在留カード等仕様書
（一般公開用）

Ver １．３

※　本仕様書は、今後の利用促進を図るために予告なしに修正又は訂正する場合があります。その際は、法務省ホームページ上にて仕様書の修正又は正誤表等を公示いたしますので、必ずご確認下さい。

　なお、仕様書の内容の正確性については万全を期していますが、法務省は、この仕様書に含まれる情報の利用に伴って発生した不利益や問題について、誰に対しても何ら責任を負うものではありません。

平成２８年４月

法務省入国管理局出入国管理情報官

目次

1 はじめに

1.1 適用範囲

本仕様書では「在留カード」及び「特別永住者証明書」(以下「在留カード等」という。)のIC モジュールにアクセスするための仕様について規定する。

そのため、この範囲を超える鍵管理方法、発行・運用・管理などの内容については記述しない。

1.2 参照規格(引用規格)

本仕様で参照する文書は、以下の通りである。

[1] 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」

[2] JIS X 6322-4:2001 「外部端子なし IC カード ― 近接型 ― 第 4 部：伝送プロトコル」

[3] JIS X 6320-4:2009 「識別カードーIC カードー第 4 部：交換のための構成，セキュリティ及びコマンド」

[4] JIS X 0201:1997 「７ビット及び８ビットの情報交換用符号化文字集合」

[5] JIS X 0213:2004 「７ビット及び８ビットの２バイト情報交換用符号化拡張漢字集合」

[6] ISO/IEC 7810:2003 “Identification cards -- Physical characteristics”

[7] ISO/IEC 14443-3:2009 “Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 3: Initialization and anticollision”

[8] ISO/IEC 14443-4:2008 “Identification cards -- Contactless integrated circuit cards -- Proximity cards -- Part 4: Transmission protocol”

[9] ISO/IEC 7816-4:2005 “Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange”

[10] ISO/IEC 18013-3:2009 “Information technology – Personal identification – ISO-compliant driving license Pert 3: Access control, authentication and integrity validation”

[11] ISO/IEC 9797-1:1999 “Information technology – Security techniques – Message Authentication Codes(MACs) – Pert 1: Mechanisms using a block cipher”

[12] JICSAP IC カード仕様 V2.0 第 3 部 共通コマンド

[13] PKCS #1 Version 1.5 “RSA Cryptography Standard”

1.3 用語の定義

本仕様書で使用する用語を下表に定義する。

表記	説明
AID	アプリケーション識別子
AP	アプリケーション
APDU	アプリケーション・プロトコル・データ・ユニット
BER	ASN.1 の基本符号化規則
CLA	クラス・バイト
DF	専用ファイル
DO	データオブジェクト
EF	基礎ファイル
EFID	EF 識別子。2バイトで表記される。
IEF	内部基礎ファイル
INS	命令バイト
L	長さ
MAC	メッセージ認証コード
MF	主ファイル
P1-P2	パラメータ・バイト
SW	SW1-SW2　状態バイト（ダッシュは，連結を示す。）
SM	セキュアメッセージング
T	タグ
TLV	タグ・レングス・バリュー
V	バリュー

本仕様書では以下の記号が適用される。

表記	説明
“0”～”9”及び”A”～”F”	16 進数
b0000…0000～b1111…1111	2 進数
(B1)	B1 の値
B1||B2	B1 と B2 の連結
#	番号
b1～b16	ビット番号

2 伝送プロトコル

2.1 初期化及び衝突防止

初期化及び衝突防止はJIS X 6322-3:2001 B型、及びISO/IEC14443-3:2009 Type Bに準ずる。

ATQB の各設定値については以下の通りとする。

PUPI : セッション毎の乱数 4 バイト
AFI : ”00”
ADC : b00
応用データ : ”00000000”

また，ATTRIB コマンド及びレスポンス設定は以下の通りとする。

上位階層の情報 : 無し
上位階層応答 : 無し

2.2 伝送プロトコル

伝送プロトコルはJIS X 6322-4:2001 B型プロトコル、及びISO/IEC14443-4:2008 Type Bプロトコルに準ずる。

3 機能仕様

在留カード等の IC モジュール機能を説明する。

3.1 論理ファイル構造

在留カード等は、図 3-1 に示す論理ファイル構造を持つ。

MF の直下に専用ファイル(DF)、基礎ファイル(EF)が配置され、各 DF の直下には EF が配置される。カードを起動した直後は MF がカレントとなる。各 DF は 16byte で符号化された DF 名(AID)により選択し、カレントとすることができる。

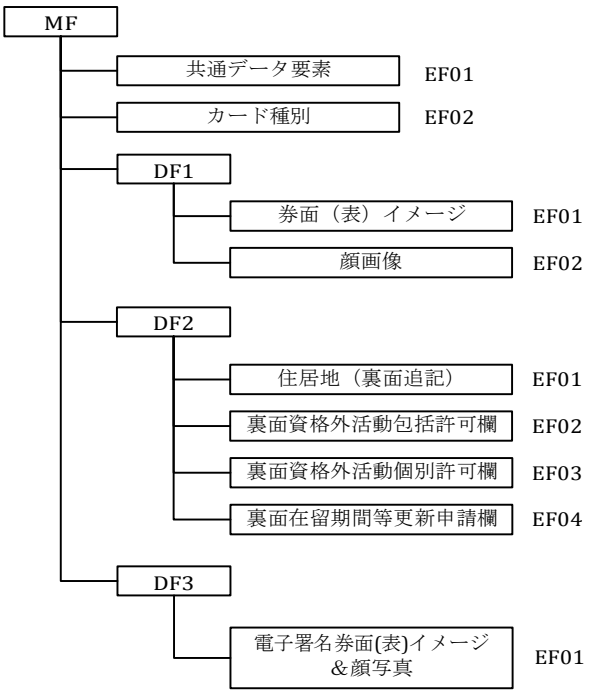


図 3-1　論理ファイル構成概念図

注) 上記ファイル構造以外に IC モジュール内部で利用するデータ(鍵情報)が記録された内部基礎ファイル(IEF)が存在する。本仕様ではそれら IEF に対する操作は行わないため、以降 IEF に関する記述は省略する。

3.2 ファイル仕様

在留カード等で利用するファイルについての定義を以下に示す。

3.2.1 主ファイル(MF)

全てのDF及びEFを配下に持つルートDFを特にMFという。
ICカード起動直後のカレントDFはMFに設定されている。

3.2.2 専用ファイル(DF)

EFを分類、整理するためのファイルをDFという。
DF配下にあるEFを利用する場合、利用対象EFの親DFを選択し、カレントDFとした後にEFを利用する。

3.2.3 基礎ファイル(EF)

端末が使用するデータを格納するファイル。
各EF にはバイナリーデータが記録されている。記録されているバイナリーデータは、3.2.3.1に記載するデータオブジェクトをひとつのデータ単位とし、複数のデータオブジェクトを連結したバイナリ列となっている。
端末では EF に記録されたバイナリーデータを読出し、データオブジェクトのタグ(T)によってデータの意味、レングス(L)によってそのデータのバリュー(V)の長さを確認することができる。

3.2.3.1 データオブジェクト(DO)

EFに格納するバイナリーデータとしてデータオブジェクト(DO)を次のように定義する。
DO はBER-TLV構造をとり、1バイトのタグ(T)、バリューの長さを示す1～3バイトのレングス(L)、バリュー(V)で構成される。1 つの EF に複数の DO が記録されている場合、TLVTLVTLV.....と、複数の DO が連結されたバイナリーデータとして記録される。

T	L	V
3.3.4 参照	“00”～”7F” “81 00”～”81FF” “82 00 00”～”82 FF FF”	値
(1)	(1～3)	(L)

図 3-2 データオブジェクト

データオブジェクト各パラメータの意味は以下のとおり。

- T の値は3.3.4 を参照のこと。
- L の符号化規則は以下のとおりとする。
  - Lが”00”～”7F”の場合：Vの長さ0～127バイトを符号化する。
  - Lが”81 00”～”81 FF”の場合：2バイト目の値でVの長さ0～255バイトを符号化する。
  - Lが”82 00 00”～”82 FF FF”の場合：2バイト目と 3バイト目(ビッグエンディアン)でVの長さ0～65535バイトを符号化する。
- Vの意味については3.3.4 を参照のこと。

