ＪＣＭＡＳ　　G001-2

建設業務用ＩＣカード　－　カード　－　第２部：機能仕様

ＪＣＭＡＳ　Ｇ００１－２：１９９５

平成７年１２月１９日　制定
平成９年３月２５日　規格番号及び名称のみ改訂

（社）日本建設機械化協会標準化会議　審議

日本建設機械化協会規格

建設標準ＩＣカードの機能仕様

Construction Industry - Integrated Circuit Card - Functional Specifications

１．適用範囲　この規格は、建設業務に使用されるICカード（以下、カードという。）の機能の基本仕様について規定する。

なお、ここで言うICカードとは、中央処理装置（以下、CPUという。）を内蔵するICカードとする。

また、伝送プロトコルの詳細仕様を附属書Aで規定し、ICカード内のメモリに構築される基本ファイルフォーマットを附属書Bで規定する。

２．引用規格　この規格の引用規格を、次に示す。

(1)JIS X6304-1993 : 外部端子付きICカード　－　電気信号及び伝送プロトコル
(2)JIS X6306-1995 : 外部端子付きICカード　－　共通コマンド
(3)ISO/IEC 7816-3 : Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 3 : Electronic signals and transmission protocols
(4)ISO/IEC 7816-3 : Amendment 2 : - Identification cards - Integrated circuit(s) cards with contacts - Clause 9 to be inserted in part 3 : Revision of protocol type selection (DIS)
(5)ISO/IEC 7816-4 : Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4 : Inter-industry for interchange (2nd CD : 1993)
(6)ISO/IEC 7816-5 : Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 5 : Numbering system and registration procedure for application identifiers
(7)ANSI X3.92, 1981 : Data encryption algorithm

３．用語及び略号の定義

３．１　用語の定義　この規格で用いる主な用語の定義は、次のとおりとする。

(1)アクセス
カードからデータを読みとる。又はカードにデータを書込むこと。

(2)アクセス条件
カードにアクセスする際に必要な環境を定義する情報。この情報は、アクセス時に必要となるキーの組み合わせからなる。

(3)アクティブロー方式
電圧がローレベルのとき、カードに対してリセットがかかる方式。

(4)暗号アルゴリズム
データの本来の内容を第三者に対して秘密にするために、元データをかくはんする仕組み。

(5)暗証番号(PIN)
カードを使用する際に、当事者の正当性を確認するために入力される番号。

(6)アンサートゥリセット
　ICカードがサポートする電気的特性及び種別等を識別するための情報であり、最大32バイトからなる。この情報は、カードに対し電気的活性化が行われた後に、カードから出力される初期応答データである。

(7)IC
　処理又は記録機能を行うために設計された集積回路部品。

(8)IFD
　ICカードに対して、各種信号を供給しつつ、カードとのデータ授受を行う装置である(例えば、R/W、PC等、ICカードと通信を行う装置)。

(9)etu
　伝送データの、1ビットの伝送時間を表す単位。1基本時間単位。

(10)エレメンタリファイル(EF)
　レコード、データユニット、キーデータなどを格納するファイル。

(11)ステータスバイト(SW1-SW2)
　コマンドの実行結果を示す情報であり、2バイトで構成される。この規格では、略号としてSW1-SW2を使用する。

(12)カード発行者
　カード所持者に対して、ICカードを発行する機関(又はその代理人)。

(13)カード所持者
　ICカードの発行を受けた者。

(14)デディケーテッドファイル(DF)
　ファイル制御情報と割当て可能なメモリを含むファイル。1つ又は複数の親ファイルとなりうる。

(15)DF名
　カード内のデティケーテッドファイル(DF)を、一義的に識別するバイト列。

(16)ディレクトリファイル
　ISO/IEC 7816-5で規定されるエレメンタリファイル(EF)。

(17)ネゴシアブル・モード
　3.5712 MHzの周波数を供給した場合に、コマンド／レスポンスの授受を9600 bpsの伝送速度で行うモード。

(18)マスタファイル(MF)
　ファイル構造の根源に対応する、ただ1つの必須ファイル。

(19)レコード番号
　EF内のレコード個々に内部的に付与されるユニークな連続番号。

3．2　略号の定義　　この規格で用いる略号の定義は、次のとおりとする。

APDU	Application Protocol Data Unit
BWT	Block Waiting Time
CLA	Class Byte
CWT	Character Waiting Time

DAD	Destination Address
DES	Data Encryption Standard
DF	Dedicated File
EDC	Error Detection Code
EF	Elementary File
etu	Elementary Time Unit
I-block	Information Block
ICC	Integrated Circuit(s) Card, IC Card
IEC	International Electrotechnical Commission
IFD	Interface Device
IFS	Information Field Size
IFSC	Information Field Size for The Card
IFSD	Information Field Size for The Interface Device
ISO	International Organization for standardization
JIS	Japanese Industrial Standard
LEN	Length
NAD	Node Address
MF	Master File
P1-P2	Parameter Byte
PCB	Protocol Control Byte
PIN	Personal Identification Number
R-block	Receive Ready Block
RFU	Reserved for Future Use
SAD	Source Address
S-block	Supervisory Block
SW1-SW2	Status Byte
TLV	Tag-Length-Value
WTX	Waiting Time Extension
XOR	Exclusive-OR

なお、この規格では、'XX'で16進表示、また、"aaa"でバイナリ表示を行う(その他は、10進表示)。

4．端子の電気的特性　JIS X6304で規定される、各端子における電気的特性を採用する。
なお、採用するに当たっては、基本特性として以下の項目をサポートすることとする。

(1)CLK
JIS X 6304に従い、アンサートゥリセット及びコマンド／レスポンス授受時において、1～5 MHzで動作すること。

(2)Vpp
JIS X 6303では、ICカード内部メモリに対するデータ書込み電圧端子(Vpp端子)を規定しているが、この規格で規定するICカードはデータメモリとしてEEPROMを想定しているため、この端子は未使用とする。したがって、この端子についての存在の要否については、この規格では規定しない。

(3)Vcc, RST, GND
JIS X 6304で規定する電気特性を採用。
なお、リセットについては、アクティブロー方式を採用する。

(4)その他
端子C4及び C8については、JIS X 6303ではRFUとなってるが、これについては、この規格で規定するICカードは未使用とする。したがって、これら2端子についての存在の要否については、この規格では規定しない。

５．ICカードの動作手順　　JIS X6304で規定される、ICカードの動作手順を採用する。
なお、採用するに当たっては、基本仕様として以下の項目をサポートすることとする。

(1)この規格で規定するICカードは、外部装置からのリセット信号（RST端子上）の立ち上がりによってリセットするものとする。

６．伝送プロトコル仕様

６．１　プロトコルタイプ　　プロトコルタイプとしては、JIS X6304で規定する“調歩同期半二重ブロック伝送プロトコルT=1”を採用する。
なお、採用に当たっては、以下に示す項目を必須とする。
また、T=1のプロトコル基本仕様については、「附属書 A T=1プロトコル基本仕様(規定)」を参照のこと。

