特定在留カード等仕様書
（一般公開用）

Ver １．０

※　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、出入国在留管理庁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、出入国在留管理庁は、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。

令和６年４月

出入国在留管理庁

目次

1 はじめに

1.1 適用範囲

本仕様書では「特定在留カード」及び「特定特別永住者証明書」（以下「特定在留カード等」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 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」
[2] JIS X 0213:2012 「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」
[3] JIS X 6319-2:2023「IC カード実装仕様－第 2 部：非接触（外部端子なし）近接型 IC カード」
[4] JIS X 6319-2:2023「IC カード実装仕様－第 3 部：共通コマンド
[5] ISO/IEC 7810:2019 “Identification cards -- Physical characteristics”
[6] ISO/IEC 14443-3:2018 “Cards and security devices for personal identification Contactless proximity objects -- Part 3: Initialization and anticollision”
[7] ISO/IEC 14443-4:2018 “Cards and security devices for personal identification Contactless proximity objects -- Part 4: Transmission protocol”
[8] ISO/IEC 7816-4:2020 “Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange”
[9] ISO/IEC 18013-3:2017 “Information technology – Personal identification – ISO-compliant driving license Pert 3: Access control, authentication and integrity validation”
[10] ISO/IEC 9797-1:2011 “Information technology – Security techniques – Message Authentication Codes(MACs) – Pert 1: Mechanisms using a block cipher”
[11] JICSAP IC カード仕様 V2.0 第３部 共通コマンド

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ISO/IEC14443-3:2018 Type Bに準ずる。
以下の項目は個人番号カード仕様に基づく。
ATQB の各設定値については以下の通りとする。

PUPI	：個人番号カード仕様に準ずる。
AFI	：個人番号カード仕様に準ずる。
ADC	：個人番号カード仕様に準ずる。
応用データ	：個人番号カード仕様に準ずる。

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	：個人番号カード仕様に準ずる。
上位階層応答	：個人番号カード仕様に準ずる。

2.2 伝送プロトコル

伝送プロトコルは ISO/IEC14443-4:2018 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

特定在留カード等は、図 3-1 に示す論理ファイル構造を持つ。

本特定在留カード等は個人番号カードの ISD(Issuer Security Domain：カードに唯一存在する)下にある将来利用のための予約領域として確保された SSD(Supplementary Security Domain)に在留 AP が搭載されることを前提とする。

在留 AP 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在留 AP がカレントではないため、在留 AP をカレントとするためには後述する SELECT コマンドを在留 AP の AID を指定して実行する。以降、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。

