平成18年度経済産業省基準認証研究開発事業

平成18年度経済産業省　産業技術研究開発委託事業
「バイオメトリクス（指紋）の互換性及び相互運用性に関する標準化」

Ⅱ章　　指紋画像とマニューシャ等実装規格の作成

報告書

平成19年3月

財団法人　ニューメディア開発協会

目　次

1. 調査研究の実施状況

1.1. 目的

生体情報（バイオメトリクス）による個人識別技術は，他人へのなりすましや，偽造を防ぐ有効な手段として期待されており，安全な社会の実現には不可欠な技術である。その実用化を推進するために，本事業では ISO/IEC JTC1 SC37 が昨年度規格制定した ISO/IEC 19794-2:2005（マニューシャ），19794-4:2005（指紋画像）など指紋認証等の互換性に関連する規格を調査・分析・研究開発を行うことにより，運用面で互換性が不十分であった要因を分析し，これに関する国際標準案を策定して，国際標準化機構（ISO）と国際電気標準会議（IEC）の合同専門委員会（JTC）1 の分科委員会（SC）37 等へ提案することを目指す。また，互換性で最も重要と推定される指紋画像の品質に関して規格提案を行うため，これまで社会的なアレルギーから取り組まれなかった指紋データベースを構築しセンサの開発や，統一評価のために利用，管理することとする。

そこで本事業では，利用業務で早期に作成を要請　されている実装規格等，以下 3 項目に示す調査研究開発を実施し，その成果を ISO/IEC JTC1 の SC37，SC17 へ提案することを目的とする。

なお，EU 諸国では，2009 年からパスポートに顔画像に加えて指紋画像の採用を義務付ける計画が進んでおり，我が国でも早期の調査・開発を行い，国際規格制定で取り残されないよう各国との調整を図り提案を実現する。

本小委員会では，IC カードへの指紋画像とマニューシャ（特徴点）等実装規格の作成を検討した。次年度以降に関連国際規格の制定内容を加えた国内統一仕様書を作成するとともに，ISO への寄書若しくは追補規格の提案を行っていく。

1.2. 実施内容

本小委員会では，指紋画像とマニューシャ等実装規格の作成に関する検討を行った。ISO/IEC 7816-11:2004, ISO/IEC 19794-2:2005（マニューシャ）, ISO/IEC 19794-4:2005（指紋画像），ISO/IEC 19785-1:2006（CBEFF），2nd FCD 19785-3:2006（TLV フォーマット）規格及び，ICAO の論理データ構造（以下「LDS」という。）に関する規格を精査した。その結果に基づき，国内統一仕様としての実装規格第一次案の作成を行った。次年度以降は関連国際規格の統一仕様書を作成するとともに，ISO への寄書若しくは追補規格の提案に向けて，

補完項目（ファイルフォーマット等）の調査を行う。

また，互換性に必要なセンサ及び PDC の信号・インターフェースの標準化のため，代表的センサ（海外２社，国内３社）の操作ソフトを分析し，共通の要素を抜粋し，信号インターフェース及びユーザインタフェースのガイドライン案としてまとめた。

1.3. スケジュール

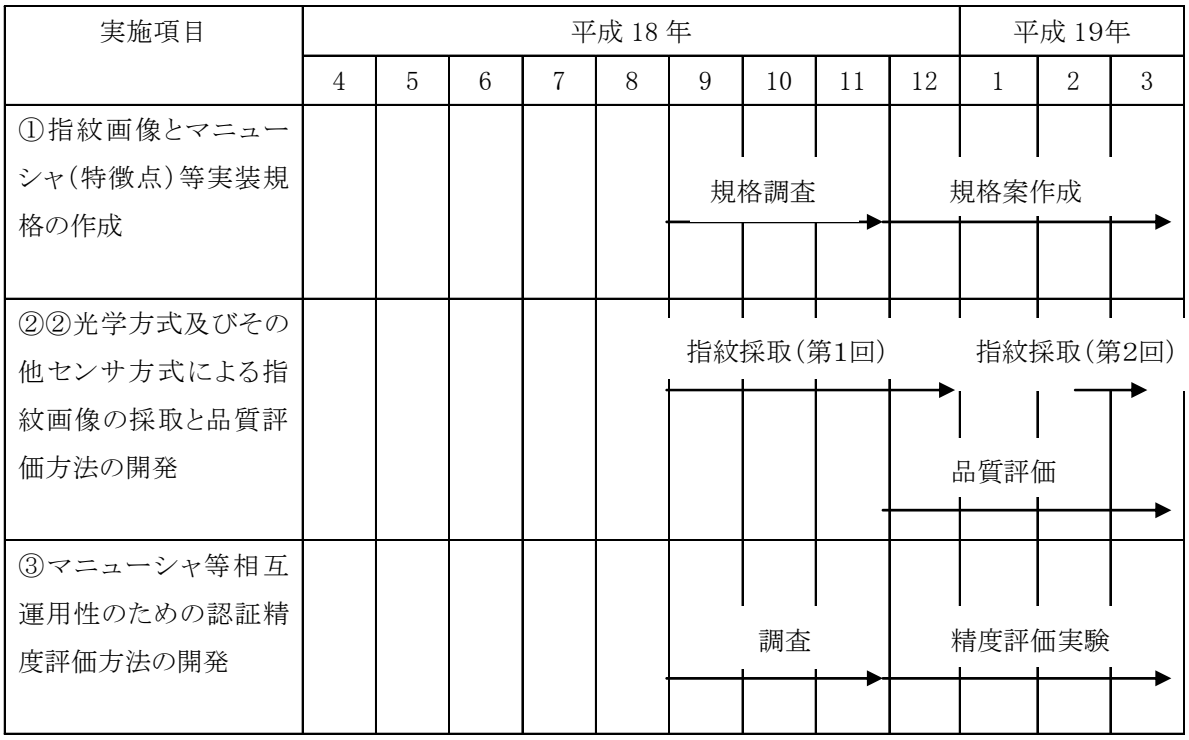


図 1-1 実施スケジュール

1.4. 委員会の体制

1.4.1. 研究組織

調査研究は，次の研究組織構成で行われた。

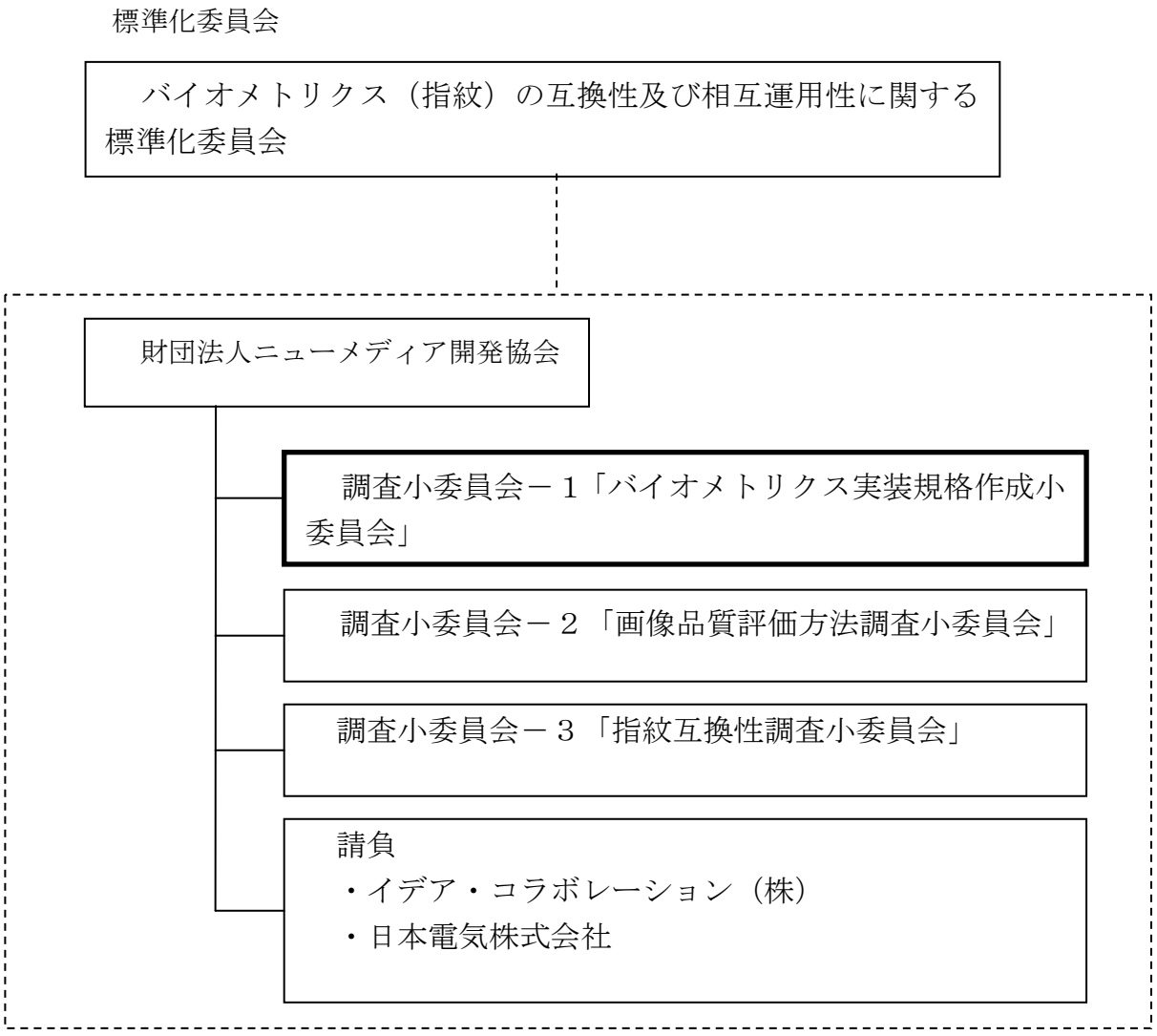


図 1-2　組織構成図

1.5. 小委員会１の構成

小委員会１の構成は次の通りである。

役割	氏名	所属	役職
委員長	新崎　卓	株式会社富士通研究所	SC37WG3 主査
委員	寄本　義一	凸版印刷株式会社	本部長付
委員	坂本　静生	日本電気株式会社メディア情報研究所	主任研究員
委員	春山　智	株式会社ＮＴＴデータ技術開発本部	シニアエキスパート
委員	朝倉　久	株式会社日立製作所　セキュリティ事業部	主任技師
委員	栗田　寛久	セキュアデザイン株式会社　R&D センター技術サポート部	SC37WG2 幹事
委員	溝口　正典	日本電気株式会社第二官庁システム事業部	バイオメトリクスエキスパート
委員	笹川　耕一	三菱電機株式会社先端技術総合研究所	プロジェクトマネージャ
オブザーバ	槇得　菊男	法務省入国管理局出入国情報管理室	補佐官
オブザーバ	坂本　秋彦	法務省入国管理局出入国情報管理室	システム企画係長
オブザーバ	森田　信輝	経済産業省産業技術環境局情報電気標準化推進室	課長補佐
事務局	林　義昭	（財）ニューメディア開発協会	主任研究員
事務局	滝沢　俊男	（財）ニューメディア開発協会	主任研究員
事務局	岸本　芳典	（財）ニューメディア開発協会	主任研究員

2. 関連規格に関する文献調査

本研究調査では，指紋画像とマニューシャ等実装規格の作成に関する検討を行うにあたり，ISO/IEC 7816-11:2004，ISO/IEC 19794-2:2005（指紋マニューシャ），ISO/IEC 19794-4:2005（指紋画像），ISO/IEC 19785-1:2006（CBEFF），2nd FCD 19785-3:2006（TLV フォーマット）規格及び，ICAO の論理データ構に関する規格を精査した。各規格の関係を図 2-1 に示す。

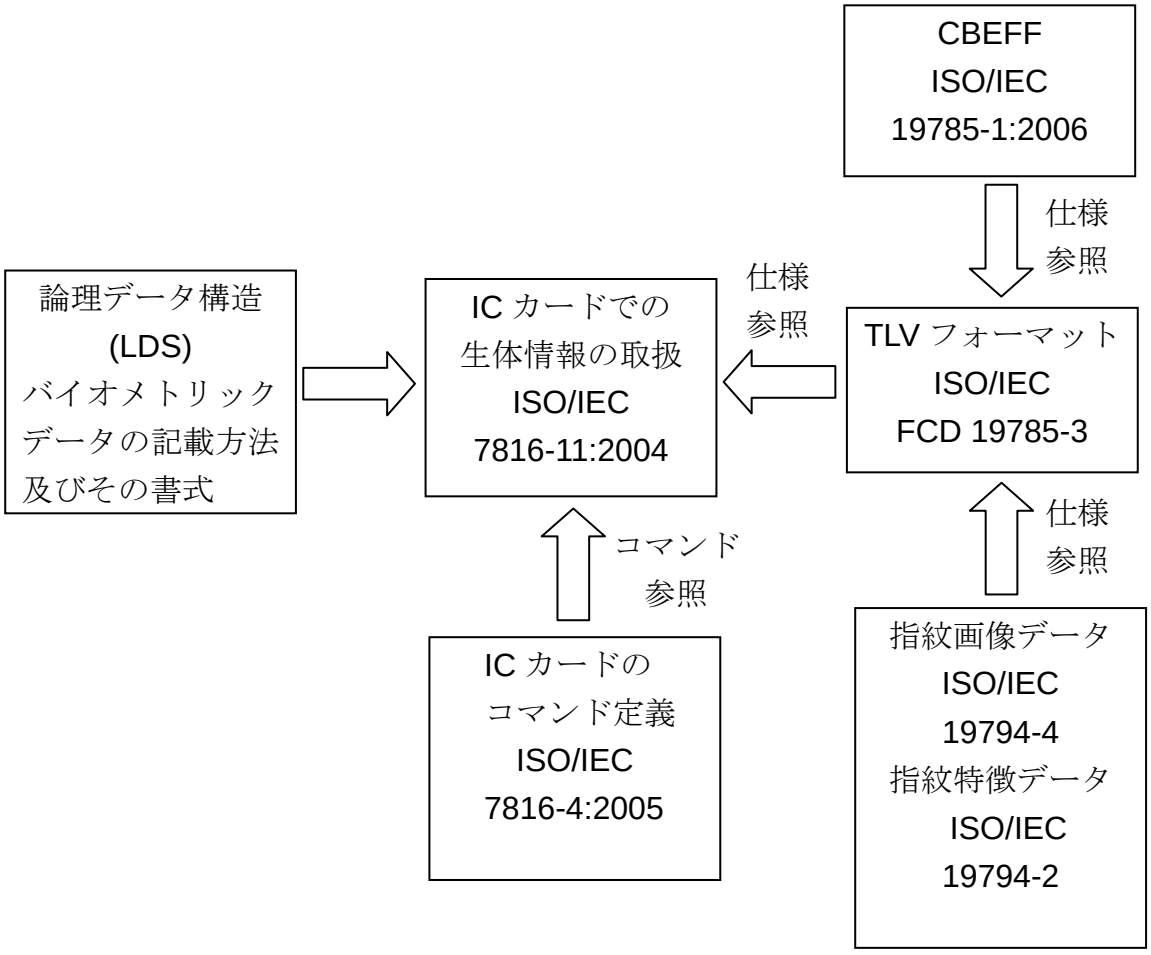


図 2.1 精査した規格の関係図

2.1. ISO/IEC 7816-11:2004

ISO/IEC 7816-11:2004 は，IC カードでバイオメトリック照合を利用するための唯一の国際規格である。IC カードを単なるバイオメトリック情報の運搬媒体として利用するカード外マッチングの用途，及びバイオメトリック照合そのものをカード内で実行するカード内マッチングの用途の双方を考慮した，データ構造及びデータ利用方法について規定する。なお，この規格では本人確認(1 対 1 照合)を対象としており，識別(1 対 N 照合)はその範囲ではない。

なお，この規格と一致規格である JIS X 6320-11 が 2007 年に発行される見込みである。

2.1.1. 関連規格

ISO/IEC 7816-11:2004 は二つの規格を引用する。これらは同時進行的に議論が進んでいたものであったため，記載の規格番号はやや古く，一つは ISO/IEC 7816-4:2003，もう一つは ISO/IEC CD 19785:2003 となっている。前者は 2003 年中に成立することを見込んでこの表記となったものであり，実際にはやや遅れて成立した ISO/IEC 7816-4:2005 が参照すべき規格である。後者は ISO/IEC JTC 1/SC 37 における議論の中で，三つの規格へ分割された。第 1 部及び第 2 部は 2006 年に成立したが，この規格が引用すべきである第 3 部は 2007 年 1 月現在なお開発が進行中であり，最新文書は ISO/IEC FCD 19785-3:2006 である。

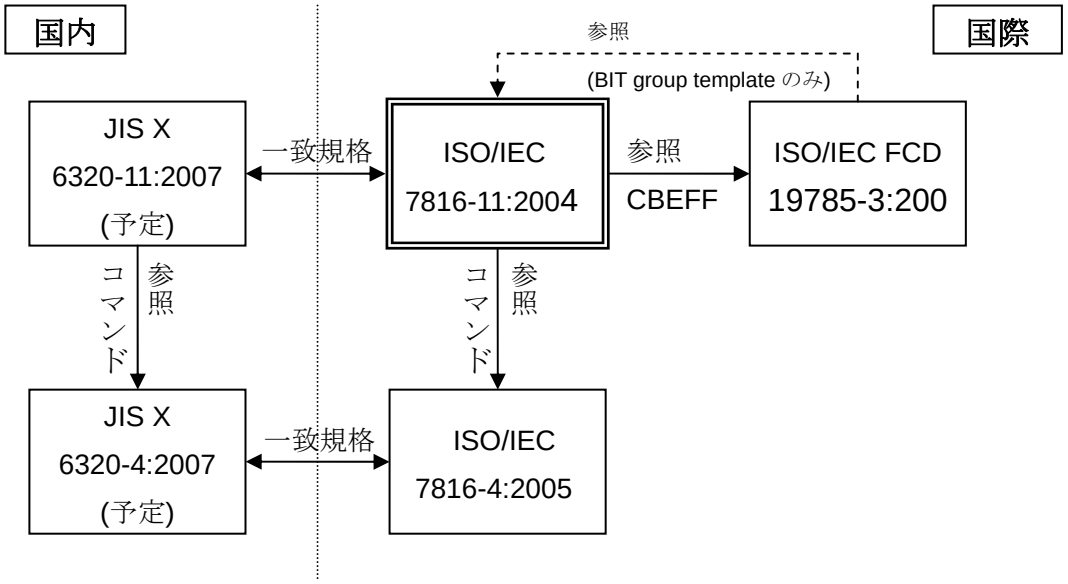


図 2.1.1 ISO/IEC 7816-11:2004 と関連する主な規格の関係

図 2-2 にこの規格と関連規格の間の簡単な関係を示す。この規格は ISO/IEC

7816-4:2005 を参照し, バイオメトリック照合を利用する際のコマンドの使い方を規定する。また ISO/IEC FCD 19785-3:2006 が規定する CBEFF (Common Biometric Exchange Formats Framework)を参照し，バイオメトリック情報データオブジェクト及びバイオメトリックデータオブジェクトを規定する。前者の内容はバイオメトリック情報テンプレートまたは複数のバイオメトリック情報テンプレートからなる BIT グループテンプレートであり，この規格では IC カードに係わる一部を除き ISO/IEC 19785-3 の規定を参照することになる予定である。

なお, BIT グループテンプレートは ISO/IEC FCD 19785-3:2006 で規定されておらず，ISO/IEC 7816-11:2004 を引用する相互依存関係にあることに注意が必要である。

JIS X 6320-11:2007 (予定)は，上述の ISO/IEC 7816-11:2004 との一致規格であり, 本邦内での利用普及を目指して 2007 年に発行される見込みである。また, 引用規格である ISO/IEC 7816-4:2005 の一致規格である JIS X 6320-4:2007 (予定)も同様に，2007 年度中の発行を目指している。

2.1.2. 想定するバイオメトリック照合手法とその処理

バイオメトリック照合に利用するコマンド及びデータの形式は，バイオメトリック照合そのものの手法や IC カードにバイオメトリック照合処理のどの役割を担わせるのかによって異なる。この規定で想定するバイオメトリック照合が附属書 A に記載されており，この附属書 A(参考情報)を理解することでこの規定全体を見通しよく理解することができる。

図 2.1.2 に，この規格の附属書 A より図 A-1 を引用して示す。この図はバイオメトリック照合における典型的な登録処理のブロック図である。

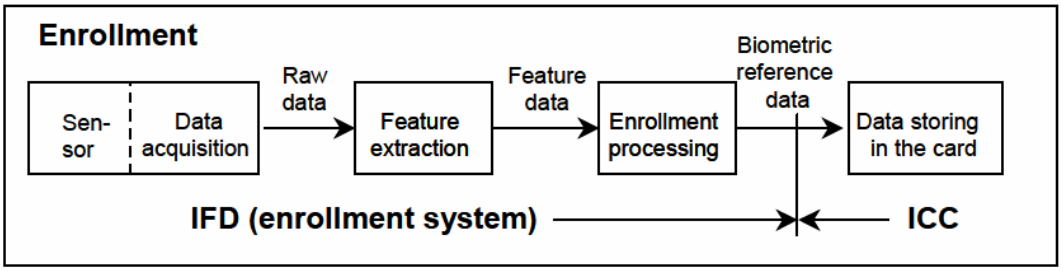


Figure A.1 — General scheme of an enrollment process

図 2.1.2 バイオメトリック照合における典型的な登録処理 (附属書 A 図 A.1 より引用)

各構成要素は左からセンサ及びデータ取得，特徴抽出，登録処理，カード内へのデータ記録である。各ブロック間を流れるデータは同じく左から，原データ，特徴データ，バイオメトリック参照データである。バイオメトリック参照データは，バイオメトリック照合分野における，登録したテンプレートに相当する用語として用いている。なお，この規格での用語テンプレートは ISO/IEC 7816-4:2005 で定義する構造化データオブジェクトの意味で用いており，注意が必要である。

同図中，右端の ICC と描かれた構成要素が IC カードに相当し，それ以外の IFD と描いた構成要素群は，カード外のインタフェースデバイスで処理される内容である。

図 2.1.3 に，この規格の附属書 A より図 A.2 を引用して示す。この図はバイオメトリック照合における典型的な本人確認処理のブロック図である。

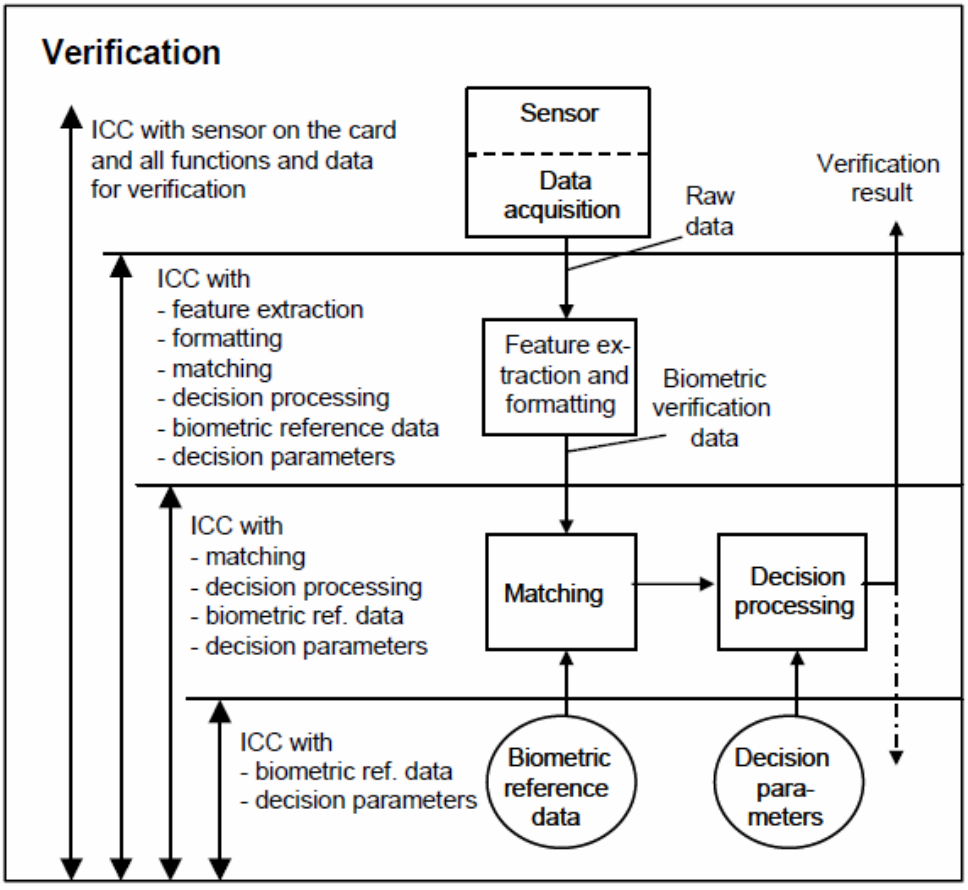


Figure A.2 — General scheme of a verification process

図 2.1.3 生体認証における典型的な本人確認処理 (附属書 A 図 A.2 より引用)

センサ及びデータ取得構成要素によって得られた原データは，特徴抽出及び書式付け構成要素によりバイオメトリック照合データへと変換される。マッチング構成要素は，このバイオメトリック照合データ及びバイオメトリック参照データを比較し，二つのデータ間の距離あるいは類似度を出力する。場合によっては IC カードに本人かどうかの判断を行う判定パラメータを記録しておき，判定処理により最終的な本人確認結果を出力する。

この本人確認処理を実施するにあたって，IC カードに何の役割を担わせるのかのバリエーションが存在する。この図では，次の四つの種類について図式化している。

1. カード上にセンサ，及び照合のためのすべての機能及びデータをもつ
2. 特徴抽出，書式付け，マッチング，判定処理の各機能，バイオメトリック参照データ及び判定パラメータの各データをもつ
3. マッチング，判定処理の各機能，バイオメトリック参照データ及び判定パラメータの各データをもつ
4. バイオメトリック参照データ及び(場合によっては)判定パラメータをもつ

次に，バイオメトリック照合を次の二つの手法に分類している。

1. 静的なバイオメトリック照合
2. 動的なバイオメトリック照合

静的なバイオメトリック照合とは，例えば顔，指紋，虹彩，静脈[1]のように，認証対象となる人物の生理学的な特徴を提示する，又は動的なバイオメトリック照合のうちあらかじめ登録済みである決めた動作を実行する手法を指す。

一方，動的なバイオメトリック照合とは，口唇の動きや署名，音声のように，認証対象となる人物の動的な行動を要求する手法を指す。つまり，バイオメトリック照合を実施する時毎にチャレンジとして，例えば『ニューメディア開発協会』などの単語を選択して認証対象となる人物に提示し，行動させること(この例の場合発話)を要求する手法である。即ち，バイオメトリック照合に用いるモーダルに応じたチャレンジを何らかの方法で入手する必要がある。

その他に注意すべき主な点として，次が挙げられている(抜粋)。

[1] ISO/IEC 7816-11:2004 において静的なバイオメトリック照合として例示された順に，著名なモーダルを抜き出して記述した。動的なバイオメトリック照合についても同様である。

- 顔，耳，指紋など，公にさらされており，誰によっても獲得あるいは計測が可能な特徴については，センサがカードに実装されている場合を除き，インタフェースデバイスからカードへは信頼できる方法で提示するのがよい。
- インタフェースデバイスは照合に関連した情報を必要としてよい。例えば，次に示すものである。
  - 指紋や顔などのバイオメトリックタイプ，右手人差し指や左手中指などのバイオメトリックサブタイプ，バイオメトリックデータの形式所有者(例えば ISO/IEC JTC 1/SC 37)及び形式タイプ(例えば ISO/IEC 19794-2:2005)
  - MANAGE SECURITY ENVIRONMENT コマンドで用いるアルゴリズム参照
  - VERIFY コマンドや EXTERNAL AUTHENTICATE コマンドで用いるバイオメトリック参照データ識別子
  - その他任意のデータ(補助データ利用について，ISO/IEC 19785-1 に例示がある)

2.1.3. 規定内容の概略

この規格の 5 条及び 6 条から，バイオメトリック照合のためのコマンド及びデータ要素について説明する。

表 2-1 に，静的及び動的なバイオメトリック照合に，カード内マッチングの際に用いるコマンドを整理した。

表 2.1.1 静的及び動的なバイオメトリック照合に用いるコマンド

種別	用いるコマンド	伝達する情報		備考
静的	VERIFY[2]	バイオメトリック参照データ識別子		複数のバイオメトリック照合を用いるときにはコマンド連鎖を用いてよい[3]
		バイオメトリック照合データ	BER-TLV データオブジェクトとして符号化してよい	
動的	GET CHALLENGE[4]	P1 でバイオメトリックアルゴリズムを指定してよい		アルゴリズム選択は MANAGE SECURITY ENVIRONMENT コマンドで行ってよい
	EXTERNAL AUTHENTICATE[5]	バイオメトリック照合データ	BER-TLV データオブジェクトとして符号化してよい	

5 条はコマンドについての規定である。冒頭，公にさらされており，誰によっても獲得あるいは計測が可能なバイオメトリック特徴については，ISO/IEC 7816-4 に規定するセキュアメッセージングによる暗号化チェックサム又は，ディジタル署名を付与してインタフェースデバイスからカードへ送る方法を例示している(規定ではない)。また，カードから読む出すバイオメトリック参照データの信頼性を保証するために，セキュアメッセージングを用いてもよい(カード内マッチング)。カードからバイオメトリック参照データの信頼性を保証するために，セキュアメッセージングを用いてもよい(カード外マッチング)。

6 条はデータ要素に関する規定である。

バイオメトリック情報テンプレートは，バイオメトリック照合に先立ち実行する読み出しコマンドによってカードから読み出される，バイオメトリックデータに関連する情報である。

表 2.1.2 に，この規格の表 1 からバイオメトリック情報データオブジェクト

[2] ISO/IEC 7816-4:2005 及びその一致規格である JIS X 6320-4:2007 (発行予定)で規定。

[3] ISO/IEC 7816-8:2004 及びその一致規格である JIS X 6320-8:2006 で規定。

[4] バイオメトリックチャレンジコードの取得に用いる。

[5] バイオメトリック照合に用いる。

を引用する。カード外マッチングの場合，このバイオメトリック情報データオブジェクトの中に，バイオメトリック参照データを含んでもよい。

表 2.1.3 に，この規格の表 2 から，BIT グループテンプレートを引用する。この図は，複数のバイオメトリック情報テンプレートを同一のアプリケーションで用いる場合には，この BIT グループテンプレートを利用しなければならない。読み出しは，GET DATA コマンドなどにより行うことができる。

もう一つのデータとして，バイオメトリック参照データ又はバイオメトリック照合データであるバイオメトリックデータがある。バイオメトリックデータは，データ要素の連結，ISO/IEC 7816-6:2004 及びその一致規格である JIS X 6320-6:2006 で規定するバイオメトリックデータ DO 内でのデータ要素の連結，又はバイオメトリックデータ内でのデータオブジェクトの連結で与えてよい。表 2.1.4 に，この規格の表 3 から，一番最後の場合に相当するバイオメトリックデータオブジェクトを引用する。

表 2.1.2 バイオメトリック情報データオブジェクト (表 1 より引用)

Table 1 — Biometric information DOs

Tag	L	Value					Presence
'7F60'	Var.	Biometric Information Template (BIT)					
		Tag	**L**	**Value**			
		'80'	1	Algorithm reference for use in the VERIFY / EXT. AUTHENTICATE / MANAGE SE command			Optional
		'83'	1	Reference data qualifier for use in the VERIFY / EXT. AUTH. / MANAGE SE command			Optional
		'A0'	Var.	Biometric information DOs defined in this standard			Optional
		'06' '41' '42' '4F'	Var. Var. Var. Var.	Tag allocation authority (see ISO/IEC 7816-6): - Object identifier (OID) - Country authority (see ISO/IEC 7816-4) - Issuer (see ISO/IEC 7816-4) - Application Identifier (AID), identifies the application and its provider (see ISO/IEC 7816-4) The default tag allocation authority is ISO/IEC JTC1/SC37.			One of these DOs is mandatory, if 'A1' is present
		'A1'	Var.	Biometric information DOs specified by the tag allocation authority (mandatory indication, see above). See also example in Annex C			Mandatory, if 'A0' is not present
				Tag	**L**	**Value**	
				'8x'/ 'Ax' '9x'/ 'Bx'	Var. Var.	DOs defined by the tag allocation authority ... (primitive / constructed) ... (primitive / constructed)	DO dependent

表 2.1.3　BIT グループテンプレート (表 2 より引用)

Table 2 — BIT group template

Tag	L	Value			Presence
'7F61'	Var.	BIT group template			
		Tag	**L**	**Value**	
		'02'	Var.	Number of BITs in the group	Mandatory
		'7F60'	Var.	BIT 1	Conditional
				...	
		'7F60'	Var.	BIT n	Conditional

表 2.1.4 バイオメトリックデータオブジェクト (表 3 より引用)

Table 3 — Biometric data DOs

Tag	L	Value			Presence
'5F2E'	Var.	Biometric data			
'7F2E'	Var.	Biometric data template			
		Tag	**L**	**Value**	
		'5F2E'	Var.	Biometric data	At least one of these DOs is present, if the template is used
		'81' / 'A1'	Var.	Biometric data with standardised format (primitive / constructed)	
		'82' / 'A2'	Var.	Biometric data with proprietary format (primitive / constructed)	

表 2.1.4 に示したように標準形式バイオメトリックデータとは別に, 性能の向上他の達成を目的として個別利用形式バイオメトリックデータをもちいてよい。

この他に照合要求情報を，照合要求情報データオブジェクト又は照合要求情報テンプレートのいずれかによって提供する。前者は短縮形式，後者は詳細形式であり，カード所持者照合のための参照データ(バイオメトリック参照データを含む)が有効又は無効かの情報(カード所持者が決定)，利用可能又は不可能かの情報(アプリーケーション提供者が決定)などの情報を含んでいる。

2.1.4. その他附属書の概略

この規格における附属書はすべて参考情報である。既に 2.1.2 節で説明した附属書 A を除く，附属書 B，C 及び D について簡単に述べる。

参考情報に位置づけられた附属書 B では，登録処理及び照合処理におけるコマンド及びデータの例示があり，具体的なコマンド列の理解に役立つ。例示の中から，次に本報告書に関連するカード外マッチングにおける例を示す。

図 2.1.5 に，この規格の附属書 B より図 B.7 を引用して示す。この図は，バイオメトリック情報テンプレートを読み出すためのコマンドの一例である。SELECT コマンドにより，バイオメトリック情報テンプレートを含むファイルを選択した後，READ BINARY コマンドで読み出す。

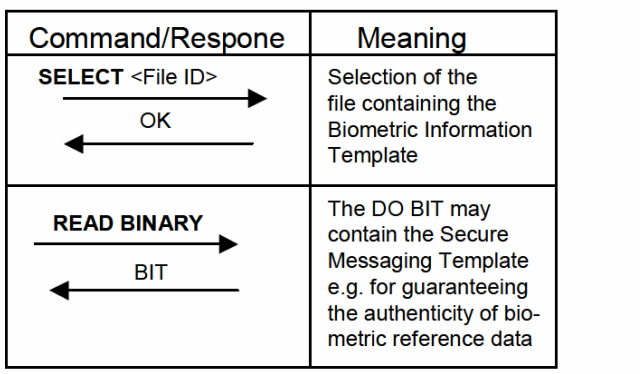


Figure B.7 — Commands for retrieval of the BIT (example)

図 2.1.5 カード外マッチングにおけるバイオメトリック情報テンプレートを読み出すためのコマンド例 (附属書 B 図 B.7 より引用)

図 2.1.6 に，この規格の附属書 B より図 B.8 を引用して示す。この図は，バイオメトリック情報テンプレート読み出しのためにあらかじめ認証が必要な場合のコマンドの一例である。GET CHALLENGE コマンドによって乱数を取得した後，EXTERNAL AUTHENTICATE コマンドでバイオメトリック情報テンプレートへのアクセス権をもつエンティティを認証する。これによって，READ BINARY コマンドで，バイオメトリック情報テンプレートを読み出す。

附属書 C は, バイオメトリック情報データオブジェクトの例を多く掲載する。この附属書はあくまでも参考情報であり，ISO/IEC 19785-3 が規定する CBEFF BER-TLV 形式を参照すべきである。なお，ISO/IEC 19785-3 は 2007 年 1 月時点で未だ FCD として議論が続いており, 附属書 C との齟齬が一部生じ始めている。留意すべき点を，2.1.5 にまとめる。