(1)NADの認識
ICカードのノードアドレスは、アンサートゥリセット出力直後に受信した正常なブロックが有するDADとする。

(2)IFSDの変更
IFSDの変更は、IFDからのIFSリクエストによって行う。

(3)S-blockとしては、以下のものを必須とする。
－IFDからのS(RESYNCH req)に対するS(RESYNCH res)。
→このS-blockの処理によって、プロトコルの開始状態に戻る。したがって、シーケンスビット及びIFSDはデフォルトに戻る(JIS X 6304の9.6.2.3.2の“規則6.2”を参照)。
－IFDからのS(IFS req)に対するS(IFS res)。
→なお、IFDからのIFS要求に対しては、アンサートゥリセットのTA3で示す値を使用する。
→S(IFS req)は、少なくとも、アンサートゥリセット又はS(RESYNCH res)送信直後に、受信可能とする。
－IFDからのS(ABORT req)に対するS(ABORT res)。

参考
a)ICカードからIFDに対してのWTX要求は、この規格では必須としない。
b)IFDからのVpp誤り通知の要求は、未定義PCBとして扱う。
c)ICカードからIFDに対してのRESYNCH要求／ABORT要求／IFS要求は、この規格では必須としない。

(4)チェーニング機能
レスポンスに対するチェーニング機能は、必須とする。

(5)IFSC
IFSCの最小値は、32 バイトとする(したがって、アンサートゥリセットのTA3の値は、'20'以上とする)。

(6)キャラクタ待ち時間(CWT)
CWT = $(2^{CWI} + 11)$作業etu　このCWIの値は、カードによって任意とする。ただし、ICカードからデータを送信する際には、CWIの値とは無関係にCWT=11etu固定とする。

(7)ブロック待ち時間(BWT)
BWT = 2^{BWI} x 960 x 372 / fs秒 + 11作業etu、ただし、0≦BWI≦9　このBWIの値は、カードによって任意とする。

なお、奨励値は、BWI = 4(したがって、BWT=約1.6秒)とする。

(8)誤り検出符号(EDC)には、1バイトのLRCを使用する。

6．2　伝送速度　　伝送速度としては、ネゴシアブルモード(アンサートゥリセット、コマンド／レスポンス授受とも、3.5712 MHzのクロック供給時に9600 bps)を基本仕様とする。
なお、コマンド／レスポンスの授受に関して、他の伝送速度で行うことについては、オプションとする。

6．3　アンサートゥリセット　　アンサートゥリセットのコーディング方法及び伝送仕様については、JIS X6304で規定される方法を基本として、採用する。

6．3．1　アンサートゥリセットの値　　この規格で規定するICカードは、少なくともISO/IEC 7816-3 : AMD 2で規定されるネゴシアブル・モードで動作するT=1プロトコルを採用する。したがって、これを示すアンサートゥリセットの値は、表1に示すとおりとする。
また、ヒストリカルバイトのコーディングについては、ISO/IEC 7816-4で規定される方法を採用する。
なお、ヒストリカルバイトとして出力すべきデータ項目については、この規格では規定しない。

表1　アンサートゥリセットの値

キャラクタ	略号	意味	値
イニシャルch.	TS	L.S.B. first/正論理	'3B'
フォーマットch.	T0	Y1='F':TA1～TD1有り K=m:ヒストリカルch.数	'Fm'
インターフェースch.	TA1	FI='1':F=372 (max. 5 MHz) DI='1':D=1	'11'
	TB1	II='00b':I=25 mA PI1='00000b':Vpp is not connected	'00'
	TC1	N='FF':N=255	'FF'
	TD1	Y2='8':TD2有り、T=1	'81'
	(TA2)	-	
	(TB2)	-	
	(TC2)	-	
	TD2	Y3='B':TA3,TB3有り、T=1	'31'
	TA3	IFSI='XX'	'XX'
	TB3	BWI=Y, CWI=Z	'YZ'
ヒストリカルch.	T1～Tm		
チェックch.	TCK	TCK=ex-or(T0～Tm)	

注：IFSI、BWI、及びCWIは、カードごとに異なる値を設定可能とする。
なお、IFSI='20'の場合には、TA3は省略可能である。
また、BWI=4かつCWI=13の場合には、TB3は省略可能である。
注：ヒストリカルキャラクタについては、別途ICカードに登録可能とすること。

6．3．2　アンサートゥリセットの伝送仕様

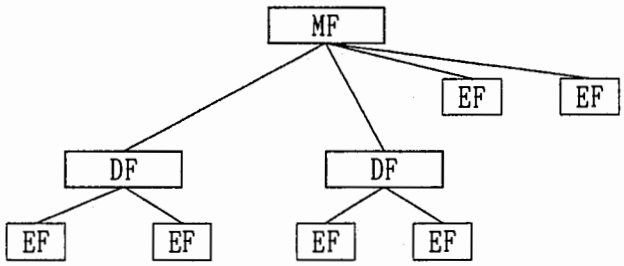
(1)伝送タイミング
アンサートゥリセットの伝送に関しては、基本的にはJIS X 6304を採用する。ただし、各キャラクタ間隔は、最大100msとする。

(2)キャラクタ再送機能について
アンサートゥリセットのキャラクタ再送機能については、この規格では必須とはしない。

7．ファイルの論理構造　　ファイルの構造については、ISO/IEC 7816-4で規定されている各項目のうち、以下のように選択して、採用する。

7．1　DFの階層　　DFの階層は図1に示すとおり１階層、つまりMF直下にDFが設定できることを最低条件とする。

図1　DFの階層



注：MF(Master File), DF(Dedicated File), EF(Elementary File)

7．2　EFタイプ　　EFタイプとしては、ISO/IEC 7816-4で規定されている以下の2種類を必須とする。

－トランスペアレントEF：EF内のデータを、バイナリイメージでアクセスするEFタイプ。
－サイクリックEF：EF内のデータを、レコードと称するデータ列を単位としてアクセスするEFタイプ。
なお、このEF内にレコードが満たされた状態においては、既存レコードのうち最旧レコードが消去され、新規レコードが追記される。

8．ファイル及びデータへのアクセス方式

8．1　DFへのアクセス　　各DFには、DF名(1～16バイトの任意長)が割り当てられ、これをSELECT FILEコマンドで選択することによって、アクセス対象DFをカレント状態にする。カレント状態となったDFにはロジカルチャネル番号が同時に付与され、以降のDF配下のEFへのアクセスは、当該ロジカルチャネル番号を使用する(アクセスコマンドのCLAで、使用ロジカルチャネルを指定する)。
なお、このDF名は、DF創成後の状態においてカード内でユニークでなければならない。

8．2　EFへのアクセス　　EFには、2バイトのEF-IDが割り当てられ、これをSELECT FILEコマンドで選択することによって、アクセス対象EFをカレント状態にする。
なお、EF-IDは、MF又はDF配下のEF群の創成後の状態において、これらEF群の範囲内においてユニークでなければならない。
また、特に、EF-IDの上位11ビットが全て"0"であるものについては、下位5ビットをShort EF-IDとして、各アクセスコマンドでアクセス対象EFを指定するために使用可能である。このShort EF-IDで指定されたEFも、カレントEFとなる。