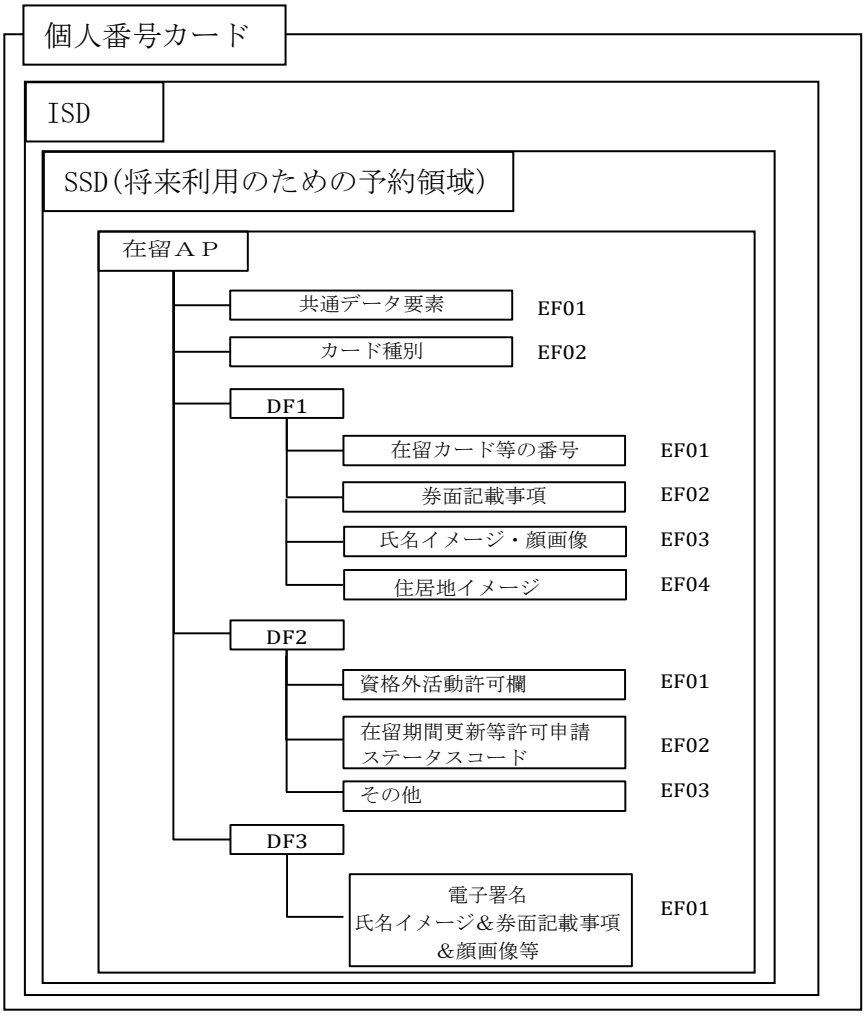


図 3-1　論理ファイル構成概念図

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。

注) 上記ファイル構造以外に、個人番号カードには、行政サービス用の各種アプリケーション（AP）が存在するが、本仕様では特に必要のない情報なので、それに関する記述は省略する。

3.2 ファイル仕様

特定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 在留カード AP

個人番号カードに搭載される在留カードサービスを提供する AP を在留 AP と定義する。
通常、在留カード AP はカレントではない。Select コマンドで在留 AP の AID を指定して実行（選択）すると、在留 AP が起動される。

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”～”81 FF” “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

特定在留カードのファイル構成を表 3-1、特定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 特定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)
在留 AP	－	－
EF01	共通データ要素	6
EF02	カード種別	4
DF1	－	－
EF01	在留カード等の番号	14
EF02	券面記載事項	76
EF03	氏名イメージ・顔画像	5508
EF04	住居地イメージ	2505
DF2	－	－
EF01	資格外活動許可欄	22
EF02	在留期間更新等許可申請 ステータスコード	3
EF03	その他	207
DF3	－	－
EF01	電子署名　氏名イメージ＆券面記載事項＆ 顔画像	704

表 3-2 特定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)
在留 AP	－	－
EF01	共通データ要素	6
EF02	カード種別	4
DF1	－	－
EF01	在留カード等の番号	14
EF02	券面記載事項	73
EF03	氏名イメージ・顔画像	5508
EF04	住居地イメージ	2505
DF2	－	－
EF01	その他	207
DF3	－	－
EF01	電子署名　氏名イメージ＆券面記載事項＆ 顔画像	704

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
在留 AP	“D3 92 F0 00 4F 01 00 00 00 00 00 00 00 00
DF1	“D3 92 F0 00 4F 02 00 00 00 00 00 00 00 00
DF2	“D3 92 F0 00 4F 03 00 00 00 00 00 00 00 00
DF3	“D3 92 F0 00 4F 04 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(特定在留カード)

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

表 3-5 アクセス権(特定特別永住者証明書)

ファイル	アクセス権
在留 AP	－
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
EF03	在留カード等番号による認証 ＆SM
EF04	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。

また、以下 **3.3.4.1～3.3.4.4、3.3.4.7～3.3.4.9** における「符号化」の内容は、扱う文字の範囲を示しており、文字の符号化方式（エンコード方式）は UTF-8（BOM なし）である。

3.3.4.1 共通データ要素 (MF/EF01)

親ファイル：MF (特定在留カード／特定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 (特定在留カード／特定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”	2	カード種別	JIS X0201	05：第２世代在留カード 06：第２世代特別永住者証明書 07：特定在留カード 08：特定特別永住者証明書 例)特定在留カードの場合は”30 37”

3.3.4.3 在留カード等の番号 (DF1/EF01)

親ファイル：DF1 (特定在留カード／特定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
“C2”	12	在留カード等の番号	JIS X0201	英字＋数字：年度/発行組織/年齢区分/その他

3.3.4.4 券面記載事項 (DF1/EF02)

