸法、電気的仕様及び論理ファイル等）

１　外形寸法
別紙２の１に同じ

２　電気的仕様
(1)　電力伝送及び信号インタフェース
別紙２(1)に同じ

(2)　伝送プロトコル
別紙２(3)に同じ

３　論理ファイル
(1)　論理ファイル構成図
個人番号カードの空き領域の拡張利用領域に警察独自のカードAPを搭載し、特定免許情報等を記録する。



(2)　ファイル構成・内容、基本符号化規則 等

ア　ファイル構成

IEF/WEF	EF-ID (HEX)	EF種別	データ内容	最大データ長(バイト)	備　考
IEF01	“0006”	IEF	暗証番号(PIN)	4	
WEF01	“001A”	WEF透過	暗証番号（PIN)）設定	3	
WEF02	“001B”	WEF透過	免許情報記録	5845	
WEF03	“001C”	WEF透過	電子署名	584	

イ　アプリケーション識別子(AID)(注1)

	A I D	
	R I D	P I X
ELF-AID	“A0 00 00 02 31”	“04 00 00 00 00 00 00 00 00 00 00”(注2)
実行モジュール-AID	“A0 00 00 02 31”	“05 00 00 00 00 00 00 00 00 00 00”(注2)
インスタンス-AID	“A0 00 00 02 31”	“06 00 00 00 00 00 00 00 00 00 00”(注2)

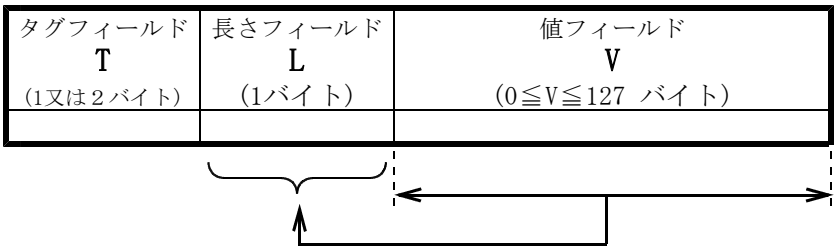
注1　AIDはJIS X 6308(ISO/IEC 7816-5)の規定による。

注2　PIXの先頭1バイトは、ELF-AID:“04”
実行モジュール-AID:“05”
インスタンス-AID:“06”　以降すべて“00”とすること。

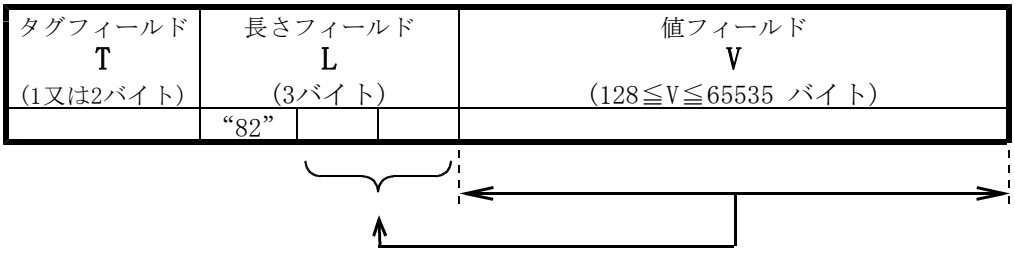
ウ　基本符号化規則

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

１又は２バイトで構成され、“C1”～“10D”の番号をタグとして付与する。

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　暗証番号(PIN)設定
格納ファイル名: WEF01(EFID=“001A”)

<table>
<tr><th>タグ</th><th>データ長
(バイト)</th><th>固/可</th><th>データ内容</th><th>符　号</th></tr>
<tr><td>“C1”</td><td>1</td><td>固</td><td>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><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><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></table></td><td>HEX</td></tr>
</table>

オ　暗証番号、アクセス権限
(ｱ)　暗証番号(PIN)
格納ファイル名: IEF01(EFID=“0006”)
a　PINは4桁の数字(JIS X 0201)とする。
b　試行許容回数を超過した場合、PINを閉塞処理すること。試行許容回数は10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。
d　PIN変更機能については免許証の運用に準ずる。
e　PIN設定の値フィールド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)　アクセス権限