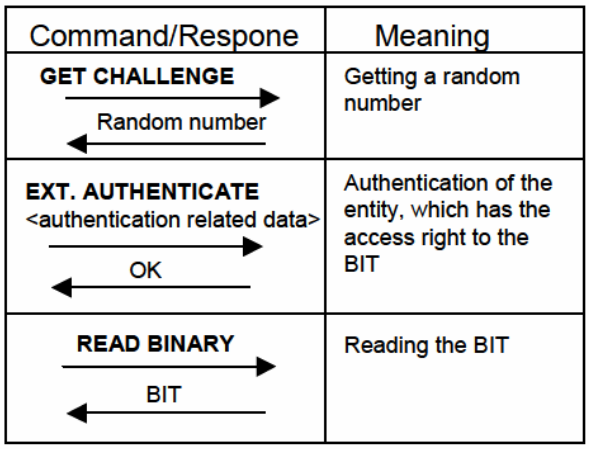


Figure B.8 — Commands for retrieval of the BIT after performing an authentication procedure (example)

図 2.1.6 カード外マッチングにおける認証手続きの実施後にバイオメトリック情報テンプレートを読み出すためのコマンド例 (附属書 B 図 B.8 より引用)

附属書 D では，セキュアメッセージングの利用法についての参考情報を記述する。例えばバイオメトリック情報テンプレートを，プライバシ保護及び／又は完全性検証のために, それぞれ暗号化や, 署名又は MAC の利用をしてもよい。セキュアメッセージングによって実現してもよく，具体的な符号化例を示している。

2.1.5. 留意点

既に述べたとおり引用規格として記載の番号はやや古く，ISO/IEC 7816-4:2005 及び，まだ正式に IS として成立してはいないが ISO/IEC FCD 19785-3:2006 となる(2007 年 1 月現在)。

この規格の附属書 C で示されている 2 バイト長の製品識別子は, ISO/IEC FCD 19785-3:2006 では次のとおり規定されており，齟齬が生じている。

- 2 バイト長の製品所有者及び，2 バイト長の製品タイプの結合であり，4 バイト長

なお製品所有者及び製品タイプは，製品識別子と同じく IBIA が登録管理を行う。

同じく附属書 C における表 C.2 及び表 C.3 で示すバイオメトリックタイプ及びバイオメトリックサブタイプは，ISO/IEC FCD 19785-3:2006 では歴史的に使われてきた要約値の符号化と題する表へと移された。また ISO/IEC FCD 19785-3 におけるバイオメトリックタイプ及びバイオメトリックサブタイプについて，歴史的経緯及び現在のバイオメトリック技術を鑑みた定義をどうする

か ISO/IEC JTC 1/SC 37 で審議が続いている。

2.2. ISO/IEC 7816-4：2005

ISO/IEC 7816-4(対応 JIS 原案作成中)は，IC カードのファイル構造やコマンド機能の規定で，今回の改定で，外部端子付 IC カード以外に，外部端子なし IC カードにも使用される規定となった。同時に，ISO/IEC 7816 シリーズのほかの部に存在していた関連規定もこの部にまとめ直している。

「1 適用範囲」で，次のように，この部の規定している内容を示している。

・カードのインタフェースで交換されるコマンド・レスポンス対の内容。
・カードのデータ要素及びデータオブジェクトの読出し手段。
・カードの動作特性について記述する管理情報バイトの構造及び内容。
・コマンドを処理するときに，カードのインタフェースに現れるカードのアプリケーション及びデータの構造
・カードのファイル及びデータへのアクセス方法。
・カードのファイル及びデータにアクセスする権限を定義するセキュリティ機構。
・カードのアプリケーションを識別し指定するための手段及び機構。
・セキュアメッセージングの方法。
・カードよって処理される暗号化アルゴリズムへのアクセス方法。しかし，これらのアルゴリズムについては記述しない。

2.2.1. 情報交換のためのコマンドとレスポンスの構成

コマンド・レスポンス対

通常，端末から IC カードにコマンドが送られ，IC カードがコマンドを受け入れた後に，コマンド処理を行い，レスポンスとしてカードから端末へ送り返される。一つの処理は，このコマンドとレスポンスの対で構成される。

2.2.1.1. コマンド

処理に対応するコマンドとその INS (instruction byte)の値 16 進数を次に示す。

表 **2.2.1**　アルファベット順のコマンド

コマンド名	**INS**	参照
ACTIVATE FILE	“44”	第 9 部
APPEND RECORD	“E2”	7.3.7
CHANGE REFERENCE DATA	“24”	7.5.7
CREATE FILE	“E0”	第 9 部
DEACTIVATE FILE	“04”	第 9 部
DELETE FILE	“E4”	第 9 部
DISABLE VERIFICATION REQUIREMENT	“26”	7.5.9
ENABLE VERIFICATION REQUIREMENT	“28”	7.5.8
ENVELOPE	“C2”, “C3”	7.6.2
ERASE BINARY	“0E”, “0F”	7.2.7
ERASE RECORD (S)	“0C”	7.3.8
EXTERNAL(/ MUTUAL) AUTHENTICATE	“82”	7.5.4
GENERAL AUTHENTICATE	“86”, “87”	7.5.5
GENERATE ASYMMETRIC KEY PAIR	“46”	第 8 部
GET CHALLENGE	“84”	7.5.3
GET DATA	“CA”, “CB”	7.4.2
GET RESPONSE	“C0”	7.6.1
INTERNAL AUTHENTICATE	“88”	7.5.2
MANAGE CHANNEL	“70”	7.1.2
MANAGE SECURITY ENVIRONMENT	“22”	7.5.11
PERFORM SCQL OPERATION	“10”	Part 7
PERFORM SECURITY OPERATION	“2A”	第 8 部
PERFORM TRANSACTION OPERATION	“12”	Part 7
PERFORM USER OPERATION	“14”	Part 7
PUT DATA	“DA”, “DB”	7.4.3
READ BINARY	“B0”, “B1”	7.2.3
READ RECORD (S)	“B2”, “B3”	7.3.3
RESET RETRY COUNTER	“2C”	7.5.10
SEARCH BINARY	“A0”, “A1”	7.2.6
SEARCH RECORD	“A2”	7.3.7

SELECT	“A4”	7.1.1
TERMINATE CARD USAGE	“FE”	第 9 部
TERMINATE DF	“E6”	第 9 部
TERMINATE EF	“E8”	第 9 部
UPDATE BINARY	“D6”, “D7”	7.2.5
UPDATE RECORD	“DC”, “DD”	7.3.5
VERIFY	“20”, “21”	7.5.6
WRITE BINARY	“D0”, “D1”	7.2.4
WRITE RECORD	“D2”	7.3.4

注） 第 9 部 : ISO/IEC 7816-9，Part 7 : ISO/IEC 7816-7，第 8 部 : ISO/IEC 7816-8 を示す。

2.2.1.2. 状態バイト

送られてきたコマンドについてICカード側の処理後の状態を端末に知らせる情報。レスポンスで SW1-SW2 として端末に返す。

2.2.1.3. データオブジェクト

IC カードのファイルに格納するデータを，TLV 形式で符号化する場合には，すべてのデータフィールド又はデータフィールドの連結はデータオブジェクトの連続とする。TLV 形式とは，タグ・長さ・値(tag，length，value)の構造で，value の位置に格納されるデータが記述される。

2.2.1.4. BER-TLV 長さフィールド

BER-TLV データオブジェクトは，二つ又は三つの連続するフィールド[必す(須)タグフィールド，必す(須)長さフィールド及び条件付きの値フィールド]で構成される。このときの，長さフィールドは次に示す構成をとる。

表 2.2.2　ISO/IEC 7816 群の BER-TLV 長さフィールド

構成バイト数	1 バイト目	2 バイト目	3 バイト目	4 バイト目	5 バイト目	表現可能な値
1 バイト	“00”～“7F”	-	-	-	-	0 ～ 127
2 バイト	“81”	“00”～“FF”	-	-	-	0 ～ 255
3 バイト	“82”	“0000” ～ “FFFF”		-	-	0 ～ 65 535
4 バイト	“83”	“000000” ～ “FFFFFF”			-	0 ～ 16 777 215
5 バイト	“84”	“00000000” ～ “FFFFFFFF”				0 ～ 4 294 967 295

2.2.2. アプリケーションとデータの構造

ここでは，共通クラスでコマンドを処理する場合にインタフェース上に現れるアプリケーションとデータの構造を規定しており，2 種類の構造，専用ファイル(DF)及び基礎ファイル(EF)が提供されている。

次に示す例は，インタフェース上にファイル構成のの根幹となる DF（MF と呼ばれる）が現われる構造である。

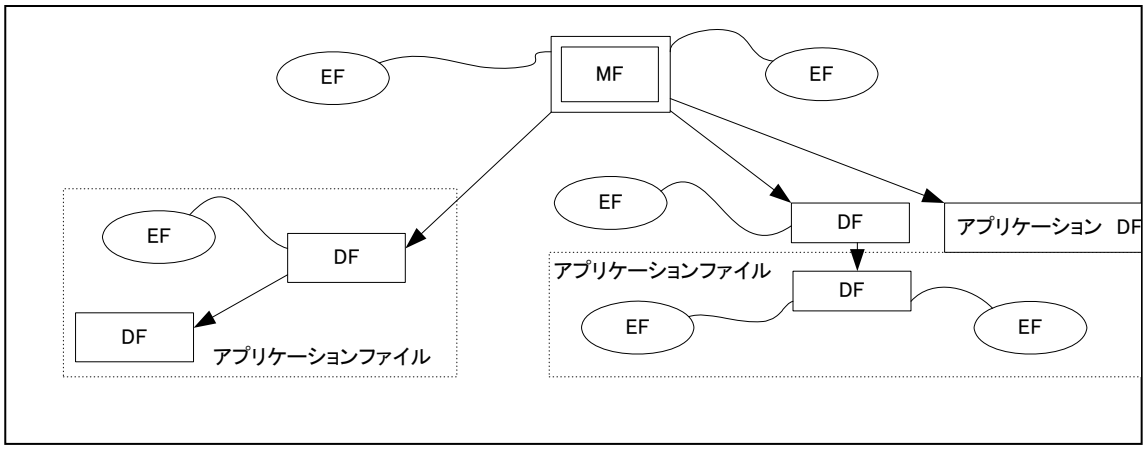


図 2.2.1　DF の階層構造の例

また，図 2.2.2 には，インタフェース上に MF が現れない並列のアプリケーション DF(すなわち，明白な階層のない DF)の例を示す。

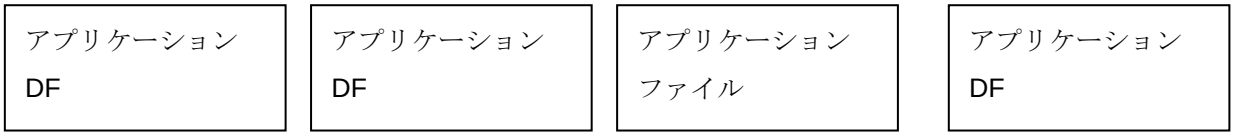


図 2.2.2　独立しているアプリケーション DF の例

2.2.2.1. 構造選択

構造選択により，図 2.2.1 及び図 2.2.2 で示す構造内のデータへアクセスが可能になる。構造が DF の場合にはその配下の構造へのアクセスが可能になる。次の四つの方法がある。

DF 名による選択　DF 名によって，DF を参照する。

ファイル識別子による選択　ファイル識別子によって，ファイル(DF，EF)を参照する。

パスによる選択　パスによって，ファイル(DF，EF)を参照する。

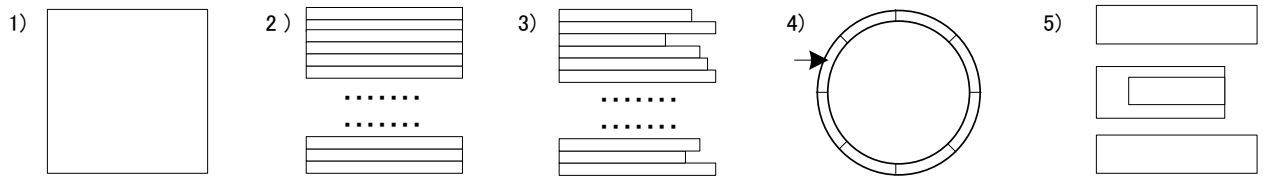
短縮 EF 識別子による選択　短縮 EF 識別子によって，EF を参照する。

2.2.2.2. データ参照方法

EF では，**透過構造・レコード構造・TLV 構造の**三つの構造が規定されている。

レコード構造には，固定長順編成・可変長順編成・固定長循環順編成の三種類が存在する。

EF 内のデータを参照するために，カードは，図 2.2.3 に示す五つの構造の中から，少なくとも一つは提供することになっている。



1) 透過構造
2) 固定長順編成構造
3) 可変長順編成構造
4) 固定長循環順編成構造
5) TLV 構造

図 2.2.3　EF の構造

2.2.3. セキュリティ機構

2.2.3.1. 概要

リセット応答後や認証手続き実行後の IC カード内部のセキュリティに関する現在の状態を表すものとして，セキュリティステータスが存在する。

セキュリティステータスは，次の 4 種類がある。

－グローバルセキュリティステータス
－アプリケーション特有セキュリティステータス
－ファイル特有セキュリティステータス
－コマンド特有セキュリティステータス

2.2.4. セキュアメッセージング

二つの基本的なセキュリティ機能(データ機密性及びデータ認証)によって，コマンド・レスポンス対，又は連続するデータフィールドの連結(コマンド連鎖又は“61”に設定された SW1 の使用による)のすべて又は一部を保護する方法をセキュアメッセージング(SM)という。

2.2.4.1. SM フィールド及び SM データオブジェクト

セキュアメッセージング行う場合には, SM テンプレート(タグ“7D”)と同様に, SM の書式による任意のコマンド又はレスポンスのデータフィールドを SM フィールドと規定している。

2.2.4.2. 基本 SM データオブジェクト

基本 SM データオブジェクトには，**平文をカプセル化する SM データオブジェクト**，**機密性のための SM データオブジェクト**，**及び**認証のための SM データオブジェクトがある。

平文をカプセル化する SM データオブジェクトでは，SM フィールド，及び BER-TLV で符号化されていないデータに対しては，カプセル化することが必す(須)としている。

2.2.4.3. 補助 SM データオブジェクト

補助 SM データオブジェクトには, セキュリティ環境識別子，レスポンス記述子テンプレート及び制御参照テンプレートがある。

制御参照テンプレートでは，対称又は非対称の暗号技術(CT-sym 及び CT-asym)を使用した，認証(AT)，かぎ(鍵)共有(KAT)，ハッシュコード(HT)，暗号化チェックサム(CCT)，ディジタル署名(DST)及び機密性(CT)に有効な六つの制御参照テンプレートが定義されている。

2.2.4.4. コマンド･レスポンス対への SM の影響

セキュアメッセージングを適用することにより，コマンド及びレスポンスの本体部等に変更が加わる。この対応を図 2.2.4 と図 2.2.5 に示す。

図 2.2.4 にコマンド・レスポンス対を示す。

コマンドヘッダ部	コマンド本体部
CLA INS P1 P2	[Lc フィールド] [データフィールド] [Le フィールド]

レスポンス本体部	レスポンス後続部
[データフィールド]	SW1-SW2

図 2.2.4　コマンド・レスポンス対

図 2.2.5 は，図 2.2.4 に対応する SM 化したコマンド・レスポンス対を示す。

コマンドヘッダ部	コマンド本体部
CLA* INS P1 P2	[新 Lc フィールド] - {[セキュアデータフィールド] = [T-Nc-データバイト] - [T-“01” 又は “02”-Le]} - [新 Le フィールド]

レスポンス本体部	レスポンス後続部
[セキュアデータフィールド] = [T-Nr-データバイト] - [T-“02”-SW1-SW2]	SW1-SW2

図 2.2.5　SM 化したコマンド・レスポンス対

2.2.5. 交換のためのコマンド

この箇条では，次の六つのグループで示す交換のためのコマンドを規定し，すべてのコマンド又は採用したコマンドのすべての任意選択を採用することは，この規格に準じるすべてのカードに対して必す(須)ではないとしている。

1) 選択
2) データ単位の取扱い
3) レコードの取扱い
4) データオブジェクトの取扱い
5) 基本セキュリティの取扱い
6) 伝送用コマンドの取扱い

次に，六つのグループ及びグループに属するコマンドの概要について述べる。

2.2.5.1. 選択

リセット応答の後，管理情報バイト又は初期データ列で別段の定めがない限り MF 又はアプリケーション DF は，暗黙的に基本論理チャネルを用いて選択される。

2.2.5.1.1. SELECT コマンド

SELECT コマンドは，処理が完了したとき，CLA で番号付けられた論理チャネルを開き，開けない場合(ファイルが閉そく(塞)しているなど)でも，その論理チャネルでカレント構造を設定する。

2.2.5.1.2. MANAGE CHANNEL コマンド

MANAGE CHANNEL コマンドは，処理が完了したとき，基本チャネル以外の論理チャネルを開閉する。チャネルは，1～19(これより大きい番号は将来使用するために予約される)の番号を付ける。

2.2.5.2. データ単位の取扱い

2.2.5.2.1. データ単位

データ単位を提供する各 EF 内で，オフセットは各データ単位を参照しなければならない。EF の最初のデータ単位に対し 0 から，オフセットは，その後のデータ単位ごとに一つずつ増加される。オフセットデータ要素は，最小バイト数で 2 進符号化する。EF に含まれていないデータ単位への参照は誤りとする。

2.2.5.2.2. READ BINARY コマンド

レスポンスデータフィールドは，データ単位をサポートする EF の内容又は内容の一部を与える。

2.2.5.2.3. WRITE BINARY コマンド

WRITE BINARY コマンドは，ファイル属性に従って EF 内で次の動作のいずれか一つを開始する:

－コマンドデータフィールドで与えられたビットの一度だけの書込み(データ単位の列が論理的消去状態でない場合，コマンドは中断しなければならない)。

－カード内の既存ビットとコマンドデータフィールドで与えられたビットとの論理和(ファイルのビットの論理的消去状態は 0 とする)。

－カード内の既存ビットとコマンドデータフィールドで与えられたビットとの論理積(ファイルのビットの論理的消去状態は 1 とする)。

2.2.5.2.4. UPDATE BINARY コマンド

UPDATE BINARY コマンドは，コマンドデータフィールドで与えられたビットで EF 内の既存ビットの更新を開始する。処理が完了した時，各指定されたデータ単位の各ビットは，コマンドデータフィールドで指定した値となる。

2.2.5.2.5. SEARCH　BINARY コマンド

SEARCH BINARY コマンドは，データ単位をサポートする EF 内の検索を開始する。レスポンスデータフィールドは，データ単位のオフセットを与える。

2.2.5.2.6. ERASE BINARY コマンド

ERASE BINARY コマンドは，与えられたオフセットから始まる EF の内容又は内容の一部を連続して論理的消去状態に設定する。

2.2.5.3. レコードの取扱い

2.2.5.3.1. レコード

レコードをサポートする各 EF 内において，レコード番号及び／又はレコード識別子によって各レコードを参照しなければならない。EF に含まれていないレコードへの参照は誤りとする。

レコード番号による参照　各レコード番号は，唯一かつ連続的に付番する。

－順編成構造。

－循環順編成構造。

2.2.5.3.2. 共通事項

このグループに属するコマンドは，レコードをサポートしない EF に適用した場合中断しなければならない。

このグループの各コマンドは，短縮 EF 識別子を使用してもよい。処理が完了した場合，識別された EF はカレントになり，レコードポインタはリセットされる。コマンド発行時にカレント EF がある場合，プロセスは，EF を示さずに(対応する 5 ビットをすべて 0 に設定することによって)実行してもよい。

2.2.5.3.3. READ RECORD (S) コマンド

レスポンスデータフィールドは，EF 内の指定されたレコードの内容又は単一レコードの先頭部分の内容の一部を与える。

2.2.5.3.4. WRITE RECORD コマンド

WRITE RECORD コマンドは，一つの EF 内で次の動作のいずれか一つを開始する。

2.2.5.3.5. UPDATE RECORD **コマンド**

UPDATE RECORD コマンドは，コマンドデータフィールドで与えられたビットで特定されたレコードの更新を開始する。

2.2.5.3.6. APPEND RECORD コマンド

APPEND RECORD コマンドは，順編成構造をもつ EF の終わりに新規レコードを書込みすること，又は循環順編成構造をもつ EF のレコード番号 1 を書込みすることのいずれかを実行する。

2.2.5.3.7. SEARCH RECORD コマンド

SEARCH RECORD コマンドは，ある EF 内に格納されたレコードに対し，単純な，拡張された，又は個別の検索を実行する。

2.2.5.3.8. ERASE RECORD (S) コマンド

ERASE RECORD(S)コマンドは，P1 によって参照するレコードを論理的消去状態に設定する。又は，P1 によって参照するレコードからファイルの最後まで連続して論理的消去状態に設定する。

2.2.5.4. データオブジェクトの取扱い

2.2.5.4.1. 共通事項

このグループに属するコマンドは，データオブジェクトをサポートしない構造(DF 又は EF)に適用した場合には，中断しなければならない。

2.2.5.4.2. GET DATA コマンド

GET DATA コマンドは，カレントコンテキスト(例えばアプリケーションに特有の環境又はカレント DF)の中で，データオブジェクトをサポートする EF 又は一つの(構造化された)データオブジェクトの内容のいずれかを読み出す。

2.2.5.4.3. PUT DATA コマンド

PUT DATA コマンドは，カレントコンテキスト(例えばアプリケーションに特有の環境又はカレント DF)の中で，データオブジェクトをサポートする EF 又は一つの(構造化された)データオブジェクトの内容のいずれかの処理を開始する。

2.2.5.5. 基本セキュリティの取扱い

2.2.5.5.1. 共通事項

このグループに属するコマンドは，アルゴリズム及び関連する参照データ(例えばかぎ(鍵))を参照するために P1-P2 を使用する。カレントかぎ(鍵)及びカレントアルゴリズムがある場合，コマンドは暗黙的にそれらを使用してもよい。

2.2.5.5.2. INTERNAL AUTHENTICATE コマンド

INTERNAL AUTHENTICATE コマンドは，接続装置によって送られた乱数データ及びカードに格納された関連する秘密データ(例えば，かぎ(鍵))を使用して，カードによって認証データの計算を開始する。

2.2.5.5.3. GET CHALLENGE コマンド

GET CHALLENGE コマンドは，セキュリティに関連する手続き(例えば EXTERNAL AUTHENTICATE コマンド)で使用されるチャレンジ(例えば，暗号認証のための乱数，又は声紋を使用した生体情報認証のせりふ)を発行することを要求する。

2.2.5.5.4. EXTERNAL AUTHENTICATE コマンド

EXTERNAL AUTHENTICATE コマンドは，カードから先行して発行されたチャレンジ(例えば GET CHALLENGE コマンドによる)とカードに格納された(秘密の)かぎ(鍵)と接続装置から送信された認証データとを使ったカードによる計算の結果(合否)に従って，セキュリティステータスを更新する。

MUTUAL AUTHENTICATE 機能　MUTUAL AUTHENTICATE 機能は，EXTERNAL と INTERNAL AUTHENTICATE コマンドと同様に使われる。

2.2.5.5.5. GENERAL AUTHENTICATE コマンド

GENERAL AUTHENTICATE コマンドは，EXTERNAL，INTERNAL 及び MUTUAL AUTHENTICATE 機能を再定義する。３交信認証方式(トリプルズ)の交換は，二つ以上の GENERAL AUTHENTICATE コマンド・レスポンス対を要求する。そのようなコマンド・レスポンス対は連鎖していてもよい。

2.2.5.5.6. VERIFY コマンド

VERIFY コマンドは，接続装置から送られた検証データ(例えばパスワード)又はカード上のセンサから送られた検証データ(例えば指紋)と，格納されている参照データとの比較をカード内で開始する。

2.2.5.5.7. CHANGE REFERENCE DATA コマンド

CHANGE REFERENCE DATA コマンドは，カードに格納されている参照データを接続装置から送られる新しい参照データに置換するか，又は接続装置から送られた検証データとそれらの比較を開始し，その結果でそれらを接続装置から送られた新しい参照データに置換する。

2.2.5.5.8. ENABLE VERIFICATION REQUIREMENT コマンド

ENABLE VERIFICATION REQUIREMENT コマンドは，検証データと参照データを比較する要求を実行可能にする。

2.2.5.5.9. DISABLE VERIFICATION REQUIREMENT コマンド

DISABLE VERIFICATION REQUIREMENT コマンドは，検証データと参照データを比較する要求を実行不可能にする。また，検証データと他の参照データを比較する要求を実行可能にしてもよい。

2.2.5.5.10. RESET RETRY COUNTER コマンド

RESET RETRY COUNTER コマンドは，参照データ再試行カウンタを初期値にリセットするか，又は参照データ再試行カウンタの初期値へのリセット完了後に参照データを変更する。

2.2.5.5.11. MANAGE SECURITY ENVIRONMENT コマンド

MANAGE SECURITY ENVIRONMENT コマンドは，セキュアメッセージング及びセキュリティコマンド(例えば EXTERNAL，INTERNAL，GENERAL AUTHENTICATE，さらに JIS X 6320-8 の PERFORM SECURITY OPERATION 参照)の下処理をする

KEY DERIVATION 機能 主(マスタ)かぎ(鍵)概念を適用すると，主(マスタ)かぎ(鍵)を格納しているカード内でかぎ(鍵)の派生を必要とする場合がある。かぎ(鍵)を派生するために MANAGE SECURITY ENVIRONMENT コマンドを使用する。

2.2.5.6. 伝送用コマンドの取扱い

2.2.5.6.1. GET RESPONSE コマンド

GET RESPONSE コマンドは，利用可能な伝送プロトコルでは送信することができなかったレスポンス APDU 又はその一部分を送信する。

2.2.5.6.2. ENVELOPE コマンド

ENVELOPE コマンドは，利用可能な伝送プロトコルでは送信することができ

なかったコマンド APDU 又は BER-TLV データオブジェクトのいずれか，又はそれらの一部分を送信する。

2.2.6. アプリケーション非依存のカードサービス

アプリケーションに依存しないカードとして共通のサービスとして，次の六つの“カードサービス”を規定している。

1) カード識別
2) アプリケーション識別及び選択
3) パスによる選択
4) データ読出し
5) データ要素読出し
6) カードに起因するバイト列

次に，六つのカードサービスの概要について述べる。

2.2.6.1. カード識別

このサービスにより，接続装置がカードを識別し，それを取扱うことができる。カードの動作特性を示す管理情報バイトが提供される。

2.2.6.2. アプリケーション識別及び選択

このサービスは，カードで提供されているすべてのアプリケーションを識別し，選択する方法と同様に，もしあるならば，どのアプリケーションがカード内で活性化されているかを接続装置が知るようにする。

2.2.6.3. パスによる選択

このサービスは，パス，すなわち 3 バイト以上で構成するファイル参照データ要素によって EF 及び名前を持たない DF も選択できる。

2.2.6.4. データ読出し

このサービスは, 接続装置が DF 及び EF に格納されたデータを読み出せるようにする。

－READ BINARY コマンド
－READ RECORD(S)－GET DATA コマンド

2.2.6.5. データ要素読出し

このサービスは，接続装置が交換のために使用される共通データ要素を読み出せるようにする。

・共通データオブジェクトは，GET DATA コマンドによって読み出されてもよい。

2.2.6.6. カードが作り出すバイト列

このサービスは，カードがバイト列を作り出せるようにする。

この箇条では次の三つの方法を規定する。

－カードが，バイト列を出したいことを示すトリガとしての SW1-SW2 の使い方。このようにして，カードは，返答を期待できる。

－接続装置が，カードから問い合わせ文を読出すための GET DATA コマンド及びカードへの返答を送信するための PUT DATA コマンドの使い方

－バイト列の構成方法

2.2.7. 附属書

この規格には，次の四つの附属書が散在するが，参考であり，規定の一部ではない。

附属書 A (参考)
オブジェクト識別子及びタグ割付け体系の例
附属書 B (参考)
セキュアメッセージングの例
附属書 C (参考)
ENERAL AUTHENTICATE コマンドによる認証機能の例
附属書 D (参考)
発行者識別番号を使用するアプリケーション識別子

2.3. ICAO 仕様(Doc 9303-1)の LDS(Logical Data Structure)

2.3.1. LDS の概要

バイオメトリック情報を格納し携行して使用する機械可読渡航文書(パスポート)の仕様は，ICAO（International Civil Aviation Organization）で策定されており, 通称 Doc 9303-1 と呼ばれている。正式なこのドキュメントの名称は,「Machine Readable Travel Documents Part 1 **Machine Readable Passports** 」で, 最新の第 6 版は 2 分冊「Volume 1 **Passports with Machine Readable Data Stored in Optical Character Recognition Format**」「Volume 2 **Specifications for Electronically Enabled Passports with Biometric Identification Capability**」で構成されている。

Doc 9303-1 の Vol 2 に, e パスポートでのバイオメトリックデータの記載方法及びその書式についての論理データ構造(LDS)が記述されている。

LDS には, アプリケーションに共通な情報を格納するファイル（EF.COM）, 16 個の Data Group（DG）のファイル（EF.DG1～DG16）と，このうちの 15 個のファイル（DG1～DG15）の値について各々のハッシュ値を求め，これらをまとめディジタル署名を付与した情報を格納するファイル(EF.$SO_{D.}$)が存在する。また，各ファイルは，透過構造となっている。

次の，その構造を示す。

Data Group	**Mandatory (M)/ Optional (O)**	**Data Item**	
Common	M	Common data	
	Detail(s) recorded in MRZ of the MRTD		
DG1	M	Machine readable zone (MRZ) data	
	Machine assisted identity confirmation detail(s) — Encoded identification feature(s)		
DG2	M	**GLOBAL INTERCHANGE FEATURE**	Encoded face
DG3	O	Additional feature	Encoded finger(s)
DG4	O	Additional feature	Encoded iris(es)
	Machine assisted identity confirmation detail(s) — Displayed identification feature(s)		
DG5	O	Displayed portrait	
DG6	O	Reserved for future use	
DG7	O	Displayed signature or usual mark	
	Machine assisted security feature verification — Encoded security feature(s)		
DG8	O	Data feature(s)	
DG9	O	Structure feature(s)	
DG10	O	Substance feature(s)*]*	
	Additional personal detail(s)		
DG11	O	Additional personal Data Elements	
	Additional document detail(s)		
DG12	O	Additional document Data Elements	
	Optional detail(s)		
DG13	O	Discretionary Data Element(s) defined by issuing State or organization	
	Reserved for future use		
DG14	O	Reserved for future use	
DG15	O	Active Authentication Public Key Info	
	Person(s) to notify		
DG16	O	Person(s) to notify Data Element(s)	
SO_D	M	Security Data	

図 2.3.1 ファイル構造

2.3.2. LDS の問題

2.3.2.1. 構造による問題

LDS のデータを処理するためには，始めに EF.COM を読み，その情報からどの DG が存在するかを判断し，DG16 以外のそれに対応した DG を全て読み出してハッシュをとり，署名が改竄されていない事を確認する必要がある。

目的の DG 以外に，他の DG も読み出してハッシュをとることから処理時間が多くかかる。

2.3.2.2. ICAO 仕様で規定しているアクセスコマンドの問題

透過構造ファイルを用いていること，及び，1 コマンドで読み出せるデータ長が 2Byte の拡張 Le(最大 64kByte)ではなく 1Byte の Le 指定（最大 256Byte）であるため，Offset 値を変更しながら複数回の READ BINARY コマンドを繰返し用いて読み出さなければならない。

例えば，10kByte のデータを読み出す場合には，40 回以上繰返し READ BINARY コマンドを処理する必要があるため，39 回以上のコマンド解析処理時間が多くかかる。

2.4. ISO/IEC 19785-1：2006

バイオメトリック汎用データ交換フォーマットの枠組み：データ要素仕様

本国際規格は，生体認証技術を応用して異なるベンダーにより構築される複数のアプリケーションやシステム間においてデータの相互交換を可能にすることを目的として，バイオメトリック汎用交換フォーマットの枠組みと構成(Common Biometric Exchange Formats　Framework(CBEFF))を策定している。

2.4.1. ISO/IEC 19785-1 バイオメトリック汎用データ交換フォーマットの枠組みー第一部：データ要素仕様

次の項目について概念，その意味および変換方法の定義と CBEFF 仕様を実現するために必要となる論理データ要素の定義について記述されている。

1) CBEFF の符合化された実体であるバイオメトリック情報レコード（Biometric Information Record(BIR)）の構造とデータ要素の定義
2) 本 CBEFF 規格が応用されると想定できる領域の定義
3) CBEFF 規格に準拠する CBEFF パトロンが公開する CBEFF パトロンフォーマットの概念の定義
4) CBEFF パトロンフォーマットの定義中で使用される CBEFF データ要素の論理値と意味の定義
5) CBEFF パトロンが CBEFF データ要素を使用して，BIR 中の標準バイオメトリック・ヘッダー（SBH）の内容とコード化方法を定義する方法（CBEFF パトロンフォーマットの定義方法）
6) BIR 中のバイオメトリック・データ・ブロック（BDB）のフォーマット識別方法について
   ただし，BDB フォーマットの標準化と相互互換性については本規格では取り扱わない。
7) 一つの CBEFF パトロンフォーマットから異なる CBEFF パトロンフォーマットへの変換方法の定義
8) 個別の CBEFF パトロンフォーマット内で定義される CBEFF データ要素の論理値のコード化は本規格の範囲外である
9) Biometric Registration Authority の活動内容（バイオメトリック組織体識別子の発行，BDB フォーマット，CBEFF パトロンフォーマット，セキ

ュリティ・ブロックフォーマット，バイオメトリック製品の登録）は ISO/IEC 19785-2 で定義されている。

10) ISO/IEC JTC 1/SC37 が CBEFF パトロンとして定義した CBEFF パトロンフォーマットは，ISO/IEC 19785-3 にまとめられている。

11) 生体認証情報の不当な利用と普及から個人のプライバシーを保護する問題は本規格の範囲外である。

2.4.2. 一般仕様

1) CBEFF 単一 BIR 構造と CBEFF 複合 BIR 構造両者による CBEFF パトロンフォーマットが可能である。

2) CBEFF パトロンフォーマットは，登録することが出来（必須ではない），（CBEFF パトロンにより割り付けられた）Biometric Registration Authority が発行した CBEFF パトロンフォーマット識別子を備えている。(ISO/IEC 19785-2 参照)
（注意） 登録されていないパトロンフォーマットは BIR の相互互換性や伝送が必要な環境においては有用ではないであろう。

3) 単一 CBEFF パトロンフォーマットは，通常一つの与えられた利用領域のみで使用されることを意味しているため，その識別は明確に定義されていないであろう。一つの利用領域において，複数の CBEFF パトロンフォーマットが（おそらく，歴史的な理由により）必要な場合は，それらの識別は，その利用領域内において必要であり必須ではないが，CBEFF パトロンにより発行された識別子を利用するか CBEFF パトロンによる識別方法が使用できる。

4) CBEFF バイオメトリック組織体は BDB フォーマットと SB フォーマットを定義することが出来，これらに識別子を割り付けることが出来る。BDB フォーマット識別子と SB フォーマット識別子は 1～65535 の間の整数値である。各識別子は，CBEFF バイオメオトリック組織体により定義された BDB フォーマットおよび SB フォーマットの中でそれぞれ異なった値でなければならない。このバイオメトリック組織体は，この BDB または SB フォーマットの SB フォーマット・オーナーまたは BDB フォーマットオーナーと呼ばれる。このように BDB フォーマットは「BDB フォーマットオーナー ： BDB フォーマット識別子」の組み合わせにより識別される。そして SB フォーマットは「SB フォーマットオーナ

ー　：　SB フォーマット識別子」の組み合わせで識別される。BDB または SB フォーマット・オーナーは（必須ではないが）ISO/IEC 19875-2 に従って BDB または SB フォーマット識別子を登録することが出来る。

5) CBEFF の最終目標は一つの BIR 内の各 BDB と SB のフォーマットを個々に識別することである。BDB または SB フォーマットオーナーと BDB または SB フォーマット識別子の組み合わせがこの目的のためにさいようされている。

6) もう一つの最終目標は，一つの BIR 内の一つの BDB の生成者に固有な識別子を割り付けて明確に識別できるようにすることである。BDB 製品オーナーと BDB 製品識別子の組みあわせは，パトロンフォーマット内に含まれた場合，この目的のために利用できる。CBEFF バイオメトリック組織体はソフトウェアまたはハードウェア製品にバイオメトリック製品識別子を割り付けることが出来る。この製品は（必須ではないが）この組織体によって生産されたものかまたは仕様を定義されたものである。バイオメトリック製品識別子は，1～65535 の間の整数値であり，CBEFF バイオメトリック組織体により識別子を割付られたバイオメトリック製品の中において明確に識別できる値でなければならない。このバイオメトリック・オーガナイゼーションはその製品のバイオメトリック製品オーナーと呼ばれる。このように，製品は，「バイオメトリック・製品オーナー　：　バイオメトリック製品識別子」の組み合わせにより識別される。バイオメトリック製品オーナーは，ISO/IEC 19785-2 に従ってバイオメトリック製品識別子を登録することが出来る（必須ではない。）