8．3　レコードへのアクセス　　サイクリックEF内に格納されている各レコードには、論理的なレコード番号(1バイト。範囲は'01'～'FE')が内部的に付与される。このレコード番号を各コマンドのパラメタで指定することによって、読みだし／書き換え対象とするレコードを特定する。
なお、図2に示すとおり、サイクリックEF内のレコード番号の付与方法に関しては、ISO/IEC 7816-4の規定を採用する。

図2　レコード番号の付与方法

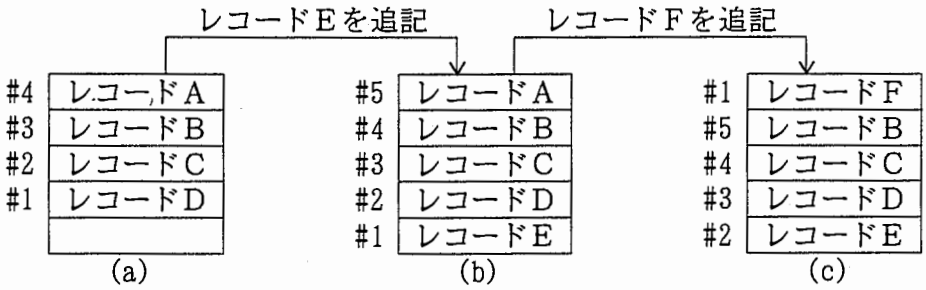


図2(a)は、4本のレコードが格納されている状態であり、最新レコードはレコードDである。したがってこの状態では、レコードDにレコード番号1が付与される。

この状態において、レコードEを追加した状態が図2(b)である。図示するように、レコードEが最新レコードとしてEFの空き領域に格納され、かつレコード番号1が付与される。

また、これによって、既存のレコードに付与されていたレコード番号はリナンバされる。

次に図2(b)の状態において、レコードFを追加した状態が図2(c)である。図示するように、図2(b)における最旧レコードAが消去され、これによって得られた空き領域にレコードFが格納される。このとき、レコードFが最新レコードとなるため、レコード番号1が付与される。

また、これによって、既存レコードに付与されていたレコード番号はリナンバされる。

補足：このようなレコード番号付与方法を採用することによって、コマンドでレコード番号1を指定することで、一義的に最新レコードがアクセス対象となる。

さて、レコードフォーマットは、システムの将来性／拡張性等を考慮し、ISO/IEC 7816-4で規定されている“簡易TLV”を採用する。フォーマットは、図3に示すような短縮フォーマットを必須とする。

図3　短縮フォーマット

レコード長が'00'～'FE'の場合：

(1ﾊﾞｲﾄ)	(1ﾊﾞｲﾄ)	(0～254ﾊﾞｲﾄ)
タグ	長さ	バリュー

なお、'0000'～'FFFF'の範囲のレコード長を扱える拡張フォーマットは、この規格では必須としない。

8．4　バイナリデータへのアクセス　　トランスペアレントEF内に格納されている各バイナリデータ(ISO/IEC 7816-4で規定されている“データユニット”に相当する。なお、この規格で規定するデータユニットのサイズは、1バイトとする。)には、相対アドレス(当該EFの先頭データが、アドレス'0000'をもつ)が内部的に付与される。このアドレスと、さらに長さを指定することによって、読出し／書換え対象領域を特定する。

注：Short EF-IDを同時に指定する場合には、指定可能な相対アドレスは'00'～'FF'に制限される(カレントEFにアクセスする場合には、'0000'～'7FFF'の範囲で指定可能となる。)。

9．ロジカルチャネル　　この規格で規定するICカードは、ISO/IEC 7816-4で規定されているロジカルチャネル機能採用する。

なお、この機能の採用に当たって、以下に示す項目を基本機能とする。

(1)チャネルの本数

ロジカルチャネルの本数は、最低2本(即ち、#0,#1)とする。

(2)チャネルの割り当て方法

ATR直後は、少なくともロジカルチャネル#0はMFに割り当てられる。

なお、利便性を考慮し、ロジ　　カルチャネル#1も同時にMFに割り当てられることとする。
また、DF又はEFに対しては、SELECT FILEコマンドを使用してロジカルチャネル#1を割り当てることとする。

(3)チャネルの使用方法
SELECT FILE以外のコマンドにおいては、これをアクセスする際に使用するロジカルチャネル番号をCLA(b2, b1)で指定する。
なお、ATR直後においては、各コマンドにおいて両チャネルが使用可能となる。

１０．個別コマンド　　この項に規定されているコマンドの各機能は、ISO/IEC 7816-4で規定されているInterindustryコマンド機能のミニマムセット、及び同規格で規定されていないもので必要とされる機能である。ただし、その他の機能をサポートすることは制限しないこととする。

(1)コマンド／レスポンスAPDUのフォーマット
各コマンドにおけるコマンド／レスポンスのフォーマットは、ISO/IEC 7816-4で規定されているAPDUフォーマットを採用する。これらのAPDUは、ISO/IEC 7816-4のANNEX Bで規定されるとおり、T=1におけるI-blockのINFORMATION部に相当するものである。
なお、APDUにおけるLc及びLeは、拡張できることとする。
以下に規定するコマンドにおいては、コマンド／レスポンスのフォーマットとしてAPDUのみを記載する。

(2)コマンド／レスポンスAPDUのコーディング
各コマンドにおけるコマンド／レスポンスAPDUのコーディングは、ISO/IEC 7816-4で規定されているコマンドについては、同規格に規定されているコーディングを採用する。
また、同規格に規定されていない一部のコマンドについては、この規格で独自に規定するものである。
なお、各コマンドメッセージ内のCLAバイトの下位ニブルの値については、ISO/IEC 7816-4のCLAコーディング規約を採用し、以下のとおりとする。

b4,3 = "00"…“セキュアメッセージング機能を使用せず”を示す
b2,1 = ロジカルチャネル番号("00"又は"01")

なお、この下位ニブルで指示される他の機能をサポートすることは、この規格では制限しない。
また、CLAの上位ニブルの値についても、ISO/IEC 7816-4のCLAコーディング規約を採用し、以下のとおりとする。

'0X' = ISO/IEC 7816-4で規定されているコマンド
'8X' = ISO/IEC 7816-4で規定されているコマンドではないが、コマンド／レスポンスのフォーマットは当該規格に準拠する

また、上記2種類のコマンド系列に対するステータスコードの値については、ISO/IEC 7816-4を採用する。
なお、この規格では、ステータスコードの意味付けとしてその概要のみを規定し、個々における発生原因、発生(優先)順位等の具体的な規定はしない。

１０．１　READ BINARYコマンド

(1)機能

Short EF-IDで指定したトランスペアレントEF内、又はカレントとなってるトランスペアレントEF内のバイナリデータを、アドレスと長さを指定することによって読出す。