<table>
<tr><th>WEF</th><th>EF-ID
(HEX)</th><th>読出</th><th>書換え</th><th>備　考</th></tr>
<tr><td>WEF01</td><td>“001A”</td><td>【FREE】
(FREE)</td><td rowspan="3">禁止</td><td rowspan="3"></td></tr>
<tr><td>WEF02</td><td>“001B”</td><td>【PIN】
(DPIN)</td></tr>
<tr><td>WEF03</td><td>“001C”</td><td>【PIN】
(DPIN)</td></tr>
</table>

【WEF01の値フィールドVのb1が１である場合】
(WEF01の値フィールドVのb1が０である場合)

カ　書き込み内容

(ｱ)　格納ファイル名：WEF02(EFID=“001B”)

タグ	最大データ長(バイト)	データ内容	符　号	免許情報記録	運転経歴情報
“C2”	7	運転経歴情報記録年月日（元号YYMMDD）	0201	－	○
“C3”	1	運転者区分（優良・一般・違反）	HEX	－	○
“C4”	6	免許証の色区分（優良・新規・その他）	0208	○	－
“C5”	7	免許情報記録の有効期間の末日	0201	○	－
“C6”	80	免許の条件１	0208	○	－
“C7”	80	免許の条件２	0208	○	－
“C8”	80	免許の条件３	0208	○	－
“C9”	80	免許の条件４	0208	○	－
“CA”	256	欠字１		○	－
“CB”	256	欠字２		○	－
“CC”	80	免許の条件５	0208	○	－
“CD”	80	免許の条件６	0208	○	－
“CE”	80	免許の条件７	0208	○	－
“CF”	80	免許の条件８	0208	○	－
“D0”	80	免許の条件９	0208	○	－
“D1”	80	免許の条件10	0208	○	－
“D2”	80	免許の条件11	0208	○	－
“D3”	80	免許の条件12	0208	○	－
“D4”	256	欠字３		○	－
“D5”	256	欠字４		○	－
“D6”	256	欠字５		○	－
“D7”	80	備考１	0208	○	○
“D8”	80	備考２	0208	○	○
“D9”	80	備考３	0208	○	○
“DA”	80	備考４	0208	○	○
“DB”	80	備考５	0208	○	○
“DC”	80	備考６	0208	○	○
“DD”	80	備考７	0208	○	○
“DE”	80	備考８	0208	○	○
“DF”	80	予備１	0208	○	－
“E0”	80	予備２	0208	○	－
“E1”	80	予備３	0208	○	－
“E2”	80	予備４	0208	○	－
“E3”	80	予備５	0208	○	－
“E4”	80	予備６	0208	○	－
“E5”	80	予備７	0208	○	－
“E6”	80	予備８	0208	○	－
“E7”	12	免許情報記録番号	0201	○	－
“E8”	12	運転経歴情報記録番号	0201	－	○
“E9”	7	免許の年月日(二・小・原)	0201	○	○
“EA”	7	免許の年月日(他)	0201	○	○
“EB”	7	免許の年月日(二種)	0201	○	○
“EC”	1	免許の種類（大型）	HEX	○	○
“ED”	1	免許の種類（普通）	HEX	○	○
“EE”	1	免許の種類（大特）	HEX	○	○
“EF”	1	免許の種類（大自二）	HEX	○	○
“F0”	1	免許の種類（普自二）	HEX	○	○

“F1”	1	免許の種類（小特）	HEX	○	○
“F2”	1	免許の種類（原付）	HEX	○	○
“F3”	1	免許の種類（け引）	HEX	○	○
“F4”	1	免許の種類（大二）	HEX	○	○
“F5”	1	免許の種類（普二）	HEX	○	○
“F6”	1	免許の種類（大特二）	HEX	○	○
“F7”	1	免許の種類（け引二）	HEX	○	○
“F8”	1	免許の種類（中型）	HEX	○	○
“F9”	1	免許の種類（中二）	HEX	○	○
“FA”	1	免許の種類（準中型）	HEX	○	○
“FB”	7	RFU1		○	○
“FC”	7	RFU2		○	○
“FD”	7	RFU3		○	○
“FE”	7	RFU4		○	○
“FF”	7	RFU5		○	○
“100”	7	RFU6		○	○
“101”	7	RFU7		○	○
“102”	7	RFU8		○	○
“103”	7	RFU9		○	○
“104”	7	RFU10		○	○
“105”	7	RFU11		○	○
“106”	7	RFU12		○	○
“107”	2000	モノクロ写真（JPEG2000）		○	○