7) CBEFF は本規格書 6.5 節においてオプションとしてのデータ要素を定義している。これはパトロン・フォーマットの符号化には，ある特定の条件化においてのみ含まれる，または決して含まれることがない，または常に含まれるデータ要素が必要であることを意味している。もし，パトロンフォーマットが決して含まれないデータ要素を必要とする場合は，そのパトロンフォーマットには，そのデータ要素の符号化がされないか，論理値が定義されてなく，そのデータ要素への任意の変換において論理値 NO VALUE AVAILABLE が割り付けられる。そのパトロンフォーマットのデータ要素が常にまたは条件付で含まれる場合は，論理値 NO VALUE AVAILABLE に符号を割り付けなければならない。そして CBEFF データ要素の他の論理値はオプションとして定義することができる。”オ

プション“と記述されたデータ要素を含む CBEFF パトロンフォーマットはそのパトロンフォーマットが提供する CBEFF 規定の論理値を数値化することができる。

8) CBEFF パトロンフォーマットの定義において，必須と定義されたデータ要素について，論理値 NO VALUE AVAILABLE が定義されているものはない。

9) CBEFF パトロンフォーマットの仕様において，データ要素の順序に対する要求仕様はない。

10) CBEFF 規格では，全ての情報が暗号化されている環境下を除き，全 SBH が暗号化されていないことを一般要求仕様としている。CBEFF の重要な最終目的の一つとして，生体認証アプリケーションが BDB の内容を確認せずに特定の BDB の処理が必要かどうかを簡単に決定できることである。暗号化されていない SBH において符号化されたデータ要素はこの決定が出来るようにするためのものである。

注） CBEFF 規格においては，アプリケーションが BDB の処理を行なうことを決定するまでは処理されない任意の CBEFF 定義データ要素は暗号化されることを許容する。

11) もし単一 BIR が MAC またはディジタル署名のどちらかを完全性チェックのために利用する場合は, SBH と BDB はこれらが付与されたデータ内に含まれなければならない。複合 BIR の場合は，オプションとして BIR 全体との結合方式を利用することが出来，また複合 BIR 中の個別の単一または複合 BIR に対して使用することも出来る。

12) CBEFF パトロンフォーマット仕様では，一つの BIR 中の BDB は特定の暗号アルゴリズム（SB 内で動的に，またはパトロンフォーマット内にて静的に）を使用して暗号化されていること, また暗号化されていない BDB と，オプションとして任意の（動的または静的な）既知の暗号アルゴリズムを使用したり，特定の暗号アルゴリズムを使用しなければならないと規定されている。

注） 暗号化と完全性を利用するにあたり，暗号と完全性のアルゴリズムを

利用機関の間で決定し，これらのアルゴリズムに関連したパラメータとキーについて合意されたことを定義しなければならない。本国際標準規格は，これらの暗号化と完全性のパラメータに関する合意方法については，予め定義はしないが，CBEFF データ要素（その SB）のために使用する暗号化と完全性のアルゴリズムを提供する。また，その SB の内容とそのフォーマットを識別する CBEFF データ要素も提供する。

13) BDB は８ビットの整数倍であり，それ自身がデータ長を制限しない。

注）BDB のデータ長を決定ずける CBEFF 定義のデータ要素は存在しない。すなわち，これは論理レベル（コード化に依存しない）には関係しない符号化の問題であるからである。

2.4.2.1. CBEFF 単一 BIR 構造による CBEFF パトロンフォーマットの定義

CBEFF 単一 BIR 構造を用いて定義された一つの BIR に対する CBEFF パトロンフォーマットにおいては，CBEFF データ要素に対応するフィールドが単一 SBH の部分に含まれなければならない。(規格書 6.2.1 節参照) SBH の後ろに一つの単一 BDB（任意の標準化されたもの, またはベンダーが定義したもの 一規格書 6.2.2 節参照）のフィールドが続かなければならない。(CBEFF パトロン・フォーマット規定の要求仕様により, BIR の全てのインスタンスまたはいくつかのインスタンスについて)BDB の後ろにはセキュリティ・ブロック（SB） (規格書 6.2.3 節参照)が存在できる。Figure 1 にそのような BIR を示す。BIR の各セクションは次の節にて定義されている。

Figure 1 Simple BIR structure

SBH	BDB	SB (optional)

2.4.2.1.1. 標準バイオメトリック・ヘッダー(SBH)

本節では， CBEFF 単一 BIR 構造を用いて定義された一つの BIR を使用するために，CBEFF パトロンが SBH を定義するための要求仕様を策定している。

1) SBH は CBEFF データ要素の論理値が完全な形で符号化されたものであり,

CBEFF パトロンが定義した追加の論理値(オプション設定)も同時に符号化されたものである。そして BDB と SB のレコード長を規定したものを含まなければならない。

次の CBEFF データ要素は単一 BIR 構造の SBH 内に符号化されていなければならない(必須)

CBEFF_BDB_format _owner (規格書 6.5.1 節参照)
CBEFF_BDB_format_type (規格書 6.5.2 節参照)
CBEFF_BDB_encryption_options (規格書 6.5.3 節参照)
CBEFF_BIR_integrity_options （規格書 6.5.4 参照）

注) 全ての BDB が暗号化されている場合，および全ての BDB が暗号化されていない場合の両者について，パトロンフォーマットは，CBEFF_BDB_encription_options をゼロ・レングス・フィールドとして符号化することを定義できる。同様に，BIR の CBEFF_BIR_integrity_options を定義できる。

2.4.2.1.2. バイオメトリック・データ・ブロック（BDB）

BDB は一つまたは複数のバイオメトリック・サンプルまたはバイオメトリック・テンプレートを含む任意の定義されたフォーマットを持つデータのブロックである。SBH 内で符号化され必須項目となっている CBEFF データ要素 CBEFF_BDB_format_owner （規格書 6.5.1 節参照）と CBEFF_BDB_format_type(規格書 6.5.2 節参照)が BDB のフォーマットを識別する。

注）BDB フォーマットは販売元，標準化団体，業界団体が定義することができる。すなわち，これらの組織体は ISO/IEC 19785-2 に従って CBEFF バイオメトリック組織体識別子（CBEFF_BDB_format_owne r の値を提供する）を得るために登録され，定義された BDB フォーマットとその BDB フォーマット識別子（CBEFF_BDB_format_type の値を示す）を割り付ける

2.4.2.1.3. セキュリティ・ブロック （SB）

CBEFF は一つのセキュリティ・ブロックフォーマット・オーナーにより完全に規定された構造の最上位レベルに SB を定義する。 そしてこのオーナーに対して固有なセキュリティ・ブロックフォーマット識別子を割り付けこの SB を識

別する。

次の論理値が両者共に，または一方のみ利用される場合，CBEFF パトロンフォーマットの仕様として SB の存在が定義されなければならない。

CBEFF_BIR_integrity_options　の論理値　INTEGRITY
CBEFF_BDB_encryption_options の論理値　ENCRYPTION

2.4.2.2. CBEFF 複合 BIR 構造を用いた CBEFF パトロンフォーマットの定義

1) CBEFF パトロンは，一つの BIR 内に同種または異種(例えば，指紋，顔と音声のそれぞれの BDB や複数の指の指紋 BDB)のバイオメトリック・データ・タイプの複数 BDB を備えた CBEFF パトロンフォーマットを定義することが出来る。CBEFF 複合 BIR 構造がその要求仕様を満たしている。Figure 2 は，指の特徴点データと虹彩データを含む CBEFF 複合 BIR 構造を基にしたパトロンフォーマットの例である。

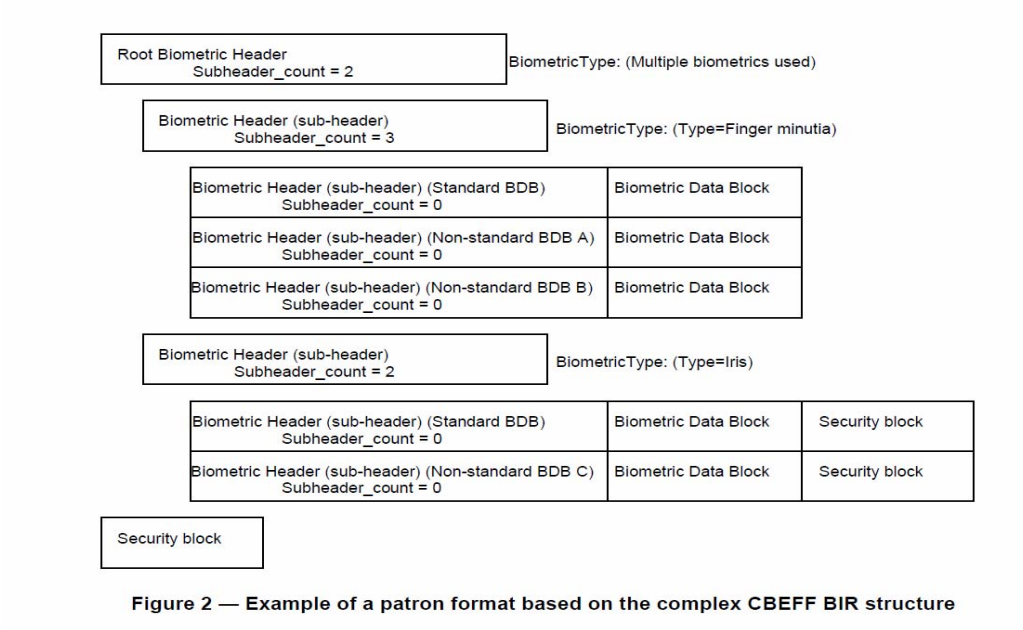


Figure 2 — Example of a patron format based on the complex CBEFF BIR structure

図 2.4.1

2) CBEFF 複合 BIR 構造に基づく CBEFF パトロンフォーマットは次の構成から成る。

a) 最初の CBEFF 単一 SBH (ルート・ヘッダー)
b) この後に次のどちらかが続く
　①一つまたは複数のゼロレベルのサブヘッダー
　②ゼロレベルではない一つまたは複数のサブヘッダー

c) そしてオプションとしてのセキュリティブロック
パトロンフォーマットがこのセキュリティブロックを含む場合，ルートヘッダーは，CBEFF データ要素である CBEFF_BIR_integrity_options の論理値　INTEGRITY をサポートしなければならない。このセキュリティ・ブロックの適用範囲は全複合 BIR である。

注)　規格書 6.3.5 節では，CBEFF データ要素
CBEFF_BIR_encryption_options はルートヘッダーではサポートされないことが要求されている。

3) ゼロレベル・サブヘッダー・ブロックは次の構成となる。

注）　ゼロレベル・サブヘッダー・ブロックは CBEFF 単一 BIR 構造に準拠する。単一 BIR は複合 BIR の一部分であるので，単一 BIR パトロンフォーマットを定義する CBEFF パトロンは，複合 BIR のより上位のレベルの論理値について継承（規格書 6.3.7 節参照）が許容できるかどうかを考慮しなければならない。　もし，いくつかの値の継承が許容出来ない場合は，単一パトロンフォーマットがこれらの値を継承するデータ要素と論理値を提供しなければならない。

a) CBEFF_subheader_count データ要素として符号化された論理値 ZERO を持つ一つの SBH
b) 一つの BDB
c) セキュリティ・ブロック(オプション)

もし，一つのパトロンフォーマットがこのゼロレベルの完全性をサポートするためにこのセキュリティ・ブロックを含む場合，このゼロレベル・ブロックのサブヘッダー（または，ルート・ヘッダーではなくより上位のレベルのサブヘッダー・ブロック）が CBEFF データ要素、CBEFF_BIR_integrity_options の論理値　INTEGRITY をサポートしなければならない。このセキュリティ・ブロックの適用範囲はこの一つのゼロレベル・サブヘッダーのみである。

4) ゼロレベル以外のサブヘッダー・ブロックは次の構成となる。
a) 一つのサブヘッダーの個数（値がゼロでないこと）を含む一つの CBEFF SBH

ｂ）この後に次のどれかが続く
①一つまたは複数のゼロレベル・サブヘッダーブロック
②一つまたは複数のゼロレベル以外のサブヘッダー・ブロック

5) ルートヘッダーとサブヘッダー・ブロックは，データ要素、CBEFF_subheader_count の全論理値について符号化された値をサポートしなければならない。

注）この CBEFF データ要素の論理値は 0 から 255 の間の整数値である。CBEFF 複合 BIR 構造は任意の数のレベルをサポートするが，一つのレベル内におけるサブヘッダー・ブロック（すなわち BDB）の最大個数は 255 である。必要であれば一つのレベルに 255 以上のサブヘッダーが必要なパトロンフォーマットとして，次のより上位のレベルのサブヘッダー・ブロックを新しく続きの個数として定義することができる。

6) 一つの BIR において各 BDB のレベルまたはその上のレベルにおいて，最小として一つの SBH 内に, CBEFF データ要素 CBEFF_BDB_format_owner と CBEFF_BDB_format_type が必須である。もし，一つの BDB 上の SBH の階層構造において、複数のレベルにこれらのデータ要素が含まれる場合は, BDB にもっとも近いレベルの値が BDB に適用される値と解釈されるべきである。

7) CBEFF データ要素 CBEFF_BDB_encryption_options は，各ゼロレベルの SBH 内で符合化されるべきであり，BIR のほかレベルにおける SBH 内で符合化されてはいけない。

注）　この要求仕様は CBEFF の最終目標として，BDB のみの暗号化を許容し，全 SBH の暗号化は行なわないことを強調したものである。

8) ゼロレベル以外の CBEFF サブヘッダーは，CBEFF_subheader_count として，次に続く下位レベルに存在するサブヘッダー・ブロックの個数に相当する論理値を符合化していなければならない。

9) 複合（CBEFF）BIR 構造を使用して定義された CBEFF パトロンフォーマットでは, 次に示す BIR の符号化に関する要求定義を満たさなければならない。

a) デフォルトとして，下位レベルの各データ要素は次の上位レベルの対応するデータ要素の論理値を継承しなければならない。（本規格書 6.3.5 節を参照）
b) 一つのサブヘッダー・ブロックに一つのデータ要素の符合化されたものが存在する場合，その符合化された値はその継承された値が上書きされる。

2.4.2.3. BIR の変換方法について

アプリケーションによって，同じ形式のパトロンフォーマット間または異なるパトロンフォーマット間で, 一つのパトロンフォーマットの BIR（変換元 BIR）から他のパトロンフォーマットの BIR(変換先 BIR)へ変換されることが可能である。このような変換は次に示す方法で実行される。

1) 数値化された論理値の変換方法
数値化された論理値を持つ CBEFF データ要素(必須なものとオプションについて)は，本規格書 6.5 節に示されている異なる要求仕様を例外として，a)，b)で規定されている対応方法に従わなければならない。

注）本規格書 6.5 節では，論理値が変換先 BIR において符合化される方法として，変換元の論理値に依存するのではなく，変換アプリケーションへの局所的な入力により実行される場合（CBEFF では定義されていない）についての別の要求仕様を定義している。

a) 変換元 BIR の論理値が変換先 BIR パトロンフォーマットでサポートされている場合は，その論理値は変換先と変換元の間で対応付けられていなければならない。

b) 変換元 BIR 内の論理値が変換先 BIR パトロンフォーマットによりサポートされない場合，その論理値は変換先 BIR 内の CBEFF データ要素において，論理値 NO VALUE AVAILABLE に対応付けられていなければならない。

2) 数値化されたデータ要素以外の値の変換方法
キャラクター文字列, 8 進数表示文字列, 日付, 少数の論理値を持つ CBEFF データ要素（必須なもの及びオプションについて）に対しては，データ要素の値の対応方法は本規格書 6.5 節においてデータ要素の定義として規定

されている。

2.4.2.4. CBEFF データ要素

本規格書6.5節ではCBEFF定義の各データ要素に対して定義と論理値が規定されている。

注）本規格書 6.5 節内の各小節は，次の順位で記述されている。: 必須データはデータ要素の名前でアルファベット順になっており，次にオプションとなっているデータ要素がその名前のアルファベット順に記載されている。例外は，CBEFF_BDB_biometric_type が CBEFF_BDB_biometric_subtype の前に記述されている。これは, _type と_subtype が情報の階層構造に準拠したものであり，_type を_subtype の前に定義するのがより自然であるためである。

1) CBEFF_BDB_format_owner

・属性

必要性： 必須

論理値： 整数 0 から 65,535 の値

内容： 本データ要素の符号化により，そのコードの付いた SBH に連携した BDB フォーマットを定義した標準化団体, 標準化ワークグループ, 業界団体，またその他の CBEFF バイオメトリック組織体が識別される。 CBEFF 規格により，CBEFF BDB フォーマットを定義する組織は，このデータ要素内にコード化される固有の識別子（ISO/IEC 19785-2 参照）を得るために，Biometirc Registration Authority に登録される。本データ要素の論理値は，この識別子が取りえる全ての値であり全てのパトロンフォーマットをサポートする。

注）CBEFF_BDB_format_owner データ要素内で使用される CBEFF バイオメトリック組織体識別子は，CBEFF_BDB_format_type（6.5.2 節参照）内で使用される BDB フォーマット識別子と共に一つの BDB の特定なフォーマットを明確に識別するために使用される。一つの BDB フォーマットは一つのバイオメトリック組織体により”所有 “される。BDB フォーマット仕様は発行される(公開)場合もあり，発行されない(非公開)場合もありえる。BDB フォーマット識別子は登録することが出来る（必須ではない） （本規格書 6.5.2 節参照）

・変換仕様

変換元 BIR から変換先 BIR への変換において, CBEFF_BDB_format_owner と CBEFF_BDB_format_type は，BDB もまた変換される場合を除きコピーされなければならない。BDB が変換される場合は, 変換先の BIR において, 変換先の BDB フォーマットオーナーとフォーマットタイプが識別されなければならない。

注）BDB フォーマットの変換は実装オプションである。

2) CBEFF_BDB_format_type

・属性

必要性：　必須

論理値：　整数値　0 から 65,535

内容：　本データ要素の符号値により，CBEFF_BDB_format_owner 内に記録されている CBEFF バイオメトリック組織体が定義した特定の BDB フォーマットを識別する。これは，標準化団体または，業界団体のような CBEFF バイオメトリック組織体により登録，発行された標準 BDB フォーマットであるか, 標準化されていない非公開の BDB フォーマットである。BDB フォーマットの登録はオプションである。登録されたか，されないかに関わらず，この識別子は 16 ビットの非負数値であり，CBEFF バイオメトリック組織体識別子により明確に区別される。本データ要素の論理値は本識別子の全ての可能な値の集合でありこれらが全てサポートされなければならない。

・変換仕様

本規格書 6.5.1.2 参照

3) CBEFF_BDB_encryption_options

・属性

必要性：　必須（ただし，6.5.3.2 節参照）

論理値：

NO ENCRYPTION: BDB は暗号化されていない

ENCRYPTION:　BDB は暗号化されている

内容：　本データ要素の符号値は，BDB が暗号化されているか，いないかを定義する。

・パトロンフォーマット仕様に対する要求仕様
次の要求仕様が適用される
CBEFF パトロンフォーマットは最低一つの論理値をサポートしなければならない。

注）パトロンフォーマットがこのデータ要素として一つの論理値のみをサポートする場合は，この論理値をゼロレングス・フィールドとして符号化することが出来る。

パトロンフォーマットが ENCRYPTION をサポートする場合，これらの情報が予めパトロンフォーマット仕様で定義されている場合を除き，CBEFF データ要素である CBEFF_SB_format_owner と CBEFF_SB_format_type がサポートされなければならない。

このデータ要素は使用されない場合，またはどのセキュリティ・オプションが使用されているかを示す他の方法が存在する場合，CBEFF パトロンフォーマットにおいてサポートされる必要はない。

複合 BIR において，このデータ要素はゼロレベルのサブヘッダーにおいてのみサポートされなければならない。

・変換仕様
変換元 BIR から変換先 BIR への変換において，本データ要素の論理値は，BDB の暗号化された状態が変更される場合を除いてコピーされなければならない。BDB の暗号化された状態が変更される場合は，変換先の BIR において変換先の BDB の暗号化状態が符号化されなければならない。もし，変換先 BDB の暗号化状態が ENCRYPTED である場合は，変換先 BIR は本規格書 6.5.3.2 節　b）で定義された要求仕様を満たすパトロンフォーマットに準拠しなければならない。

注）BDB の暗号化状態の変換は実装オプションである。

4) CBEFF_BIR_integrity_options

・属性
必要性：　必須
論理値：

NO　INTEGRITY: 完全性検証は BIR に使用されていない。
INTEGRITY：　BIR に完全性検証が使用されている。
内容：　本データ要素の符号値により，BIR に完全性検証が使用されているか，いないかが定義されている。

・パトロンフォーマット仕様に対する要求仕様
次の要求仕様が適用される。
CBEFF パトロンフォーマットは，最低一つの論理値をサポートしなければならない。

注）　パトロンフォーマットがこのデータ要素として一つの論理値のみをサポートする場合は，この論理値をゼロレングス・フィールドとして符号化することが出来る。

パトロンフォーマットが論理値　INTEGRITY をサポートする場合，このような全ての情報がこのパトロンフォーマット仕様により予め定義されている場合を除き，CBEFF データ要素である CBEFF_SB_format_owner と CBEFF_SB_format_type がサポートされなければならない。

・変換仕様
変換元のパトロンフォーマットを変換先のパトロンフォーマットへ変換する場合，変換先の BIR 内で符号化される本データ要素の論理値として変換先 BIR に適用される完全性検証オプションの値を定義すること。更に変換先 BIR の完全性検証の状態が INTEGRITY の場合，変換先 BIR は本規格書 6.5.4.2 節　b)に記載される要求仕様を満たすパトロンフォーマットに準拠しなければならない。

5) CBEFF_subheader_count

・属性
必要性:　CBEFF 複合 BIR 構造に基づくパトロンフォーマット内の全 SBH 中に必須（規格書 6.3 節参照）
CBEFF 単一 BIR 構造に基づくパトロンフォーマットにおいては存在する場合と存在しない場合がありえる。
論理値：　整数値　0 から　255 の間の値

内容： 本データ要素の符号化により，ルートヘッダーまたはカレントヘッダーの下の次のレベルにおけるサブヘッダーの数を定義する。複合 BIR 構造の最下部のレベル，または単一 BIR 構造において，本データ要素の論理値はゼロでなければならない。

6) CBEFF_BDB_biometric_type

・属性

必要性： オプション

論理値：Table 1 参照

内容： 本データ要素の符合化により， CBEFF 単一 BIR 構造の BDB または複合 BIR 構造におけるゼロレベル・サブヘッダー・ブロックの BDB 内に蓄積された身体的または行動的なデータのタイプを伝送する。

・CBEFF パトロンはこれらの論理値の中から任意のサブセットを利用し、利用領域に応じて追加の論理値を定義することが出来る。これらの追加される論理値は，MULTIPLE BIOMETRIC TYPES が復号化された場合に，個別のタイプを正確に数値化することをサポートするためにこれらの値の任意な組み合わせを含むことができる。ビットマップ表示が可能である。

Table 1 — Abstract values for BDB_biometric_type

Named abstract value	Typically has an associated subtype? (see 6.5.7)
NO VALUE AVAILABLE	No
MULTIPLE BIOMETRIC TYPES	No
Biological type abstract values	
BODY ODOR	No
DNA	No
EAR	Yes
FACE	No
FINGER	Yes
FOOT	Yes
HAND (FINGERS)	Yes
HAND (PALM)	Yes
HAND (VEIN)	Yes
IRIS	Yes
RETINA	Yes
Behavioural type abstract values	
GAIT	No
KEYSTROKE	No
LIP MOVEMENT	No
SIGNATURE/SIGN	No
VOICE	No

図 2.4.2

・変換仕様

本規格書 6.4.1 参照

・もし変換元のパトロンフォーマットが上記論理値本(規格書 6.5.6.1.1 節参照)を結合し多くの追加論理値を表現するためにビットマップを使用しており，変換先のパトロンフォーマットではそのようなビットマップが使用されていない場合は，変換先のパトロンフォーマット中に MULTIPLE BIOMETRIC TYPES 論理値が設定されなければならない。

7) CBEFF_BDB_biometric_subtype

・属性

必要性： オプション

論理値： Table 2 参照

内容： 本データ要素の論理値は，CBEFF_BDB_biometric_type の論

理値に応用される区別子である。

例： もし，パトロンフォーマットが BDB バイオメトリック・タイプとして RETINA をサポートする場合，そのパトロンフォーマットは，BDB バイオメトリック・サブタイプとして論理値 RIGHT と LEFT の使用を指定するであろう。

Table 2 — Abstract values for CBEFF_BDB_biometric_subtype

Abstract values
NO VALUE AVAILABLE
RIGHT
LEFT
LEFT THUMB
LEFT POINTER FINGER
LEFT MIDDLE FINGER
LEFT RING FINGER
LEFT LITTLE FINGER
RIGHT THUMB
RIGHT POINTER FINGER
RIGHT MIDDLE FINGER
RIGHT RING FINGER
RIGHT LITTLE FINGER
NOTE 1 A BDB format specification determines which (if any) of these qualifiers apply to that BDB format.

図 2.4.3

・変換仕様
規格書 6.4.1 参照

8) CBEFF_BDB_challenge_response

・属性
必要性： オプション
論理値：
NO VALUE AVAILABLE
0, 1, またはそれ以外の 8 進数表示の平文データ

内容： 本データ要素の符合化には，BDB 内のバイオメトリック・テンプレートに対して照合を試みるユーザにチャレンジまたはプロンプトを与えるために使用するデータが含まれる。パトロ

ンフォーマット仕様では, 本データ要素の内容がそのパトロンフォーマットで規定され暗号技術による暗号化や関連した SB 内において暗号化されることを許容する。

・もしバイオメトリック・タイプが音声認識に対応した VOICE の場合，本データ要素にはシステムが認証を求めている対象者に発声を促す言葉や, その言葉を含むデータベースへのポインターを保存することができる。本データ要素の値として NO VALUE AVAILABLE 以外の値を含むパトロンフォーマットは，この平文データの内容を定義しなければならない。

・変換仕様

このチャレンジーレスポンス・データ要素（そして，その内容）は BDB の内容として定義することが出来る。変換先のパトロン・フォーマットが NO VALUE AVAILABLE のみをサポートする場合を除いて, 変換アプリケーションは，この内容を変換元 BIR から変換先 BIR へ直接コピーしなければならない。

注）NO VALUE AVAILABLE への変換は BDB を使用不可に変えることがある。

9) CBEFF_BDB_creation_date

・属性

必要性：　オプション

論理値：

NO VALUE AVAILABLE

2000-01-01T00:00:00Z から 3000-12-31T23:59:59Z までの値

内容：　本データ要素は，BDB 内のバイオメトリック・データがキャプチャされた瞬間の UTC 日付と時間（ISO 8601 参照）を定義する。CBEFF は本データ要素に対して，論理値として 1 秒の精度をサポートすることを要求する。

ISO 8601 拡張日付―時間フォーマットが ISO/IEC 19875 の本文の部分において日付―時間データ要素の仕様として用いられている。

UTC は ISO 8601 で定義されているように Coordinated Universal Time の省

略である。

CBEFF は，UTC 日付―時間の瞬間が生成日付として合理的な近時値として解釈することを要請する。

1 秒以外の日付―時間精度を必要とする CBEFF パトロンは, 独自のデータ要素と論理値を定義することが出来る。

パトロン・フォーマット符合化において，日付―時間の論理値として ISO 8601 拡張日付―時間フォーマット以外のフォーマットを使用することができる。(特にバイナリーフォーマットを使用できる)

・変換仕様
規格書 6.4.1 参照

・変換先のパトロンフォーマットが異なった時間単位を用いて論理値を定義している場合，その論理値は CBEFF 定義のものとは異なる。しかし，変換先のパトロンフォーマット仕様として，それが提供する論理値に対し，精度の粗密を調節して変換元の論理値との間に対応表を定義することが出来る。もしこの様な対応表が定義されない場合は，NO VALUE AVAILABLE が対応させられる。

10) CBEFF_BDB_index

・属性
必要性： オプション
論理値：
NO VALUE AVAILABLE
一つの識別子
内容: 本データ要素は BDB に関連した一つのオブジェクトの識別子を運ぶ。しかし, このデータ要素は関連した BDB とは分離されている。パトロンフォーマット仕様によりその論理値がこの中に定義される。もしこのデータ要素が複合 BIR パトロンフォーマット内に含まれるならば, そのフォーマット中においてそのデータ要素の意味を複合構造の異なる階層で定義しなければならない。

注）典型的な例として，このデータ要素には，BDB 内に存在するバイオメト

リック・データの被採取者に一致する一つのデータベース内のレコードのインデックスが保管されている。パトロンフォーマットではこのデータ要素に対し，これと同じ種類の内容を定義することができる。

・変換仕様

CBEFF BIR を変換元パトロンフォーマットから変換先パトロンフォーマットへ変換する時，このデータ要素の符合化された値は変換先の利用領域の状況に一致しなければならない。その値は，変換先パトロンフォーマットの利用領域，変換アプリケーション特有の情報に依存し，NO VALUE AVAILABLE となることもある。

11) CBEFF_BDB_processed_level

・属性

必要性：　オプション

論理値：

NO VALUE AVAILABLE

RAW (本規格書 4.23 節参照)

INTERMEDIATE（本規格書 4.21 節参照）

PROCESSED（本規格書 4.22 節参照）

内容：本データ要素の符合化によりバイオメトリック・サンプルまたは ISO/IEC 19784-1:2006 の BDB 内に保存されたテンプレートの処理状態を保持する。

・変換仕様

変換元パトロンフォーマットフォーマットから変換先パトロンフォーマットへ一つの CBEFF BIR を変換するとき，変換先 BIR 中の論理値は，変換先 BDB の処理レベルを保持しなければならない。もし，変換アプリケーションが BDB に対して何の処理も実行しない場合は，変換先 CBEFF BIR 内のその値は変換元 CBEFF BIR からコピーされるか，コピーされる値がサポートされない場合は，NO VALUE　AVAILABLE でなければならない。

12) CBEFF_BDB_product_owner

・属性

必要性：　オプション　－　本データ要素は，CBEFF_BDB_product_type が同時に含まれる場合を除き，一つのパトロンフォーマットに

含まれてはいけない。（本規格書 6.5.13 節参照）

論理値：

NO VALUE　AVAILABEL

整数値　1 から　65,535

内容：　本データ要素は BDB を生成した製品（すなわち，BSP または変換アプリケーション）を所有する登録されたバイオメトリック組織体を識別する。CBEFF_BDB_product_owner の内容は，一つのバイオメトリック組織体識別子（Biometric Registration Authority により割り付けられた，正の 16 進数）でなければならない。

注 1 オプションである CBEFF_BDB_product_owner データ要素内(存在する場合)の符合化されたバイオメトリック組織体識別子は, 必須データ要素である CBEFF_BDB_format_owner 内に符合化されたものと同じであるかまた異なるものであることが可能である。

注 2 CBEFF は Biometric Registration Authority が全てのバイオメトリック組織体に対してゼロ（16 進数 0000 ）の値を割付ないことを要請している。パトロンフォーマット仕様は，この値を NO VALUE AVAILABＬＥとして使用することが有用であると見なしている。

・変換仕様

変換元パトロンフォーマットから変換先パトロンフォーマットへ一つの CBEFF BIR を変換する場合，もし変換アプリケーションが BDB の内容を変得る場合(例えば，処理レベルを　生データ（RAW）から中間データ（INTERMEDIATE）へ変化させる場合など)，変換アプリケーションが変換先データ要素に NO VALUE AVAILABLE を符号化するように要求されている場合を除き、変換先 BIR 内の CBEFF_BDB_product_owner により変換アプリケーション自身を所有するバイオメトリック組織体が識別されなければならない。もし変換アプリケーションが BDB を修正しない場合は，変換元 BIR の論理値が変換先データ要素に対応させられなければならない。

13) CBEFF_BDB_product_type

・属性

必要性：　オプション　－　このデータ要素は，CBEFF_BDB_product_owner が同時に含まれる場合（本規格書 6.5.12 節参照）を除き，パトロンフォーマットに含ま

れてはいけない。

論理値：

NO VALUE AVAILABLE

1 から　65,535 の間の正数値

内容：　本データ要素は BDB を生成した製品（すなわち，BSP または変換アプリケーション）を識別する。製品識別子はその製品を製作し所有する登録されたバイオメトリック組織体により割付られた正の 16 進数であり，そのバイオメトリック組織体は CBEFF_BDB_owner データ要素により識別される。

・変換仕様

もし変換アプリケーションが CBEFF_BDB_product_owner 内の値を変更する場合，変換先 BIR 内のこのデータ要素は，それ自身，変換アプリケーションを識別するかまたは, NO VALUE AVAILABLE でなければならない。一方変換元 BIR の値は，変換先 BIR へ対応させられるか，NO VALUE AVAILABLE でなければならない。

14) CBEFF_BDB_purpose

・属性

必要性：　オプション

論理値：

NO VALUE AVAILABLE

VERIFY

IDENTITY

ENROLL

ENROLL　FOR VERIFICATION ONLY

ENROLL　FOR IDENTIFICATION ONLY

AUDIT

内容：　本データ要素は BDB の想定された使用方法を識別する。(ISO/IEC 19784-1:2006 の 7.12 節参照)

注）　CBEFF_BDB_purpose そして BioAPI_BIR_PURPOSE は意味的に同等である。

・変換仕様

CBEFF BIR を変換元パトロンフォーマットから変換先パトロンフォーマットへ変換する場合, 変換先 BIR 内の値は変換先 BDB の目的を保持しなけ

ればならない。（例えば，変換アプリケーションは上記の論理的な目的の一つである処理された BDB へ生の BDB を変換処理することができる。） もし変換アプリケーションがそのような処理を実行しない場合は, 変換元 BIR から変換先 BIR 内の値へコピーされるか，変換先 BIR 内でサポートされない場合は，NO VALUE AVAILABLE とならなければならない。

15) CBEFF_BDB_quality

・属性

必要性： オプション

論理値：

NO VALUE AVAILABLE

QUALITY NOT SUPPORTED BY BDB CREATOR

QUALITY SUPPORTED BY BDB CREATOR BUT NOT SET

0 から 100 までの整数の品質値， 100 が最も品質が高いことを表す。

内容： このデータ要素は BDB 内のバイオメトリック・データの品質を規定する。（ISO/IEC 19784-1:2006 第 7 節内の BioAPI_Quality データ構造を参照）

・変換仕様

本規格書 6.4.1 節参照

16) CBEFF_BDB_validity_period

・属性

必要性： オプション

論理値：

NO VALUE AVAILABLE

2000-01-01 から 3000-12-31 までの値

内容： 本データ要素は，BDB の値が正当であると評価できる時間間隔（賞味期間）を含んでいる。本規格書 6.5.9 節と CBEFF 要求仕様に関する注意書き, 時間表示と関連するその他の考慮すべき事項を参照すること。

注 1 二つの時間表示の間の”/”文字は時間間隔の開始時間と終了時間を規定するために使用されている。

注２　1 日以外の日付―時間精度を必要とする CBEFF パトロンは，独自の日付要素と論理値を規定することができる。

注３　パトロンフォーマットの符号化において ISO 8601 拡張日付―時間フォーマット以外のフォーマットを使用することが出来る。（特に 2 進表示のフォーマットを使用出る）

・変換仕様

BDB の正当な使用期限の考慮に関するシステム要求は次の二つのどちらかが発生源となる。

管理上の要求が正当な使用期限を限定する。例えば，一人のユーザーが BDB を認証に利用し成功したとき，ある一つの特権を認可される有効期限を定義することができる。この期限の経過後は，その認証は照合に使用されるバイオメトリック・テンプレートは変えずに次の期限まで更新することができる。またはバイオメトリック・テンプレートの経年変化に関連した技術的な要求により，使用される BDB が照合に対して十分な精度を保てなくなる期限を規定することができる。

本データ要素を含むパトロンフォーマット仕様は，本データ要素が変換先 BIR で使用される時の変換方法を定義しなければならない。

17) CBEFF_BIR_creation_date

・属性

必要性：　オプション

論理値：

NO VALUE AVAILABLE

2000-01-01T00:00:00Z　から　3000-12-31T23:59:59T　までの値

内容：　本データ要素は，BSP または変換アプリケーションにより BIR が生成された瞬間の UTC 日付と時間（ISO 8601 参照）を定義する。CBEFF は，パトロンフォーマット仕様が本データ要素に対して論理値の精度として 1 秒の値を保つように要請している。本規格書 6.5.9 節と時間表示およびそれに関連した考慮事項についての CBEFF の要求仕様の注釈を参照すること。