(2)セキュリティ条件

アクセス対象となっているEFに付与されている、読出し関連のアクセス条件を参照する。

(3)コマンドメッセージ

表2.1 READ BINARYコマンドAPDU

CLA	'OX'
INS	'BO'
P1-P2	表10.2のとおり
Lc部	なし
データ部	なし
Le部	読出しデータ長

表2.2 READ BINARYコマンドのP1-P2コーディング

P1								P2	意味付け
b8	7	6	5	4	3	2	1		
0	x	x	x	x	x	x	x	'XX'	相対アドレス(15ビット：'0000'～'7FFF')
1	0	0	x	x	x	x	x	-	Short EF-ID
1	0	0	-	-	-	-	-	'XX'	相対アドレス(8ビット：'00'～'FF')

長さについては、指定長さが1～256バイトの場合、1バイトのLe部でこれを示す('01'～'00'をコーディングする)。

また、1～65,536バイト(実際にはEFサイズが最大値となる)の場合には、3バイトのLe部とし、下位2バイト(上位先順)でこれを示す(上位1バイト目は、'00'固定)。

また、Short EF-ID = "00000"時には、カレントとなっているトランスペアレントEFを参照する。

(4)レスポンスメッセージ

表2.3 READ BINARYレスポンスAPDU

データ部	読出しバイナリデータ
SW1-SW2	ステータスコード

(5)ステータスコード

表2.4 READ BINARY関連ステータスコード

SW1	SW2	意味付け
90	00	正常終了
62	82	条件付き正常終了(指定長さ以下のデータ長)
67	00	Lc/Le異常
68	81	CLA機能異常(ロジカルチャネル未サポート)
	82	〃　(セキュアメッセージング未サポート)
69	81	実行条件異常(ファイル構造不適合)
	82	〃　(アクセス条件不備)
	86	〃　(カレントEF無し)
6A	82	パラメタ異常(該当ファイル無し)
	86	〃　(P1-P2異常)
6B	00	パラメタ異常(アドレス異常)
6D	00	INS異常
6E	00	CLA未サポート

１０．２　READ RECORDコマンド

(1)機能

Short EF-IDで指定したサイクリックEF内、又はカレントサイクリックEF内のレコードを、レコード番号を指定することによって読出す。

(2)セキュリティ条件

アクセス対象となっているEFに付与されている、読出し関連のアクセス条件を参照する。

(3)コマンドメッセージ

表2.5 READ RECORDコマンドAPDU

CLA	'OX'
INS	'B2'
P1	レコード番号
P2	b8-b4 = Short EF-ID, b3,2,1='100'
Lc部	なし
データ部	なし
Le部	'00, 00, 00'

なお、Le部は、読出し対象レコード長に依存しないように、'00 00 00'(固定)とする。
また、Short EF-ID = "00000"時には、カレントサイクリックEFを参照する。

(4)レスポンスメッセージ

表2.6 READ RECORDレスポンスAPDU

データ部	読出しレコード
SW1-SW2	ステータスコード

(5)ステータスコード

表2.7 READ RECORD関連ステータスコード

SW1	SW2	意味付け
90	00	正常終了
62	81	条件付き正常終了(出力データ内異常あり)
67	00	Lc/Le異常
68	81	CLA機能異常(ロジカルチャネル未サポート)
	82	〃　(セキュアメッセージング未サポート)
69	81	実行条件異常(ファイル構造不適合)
	82	〃　(アクセス条件不備)
	86	〃　(カレントEF無し)
6A	81	パラメタ異常(機能未サポート)
	82	〃　(該当ファイル無し)
	83	〃　(該当レコード無し)
	86	〃　(P1-P2異常)
6D	00	INS異常
6E	00	CLA未サポート

１０．３　UPDATE BINARYコマンド

(1)機能

Short EF-IDで指定したトランスペアレントEF内、又はカレントとなってるトランスペアレントEF内の指定したアドレスから、指定した長さ分のバイナリデータを書換える。

(2)セキュリティ条件

アクセス対象となっているEFに付与されている、書換え関連のアクセス条件を参照する。

(3)コマンドメッセージ

表2.8 UPDATE BINARYコマンドAPDU

CLA	'OX'
INS	'D6'
P1-P2	表10.2のとおり
Lc部	データ部長
データ部	書換えバイナリデータ長
Le部	なし

表2.9 UPDATE BINARYコマンドのP1-P2コーディング

P1								P2	意味付け
b8	7	6	5	4	3	2	1		
0	x	x	x	x	x	x	x	'XX'	相対アドレス(15ビット：'0000'～'7FFF')
1	0	0	x	x	x	x	x	-	Short EF-ID
1	0	0	-	-	-	-	-	'XX'	相対アドレス(8ビット：'00'～'FF')

書換えデータ長が1～255バイトの場合、1バイトのLc部でこれを示す。

また、1～65,535バイト(実際にはEFサイズが最大値となる)の場合には、3バイトのLc部とし、下位2バイト(上位先順)にてこれを示す(上位1バイト目は、'00'固定)。

また、Short EF-ID = "00000"時には、カレントトランスペアレントEFを参照する。

(4)レスポンスメッセージ

表2.10 UPDATE BINARYレスポンスAPDU

データ部	なし
SW1-SW2	ステータスコード

(5)ステータスコード

表2.11 UPDATE BINARY関連ステータスコード

SW1	SW2	意味付け
90	00	正常終了
65	81	データ書込み異常
67	00	Lc/Le異常
68	81	CLA機能異常(ロジカルチャネル未サポート)
	82	〃　(セキュアメッセージング未サポート)
69	81	実行条件異常(ファイル構造不適合)
	82	〃　(アクセス条件不備)
	86	〃　(カレントEF無し)
6A	82	パラメタ異常(該当ファイル無し)
	84	〃　(書込みスペース無し)
	86	〃　(P1-P2異常)
6B	00	パラメタ異常(アドレス異常)
6D	00	INS異常
6E	00	CLA未サポート

１０．４　UPDATE RECORDコマンド

(1)機能

Short EF-IDで指定したサイクリックEF内、又はカレントサイクリックEF内のレコードを、レコード番号を指定することによって書換える。

(2)セキュリティ条件

アクセス対象となっているEFに付与されている、書換え関連のアクセス条件を参照する。

(3)コマンドメッセージ

表2.12 UPDATE RECORDコマンドAPDU

CLA	'OX'
INS	'DC'
P1	レコード番号
P2	b8-b4 = Short EF-ID, b3,2,1='100'
Lc部	データ部長
データ部	書換えレコード
Le部	なし

書換えデータ長が1～255バイトの場合、1バイトのLc部でこれを示す。

また、1～65,535バイト(実際にはEFサイズが最大値となる)の場合には、3バイトのLc部とし、下位2バイト(上位先順)にてこれを示す(上位1バイト目は、'00'固定)。