(ｲ) 格納ファイル名：WEF03(EFID=“001C”)

“108”	256	電子署名	BINARY	○	－
“109”	16	シリアル番号	0201	○	－
“10A”	48	RFU	0201	○	－
“10B”	80	発行者名	0201	○	－
“10C”	130	主体者名	0201	○	－
“10D”	32	主体者鍵識別子	BINARY	○	－

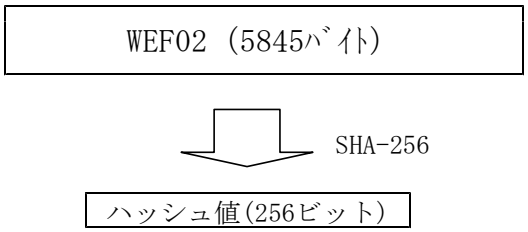
4 電子署名

(1) ハッシュアルゴリズム

SHA-256とする。

WEF02 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。

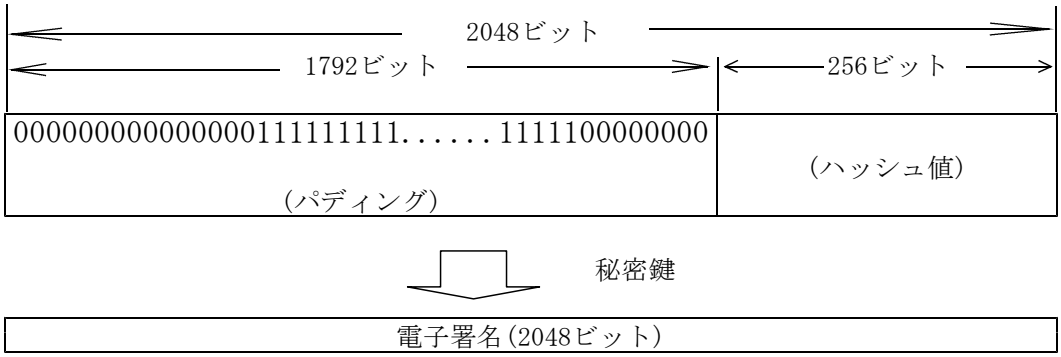
WEF02 の順序等を下図に示す。



(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)

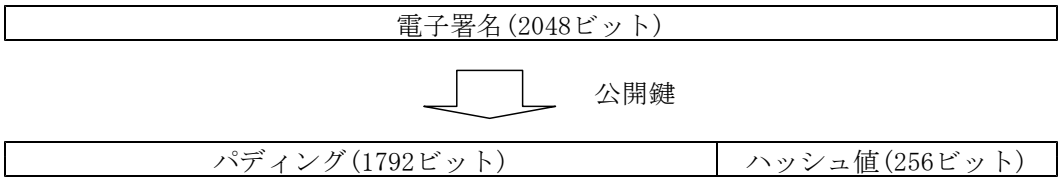


パディング：上位16ビット =b“0000 0000 0000 0001”
下位８ビット =b“0000 0000”
残りのビットはすべてb“1”

(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、免許情報記録個人番号カードとして正規に作成されたものでないか、WEF02 について改ざんがなされた可能性がある。