・変換仕様

変換元パトロンフォーマットから変換先パトロンフォーマットへ CBEFF

BIR を変換する場合，変換先 BIR における本データ要素の論理値は変換先 BIR が生成された日付および時間であるか，NO VALUE AVAILABLE でなければならない。

18) CBEFF_BIR_creator

・属性

必要性：　オプション

論理値：

NO VALUE AVAILABLE

ISO 10646 キャラクタ・セットから選択した文字列を用いた人間が解読可能な名称

注）　実際に使用される BIR 内のこれらの符号化は，そのパトロンフォーマットによって決定される。

内容：　本データ要素は，その人間が解読可能な名称によって、 CBEFF BIR を生成したアプリケーションに対して責務を要する組織を識別する。

例　機械読み取り可能な旅券内のバイオメトリック・データが”US Dep of State” や “Passport Australia”により生成されたものであったりする。

・変換仕様

変換元パトロンフォーマットから変換先パトロンフォーマットへ CBEFF BIR を変換する場合，変換先 BIR 内の本データ要素の論理値は，その変換アプリケーションに対して責務を有する組織を識別するか NO VALUE AVAILABLE でなければならない。

19) CBEF_BIR_index

・属性

必要性：　オプション

論理値：

NO VALUE AVAILABLE

一つの識別子

内容：　本データ要素は，識別する外部の関連付けされた対象が一つの単一 BDB ではなく（本規格書 6.5.10 節参照），全 BIR であることを除き，CBEFF_BDB_index に類似している。

・変換仕様

変換元パトロンフォーマットから変換先パトロンフォーマットへ CBEFF BIR を変換する時，本データ要素の値は，変換先の利用領域の状況に依存する。その値は変換アプリケーションに固有な情報に依存するか，NO VALUE AVAILABLE となる。

20) CBEFF_BIR_patron_format_owner

・属性

必要性： オプション － CBEFF_BIR_patoron_format_type が同時に含まれる場合を除き，本データ要素はパトロンフォーマットに含まれてはいけない。（本規格書 6.5.1 節参照）

論理値：

NO VALUE AVAILABLE

１から 65,535 の間の整数

内容: 本データ要素の符号化は現在考慮中の SBH とは異なる外部分に存在する一つの SBH のパトロンフォーマットに対して、責任をもっている CBEFF パトロンとしての CBEFF バイオメトリック組織体を識別する。CBEFF は，任意の組織体は Biometric Registration Authority に登録され，本データ要素内で符号化される固有識別子を取得しなければならないことを要求する。（ISO/IEC 19785-2 参照） この固有な識別子は 16 進表示の正整数である。本データ要素の論理値はこの識別子の全ての可能な値の集合であり，この全ての値がサポートされなければならない。

注） 一つのパトロンフォーマットがこのデータ要素を使用して自己の識別を行うことはできない。なぜならは，そのフォーマット自身を熟知せずにはそのヘッダーの復号化ができないからである。

21) CBEFF_BIR_patron_type

・属性

必要性： オプション－本データ要素は，CBEFF_BIR_patron_format_owner がパトロンフォーマットに同時に含まれる場合を除き，パトロンフォーマット内に含まれてはいけない。

論理値：

NO VALUE AVAILABLE

1 から 65,535 の間の整数

内容： 本データ要素の符号化により，現在考慮している BIR の外部分に存在する一つの BIR について，CBEFF パトロンフォーマット識別子を定義する。 この参照されたパトロンフォーマットに関して被責務を有する CBEFF パトロンはそのパトロンフォーマット識別子を割り付けし，Biometric Registration Authority へ登録する。この固有な識別子は 16 進表示の正整数である。このデータ要素の論理値はこの識別子の全ての可能な値の集合であり，この全ての値がサポートされなければならない。

・変換仕様

本規格書 6.5.20.2 節参照

22) CBEFF_BIR_payload

・属性

必要性： オプション

論理値：

NO VALUE AVAILABLE

平文 8 進表示の文字列

内容： 本データ要素の符号化には，任意のデータが含まれる。 本データの形式と利用方法は CBEFF では定義されていない。

注） 任意のデータとは，例えば テキスト文字列である；これは暗号化されることが可能である；データ要素内で完全性検証機能を付加することができる；構造を定義することが出来る。CBEFF は本データ要素の符号化について何の制限も付与せず，CBEFF パトロンフォーマット仕様として追加の定義や制限が用意されてはいない。

・変換仕様

CBEFF BIR を変換元パトロンフォーマットから変換先パトロンフォーマットへ変換する場合，変換先 BIR 内にある本データ要素の符号化は変換先 BIR に設定されたパトロンフォーマット仕様に準拠しなければならない;また，この値として NO VALUE AVAILABLE も可能である。

23) CBEFF_BIR_Validity_period

・属性

必要性： オプション

論理値：

NO VALUE AVAILABLE

2000-01-01 から 3000-12-31 までの値

内容： 本データ要素は BIR が正当に使用できる使用期限（この期限の以前，以後は含まず）を伝達する。 本規格書 6.5.9.1 節と CBEFF 仕様として時間表示とそれに関連する考慮事項について記載された注釈を参照のこと。 本規格書 6.5.16 節と使用期限に対する CBEFF 仕様の注釈を参照のこと。

・変換仕様

CBEFF は, このデータ要素が変換先 BIR で使用される場合このデータ要素の変換法則が本データ要素を含むパトロンフォーマット仕様において定義されることを要求する。

注） 本規格書 6.5 節の正当な使用期限の変換に関する考察を参照のこと。 BIR の正当な使用期限については，生体認証技術に基づいた考察，検討は用いられない。

24) CBEFF_patron_header_version

・属性

必要性： オプション

論理値：

NO VALUE AVAILABLE

パトロンフォーマットのバージョンを定めるパトロンフォーマット仕様により定義された論理値

内容： 本データ要素の符号化により，BIR が準拠するパトロンフォーマット仕様の改訂番号（バージョン）が規定されている。

パトロンフォーマット仕様は本データ要素を主要構成子（メジャー）のみでまたは主要構成子と補助構成子（マイナー）により定義することが出来る。(必須ではない)

改訂番号 1（バージョン 1）が存在しない場合，連続的な改訂番号識別子を使用することは出来ない。(そして改訂番号 2（バージョン 2）に符号化されたものは，改訂番号 1 と符号化されたものとほぼ同一のものである） すなわち，改訂番号 1（バージョン 1）と符号化されたものは，改訂番号を決定するために，後続の改訂番号を持つものを復号化出来なければならないからである。

・変換仕様

変換元パトロンフォーマットから変換先パトロンフォーマットへ CBEFF BIR を変換する場合，変換先 BIR 内の論理値は変換先パトロンフォーマット仕様の改訂番号（バージョン）が反映されていなければならない。

25）CBEFF_SB_fromat_owner

・属性

必要性：　オプション　－　本データ要素は CBEFF_SB_format_type が同時に含まれる場合を除き，パトロンフォーマットに含まれてはいけない。（本規格書 6.5.26 参照）

論理値：

NO VALUE AVAILABLE

１から 65,535 の間の値

内容：　本データ要素の符号化により，現在考察している BIR の一部分であるセキュリティ・ブロックフォーマットに関して被責務者である CBEFF バイオメトリック組織体（セキュリティ・ブロックフォーマット・オーナー）を定義する。CBEFF は本データ要素内に符号化された固有な識別子を得るため，Biometric Registration Authority にこれらの組織体が登録されることを要求している。この固有な識別子は 16 進表示の正整数である。本データ要素の論理値は，この識別子の全ての可能な値の集合であり，これらの全ての値がサポートされなければならない。

注）　CBEFF_SB_format_owner で使用される CBEFF バイオメトリック組織体識別子は，CBEFF_SB_format_type で使用される SB フォーマット識別子と共に，一つの SB の特別なフォーマットを明確に識別する。SB のフォーマットは一つのバイオメトリック組織体により“所有”される。SB フォーマット仕様は発行（公開）または非発行（非公開）とすることができる。この識別子は登録することが出来る（必須ではない）（本規格書 6.5.26 節参照）

・変換仕様

変換元パトロンフォーマットから変換先パトロンフォーマットへ CBEFF BIR を変換する場合，変換先 BIR 内の論理値は，変換先 BIR に設定されたパトロンフォーマット仕様に準拠しなければならない；この値として，NO VALUE AVAILABLE を使用することができる。

26) CBEFF_SB_format_type

・属性

必要性：オプション　－　本データ要素は CBEFF_SB_format_owner が同時に含まれる場合を除き，パトロンフォーマットに含まれてはいけない。（本規格書 6.5.25 節参照）

論理値：

NO VALUE AVAILABLE

1 から 65,535 の間の値

内容：　本データ要素の符号化において，現在考慮中の BIR の一部分であるセキュリティブロックのセキュリティブロックフォーマット識別子を指定する。参照したフォーマットに被責務を有するセキュリティブロック・フォーマット・オーナーはセキュリティ・ブロックフォーマット識別子の値を割付けその値を Biometric Registration Authority に登録することが出来る。この固有な識別子は 16 進表示の正整数である。本データ要素の論理値は本識別子の全ての可能な値の集合であり，この全ての値をサポートしなければならない。

27) CBEFF_version

・属性

必要性：　オプション

論理値：

NO VALUE AVAILABLE

主要値は 1 から 15 の間の値であり，補助値が 0 から 15 の間の値である。

内容：　本データ要素の復号化により，CBEFF パトロンフォーマットの仕様において使用される CBEFF の改訂番号（バージョン）を伝達する。国際規格の中で規定された CBEFF の改訂番号（バージョン）の値は，

主要値＝“02”

補助値＝“00”

である。

注）　主要値“01”は CBEFF の非 ISO バージョンとして以前使用されていた。

・変換仕様

変換先 BIR 内における値には，変換先パトロンフォーマットが根拠としている CBEFF の改訂番号（バージョン）が反映されていなければならない。

2.4.2.5. 付録について（これは標準の一部である）
パトロンフォーマット適合性記述文書に関する記述書式と内容

A.1 必須事項

ISO/IEC 19785-1 規格に準拠する一つの CBEFF パトロンフォーマットを発行しようとする登録された CBEFF パトロンは, 公開されたパトロンフォーマット仕様の一部として本規格書付録 A.2 節内で定義されたパトロンフォーマット適合性記述文書（PFCS）が組み込まれていなければならない。

一つの完全な PFCS は, オプションである論理値のどれがサポートされるか, そして追加の論理値がパトロンフォーマットに含まれているかどうか，そして本規格書 6.5.10 節，6.5.16 節，6.5.19.1 節および 6.5.23.2 節それぞれのデータ要素が含まれる場合は，これらの節の要求仕様を満たしているかどうかに関する宣言文が含まれなければならない。

更に，CBEFF 定義値に追加された値として，または CBEFF 定義値の代替値として，このどちらか一方の方式で，非 CBEFF 論理値が定義および規定されているかが記述されていなければならない。

PFCS には多様な利用者があり，以下の利用者を含む：CBEFF パトロンは，ISO/IEC 19785 の本文の部分に対する非適合の失敗を犯す危険性を削減するための監視リストとして利用する。

パトロン仕様の利用者（熱心な利用者）は，パトロンフォーマットの性能機能の詳細記述文書として利用する。

実装を行う利用者（熱心な利用者）は，本パトロンフォーマットと他の異なるパトロンフォーマット間での伝送において発生する可能性がある情報の消失をあらかじめ検証するための基礎資料として利用する。異なる値の論理値をサポートするパトロンフォーマット間での伝送においては情報の消失は避けられないが，非互換なパトロンフォーマットの PFCS により，そのような消失を通常予測することが出来る。

プロトコル試験者は，一つのパトロンフォーマットを生成したり処理すると称する実装機器の、適合度合いを検証できる適当な試験環境を選択する基礎と

して利用する。

A. 2 パトロンフォーマット適合性記述文書の構成要素

一つの PFCS は次に示す小節に規定した構成要素により組み立てられねばならない。

A. 2. 1識別情報

次に示す形式の表により，問題とするパトロンフォーマット仕様が要求された識別情報を含み適合性を表現する PFCS 仕様を満たしていることが表現できる。(本規格書 2.1 節参照) イタリック体表記の部分には，CBEFF パトロンにより提供されべき情報が記載されている。

図 2.4.4

Required Information	Patron format reference
i) Patron name	*See [corresponding clause]*
ii) Patron identifier (decimal & hex)	*See [corresponding clause]*
iii) Patron format name	*See [corresponding clause]*
iv) Patron format identifier (decimal & hex)	*See [corresponding clause]*
v) Patron format ASN.1 object identifier	*See [corresponding clause]*
vi) Domain of use description	*See [corresponding clause]*
vii) Patron format version	*See [corresponding clause]*
viii) CBEFF version	*See [corresponding clause]*
ix) Supported CBEFF-defined data elements and abstract values	*See [corresponding clause]*
x) Patron defined data elements and abstract values	*See [corresponding clause]*

A. 2. 2 CBEFF 定義のデータ要素と論理値

次に示す形式の表は，CBEFF 定義のデータ要素に関する情報を提供することによりＰＦＣＳ要求仕様を満たしている。イタリック体表記の部分には，CBEFF パトロンにより提供されべき情報が記載されている。この例の中で，”Yes”または“No”および“No”または “NA”を含む部分は，CBEFF 準拠パトロンフォーマットに対する PFCS の対応部分には “Yes”または “NA”が含まれなければならない。

CBEFF data element name	Mandatory/ optional	Patron format field name	Abstract values specified?	Encodings specified?
CBEFF_BDB_format_owner	Mandatory	*Name of equivalent field*	*Yes or No*	*Yes or No*
CBEFF_BDB_format_type	Mandatory	*Name of equivalent field*	*Yes or No*	*Yes or No*
CBEFF_BDB_encryption_options	Mandatory	*Name of equivalent field*	*Yes or No*	*Yes or No*
CBEFF_BIR_integrity_optons	Mandatory	*Name of equivalent field*	*Yes or No*	*Yes or No*
CBEFF_BDB_index	*Mandatory/ optional/ absent*	*Name of equivalent field*	(Abstract values and semantics specified as required by 6.5.10?) *Yes or No or NA*	*Yes or No*
CBEFF_BDB_validity_period	*Mandatory/ optional/ absent*	*Name of equivalent field*	(Abstract values and semantics specified as required by 6.5.16?) *Yes or No or NA*	*Yes or No*
CBEFF_BIR_index	*Mandatory/ optional/ absent*	*Name of equivalent field*	(Abstract values and semantics specified as required by 6.5.19?) *Yes or No or NA*	*Yes or No*
CBEFF_BIR_validity_period	*Mandatory/ optional/ absent*	*Name of equivalent field*	(Abstract values and semantics specified as required by 6.5.23?) *Yes or No or NA*	*Yes or No*
CBEFF optional data element that is mandatory in the patron format	Mandatory	*Name of equivalent field*	*Yes or No*	*Yes or No*
CBEFF optional data element that is optional in the patron format	Optional	*Name of equivalent field*	*Yes or No*	*Yes or No*
etc.				

図 2.4.5

A. 2. 3 パトロン定義のデータ要素と論理値

次に示す形式の表は，パトロンにより定義されたデータ要素に関する情報を用意することにより PFCS 要求仕様を満たしている。この例において “Yes or No” を含む部分は，CBEFF 準拠パトロンフォーマットに対する適合性記述文の中では全て“Yes”でなければならない

Patron format data element name	Mandatory/ optional	Patron format field name	Abstract values specified?	Encodings specified?
Data element 1	*Mandatory or Optional*	*Name of equivalent field*	*Yes or No*	*Yes or No*
Data element 2	*Mandatory or Optional*	*Name of equivalent field*	*Yes or No*	*Yes or No*
etc.				

図 2.4.6

2.5. ISO/IEC FCD 19785-3:2006

2.5.1. ー第三部パトロンフォーマット仕様

本標準は未だ国際規格として成立しておらず、国際規格草案の段階であるため、ISO/IEC JTC1/SC37/N1713 文書の内容をまとめたものである。この規格草案文書は ISO/IEC19785 国際規格の中で、想定される様々な利用領域において一般的な使用が想定できるいくつかのパトロンフォーマットを定義している。この文書の中で定義されているパトロンフォーマット仕様は以下の 7 種類である。

(1)ビットオリエンテッド単一最小パトロンフォーマット
(2)バイトオリエンテッド単一最小パトロンフォーマット
(3)バイトオリエンテッド固定長フィールドビットマップ内在パトロンフォーマット
(4)ビットオリエンテッド固定長フィールドビットマップ内在パトロンフォーマット
(5)トークンおよびスマートカード用 TLV 符合化パトロンフォーマット
(6)複合パトロンフォーマット
(7)XML パトロンフォーマット

ここでは、これらの中から(5)の「トークンおよびスマートカード用 TLV 符合化パトロンフォーマット」について説明する。

2.5.1.1. パトロンフォーマット仕様:
トークンおよびスマートカード用 TLV 符号化パトロンフォーマット

2.5.1.1.1. 本フォーマットの識別情報

(1) パトロン名称：
ISO/IEC JTC1/SC37
(2) パトロン識別子：
257 (0101Hex)
これは、ISO/IEC19785-2 で定義された Biometric Registration Authority により割付けられている。
(3)パトロンフォーマット名称
ISO/IEC JTC 1/SC37 TLV-encorded patron format, for use with smartcards or other token
(4) パトロンフォーマット識別子
5 (0005 Hex)
これは ISO/IEC 19785-2 に従い登録されている。
(5) 本パトロンフォーマットに対する ASN.1 オブジェクト識別子
{iso registration-authority cbeff(19785) biometric-organization(0) jtc-sc37(257) patron format(1) tlv-encorded(5)}
または、XML 値表記法により
1.1.19785.0.257.1.5
(6)バージョン識別子
本仕様のパトロンフォーマットは次のバージョン識別子を持っている
主要番号(1) 補助番号 91)

(7)CBEFF バージョン

本仕様は CBEFF バージョン(主要番号　２、補助番号 0)に準拠している。

2.5.1.1.2. 利用領域

想定する利用領域は、バイオメトリクスとトークンを利用する全てのアプリケーションである。特に主要な利用領域は、ISO/IEC 7816 で規定されているスマートカードであり、このパトロンフォーマットはカード内照合とカード外照合の両方式への応用を考慮している。また、生体認証と連結したラジオ周波数帯域の電波を使用した認証タグやバーコードの様なあらゆるトークンの使用にこのパトロンフォーマットを応用することができる。

2.5.1.1.3. 一般仕様

(1)本規格草案文書(以後、本文と省略する)では、“ISO/IEC JTC1/SC37 トークンまたはスマートカード用 TLV 符号化パトロンフォーマット”と命名された CBEFF パトロンフォーマットの仕様を規定している。

(2)あらゆる TLV 符号化アプリケーションで使用される多くの CBEFF データ要素について１つの TLV 符号化を規定している。本文で規定されている特別な形式の TLV 符号化は ASN.1Basic Encoding Rule(ISO/IEC 8825-1 参照)により実現されている。

(3)ISO/IEC 7816-4 および　ISO/IEC7816-11 が必要な交換仕様として定義したもの

a) カード内照合

1) 外部における生体認証処理の実行に先立つスマートカードまたは他のトークンからの情報の検索
2) スマートカード上での生体認証の実行に対するコマンド
3) 登録の方式（スマートカードまたは他のトークン内に於ける情報の記憶方式)
4) スマートカードと外部システム間における信頼チャネル生成に対するセキュリティ機能

b)　カード外照合

- サービスを提供するシステム（例えば、入出国管理システム）で使用されるスマートカードから生体認証に関連したデータを読み出すためのコマンド
- 生体認証に関連したデータのセキュリティ機能

(4)　本 CBEFF パトロンフォーマットは ASN.1Distinguished Encoding Rules（ISO/IEC 8825-1 参照）を使用して ASN.1 タイプ BiometricInformationTemplate と定義されている。また、本パトロンフォーマットに対して表形式の定義も与えられている。(本文 11.11 節参照)

(5)　用語 Biometric Information template は、ISO/IEC 7816-11 で省略記号

BIT が使用されている。この用語および省略記号は、バイオメトリック情報レコード及びBIR と同義語であり本規格書内においてはISO/IEC7816-11 との関係が重要な場合に使用されている。

(6) ASN.1 Basic Encoding Rules を使用して符号化されたASN.1 タイプのBiometricHeaderTemplate の構成要素もまたISO/IEC 7816-11 において使用するために定義されている。

(7) ISO/IEC 7816-11 では、用語Biometric Header Template は省略記号BHT と共に使用されており、これらは、標準バイオメトリックヘッダーおよびその省略記号SBH と同義語であり ISO/IEC 7816-11 との関連性が重要な場合に本規格書内で使用されている。

(8) 用語Biometric Information Data Object（バイオメトリック情報データオブジェクト）が ISO/IEC 7816-11 で特定のASN.1 タイプのTLV 符号化を参照するために使用されている。これは本文Table 11,1 に記載されており定義は本文11.10 節に記載されている。

表 2. 5. 1

Table 11.1 – Biometric Information Data Objects with the Biometric Header Template Data Objects defined in 11.10

Biometric Information Data Object	ASN.1 type or component name (see 11.10)	Tag (hex)
Biometric Information Template	BiometricInformationTemplate	'7F60'
Group BIT	GroupBIT	'7F61'
BDB Reference Data	bdbReferenceData	'5F2E' or '7F2E'
BIR Payload	birPayLoad	'53' or '73'
BIR Security Block	securityBlock	'7F3D'
For use only in Biometric Information Template:		
Biometric Header Template	biometricHeaderTemplate	'A1'
Algorithm Reference	algorithmReference	'80'
Reference Data Qualifier	referenceDataQualifier	'83'
For use only in Biometric Header Template:		
Patron Header Version	patronHeaderVersion	'80'
BDB Biometric Type	bdbBiometricType	'81'
BDB Biometric Subtype	bdbBiometricSubType	'82'
BDB Creation Date	bdbCreationDate	'83'
BIR Creator	birCreator	'84'
BDB Validity Period	bdbValidityPeriod	'85'
BDB PID	bdbPID	'86'
BDB Format Owner	bdbFormatOwner	'87'
BDB Format Type	bdbFormatType	'88'
BIR Index	birIndex	'90'
Matching Algorithm Parameters	matchingAlgParameters	'91' or 'B1'
Security Options	securityOptions	'92'

(9) CBEFF 準拠であるためには、本パトロンフォーマットが完全にサポートしないデータ要素に対しては、論理値として NO VALUE AVAILABLE が与えられていなければならない。また、この要求仕様を満たすために、バイオメトリック・ヘッダー・テンプレート内に存在するデータオブジェクトに対してタグが本文 Table 11.2 に示される様に、予約され割り付けられていなければならない。これらのタグの値が、任意のタグ割当当局によってバイオメトリック・ヘッダー・テンプレート内に現れるデータオブジェクトに割り付けられることはできない。これらのデータオブジェクトは本パトロンフォーマットの本バージョンにおける符号化では使用してはいけない。そしてこれらを除外するためには、関連した CBEFF データ要素の論理値として NO VALUE AVAILABLE が表示されていなければならない。

表 2.5.2

Table 11.2 – Reserved tag values

ASN.1 tag value	Tag (hex) value	Corresponding CBEFF data element
[19]	'93'	CBEFF_BDB_challenge_response
[20]	'94'	CBEFF_BDB_index
[21]	'95'	CBEFF_BDB_processed_level
[22]	'96'	CBEFF_BDB_purpose
[23]	'97'	CBEFF_BDB_quality
[24]	'98'	CBEFF_BIR_creation_date
[25]	'99'	CBEFF_BIR_patron_format_owner
[26]	'9A'	CBEFF_BIR_patron_format_type
[27]	'9B'	CBEFF_BIR_validity_period
[28]	'9C'	CBEFF_version

2.5.1.1.4. ASN.1 仕様

```
CBEFF-SMARTCARD-BIDO
-- The abbreviation BIDO is used for Biometric Information Data Object
{iso standard 19785 part(1) modules(0) types-for-smartcard(8)}
DEFINITIONS
IMPLICIT TAGS ::=

BEGIN

-- In all cases, omission of an optional component that represents a
-- CBEFF data element is the encoding of the NO VALUE AVAILABLE for
-- that data element.

PatronHeaderVersion  ::= OCTET STRING (SIZE(2))
      -- CBEFF_patron_header_version
      -- The first octet encodes the major version number
      -- The second octet encodes the minor version number

BiometricType        ::= OCTET STRING (SIZE(1..3))
      -- CBEFF_BDB_biometric_type

      -- The encoding of the abstract values in the value part of the
      -- TLV shall be the Recommended Encodings specified in Table 11.5.
      -- Note that this is different from the encoding of this type in
      -- Table A.1 and in other patron formats specified in this part of
      -- ISO/IEC 19785.

BiometricSubType     ::= OCTET STRING (SIZE(1))
      -- CBEFF_BDB_biometric_subtype
      -- The encoding of the abstract values in the value part of the
      -- TLV shall be the Recommended Encodings specified in Table 11.6.
      -- Note that this is different from the encoding of this type in
```

```
      -- Table A.2 and in other patron formats specified in this part of
      -- ISO/IEC 19785.

BCDTime               ::= OCTET STRING (SIZE(7))
      -- BCD encoded timestamp with format ' YYYYMMDDHHMMSS'

Creator               ::= UTF8String
      -- CBEFF_BIR_creator

BCDDate               ::= OCTET STRING (SIZE(4))
      -- BCD encoded date with format 'YYYYMMDD'

BCDDatePeriod ::= OCTET STRING (SIZE(8))
      -- Two concatenated BCD encoded dates with format YYYYMMDDYYYYMMDD

ProductID             ::= OCTET STRING (SIZE(4))
      -- CBEFF_BDB_product_owner in the first two octets
      -- CBEFF_BDB_product_type in the last two octets

FormatOwner           ::= OCTET STRING (SIZE(2))
      -- CBEFF_BDB_format_owner

FormatType            ::= OCTET STRING (SIZE(2))
      -- CBEFF_BDB_format_type

BIRIndex              ::= OCTET STRING
      -- CBEFF_BIR_index

CombinedSecurityOptions ::= OCTET STRING (SIZE(2))
      -- Both CBEFF_BDB_encryption_options and
      -- CBEFF_BIR_integrity_options
      -- The first octet encodes NO ENCRYPTION as zero
      -- and ENCRYPTION as 1.
      -- The second octet encodes NO INTEGRITY as zero
      -- and INTEGRITY as 1.

BiometricInformationTemplate ::= [APPLICATION 96] SET {
      algorithmReference       [0] OCTET STRING (SIZE(1)) OPTIONAL,
      -- A non-CBEFF data element - see ISO/IEC 7816-11
      referenceDataQualifier   [3] OCTET STRING (SIZE(1)) OPTIONAL,
      -- A non-CBEFF data element - see ISO/IEC 7816-11
      biometricHeaderTemplate  [1] BiometricHeaderTemplate,
      bdbReferenceData     [APPLICATION 46] OCTET STRING OPTIONAL,
      -- A CBEFF BDB, mandatory for off-card-matching
      birPayLoad           [APPLICATION 19] OCTET STRING OPTIONAL,
      -- CBEFF_BIR_payload, contents defined by ISO/IEC 7816-11
      securityBlock        [APPLICATION 61] OCTET STRING OPTIONAL
      -- A CBEFF security block, structure and contents defined by ISO/IEC 7816-11
      }

GroupBIT ::= [APPLICATION 97] SET OF BiometricInformationTemplate

BiometricHeaderTemplate ::= SET {
      patronHeaderVersion      [0]  PatronHeaderVersion
                                    DEFAULT'0101'H,
      -- The absence of this Data Object represents NO VALUE AVAILABLE
      bdbBiometricType         [1]  BiometricType OPTIONAL,
      bdbBiometricSubType      [2]  BiometricSubType OPTIONAL,
      -- Required to be absent unless bdbBiometricType is present
      bdbCreationDate          [3]  BCDTime OPTIONAL,
      -- CBEFF_BDB_creation_date
      birCreator               [4]  Creator OPTIONAL,
      bdbValidityPeriod        [5]  BCDDatePeriod OPTIONAL,
      bdbPID                   [6]  ProductID OPTIONAL,
      bdbFormatOwner           [7]  FormatOwner,
      bdbFormatType            [8]  FormatType,
      birIndex                 [16] BIRIndex OPTIONAL,
      matchingAlgParameters    [17] OCTET STRING OPTIONAL,
      -- A non-CBEFF data element - see ISO/IEC 7816-11
      securityOptions          [18] CombinedSecurityOptions OPTIONAL
      }
       END
```

2.5.1.1.5. カード内照合で使用されるバイオメトリック情報テンプレート

(1)　カード内照合で使用されるバイオメトリック情報テンプレート（BIT）が本文 Table 11.3 に記述されている。BIT は次の下部構造を備えている。

a)　ISO/IEC 7816-11 で定義されたデータオブジェクト(16 進表示タグ‘80’、’83’の付いたもの)
これは ISO/IEC 7815-4 で定義された生体認証に使用される産業間共通コマンドに関連した値を含む

b)　ISO/IEC 7816-11 で定義された’A1’タグ付のバイオメトリック・ヘッダー・テンプレート(BIT)
BHT 内で入れ子になったデータオブジェクトのタグ割付当局は ISO/IEC JTC 1/SC37 である。(デフォルトのタグ割付当局)

注）このタグ割付当局に対する ASN.1 オブジェクト識別子は
{iso standard 19785 part(3) tag-allocation(1) clause-11(0) }
である。

c) カード内照合に関連した CBEFF データ要素に対するデータオブジェクト

d) カード内照合に固有なバイオメトリックデータオブジェクト
このデータオブジェクトは１６進表示タグ’91’または’B1’が付けられたバイオメトリック照合アルゴリズムパラメータと定義されている。

(2) Table 11.3 に示された BIT の使用方法、すなわち BIT は利用者の生体認証が実行される前に読み取られること、企業間共通コマンドにより実行される生体認証処理について、そしてセキュリティに関する要求仕様は ISO/IEC 7816-11 で規定されている。

表 2.5.3 カード内照合のために使用されるバイオメトリック情報テンプレート

タグ	長さ	値					有無
‘7F60’	可変長	バイオメトリック情報テンプレート(BIT)					
		タグ	長さ	値			
		‘80’	1	ISO/IEC 7814-4 で定義された VERIFY / EXT.AUTHENTICATE / MANAGE SE コマンドで使用するためのアルゴリズム参照			任意
		‘83’	1	ISO/IEC 7814-4 で定義された VERIFY / EXT.AUTHENTICATE / MANAGE SE コマンドで使用するための参照データ修飾子			任意
		‘A1’	可変長	バイオメトリックヘッダーテンプレート(BIT) タグ割付当局:ISO/IEC JTC 1/SC37			必須
				タグ	長さ	値	
				‘80’	2	CBEFF_patron_header_version （デフォルト値 ‘0101’）	必須 （存在しない場合はデフォルト値を用いる）
				‘90’	可変長	CBEFF_BIR_index カード外のアプリケーションの状況において、このバイオメトリックデータセットを参照するために使用する一意の識別子	任意
				‘81’	1-3	CBEFF_BDB_biometric_subtype Table 11.5 参照	任意

タグ	長さ	値					有無
		タグ	長さ	値			
				タグ	長さ	値	
				‘82’	1	CBEFF_BDB_biometric_subtype Table 11.6 参照	任意 バイオメトリックタイプと共にのみ使用
				‘83’	7	CBEFF_BDB_creation_date バイオメトリック参照データの生成日時;14 桁 BCD （YYYYMMDDHHMMSS）	任意
				‘84’	可変長	CBEFF_BIR_creator	任意
				‘85’	8	CBEFF_BDB_validity_period 有効期間　2組の日付:１６桁 BCD （YYYYMMDDYYYYMMDD）	任意
				‘86’	4	CBEFF_BDB_product_owner CBEFF_BDB_product_type 製品オーナーと製品タイプの結合体で、バイオメトリック参照データを生成した製品を識別する	任意
				’87’	2	CBEFF_BDB_format_owner バイオメトリック照合データのフォーマットオーナーでこの値は Biometircs Registration Authority が割付けたものである。	必須
				‘88’	2	CBEFF_BDB_format_type フォーマットオーナーにより規定されたバイオメトリック照合データのフォーマットタイプ	必須
				‘91’/ ’B1’	可変長	バイオメトリックマッチングアルゴリズムパラメータ(基本型/構造型) 注記4参照	任意

注記 1 本表には、19785-1 で定義されたバイオメトリックデータブロックは存在せす、バイオメトリック参照データは、この BIT 内ではなく IC カード内に別々に記録される。バイオメトリック照合データ（データオブジェクト中でタグ’87’と’88‘が付けられたフォーマットオーナーとフォーマットタイプ）が、例えば ISO/IEC 7816 VERIFY コマンドを使用してカードに提供されなければならない。

注記 2 本表には、ペイロードは存在しない。アプリケーションが利用する場合、バイオメトリック照合の成功完了後にペイロードへのアクセスが通常許可される。ペイロードは、GETDATA または READ BINARY のような ISO/IEC7816 定義の産業間共通アクセスコマンドを用いて読み出すことができる。

注記 3 ICカードの外界においては、照合データに必要な構造を確認するためにフォーマットオーナー/フォーマットタイプを使用する。カード内のマッチングアルゴリズムは、フォーマットオーナー/フォーマットタイプに従って照合データの処理を実行でき、アルゴリズム参照データオブジェクトが存在する場合は、アルゴリズム参照により指定される。

注記 4 バイオメトリックマッチングアルゴリズムデータオブジェクトは、IC カード内に実装されたマッチングアルゴリズムのあらゆる特別なパラメータ、例えば、バイオメトリック照合データ内において想定されるマニューシャの最大数などを提供する。このデータオブジェクトは BDB フォーマットオーナーにより定義される。(ISO/IEC 19794-2 参照)

2.5.1.1.6. カード外照合に使用されるバイオメトリック情報テンプレート

カード外照合に使用されるバイオメトリック情報テンプレート BIT が本文 Table11.4 に示されている。

Table 11.4 に示されたデータ構造は、スマートカード以外に、磁気カード、光メモリーカード、2 次元バーコード等の他の方式のカードで使用できる。BIT は次に示す下部構造を備えている。

(ア)　　ISO/IEC7816-11 で定義されたタグ’A1’が付いたバイオメトリックヘッダーテンプレート

BHT に入れ子になっているデータオブジェクトに対するタグ割付当局は ISO/IEC JTC1/SC37（デフォルトとしてのタグ割付当局）である。

注記　－　このタグ割付当局に対する ASN.1 オブジェクト識別子は以下に示す。

{iso standard 19785 part(3) tag-allocation(1) clause-11(0)}

(イ)　　カード外照合に関連した CBEFF データ要素に対するバイオメトリックデータオブジェクト

(ウ)　　ISO/IEC7816-11 で定義されたタグが付いたバイオメトリック参照データオブジェクト（基本型/構造型）；これは、CBEFF バイオメトリックデータブロック(BDB)を表す。

ｄ）ペイロード

これは､ISO/IEC7816-6 においてタグ’53’又は’73’が付けられオプションとしてデータオブジェクトの内容として定義されている。

（エ）データセキュリティのためのセキュリティブロック（Ｔａｂｌｅ 11.4 の注記 1 参照）

表 2.5.4 カード外照合に使用されるバイオメトリック情報テンプレート

タグ	長さ	値					有無
‘7F60’	可変長	バイオメトリック情報テンプレート(BIT)					
		タグ	長さ	値			
		‘A1’	可変長	バイオメトリックヘッダーテンプレート(BIT) タグ割付当局:ISO/IEC JTC 1/SC37			必須
				タグ	長さ	値	
				‘92’	2	CBEFF_BDB_encryption_options CBEFF_BIR_integrity_options 最初の8ビットでの符号化 ‘00’: NO ENCRYPTION ‘01’: ENCRYPTION 2 番目の8ビットでの符号化 ‘00’: NO INTEGRITY ‘01’: INTEGRITY	任意（オプション）
				‘80’	2	CBEFF_patron_header_version （デフォルト値:’0101’）	必須（存在しない場合は、デフォルト値を用いる）
				‘81’	1-3	CBEFF_BDB_biometric_type Table 11.5 参照	任意
				‘82’	1	CBEFF_BDBD_biometric_subtype Table 11.6 参照	任意 biometric type と共にのみ使用
				‘83’	7	CBEFF_BDB_creation_date バイオメトリック参照データの生成日時 14 桁 BCD:(YYYYMMDDHHMMSS)	任意
				‘84’	可変長	CBEFF_BIR_creator	任意
				‘85’	8	CBEFF_BDB_validity_period 2 組の日付(有効期間):16 桁 BCD (YYYYMMDDYYYYMMDD)	任意
				‘86’	4	CBEFF_BDB-product_owner CBEFF_BDB_product_type 製品オーナーと製品タイプの連結体 バイオメトリック参照データを生成した製品を識別する	任意
				‘87’	2	CBEFF_BDB_format _owner バイオメトリック参照データのフォーマットオーナー この値は Biometrics Registration Authority により割付けられる	必須
				‘88’	2	CBEFF_BDB_format_type バイオメトリック参照データのフォーマットタイプ この値は Biometrics Registration Authority により割付けられる	必須