親ファイル：DF1 (特定在留カード／特定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
“C5”	8	有効期限満了日	JIS X0201	YYYYMMDD 例)2024 年 3 月 31 日の場合 ”3230323430333331”
“C6”	8	生年月日	JIS X0201	YYYYMMDD 同上
“C7”	1	性別コード	JIS X0201	1:男　2:女　3:不詳
“C8”	3	国籍	JIS X0201	国籍コード
“C9”	10	在留資格	JIS X0201	在留資格コード(3 桁)+YYMMDDD
“CE”	4	在留期間	JIS X0201	YYMM　もしくは　DDD 永住者の場合**年**月、 特定活動の場合***日と格納
“CA”	2	許可の種類	JIS X0201	在留資格許可コード（2 桁） 特別永住者証明書は項目無し
“CB”	8	許可年月日	JIS X0201	YYYYMMDD 特別永住者証明書は項目無し
“CC”	1	就労制限の有無	JIS X0201	0:無し 1:有り(在留資格に基づく就労活動のみ可) 2:有り(就労不可) 3:有り(指定書により指定された就労活動のみ可) 特別永住者証明書は項目無し
“CD”	8	在留期間の満了日	JIS X0201	YYYYMMDD 特別永住者証明書は項目無し

3.3.4.5 氏名イメージ・顔画像 (DF1/EF02)

親ファイル：DF1 (特定在留カード／特定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”	2500	氏名印字イメージ	Binary	MMR 圧縮(tiff)
“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

3.3.4.6 住居地イメージ (DF1/EF03)

親ファイル：DF1 (特定在留カード／特定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

“DFD1”	2500	住居地印字イメージ	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

3.3.4.7 資格外活動許可欄 (DF2/EF01)

親ファイル：DF2 (特定在留カードのみ)

タグ	最大データ長 (バイト)	データ		
		内容	符号化	詳細
“D5”	7	包括許可欄	JIS X0201	在留資格コード
“D6”	8	包括許可期限	JIS X0201	YYYYMMDD 例)2024 年 3 月 31 日の場合 ”3230323430333331”
“D7”	1	個別許可欄	JIS X0201	0:無し 1:有り 例)無しの場合は”30”

3.3.4.8 資格外活動許可欄 (DF2/EF02)

親ファイル：DF2 (特定在留カードのみ)

タグ	最大データ長 (バイト)	データ		
		内容	符号化	詳細
“D8”	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)無しの場合は”30”

3.3.4.9 その他 (DF2/EF03)

親ファイル：DF2 (特定在留カード／特定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
“D9”	1	出入国在留管理庁長官が記載した旨	JIS X0201	0:無し 1:出入国在留管理庁長官が記録 例)無しの場合は”30”
“DE”	200	予備	JIS X0213:2004	最大 100 文字想定

3.3.4.10　　チェックコード、公開鍵証明書 (DF3/EF01)

親ファイル：DF3　(特定在留カード／特定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
“DC”	104	チェックコード(署名値)	Binary	ASN.1 形式 2 つの署名値を結合した値
“DD”	594	公開鍵証明書	Binary	X.509 (ver.3) 形式 ECDSA(NIST P-384 SHA256)を想定

※想定のファイルサイズとし、署名の詳細は別途規定する。

3.3.5　1 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

1 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

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

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

*3　ただし、1 歳未満であっても 1 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。

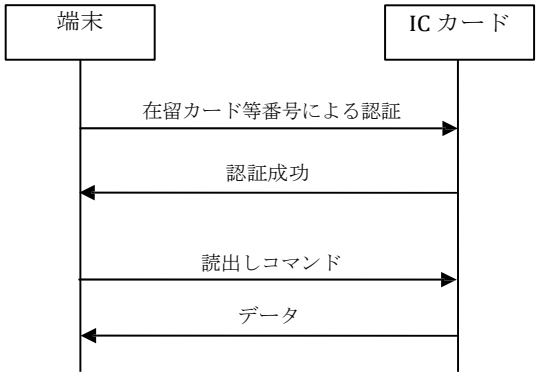


図 3-3　在留カード等番号による認証

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配送」を参照のこと。

3.4.3 電子署名

在留カード等では「氏名イメージ」、「券面記載事項」及び「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

署名検証方法については、IC カードから読み出した公開鍵証明書と署名値 r と署名値 s が結合されたチェックコードを使用して楕円曲線 DSA 署名アルゴリズム（ECDSA）での検証を実施する。ドメインパラメータについては、発行事業者と決定する。