3.3 データ内容

3.3.1 ファイル構成

在留カードのファイル構成を表 3-1、特別永住者証明書のファイル構成を表 3-2 に示す。

表 3-1 在留カードファイル構成

ファイル	ファイル内容	ファイル容量(byte)
MF	－	－
EF01	共通データ要素	6
EF02	カード種別	3
DF1	－	－
EF01	券面（表）イメージ	7004
EF02	顔画像	3004
DF2	－	－
EF01	住居地（裏面追記）	342
EF02	裏面資格外活動包括許可欄	122
EF03	裏面資格外活動個別許可欄	122
EF04	裏面在留期間等更新申請欄	3
DF3	－	－
EF01	電子署名　券面（表）イメージ&顔画像	1464

表 3-2 特別永住者証明書ファイル構成

ファイル	ファイル内容	ファイル容量(byte)
MF	－	－
EF01	共通データ要素	6
EF02	カード種別	3
DF1	－	－
EF01	券面（表）イメージ	7004
EF02	顔画像	3004
DF2	－	－
EF01	住居地（裏面追記）	342
DF3	－	－
EF01	電子署名　券面（表）イメージ&顔画像	1464

3.3.2 DF 名（AID）

各 DF の AID は在留カード、特別永住者証明書共に共通で表 3-3 のとおりとする。

表 3-3　AID(在留カード／特別永住者証明書共通)

DF	AID
DF1	“D3 92 F0 00 4F 02 00 00 00 00 00 00 00 00 00”
DF2	“D3 92 F0 00 4F 03 00 00 00 00 00 00 00 00 00”
DF3	“D3 92 F0 00 4F 04 00 00 00 00 00 00 00 00 00”

3.3.3 アクセス権

在留カードの各 EF データを読み出すために必要なアクセス権を表 3-4、特別永住者証明書の各 EF データを読み出すために必要なアクセス権を表 3-5 に示す。

表 3-4　アクセス権(在留カード)

ファイル			アクセス権
MF			－
	EF01		Free
	EF02		Free
	DF1		－
		EF01	在留カード等番号による認証 ＆SM
		EF02	在留カード等番号による認証 ＆SM
	DF2		－
		EF01	在留カード等番号による認証
		EF02	在留カード等番号による認証
		EF03	在留カード等番号による認証
		EF04	在留カード等番号による認証
	DF3		－
		EF01	在留カード等番号による認証

表 3-5 アクセス権(特別永住者証明書)

ファイル			アクセス権
MF			－
	EF01		Free
	EF02		Free
	DF1		－
		EF01	在留カード等番号による認証 & SM
		EF02	在留カード等番号による認証 & SM
	DF2		－
		EF01	在留カード等番号による認証
	DF3		－
		EF01	在留カード等番号による認証

注 1）SM はセキュアメッセージングコマンドによる実行が必要であることを示す。
注 2）Free はアクセスするための認証が必要ないことを示す。

3.3.4 EF 内データ内容

在留カード等番号による認証、及びセキュアメッセージングで読み出しが可能となるファイルのデータ内容は以下のとおり。

全てのデータオブジェクトは固定長とする。

3.3.4.1 共通データ要素 (MF/EF01)

親ファイル：MF (在留カード／特別永住者証明書共通)

タグ	最大データ長 (バイト)	データ		
		内容	符号化	詳細
"C0"	4	仕様バージョン番号	JIS X0201	0001,0002,0003...と世代管理を行う 例)0001 の場合は"30 30 30 31"

3.3.4.2 カード種別 (MF/EF02)

親ファイル：MF (在留カード／特別永住者証明書共通)

タグ	最大データ長 (バイト)	データ		
		内容	符号化	詳細
"C1"	1	カード種別	JIS X0201	1:在留カード 2:特別永住者証明書 例)在留カードの場合は"31"

3.3.4.3 券面（表）イメージ (DF1/EF01)

親ファイル：DF1 (在留カード／特別永住者証明書共通)

タグ	最大データ長 (バイト)	データ		
		内容	符号化	詳細
"D0"	7000	プレ印刷部分及び顔画像部分を除く	Binary	MMR 圧縮(tiff)

※書き込みデータサイズが最大データ長(Length)に満たない場合，データの後ろの領域は Null 値(0x00)でパディングされる

3.3.4.4 顔画像 (DF1/EF02)

親ファイル：DF1 (在留カード／特別永住者証明書共通)

タグ	最大データ長 (バイト)	データ		
		内容	符号化	詳細
"D1"	3000	顔画像	Binary	JPEG2000 カラー画像

※書き込みデータサイズが最大データ長(Length)に満たない場合，データの後ろの領域は Null 値(0x00)でパディングされる

3.3.4.5 住居地（裏面追記） (DF2/EF01)

親ファイル：DF2 (在留カード／特別永住者証明書共通)

タグ	最大データ長（バイト）	データ		
		内容	符号化	詳細
“D2”	8	追記書き込み年月日	JIS X0201	YYYYMMDD 例)2012 年 3 月 10 日の場合 ”3230313230333130”
“D3”	6	市町村コード	JIS X0201	全国地方公共団体コード(6 桁) https://www.j-lis.go.jp/code-address/jititai-code.html 参照 例)東京都千代田区の場合、 地方公共団体コード：131016 →”313331303136”
“D4”	320	住居地	JIS X0213:2004	最大 80 文字※

※書き込みデータサイズが最大データ長に満たない場合，Null 値を挿入

3.3.4.6 裏面資格外活動包括許可欄 (DF2/EF02)

親ファイル：DF2 (在留カード)

タグ	最大データ長（バイト）	データ		
		内容	符号化	詳細
“D5”	120	包括許可欄記載内容	JIS X0213:2004	-

※発行済みの在留カードに対し，資格外活動許可（包括）の有無を“無”として在留カードを書き換えた場合，タグ・最大データ長・データすべてに Null 値(0x00)が格納される。

3.3.4.7 裏面資格外活動個別許可欄 (DF2/EF03)

親ファイル：DF2 (在留カード)

タグ	最大データ長（バイト）	データ		
		内容	符号化	詳細
“D6”	120	個別許可欄記載内容	JIS X0213:2004	-

※発行済みの在留カードに対し，資格外活動許可（個別）の有無を“無”として在留カードを書き換えた場合，タグ・最大データ長・データすべてに Null 値(0x00)が格納される。

3.3.4.8　　裏面在留期間等更新申請欄 (DF2/EF04)

親ファイル：DF2　(在留カード)

タグ	最大データ長（バイト）	データ		
		内容	符号化	詳細
“D7”	1	在留期間更新等許可申請ステータスコード	JIS X0201	0:無し 1:申請中 例)申請中の場合は”31”

3.3.4.9　　チェックコード，公開鍵証明書 (DF3/EF01)

親ファイル：DF3　(在留カード／特別永住者証明書共通)

タグ	最大データ長（バイト）	データ		
		内容	符号化	詳細
“DA”	256	チェックコード	Binary	3.4.3 参照
“DB”	1200	公開鍵証明書	Binary	X.509（ver.3）形式 CER 符号化ファイル(拡張子 cer)

※平成２４年７月９日から同年８月５日までの間に発行された一部の在留カード及び特別永住者証明書について，電子署名（チェックコード及び公開鍵証明書）に固定値が格納された在留カード等が存在している。この固定値に関する情報は，在留カード等仕様書（別紙）を参照すること。また，固定値に関する情報の入手方法については，入国管理局のホームページを参照すること。

3.3.5　16 歳未満の在留カード及び特別永住者証明書のデータ取り扱いについて

16 歳未満の中長期在留者（永住者含む）及び特別永住者に交付されるカードでは以下のデータはカード内に格納されない。*3

- 顔写真(DF1/EF02)*1
- チェックコード，公開鍵証明書(DF3/EF01)*2

*1　DF3/EF01 には「Tag1 バイト(0xDA)・Length1 バイト(0x00)・Tag1 バイト(0xDB)・Length1 バイト(0x00)・以降 Null 値(0x00)埋め」が格納される。