タグ	長さ	値					有無
				‘90’	可変長	CBEFF_BIR_index カード外部におけるアプリケーションの環境においてこのバイオメトリックデータセットを参照するために使用する一意の識別子	任意
						カード	
				‘5F2E’/‘7F2E’	可変長	CBEFF_BDB バイオメトリック参照データ(基本型または構造型)； 注記 3 参照	必須
				‘53’/’73’	可変長	CBEFF_BIR_payload ペイロードのための任意データ(基本型または構造型)	任意
				‘5F3D’/’7F3D’	可変長	CBEFF セキュリティブロック データセキュリティのためのセキュリティブロック(基本型おまたは構造型) 注記 1、2 参照	条件付

注記 1　署名と MAC に関するフィールドの装備や、暗号化と完全性に関する指針として本規格が提供するセキュリティ機能は、ISO/IEC7816-11 で定義されたセキュアメッセージングテンプレートを使用することにより、より柔軟で高機能な方法が提供されている。

注記 2　署名と MAC は、署名ブロックデータオブジェクトの前に位置する BHT のタグ”A1”で始まり、そのデータオブジェクトの最後のバイト部分で終了する全てのバイト部分をカバーしている。

注記 3　バイオメトリック参照データの構造を構築する場合、利用者に実行をうながすために生体認証技術を用いたチャレンジ機能を統合したり、標準化されたバイオメトリックデータと固有構造のものとを結合することが可能である。これらの個々のデータオブジェクトは ISO/IEC 7816-11 で規定されている。

2.5.1.1.7. BIT グループデータオブジェクト

複数の BIT を BIT グループ内に入れ子にすることが出来る。(タグ’7F61”これは ISO/IEC7816-11 で定義されている。) カード内照合とカード外照合の両者に対する BIT グループ・データオブジェクトの構築と使用については ISO/IEC7816-11 に規定されている。

2.5.1.1.8. バイオメトリック・タイプおよびサブタイプの符号化と論理値

規格草案に Table 11.5 および Table 11.6 が掲載されている。

Table 11.5 CBEFF_BDB_biomtric_type の論理値と符号化

論理値の名称	値の符号化	サブタイプの利用
NO VALUE AVAILABLE	‘00 00 00’	
複数のバイオメトリックタイプ	’80 00 00’	
身体的なバイオメトリックタイプ		
身体の匂い	’40 00 00’	
DNA	’20 00 00’	X
耳	’10 00 00’	
顔	’08 00 00’	
指	’04 00 00’	X
足	’02 00 00’	X
手(複数指)	’00 80 00’	X
手(手のひら)	’00 40 00’	X
‘手(静脈)	’00 20 00’	X
虹彩	’00 10 00’	X
網膜	’00 02 00’	
行動的なバイオメトリックタイプ		
歩き方	’00 01 00’	
キーストローク	’00 00 80’	
口唇の動き	’00 00 40’	
署名	’00 00 20’	
音声	’00 00 10’	
注記 歴史的な理由により次の値が予約されている:’01 00 00”(手形)、’00 04 00’(顔の熱画像)、’00 08 00’(手の熱画像)		

Table 11.6 CBEFF_BDB_biometric_subtype の論理値と符号化

b8	b7	b6	b5	b4	b3	b2	b1	バイオメトリックサブタイプ
0	0	0	0	0	0	0	0	情報無し
						0	1	右
						1	0	左
			0	0	0			意味無し
			0	0	1			親指
			0	1	0			人差し指
			0	1	1			中指
			1	0	0			薬指
			1	0	1			小指
X	X	X						将来のために予約されている
注記　このオプションとしてのフィールドはバイオメトリックタイプのどのサンプルが存在するかを指定する。 （例　右人差し指） このフィールドは、Table 11.5 に示された CBEFF_BDB_biometric_type と共にのみ使用する。								

2.5.1.1.9. CBEFF 定義のデータ要素と論理値

CBEFF データ要素名	必 須 / 任意	パトロンフォーマットフィールド名	論理値の定義	符号化の定義
CBEFF_patron_header_verison	必須	CBEFF_patoron_header_version	有	有
CBEFF_BIR_index	任意	CBEFF_BIR_index	有	有
CBEFF_BDB_biometric_type	任意	CBEFF_BDB_biometric_type	有	有
CBEFF_BDB_biometric_subtype	任意	CBEFF_BDB_biometirc_subtype	有	有
CBEFF_BDB_creation_date	任意	CBEFF_BDB_creation_date	有	有
CBEFF_BDB_creator	任意	CBEFF_BDB_ceator	有	有
CBEFF_BDB_validity_period	任意	CBEFF_BDB_valid_period	有	有
CBEFF_BDB_product_owner	任意	CBEFF_BDB_poduct_owner	有	有
CBEFF_BDB_product_type	任意	CBEFF_BDB_product_type	有	有
CBEFF_BDB_format_owner	必須	CBEFF_BDB_format_owner	有	有
CBEFF_BDB_format_type	必須	CBEFF_BDB_format_type	有	有
CBEFF_BIR_payload	任意	CBEFF_BIR_payload	有	有
CBEFF_BDB_encryption_options	注記参照	Zero length encoding	注記参照	注記参照
CBEFF_BIR_integrity_options	注記参照	Zero length encoding	注記参照	注記参照
BDB	必須	BDB	無し	無し
セキュリティブロック	条件付き	セキュリティブロック	注記参照	注記参照

注記） 暗号化と完全性のオプションはカード内照合では利用できない。なぜならば、Table 11.3 に記載された情報のみが読み取られ、その時 BDB はカード内に残り、そのカードが照合処理に使用するからである。２つのカード照合方式についての暗号化と完全性についての情報はそれぞれ Table 11.3 と Table 11.4 の注記を参照すること。

2.6. ISO/IEC 19794-4：2005　指紋画像データ交換フォーマット

2.6.1. データ交換フォーマット制定の背景

従来のバイオメトリック認証システムでは，認証性能を向上させるため，生体情報を入力するセンサ部，入力された画像を処理する画像処理部と照合を行うマッチング部の結びつきを強くし，一体としてチューニングする方法が用いられてきた。例えば，スタンドアロン利用での入退出管理装置や 1 人で利用するモバイル端末では，この方法でも問題はなかった。しかし，バイオメトリック認証が普及し，基盤機能としての性質を増すにつれて，バイオメトリックデータの互換性が重視されている。

大規模システムへの適用では，生体情報入力用のセンサを変えた場合にも，再登録作業をせずに従来から登録済みの利用者の登録データを利用することが求められる。また，照合を行うマッチング部についてもデータの後方互換性の維持が必要である。例えば，電子パスポートへのバイオメトリック認証の適用では，多国間での相互運用に伴い，複数の装置ベンダーが対応できる互換フォーマットの仕組みが必要である。

バイオメトリックデータ互換フォーマットが本格的に用いられたのは犯罪捜査向けの自動指紋識別システム（AFIS：Automated Fingerprint Identification）である。米国では州，市，群ごとに購入した，異なるベンダーの AFIS の互換性を維持するために ANSI/NIST によるフォーマット（ANSI/NIST-ITL 1-2000）を作成している。また，光学的に指紋を採取するためのライブスキャナの仕様や指紋原紙にインクで採取した指紋画像を読み取るスキャナの仕様は，FBI により Image Quality Specifications（IQS）として作成されている。これらの規格は，，19794-4 指紋画像交換フォーマットの国際標準規格の基礎となっている。

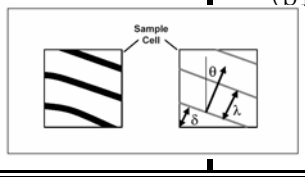
2002 年に設立された ISO/IEC JTC 1/SC 37 では，バイオメトリクス（生体認証）技術に関する標準化を行っている。SC37 は六つの WG で構成され用語，アプリケーションインターフェース，データ互換フォーマット，システムプロファイル，精度評価，法制度に関連した標準規格の策定を進めている。

データ互換フォーマットを扱う ISO/IEC 19794 シリーズにおいて，指紋に関わる交換データフォーマットは，次の 4 種類規定されている。

1) ISO/IEC 19794-4：指紋画像データ
2) ISO/IEC 19794-2：指紋特徴点データ
3) ISO/IEC 19794-3：指紋スペクトラルパターンデータ
4) ISO/IEC 19794-8：指紋スケルトンパターンデータ

表 2.6.1 に各指紋データフォーマットの概要を示す。

表 2.6.1　指紋データ交換フォーマットの規格概要

原データ	交換データ	符号化	パラメータ
指紋画像	Part 4 画像 	Raw WSQ JPEG JPEG2000 PNG	解像度，階調，画像サイズ 指（左/右，親-小指）/掌部位 入力法，品質 ［複数 D 収容可：指/View］
	Part 2 特徴点 	特徴点： 種類/位置/向き/品質 （固定長） 特徴点数	解像度，原画像サイズ， 指（左/右，親指-小指） 入力法，品質 ［複数 D 収容可：指/View］
	Part 3 パターン Spectral (FDIS) 	隆線： 傾き/波長/位相/品質 （bit 数可変）	解像度，セルサイズ/数 指（左/右，親指-小指） 入力法，品質 ［複数 D 収容可：指/View］
	Part 8 パターン Skeletal (FCD) 	特徴点：種/向き/位置 隆線方向：向き/終端 （bit 数可変）	解像度，原画像サイズ 指（左/右，親指-小指） 入力法，品質，ステップ長 ［複数 D 収容可：指/View］

2.6.2. ISO/IEC 19794-4 制定の背景

2005 年に発行された，ISO/IEC 19794-4 では指紋画像のデータ交換フォーマットを規定する。指紋画像データは指紋画像を交換するため，ベンダによる画像処理方式，特徴抽出方式や照合方式の違いによる影響を受けにくい特徴がある。19794-4 の米国の ANSI INCITS 381 がベースである。ANSI INCITS 381 よりも後に成立している関係上，品質値の範囲，レコード長の定義など異なる部分がある。

2.6.3. ISO/IEC 19794-4 の概略

19794-4 フォーマットは，一つの General record header と一つまたは複数の Finger image header record で構成される。各々の Finger image header record に指紋画像（1 指または 4 指平面）または掌紋画像が 1 枚記録される。4 指平面印象は，一つの指紋画像としてカウントされる。

General record header
Finger image header record（１）
:
Finger image header record（255）

図 2.6.1　指紋画像データのヘッダ構造

19794-4 の General record header で扱える Finger image header record の最大数は 255 と記載されている。従って一つの 19794-4 形式の指紋画像データで，最大 255 枚の指紋／掌紋画像を記録することが可能である。255 枚の指紋／掌紋画像では勿論同一指の画像も取り扱いが可能である。これらの画像は一意に決定される View Number で管理され，Finger/Palm Position により同一部のデータであるか否かが確認できる。

Field	Size	Valid values
Finger/palm position	1 byte	0-15; 20-36
Count of views	1 byte	1-256
View number	1 byte	1-256

図 2.6.2　View Number と Finger/Palm Position

ISO/19794-4:2005 中で，Count of views と View number については，Valid values として 1-256 の値が指定されているが,正しくは 0-255 もしくは，1-255 ではないかと思われる。この記述については今後も注意が必要である。

デバイス ID，スキャナ解像度，画像解像度，階調，圧縮の有無等は，General record header で定義される。各々の Finger image header record には，同一のキャプチャデバイスから採取された画像が格納されると考えても良い。

解像度は 49ppcm(pixels/centimeter)から 394ppcm まで段階的に定義されている。階調は，197ppcm（500ppi）以上は 8bit で定義されている。また，ダイナミックレンジ（グレイスケールレベル）についても，2 から 200 で解像度に合わせて段階的に定義されている。これらは，Image acquisition settings levels として一覧表に定義されている。圧縮アルゴリズムは，ビット詰め，WSQ，JPEG，JPEG2000，PNG が定義されている。500ppi の画像を WSQ で圧縮する場合は 15:1 を上限として規定している。500ppi よりも高い解像度の画像には JPEG2000 が推奨されている。

対応する押捺方式は，平面指紋（ライブ採取，インク押捺），回転指紋（ライブ採取，インク押捺），遺留指紋，Swipe 指紋，非接触指紋（ライブ採取）の 9 通りである。19794-4 の Normative ANNEX A には採取を行うスキャナの規格として Image Quality Specifications (IQS)が記載されており，画像歪，MTF 等の性能仕様が規定されている。

19794-4 にはサンプル品質を 1（低品質）から 100（高品質）の値で格納できるようにしている（規格本文中では 0 から 100、図表では 1 から 100 と定義で矛盾あり）が，品質の算出方法については定義されていない。サンプル品質については，ISO/IEC 29794 シリーズとして 2005 年から検討が開始されている。

表 2.6.2　特性，忠実度，有用性の関係

		Fidelity	
		Low	High
Character	Low	Low fidelity and low character results in low utility. Recapture might improve utility. However, if possible use of another biometric is recommended.	High fidelity and low character results in low utility. Recapture will not improve utility. Use of another biometric is recommended.
	High	Samples with high character and low fidelity typically will not demonstrate high utility. Utility can be improved upon recapture or image enhancement techniques.	Samples with high character and high fidelity indicate capture of useful sample. High utility is expected.

29794-1 ではバイオメトリックサンプル品質を特性（Character）と忠実度（Fidelity）の物差しを使って有用性(Utility)を定義している。特性が良好で忠実度が高いほど有用性が高い定義し，有用性はパフォーマンスをより近しく示すものと記載されている。

29794-1 では，得られた品質から，予測された他人受入率（psFAR）や予測された本人拒否率(psFRR)を算出してシステムに活用する品質参照モデルが示されている。

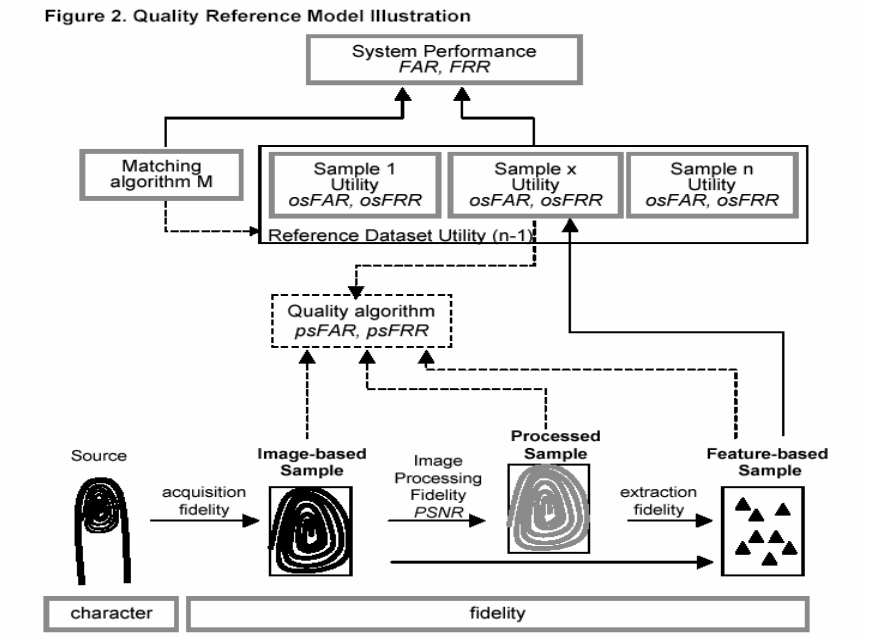


図 2.6.3 品質参照モデル

ISO/IEC 19784-1:2006（BioAPI）では，バイオメトリックサンプルの品質値を 0 を最低品質，100 を最高品質として定義しているが，29794-1 では 1 を最低品質，100 を最高品質として定義している。これらの不統一については，今後解消されていくものと思われるが，現時点では注意が必要である。

29794-1 では，品質の高い方から Excellent(76-100)，Adequate (51-75), Marginal(26-50), Unacceptable(1-25)として品質を四つのカテゴリに分けている。しかしながら，1 バイトの品質値を算出するための方法については，記述されていなかった。

表 2.6.3 品質カテゴリの 4 分類と定義

Quality Category	Definition
Excellent (76-100)	The sample will result in good authentication performance in all application environments.
Adequate (51-75)	The sample will result in good authentication performance in most application environments. For demanding applications, it may be necessary to obtain a higher quality sample.
Marginal (26-50)	The sample may result in poor authentication performance. If possible, replace the sample
Unacceptable (1-25)	The sample cannot be used for proper authentication.

この問題を解決するため，バイオメトリックサンプル品質についての議論を行うラポータ・グループが立ち上げられ，バイオメトリックサンプル品質の取り扱いに関する議論がなされた。現段階では品質値を算出するアルゴリズムを一つにまとめるのは困難であるとの検討結果を受けて，新たにバイオメトリックサンプル品質値を取り扱うための枠組みを規定するためのプロジェクトが立ち上がった。これが 29794 シリーズである。29794-1 ではフレームワークを定義し，29794-4 では指紋画像の品質に関わる部分を定義する。当初は，29794-1 と 29794-4 共に IS 化を目指していたが，2007 年 1 月の SC37 ウエリントン会議において，29794-4 は TR を目指して進められることに決まった。

2.7. ISO/IEC 19794-2：2005

2.7.1. IISO/IEC 19794-2 制定の背景

19794-2 は, 指紋の代表的な照合方式である特徴点方式のためのデータ交換フォーマットである。圧縮された指紋画像に比べても 10 分の 1 以下のデータサイズにできる特長がある。指紋データを IC カード内に格納する場合，データがコンパクトであることは，低コスト化や読み出し時間の短縮においてメリットがある。

19794-2 も, 電子パスポート用の指紋画像フォーマットとして ICAO 文書に参照されている。さらには，ILO が発行する船員手帳への適用も検討されている。19794-2 のベースは米国の ANSI/INCITS 378 である。米国で ANSI/INCITS 378 の発行年が 2004 であり，19794-2 の発行年が 2005 年であることから，両者の間には僅かな違いがある。しかしながら，NIST が ANSI/INCITS 378-2004 フォーマットを用いて行った実験，Performance and Interoperability of the INCITS 378 Fingerprint Template は，19794-2 フォーマットを用いたときの性能を想定する上での参考となる情報である。NIST や ILO（船員手帳）等による実証実験の結果を受けて，特徴点データの共通性を確保するため，指紋特徴点の定義を

明確化するための Amendment 提案がなされている。

2.7.2. ISO/IEC 19794-2 の内容

19794-2 のヘッダで定義されている情報は, 指紋画像データで定義されている内容とほぼ同様であるが若干の違いがあると同時に, 19794-4 のようにヘッダが General record header と Finger image header record として明示的に定義されていない。19794-2 では 19794-4 と同様に View Number と Finger Position を用いて同じ指の情報を扱えるようにしている。19794-2 では 19794-4 とは異なり View Number は 0-15 までの値として定義されている。Finger Position Code では，掌紋（Palm）はサポートされていない。データは，レコード全体の情報，View 毎の情報，特徴点（マニューシャ）毎の情報で構成されている。

2.7.3. Record format と Card format

19794-2 では Finger Minutiae Record Format と IC カードへの格納用として Finger Minutiae Card Format が規定されている。さらに Finger Minutiae Card Format は, Normal Size Finger Minutiae Format と Compact Size Finger Minutiae Format に分かれている。Compact Size Finger Minutiae Format ではデータ量を少なくするために特徴点位置や向きの分解能を低く定義している。

先に述べたように，19794-2 では 19794-4 のようにヘッダが General record header と Finger image header record として明示的に定義されていない。このため Card Format に Finger Minutiae Record Format の Record header を含むか含まないかが不明確になるという問題があり，2007 年 1 月のニュージーランド会議で対応策が検討された。結論として，Record header 有/無しの両方のフォーマットを認める方針で進めることになったが，具体的な対応方法は決まっていない。

19794-2 では特徴点の必須情報として，指紋特徴点の種類，座標，方向を定義している。細線化処理毎の端点位置の違いが出ないよう，端点は指紋谷線の分岐点として定義されている。分岐点の定義は指紋隆線の分岐点として定義されている。Finger Minutiae Card Format では細線化した指紋隆線の端点を用いることが許されている。19794-2 では各フォーマットで指紋特徴点の位置情報や方向の分解能について細かく定義されているため，同じ 19794-2 規格のデータといえども，互換性に留意することが必要である。

認証精度を向上させるためのオプションデータとして，指紋中心（コア），三角州（デルタ），特徴点間の隆線本数が定義されている。また，ZONE Quality と呼ばれる指紋画像を複数セルに分割した際の各セルの品質データを持つことができる。

対応する押捺方式は，平面指紋（ライブ採取，インク押捺），回転指紋（ライブ採取，インク押捺），遺留指紋，遺留指紋の写真，薬品等で検出された遺留指紋，トレースされた遺留指紋，Swipe 指紋，非接触指紋（ライブ採取）の 9 通りであり，19794-4 の指紋画像データの定義とは若干異なる。

19794-2 の Normative ANNEX B には採取を行うスキャナの規格として Image Quality Specifications (IQS)が記載されており，画像歪，MTF 等の性能仕様が規定されている。

3. 指紋センサ（スキャナ）I/F に関する調査

3.1. 操作ソフト及びユーザインタフェースの分析

国内 3 社，海外 2 社のスキャナに添付された操作ソフトのユーザーインターフェースに関する分析を行った。海外 2 社のスキャナについては，添付のサンプルソフトを調査に用いた。海外 2 社のスキャナに添付されていたソフトウェアはサンプルソフトであり，操作及びユーザーインターフェースの参考になるものは添付されていない。

Aware 社の ICAO／NIST Pack に添付されているドキュメントを，指紋採取時のユーザーインターフェース調査の観点から調べたが，これらに関する記述は無かった。Aware 社の ICAO／NIST Pack は，指紋画像，顔画像，虹彩画像のデータを標準規格のフォーマットで取り扱うためのソフトウェアパッケージである。ICAO Pack では SC37 で規格化されたデータ交換フォーマットの形式（ISO/IEC 19794 シリーズ），バイオメトリック汎用データ交換フォーマットの枠組み（CBEFF）による形式（ISO/IEC 19785 シリーズ）で扱うためのツールが提供されている。NIST Pack では ANSI のフォーマット形式（例：ANSI/INCITS 397，ANSI/INCITS 381 等）で扱うためのツールが提供されている。指紋認証実施に関係するものとしては，品質評価ソフトウェアが添付されているが，ライブスキャナを制御するためのアプリケーションは添付されていない。

指紋認証に関しての専門化ではない，一般の利用者に対して指紋認証時に適切な指紋画像を取得するためのユーザーインターフェースの取り組みは，PC 等へのログイン時に認証に用いられている民生機器で数多く見られる。今回は，国内 3 社の PC ログイン向けの民生機器についてのマニュアル等の調査を行った。

PC ログイン向けの民生機器では，傍に専門知識のある人間が立ち会わないで利用者に適切な指紋画像を入力される必要があるため，ユーザーインターフェースに様々な工夫がこらされている。また，指紋センサ（ライブスキャナ）についても，個々の指の状態に合わせて感度のキャリブレーションを行う装置が殆どである。

これらの製品で，ほぼ共通しているのは次の仕様である（全ての製品ではない）。

- 採取を行っている指紋画像の表示
- 指紋押捺操作に対してのフィードバック
  - 押捺面積不足の通知

－ 指紋中心等の検出による位置ずれの通知
－ 画像判定による湿潤／乾燥状態の通知

・適切な指の置き方の説明
－ マニュアルへの記載
－ ソフトウェア画面での指紋入力方法の図示

具体的な例を以下に示す。図 3-1 は，指紋入力画面の例である。指紋入力画面に十字型の枠を示し，ここに指紋の中心（コア）部分を入力することにより，安定した照合性能を得る配慮がなされている。

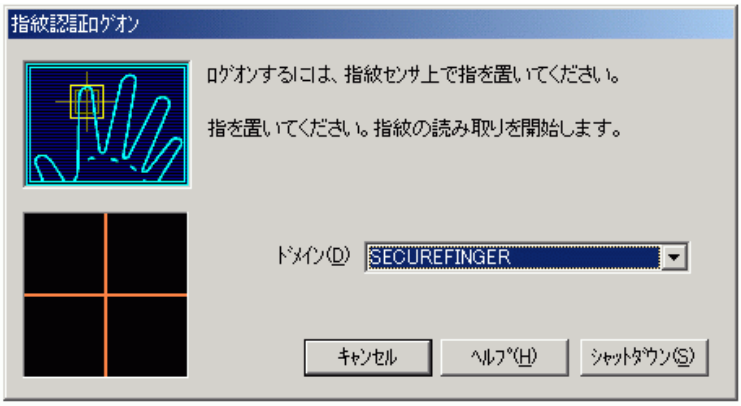


図 3.1.1　指紋入力画面の例１

次の例では，指紋入力画面で画像表示と同時に，図によって指の置き方を示している例である。具体的に指の置き方を示すことで，初めての利用者にも理解しやすい内容となっている。

図 3.1.2　指紋入力画面の例２

下記の例では，指紋の登録画面に移る前に，指紋センサへの適切な指の置き方を図示している例である。OK ボタンを押してから，登録画面に遷する。登録時に適切な指の置き方を示し，その後に安定した運用を行うことを目的としている。この画面は，動画として提供され，適切な指の置き方を示すと同時に不適切な指の置き方（指が立っている状態）も示されている。

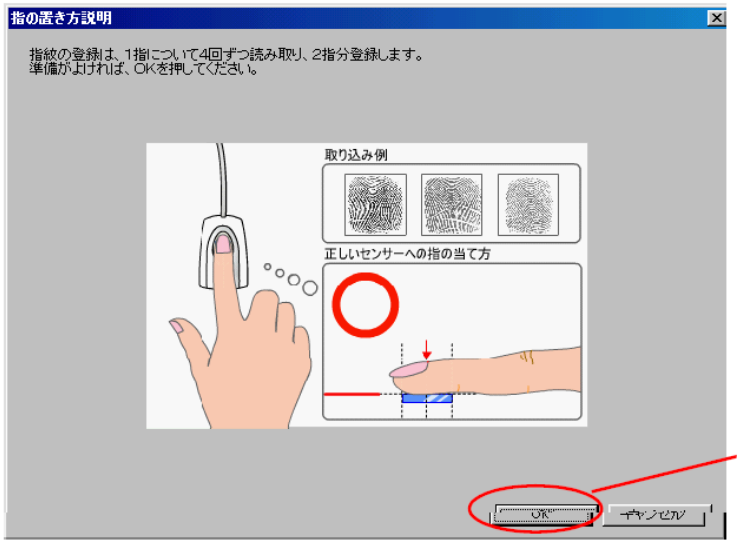


図 3.1.3　指紋入力方法の説明画面

指紋入力要求画面での指紋画像表示機能は，今回調査した，国内 3 社のスキャナ製品でサポートされていた。入力画像を表示することは，ユーザーに対しての有効なフィードバック手段であることが理由と考えられる。

3.2. インターフェース調査

国内 3 社，海外 2 社のスキャナインターフェースを調査した。5 社のうち 4 社が PC との接続に USB インターフェースを用いており， 1 社は IEEE1394 を用いている。 5 社共にスキャナに関するコマンドは異なっている。

海外 2 社のスキャナは，一般にライブスキャナと呼ばれるもので指紋画像を採取するための API 仕様が公開されている。国内 3 社のスキャナは，主に PC ログイン等の用途で用いられるものであり，指紋認証ソフトを含む専用のアプリケーション/ユーティリティを使うことが前提とされている。表 3-1 から 3-5 に調査したスキャナの装置仕様を示す。

(1) CrossMatch 製 ACC01394

表 3.2.1　1 指ライブスキャナ ACCO1394 の製品仕様

Scanner functions	Scanned fingers types	Single flat fingers Single rolled fingers
	Fingerprint capture format	30mm x 30mm
	Scanner interface	IEEE 1394
	Scanner resolution	500 ppi
	Scanner image size (H x V)	600 x 600 pixel
Scanner Dimensions	Scanner size (H x W x D)	80 x 60 x 160 mm
	Scanner weight	0.83 kg
Operation & Environmental Conditions	Operating Environment	Indoor, on table top
	Operating Conditions	15-35℃ 10-80% humidity

(2) CrossMatch 製 Verifyer300 LC 2.0

表 3.2.2 1 指ライブスキャナ Verifyer300 LC 2.0 の製品仕様

Resolution	500DPI ± 1%
Moduration Transfer Function	50% at 10 cycles per milimeter at finger platen
Linearity and Rectilinearity	Less than 1 pixel (average)
Illumination Uniformity	Less than 50% variation center to corners
Platen Size	30.5mm x 30.5mm
Output(Digital)	USB 2.0
Power(Digital)	5V DC (supplied by PC)
Temperature Range	-18℃-40℃
Humidity Range	10-90% non-condensing, splash-regsistant
Weight	0.45kg
Dimensions(H x L x W)	62mm x 162mm x 83mm

(3) NEC 製 PU800-30

表 3.2.3　PU800-30 の製品仕様（スキャナ部）

センサ	画像センサ	指内散乱光直接読み取り方式
	センサエリア	18mm x 15mm
	密度	800dpi
	インターフェース	USB Rev.1.1
	電源	USB より供給
	消費電力	2.5W 以下
	温・湿度条件	10-35℃　20-80%
	外形寸法	75(W) x 75(D) x 25(H)
	質量	75g 以下

(4) 三菱電機製 DT-TP

表 3.2.4　DT-TP の機器仕様（スキャナ部）

機器仕様	
センサー部	指内部特性検出型光学センサー
指置き形状	指の第１関節部と、指先部の１点ないしは２点支持
上位 I/F	USB　1.1　（または RS-232C）
外形寸法	45mm(幅)×94mm(高)×90mm(奥)
質量	約 140g（本体）
電源	DC5V 最大 5W
動作環境	温度：　0～40℃ 湿度：　85%RH 以下 照度：　5000 ルクス以下

(5) 富士通製 FS-230U

表 3.2.5　FS-230U の機器仕様（スキャナ部）

機器仕様	
指紋センサー	静電容量式半導体センサー
センサエリア	12.8mm(W) x 15mm(H)
解像度	500dpi
I/F	USB
消費電流	100mA 以下
外形寸法	38mm(幅)×18mm(高)×60mm(奥)
質量	約 65g（本体）
電源	USB
使用条件	温度：　10～35℃ 湿度：　20～80%

4. 実装規格案

4.1. 序文

この規格は，2004 年に第 1 版として発行された ISO/IEC 7816-11:2004, Identification cards ― Integrated circuit cards ― Part 11: Personal verfication through biometric methods を基に作成した実装規格である。

4.2. 適用範囲

本実装規格は，バイオメトリックデータを IC カードに格納し認証に利用する際の指針を示すものとする。同時に，必要なファイルフォーマット形式及びコマンドを示すものとする。詳細なコマンド・シーケンスを定義するものではない。

想定するアプリケーションターゲットは， 公務員や企業従業員向けの ID カード用途などでの，IC カードに格納された指紋情報を用いた本人確認用途であり，比較的高いセキュリティと複数ベンダシステムでの相互運用を想定した互換性が求められるものとする。

本規格では次のようなアプリケーションを対象とする

1) IC カード製造者は，必要なファイルをあらかじめ作成するとともに輸送鍵により保護すること。
2) 対象とするカードは，カード上に指紋センサが搭載されていない，オフ・カード・マッチング型のカードとする。
3) IC カードに格納するための生体情報の取得をカードに格納することはリアルタイムに行わない。生体情報を，一度，安全なデータベースに保管した後，IC カードへの生体情報の書き込みを行う。
4) IC カード内のアプリケーションはマルチ AP とする。AP 毎にファイルが一つ対応し，その中で VIT を管理する。
5) 生体情報に関しての書式付けはカード外のアプリケーションが行う。
6) IC カードの利用を停止する場合は，カード外アプリケーション側で停止する。IC カードに停止コマンドを発行することはない。AP 毎の停止だけを扱うものとする。
7) IC カード内の生体情報の更新・追加は行わない。再登録を行う場合は，発行手続きと同じ手順をとる。

本規格では次のものは対象としない。
1) 追記型・更新型のフォーマット
2) オン・カード・マッチング

本規格の対象者は，IC カード技術者，及び，バイオメトリック認証技術者を想定し，IC カード技術者及びバイオメトリック認証技術者から要求に対応し，両者の理解の促進に供することを目的とする。

4.3. 引用規格

次に掲げる規格（国際規格）は，この規格に引用されることによって，この規格の規定の一部を構成する。
これらの引用規格のうちで，西暦年を付記してあるものは，記載の年の版を適用し，その後の改正版（追補を含む。）には適用しない。西暦年の付記がない引用規格は，その最新版（追補を含む。）を適用する。

ISO/IEC 7816-4:2005
ISO/IEC 7816-11:2004
ISO/IEC 19785-1：2006
ISO/IEC 2nd FCD 19785-3：2006
ISO/IEC 19794-2：2005
ISO/IEC 19794-4：2005

4.4. 用語及び定義

この規格で用いる主な用語及び定義は，次による。

4.4.1.
バイオメトリックデータ (Biometric data)
バイオメトリック照合に使われる特徴を符号化したデータ

4.4.2.
バイオメトリック情報 (Biometric information)
照合データを構成するために IC カードの外で必要とする情報

4.4.3.