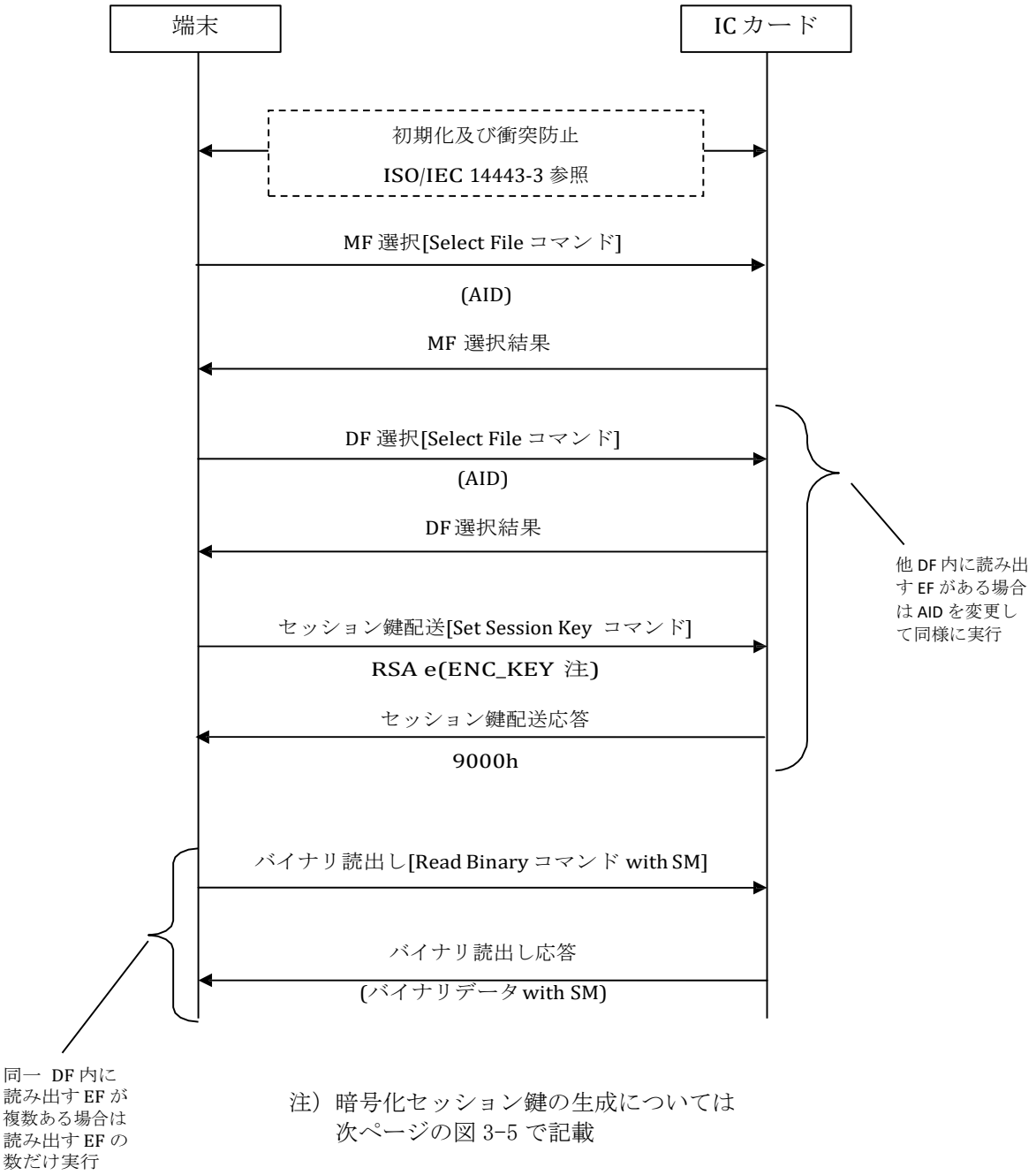
3.5　データの読み出し手順

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 3-4 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。