また、Short EF-ID = "00000"時には、カレントサイクリックEFを参照する。

(4)レスポンスメッセージ

表2.13 UPDATE RECORDレスポンスAPDU

データ部	なし
SW1-SW2	ステータスコード

(5)ステータスコード

表2.14 UPDATE RECORD関連ステータスコード

SW1	SW2	意味付け
90	00	正常終了
65	81	メモリ書込み異常
67	00	Lc/Le異常
68	81	CLA機能異常(ロジカルチャネル未サポート)
	82	〃　(セキュアメッセージング未サポート)
69	81	実行条件異常(ファイル構造不適合)
	82	〃　(アクセス条件不備)
	86	〃　(カレントEF無し)
6A	81	パラメタ異常(機能未サポート)
	82	〃　(該当ファイル無し)
	83	〃　(該当レコード無し)
	84	〃　(書込みスペース無し)
	85	〃　(LcとTLV構造との不整合)
	86	〃　(P1-P2異常)
6D	00	INS異常
6E	00	CLA未サポート

１０．５　APPEND RECORDコマンド

(1)機能

Short EF-IDで指定したサイクリックEF内、またはカレントサイクリックEF内に、レコードを追記する。追記したレコードはレコード#1となる。特に、EF内にレコードがいっぱいになっていた場合には、最旧レコードが消去され、入力されたレコードが追記される(6.3参照のこと)。

(2)セキュリティ条件

アクセス対象となっているEFに付与されている、書換え関連のアクセス条件を参照する。

(3)コマンドメッセージ

表2.15 APPEND RECORDコマンドAPDU

CLA	'OX'
INS	'E2'
P1	'00'
P2	b8-b4 = Short EF-ID, b3,2,1='000'
Lc部	データ部長
データ部	追記レコード
Le部	なし

書換えデータ長が1～255バイトの場合、1バイトのLc部でこれを示す。また1～64キロバイト(実際にはEFサイズが最大値となる)の場合には、3バイトのLc部とし、下位2バイト(上位先順)でれを示す(上位1バイト目は、'00'固定)。

また、Short EF-ID = "00000"時には、カレントレコードEFを参照する。

(4)レスポンスメッセージ

表2.16 APPEND RECORDレスポンスAPDU

データ部	なし
SW1-SW2	ステータスコード

(5)ステータスコード

表2.17 APPEND RECORD関連ステータスコード

SW1	SW2	意味付け
90	00	正常終了
65	81	メモリ書込み異常
67	00	Lc/Le異常
68	81	CLA機能異常(ロジカルチャネル未サポート)
	82	〃　(セキュアメッセージング未サポート)
69	81	実行条件異常(ファイル構造不適合)
	82	〃　(アクセス条件不備)
	86	〃　(カレントEF無し)
6A	82	パラメタ異常(該当ファイル無し)
	84	〃　(書込みスペース無し)
	85	〃　(LcとTLV構造との不整合)
	86	〃　(P1-P2異常)
6D	00	INS異常
6E	00	CLA未サポート

１０．６　SELECT FILEコマンド

(1)機能

DF名を指定することによって、アクセス対象とするDFをカレント状態にし、ロジカルチャネルを割り当てる。又は、EF-IDを指定することによって、対象とするカレントDF又はMF配下のEFをカレント状態にする。

注：アンサートゥリセット直後は、MFが暗黙的にカレント状態となっており、ロジカルチャネル#0及び#1が割り当てられている。
注：割り当てるべきロジカル番号は、このコマンドのCLAで指定する。
注：あるロジカルチャネルに対するカレントDFを変更する場合には、前のDFはカレントDFでなくなる。

(2)セキュリティ条件

フリーとする。

(3)コマンドメッセージ

表2.18 SELECT FILEコマンドAPDU

CLA	'OX'
INS	'A4'
P1	DF選択時には'04', EF選択時には'02'
P2	'OC'
Lc部	データ部長(DF選択時は'01'～'10', EF選択時は'02')
データ部	DF選択時はDF名, EF選択時はEF-ID
Le部	なし

(4)レスポンスメッセージ

表2.19 SELECT FILEレスポンスAPDU

データ部	なし
SW1-SW2	ステータスコード

(5)ステータスコード

表2.20 SELECT FILE関連ステータスコード

SW1	SW2	意味付け
90	00	正常終了
67	00	Lc/Le異常
68	81	CLA機能異常(ロジカルチャネル未サポート)
	82	〃　(セキュアメッセージング未サポート)
6A	81	パラメタ異常(機能未サポート)
	82	〃　(該当ファイル無し)
	86	〃　(P1-P2異常)
6D	00	INS異常
6E	00	CLA未サポート

１０．７　VERIFYコマンド

(1)機能

Short EF-IDで指定したキーEF内、又はカレントキーEF内のPIN(パスワード)と、入力したPIN(パスワード)とを照合し照合状態を確立する。

注：照合不一致となった場合には、それの痕跡を記憶する(11.4参照のこと)。

(2)セキュリティ条件

フリーとする。

(3)コマンドメッセージ

表2.21 VERIFYコマンドAPDU

CLA	'OX'
INS	'20'
P1	'00'
P2	b8,7,6 = '100', b5-b1 = Short EF-ID
Lc部	データ部長('01'～'10')
データ部	PIN(パスワード)
Le部	なし

Short EF-ID = "00000"時には、カレントキーEFを参照する。

(4)レスポンスメッセージ

表2.22 VERIFYレスポンスAPDU

データ部	なし
SW1-SW2	ステータスコード

(5)ステータスコード

表2.23 VERIFY関連ステータスコード

SW1	SW2	意味付け
90	00	正常終了
63	00	ウォーニング(照合エラー)
65	81	メモリ書込み異常
67	00	Lc/Le異常
68	81	CLA機能異常(ロジカルチャネル未サポート)
	82	〃　(セキュアメッセージング未サポート)
69	84	実行条件異常(キーロック済み)
	86	〃　(カレントEF無し)
6A	81	パラメタ異常(機能未サポート)
	82	〃　(該当ファイル無し)
	86	〃　(P1-P2異常)
6D	00	INS異常
6E	00	CLA未サポート

１０．８　INTERNAL AUTHENTICATEコマンド

(1)機能

Short EF-IDで指定したキーEF内、又はカレントキーEF内のキーを使用して、入力したチャレンジデータを暗号化し(カード認証コードを生成)、結果を出力する。同コードによって、カード又はアプリケーションの正当性をチェックする。

カードの正当性確認のためにMF直下のキーを、また、アプリケーションの正当性確認のためにDF直下のキーを、それぞれ対象にする。

(2)セキュリティ条件

フリーとする。

(3)コマンドメッセージ

表2.24 INTERNAL AUTHENTICATEコマンドAPDU

CLA	'0X'
INS	'88'
P1	'00'
P2	b8,7,6 = '100', b5-b1 = Short EF-ID
Lc部	データ部長('08')
データ部	チャレンジ
Le部	'08'