バイオメトリック参照データ (Biometric reference data)
バイオメトリック照合データと比較するためにカードに記録するデータ

4.4.4.
バイオメトリック照合 (Biometric verification)
バイオメトリック参照データに対して，バイオメトリック照合データを 1：1 で比較することで，本人確認を行う処理

4.4.5.
バイオメトリック照合データ (Biometric verification data)
バイオメトリック参照データと比較するため，本人確認処理中に採取するデータ

4.4.6
テンプレート (Template)
ISO/IEC 7816-4 による
警告－用語“テンプレート”は，構造化したデータオブジェクトの値フィールドを意味する。“特徴抽出後のバイオメトリックデータ”と混同してはならない。
注記 ISO/IEC 7816-4:2005 に対応する JIS X 6320-4 を現在策定中であり，その内容との整合に留意する必要がある。

4.4.7
マッチング (Matching)
バイオメトリックデータ相互の比較を行い，互いの類似度（距離）を算出する処理

4.5. 記号及び略号

この規格で用いる主な記号及び略号は，次による。

AID	アプリケーション識別子	Application Identifier
AT	認証テンプレート[1)]	Authentication Template
BER	基本符号化規則	Basic Encoding Rules
BIT	バイオメトリック情報テンプレート[2)]	Biometric Information Template
BD	バイオメトリックデータ	Biometric Data
BDP	個別利用形式で表現するBD	BD in proprietary Data
BDS	標準化形式で表現するBD	BD in standardized format
BDT	バイオメトリックデータテンプレート	Biometric Data Template
CCT	暗号化チェックサムテンプレート[3)]	Cryptographic Checksum Template
CRT	制御参照テンプレート	Control Reference Template
CT	機密テンプレート[4)]	Confidentiality Template
DE	データ要素	Data Element
DF	専用ファイル	Dedicated File
DO	データオブジェクト	Data Object
DST	ディジタル署名テンプレート[5)]	Digital Signature Template
EFID	基本ファイルID	Elementary File ID
FCI	ファイル制御情報	File Control Information
ID	識別子	Identifier
L	長さ	Length
OID	オブジェクト識別子	Object Identifier
RD	参照データ	Reference Data
SE	セキュリティ環境	Security Environment
SM	セキュアメッセージング	Secure Messaging
TLV	タグ-長さ-値	Tag-Length-Value
UQ[6)]	使用修飾子[7)]	Usage Qualifier
VIDO	照合要求情報データオブジェクト	Verification requirement Information Data Object
VIT	照合要求情報テンプレート	Verification requirement Information Template

注 [1)] ISO/IEC 7816-4 では，略号 AT は control reference template for authentication に変更されている。なお JIS X 6320-6 では認証制御参照テンプレートとした。

注 2) ISO/IEC 7816-15 では，略号 BIT でなく，Biometric_Information_Template と記した。

注 3) ISO/IEC7816-4 では，略号 CCT は control reference template for cryptographic checksum に変更されている。

注 4) ISO/IEC7816-4 では，略号 CT は control reference template for confidentiality に変更されている。

注 5) ISO/IEC7816-4 では，略号 DST は control reference template for digital signature に変更されている。

注 6) この略語は附属書 B に示されている。

注 7) 現在策定中の JIS X 6320-4 にて，対応する訳語を検討しており，その内容との整合を留意する必要がある。

4.6. 登録／照合処理のモデル

図 4.6.1 は ISO/IEC 7816-11:2004 による IC カードに生体情報を格納する際の一般的な枠組みである。センサから取得された生体情報原データは容量が大きいため特徴抽出処理によりデータ量を小さくして，カードへのデータ記録を行う事が記載されている。通常の登録処理においてはバイオメトリック参照データを，書式情報と共に，記録及び照合のためにカードへと安全な方法によって送る。本規格の登録モデルとして図 4.6.1 を用いる。記録された生体情報は，PIN などによるアクセス管理が必要な場合がある。照合モデルについても同様に図 4.6.2 を用いる。

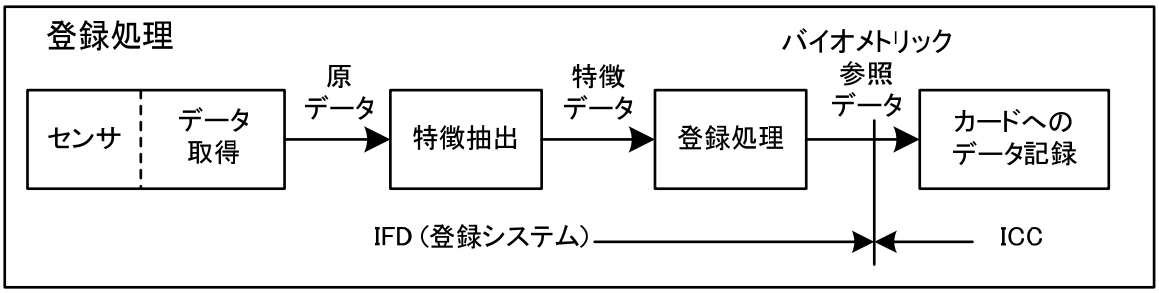


図 4.6.1　本規格における登録モデル

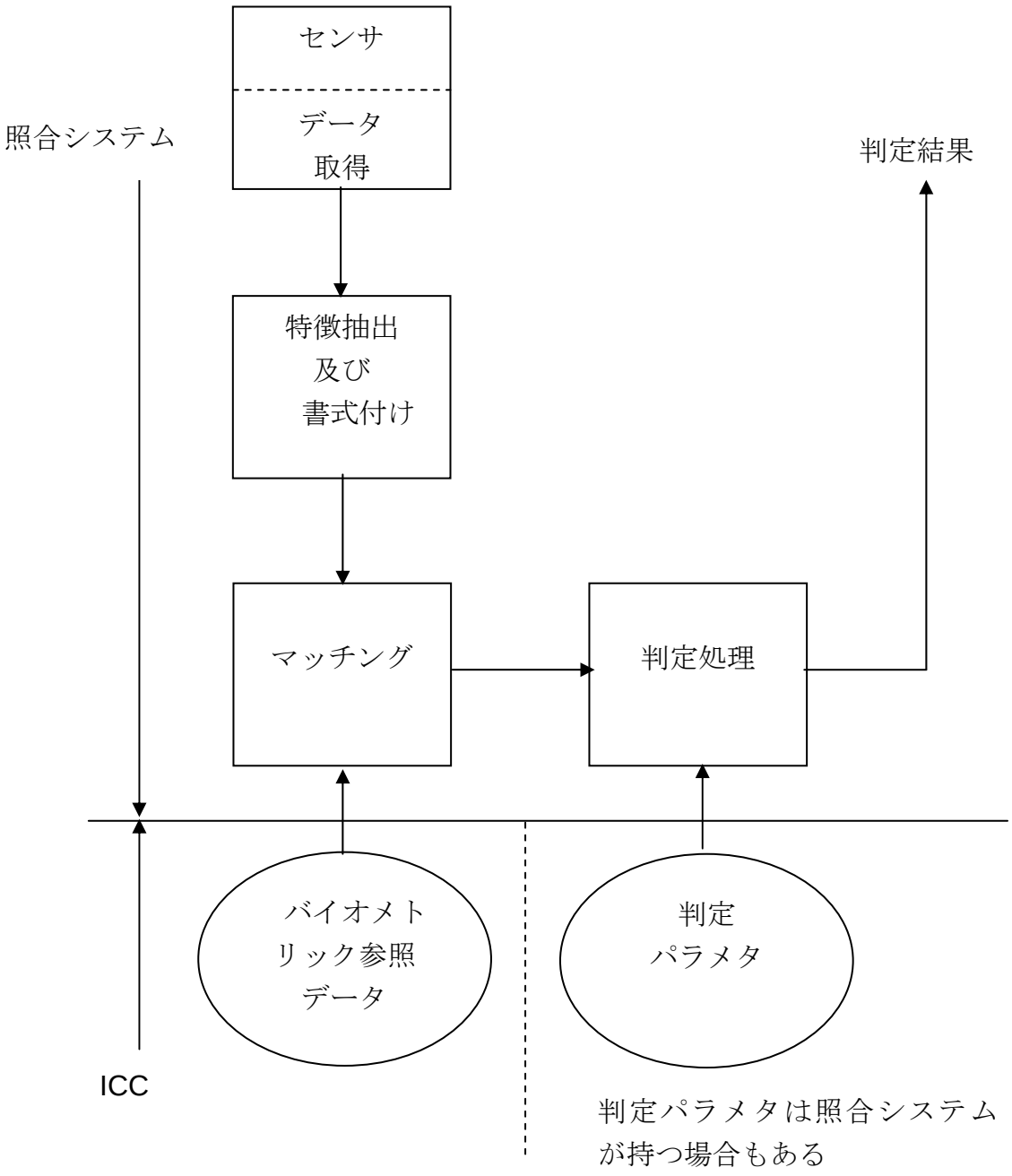


図 4.6.2　本規格が想定する照合モデル

4.7. IC カードライフサイクル

本節では，バイオメトリクスデータを格納し認証に用いる際の IC カードのライフサイクル管理方法について規定する。

IC カードのライフサイクルは，IC カードを利用する業務の運用形態やセキュリティポリシによって様々になるため，ここでは，まずは一般化した IC カードライフサイクルを定義し，それに基づき，特にバイオメトリクスに関するライフサイクル管理方法を規定するものとする。

本実装規格では，一般化された IC カードのライフサイクルを定義するにあたり，対象の IC カードの運用形態を単純化するため，以下条件を前提とする。

(1) 関係者

対象のICカードシステムに関わる関係者は，ICカードの製造を行う「ICカード製造者」と，ICカード発行主体である「ICカード発行者」，ICカード発行者からICカードの提供を受けサービスを享受する「ICカード所持者」とする[6]。

(2) 関係者の役割

「ICカード発行者」は単一の主体とし，ICカード発行の他，サービス提供，運営をすべて行うものとする。また，「ICカード発行者」以外の主体が，本ICカードを用いたサービスの提供もしくはICカードサービスへの参加を行わないものとする[7]。

4.7.1. 本規格で想定する IC カードのライフサイクル

前述の前提条件に従い一般化した IC カードのライフサイクルを以下図 4.7.1 に示す。以降，本実装規格では，本節のライフサイクルモデルを前提とする。

[6] 厳密には，IC カード発行者から IC カードの「貸与」を受け，それを用いてサービスを享受するケースもあるが，IC カードを所持する関係者をすべて「IC カード所持者」と定義する。

[7] 例えば，他の主体が発行した IC カードに，別途 IC カード AP をダウンロードし，新たな「サービス提供」を行う場合や，電子マネーなど，IC カード発行主体（サービス提供，運営主体）と，各店舗などの「サービスに参加する」主体が異なる場合などを指す。

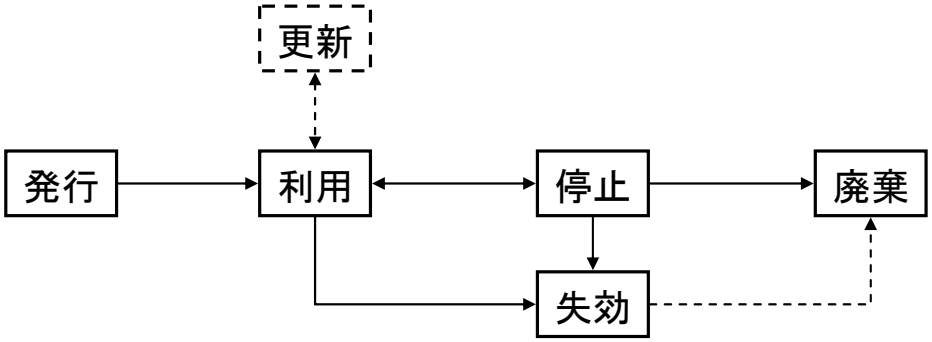


図 4.7.1 一般的な IC カードのライフサイクル

以下，図 1 の各プロセスの内容を示す。

4.7.1.1. 発行

IC カード発行者によって，IC カードを利用できる状態で利用者に提供するプロセス。発行プロセスは IC カード内部の状態に応じてさらに以下のプロセスに分類する。

① 0 次発行

IC カード製造者が，IC カード製造，初期設定，必要なファイルの書き込み処理を行い，1 次発行者に向け空の IC カードを発行するプロセス。

IC カード製造者は，決められた仕様書のとおり IC カードを製造し，発行された IC カードを IC カード発行者に安全に受け渡すため，別途策定された規定に従ったセキュリティ設定（輸送鍵の設定等）を実施する。

② 1 次発行

IC カード発行者が，カード AP のインストールなど，IC カードへの業務情報の設定を行うプロセス。ここでは IC カード所持者の情報は記録されていない状態で発行される。

③ 2 次発行

IC カード発行者が，IC カード所持者の情報を登録し，サービスで利用できる状態にして IC カード所持者に提供するプロセス。

4.7.1.2. 利用

IC カード所持者が，IC カードをサービスで正常に利用可能なプロセス。

4.7.1.3. 更新

発行済み IC カードの更新を行うプロセス。IC カードのセキュリティ情報（暗号鍵など），業務情報，IC カード所持者の個人情報の変更が必要になっ

た場合に実施される。

ここでは，一般的な IC カードのプロセスとして挙げたが，本実装規格では IC カード内の格納情報の追記・更新を行わない前提のため，本プロセスは対象外とする。

4.7.1.4. 停止

何らかの理由により一時的に IC カードもしくは IC カード内のカード AP の利用が停止されるプロセス。IC カード発行者が認めた場合は停止解除を行い，通常の「利用」プロセスに移行する。一般に停止される理由には以下が挙げられる。

- IC カード所持者による申請 （例：長期に利用しない場合の停止申請）
- セキュリティポリシ上の理由（例：PIN 照合時のロックなど）

上記の停止処理の実行は，IC カードに対するコマンド発行により IC カード自体の利用もしくは IC カード内のアプリケーションファイルの利用を停止する方法と，IC カード内の状態は変えずに IC カード外のシステム側で IC カードの利用を停止する方法が考えられる。

本実装規格では，IC カードへの停止コマンドの発行は行わないものとし，後者の IC カード外のシステム側で停止を行うケースのみを対象とする。但し，PIN 照合時のロック（上限を超えてリトライが行われた場合の IC カードのロック機能）のみ検討の対象とする。

4.7.1.5. 失効

IC カードシステムのセキュリティポリシに従い，IC カードの利用権限が失効されるプロセス。停止プロセスとは異なり，一度失効されると利用プロセスへの移行は行なえず廃棄プロセスに移行する。（再度サービスを享受するためには再発行を行う。）

一般に失効処理が行われる理由には以下が挙げられる。

- IC カードの紛失・盗難により IC カード所持者が失効申請を行った場合。
- IC カード及びシステムのセキュリティ強度（暗号強度など）が，セキュリティポリシを満たさなくなったと判断される場合。

上記の失効処理の実行は，前述の停止処理と同様，IC カードに対するコマンドの発行により実施されるケースと，IC カード内の状態は変えずに IC カード外のシステム側で失効処理を行う方法が考えられる。

本実装規格では，IC カードへの失効コマンドの発行は行わないものとし，後者の IC カード外のシステム側で失効を行うケースのみを対象とする。

4.7.1.6. 廃棄

停止あるいは失効された IC カードを，必要に応じて IC カード発行者が回収し，あらかじめ決められた方法で破棄するプロセス。

回収された IC カードが不正に利用されないよう安全な方法で破棄を行う。

4.7.2. 生体認証を導入した場合のライフサイクル管理方法

前節の IC カードのライフサイクルモデルに従い，各プロセスで実施する生体認証処理の内容を以下に示す。

4.7.3. 発行

発行プロセスでは，生体データの登録処理を実施する。登録処理は，IC カードシステムの運用規定に従い，決められた手段で取得した生体データ（バイオメトリック参照データ，テンプレートとも呼ぶ）と生体データの追加情報を IC カード内に安全な方法で送信，記録する。

上記の登録処理は，IC カードのライフサイクルの内，発行（2 次発行）のプロセスにて実施する。

登録処理での生体データの取得方法としては，IC カード所持者が登録施設に出向き直接採取を行う方法と，顔画像（顔写真）など郵送／オンラインにて提出する間接採取の方法とがある。

直接採取の場合，IC カード発行申請時に生体データの取得を行うケースと，IC カード発行申請を郵送・オンラインなど遠隔で受け付け，後日，IC カード提供時（交付時）に生体データの登録処理を実施するケースがある[8]。

生体データの登録にあたっては，IC カードシステムのセキュリティポリシ及び運用規定に従い，十分な利用者の身元確認を行った上で，適切な方法で生体データの取得，登録処理を行わなければならない。

前者の直接採取の場合は，IC カード発行者が生体データ取得に立ち会い正しく登録処理がなされているか確認を実施するものとする。

また，後者の間接取得の場合，IC カード提供時（交付時）に，IC カード

[8]尚，IC カードへの生体データの登録（生体認証の利用）を IC カード所持者の任意として，生体データの登録を行わず発行された IC カードに，後日，生体データの登録を追記型で行うケースも考えられるが，本実装規格では対象外とする。

申請者とICカードの提供を受けるICカード所持者の厳密な一致確認を実施する。生体認証により IC カード内の生体データと交付を受ける人物の生体情報との一致確認を行っても良い。

登録される生体データは，十分な認証精度を発揮できるよう，規定の品質評価（品質判定）を行うべきである。

また，指紋や静脈，虹彩など一人の人物から複数の生体データが取得可能な場合には，登録に用いるサブタイプ（指種，眼の左右など）の選択ルール[9]を，あらかじめICカードシステムの運用規定として決定しておき，それに従って正しいサブタイプのデータを登録する必要がある。

4.7.3.1. 更新

更新のプロセスについては，本規格の対象外とするが，生体データの更新処理を行うメリットと実施にあたっての今度の検討課題を以下に記す。

更新プロセスでは，IC カードに登録処理を行った生体データの更新（再登録）処理を行うことにより，登録された生体データが低品質の場合や，生体データの経年変化が発生した場合に，認証精度の低下をある程度防止することができると考えられる。

一方で，容易な更新（再登録）を許可する場合に，更新時の生体データのすり替えによる成りすましなどの脅威が考えられるため，更新を行う人物の厳密な身元確認や，更新前と再登録を行う人物が合致するかの厳密な確認を行うなどの対策が必須となる。

上記の生体データの更新（再登録）の可否と，許可する場合に生体データの更新（再登録）時の対策方法などについては，あらかじめ IC カードのセキュリティ要件を勘案の上，IC カードシステムのセキュリティポリシ及び運用規定として定める必要がある。

4.7.3.2. 利用

利用プロセスでは，IC カード所持者のサービス利用時（IC カード AP へのアクセス時）に，IC カード内に記録された生体データと，IC カードを利用する人物から取得した生体データ間の照合処理を行い，IC カード所持者の本人確認を実施する。

照合処理の実行にあたっては，本人拒否誤り発生時の最大リトライ回数（再試行回数）を設定し，リトライ回数を超えた場合に IC カードのロック

[9] ここでは，取得する指種の規定，複数指種からの任意選択，取得未対応時に採取する指種の優先順位を行うなどのルールを指す。

（停止処理の実施）を行ってよい。本設定は IC カードシステムのセキュリティ要件と生体認証の認証性能を勘案し，IC カードシステムのセキュリティポリシとして規定する。

4.7.3.3. 停止

生体認証の判定結果（最大リトライ回数を超えて本人と判定されない場合など）により，利用プロセスから停止プロセスに移行した場合には，再度，利用を許可する場合に，不正者の成りすましの可能性を勘案し，十分な身元確認を実施する必要がある。

4.7.3.4. 失効，廃棄

失効，廃棄のプロセスでは，IC カードの確実な廃棄とともに，IC カードおよび IC カードシステムに登録した生体データの確実な廃棄を実施する。

これらの廃棄方法については，IC カードシステムのセキュリティポリシ及び運用規定にて規定する。

4.8. バイオメトリックデータの登録／照合処理のモデル

4.8.1. 本規格が想定するアプリケーション

1) IC カード製造者及び IC カード発行者によって IC カードを利用できる状態で利用者に提供するプロセスは三つに分類する。

① 0 次発行 : IC カード製造業者が，初期設定を行い 1 次発行者に向けて空のカードを発行するプロセス。カードは輸送鍵などで保護される。

② 1 次発行 : IC カード発行者（サービス提供者）が，カード AP のインストールなど，IC カードへの業務情報の設定を行うプロセス。ここでは IC カード所持者の情報は記録されていない状態で発行される。

③ 2 次発行 : IC カード発行者（サービス提供者）が，IC カード所有者の情報を登録し，サービスで利用できる状態にして IC カード所持者に提供するプロセス。

2)IC カード製造者は，必要なファイルをあらかじめ作成するとともに輸送鍵により保護すること。

3)対象とするカードは，カード上に指紋センサが搭載されていない，オフ・カード・マッチング型のカードとする。

4)2 次発行において, IC カードに格納するための生体情報を本人から取得し，IC カードへの生体情報の書込処理を行う。

5)生体情報の取得時には信用のおける第 3 者が立会う。公証人は提供者から身分証明書などの所有物または情報（公開または秘密であることを問わない）など身分を担保できる情報を用いて本人確認を行う。

6)IC カード内のアプリケーションはマルチ AP とする。AP 毎にファイルが 1 つ対応し，その中で VIT を管理する。

7)生体情報に関しての書式付けはカード外のアプリケーションが処理を行う。

8)取得した生体情報を IC カードに書き込む際は，正当な権限のあるものが輸送鍵を用いてカードの書込制限を解除する。

9)生体情報は IC カードの安全な領域に格納され，照合時に生体情報を読み出す場合には，セキュアメッセージング等，何らかの安全な手段を用いて読み出す。

10)IC カードの利用を停止する場合は，カード外アプリケーション側で停止する。IC カードに停止コマンドを発行することはない。AP 毎の停止だけを扱うものとする。

11)IC カード内の生体情報の更新・追加は行わない。再登録を行う場合は，発行手続きと同じ手順をとる。

12)IC カードの失効についても，カード外アプリケーション側で利用者の ID（マルチ AP を想定した ID)を失効させる。IC カードに停止・失効コマンドを発行することはない。

13)具体的な IC カードの廃棄方法は規定しない。

14)IC カード提供時（交付時）には，IC カード申請者と IC カードの提供を受ける IC カード所持者の一致確認の実施を行う。実施の方法として，交付する IC カードでの確認照合等の手段がある。その他の本人確認方法として，身分証明書などの所有物または情報など身分を担保できる情報を用いる。また，発行する IC カードの券面情報を用いても良い。

4.8.2. 登録処理

4.8.2.1. 一般的な登録モデル

図 4.8.1 は JIS X 6320-11 による IC カードに生体情報を格納する際の一般的な枠組みである。センサから取得された生体情報原データは容量が大きいため特徴抽出処理によりデータ量を小さくして，カードへのデータ記録を行う事が一般的である。通常の登録処理においてはバイオメトリック参照データを，書式情報と共に，記録及び照合のためにカードへと安全な方法によって送っても

良。

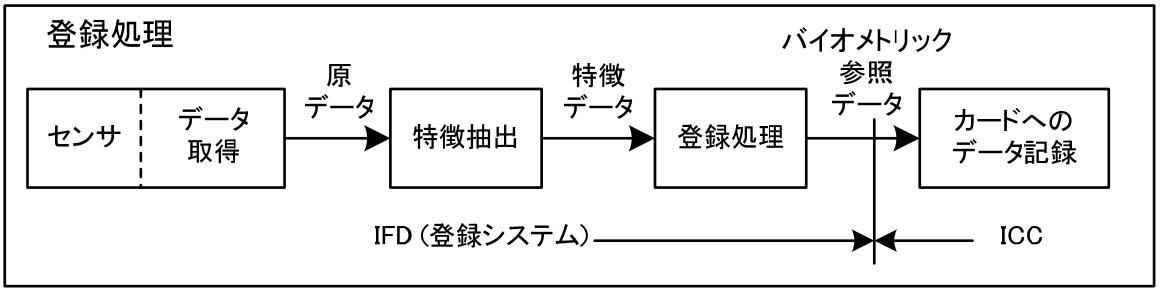


図4.8.1 JIS X 6320-11による登録処理の一般的な枠組

実際の登録処理では，圧縮処理や書式付けが登録システム側で行われる。

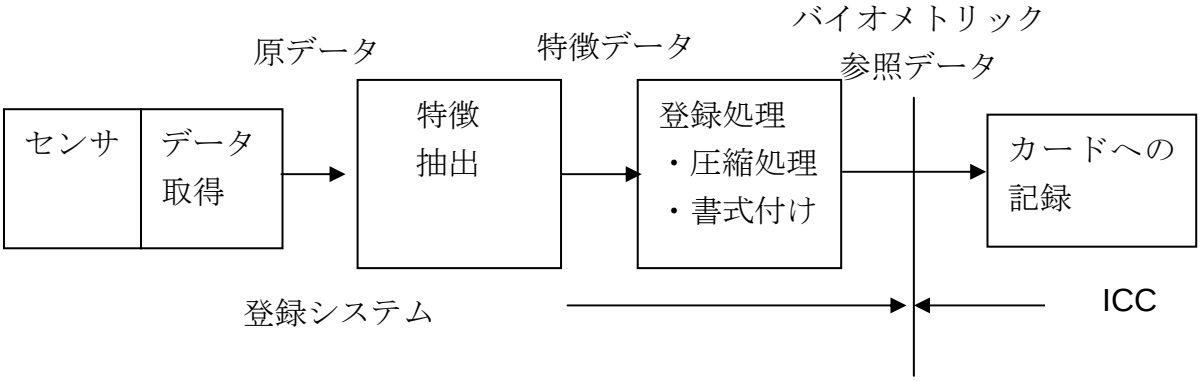


図4.8.2 実際の登録処理

4.8.2.1.1. 品質判定

取得した原データの品質判定である。所定の品質以上の原データを格納することにより，その後の運用で安定した照合性能を得る事が出来る。品質判定処理は，データ取得もしくは特徴抽出処理の中で行われる。

4.8.2.1.2. 確認照合

取得した原データから特徴抽出を行い，登録処理用のデータを作成する。カードへのデータ記録を行う前に，再度，照合用の原データを入力して照合確認を行う。登録用のバイオメトリック参照データが所定の一致率を満たすもので

あることを確認し，安定した運用につなげることが出来る。確認照合と品質判定が一体となっている場合もある。

4.8.2.1.3. 指紋登録指の選択

運用ポリシーにより，1）予め登録する指を決めている場合，2）品質や利き手を考慮して指紋を登録する指を選択する場合，がある。1 回書き込みの場合，登録する全ての指の原データを採取し，適切なバイオメトリック参照データが得られたことを確認し，カードへの記録を行う。指を選択して書き込む場合は，1)できる限り良い品質の指を登録する方法や，2)予め指定された指を書き込む方法がある。

4.8.2.2. 原データの登録モデル

実際には，原データをそのままカードに記録する場合もある。その際には登録データを圧縮してカードに記録するのが普通である。指紋画像交換フォーマット（ISO/IEC 19794-4：2005）では，圧縮方法，圧縮率についての規定がされている。指紋画像データは 1 指平面押捺の場合，幅 20mm×長さ 25mm 程度の領域で採取すると考えら場合，8 ビット階調，解像度を 500ppi で計算すると，原画像データは 193KB 程度の容量となる。19794-4 では WSQ で 1/15 の圧縮を上限としているため，1 指あたり 13KB 程度のデータ量を扱うことになる。

通常の指紋認証システムでは，指の怪我等に備えて複数の指を登録する場合が殆どである。従って，原データを登録する場合にも，概念上は図 4.8.1 であるが，実際には図 4.8.3 のように書式付けを行って，IC カードに格納する必要がある。

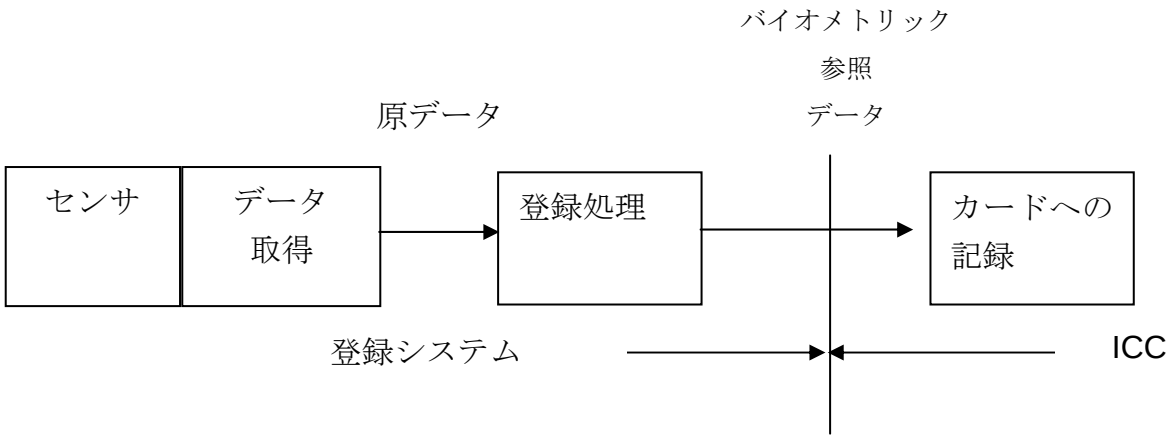


図4.8.3 原データを記録する場合

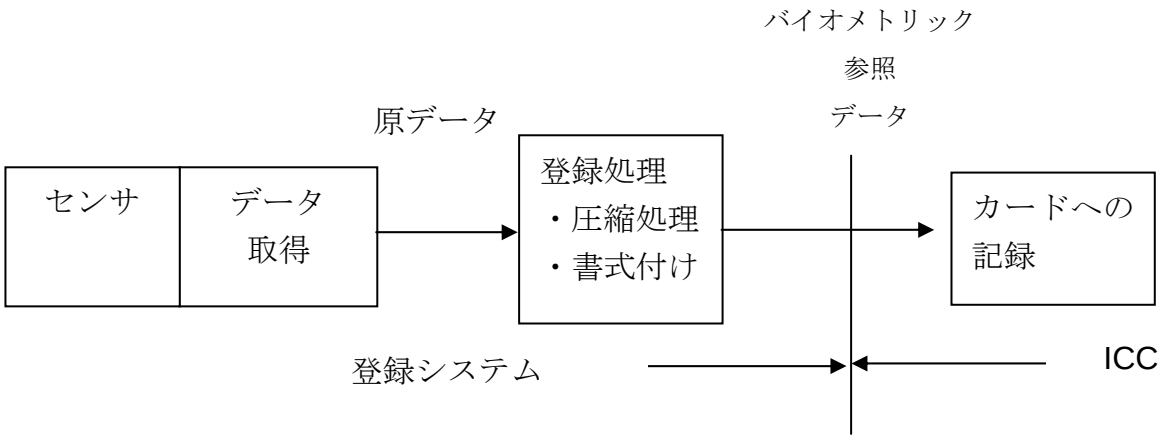


図4.8.4 実際の登録

4.8.2.3. リアルタイム登録モデル

リアルタイム登録モデルとは，データ取得後に順次カードへ記録していくモデルである。一般的には，参照用の特徴データを登録システムに保管せず，カードに参照データを記録したあとは登録システムから消去する運用がされている。利用者からの生体情報の取得と IC カードへの書き込みを同時に行うため，その場で発行を待つことが必要となる。後日送付する方法とのシステム上のトレードオフを考慮することが望ましい。

4.8.2.4. オフライン登録モデル

オフライン登録モデルとは，データ取得とカードへの記録を分けて行う処理である。参照用の特徴データを登録システムに保管する仕組みを持ち，参照用データを保持しておく。

その後，複数のカードに対しての一括登録処理を行う。カードに記録した後も参照データを保持しておけば，紛失によるカード再発行時にも，本人立会いで原データの再取得を行わずに同じ生体情報が格納されたカードを再発行することが可能という利点がある。

4.8.2.5. 登録用データの作成

登録用データは，生体情報（原データ，または，特徴データ）に書式付けを行った後，IC カードに格納する。

4.8.3. 認証時のカードアクセス方法

生体情報は機微情報であるため，IC カードに生体情報はセキュアな領域に格

納する必要がある。セキュアな領域にある生体情報を読み出すためには，PIN 等でロックを解除して読み出す必要がある。

生体認証を行うにあたって，アプリケーションは，IC カードに対して PIN 等を入力する必要がある。

4.8.4. 照合モデル

4.8.4.1. 一般的な照合モデル

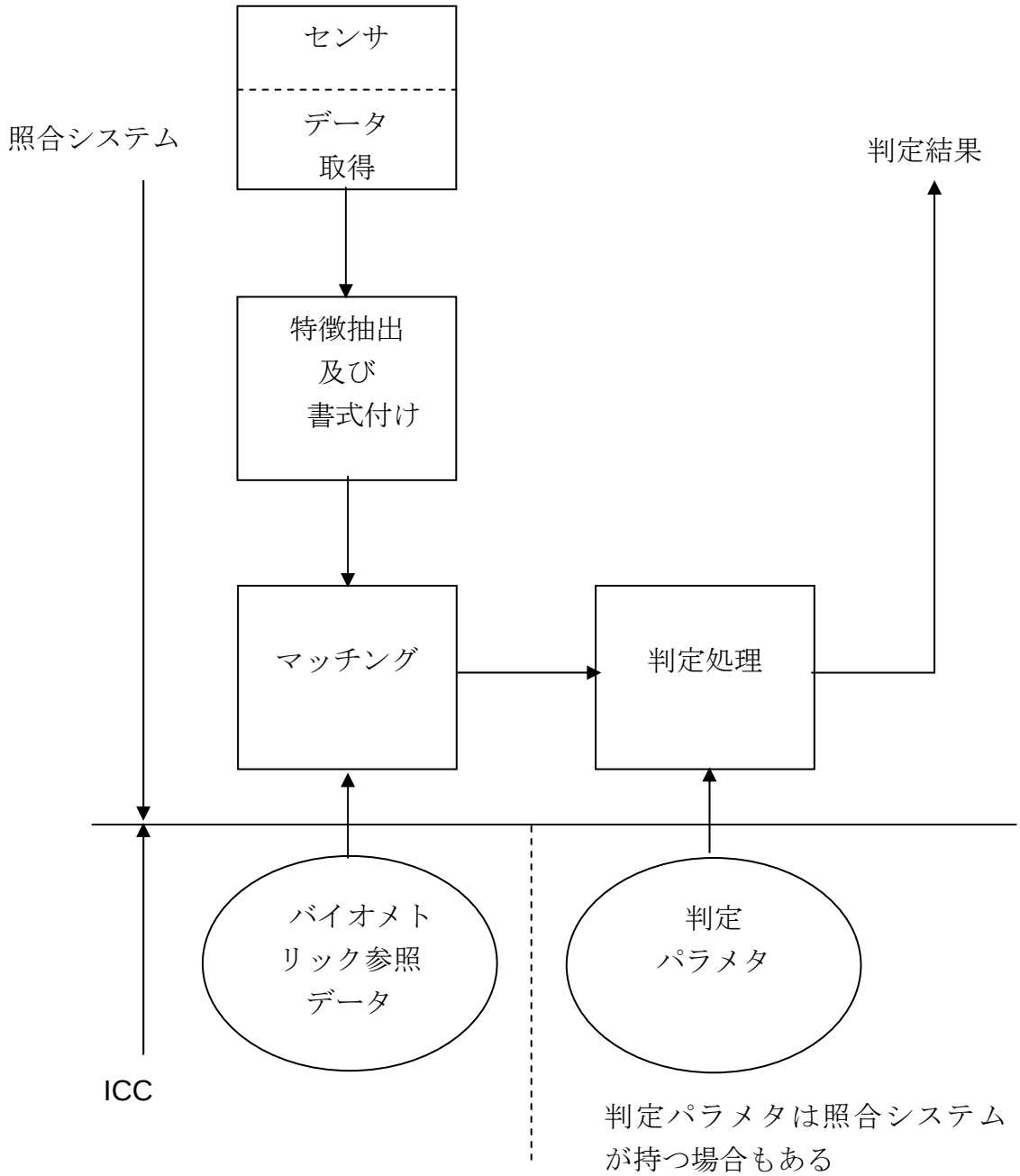


図 4.8.5　一般的な照合モデル

図 4.8.5 は一般的な照合モデルである。センサから取得された生体情報原デー

タに特徴抽出処理を行った後，カードからバイオメトリック参照データを呼び出し，両データをマッチングして判定処理を行う。照合処理においてはバイオメトリック参照データを，必要であれば判定パラメタと共に，照合システムにカードから安全な方法によって送る。判定パラメタは，照合システムが保持する場合とカードが保持する場合がある。

4.8.4.1.1. 複数指が登録（格納）されている場合の照合

複数指が格納されている場合，特定の指の指紋データを IC カードから読み出して照合を行う場合と，IC カードに格納されている全ての指紋データを読み出して照合する場合がある。

全ての指紋データを読み出した場合は，指の指定を行うのではなく，1 対多指の照合を行っても良い。

4.8.4.1.2. 照合時のリトライ

照合リトライは，IC カードから指紋データの読み出し方で 2 通りの方法に別れる。全ての登録指紋データを読み出した場合は，再度，全ての登録指紋データと照合データのマッチングを行うため，照合に使う指を変えた場合でも処理の流れは変わらない。指定した指の指紋データを読み出す方法では，照合する指を変えた場合は，再度，指定された指の指紋データを呼び出す必要がある。

リトライカウンタの管理はカード外のアプリケーションによって管理される。

4.8.4.2. パラメタ設定

生体認証では，照合時に本人と判定するための一致度の閾値を持つ必要がある。このパラメタの設定値は，IC カード内に生体情報と一緒に格納する方法と，照合時にアプリケーション側から渡す方法がある。

4.9. 対象とするバイオメトリックデータ形式

4.9.1. 本規格が対象とするファイルフォーマット

本規格が対象とする，バイオメトリックデータのファイルフォーマット形式は，ISO/IEC 19785-1 で規定される CBEFF（Common Biometric Exchange Formats Framework）である。

本規格では，現在制定中の ISO/IEC 19785-3 で規定される TLV 形式のパトロンフォーマット（電子パスポートで用いられているフォーマット）と共に，ISO/IEC 19785-1 の ASN.1 の形式に則った他のパトロンフォーマットも対象としても良い。

4.9.2. 本規格が対象とする指紋データ交換フォーマット

本規格が対象とする, 指紋データ交換フォーマットは, ISO/IEC 19794-4:2005 で規定される指紋画像データ交換フォーマット, または, ISO/IEC 19794-2:2005 で規定される指紋特徴データ交換フォーマットである。

4.9.2.1. 19794-4 で定義されるフォーマット

指紋画像データ交換フォーマットでは，回転指紋と平面指紋が定義されているが，回転指紋では利用者の高い習熟が求められるため，平面指紋の利用を推奨する。

解像度については，IC カードの容量やデータ読み出し速度を考慮し，500dpi を推奨する。

4.9.2.2. 19794-2 で定義されるフォーマット

指紋特徴データ交換フォーマットでは 3 種類のフォーマットが定義される。

1)指紋特徴点レコードフォーマット

2)指紋特徴点カードフォーマット

①ノーマルフォーマット

②コンパクトフォーマット

指紋特徴データフォーマットについては，現時点では指紋マニューシャレコードフォーマットを推奨する。押捺方式は，回転押捺ではなく平面押捺を推奨する。指紋マニューシャレコードフォーマットを用いた場合の性能については，MINEX の実験結果が参考になる。

カード･フォーマットは 7816-11 向けに作成されたものであるが, SC37/WG3 でレコードヘッダの有り･無しのフォーマットを併用する取り扱い方が審議中で

あること，ノーマルフォーマットとコンパクトフォーマットの互換性についての検証が十分に行われていないことを留意して利用することが望ましい。

4.10. ファイル形式及びコマンド

4.10.1. 条件等

4.10.1.1. 前提条件

今回の検討対象は，オフカードマッチングの本人バイオメトリクス情報による 1 対 1 照合であり，カード利用中のバイオメトリクス情報の更新，追記は行わないことを前提としている。