注）暗号化セッション鍵の生成については
次ページの図 3-5 で記載

図 3-4　データ読出しシーケンス

3.5.2　認証処理シーケンス

特定在留カード等でデータを読み出す際の認証処理シーケンスを図 3-5 に示す。

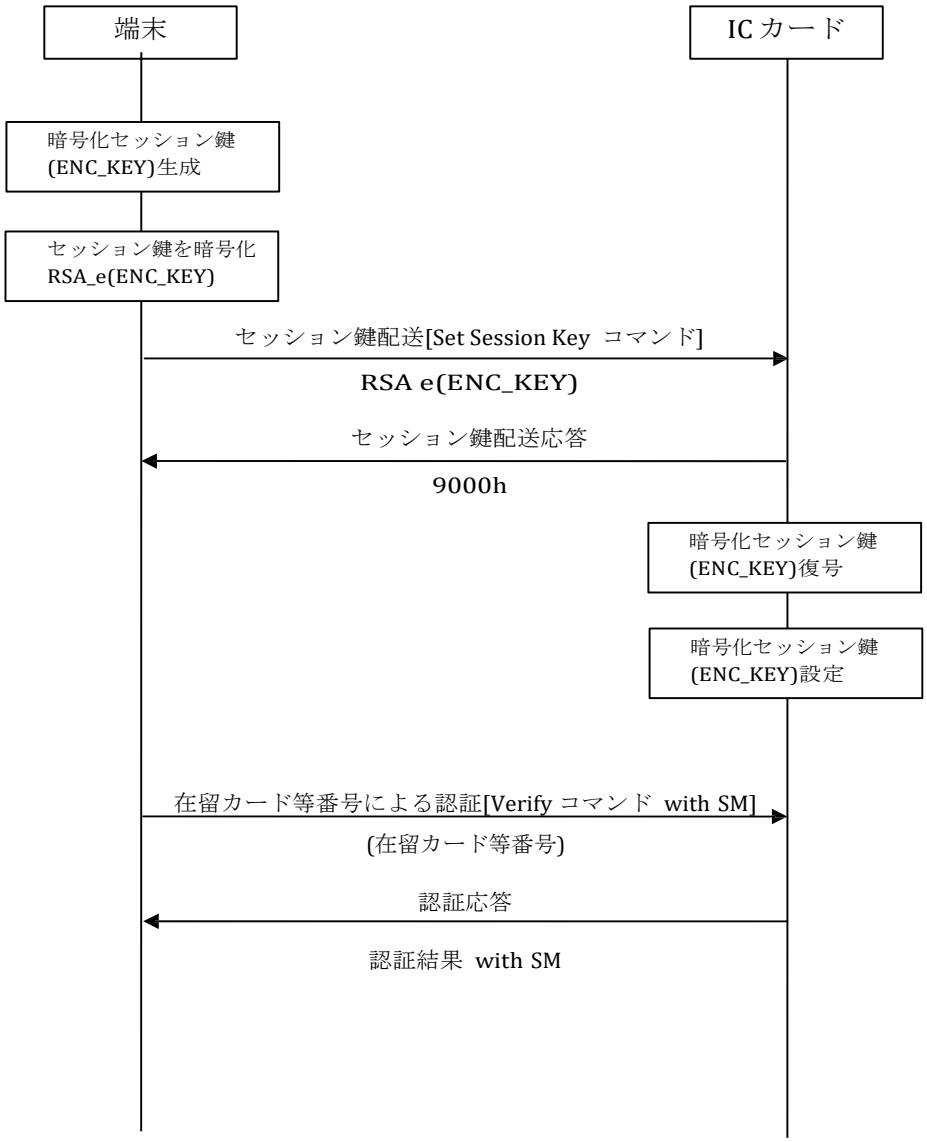


図 3-5　認証処理シーケンス

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
SET SESSION KEY	“AE”	4.2.3
MANAGE SECURITY MNVIRONMENT	“22”	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 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 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、在留 AP または DF あるいは、EF 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。
- 選択する EF は EF-ID (2 バイト)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

在留 AP 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	2	“D3 92 F0 00 4F 01 00 00 00 00 00 00 00 00 00 00 ”	在留 AP の AID

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。

EF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	“02”	EF選択
3	P2	1	”0C”	レスポンスデータ無し
4	Lc	1	”02”	データ部の長さ
5	データ	16	“XX XX”	選択する EF の EF-ID (2 バイト)。

(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、個人番号カードでは”6700”等のエラーになる場合が多いので、留意のこと。

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

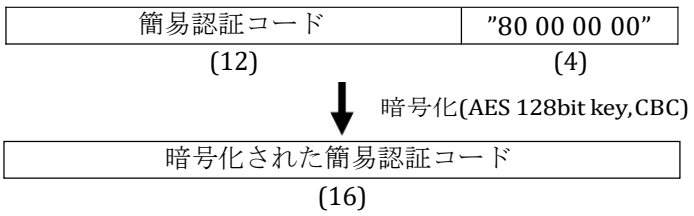
- セキュアメッセージング(SM　コマンド)により本コマンドを実行すること。
- 照合失敗許容回数は無制限とする。(IC　カード内に照合失敗回数を記録しない。)