*2　チェックコード，公開鍵証明書なしの場合，DF3/EF01 には「Tag1 バイト(0xDA)・Length1 バイト(0x00)・以降 Null 値(0x00)埋め」が格納される。

*3　ただし，16 歳未満であっても 16 歳の誕生日の半年前に交付されたカードに関してはこの限りではありません。

3.4　セキュリティ機能

在留カード等ではセキュリティ機能として主に以下の 3 つの機能を持つ。

1. 在留カード等番号による認証
   各 EF にアクセスするための認証を行う機能。認証に成功し、アクセス権を得ることで各 EF に記録されているデータを読み出すことができる。
2. セキュアメッセージング
   端末と IC カード間の通信を暗号化し、盗聴を防止する機能。
3. 電子署名
   各 EF に記録されているデータが偽造・改ざんされていないことを検証する機能。読み出したデータの電子署名を検証することで、そのデータが偽造・改ざんされたものである場合は検知することができる。

各セキュリティ機能の詳細を以下に示す。

3.4.1　在留カード等番号による認証

画面より手入力された在留カード等番号と IC チップ内部に記録されている簡易認証コードの照合を行う。

在留カード等番号による認証が成功することにより、民間で読み出し可能な情報への読み出しアクセスが可能となる。そのため、記録されている情報を読み出す場合は図 3-3 のように読出し前に在留カード等番号による認証を行う必要がある。

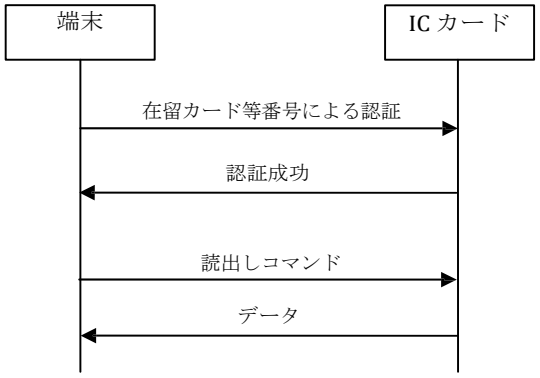


図　3-3　在留カード等番号による認証

3.4.2　セキュアメッセージング

本機能は、端末と IC カードとの間で授受されるコマンドまたはレスポンスを暗号化するための機能である。セキュアメッセージングで暗号化に用いる鍵はセッションの度に生成されるセッション鍵を使用する。

詳細については 4.2「コマンド機能及びコマンドパラメータ」、及び別添1「セキュアメッセージングセッション鍵交換」を参照のこと。

3.4.3 電子署名

在留カード等では「券面(表)イメージ」と「顔画像」に対して計算された電子署名が記録されている。IC カードの情報を読み出した際に電子署名を検証することでその情報が偽造・改ざんされたものでないかを確認することができる。

3.4.3.1 署名検証方法

IC カードから読み出したチェックコードを上位端末で検証する場合、図 3-4 の手順で検証する。検証に利用する公開鍵等の情報についてはチェックコードと共に DF3/EF01 のファイルに記録されている。(3.3.4.9 参照)

下記手順の④で比較したハッシュ値が一致しなかった場合、その IC カードのデータは改ざんされている可能性があるため、上位端末にて適切なエラー処理をすることが必要となる。

なお，平成２４年７月９日から同年８月５日までの間に発行された一部の在留カード及び特別永住者証明書について，電子署名（チェックコード及び公開鍵証明書）に固定値が格納された在留カード等が存在するため，下記の署名検証方法手順を実施した結果，署名検証が成功しない場合が存在する。この固定値に関する情報は，在留カード等仕様書（別紙）を参照すること。また，固定値に関する情報の入手方法については，入国管理局のホームページを参照すること。