Short EF-ID = "00000"時には、カレントキーEFを参照する。

(4)レスポンスメッセージ

表2.25 INTERNAL AUTHENTICATEレスポンスAPDU

データ部	カード認証コード
SW1-SW2	ステータスコード

(5)ステータスコード

表2.26 INTERNAL AUTHENTICATE関連ステータスコード

SW1	SW2	意味付け
90	00	正常終了
67	00	Lc/Le異常
68	81	CLA機能異常(ロジカルチャネル未サポート)
	82	〃　(セキュアメッセージング未サポート)
69	84	実行条件異常(キーロック済み)
	86	〃　(カレントEF無し)
6A	81	パラメタ異常(機能未サポート)
	82	〃　(該当ファイル無し)
	86	〃　(P1-P2異常)
6D	00	INS異常
6E	00	CLA未サポート

１０．９　EXTERNAL AUTHENTICATEコマンド

(1)機能

Short EF-IDで指定したキーEF、又はカレントキーEF内のキーを使用して、内部に保持されているチャレンジデータを暗号化した結果と、入力したIFD認証コードとを比較する。これによって、認証(照合)状態を確立する(11.5.3参照のこと)。

なお、このコマンドで使用するチャレンジデータは、このコマンド実行直前に実行された(つまり、複数回実行されたもののうち最終のもの)GET CHALLENGEコマンドで出力したものが使用される。

注：照合不一致となった場合には、それの痕跡を記憶する(11.4参照のこと)。

(2)セキュリティ条件

フリーとする。

(3)コマンドメッセージ

表2.27 EXTERNAL AUTHENTICATEコマンドAPDU

CLA	'OX'
INS	'82'
P1	'00'
P2	b8,7,6 = '100', b5-b1 = Short EF-ID
Lc部	データ部長('08')
データ部	IFD認証コード
Le部	なし

Short EF-ID = "00000"時には、カレントキーEFを参照する。

(4)レスポンスメッセージ

表2.28 EXTERNAL AUTHENTICATEレスポンスAPDU

データ部	なし
SW1-SW2	ステータスコード

(5)ステータスコード

表2.29 EXTERNAL AUTHENTICATE関連ステータスコード

SW1	SW2	意味付け
90	00	正常終了
63	00	ウォーニング(照合エラー)
65	81	メモリ書込み異常
67	00	Lc/Le異常
68	81	CLA機能異常(ロジカルチャネル未サポート)
	82	〃　(セキュアメッセージング未サポート)
69	84	実行条件異常(キーロック済み)
	86	〃　(カレントEF無し)
6A	81	パラメタ異常(機能未サポート)
	82	〃　(該当ファイル無し)
	86	〃　(P1-P2異常)
6D	00	INS異常
6E	00	CLA未サポート

１０．１０　GET CHALLENGEコマンド

(1)機能
　乱数(チャレンジデータ)をカード内部で生成し、これを出力する。

(2)セキュリティ条件
　フリーとする。

(3)コマンドメッセージ

表2.30 GET CHALLENGEコマンドAPDU

CLA	'0X'
INS	'84'
P1	'00'
P2	'00'
Lc部	なし
データ部	なし
Le部	'08'

(4)レスポンスメッセージ

表2.31 GET CHALLENGEレスポンスAPDU

データ部	乱数(チャレンジデータ)
SW1-SW2	ステータスコード

(5)ステータスコード

表2.32 GET CHALLENGE関連ステータスコード

SW1	SW2	意味付け
90	00	正常終了
65	81	メモリ書込み異常
67	00	Lc/Le異常
68	81	CLA機能異常(ロジカルチャネル未サポート)
	82	〃　(セキュアメッセージング未サポート)
6A	86	パラメタ異常(P1-P2異常)
6D	00	INS異常
6E	00	CLA未サポート

１０．１１　CHANGE PINコマンド

このコマンドは、ISO/IEC 7816-4で規定されていないコマンドであり、今後の動向によっては、“エンハンストコマンド”という位置付けで国際標準化される可能性がある。

(1)機能

Short EF-IDで指定したキーEF、又はカレントキーEF内に格納されているPIN(パスワード)を、入力した新規PIN(パスワード)に変更する。

(2)セキュリティ条件

アクセス対象となっているEFに付与されている、書換え関連のアクセス条件を参照する。

(3)コマンドメッセージ

表2.33 CHANGE PINコマンドAPDU

CLA	'8X'
INS	'32'
P1	'00'
P2	b8,7,6 = '100', b5-b1 = Short EF-ID
Lc部	データ部長('01'～'10')
データ部	PIN(パスワード)
Le部	なし

Short EF-ID = "00000"時には、カレントキーEFを参照する。

(4)レスポンスメッセージ

表2.34 CHANGE PINレスポンスAPDU

データ部	なし
SW1-SW2	ステータスコード

(5)ステータスコード

表2.35 CHANGE PIN関連ステータスコード

SW1	SW2	意味付け
90	00	正常終了
65	81	メモリ書込み異常
67	00	Lc/Le異常
68	81	CLA機能異常(ロジカルチャネル未サポート)
	82	〃　(セキュアメッセージング未サポート)
69	82	実行条件異常(アクセス条件不備)
	86	〃　(カレントEF無し)
6A	82	パラメタ異常(該当ファイル無し)
	86	〃　(P1-P2異常)
6D	00	INS異常
6E	00	CLA未サポート

１１．セキュリティ管理

１１．１　アクセス条件とキーの照合状態　　アクセス条件とは、個々のEFに対し、誰が(どの当事者が)又はどのノードが指定コマンドを実行できるかを規定したものである(この条件の設定は、カード初期発行時に発行者によって設定される)。このアクセス条件は、当事者のキー(PIN又はパスワード)及びノードキー(端末等が所有するキー)の組合せ情報によって構成される。

EFBごとに異なるアクセス条件を設定することによって、アクセス当事者及びアクセスノードの限定がEFごとに可能となる。

一方キーの照合状態とは、VERIFYコマンド又はEXTERNAL AUTHENTICATEコマンドの結果、現在どのキーが照合済み(又は認証済み)であるかを示した情報である。この情報はICカード内のRAMに保持されており、アクセスコマンドが入力される度に前述したアクセス条件と比較することによって、アクセスの可否を判定する。

１１．２　アクセス条件の種類　　ICカード内の各ファイルには、コマンドのアクセス種別によって、異なるアクセス条件を設定できる。アクセス種別とは、カードに対してアクセスするコマンドの機能を分類したものである。

この規格で規定するICカードは、各ファイルに対し、以下のアクセス種別ごとのアクセス条件を設定できることとする。

データEF　：読出し系、及び書換え系
キーEF　　：書換え系、及びロック解除系

また、各アクセス条件情報として、7種のアクセスキーの組合せ(OR条件)、及びキーの照合を必要としない“フリーアクセス”条件の設定を可能とする。

なお、パスワードとして、MF配下のパスワード及びDF配下のパスワードを合計して、8個を登録可能なこととする。

１１．３　照合状態の遷移　　この規格で規定するICカードは、2つ以上のロジカルチャネルをサポートすることになるが、各々のロジカルチャネルにおいては、ISO/IEC 7816-4に従い、以下に示す“照合状態の遷移”に関する規則を実現可能なこととする。