(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 AES 128bit key 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、個人番号カードでは”6700”等のエラーになる場合が多いので、留意のこと。

4.2.3 SET SESSION KEY コマンド

(1) 定義及び利用場面

－ 本コマンドは、暗号か使用する。

(2) 使用条件及びセキュリティ条件

－ 配送用鍵(復号化用)を格納している EF に対する当該困難度の実行を許可するセキュリティステータスを満たすこと。
－ セッション鍵はカレント SE で指定された暗号アルゴリズムに対応する鍵を使用する。
－ 暗号化されたセッション鍵は、カード内でカレント SE で指定された配送用鍵(復号化用)によって、復号化される。
－ 配送用鍵(復号化用)を格納している IEF には、当該コマンドの実行が許可されているキー属性が設定されていること。
－ 外部装置から配送された鍵を使用するセキュアメッセージングを行う場合、事前に本コマンドを実行する必要がある。
－ 本コマンドで保持されたセッション鍵は、ISD、SSD、カードＡＰを選択した時、あるいはカードを非活性化した時にクリアされる。

(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	“80”	平文独自コマンド
1	INS	1	“AE”	SET SESSION KEY コマンド
2	P1	1	“00”	特に無し
3	P2	1	”00”	特に無し
4	Lc	1 or 3	可変	暗号化した鍵の長さ
5 or 7	データ	可変	可変	暗号化した鍵

(i) データ部：暗号化データ

必要なセッションキーを以下のように BER-TLV フォーマットで表し、配送用鍵(暗号化用)で暗号化する。

・暗号化のみの時：TAG=A0h + LENGTH + VALUE(80h + LENGTH + 暗号化用セッション鍵の元　　データ(32 バイト固定))
・CCS のみの時：TAG=A0h + LENGTH + VALUE(81h + LENGTH + CCS 用セッション鍵の元データ(32 バイト固定))
・暗号化+CCS のみの時：TAG=A0h + LENGTH + VALUE(80h + LENGTH + 暗号化用セッション鍵の元データ(32 バイト固定) + 81h + LENGTH + CCS 用セッション鍵の元データ(32 バイト固定))

SET SESSION KEY コマンドのデータ部について、配送用鍵による暗号化前の「暗号化用セッション鍵の元データ」及び「CCS 用セッション鍵の元データ」の長さは、32 バイト固定とする。セキュアメッセージングで AES128bit を使用する場合は、32 バイトのうち先頭 16 バイトを使用する。

暗号化は RSA を使用し暗号化のフォーマットは PKCS#1v2.2 に定義される RSA-OAEP に従う。

(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。
“64”	“00”	ファイル制御情報に異常がある。
“66”	“F1”	セキュリティ環境自体に異常がある。
	“F2”	セキュリティ環境が指定シアタ IEF 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”	“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”	“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”	“FD”	パディング異常。
“6A”	“80”	データフィールドの中の値が正しくない。
“6A”	“86”	P1-P2 の値が正しくない。
“6A”	“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(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 MANAGE SECURITY ENVIRONMENT コマンド

(1) 定義及び利用場面

- 本コマンドは、暗号アルゴリズム、暗号鍵、補助データ等の SE データオブジェクトをカレント DF に設定・更新するために使用する。
- SE データオブジェクトの設定／変更は、次の手順となる.
  （ｉ）セキュアメッセージや検証等の機能ごとに、SE データオブジェクトを指定する.
  （ⅱ）この処理を必要な機能について繰り返す.
- SE データオブジェクトは、カレントの SE-WEF(EF-ID=2F03h)に保持される。
- SE-WEF は、BER-TLV フォーマット対応の可変長準編成とする。

(2) 使用条件及びセキュリティ条件

- カレントが閉塞状態でないこと。
- カレント DF に対する該当コマンドの実行を許可するセキュリティステータスを満たすこと。

(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”	平文独自コマンド
1	INS	1	“22”	MANAGE SECURITY ENVIRONMENT コマンド
2	P1	1	下表参照	下表参照
3	P2	1	下表参照	下表参照
4	Lc	1 or 3	可変	暗号化した鍵の長さ
5 or 7	データ	可変	可変	暗号化した鍵