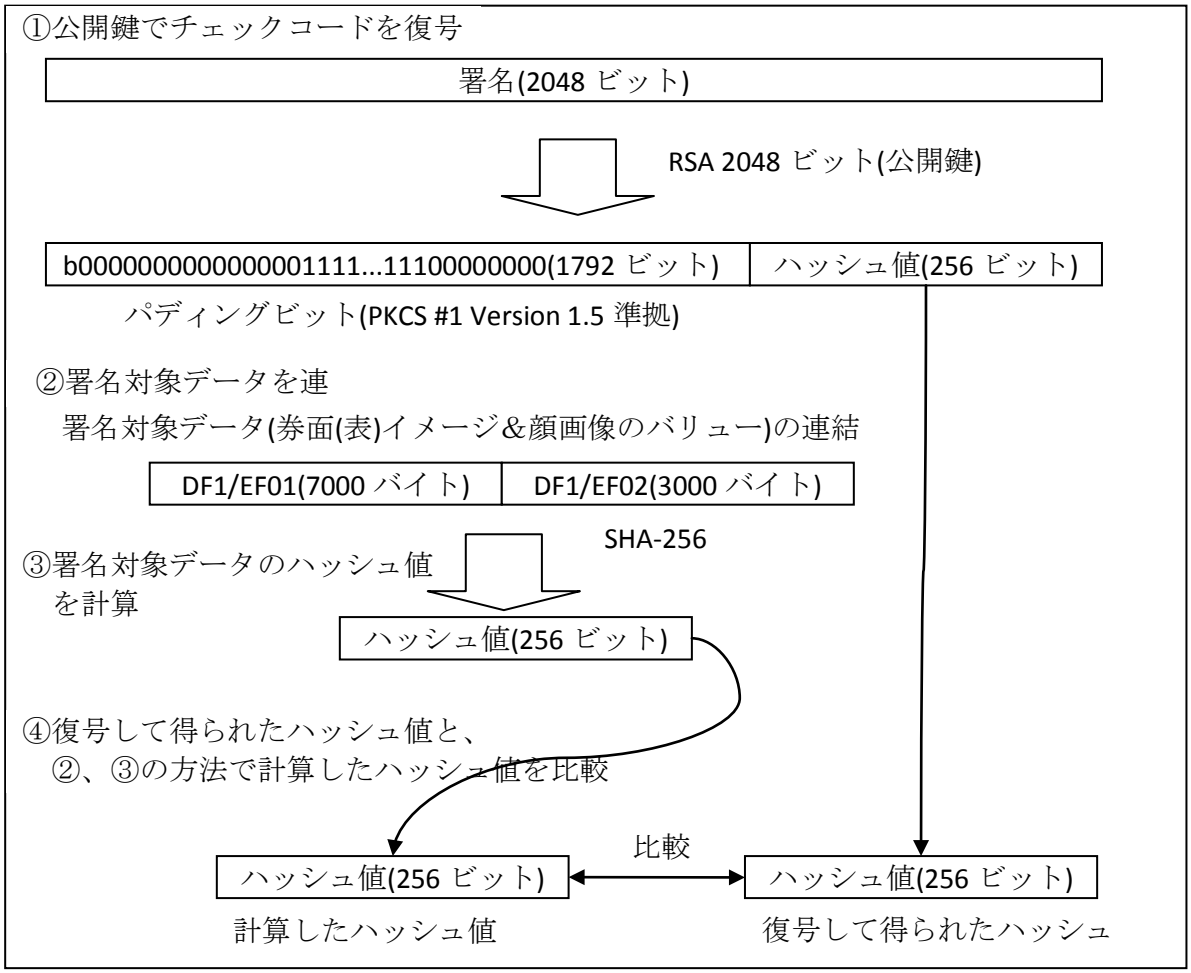


図 3-4　署名検証方法

3.5　データの読み出し手順

在留カード等のデータを読み出す場合のアクセス手順を説明する。

3.5.1　データ読み出しシーケンス

在留カード等のデータは図　3-5 に示すデータ読み出しシーケンスに準じた処理によって読み出すことができる。認証部分については 3.5.2 を参照のこと。

読み出しシーケンスの途中でエラー等により失敗したとき、データ読み出しを再度行う場合はシーケンスの最初から再実行すること。

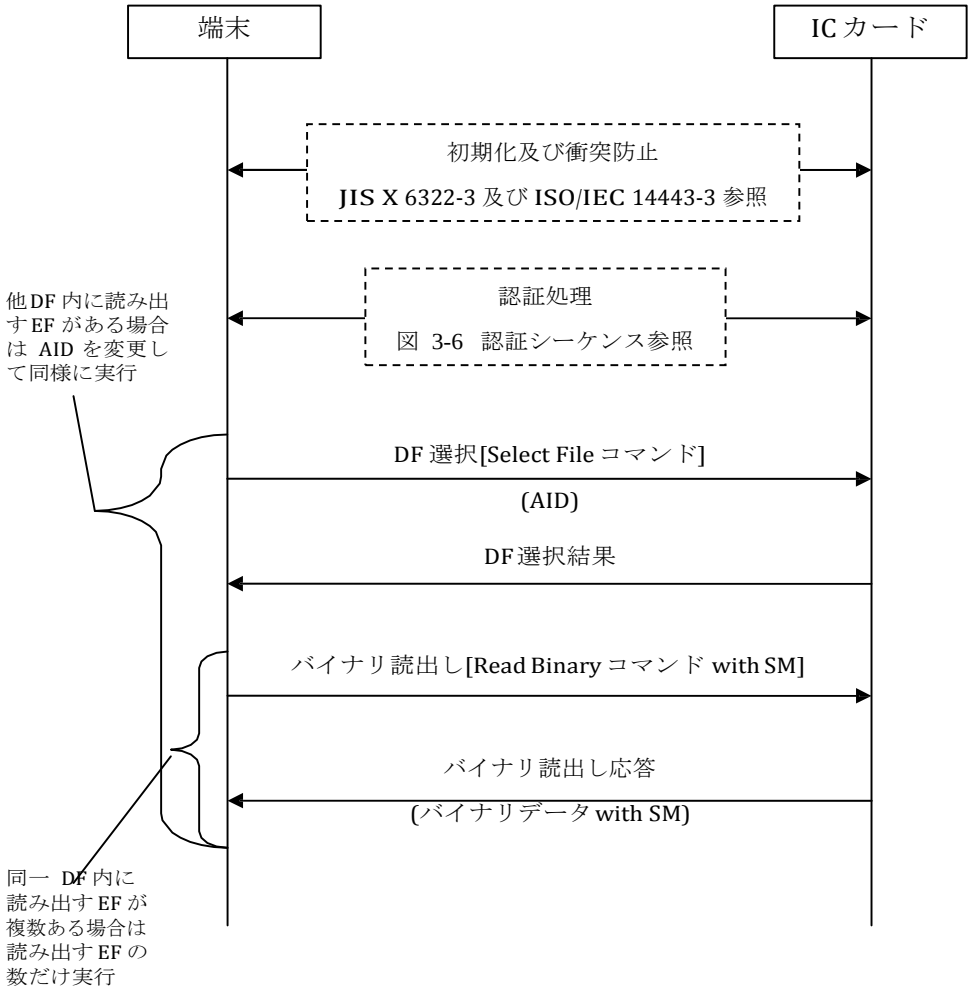


図 3-5　データ読出しシーケンス

3.5.2　認証シーケンス

在留カード等でデータを読み出す際の認証シーケンスを図 3-6 に示す。

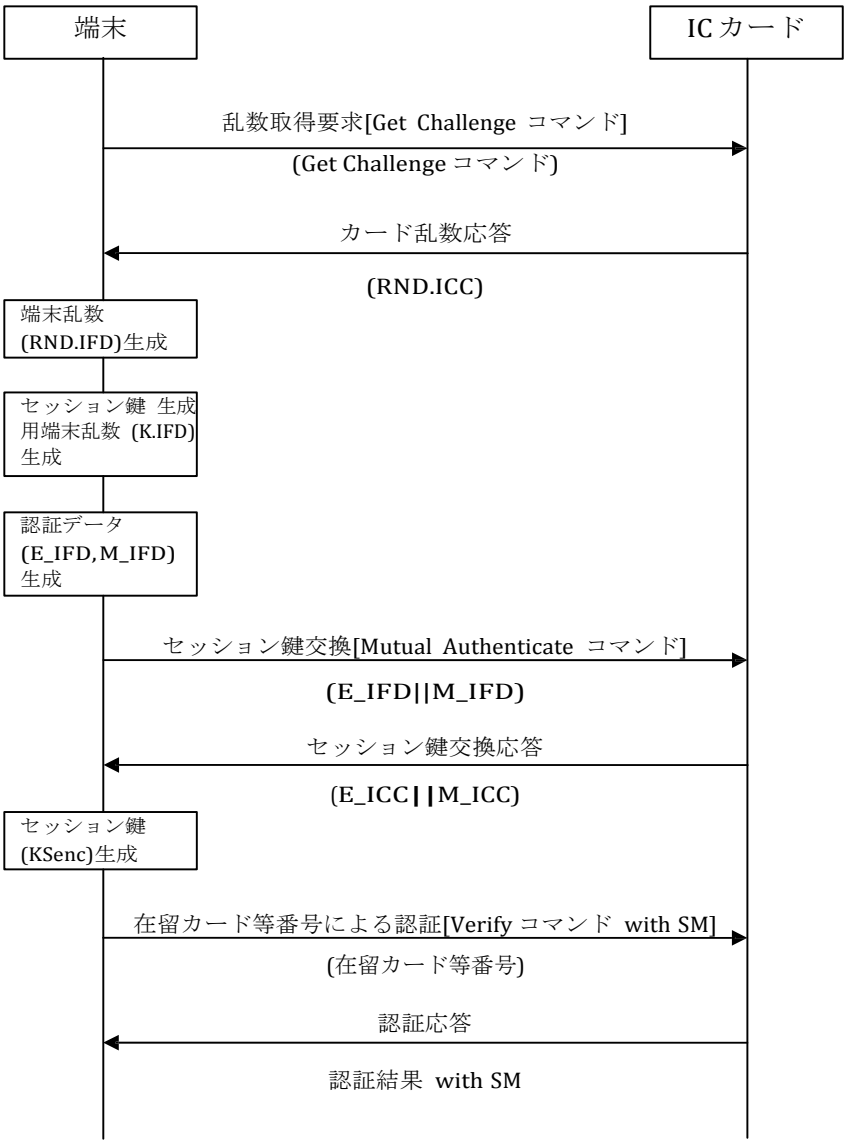


図 3-6　認証シーケンス

4 コマンド仕様

端末と IC カードで送受信するコマンド及びレスポンス仕様について記述する。

4.1 コマンド共通仕様

コマンドはヘッダー部のパラメータ「CLA」、「INS」、「P1」、「P2」、ボディ部のパラメータ「Lc」、「データ」、「Le」から構成され、図 4-1 のようにそれらのパラメータを連結したものをコマンドメッセージ(コマンド APDU)とする。ヘッダー部は各コマンドに対して必須のパラメータである。ボディ部はオプションのパラメータであり、各コマンドに応じて必要なパラメータのみを連結する。各パラメータの意味を表 4-1 に示す。コマンド毎の各パラメータ値は 4.2 以降の各コマンド説明を参照のこと。

ヘッダー部(必須パラメータ)				ボディ部(オプションパラメータ)		
CLA	INS	P1	P2	Lc	データ	Le

図 4-1　コマンドメッセージ(コマンド　APDU)の構成

表 4-1　コマンドメッセージ各パラメータの意味

パラメータ名	長さ	意味
CLA	1	クラスバイト(4.1.1 参照)
INS	1	コマンドバイト(4.1.2 参照)
P1	1	パラメータバイト 1(4.1.3 参照)
P2	1	パラメータバイト 2(4.1.3 参照)
Lc	1 or 3	Lc フィールド(4.1.4 参照)
データ	n	データフィールド(コマンド)(4.1.5 参照)
Le	1 or 2 or 3	Le フィールド(4.1.6 参照)

コマンドに対して IC カードから返送されるレスポンスメッセージ(レスポンス APDU)は「データ」、「SW1」、「SW2」から構成され、図 4-2 のように連結されて返送される。「データ」はコマンドに対して IC カードが返送するデータであり、返送されるべきデータが無い場合はレスポンスメッセージにデータは存在しない。SW1 及び SW2 はコマンドの処理状態を示し、レスポンスメッセージに必ず存在する。各パラメータの意味を表 4-2 に示す。コマンド毎の各パラメータの詳細については 4.2 以降の各コマンド説明を参照のこと。