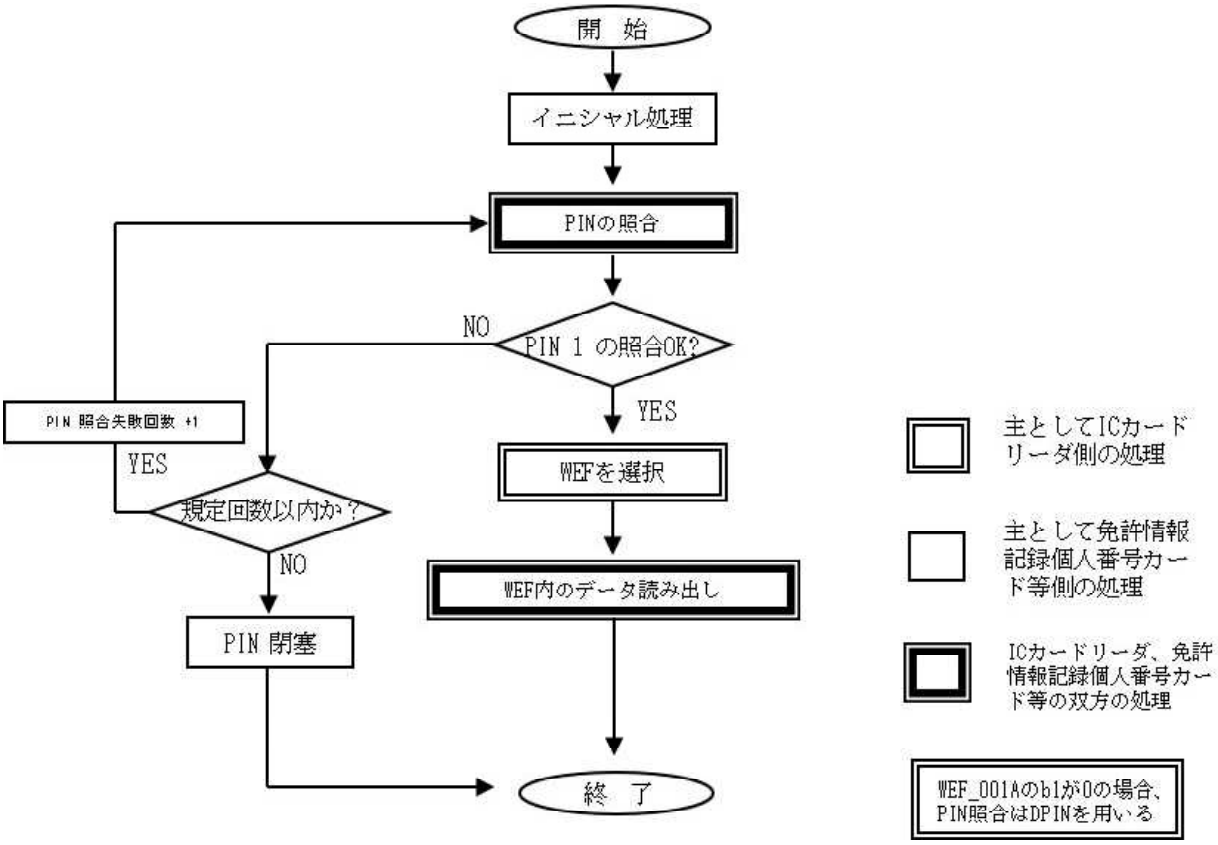
5　記録データの読み出し

(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。基本コマンドを別添３－１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)



基本コマンド

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

1　SELECT FILE コマンド

(1)　機能

指定のEF(AP)をカレント状態に設定する。AP起動直後は、どのEFも選択されていない。

(2)　使用条件

認証状態に関係なく使用可能なコマンドである。

(3)　コマンドメッセージ

CLA:　00h
INS:　A4h
P1:　02h: EF 選択時
　　04h: AP 選択時
P2:　0Ch
Lc:　Data 部の長さ(バイト)
Data: EF 選択時は、ファイル識別子 (EF-ID)
　　AP 選択時は、AID

(4)　レスポンスメッセージ

SW1-SW2:ステータスワード

項番	SW1	SW2	意味
1	90	00	正常終了
2	67	00	Lc,Le フィールドが間違っている。
3	6A	82	EF-ID が一致しない。
4	6A	86	P1,P2の値が正しくない。

2　VERIFY コマンド

(1)　機能

端末から送られた照合キーをカード内で比較する。
VERIFY が成功した場合のみ、照合状態のコマンドを実行することができる。
ボディが空のときは、再試行可能回数を取得できる。