P1 の意味

P1								意味
b8	b7	b6	b5	b4	b3	b2	b1	
1	0	0	0	-	-	-	-	検証、暗号、外部認証
0	1	0	0	-	-	-	-	計算、復号、内部認証
0	0	1	1	-	-	-	-	セキュアメッセージングコマンド・レスポンス
-	-	-	-	0	0	0	1	SET
その他の値								RFU

P2 の意味

P2								意味
b8	b7	b6	b5	b4	b3	b2	b1	
A4h								認証系コマンド用
B6h								署名生成または検証系コマンド用
B8h								セキュアメッセージング（暗号化用）
B4h								セキュアメッセージング（ＣＣＳ用）
その他の値								RFU

(ii)　データ部：暗号化データ

タグ	長さ	データ
“83”	2	以下の鍵が格納される IEF-ID 暗号化用秘密鍵：SET SESSION KEY

上記以外の規定もあるが、割愛する。

(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
“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である。
“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。
“69”	“FA”	カードが廃止状態である。
“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

4.2.5 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 05”	データ部の長さ
7	データ	5	“96 03 00 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
“81”	在留カード等の番号	DF1/EF01
“83”	券面記載事項	DF1/EF02
“84”	氏名イメージ・顔画像	DF1/EF03
“86”	住居地イメージ	DF1/EF04

(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”	資格外活動許可欄	DF2/EF01(在留カードのみ)
“82”	在留期間更新等許可申請 ステータスコード	DF2/EF02(在留カードのみ)
“83”	その他	DF2/EF03

(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。

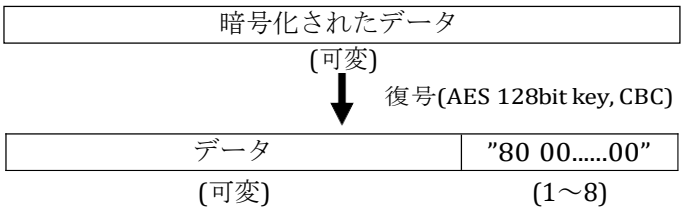
T	L	V
"86"	3.2.3.1 参照	"01"||暗号化されたデータ
(1)	(1～3)	(L)

(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AES 128bit key 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。



(iii)　長いデータの分割読出し

個人番号カードは、SM で暗号化して読み出す際に長さに制限が存在する場合がある。

その制限値の有無、制限値については、地方公共団体情報システム機構へ確認を要する。

また、制限がある場合は、その制限の範囲内で読み出すこととし、氏名イメージ、顔画像、住居地イメージなどはその制限値内で何度かに分けて(Read Binary コマンドを何度か実行)読み出すこととする。

(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配送

セキュアメッセージング等で使用する各アルゴリズム、メソッドは以下とする。

表 1 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*	AES 128bit　CBC モード
Block Length *n*	128bit
Key Length *k*	128bit
MAC Algorithm *m*	CMAC using AES-128 (NIST SP 800-38B(CMAC AES))
鍵配送の暗号	RSA 2048bit
鍵配送の暗号化パディング	RSA-OAEP(PKCS#1V2.2)

セキュアメッセージングの元鍵の生成及び配送方法

セキュアメッセージング用セッション鍵の元鍵の生成は下記の手順に従って行う。

Step1. セッション鍵の元鍵の生成

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。

Step2. 暗号化元データの作成

以下の配送前の暗号化元データを作成する。

Seed = 乱数(16 バイト)

TAG = “A0 44” || “80 20” || Kenc || Seed || “81 20” || Kmac || Seed

Step3. 暗号化データ生成

上記 TAG のデータを RSA-OAEP にパディングして 2048bit にしたのち、RSA の配送鍵で暗号化する。

Step4. 相互認証

SET SESSION KEY コマンドを実行。

コマンド APDU

CLA	INS	P1	P2	Lc	データ
“80”	“AE”	“00”	“00”	“000100”	暗号化済み セッション鍵の元鍵

レスポンス APDU

SW1	SW2
“90”	“00”

別添 2　読出しシーケンス コマンド例

氏名イメージ・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”
※ *h* は SHA-1 とする

●セキュアメッセージング用セッション鍵配送部
1. セキュリティ環境の設定
暗号化されたセッション鍵を復号する鍵の ID をセキュリティ環境に設定されている必要がある。
特定在留カード等では、配布前にセキュリティ環境が設定されていることを前提とする。

2. Seed の生成
乱数生成機能を利用して 、それぞれ 16、32 バイトの Seed を生成する。

Seed1 = 乱数(16 バイト)
Seed2 = 乱数(32 バイト)