データ部	状態バイト部	
データ	SW1	SW2

図 4-2　レスポンスメッセージ(レスポンス　APDU)の構成

表 4-2　レスポンスメッセージ各パラメータの意味

パラメータ名	長さ	意味
データ	n	データフィールド(レスポンス)(4.1.7 参照)
SW1	1	状態バイト 1(4.1.8 参照)
SW2	1	状態バイト 2(4.1.8 参照)

4.1.1 クラスバイト

コマンドのクラスバイト(CLA)は、セキュアメッセージング機能の適用の有無を表す。下表に本仕様で規定する CLA の符号化規則を示す。
下記以外の値は本仕様では使用しない。

表 4-3 クラスバイト定義

値	意味
”00”	平文コマンド(SM 非適用)
“08”	SM コマンド(SM適用)

4.1.2 コマンドバイト

コマンドバイト(INS)は、処理されるコマンドを示す。IC カードアプリケーションはコマンドを受信すると、INS で示されたコマンドの機能を実行する。

表　4-4 コマンド名と INS の対応リスト

コマンド名	INS	参照
SELECT FILE	“A4”	4.2.1
VERIFY	“20”	4.2.2
GET CHALLENGE	“84”	4.2.3
MUTUAL AUTHENTICATE	“82”	4.2.4
READ BINARY	“B0”	4.2.5

4.1.3 パラメータバイト

コマンドのパラメータバイト(P1,P2)は、各コマンド固有機能のパラメータを符号化する。
各コマンドの P1、P2 符号化と意味については 4.2 以降の各コマンド説明に記載する。

4.1.4 Lc フィールド

Lc フィールドは後続するデータフィールドの長さを示す。データフィールドが存在しない場合、Lc フィールドも存在しない。

4.1.5 データフィールド(コマンド)

コマンドのデータフィールドは、各コマンド機能に応じたデータを設定する。
各コマンドのデータフィールドの内容については 4.2 節に記載する。

4.1.6 Le フィールド

Le フィールドは IC カードのレスポンスにデータフィールドを要求することを示す。各コマンドのレスポンスにデータフィールドが存在する場合、コマンドの Le フィールドが存在する。レスポンスにデータフィールドが存在しない場合、コマンドの Le フィールドも存在しない。

4.1.7 データフィールド(レスポンス)

レスポンスのデータフィールドは、各コマンド機能に応じたデータが IC カードから返送される。

各コマンドに対応したレスポンスデータフィールドの内容については 4.2 節に記載する。

4.1.8 状態バイト

レスポンスの状態バイト(SW1,SW2)は、コマンドの処理状態を示す。

各状態バイトが示す意味は表 4-5 のとおりとする。

表 4-5　ステータスワード一覧

SW1	SW2	意味
“62”	“83”	(選択された) DF が閉そく（塞）している。
		選択された EF の親 DF が閉そく（塞）している。
“63”	“00”	照合不一致。
“63”	“CX”	照合不一致。［“X”によって，残りの再試行可能回数(1～15)を示す。］
“64”	“00”	ファイル制御情報に異常がある。
“65”	“81”	メモリへの書込みが失敗した。
“67”	“00”	Lc 及び Le フィールドが間違っている(検査誤り)。
		APDU の長さが間違っている。
“68”	“81”	指定された論理チャネル番号によるアクセス機能を提供しない。
“68”	“82”	CLA バイトで指定されたセキュアメッセージング機能を提供しない。
“69”	“81”	ファイル構造と矛盾したコマンド。
“69”	“82”	セキュリティステータスが満足されない。
“69”	“83”	認証方法を受け付けない。
“69”	“84”	参照された IEF が閉そく（塞）している。
“69”	“85”	コマンドの使用条件が満足されない。
“69”	“86”	カレント EF がない。
“69”	“87”	コマンドデータとして，セキュアメッセージングに必要なデータオブジェクトが存在しない。
		セキュリティ環境内に，セキュアメッセージングに必要なデータオブジェクトが存在しない。
“69”	“88”	セキュアメッセージング関連のタグの値が正しくない。
		セキュアメッセージング関連のデータオブジェクトの長さが正しくない。
		セキュアメッセージング関連のデータオブジェクトの値が正しくない。
		セキュアメッセージング関連のデータオブジェクトの順序が規定外。
		コマンドデータとして，セキュアメッセージングについて処理できないデータオブジェクトが存在している。
		その他，セキュアメッセージング関連の TLV 構造を正しく処理できない。
“69”	“99”	アプリケーションは選択されていない。
“6A”	“80”	データフィールドのタグが正しくない。
“6A”	“81”	機能が提供されていない。
“6A”	“82”	アクセス対象ファイルがない。
		短縮 EF 識別子で指定した EF がない。
“6A”	“84”	ファイル内のメモリ残容量が足りない。
“6A”	“85”	Lc の値が TLV 構造に矛盾している。
“6A”	“86”	P1-P2 の値が正しくない。
“6A”	“87”	Lc の値が P1-P2 と矛盾している。
“6A”	“88”	参照された鍵が正しく設定されていない。
“6B”	“00”	EF 範囲外にオフセットした(検査誤り)。
“6D”	“00”	INS が提供されていない(検査誤り)。
“6E”	“00”	CLA が提供されていない(検査誤り)。
“6F”	“00”	自己診断異常(検査誤り)。
“90”	“00”	正常終了

4.2 コマンド機能及びコマンドパラメータ

各コマンドの定義、及び各パラメータ値等について説明する。

4.2.1 SELECT FILE コマンド

(1) 定義及び利用場面

- 本コマンドは、MF またはDF を選択するために使用する。
- 選択する DF はDF 名(AID)によって指定する。

(2) 使用条件及びセキュリティ条件

- 特に無し

(3) コマンドメッセージ

MF 選択

オフセット	パラメータ名	長さ	値	意味
0	CLA	1	“00”	平文コマンド
1	INS	1	“A4”	SELECT FILE コマンド
2	P1	1	“00”	MF 選択
3	P2	1	”00”	MF 選択
4	Lc	1	”02”	データ部の長さ
5	データ	2	“3F 00”	MFID

DF選択

オフセット	パラメータ名	長さ	値	意味
0	CLA	1	“00”	平文コマンド
1	INS	1	“A4”	SELECT FILE コマンド
2	P1	1	“04”	DF選択
3	P2	1	”0C”	レスポンスデータ無し
4	Lc	1	”10”	データ部の長さ
5	データ	16	“D3 92 F0 00 4F XX XX XX XX XX XX XX XX XX XX XX XX”	選択する DF の DF 名 (AID)。3.3.2 参照。

(4) レスポンスメッセージ

オフセット	パラメータ名	長さ	値	意味
0	SW1	1	下表参照	下表参照
1	SW2	1	下表参照	下表参照

(5) ステータスワード

SW1	SW2	意味
“62”	“83”	(選択された) DF が閉そく（塞）している。
		選択された EF の親 DF が閉そく（塞）している。
“64”	“00”	ファイル制御情報に異常がある。
“67”	“00”	Lc 及び Le フィールドが間違っている(検査誤り)。
		APDU の長さが間違っている。
“68”	“82”	CLA バイトで指定されたセキュアメッセージング機能を提供しない。
“69”	“85”	コマンドの使用条件が満足されない。
“69”	“88”	セキュアメッセージング関連のタグの値が正しくない。
		セキュアメッセージング関連のデータオブジェクトの長さが正しくない。
		セキュアメッセージング関連のデータオブジェクトの値が正しくない。
		セキュアメッセージング関連のデータオブジェクトの順序が規定外。
		コマンドデータとして，セキュアメッセージングについて処理できないデータオブジェクトが存在している。
		その他，セキュアメッセージング関連の TLV 構造を正しく処理できない。
“69”	“99”	アクセス対象ファイルの選択が失敗した。
“6A”	“82”	アクセス対象ファイルがない。
“6A”	“86”	P1-P2 の値が正しくない。
“6A”	“87”	Lc の値が P1-P2 と矛盾している。
“6D”	“00”	INS が提供されていない(検査誤り)。
“6E”	“00”	CLA が提供されていない(検査誤り)。
“6F”	“00”	自己診断異常(検査誤り)。
“90”	“00”	正常終了