バイオメトリクス認証用のファイルは, 一つの DF 内で完結していることを前提に検討する。

また，IC カードは，マルチアプリケーションタイプでもシングルアプリケーションでもよいが，バイオメトリクス認証機能は，それぞれのアプリケーションに閉じて使用されるものと仮定する。

カード製造者からは，カードが輸送鍵でロックされている状況でカード発行者に渡される。発行者は，それを解除して既に存在する指定 EF 内に Biometrics Information Template(BIT)に格納されたバイオメトリクス情報を書き込む

4.10.1.2. 記載方針

バイオメトリクス情報を一括して読み出す場合，及び個々に呼び出す場合に分けて，それぞれ，どのようなファイルに格納し，どのようなコマンドを用いて読み出しすることが，収納効率及び処理速度の点で良いかを検討する。

運用時の相互互換性を主としているが，IC カードのカードライフサイクルを考慮して発行時のコマンド，アプリケーション停止，再開，カードの利用停止，廃棄に係わる管理用のコマンドも参考として記述する。

4.10.2. ファイル

4.10.2.1. ファイルの種類

バイオメトリクス認証用のファイルは，一つの DF で完結し，アプリケーション実行のために複数の EF ファイルが存在している。EF には，使用目的に合わせて次のような種類がある。図 4.10.1 に EF の種類を示す。

1) 透過構造　情報を論理的な切れ間なしに詰め込むことが可能。アクセスしたいメモリアドレスのオフセット指定と数の指定が可能。
2) 固定長順編成構造　情報を原則記録発生順一つの固定長レコードとしてまとめたもので，ファイルに複数記録できる。レコード番号及びレコード識別子によりアクセスできる。

3) 可変長順編成構造　情報を原則記録発生順一つの可変長レコードとしてまとめたもので，ファイルに複数記録できる。レコード番号及びレコード識別子によりアクセスできる。
4) 固定長循環順編成構造　情報を記録発生順に一つの固定長レコードとしてまとめたもので，ファイルに一定数まで記録できる。新しい情報が発生すると記録されているレコードのうち，最旧レコードが更新される。通常レコード番号によりアクセスできる。
5) TLV 構造　情報を (T(識別子)-L(V の長さ)-V(値))であらわされるオブジェクトとして取り扱う。また，複数の T-L-V を一つの塊とする構造化データオブジェクトとして扱うことも可能。

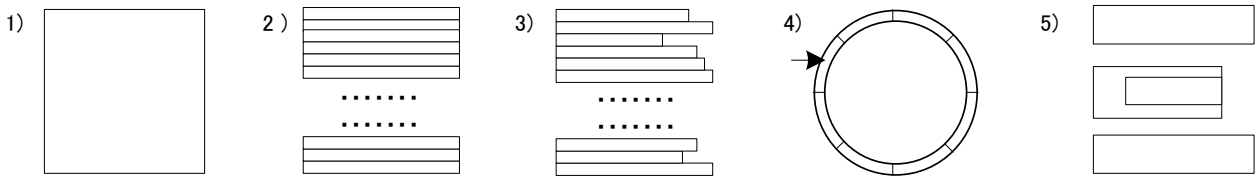


図 4.10.1　EF の種類

4.10.2.2. ファイルの構成例

既にIC旅券等でバイオメトリクスの利用ファイルが規定されているが，各アプリケーション提供者によって，セキュリティポリシがことなることから，標準的なファイル構成とすることは，困難である。次の例は，一つのアプリケーションEFとバイオメトリクス情報EFとその補助情報，それに原本性確認のためのEFを持たせたものである。また，共通情報ファイル(EF.COM)には，このアプリケーションのバージョン番号等が記憶される。

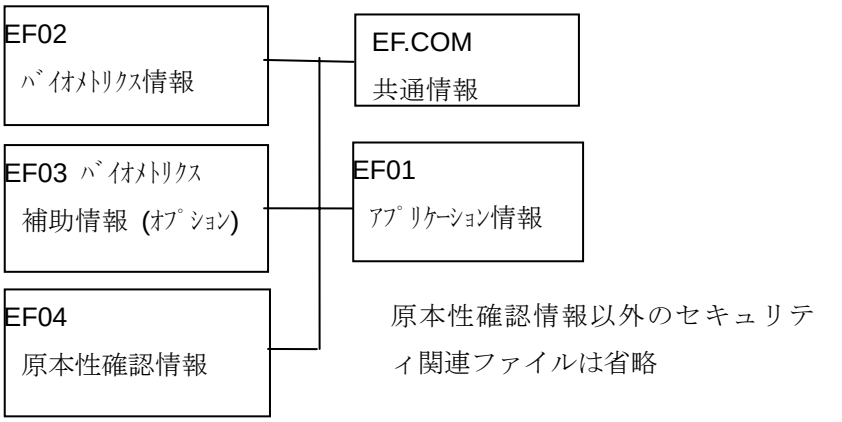


図 4.10.2 ファイル構成

4.10.2.3. ファイルの構造

4.10.2.3.1. 一括して呼び出す場合

オフカードマッチングの場合，IC カード内に記録されているバイオメトリクス参照情報を，指定されたセキュリティ解除の後に端末上へ一括して読みだし，端末上でセンサから来るバイオメトリクス情報との照合を行うのである。一括で読み出すには，記憶されるファイルの種類に従って，次の 2 通りが考えられる。

なお，この場合，IC カードからのバイオメトリクス参照情報の読み出しの際には，ブロック連鎖をもちいて，かつ第 3 者による盗み見されないように，セキュアメッセージングを行うことが望ましい。

1) 透過ファイルにすべてのバイオメトリクス情報を書き込み，それらを一括で読み出す。

2) データオブジェクトファイルに一つの構造化データオブジェクトを用意して，必要なデータオブジェクトを一纏めにして書き込む。すなわち，最初の識別子(タグ)がいわばバイオメトリクス情報の親タグとなり，その下に必要な複数のデータオブジェクトを入れ子構造で格納する方式である。それを読み出す場合には，最初の数バイトを読みだし，親のタグと次に来る長さ情報に従って読み出せば，そのファイルのバイオメトリクス情報全体を読み出すことが可能となる。

1) 透過ファイル

T	L	V 右親指	T	L
V 右人差し指	T	L	V 右中指	T
L	V 右薬指	T	L	V 右小指
T	L	V 右親指	T	L
V 右人差し指	T	L	V 右中指	T
L	V 右薬指	T	L	V 右小指

2) データオブジェクトファイル

T	L			
		T	L	V 親指
		T	L	V 人差し指
		T	L	V 中指
		T	L	V 薬指
		T	L	V 小指
		T	L	V 親指
		T	L	V 人差し指
		T	L	V 中指
		T	L	V 薬指
		T	L	V 小指

図 4.10.3 透過ファイルとデータオブジェクトファイル

注) 現在の ISO/IEC 7816-4 の規定では, ファイルの最大が 64k バイトであり,

4.10.2.3.2. 個々に呼び出す場合

次のような方法が考えられる。

1. 一つ一つのバイオメトリクス情報をそれぞれ個別の EF に格納する。透過ファイルでもデータオブジェクトファイルのいずれでも良い。いずれの場合でもそれぞれのファイルの最大は 64k バイトに限定される。

右手の EF ファイル

EF02 親指	EF03 人差し指	EF04 中指	EF05 薬指	EF06 小指

左手の EF ファイル

EF07 親指	EF08 人差し指	EF09 中指	EF10 薬指	EF11 小指

図 4.10.4 個別の透過 EF に格納

2. データオブジェクトファイルに，例えば左右の 5 指のそれぞれのバイオメトリクス情報を纏めてデータオブジェクト形式にして記憶する。ファイルの最大が 64k バイトなので，左右別々のファイルとしなければならない。

右手 EF

T	L			
		T	L	V 親指
		T	L	V 人差し指
		T	L	V 中指
		T	L	V 薬指
		T	L	V 小指

左手 EF

T	L			
		T	L	V 親指
		T	L	V 人差し指
		T	L	V 中指
		T	L	V 薬指
		T	L	V 小指

図 4.10.5 個別のデータオブジェクトファイルに格納

4.10.3. コマンド

4.10.3.1. 書き込みコマンド

カード製造者からは，カードが輸送鍵でロックされている状況でカード発行者に渡される。発行者は，それを解除して既に存在する指定 EF 内に Biometrics Information Template(BIT)に格納されたバイオメトリクス情報を書き込む

1). 輸送鍵解除

発行者と製造者間の取り決めにより，次のようなカード輸送時の安全が図ることが望ましい。

- 製造者からの IC カードが正しい引渡し相手であることを確認する手段が PIN の場合　VRIFY コマンド
- 製造者からの IC カードが正しい引渡し相手であることを確認する手段が外部認証の場合　EXTERNAL AUTHENTICATION コマンド
- 製造者からの正しい IC カードであることを発行者が確認する手段が内部認証の場合　INTERNAL AUTHENTICATE コマンド

備考　EXT/INT AUTH は，MUTUAL AUTH, GENERAL AUTH コマンドで代替可能である。

2)　書き込むファイルを選択する。SELECT コマンドを用いる。

3) 書込みコマンド

発行時の実行条件は，輸送鍵によって正しい発行者に引き渡されたことになるので，通常，これ以外に書込み/読取りの実行条件は別途指定しない。すなわち，発行者は自由に書込み読取り処理を実行できる。ただし，発行者による発行処理が終了した以降のカードライフサイクルでは，書込み機能が実行できないようにしなければならない。EF の種類により，次のファイルと書込みコマンドが使用される。

1)　透過ファイルの場合は，WRITE BINARY コマンドを用いる。
　データオブジェクトファイルの場合は，PUT DATA コマンドを用いる。
実行条件　特に必要無い

2) 書き込んだ情報を読み出して確認しても良い。
　透過ファイルの場合，READ BINARY コマンド用いる。

データオブジェクトファイルの場合，GET DATA コマンドを用いる。
実行条件　特に必要無い

3)書込み機能が実行できないようにするアクセス権を設定する。
SET ATTRIBUTE コマンド(JIS X6319-3 参照)

4) 電子署名
書き込み情報の発行者の特定及び原本性保証のために，保護する情報全体のハッシュをとり，発行者のプライベート鍵で電子署名を付加することを推奨する。
今回の仕様では，外部で計算されたものを指定のファイルに格納し，バイオメトリクス情報を読み出すときに，同時にこのファイルも読みだして発行者の特定及び原本性保証の確認をおこなう。

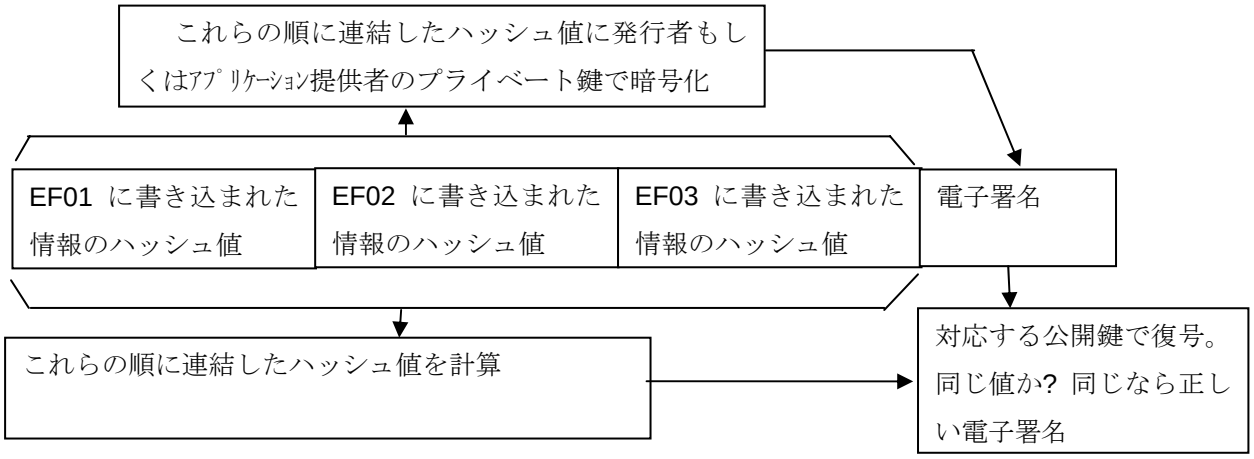


図 4.10.6 発行者の特定及び原本性保証の例

2) 運用コマンド
機能　ファイル内のすべてのバイオメトリクス情報を一括して端末に読み出す。
実行条件　読みだし条件が満たされたときに実行可能となる。
(1) DF を選択し，読み出したい EF を選択する: SELECT Command
(2) EF をアクセスするためのセキュリティ要件を解除する。
・パスワードの場合　VERIFY Command
・ 相互認証の場合　Mutual Authentication (EXTERNAL AUTHENTICATE command + INTERNAL AUTHENTICATE Command , GENERAL

AUTHENTICATE command)
(3) EF のすべての情報を読み出す。
・ 透過ファイル　READ BINARY Command
・ データオブジェクトファイル GET DATA Command(一つのファイルに一つの構造化データオブジェクトが存在)

4.10.3.2. オプションコマンド

カードのライフサイクルに従ったコマンド機能を次に記す。

4.10.3.2.1. ファイル創生機能

CREATE FILE コマンド
セキュリティを設定する方法は，特に定めない。

4.10.3.2.2. アプリケーション提供者がアプリケーション利用の停止をする機能

今回はアプリケーションが対応するので，特に定めない。

4.10.3.2.3. アプリケーション提供者がアプリケーション利用の再開する機能

今回はアプリケーションが対応するので，特に定めない。

4.10.3.2.4. パスワード/バイオメトリクス認証の停止を解除する機能

RESET RETRY COUNTER コマンド

4.10.3.2.5. カード発行者がカードの利用を停止する機能

今回はアプリケーションが対応するので，特に定めない。

4.10.4. コマンド機能

ここで，規定するコマンドは，ISO/IEC 7816-4 (JIS X 6320-4)に準拠しているが，バイオメトリクスのアプリケーションの目的と相互運用性のために，機能が制限されている。なお，ISO 規格が変更された場合は，原則として，他のアプリケーションに対応するために変更することがあり得る。また，ここにある以外のコマンドや機能を実装しても，それらがここに規定されているコマンドに害を与えないならば，追加してもかまわない。

4.10.4.1. CLA バイト

コマンドのクラスバイト CLA は，**ISO/IEC 7816-4** に対する準拠の程度，コ

マンドブロック制御の有無，セキュアメッセージング機能の適用の有無，及びロジカルチャネル番号を表す。**表**にこの規格で規定する CLA の符号化規則を示す。

・コマンドブロック制御を使用する。
・ロジカルチャネルは，0 チャネルのみサポートする。

表 4.10.1　CLA の符号化規則

b8	b7	b6	b5	b4	b3	b2	b1	意味
0	0	0	0	-	-	-	-	ISO/IEC 7816-4/8/9 準拠コマンド
1	0	0	0	-	-	-	-	ISO/IEC 7816-4/8/9 準拠コマンド以外
				0				コマンドブロック制御 チェーンの最後のブロック，或いは唯一のブロックである。
				1				チェーンの最後のブロックではない。
-	-	-	-	0	0	-	-	SM 非適用
-	-	-	-	1	1	-	-	SM 適用(コマンドヘッダ認証つき)
-	-	-	-	-	-	x	x	ロジカルチャネル番号(b2-b1=b”00”　推奨)

備考 その他の値については，この規格で留保する。

4.10.4.2. INS について

INS の 1 ビット目が’0’の場合は(偶数)は，従来どおりのバラメタを使用する。

INS の 1 ビット目が’1’の場合は(奇数)は，データフィルドに BER-TLV によるバラメ-タが存在する。

4.10.4.3. セキュリティ環境

1) 概要

カードにおけるセキュリティ環境 (SE) は，セキュリティ機構の定義情報であり，この規格の次の機能を使うときに有効になる。この規格では，セキュリティ環境の設定手順は規定しない。したがって，MANAGE SECURITY ENVIRONMENT コマンドの使用は，必す（須）ではない。

－　セキュリティ関連コマンド
－　セキュアメッセージング

2) セキュリティ環境の選択

現在選択されているセキュリティ環境をカレント SE という。カードのリセット直後においては，ネイティブ形 IC カードの場合におけるリセット直後のカレント SE は，MF の SE がカレント SE となる。これをグローバル SE という。プラットフォーム形 IC カードの場合におけるリセット直後のカレント SE は，

リセット直後のカレント DF における SE がカレント SE となり，リセット直後にカレント DF が存在しない場合には，各アプリケーションから参照できる SE（グローバル SE）がカレント SE となる。

アプリケーション固有のセキュリティ環境が設定されている場合には，MF 直下の DF 選択時にこのセキュリティ環境が暗黙的に選択され，カレント SE となる。各 DF が一つの SE をもつことができる。任意選択として規定する第 2 階層以下の DF は，SE をもたず，カレント SE が暗黙的に選択される。

アプリケーション固有のセキュリティ環境が設定されていない DF が選択された場合には，グローバル SE がカレント SE となる。

カレント SE は，

－　別のアプリケーションの選択

－　ウォームリセットの実行

－　カードの非活性化

までは，有効とする。

4.10.5. コマンドセット

次のコマンドセットを用いる。

表 4.10.2 コマンドセット

項番	コマンド名	CLA	INS	セキュリティ属性 参照ファイル	アクセスモード レベル
4.8.7.1	**発行用コマンド** (発行以後は使用付加としなければならない)				
4.8.7.1.1	CREATE FILE	“0X”	“E0”		
4.8.7.1.2	MANAGE ATTRIBUTE	“8X”	“8A”		
4.8.7.2	**透過ファイル書込み用コマンド**				
4.8.7.2.1	WRITE BINARY	“0X”	“D0” “D1”	WEF	初期書込み
4.8.7.3	**データオブジェクトファイル読取用コマンド**				
4.8.7.3.1	PUT DATA	“0X”	“DA”	DO-EF	追記更新
4.8.7.4	基本コマンド				
4.8.7.4.1	SELECT	“0X”	“A4”	－	－
4.8.7.4.2	VERIFY	“0X”	“20”	－	－
4.8.7.4.3	GET CHALLENGE	“0X”	“84”	－	－
4.8.7.4.4	EXTERNAL AUTHENTICATE	“0X”	“82”	－	－
4.8.7.4.5	INTERNAL AUTHENTICATE	“0X”	“88”	IEF	計算
4.8.7.5	**透過ファイル読取用コマンド**				
4.8.7.5.1	READ BINARY	“0X”	“B0” “B1”	WEF	読出
4.8.7.6	**データオブジェクトファイル読取用コマンド**				
4.8.7.6.1	GET DATA	“0X”	“CA”	DO-EF	読出
4.8.7.7	**管理運用コマンド**				
4.8.7.7.1	RESET RETRY COUNTER	“0X”	“2C”	IEF	閉そく（塞）解除
4.8.7.8	**セキュリティ関連コマンド**				
4.8.7.8.1	GET SESSION KEY	“8X”	“D0”	－	－

4.10.5.1. 創生系コマンド

4.10.5.1.1. CREATE FILE コマンド

a）定義及び範囲

－ このコマンドは，カレント DF 直下に，その DF 又は EF 管理情報を創生するために使用する。

b) 使用条件及びセキュリティ条件

－ セキュリティステータスが，指定された論理チャネルが獲得したカレント DF の DF 管理情報内にある DF 又は EF 創生系セキュリティ属性を満たす場合には，このコマンドを実行することができる。

－ DF 創生直後，カレント DF は変化しない。

－ このコマンドによって創生された直後のファイルは，セキュリティ属性が未設定（フリー）の状態となる。

c) コマンドメッセージ

1) コマンド APDU

CLA	INS	P1	P2	Lc	データ
“0X”	“E0”	“XX”	“XX”		
(1)	(1)	(1)	(1)	(1)	(可変)

パラメタ名	長さ	意味	備考
P1	1	ファイル記述バイト	**JIS X6319-3 附属書 10 表 2** 参照
P2	1	“00”	固定
Lc	1 又は 3	データ部の長さ	
データ	可変	管理情報	

管理情報

タグ	長さ	タグ	長さ	データ
“62”	-	“85”	-	個別利用情報 (**JIS X6319-3 附属書 10 表 4，附属書 10 表 8** 参照)

ファイル記述バイト

b8	b7	b6	b5	b4	b3	b2	b1	意味
0	-	-	-	-	-	-	-	ファイルアクセス方法
0	0	-	-	-	-	-	-	非共有ファイル
0	-	x	x	x	-	-	-	ファイルタイプ
0	-	0	0	0	x	x	x	WEF
0	-	-	-	-	0	0	1	透過型構造
0	-	0	0	1	0	0	0	IEF
0	-	1	1	1	0	1	0	DO-EF：SIMPLE－TLV
0	-	1	1	1	0	0	1	DO-EF：BER-TLV
0	-	1	1	1	0	0	0	DF
x	x	x	x	x	x	x	x	他の値はこの規格では留保。

DF 創生時のデータ部

フィールド名	長さ	意味	備考（FCP との対応）
サイズ	2	DF 自身の管理情報は含まない。	Tag=“80”に対応
DF 名	1～16	DF 名。	Tag=“84”に対応

DF 創生時のデータ部

サイズ	DF 名
(2)	(1～16)

( )内はバイト数

WEF 及び DO-EF 創生時のデータ部

フィールド名	長さ	意味	備考（FCP との対応）
EF-ID	2	WEF の EF-ID	Tag=“83”に対応
構造	0	DO-EF 透過構造	Tag=“82”のファイル記述バイトに対応。 P1 パラメタで指定する。
Tag 対応種別	0	簡易 TLV 及び BER-TLV	P1 パラメタで指定
ファイル サイズ	4	DO 構造のとき 全容量 透過構造のとき 全容量	① Tag=“82”にほぼ対応 ②③ 対応 Tag なし

WEF 及び DO-EF 創生時のデータ部

EF-ID	ファイルサイズ
(2)	(4)

( )内はバイト数

IEF 創生時のデータ部

フィールド名	長さ	意味	備考（FCP との対応）
EF-ID	2	IEF の EF-ID	Tag=“83”に対応
かぎ（鍵）サイズ	2	かぎ（鍵）の最大許容長([1]) 照合かぎ（鍵）：バイト 暗号用かぎ（鍵）：バイト	なし
再試行可能回数最大許容値	1	再試行可能回数の最大許容回数 （1～15 回，無制限は“00”を設定）	なし
暗号アルゴリズム識別子	3	暗号アルゴリズム識別子（**JIS X6319-3 附属書 4** 参照）	なし
かぎ（鍵）データ	可変	TLV 構造で表す。 Tag=“81”：平文かぎ（鍵） Tag=“82”：共通かぎ（鍵） Tag=“83”：一時的公開かぎ（鍵）([2]) Tag=“A1”：RSA かぎ（鍵）テンプレート Tag=“90”：e　Tag=“91”：n Tag=“92”：d　Tag=“93”：p || q CRT 対応の場合 Tag=“94”：p || q || d mod(p-1) || d mod(q-1) || 1/q mod p として， PK：Tag90 || Tag91 SKwithoutCRT：Tag92 || Tag91, Tag92 || Tag93 SKwithCRT：Tag94 Tag=“A2”：ECC かぎテンプレート	なし

注([1]) かぎ（鍵）サイズは，かぎ（鍵）データの値（V）だけの最大許容長を表す。

([2]) 一時的公開かぎ（鍵）をセキュリティ属性に定義する場合には，この Tag にて一時的公開かぎ（鍵）の IEF を生成し，その IEF_ID をセキュリティ属性値を示す AMDOs に設定する。

備考 RSA かぎ（鍵）テンプレートにおける二つの素数（p，q）の大小関係は，現状の演算機では必要はないため削除した。

EF-ID	かぎ（鍵）サイズ	再試行可能回数 最大許容値	暗号アルゴリズム 識別子	かぎ（鍵）データ
(2)	(2)	(1)	(3)	(可変)

( )内はバイト数

d) 応答メッセージ

1) 応答 APDU

SW1	SW2
(1)	(1)

パラメタ名	長さ	意味	備考
SW1	1		e) 参照
SW2	1		e) 参照

e) 状態ワード

1) 処理完了(正常処理及び警告処理)

SW1	SW2	ステータスコードの意味
“90”	“00”	正常終了

2) 処理中断(共通:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“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。
	“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”	“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。
	“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）。

3) 処理中断（個別:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“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。
“65”	“81”	メモリへの書込みが失敗した。
“69”	“82”	セキュリティステータスが満足されない。
	“85”	DF 名の長さが間違っている。
		EF-ID が正しくない。
		WEF のサイズが正しくない。
		WEF の DO 構造の指定が正しくない。
		かぎ（鍵）の最大サイズが正しくない。
		かぎ（鍵）の種別が正しくない。
		かぎ（鍵）の再試行可能回数最大許容値指定が正しくない。
		かぎ（鍵）の暗号アルゴリズム指定が正しくない。
		かぎ（鍵）データの構造，長さが正しくない。
“6A”	“80”	データフィールドのタグが正しくない。
	“84”	ファイル内のメモリ残容量が足りない。
	“85”	Lc の値が TLV 構造に矛盾している。
	“89”	EF が既に存在する。（7816-9）
	“8A”	同一 DF 名が既に存在する（7816-9）

f) 特記事項

－ このコマンドによって創生したファイルは，MANAGE ATTRIBUTE コマンドを用いてセキュリティ属性を設定する必要がある。

4.10.5.1.2. MANAGE ATTRIBUTES コマンド

a) 定義及び範囲

－ このコマンドは，ファイルに関連する属性（例えば，FCI にあるセキュリティ属性など）の設定及び更新のために使用する。

b) 使用条件及びセキュリティ条件

－ このコマンドは，セキュリティステータスがこの処理のためのセキュリティ属性を満足するときだけ実行可能とする。EF の場合には，それが属する DF 又は MF の創生系セキュリティ属性，DF 又は MF の場合には，自身の創生系セキュリティ属性を参照する。

－ このコマンドは，その目的のファイルを明確に特定（カレント状態に）

しなければならない。

c) コマンドメッセージ

1) コマンド APDU

CLA	INS	P1	P2	Lc	データ
“8X”	“8A”	“XX”	“AB”		
(1)	(1)	(1)	(1)	(1 又は 3)	(可変)

パラメタ名	長さ	意味	備考
P1	1	P1=“X2”の場合 EF，P1=“X4”の場合 DF	P1 符号化参照
P2	1	“AB”：セキュリティ属性（拡張）	固定
Lc	1 又は 3		
データ	可変	P2 がタグの場合には，セキュリティ属性値を示す AMDOs （AM1SCs　AM2SCs　　AMnSCs）	

2) P1 符号化

b8	b7	b6	b5	b4	b3	b2	b1	意味
0	0	0	0	0	x	x	x	設定
0	0	1	0	0	x	x	x	更新
x	x	x	-	-	0	1	0	カレント EF
x	x	x	-	-	1	0	0	カレント DF
x	x	x	x	x	x	x	x	その他の値は，この規格で留保

d) 応答メッセージ

1) 応答 APDU

SW1	SW2
(1)	(1)

パラメタ名	長さ	意味	備考
データ	可変	なし	
SW1	1		e) 参照
SW2	1		e) 参照

e) 状態ワード

1) 処理完了(正常処理及び警告処理)

SW1	SW2	ステータスコードの意味
“90”	“00”	正常終了

2) 処理中断(共通:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“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。
	“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”	“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。
	“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）。

3) 処理中断(個別:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“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。
“65”	“81”	メモリへの書込みが失敗した。
“69”	“82”	セキュリティステータスが満足されない。
	“84”	参照された IEF が閉そく（塞）している。
	“85”	コマンドの使用条件が満足されない。
“6A”	“80”	データフィールドのタグが正しくない。
	“85”	Lc の値が TLV 構造に矛盾している。
	“87”	Lc の値が P1-P2 に矛盾している。

4.10.5.2. 透過ファイル書込み用コマンド

4.10.5.2.1. WRITE BINARY コマンド

a) 定義及び範囲 このコマンドの定義及び範囲は，次による。

－ このコマンドは，バイナリデータの初期書込みを行うために使用する。なお，書込み対象領域内に，初期値以外の既存バイナリデータが存在する場合には，このコマンドによって更新することはできない。

－ INS=”D0”では，オフセットアドレスの設定が 15 ビット 32k バイトまでしか設定できないため，それ以上は，INS=”D1”で，データフィールドにオフセットアドレスを設定すること。

b) 使用条件及びセキュリティ条件 このコマンドの使用条件及びセキュリティ条件は，次による。

－ コマンドは，有効な短縮 EF 識別子によって指定した EF，又はカレント EF に対して実行される。なお，指定した EF は，カレント EF となる。

－ このコマンドは，セキュリティステータスが EF に定義された書込み系コマンドに対するセキュリティ属性を満たす場合において，実行することができる。

－ 透過構造以外の EF に対し，このコマンドが適用された場合には，コマンドの処理を中断しなければならない。

c) コマンドメッセージ

1) コマンド APDU

偶数 INS

CLA	INS	cP1	P2	L	データ
“0X”	“D0”	“XX”	“XX”		
(1)	(1)	(1)	(1)	(1 又は 3)	(可変)

パラメタ名	長さ	意味	備考
P1-P2	1	書込み対象短縮 EF 識別子及び書き込むべき最初のバイナリデータの相対アドレス	P1-P2 符号化参照
Lc	1 又は 3	書込みバイト数	
データ	可変	書込み用バイト列	

奇数 INS

CLA	INS	cP1	P2	Lc	オフセットﾃﾞｰﾀｵﾌﾞｼﾞｪｸﾄ(T-L-V)	データ
“0X”	“D1”	“00”	“00”			
(1)	(1)	(1)	(1)	(1 又は 3)	5	(可変)

パラメタ名	長さ	意味	備考
P1-P2	各 1	EFID	
Lc	1 又は 3	オフセットデータオブジェクト(T-l-V)+書き込みデータの長さ	
T-L-V	5	書き込むべき最初のバイナリデータの相対アドレス 256 バイト以上 64k バイトまで T-(L=3)-(V82- XX-XX)	
データ	可変	書込み用バイト列	

2) P1-P2 符号化 (奇数 INS の場合，EFID をあらわす)

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”	相対アドレス(15 ビット)
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 識別子(全ビットは等しくない)
1	0	0	-	-	-	-	-	“XX”	相対アドレス(8 ビット)

d) レスポンスメッセージ

1) レスポンス APDU

SW1	SW2
(1)	(1)

e) 状態ワード

1) 処理完了(正常処理及び警告処理)

SW1	SW2	ステータスコードの意味
“90”	“00”	正常終了

2) 処理中断(共通:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“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。
	“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”	“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。
	“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)。

3) 処理中断(個別:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“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。
“65”	“81”	メモリへの書込みが失敗した。
“69”	“81”	ファイル構造と矛盾したコマンドとする。
	“82”	セキュリティステータスが満足されない。
	“85”	書込み対象箇所が，初期状態でない。
	“86”	カレント WEF がない。
“6A”	“82”	短縮 EF 識別子で指定した WEF がない。
	“84”	ファイル内のメモリ残容量が足りない。
“6B”	“00”	EF 範囲外にオフセットした(検査誤り)。

4.10.5.3. データオブジェクトファイル読取用コマンド

4.10.5.3.1. PUT DATA コマンド

a) 定義及び範囲 このコマンドの定義及び範囲は，次による。

－ このコマンドは，DO-EF に，P1-P2 で指定されたタグのデータオブジェクトを新規に書き込む，又は変更する処理を行う。

b) 使用条件及びセキュリティ条件 このコマンドの使用条件及びセキュリティ条件は，次による。

－ このコマンドは，セキュリティステータスが該当データオブジェクトの追記及び更新セキュリティを満足している場合において，実行することができる。

－ P1-P2 でタグ指定した DO がカレント DF 直下のすべての DO-EF に存在せず，かつ，DO-EF がカレント EF となっており，このコマンドは P1-P2 でタグ指定された DO をカレント DO-EF に追加する。

－ P1-P2 でタグ指定した DO がカレント DF 直下のある一つの DO-EF の中に存在し，その DO が存在する DO-EF をカレント EF とし，その DO を更新する。よって DO の更新時には，DO-EF をあらかじめ選択する必要はない。

－ 更新時においては, 追記時と同一サイズ以下の DO で更新が可能とする。同一サイズより大きな指定では SW1-SW2=“6985”が出力される。

－ このコマンドを実行して追記処理が行われる場合には, DO-EF 以外の EF が選択されているとき，処理を中断しなければならない。

c) コマンドメッセージ

1) コマンド APDU

CLA	INS	P1	P2	Lc	データ
“0X”	“DA”	“XX”	“XX”		
(1)	(1)	(1)	(1)	(1 又は 3)	(可変)

パラメタ名	長さ	意味	備考
P1-P2	2	タグ指定情報	P1-P2 符号化参照
Lc	1 又は 3		
データ	可変	値	

2) P1-P2 符号化

P1-P2	意味
“0040” - “00FE”	1 バイトの BER-TLV タグを P2 で表す。
“0201” - “02FE”	1 バイトの SIMPLE-TLV タグを P2 で表す。
“4000” - “FFFF”	2 バイトの BER-TLV タグを P1-P2 で表す。
他の値	この規格で留保

d) レスポンスメッセージ

1) レスポンス APDU

SW1	SW2
(1)	(1)

パラメタ名	長さ	意味	備考
SW1	1		**e)** 参照
SW2	1		**e)** 参照

e) 状態ワード

1) 処理完了(正常処理及び警告処理)

SW1	SW2	ステータスコードの意味
“90”	“00”	正常終了

2) 処理中断(共通:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“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。
	“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”	“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。
	“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)。

3) 処理中断(個別:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“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。
“65”	“81”	メモリへの書込みが失敗した。
“69”	“82”	セキュリティステータスが満足されない。
	“85”	コマンドの使用条件が満足されない。
	“86”	ファイルがない。
“6A”	“84”	ファイル内のメモリ残容量が足りない。
	“85”	Lc の値が TLV 構造に矛盾している。

4.10.5.4. 基本コマンド

4.10.5.4.1. SELECT コマンド

a) 定義及び適用範囲 このコマンドの定義及び範囲は，次による。

－ このコマンドは，論理チャネルに対してカレントファイルを設定するために使用する。以降のコマンドは，論理チャネルを介してカレントファイルを暗黙的に参照することができる。

－ DF の選択は，DF をカレントファイルとする。DF 選択の直後，その配下にカレント EF は存在しない。

－ EF の選択は，対象 EF をカレントファイルとする。

備考 本来, 対象 EF を選択することによって親ファイルが選択されることから，親ファイルが選択される旨を削除した。

b) 使用条件及びセキュリティ条件 このコマンドの使用条件及びセキュリティ条件は，次による。

－ コマンドが正常終了及び警告終了した場合には，セキュリティステータスが変化することがある。

－ コマンドの実行誤りが生じた場合には，カード内のすべてのセキュリティステータスは保持される。

－ コマンドの実行によって，DF 又は該当 EF の親 DF の閉そく（塞）状態が通知された場合には(SW1-SW2 = “6283”)，そのファイルを(活性化するために)，カレントファイルとなる。

－ レスポンスデータでは，次を応答する。

Tag=“6F”:FCI テンプレート
Tag=“84”:DF 名［必す（須）］
Tag=“85”:DF の全容量及び残容量(任意選択)

なお，レスポンスデータには他のデータオブジェクトが存在していてもよい。

c) コマンドメッセージ

1) コマンド APDU

・DF 選択(FCI 要求あり) ([1])

CLA	INS	P1	P2	Lc	データ	Le
“0X”	“A4”	“XX”	“XX”			
(1)	(1)	(1)	(1)	(1)	(1～16)	(0 又は 1)

・EF の選択(FCI 要求なし)

CLA	INS	P1	P2	Lc	データ
“0X”	“A4”	“XX”	“XX”		(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	P1 符号化参照
P2	1	選択機能	P2 符号化参照
Lc	1	ファイル識別子又はファイル名の長さ	
データ	1～16	ファイル識別子又はファイル名	
Le	1	FCI データのバイト数	“00”固定

2) P1 符号化　この仕様では次の機能だけの符号化を行う

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)
0	0	0	0	0	1	0	0	DF 名選択(データ部:DF 名)
x	x	x	x	x	x	x	x	他の値はこの規格で留保

3) P2 符号化　この仕様では次の機能だけの符号化を行う。

b8	b7	b6	b5	b4	b3	b2	b1	**意味**
0	0	0	0	0	0	-	-	FCI 任意選択テンプレート応答
0	0	0	0	1	1	-	-	FCI 応答なし
0	0	0	0	-	-	0	0	最初又は唯一のファイル
0	0	0	0	-	-	1	0	次ファイル(部分 DF 名指定可能)
x	x	x	x	x	x	x	x	他の値はこの規格で留保