なお、この規則におけるDFは、MF直下に存在するDFのみを対象とする。したがって、DF配下の子DF等に関わる照合状態の遷移の規則については、この規格の適用範囲外である。

規則1：前回のカレントDFと同一のDFを選択した場合には、前回のカレントDF固有の照合状態は維持される。
規則2：前回のカレントDFと別のDFを選択した場合には、前回のカレントDF固有の照合状態は失われる。
規則3：MFにおける照合状態は、維持される。
規則4：カードに対し電気的非活性化又はリセットが行われると、全ての照合状態は失われる。

照合状態は、上記の規則にしたがって各ロジカルチャネルごとに管理される。

なお、コマンドアクセス時に照合状態を参照する場合には、ISO/IEC 7816-4で許容する“照合状態の共有”の概念を採用する。

この照合状態の共有とは、一方のロジカルチャネルで獲得した照合状態を、他方ロジカルチャネルでアクセスした時点で参照することである(もちろん自身で獲得した照合状態も、同時に参照する)。

例えば、カードの状態が図4に示すようになっているとする。

図4　照合状態の共有

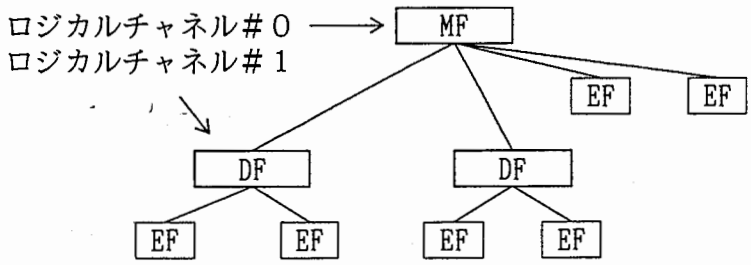


図4に示す状態では、MF配下のEFに対してはロジカルチャネル#0が、また、DF配下のEFに対してはロジカルチャネル#1が、それぞれのアクセスに使用される。

さて、この状態でロジカルチャネル#0を使用して、図4中キーAを照合すると、この照合状態は当該チャネルが獲得したものとなる。そしてこの後、ロジカルチャネル#1を使用してDF配下のEFをアクセスする場合には、照合状態の共有が行なわれ、結果的にキーAの照合結果を参照することになる。

また、この状態でロジカルチャネル#1を使用して、図4中キーBを照合すると、この照合状態は当該チャネルが獲得したものとなる。そしてこの後、ロジカルチャネル#0を使用してMF配下のEFをアクセスする場合には、同様に照合状態の共有が行われ、結果的にキーBの照合結果を参照することになる。

つまり照合状態の共有は、一般的に以下の規則にしたがってなされる。

規則1：アクセスに使用するロジカルチャネルがMFに割り当てられている場合、他のロジカルチャネルが獲得した照合状態を共有する。

規則2：アクセスに使用するロジカルチャネルがDFに割り当てられている場合、ロジカルチャネルが獲得した照合状態のうち、共有されているファイル配下のキーの照合状態を共有する。

なおこの規格で規定されるICカードにおいては、これがサポートするロジカルチャネルを使用する場合、ロジカルチャネル#0をMF配下のアクセスのために固定的に使用する。したがって、各チャネルが獲得した照合状態は、いかなる場合においても共有されることになる。

１１．４　パスワードの自動ロック機能

VERIFYコマンドを使用することによるパスワードの不正試行によって、当該パスワードが解析されるのを防止するため、パスワードの不正試行による自動ロック機能をサポートすることとする。

自動ロック機能は、VERIFYコマンドによってパスワード照合異常となった回数をカード内部で自動的に記憶し、所定の上限値に達したことを検出すると、以降の照合処理が行なえないようにすることで達成される。

この機能に関し、少なくとも以下に示す要件を満足すること。

(1)不正試行回数の計数は、各パスワードごとに独立して行える。
(2)正常な照合処理が行われた場合、対象となるパスワードに対応する不正試行回数がクリアされる。
(3)各パスワードに対し、不正試行回数の上限値を設定できること。
(4)設定上限値としては、1～15回目の範囲で任意にロックが行われるよう設定可能とすること(n回目と指定した場合には、n回目の不正使用時に当該PINがロックされることを示す)。さらに、無制限を設定可能とする。

なお、ロックされる前後の、照合不一致を示すステータスコードは、以下のとおりとする。

ロック前：'6300'ロック後：'6984'

例：3回目でロックが行われるように設定した場合、
1回目の不当PIN入力→ステータスコード'6300'

2回目の　〃　→　〃　'6300'
3回目の　〃　→　〃　'6984'

(5)不正試行回数は、カードの電気的非活性化によって変化しないこと。

なお、これらの諸機能は、EXTERNAL AUTHENTICATEコマンドで外部認証を行う際に使用されるキーに対しても、同様に実現できること。

１１．５　暗号化機能について　この規格で規定する暗号化機能は、外部装置によるICカード認証（INTERNAL AUTHENTICATEコマンド）及びICカードによる外部装置認証（EXTERNAL AUTHENTICATEコマンド）の認証処理に使用される。使用される暗号アルゴリズムは、DES（ANSI X3.92)を採用する。
なお、外部装置におけるキーデータの管理については、この規格の適用範囲外である。

１２．特記事項　以下に、この規格で特記すべき事項を示す。

１２．１　基本ファイルフォーマット　附属書Bに示すファイルフォーマットを基本ファイルフォーマットとし、ICカード内のメモリに構築可能なこととする。

１２．２　その他の機能　この規格で規定される諸機能のほかに、以下の機能をサポートすること。
・PIN(パスワード)のロック解除機能
・ファイルの再編成機能
なお、これらの機能は、発行者の権限のみによって使用されるものである。したがって、セキュリティ上の理由によって、この規格では規定しない。

附属書 A　T=1プロトコル基本仕様(規定)

A.1　伝送マトリクス(T=1プロトコル)

この規格で規定するICカードは、前述したように、JIS X 6304で規定されているT=1プロトコルを採用している。この規格を採用するに当たっては、1.6.1で記述した機能を必須項目とする。

以下に、T=1プロトコルでの伝送マトリクスを示す。

附属書表1.1 T=1プロトコル伝送マトリクス

ｲﾍﾞﾝﾄ / ｽﾃｰﾀｽ	I-block			R-block		ｴﾗｰﾌﾞﾛｯｸ入力	
	継続無し I(S,0) 受信	継続あり I(S,1) 受信	異常ﾌﾞﾛｯｸ 受信	R(S)受信	異常block 受信	ｴﾗｰ電文 受信	異常NAD 電文受
1.ﾌﾟﾛﾄｺﾙ開始後 I-block待ち	Sub1	Don't care	R(s=0)送信 →1	←	←	←	(無応答)
2. 継続無しI(s,0) 送信後ﾌﾞﾛｯｸ待ち	Sub1	Don't care	R(s)送信 →2	S=s:I(s,0) 再送→2 S=s':R(s) 送信→2	R(s)送信 →2	←	(無応答)
3. 継続ありI(s,1) 送信後ﾌﾞﾛｯｸ待ち	R(s)送信 →3	Don't care	R(s)送信 →3	S=s:I(s,1) 再送→2 S=s': →Sub1	R(s)送信 →3	←	(無応答)