(6) 特記事項

－ Lc 値よりもコマンドデータ長が大きい場合、Lc の値を正として処理を行う。

4.2.2 VERIFY コマンド

(1) 定義及び利用場面

- 本コマンドは、端末から送られた簡易認証コード(在留カード等番号)を照合し、在留カード等番号による認証を行うために使用する。
- 認証が失敗した場合、SW1-SW2="6300"が返送される。
- 認証状態は現在の状態に関わらず、照合の結果により更新される。

(2) 使用条件及びセキュリティ条件

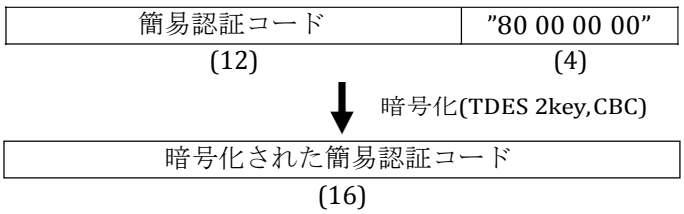
- セキュアメッセージング(SM　コマンド)により本コマンドを実行すること。
- 照合失敗許容回数は無制限とする。(IC　カード内に照合失敗回数を記録しない。)

(3) コマンドメッセージ

オフセット	パラメータ名	長さ	値	意味
0	CLA	1	"08"	SM コマンド
1	INS	1	"20"	VERIFY コマンド
2	P1	1	"00"	特に無し
3	P2	1	"86"	簡易認証
4	Lc	1	"13"	データ部の長さ
5	データ	19	"861101"||暗号化された簡易認証コード	SM 化データオブジェクト

(i)　暗号化された簡易認証コードの生成方法

① 簡易認証コード(12 バイト)にパディング("80 00 00 00")を付加し、16 バイトのバイナリ列とする。
② ①のバイナリ列をセキュアメッセージング用セッション鍵で暗号化する。暗号アルゴリズムはTDES 2key CBC モード、IV="00 00 .... 00"とする。



(4) レスポンスメッセージ

オフセット	パラメータ名	長さ	値	意味
0	SW1	1	下表参照	下表参照
1	SW2	1	下表参照	下表参照

(5) ステータスワード

SW1	SW2	意味
“62”	“83”	DF が閉そく（塞）している。
“63”	“00”	照合不一致。
“64”	“00”	ファイル制御情報に異常がある。
“67”	“00”	Lc 及び Le フィールドが間違っている(検査誤り)。
		APDU の長さが間違っている。
“68”	“81”	指定された論理チャネル番号によるアクセス機能を提供しない。
“68”	“82”	CLA バイトで指定されたセキュアメッセージング機能を提供しない。
“69”	“81”	ファイル構造と矛盾したコマンド。
“69”	“82”	セキュリティステータスが満足されない。
“69”	“84”	参照された IEF が閉そく（塞）している。
“69”	“85”	コマンドの使用条件が満足されない。
“69”	“86”	カレント EF がない。
“69”	“88”	セキュアメッセージング関連のタグの値が正しくない。
		セキュアメッセージング関連のデータオブジェクトの長さが正しくない。
		セキュアメッセージング関連のデータオブジェクトの値が正しくない。
		セキュアメッセージング関連のデータオブジェクトの順序が規定外。
		コマンドデータとして，セキュアメッセージングについて処理できないデータオブジェクトが存在している。
		その他，セキュアメッセージング関連の TLV 構造を正しく処理できない。
“6A”	“82”	短縮 EF 識別子で指定した EF がない。
“6A”	“86”	P1-P2 の値が正しくない。
“6D”	“00”	INS が提供されていない(検査誤り)。
“6E”	“00”	CLA が提供されていない(検査誤り)。
“6F”	“00”	自己診断異常(検査誤り)。
“90”	“00”	正常終了

(6) 特記事項

－ Lc 値よりもコマンドデータ長が大きい場合、Lc の値を正として処理を行う。

4.2.3 GET CHALLENG コマンド

(1) 定義及び利用場面

－ 本コマンドは、後続の MUTUAL AUTHENTICATE コマンドに先立って IC カードからチャレンジを取得するために使用する。

(2) 使用条件及びセキュリティ条件

－ 特に無し

(3) コマンドメッセージ

オフセット	パラメータ名	長さ	値	意味
0	CLA	1	“00”	平文コマンド
1	INS	1	“84”	GET CHALLENGE コマンド
2	P1	1	“00”	特に無し
3	P2	1	”00”	特に無し
4	Le	1	“08”	8 バイトのチャレンジ要求

(4) レスポンスメッセージ

オフセット	パラメータ名	長さ	値	意味
0	データ	8	乱数	カードチャレンジ
8	SW1	1	下表参照	下表参照
9	SW2	1	下表参照	下表参照

(5) ステータスワード

SW1	SW2	意味
“62”	“83”	DF が閉そく（塞）している。
“64”	“00”	ファイル制御情報に異常がある。
“67”	“00”	Lc 及び Le フィールドが間違っている(検査誤り)。
		APDU の長さが間違っている。
“68”	“81”	指定された論理チャネル番号によるアクセス機能を提供しない。
“68”	“82”	CLA バイトで指定されたセキュアメッセージング機能を提供しない。
“69”	“85”	コマンドの使用条件が満足されない。
“69”	“88”	セキュアメッセージング関連のタグの値が正しくない。
		セキュアメッセージング関連のデータオブジェクトの長さが正しくない。
		セキュアメッセージング関連のデータオブジェクトの値が正しくない。
		セキュアメッセージング関連のデータオブジェクトの順序が規定外。
		コマンドデータとして，セキュアメッセージングについて処理できないデータオブジェクトが存在している。
		その他，セキュアメッセージング関連の TLV 構造を正しく処理できない。
“6A”	“86”	P1-P2 の値が正しくない。
“6D”	“00”	INS が提供されていない(検査誤り)。
“6E”	“00”	CLA が提供されていない(検査誤り)。
“6F”	“00”	自己診断異常(検査誤り)。
“90”	“00”	正常終了

(6) 特記事項

－　特に無し

4.2.4 MUTUAL AUTHENTICATE コマンド

(1) 定義及び利用場面

- 本コマンドは、カードと接続装置間でセキュアメッセージング用セッション鍵を共有するために使用される。

(2) 使用条件及びセキュリティ条件

- コマンドを実行するためには、直前にカードからチャレンジを取得していること。
- コマンドが失敗した場合には、再度カードからチャレンジを取得すること。
- カードを非活性化した場合、セッション鍵はクリアされる。

(3) コマンドメッセージ

オフセット	パラメータ名	長さ	値	意味
0	CLA	1	“00”	平文コマンド
1	INS	1	“82”	MUTUAL AUTHENTICATE コマンド
2	P1	1	“00”	特に無し
3	P2	1	”00”	特に無し
4	Lc	1	”28”	データ部の長さ
5	データ	40	E_IFD||M_IFD	別添 1 参照
45	Le	1	“00”	

(4) レスポンスメッセージ

オフセット	パラメータ名	長さ	値	意味
0	データ	40	E_ICC||M_ICC	別添 1 参照
40	SW1	1	下表参照	下表参照
41	SW2	1	下表参照	下表参照

(5) ステータスワード

SW1	SW2	意味
“62”	“83”	DF が閉そく（塞）している。
“63”	“00”	照合不一致。
“64”	“00”	ファイル制御情報に異常がある。
“67”	“00”	Lc 及び Le フィールドが間違っている(検査誤り)。
		APDU の長さが間違っている。
“68”	“81”	指定された論理チャネル番号によるアクセス機能を提供しない。
“68”	“82”	CLA バイトで指定されたセキュアメッセージング機能を提供しない。
“69”	“85”	コマンドの使用条件が満足されない。
“69”	“88”	セキュアメッセージング関連のタグの値が正しくない。
		セキュアメッセージング関連のデータオブジェクトの長さが正しくない。
		セキュアメッセージング関連のデータオブジェクトの値が正しくない。
		セキュアメッセージング関連のデータオブジェクトの順序が規定外。
		コマンドデータとして，セキュアメッセージングについて処理できないデータオブジェクトが存在している。
		その他，セキュアメッセージング関連の TLV 構造を正しく処理できない。
“6D”	“00”	INS が提供されていない(検査誤り)。
“6E”	“00”	CLA が提供されていない(検査誤り)。
“6F”	“00”	自己診断異常(検査誤り)。
“90”	“00”	正常終了