3. lHASH、配送する鍵メッセージ、PS(パディング)の編集
lHASH = “E3 B0 C4 42 98 FC 1C 14 9A FB F4 C8 99 6F B9 24
27 AE 41 E4 64 9B 93 4C A4 95 99 1B 78 52 B8 55”
M(メッセージ) = “A0 44” || “80 20” || Kenc || Seed1 || “81 20” || Kmac || Seed1
PS(パディング) = “00 00 ・・・ 00” 120 バイト

4. 暗号化対象データ EM の編集
DB = lHASH || PS || 01 || M (全部で 223 バイト)

MaskedDB = DB ⊕ MGF1(32→223)(Seed2) (全部で 223 バイト)
H0 = sha256(Seed2 || “00 00 00 00”)
H1 = sha256(Seed2 || “00 00 00 01”)
H2 = sha256(Seed2 || “00 00 00 02”)
H3 = sha256(Seed2 || “00 00 00 03”)
H4 = sha256(Seed2 || “00 00 00 04”)
H5 = sha256(Seed2 || “00 00 00 05”)
H6_31 = sha256(Seed2 || “00 00 00 06”)のうち、左 31 バイト)
MGF1(32→223)(Seed2) = H0 || H1 || H2 || H3 || H4 || H5 || H6_31

MaskedSeed = Seed2 ⊕ sha256(MaskedDB || “00 00 00 00”) (全部で 32 バイト)

EM = “00” || MaskedSeed || MaskedDB　(全部で 256 バイト)

5. EM を暗号化
E_EM = RSA(配送鍵, EM)

6.セキュアメッセージング用セッション鍵配送実行

Set Session Key コマンド

```
Send -> 80 AE 00 00 00 01 00 E_EM(256 バイト)
Recv <- 90 00
```

●在留カード等番号による認証部

7.イニシャルベクタの計算

イニシャルベクタの初期値(１回目)
IV = “00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01”
Kenc = “65 22 B4 E1 71 19 5B B2 18 22 3A 97 6C 04 01 11” (暗号化鍵)

E_IV = AES(暗号化, All 00(16byte), Kenc , IV)
E_IV = “BC D5 DA 65 79 AD 60 7F F9 37 A3 2B 92 57 88 D9”

8. 在留カード等番号を暗号化

Kenc = “65 22 B4 E1 71 19 5B B2 18 22 3A 97 6C 04 01 11” (暗号化鍵)
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”
E_IV = “BC D5 DA 65 79 AD 60 7F F9 37 A3 2B 92 57 88 D9”

暗号化在留カード等番号 = AES(暗号化 , E_IV, Kenc, 在留カード等番号||パディング)
暗号化在留カード等番号 = 06 22 C6 B1 A4 03 D2 FF A7 73 E2 26 F3 39 C0 6C

9.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 06 22 C6 B1 A4 03 D2 FF A7 73 E2 26 F3 39 C0 6C
Recv <- 90 00
```

●氏名イメージ・顔画像読出し部

10. DF1およびEF04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
```

Select File コマンド

```
Send -> 00 A4 02 0C 02 00 04
Recv <- 90 00
```

11. 氏名イメージ・顔画像の読出し

Read Binary コマンド(SM)

```
Send -> 08 B0 XX XX 00 00 05 96 03 00 YY YY 00 00
Recv <- 86 82 ZZ ZZ 01 [暗号化された氏名イメージ・顔画像データオブジェクト
                        YYYY(16) - 1バイト(パディング含)] 90 00
注）XX XX:読み出す位置をオフセット指定(先頭bitは0,残り15bitでオフセット指定)
    YY YY:読み出したい長さを指定
    ZZ ZZ:実際に読み出せた長さ(パディング部及びパディングインジケータ“01”を含む)
```

個人番号カードは、カードベンダーによってはセキュアメッセージングで読み出せる長さに制限が存在する。
その場合は、制限の範囲内で複数回に分けて読み出す(オフセットを移動して全体を読み出す)。
読み出したデータは都度復号化する。

●電子署名読出し部

12. 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
```

13.電子署名の読出し

Read Binary コマンド

```
Send -> 00 B0 82 00 00 00 00
Recv <- DC 68［チェックコード 104 バイト］
        DD 82 02 52［公開鍵証明書 594 バイト］90 00
```

※平文での読出しが可能(セキュアメッセージングで読み出す必要なし)