(2)　使用条件

初期状態、外部認証状態、照合状態、外部認証・照合状態で使用可能なコマンドである。
本コマンドは、短縮 EF-ID を指定して実行される。

(3)　VERIFY が成功している状態

VERIFY が成功した場合、以下が発生するまで状態が保持される。
①電源断
②他のAPを選択
③VERIFY 失敗
照合キーの試行回数許容値をクリア（初期値）する。

(4)　VERIFY が失敗している状態

ボディが空のときは、どんな場合でも状態遷移は発生しない。
戻り値 6300h 及び 63CXh (X は 0 以外)で VERIFY が失敗した場合
①初期状態の場合は、そのまま初期状態とする。
②外部認証状態の場合は、そのまま外部認証状態とする。
③照合状態の場合は、初期状態に遷移する。
④外部認証・照合状態の場合は、外部認証状態に遷移する。
戻り値 63C0h で再試行可能回数が 0 回になった場合
①初期状態の場合は、照合キー閉塞状態（初期状態）に遷移する。
②外部認証状態の場合は、照合キー閉塞状態（外部認証状態）に遷移する。
上記以外のエラーでは、状態遷移は発生しない。

(5)　コマンドメッセージ

［照合］
CLA:　00h
INS:　20h
P1:　00h
P2:　82h
Lc:　照合キーの長さ
Data: 照合キー
［再試行可能回数の取得］
CLA:　00h
INS:　20h
P1:　00h
P2:　82h

(6)　レスポンスメッセージ

SW1-SW2:ステータスワード

項番	SW1	SW2	意味
1	90	00	正常終了
2	63	00	照合不一致である。（再試行回数に制限がない場合）
3	63	CX	照合不一致である。（X は再試行可能な回数）
4	67	00	Lc,Le フィールドが間違っている。
5	69	84	（既に）IEF は閉塞している。
6	6A	86	P1,P2の値が正しくない。

3　READ BINARY コマンド

(1)　機能

EF内のバイナリデータを読み出す

(2)　使用条件

外部認証状態、照合キー閉塞状態（外部認証状態）、外部認証・照合状態で使用可能なコマンドである。

本コマンドは、カレント EF に対して実行される。

(3)　コマンドメッセージ

CLA:　00h

INS:　B0h

P1-P2: 書込み対象短縮 EF-ID 及び書き込むべき最初のバイナリデータの相対位置

Le:　読み出しバイト数

P1,P2 のコーディング

P1								P2	意味
b8	b7	b6	b5	b4	b3	b2	b1		
0	-	-	-	-	-	-	-	-	カレント EF 指定
0	x	x	x	x	x	x	x	xx	相対位置指定（15bit）
1	0	0	0	0	0	0	0	-	カレント EF 指定
1	0	0	x	x	x	x	x	-	短縮 EF-ID （全ビットは等しくない）
1	0	0	-	-	-	-	-	xx	相対位置指定（8bit）

(4)　レスポンスメッセージ

Data:指定され読み出されたデータ（可変）

SW1-SW2:　ステータスワード

項番	SW1	SW2	意味
1	90	00	正常終了
2	67	00	Lc,Le フィールドが間違っている。
3	69	82	コマンドを利用する権限がない。
4	69	86	カレント EF がない。
5	69	FC	セッションキーが設定されていない。
6	6A	86	P1,P2の値が正しくない。
7	6B	00	EF 範囲外にオフセットした。

別紙４

運転免許証（追記権限等）及び免許証追記装置の仕様

（概要）

運転免許証の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。

別紙５

個人番号カード、免許情報記録個人番号カード及び運転経歴情報記録個人番号カード（記録権限等）並びに事務処理端末等の仕様

（概要）

免許情報記録個人番号カードの免許情報の記録における記録権限及び事務処理端末等の仕様について定めている。

別紙６

運転免許証の作成及び免許情報記録個人番号カードの記録に係るシステムの仕様

（概要）

運転免許証の作成及び免許情報記録個人番号カードの記録に係るシステムの仕様について定めている。

別紙７

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。

別紙８

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。