(6) 特記事項

－ Lc 値よりもコマンドデータ長が大きい場合、Lc の値を正として処理を行う。

4.2.5 READ BINARY コマンド

(1) 定義及び利用場面

― 本コマンドは、各 EF のバイナリデータを読み出すために使用される。

(2) 使用条件及びセキュリティ条件

― 本コマンド実行前に在留カード等番号による認証が成功していること。
― 3.3.3「アクセス権」に SM 属性が設定されているファイルを読み出す場合、本コマンドはセキュアメッセージング(SM コマンド)により実行すること。SM 属性が設定されていない場合は平文による実行も可能とする。
― 本コマンドをセキュアメッセージングで実行した場合、レスポンスメッセージもセキュアメッセージング(SM レスポンス)となる。
― 本コマンドにより読出しに成功した場合、対象ファイルはカレントファイルとなる。

(3) コマンドメッセージ

平文コマンド

オフセット	パラメータ名	長さ	値	意味
0	CLA	1	“00”	平文コマンド
1	INS	1	“B0”	READ BINARY コマンド
2	P1-P2	2	下表参照	下表参照
4	Le	3	“00 XX XX”	“XX XX”が”00 00”の場合、対象ファイルのデータを全て読出し。 “XX XX”が”00 00”以外の場合は”XX XX”以下のサイズで読み出せるだけ読出し。

SM コマンド

オフセット	パラメータ名	長さ	値	意味
0	CLA	1	“08”	SM コマンド
1	INS	1	“B0”	READ BINARY コマンド
2	P1-P2	2	下表参照	下表参照
4	Lc	3	“00 00 04”	データ部の長さ
7	データ	4	“96 02 XX XX”	SM 化 Le オブジェクト。 “XX XX” の意味については平文コマンドの Le パラメータの意味を参照。
11	Le	2	“00 00”	レスポンスデータ要求

P1-P2 の意味

P1								P2	意味
b8	b7	b6	b5	b4	b3	b2	b1		
0	x	x	x	x	x	x	x	“XX”	カレントファイルを読出し。 x 及び”XX”の 15 ビットで読出しオフセットを指定。
1	0	0	x	x	x	x	x	XX	ファイルを指定して読出し。 x で読み出すファイルを指定。(指定するファイルについては下記P1 コーディングを参照) “XX”の 8 ビットで読出しオフセットを指定。

(i) MF が選択されている場合のP1 コーディング

値	意味	備考
“8B”	共通データ要素	MF/EF01
“8A”	カード種別	MF/EF02

(ii) DF1 が選択されている場合の P1 コーディング

値	意味	備考
“85”	券面（表）イメージ	DF1/EF01
“86”	顔画像	DF1/EF02

(iii) DF2 が選択されている場合の P1 コーディング

値	意味	備考
“81”	住居地（裏面追記）	DF2/EF01
“82”	裏面資格外活動包括許可欄	DF2/EF02(在留カードのみ)
“83”	裏面資格外活動個別許可欄	DF2/EF03(在留カードのみ)
“84”	裏面在留期間等更新申請欄	DF2/EF04(在留カードのみ)

(iv) DF3 が選択されている場合の P1 コーディング

値	意味	備考
“82”	チェックコード、公開鍵証明書	DF3/EF01

(4) レスポンスメッセージ

平文レスポンス

オフセット	パラメータ名	長さ	値	意味
0	データ	n	データ	データの内容については 3.3.4 参照
n	SW1	1	下表参照	下表参照
n+1	SW2	1	下表参照	下表参照

SM レスポンス

オフセット	パラメータ名	長さ	値	意味
0	データ	n	SM 化データオブジェクト	(i)SM化データオブジェクト、及び(ii)暗号化されたデータの復号方法参照 復号したデータの内容については 3.3.4 参照
n	SW1	1	下表参照	下表参照
n+1	SW2	1	下表参照	下表参照

(i)　SM 化データオブジェクト

BER-TLV(3.2.3.1 参照)でコーディングされたバイナリ列となっている。

タグ値は”86”、バリューは暗号化されたデータの先頭に”01”を連結したバイナリ列。

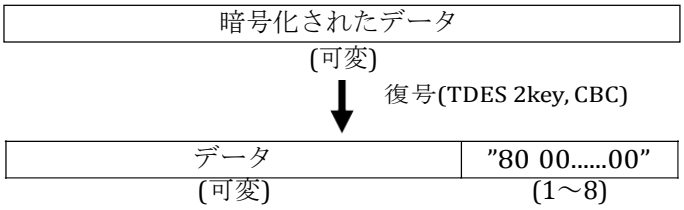
T	L	V
“86”	3.2.3.1 参照	“01”||暗号化されたデータ
(1)	(1～3)	(L)

(ii)　暗号化されたデータの復号方法

SM レスポンスの暗号化されたデータは以下の手順で復号し、データを取り出す。

① 暗号化されたデータをセキュアメッセージング用セッション鍵で復号する。暗号アルゴリズムはTDES 2key CBC モード、IV=”00 00 .... 00”とする。

②　復号されたデータからパディング(”80 00.....00”)を除去し、データを取り出す。



(5) ステータスワード

SW1	SW2	意味
“62”	“83”	DF が閉そく（塞）している。
“64”	“00”	ファイル制御情報に異常がある。
“67”	“00”	Lc 及び Le フィールドが間違っている(検査誤り)。
		APDU の長さが間違っている。
“68”	“81”	指定された論理チャネル番号によるアクセス機能を提供しない。
“68”	“82”	CLA バイトで指定されたセキュアメッセージング機能を提供しない。
“69”	“81”	ファイル構造と矛盾したコマンド。
“69”	“82”	セキュリティステータスが満足されない。
“69”	“85”	コマンドの使用条件が満足されない。
“69”	“86”	カレント EF がない。
“69”	“88”	セキュアメッセージング関連のタグの値が正しくない。
		セキュアメッセージング関連のデータオブジェクトの長さが正しくない。
		セキュアメッセージング関連のデータオブジェクトの値が正しくない。
		セキュアメッセージング関連のデータオブジェクトの順序が規定外。
		コマンドデータとして，セキュアメッセージングについて処理できないデータオブジェクトが存在している。
		その他，セキュアメッセージング関連の TLV 構造を正しく処理できない。
“6A”	“82”	短縮 EF 識別子で指定した EF がない。
“6A”	“86”	P1-P2 の値が正しくない。
“6B”	“00”	EF 範囲外にオフセットした(検査誤り)。
“6D”	“00”	INS が提供されていない(検査誤り)。
“6E”	“00”	CLA が提供されていない(検査誤り)。
“6F”	“00”	自己診断異常(検査誤り)。
“90”	“00”	正常終了

(6) 特記事項

－　特に無し

別添 1 セキュアメッセージングセッション鍵交換

認証シーケンスで使用する各アルゴリズム、メソッドは下記のものを使用する。

表 1　認証シーケンス及びセキュアメッセージングで使用するアルゴリズム

HashAlgorithm *h*	SHA-1
Block Cipher *e*	TDES 2Key
Block Length *n*	64bit
Key Length *k*	128bit
MAC Algorithm *m*	Retail MAC(ISO/IEC 9797-1 Algorithm 3 及び Padding method 2 参照)

認証シーケンス

セキュアメッセージング用セッション鍵交換のための認証シーケンスは下記の手順に従って行う。

Kenc, Kmac は共に在留カード等番号(12 バイト)を SHA-1 でハッシュ化した値の先頭 16 バイトとする。

Step1. 端末乱数生成

認証用端末乱数 RND.IFD(8byte)=乱数
セッション鍵生成用端末乱数 K.IFD(16byte)=乱数
をそれぞれ生成する。

Step2. カード乱数取得

GET CHALLENGE コマンドを実行し、
カード乱数 RND.ICC(8byte)=GET CHALLENGE レスポンスデータを取得する。

コマンド AUDU

CLA	INS	P1	P2	Le
“00”	“84”	“00”	“00”	“08”