備考 カレントの DF がない場合には，次ファイルが指定されたとき，期待するファイルが選択されない可能性がある。

レスポンスメッセージ

1) レスポンス APDU

データ	SW1	SW2
（0，4~30）	(1)	(1)

パラメタ名	長さ	意味	備考
データ	0，4~30	FCI(TAG = “6F”)テンプレート FCP (TAG = “84”, “85”)テンプレート	TAG=“84”は，必す（須）。 TAG=“85”は任意選択。
SW1	1		e) 参照
SW2	1		e) 参照

データ部

“6F”	長さ	“84”	長さ	DF 名	“85”	長さ	全容量 残容量
(1)	(1)	(1)	(1)	(0～16)	(1)	(1)	(8)

状態ワード

1) 処理完了(正常処理及び警告処理)

SW1	SW2	意味
“90”	“00”	正常終了
“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。

2) 処理中断(共通:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“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。
	“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”	“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。
	“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)。

3) 処理中断(個別:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“64”	“00”	ファイル制御情報に異常がある。
“6A”	“81”	機能が提供されていない。
	“82”	アクセス対象ファイルがない。
	“87”	Lc の値が P1-P2 と矛盾している。

4.10.5.4.2. VERIFY コマンド

a) 定義及び範囲 このコマンドの定義及び範囲は，次による。

－ このコマンドは，接続装置から送られた照合かぎ（鍵）を，カード内で比較させるために使用する。

b) 使用条件及びセキュリティ条件 このコマンドの使用条件及びセキュリ

ティ条件は，次による。

- コマンドは，有効な短縮 EF 識別子によって指定した EF，又はカレント EF に対して実行される。なお，指定した EF は，カレント EF となる。
- セキュリティステータスは，現在の状態にかかわらず，比較の結果によって更新しなければならない。また，比較不一致回数を，カード内に記録しなければならない。ただし，再試行回数を制限しない設定の場合には，比較不一致回数を，カード内に記録しない。
- 本体部が空のとき,このコマンドは残りの再試行可能回数“X”を取り出す(SW1-SW2=“63CX”)。ただし，再試行を制限しない設定の場合には，常に SW1-SW2=“6300”が返送される。
- 本体部が空でないとき，1～16 バイト長の照合かぎ（鍵）を設定する。
- セキュリティステータスフラグが立っている状態(照合正常終了状態)で再実行し，異常終了した場合には，セキュリティステータスはクリアされる。

c) コマンドメッセージ

1) コマンド APDU

CLA	INS	P1	P2	Lc	**データ**
“0X”	“20”	“XX”	“XX”		
(1)	(1)	(1)	(1)	(0 又は 1)	（なし又は可変）

パラメタ名	長さ	意　味	備考
P1	1	(特になし)	“00”固定(他の値はこの規格で留保)
P2	1	参照データの限定子	P2 符号化参照
Lc	1 又は なし		
データ	可変 又は なし	照合かぎ（鍵）（1～16 バイト）	

参考　ISO/IEC 7816-4 ではデータ部の長さについて規定はない。

2) P2 符号化

b8	b7	b6	b5	b4	b3	b2	b1	意味
1	-	-	-	-	-	-	-	特定の参照データ
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 識別子指定(b“11111”以外)
x	x	x	x	x	x	x	x	他の値はこの規格で留保

d) レスポンスメッセージ

1) レスポンス APDU

SW1	SW2
(1)	(1)

e) 状態ワード

1) 処理完了(正常処理及び警告処理)

SW1	SW2	ステータスコードの意味
“90”	“00”	正常終了

2) 処理中断(共通:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“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。
	“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”	“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。
	“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)。

3) 処理中断(個別:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“63”	“00”	照合不一致とする。
	“CX”	照合不一致。［“X”によって，残りの再試行可能回数(0～15)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。
“69”	“81”	ファイル構造と矛盾したコマンドとする。
	“83”	認証方法を受け付けない。
	“84”	参照された IEF が閉そく（塞）している。
	“86”	カレント IEF がない。
“6A”	“81”	機能が提供されていない。
	“82”	短縮 EF 識別子で指定した IEF がない。
	“88”	参照されたかぎ（鍵）が正しく設定されていない。

f) 特記事項

－ 照合正常又は不一致によるコマンド処理時間の違いが解読の手がかりとならない仕組みとするのが望ましい(応答時間を一定，又はランダム化するなど)。

－ 閉そく（塞）状態の IEF に対して，再試行可能回数を要求したとき，SW1-SW2=“63C0”を応答する。

4.10.5.4.3. GET CHARANGE コマンド

a) 定義及び範囲 このコマンドの定義及び範囲は，次による。

－ このコマンドは，乱数の出力を要求するために使用する。

b) 使用条件及びセキュリティ条件 このコマンドの使用条件及びセキュリティ条件は，次による。

－ 共通かぎ（鍵）暗号(DES，Triple DES，FEAL など)を使用した認証のために乱数を取得する場合には，ブロック長(単位:バイト)に合わせて Le を設定する。

－ その他のアルゴリズムの場合には，その規格に合致した適切な乱数の長さを用いる。

－ 乱数は次の EXTERNAL AUTHENTICATE コマンドが実行されるまで有効とする。

c) コマンドメッセージ

1) コマンド APDU

CLA	INS	P1	P2	Le
“0X”	“84”	“XX”	“XX”	
(1)	(1)	(1)	(1)	(1 又は 3)

パラメタ名	長さ	意味	備考
P1	1	(特になし)	“00”固定
P2	1	(特になし)	“00”固定
Le	1 又は 3	出力する乱数の長さ	

d) レスポンスメッセージ

1) レスポンス APDU

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	乱数	
SW1	1		e) 参照
SW2	1		e) 参照

e) 状態ワード

1) 処理完了(正常処理及び警告処理)

SW1	SW2	ステータスコードの意味
“90”	“00”	正常終了

2) 処理中断(共通:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“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。
	“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”	“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。
	“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)。

4.10.5.4.4. EXTERNAL　AUTHENTICATE コマンド

a) 定義及び範囲　このコマンドの定義及び範囲は，次による。

－ このコマンドは，カードから出力された乱数及びカードの外部認証かぎ（鍵）を用いて，接続装置から送られる外部認証コードの認証を行い，結果を出力することを要求するために使用する。

－ このコマンドでは，VERIFY CERTIFICATE コマンドで SE に一時的に保持した公開かぎ（鍵）を外部認証かぎ（鍵）として使用することも可能とする。

b) 使用条件及びセキュリティ条件　このコマンドの使用条件及びセキュリ

ティ条件は，次による。

－ コマンドは，有効な短縮 EF 識別子によって指定した EF，又はカレント EF に対して実行される。なお，指定した EF は，カレント EF となる。
－ セキュリティステータスは，現在の状態にかかわらず，認証の結果によって更新しなければならない。
－ 照合不一致の場合には，再度 GET CHALLENGE コマンドを実行して乱数を取得しなければならない。
－ 再試行回数を制限しない設定の場合及び VERIFY CERTIFICATE コマンドによって一時的に SE に保持した公開かぎ（鍵）を使用する場合には，認証不一致回数を，カード内に記録しない。

備考 一時的公開かぎ（鍵）はグローバルに参照されることから，認証不一致回数を記録せず試行回数を無制限とした。

－ 本体部が空のとき，このコマンドは残りの再試行可能回数“X”を取り出す(SW1-SW2=“63CX”)。ただし，再試行を制限しない設定の場合には，常に SW1-SW2=“6300”が返送される。
－ Lc の値及びこれによって指示されるデータ部のバイト数は，共通かぎ（鍵）暗号方式を対象とする場合には，そのブロック長(単位:バイト)とし，RSA アルゴリズムを対象とする場合には，有効な短縮 EF 識別子によって指定した EF，又はカレント EF に設定された外部認証かぎのかぎ（鍵）長 n と同じけた数(単位:バイト)とする。その他のアルゴリズムの場合には，その規格に合致した適切な乱数の長さを用いる。
－ RSA アルゴリズムを対象とする場合には，外部認証コード（上位側署名）を検証することによって認証が確認できた。

c) コマンドメッセージ

1) コマンド APDU

CLA	INS	P1	P2	Lc	データ
“0X”	“82”	“XX”	“XX”		
(1)	(1)	(1)	(1)	(1 又は 3，又は 0)	(可変，又は なし)

パラメタ名	長さ	意味	備考
P1	1	アルゴリズム識別子	“00”固定
P2	1	参照データの限定子	P2 符号化参照
Lc	1 又は 3，又は　なし		
データ	可変，又は なし	認証関連データ	

備考　この規格では一時的かぎ（鍵）を使用する場合には，P2=”00”とする。

2) P2 符号化

b8	b7	b6	b5	b4	b3	b2	b1	意味
0	0	0	0	0	0	0	0	情報なし=暗黙的指定(カレント SE 指定)
1	-	-	-	-	-	-	-	特定の参照データ
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 識別子指定(b“11111”以外)
x	x	x	x	x	x	x	x	他の値はこの規格で留保

d) レスポンスメッセージ

1) レスポンス APDU

SW1	SW2
(1)	(1)

e) 状態ワード

1) 処理完了(正常処理及び警告処理)

SW1	SW2	ステータスコードの意味
“90”	“00”	正常終了

2) 処理中断(共通:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“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。
	“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”	“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。
	“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)。

3) 処理中断(個別:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“63”	“00”	照合不一致とする。
	“CX”	照合不一致［“X”によって，残りの再試行可能回数(0～15)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。
“69”	“81”	ファイル構造と矛盾したコマンドとする。
	“83”	認証方法を受け付けない。
	“84”	参照された IEF が閉そく（塞）している。
	“85”	コマンドの使用条件が満足されない。
	“86”	カレント IEF がない。
“6A”	“81”	機能が提供されていない
	“82”	短縮 EF 識別子で指定した IEF がない。
	“88”	参照されたかぎ（鍵）が正しく設定されていない。

f) 特記事項

－ 閉そく（塞）状態の IEF に対して，再試行可能回数を要求したとき，SW1-SW2=“63C0”を応答する。

4.10.5.4.5. INTERNAL AUTHENTICATE コマンド

a) 定義及び範囲 このコマンドの定義及び範囲は，次による。

－ このコマンドは，接続装置から送られる乱数，及びカード内に格納されている内部認証かぎ（鍵）を用いて，カードによる内部認証コードの計算及び出力を要求するために使用する。

b) 使用条件及びセキュリティ条件 このコマンドの使用条件及びセキュリティ条件は，次による。

－ コマンドは，有効な短縮 EF 識別子によって指定した EF，又はカレント EF に対して実行される。なお，指定した EF は，カレント EF となる。

－ このコマンドは，セキュリティステータスが EF に定義された計算系コマンドに対するセキュリティ属性を満たす場合において，実行することができる。

－ Lc 及びこれにて指示されるデータ部のバイト数は，共通かぎ（鍵）暗号方式を対象とする場合には，ブロック長(単位:バイト)と同じ値に設定する。RSA アルゴリズムを対象とする場合には，当該アルゴリズムで扱う

かぎ（鍵）長を最大値とする可変値とする。

- Le は，共通かぎ（鍵）暗号方式を対象とする場合には，ブロック長(単位:バイト)と同じ値に設定する。RSA アルゴリズムを対象とする場合には，当該アルゴリズムで扱うかぎ（鍵）長を最大値とした値を設定可能とする。また，“00”及び“0000”を指定した場合には，生成された内部認証コードを全部出力する。
- RSA アルゴリズムを対象とする場合には，当該アルゴリズムのかぎ（鍵）長と同一の長さをもつ乱数を入力する場合には，この乱数の上位 1 ビットは少なくとも 0 でなければならない。
- その他のアルゴリズムの場合には，その規格に合致した適切な乱数の長さを用いる。

c) コマンドメッセージ

1) コマンド APDU

CLA	INS	P1	P2	Lc	データ	Le
“0X”	“88”	“XX”	“XX”			
(1)	(1)	(1)	(1)	(1 又は 3)	(可変)	(1 又は 2)

パラメタ名	長さ	意味	備考
P1	1	アルゴリズム識別子	“00”固定
P2	1	参照データの限定子	P2 符号化参照
Lc	1 又は 3		
データ	可変	乱数	
Le	1 又は 2		

2) P2 符号化

b8	b7	b6	b5	b4	b3	b2	b1	意味
0	0	0	0	0	0	0	0	情報なし=暗黙的指定(カレント SE 指定)
0	-	-	-	-	-	-	-	グローバル参照データ(カレント SE 指定)
1	-	-	-	-	-	-	-	特定の参照データ
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 識別子指定(b“11111”以外)
x	x	x	x	x	x	x	x	他の値はこの規格で留保

d) レスポンスメッセージ

1) レスポンス APDU

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	内部認証コード	
SW1	1		e) 参照
SW2	1		e) 参照

e) 状態ワード

1) 処理完了(正常処理及び警告処理)

SW1	SW2	ステータスコードの意味
“90”	“00”	正常終了

2) 処理中断(共通:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“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。
	“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”	“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。
	“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)。

3) 処理中断(個別:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“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。
“69”	“81”	ファイル構造と矛盾したコマンドとする。
	“85”	コマンドの使用条件が満足されない。
	“86”	カレント IEF がない。
“6A”	“81”	機能が提供されていない。
	“82”	短縮 EF 識別子で指定した IEF がない。
	“88”	参照されたかぎ（鍵）が正しく設定されていない。

4.10.5.5. 透過ファイル読取用コマンド

4.10.5.5.1. READ BINARY コマンド

a) 定義及び範囲 このコマンドの定義及び範囲は，次による。

－ このコマンドは, 透過構造の EF 内のデータを読み出すために使用する。

b) 使用条件及びセキュリティ条件 このコマンドの使用条件及びセキュリティ条件は，次による。

－ コマンドは，有効な短縮 EF 識別子によって指定した EF，又はカレント EF に対して実行される。なお，指定した EF は，カレント EF となる。

－ このコマンドは，セキュリティステータスが EF に定義された読出し系コマンドに対するセキュリティ属性を満たす場合において，実行することができる。

－ 透過構造以外の EF に対し，このコマンドが適用された場合には，コマンドの処理を中断しなければならない。

－ INS=”B0”では，オフセットアドレスの設定が 15 ビット 32k バイトまでしか設定できないため，それ以上は，INS=”B1”で，データフィールドにオフセットアドレスを設定すること。

c) コマンドメッセージ

1) コマンド APDU

CLA	INS	P1	P2	Le
“0X”	“B0”	“XX”	“XX”	
(1)	(1)	(1)	(1)	(1 又は 3)

パラメタ名	長さ	意味	備考
P1-P2	1	読出し対象短縮 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	P1-P2 符号化参照
Le	1 又は 3	読出しバイト数	

奇数 INS の時

CLA	INS	P1	P2	Lc	オフセットﾃﾞｰﾀｵﾌﾞｼﾞｪｸﾄ(T-L-V)	Le
“0X”	“B1”	“00”	“00”			
(1)	(1)	(1)	(1)	(1(	(5)	1 又は，2

パラメタ名	長さ	意味	備考
P1-P2	各 1	EFID をあらわす。	
Lc	1		
オフセットデータオブジェクト	5	オフセットデータオブジェクト(T-L-V) 256 バイト以上 64k バイトのとき T-(L 3)-(V 82-XX-XX)	
Le	1 又は 2	読出しバイト数	

2) P1-P2 符号化

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”	相対アドレス(15 ビット)
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 識別子(全ビットは等しくない)
1	0	0	-	-	-	-	-	“XX”	相対アドレス(8 ビット)

d) レスポンスメッセージ

1) レスポンス APDU

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	指定され読み出されたデータ	
SW1	1		e) 参照
SW2	1		e) 参照

e) 状態ワード

1) 処理完了(正常処理及び警告処理)

SW1	SW2	ステータスコードの意味
“90”	“00”	正常終了

2) 処理中断(共通:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“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。
	“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”	“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。
	“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)。

3) 処理中断(個別:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“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。
“69”	“81”	ファイル構造と矛盾したコマンドとする。
	“82”	セキュリティステータスが満足されない。
	“86”	カレント WEF がない。
“6A”	“82”	短縮 EF 識別子で指定した WEF がない。
“6B”	“00”	EF 範囲外にオフセットした(検査誤り)。

4.10.5.6. データオブジェクトファイル読取用コマンド

4.10.5.6.1. GET DATA コマンド

a) 定義及び範囲 このコマンドの定義及び範囲は，次による。

－ このコマンドは，P1-P2 で指定されたデータオブジェクトを，カレント DF の DO-EF から検索し読み出す処理を行う。

b) 使用条件及びセキュリティ条件 このコマンドの使用条件及びセキュリティ条件は，次による。

－ このコマンドは，セキュリティステータスが該当データオブジェクトの読出し系セキュリティを満足している場合において，実行することができる。

－ 応答データ部は，コマンドで指定されたタグが基本型データオブジェクトの時は V だけ, 構造型データオブジェクトのときは TLV の連結で表される。

－ カレント DF 直下で，タグ(構造化タグの場合には，その値フィールドのタグは対象外)がユニークでなければならない (SIMPLE-TLV，BER-TLV)。

－ セキュリティ属性が同じ DO は，一つの DO-EF に格納することが可能。
なお，このコマンド実行前にその DO-EF への SELECT FILE は不要とする。

－ 一つの DO-EF 内に，SIMPLE と BER の TLV は混在しない。

－ 複数タグの一括読出し機能は具備しない。

c) コマンドメッセージ

1) コマンド APDU

CLA	INS	P1	P2	Le
“0X”	“CA”	“XX”	“XX”	
(1)	(1)	(1)	(1)	(1 又は 3)

パラメタ名	長さ	意味	備考
P1-P2	2	タグ指定情報	P1-P2 符号化参照
Le	1 又は 3		“00”又は“000000”

2) P1-P2 符号化

P1-P2	意味
“0040” - “00FE”	1 バイトの BER-TLV タグを P2 で表す。
“0201” - “02FE”	1 バイトの SIMPLE-TLV タグを P2 で表す。
“4000” - “FFFF”	2 バイトの BER-TLV タグを P1-P2 で表す。
他の値	この規格で留保

備考　　5.4.3.1 を参照

d) レスポンスメッセージ

－ Le フィールドが“00”(短縮 Le フィールド)の場合には，0～256 の範囲内で，要求された 1 データオブジェクトを読み出す。

－ Le フィールドが“000000”(拡張 Le フィールド)の場合には，0～65536 の範囲内で，要求された 1 データオブジェクトを読み出す。

1) レスポンス APDU

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	値	
SW1	1		e) 参照
SW2	1		e) 参照

e) 状態ワード

1) 処理完了(正常処理及び警告処理)

SW1	SW2	ステータスコードの意味
“90”	“00”	正常終了

2) 処理中断(共通:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“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。
	“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”	“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。
	“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)。

3) 処理中断(個別:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“62”	“81”	出力データに異常がある。
	“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。
“69”	“81”	ファイル構造と矛盾したコマンドとする。
	“82”	セキュリティステータスが満足されない。
	“85”	コマンドの使用条件が満足されない。
“6A”	“88”	DO が見つからない。

4.10.5.7. 管理運用コマンド

4.10.5.7.1. RESET　RETRY　COUNTER　コマンド

a)　定義及び範囲　このコマンドの定義及び範囲は，次による。

－ このコマンドは，対象かぎ（鍵）の閉そく（塞）状態を解除するために使用する。

b)　使用条件及びセキュリティ条件　このコマンドの使用条件及びセキュリティ条件は，次による。

－ このコマンドは，有効な短縮 EF 識別子で指定した EF，又はカレント EF に対して実行する。なお，指定した EF は，カレント EF となる。

－ このコマンドは，セキュリティステータスが IEF に定義された閉そく（塞）解除系セキュリティ属性を満たす場合において，実行することができる。

－ WEF に対し，このコマンドが適用された場合には，コマンドの処理を中断しなければならない。

－ このコマンドの実行は，該当かぎ（鍵）の閉そく（塞）及び閉そく（塞）解除状態に依存しない。

－ このコマンド正常終了時，該当かぎ（鍵）の再試行可能回数を初期値にリセットする。

c)　コマンドメッセージ

1)　コマンド APDU

CLA	INS	P1	P2
“0X”	“2C”	“03”	“XX”
(1)	(1)	(1)	(1)

パラメタ名	長さ	意味	備考
P1	1	“03”:再試行可能回数を初期値にリセットする。 データ部なし。	その他はこの規格で留保
P2	1	参照データの限定子	P2 符号化参照

2)　P2 符号化

b8	b7	b6	b5	b4	b3	b2	b1	意味
1	-	-	-	-	-	-	-	特定の参照データ
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 識別子指定(b“11111”以外)
その他の値								この規格で留保

d) レスポンスメッセージ

1) レスポンス APDU

SW1	SW2
(1)	(1)

パラメタ名	長さ	意味	備考
SW1	1		e) 参照
SW2	1		e) 参照

e) 状態ワード

1) 処理完了(正常処理及び警告処理)

SW1	SW2	ステータスコードの意味
“90”	“00”	正常終了

2) 処理中断(共通:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“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。
	“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”	“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。
	“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)。

3) 処理中断(個別:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“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。
“65”	“81”	メモリへの書込みが失敗した。
“69”	“81”	ファイル構造と矛盾したコマンドとする。
	“82”	セキュリティステータスが満足されない。
	“86”	カレント IEF がない。
“6A”	“82”	短縮 EF 識別子で指定した IEF がない。

4.10.5.8. セキュリティ関連コマンド

4.10.5.8.1. GET SESSION KEY コマンド

a) 定義及び範囲 このコマンドの定義及び範囲は，次による。

－ このコマンドは，接続装置から送られるシーケンス番号（**JIS X6319-3 附属書 5** 参照）と，IC カード内部で生成した乱数とからセションキーを生成するために使用する。また，このコマンドのレスポンスとして，上記乱数を公開かぎ暗号を用いて安全に接続装置に送信する。

b) 使用条件及びセキュリティ条件 このコマンドの使用条件及びセキュリティ条件は，次による。

－ コマンドレベルは，無条件とする。

－ 事前に VERIFY CERTIFICATE コマンドによって署名検証用公開かぎ（鍵）の証明を実行していなければならない。したがって，公開かぎを IC カードに記憶している。

備考 このコマンドに対するセキュアメッセージングの適否は規定しない。

c) コマンドメッセージ

1) コマンド APDU

CLA	INS	P1	P2	Lc	データ	Le
“8X”	“D0”	“00”	“00”			
(1)	(1)	(1)	(1)	(1)	(可変)	(1 又は 2)

パラメタ名	長さ	意味	備考
P1	1	“00”固定	
P2	1	“00”固定	
Lc	1		
データ	可変	シーケンス番号（SEQ）	
Le	1 又は 2		

d) レスポンスメッセージ

1) レスポンス APDU

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	暗号化されたセションキー（附属書 5　図 1 参照）	
SW1	1		e) 参照
SW2	1		e) 参照

2) データ部

暗号文 C	署名文 S
(可変)	(可変)

e) 状態ワード

1) 処理完了(正常処理及び警告処理)

SW1	SW2	ステータスコードの意味
“90”	“00”	正常終了

2) 処理中断(共通:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“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。
	“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”	“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。
	“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）。

3) 処理中断(個別:実行誤り及び検査誤り)

SW1	SW2	ステータスコードの意味
“62”	“83”	DF が閉そく（塞）している(カレント SE 利用できず)。
“64”	“00”	ファイル制御情報に異常がある［かぎ（鍵）データが壊れている］。
“6A”	“88”	参照されたかぎ（鍵）が正しく設定されていない［かぎ（鍵）未設定］。

4.10.6. 今後の課題

4.10.6.1. ファイルについて

IC 旅券，運転免許証では，透過型の EF が採用されている。透過型 EF は，情報を詰め込むには都合が良いが，複数ある場合のデータオブジェクトの切り出しが大変面倒である。データの切り出しのしやすい EF は，レコード型やデータオブジェクト型が有効である。従って，透過型 EF とデータオブジェクトの両方の機能を混合した EF があれば，大変便利である。すなわち，READ BINARY コマンドが使われるときは，透過ファイルとして機能し，GET DATA コマンドが使われるときは，データオブジェクトファイルのように振舞うものである。FCI の設定をどのようにするのかと言う問題があるが，このようにすることで，同じファイルに格納しているバイオメトリクスの情報を一括で読むか，それとも個別で読むかと言う両方の要求を可能にするものである。

4.10.6.2. バイオメトリクス情報の照合用 VERIFY BIOMETRICS コマンドの提案

バイオメトリクスの照合には，パスワード照合と同じ VERIFY コマンドが採用されているが，バイオメトリクスの照合は，PIN やパスワードとは，かなり趣を異にしている。まず，PIN，パスワードの照合は，100%合致しているかどうかであるが，バイオメトリクスの照合では，100%合致という判定ではなく，参照照合と，どれくらい類似しているかで判断が下される。また，どのくらい類似すれば，合致と判断するかという閾値を補助データとして判定時に用いることも，バイオメトリクス情報の判定時の特徴となっている。すなわち，バイオメトリクス情報の判定は，単純な 1:1 照合ではなく，コマンド実行時に何らかのプロセッシングを含むものである。従って，VERIFY コマンドとは，別に，例えば，VERIFY BIOMETRICS コマンド(仮称)とすることにより，わかり易くかつ，バイオメトリクス照合機能の拡張が可能となるコマンド体系を実現できる。ただし，委員会では，もし，名前だけを変えても VERIFY コマンドと同じような動作(単に照合結果 Yes/No を応答するだけ)なら，提案してもあまり意味が無いのではないかと言うコメントがあった。また，「どのくらい似ているかの値を応答するのはどうか」ということについては，段々似ている情報とすることが出来るので，この値を応答することには，問題があるという意見が合った。例えば，その場合，応答する値によっては応答するかしないかの制限をつけることや，パスワードのように試行制限回数をつける対処案が考えられる。また，参照情報と全く同じ情報がセンサから来ることは無いので，そのような場合には，「合致としない」と言うこともあり得ることが，VERIFY コマンドとは異なる特徴的なものである。

4.11. バイオメトリクス情報の取り扱いについて

4.11.1. バイオメトリクス情報の伝送と格納するファイル

IC 旅券等で使用される顔画像のバイオメトリクス情報では，約 20k バイトの記憶容量が必要と言われている。また，指の指紋画像で 2 指だと記憶容量 20k から 30k バイトが必要であると言われている。IC カードの基本的な伝送では，一度に転送できる情報が最大 256 バイトまでとなっているので，20k バイトの情報を IC カードから読み出すのに，単純に情報部だけの計算として 20000 バイト÷256 バイト=78.125 回となり， 256 バイトの伝送を 79 回繰り返す必要があることになる。実際にはコマンドヘッダや識別子(タグ)，情報の長さコード等がその情報に付加され，更にバイオメトリックス情報を暗号化することや暗号化チェックサムを付加すると，更に多くを繰り返さなければならないことになる。次に実際の READ BINARY コマンドでの読みだしを外部端子なし IC カード(JIS X 6322-3 (ISO/IEC 14443-3)による伝送仕様により具体的に示す。バイオメトリクス情報は，スキミング防止等により，すべて暗号化されて伝送されるものとする。

・最大フレーム長２５６バイト

- PCB (Protocol Control Byte) … １バイト
- INF (Information) … ２５３バイト
- CRC (Cyclic Redundancy Check) … ２バイト

コマンド(セキュアメッセージング形式)

INF (Information field)

PCB (1B)	CLA (1B)	INS (1B)	P1 (1B)	P2 (1B)	Lc (1B)	Le DO (3B)	認証子 DO (10B)	Le (1B)	CRC (2B)

レスポンス(セキュアメッセージング形式)

- INF 部(２３７バイト)

INF (Information field)

PCB (1B)	ﾊﾟﾃﾞｨﾝｸﾞ指示子付暗号文 DO(237B) 暗号ﾃﾞｰﾀ(231B)+ ﾊﾟﾃﾞｨﾝｸﾞ指示子 (3B)+ ﾊﾟﾃﾞｨﾝｸﾞﾃﾞｰﾀ(3B)	SW DO (4B)	認証子 DO (10B)	SW (2B)	CRC (2B)

バイオメトリクス情報のような大きなデータを読み出すには，オフセットアドレスを進めながら２３１バイト単位での繰返し読み出しとなる。すなわち，

READ BINATY コマンドの繰返し実行となる。しかし，この方法は，効率的ではない。

・READ BINARY コマンドのオフセットアドレス情報により，読み出し位置を割り出すまでの処理時間が繰返し必要。設定ミスも起こりうる。各コマンドに各パラメータを設定する必要から，１回のレスポンスで情報読み出しが最大２３１バイトどまりとなる。

そこで考えられたのが，ブロック連鎖伝送である。一回に送ることの出来る伝送量は,IC カードの受信/送信バッファサイズに依存する規定なので,最大 256 バイトの伝送量には変わりがない(将来的には，この値を増加させることも考えられる)。しかし，最初のコマンドヘッダに全体の読みだし長さを設定すれば，以降のヘッダが簡略化されることと，オフセットアドレスは，IC カードが自動的に管理するため，それぞれの伝送での指定が必要なくなるために，その処理速度の向上が可能となる。従って，今後のバイオメトリクス情報を用いた個人確認のアプリケーションを実行するためには，このブロック連鎖伝送を用いることが望ましい。ブロック連鎖による一括読み出しでは，次のように改善が図れる。

- コマンドのオフセットアドレスバラメタで読み出し位置を設定するのは，最初の１回だけで，以降は次の読み出し位置の設定は IC 内の OS が行う。
- 送る情報の各設定は，一回だけでよいので，１回のブロック転送で最大２５３バイトのデータ読み出しが可能となる。

初回読み出しコマンド(セキュアメッセージング形式)

INF (Information field)

PCB (1B)	CLA (1B)	INS (1B)	P1 (1B)	P2 (1B)	拡張 Lc (3B)	拡張 Le DO (4B)	認証子 DO (10B)	拡張 Le (2B)	CRC (2B)

初回読み出しコマンドに対するレスポンス(セキュアメッセージング形式)

INF (Information field)

PCB (1B)	パディング指示子付暗号文 DO Tag-Length-Value の最初の一部分 (最大 249B のデータ転送)	CRC (2B)

継続ブロック応答要求コマンド (R-Block) 継続繰返し読み出し

PCB (1B)	CRC (2B)

ブロック継続レスポンス(セキュアメッセージング形式)

INF (Information field)

PCB (1B)	パディング指示子付暗号文 DO Value 部継続データ (最大 253B のデータ転送)	CRC (2B)

継続最終読み出しまで繰り返す。

継続ブロック応答要求 (R-Block)

PCB (1B)	CRC (2B)

最終ブロックレスポンス(セキュアメッセージング形式)

INF (Information field)

PCB (1B)	パディング指示子付暗号文 DO Value 部最終部分	SW DO (4B)	認証子 DO (10B)	SW (2B)	CRC (2B)

READ BINARY コマンド一括読み出し指定, ブロック連鎖読み出し

伝送速度が同じならば，ブロック連鎖機能をもちいることで，伝送時間の短縮に多少効果があるが，一番効果があるのは，伝送速度そのものを引き上げることである。しかし，伝送速度が速くなると，インターフェースによっては，伝送波形が悪化すること等により，外部雑音の影響を受けやすくなることによって安定した伝送が行えなくなり，データブロックの再送が頻繁に起こり，あまり改善されない場合も考えられる。

4.11.1.1. バイオメトリクス情報量の拡張

現在は，指 1 本あたりの指紋画像は，10k から 15k バイト程度のバイオメトリクス情報が必要であるが，将来，10 指の指紋画像を記録すると，単純計算でも 100k から 150k バイトの情報が必要なことになる。しかし，IC カードのファイルサイズの最大値は 65535 バイト('FFFF')までとなっている。従って，将来もっと大きなファイルサイズを持つことになれば，コマンド機能や FCI 等で扱うこれらの値を再検討しなければならない。また，伝送が可能な情報量としても奇数 INS を用いて, データフィールドに BER-TLV 形式にのっとった長さ表示を行っていく必要があるが，これらについての詳しい機能や取り扱いについての記載が ISO/IEC 7816-4 にあまり無いので，具体的な使用例を示す必要がある。

このように，バイオメトリクス情報の個数や正確なバイオメトリクス認証を行うために情報サイズを増加させることになるが，ここで，考えなければならないのは，アプリケーションのセキュリティ要件や内容とのバランスである。また，IC カード全体のメモリリソースを考慮しないでバイオメトリクス認証のために多くリソースを使用し，実際のアプリケーションの情報が入らないようなことでは，本末顛倒である。IC 旅券などでは国際互換性を確保するために指紋画像情報を用いるが，アプリケーションによってはマニューシャ等を用いて，情報量を少なくすることも重要である。

バイオメトリクス情報が増加すると，確かに個人確認の正確さ等は向上するかも知れないが，伝送時間や処理時間に時間がかかり，入退出アプリケーション等では用を成さないこともかんがえられる。

バイオメトリクスによる個人確認と言う機能は，単にパスワードによる個人確認の機能をより向上させたものとして扱われることがある。このようなアプリケーションでは，バイオメトリクスの個人認証として，大きなメモリエリアを使用することは望まれていない。アプリケーションが要求しているセキュリティレベルとのバランスを十分考慮して，バイオメトリクス情報量を決定していかなければならない。

4.11.1.2. バイオメトリクス情報品質と信頼性確保の技術

ファイルに格納されるバイオメトリクス情報の品質と信頼性の確保は，バイオメトリクス情報による個人確認の判定にとって大変重要な問題である。バイオメトリクスのセンサからのバイオメトリクスの生情報の品質は，以降のバイオメトリクス認証に大きな影響を与えるものであり，また，途中の信号処理等が，マッチング段階での判定の信頼性に多大な影響を与えることが知られている。小規模なアプリケーションシステムであったり，一つの企業がシステムを組み立てていくような場合は，すべてを把握することが可能であるが，所謂，オープンシステムの場合は，使用するバイオメトリクスセンサがまちまちであったり，途中の処理，最終のマッチングでも複数のベンダーがそれぞれの製品を提供してシステムを構成する場合がある。この場合，実装規格を詳細に決めて互換性を保つことを基準とするが，なお，それらが仕様書どおり作成されて指定の機能が満足されているかの確認が必要となる。更に IC 旅券でも行われた互換性試験を行うことも有効である。

また，オープンシステム等のバイオメトリクス認証システムの運用段階でのバイオメトリクス照合結果の信頼性確保のためには，ISO/IEC JTC 1/SC 27でも検討されているInformation technology — Security techniques — Authentication context for biometrics (ACBio)等を用いることも考慮する必要がある。

4.11.1.3. バイオメトリクス情報のプライバシー確保の技術

指紋やアイリスのような機微情報といわれるバイオメトリクス情報を用いた個人確認技術では，みだりに第 3 者にそれらの情報を提供するものではなく，パスワードのように個人が秘匿管理しておくべきものである。例えばセンサからのバイオメトリクス情報でも第 3 者にスキミングされることがないように細心の注意を払い，使用が終わったバイオメトリクス情報は，その装置に裸のまま放置しないことを心がけるべきである。

バイオメトリクス情報の伝送では，それを 2 者間で取り決めた鍵を用いて暗号化し，その鍵を知らない者が復号できない仕組みを持つことが必要である。

更に，どこの誰に開示するための個別化技術としては，読み取りアクセス権限カードとして，カード内に相互認証用の鍵を格納する，所謂ドクターカードのような仕組みと，特に欧州の IC 旅券で検討されている Extended Access Control(EAC)等の技術も考慮する必要がある。

5. 参考文献

[1] ISO/IEC 7816-11:2004, Identification cards - Integrated circuit cards - Part 11: Personal verification through biometric methods

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

[3] ICAO NTWG, Machine Readable Travel Documents Part 1 Machine Readable Passports Fifth Edition - 2003

[4] ICAO NTWG, Machine Readable Travel Documents, Technical Report, DEVELOPMENT OF A LOGICAL DATA STRUCTURE - LDS For OPTIONAL CAPACITY EXPANSION TECHNOLOGIES Revision -1.7, 18 May 2004.

[5] ISO/IEC 19785-1:2006, Information technology - Common Biometric Exchange Formats Framework - Part 1: Data element specification

[6] ISO/IEC FCD 19785-3, Information technology - Common Biometric Exchange Formats Framework - Part 3: Patron format specifications

[7] ISO/IEC 19794-4:2005, Information technology - Biometric data interchange formats - Part 4: Finger image data

[8] ISO/IEC 19794-2:2005 Information technology - Biometric data interchange formats - Part 2: Finger minutiae data

[9] ANSI INCITS 381-2004, Information Technology - Finger Image-Based Data Interchange Format

[10] ANSI INCITS 378-2004, Information technology - Finger Minutiae Format for Data Interchange

[11] ANSI/NIST-ITL 1-2000 Standard “Data Format for the Interchange of Fingerprint, Facial, Scarmark & Tattoo (SMT) Information” FBI: Wavelet Scalar Quantization (WSQ).