レスポンス APDU

データ	SW1	SW2
RND.ICC	“90”	“00”

Step3. 認証データ生成

端末認証暗号化データ E_IFD(32byte)=*e*[Kenc](RND.IFD||RND.ICC||K.IFD)
端末認証 MAC M_IFD(8byte)=*m*[Kmac](E_IFD)
を生成する。

Step4. 相互認証
MUTUALAUTHENTICATEコマンドを実行。

コマンド AUDU

CLA	INS	P1	P2	Lc	データ	Le
“00”	“84”	“00”	“00”	“28”	E_IFD||M_IFD	“00”

カード処理：レスポンスデータ生成

セッション鍵生成用カード乱数 K.ICC(16byte)=乱数
カード認証暗号化データ E_ICC(32byte)=e[Kenc](RND.ICC||RND.IFD||K.ICC)
カード認証 MAC M_ICC(8byte)=m[Kmac](E_ICC)
を生成し、レスポンスデータに設定する。

レスポンス APDU

データ	SW1	SW2
E_ICC||M_ICC	“90”	“00”

Step5. セキュアメッセージングセッション情報生成

暗号化セッション鍵
KSenc(16byte)=h(K.IFD ⊕ K.ICC||”00000001”)(ハッシュ化したデータの先頭 16 バイト)
を生成し、以降のセキュアメッセージングでは上記のセッション鍵を用いる。

別添 2 読出しシーケンス コマンド例

券面(表)イメージ、顔写真、電子署名を読み出す場合のシーケンスコマンド例を示す。

在留カード等番号= ”41 41 31 32 33 34 35 36 37 38 42 42”
h(在留カード等番号) = “65 22 B4 E1 71 19 5B B2 18 22 3A 97 6C 04 01 11 BD C4 AA 25”
Kenc = Kmac = “65 22 B4 E1 71 19 5B B2 18 22 3A 97 6C 04 01 11”

●セキュアメッセージング用セッション鍵交換部

1. RND.ICC の取得
Get Challenge コマンド実行

```
Send -> 00 84 00 00 08
Recv <- 5A 6E 7E 38 51 62 B7 A3 90 00
```

RND.ICC = “5A 6E 7E 38 51 62 B7 A3”

2. RND.IFD(端末乱数 8 バイト), K.IFD(端末乱数 16 バイト)の生成
RND.IFD = “11 22 33 44 55 66 77 88”
K.IFD = “40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F”

3. RND.IFD, RND.ICC, K.IFD を連結
RND.IFD||RND.ICC||K.IFD = “11 22 33 44 55 66 77 88 5A 6E 7E 38 51 62 B7 A3
40 41 42 43 44 45 46 47 48 49 4A 4B 4C 4D 4E 4F”

4. 端末認証暗号化データ計算(上記連結データを Kenc で TDES 暗号化)
E_IFD = “93 77 45 C2 08 83 A1 BA D1 E0 41 93 72 2A 15 92
37 8F 81 A8 F1 DC 58 91 57 AE B0 F7 54 4F A1 BA”

5. 端末認証 MAC 計算(E_IFD に対して Kmac で Retail MAC を計算)
M_IFD = “1A D7 FB 6A 33 89 E0 17”

6. セキュアメッセージング用セッション鍵交換実行

Mutual Authenticate コマンド

```
Send -> 00 82 00 00 28 93 77 45 C2 08 83 A1 BA D1 E0 41
        93 72 2A 15 92 37 8F 81 A8 F1 DC 58 91 57 AE B0
        F7 54 4F A1 BA 1A D7 FB 6A 33 89 E0 17 00
Recv <- 58 60 77 5B 4D 03 2C C5 64 BA 20 4B 8E A8 68 F6
        94 A7 4E 74 75 A8 FE F2 40 58 8B DA 1A F4 96 CE
        59 38 8F D6 CD 45 24 8B 90 00
```

E_ICC = “58 60 77 5B 4D 03 2C C5 64 BA 20 4B 8E A8 68 F6
94 A7 4E 74 75 A8 FE F2 40 58 8B DA 1A F4 96 CE”

M_ICC = “59 38 8F D6 CD 45 24 8B”

7. カード認証 MAC を検証(E_ICC に対して Kmac で Retail MAC を計算、M_ICC と比較)

8. RND.ICC||RND.IFD||K.ICC を取り出し(E_ICC を Kenc で TDES 復号化)

RND.ICC||RND.IFD||K.ICC = “5A 6E 7E 38 51 62 B7 A3 11 22 33 44 55 66 77 88
19 D0 49 49 0F FF 52 EE DB FC B9 30 BC 81 0E D0”

9. RND.ICC と RND.IFD を検証(復号化した値と端末が保持している RND.ICC、RND.IFD を比較)

10. 暗号化セッション鍵を計算

K.IFD ⊕ K.ICC = “59 91 0B 0A 4B BA 14 A9 93 B5 F3 7B F0 CC 40 9F”

K.IFD ⊕ K.ICC||”00000001” = “59 91 0B 0A 4B BA 14 A9 93 B5 F3 7B F0 CC 40 9F
00 00 00 01”

h(K.IFD ⊕ K.ICC||”00000001”) = “CE 94 93 8E 19 E3 B9 7D F9 6E AB CE DC 17 15 CC
84 4F 7C 89”

KSenc = “CE 94 93 8E 19 E3 B9 7D F9 6E AB CE DC 17 15 CC”

●在留カード等番号による認証部

11.　在留カード等番号にパディングを付加
在留カード等番号||パディング = ”41 41 31 32 33 34 35 36 37 38 42 42 80 00 00 00”

12. 在留カード等番号||パディングを KSenc で暗号化(TDES)
e(在留カード等番号||パディング) = “1A A8 29 73 DB 95 9A 81 1F 97 11 D7 28 F0 EE F6”

13. 在留カード等番号による認証を実行
Verify コマンド(SM)

```
Send -> 08 20 00 86 13 86 11 01 1A A8 29 73 DB 95 9A 81
        1F 97 11 D7 28 F0 EE F6
Recv <- 90 00
```

●券面(表)イメージ、顔写真読出し部

14. DF1 を選択
Select File コマンド

```
Send -> 00 A4 04 0C 10 D3 92 F0 00 4F 02 00 00 00 00 00
        00 00 00 00 00
Recv <- 90 00
```

15. 券面(表)イメージの読出し
Read Binary コマンド(SM)

```
Send -> 08 B0 85 00 00 00 04 96 02 00 00 00 00
Recv <- 86 82 1B 61 01 [暗号化された券面(表)イメージデータオブジェクト 7008 バイト
        (パディング含)] 90 00
```

16. 券面(表)イメージデータオブジェクト||パディングを取り出し(暗号化された券面(表)イ メージデータオブジェクト 7008 バイトを KSenc で TDES 復号化)
券面(表)イメージデータオブジェクト||パディング = “D0 82 1B 58　[券面(表)イメージ]
80 00 00 00”

17. 顔写真の読出し

Read Binary コマンド(SM)

```
Send -> 08 B0 86 00 00 00 04 96 02 00 00 00  00
Recv <- 86 82 0B C1 01 [暗号化された顔写真データオブジェクト 3008 バイト
        (パディング含)] 90 00
```

18. 顔写真データオブジェクト||パディングを取り出し(暗号化された顔写真データオブジェクト 3008 バイトを KSenc で TDES 復号化)

顔写真データオブジェクト||パディング = “D1 82 0B B8 [顔写真] 80 00 00 00”

●電子署名読出し部

19. DF3 を選択

Select File コマンド

```
Send -> 00 A4 04 0C 10 D3 92 F0 00 4F 04 00 00 00 00 00
        00 00 00 00 00
Recv <- 90 00
```

20. 電子署名の読出し

Read Binary コマンド

```
Send -> 00 B0 82 00 00 00 00
Recv <- DA 82 01 00 [チェックコード 256 バイト]
        DB 82 04 B0 [公開鍵証明書 1200 バイト] 90 00
```