附属書表1.2 T=1プロトコル伝送マトリクス

ｲﾍﾞﾝﾄ / ｽﾃｰﾀｽ	S-block				
	S(RES req) 受信	S(IFS req) 受信	S(ABT req) 受信	他の定義 S-block受信	異常block 受信
1.ﾌﾟﾛﾄｺﾙ開始後 I-block待ち	S(RES res) 送信→1	S(IFS res) 送信→1	S(ABT res) 送信→1	Don't care	R(0)送信 →1
2. 継続無しI(s,0) 送信後ﾌﾞﾛｯｸ待ち	S(RES res) 送信→1	S(IFS res) 送信→2	S(ABT res) 送信→2	Don't care	R(s)送信 →2
3. 継続無しI(s,0) 送信後ﾌﾞﾛｯｸ待ち	S(RES res) 送信→1	S(IFS res) 送信→3	S(ABT res) 送信→2	Don't care	R(s)送信 →3

Sub1:内部処理　　注：s'は，sの値を反転したもの

(1)継続処理完結時→I(s,0)送信→2

(2)継続ﾌﾞﾛｯｸ存在→I(s,1)送信→3

なお、表中の"Don't care"は、対応するイベント自体がオプションであることによって、カードごとに処理が異なることを示す。したがって、処理内容／応答ブロックの詳細については、この規格では規定しない。

また、JIS X 6304に従い、表中のR-block(異常ステータス表示付き)送信を連続2回行った場合には、次のR-block(異常ステータス表示付き)送信タイミング時にレスポンスを応答せずに、ブロック入力待ち状態になる。

A.2　異常電文の定義

第A.1表に示した、伝送マトリクスのイベントとして想定する異常電文の定義は、I-block、R-block、及びS-blockに共通して、JIS X 6304で規定される以下の定義を採用する。

(1)ブロック内の一つ以上のキャラクタにパリティ誤りがあるとき、又はEDC誤りがあるとき

(2)無効PCB(未知のコーディングのPCB)を受信したとき
(3)無効LEN(伝送誤り、又はLENの値がIFSC若しくはIFSDに適合しない。)を受信したとき
(4)同期はずれ(アンダーラン)のとき
　アンダーラン：受信したLENに示された数のキャラクタを受信できないとき

また、以下の場合を異常電文として追加する。

(5)ブロック長が3バイト以下のとき
(6)受信したブロックのNADが以下の状態の場合：
－b8及びb4が、共に"0"でなかった
－SAD及びDADが同一値であった(ただし、SAD=DAD=0は除く)
(7)R-block/S(RESYNC req)-block/S(ABORT req)のLENの値が、'00'以外であった。
(8)S(IFS req)-blockのLENの値が、'01'以外であった。

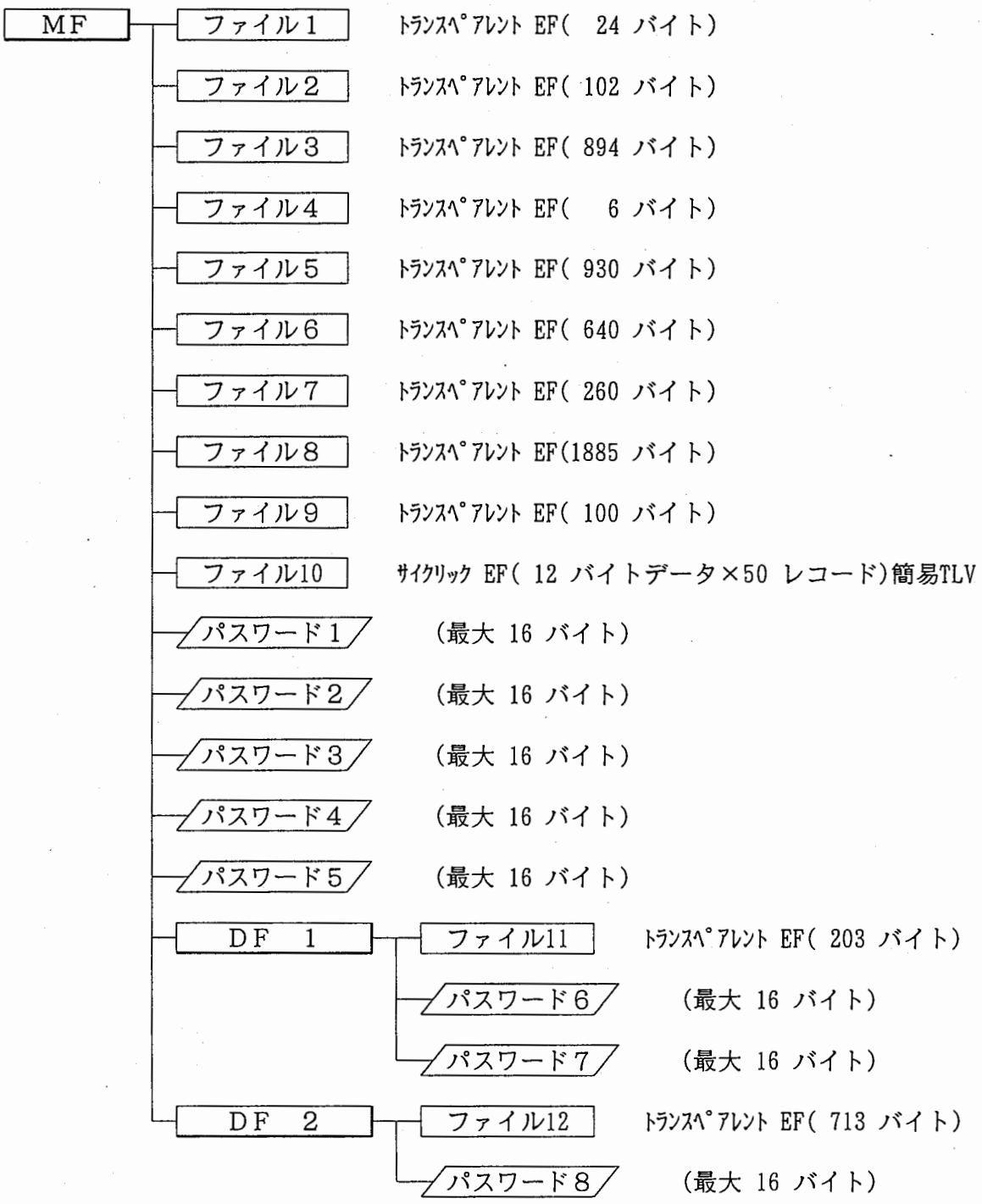
A.3　プロトコル上のその他の規定
T=1プロトコルを実施するに当たっては、以下の項目を必須とする。

(1) ICカードからブロックを送信する場合、NADのb8及びb4は"0"(固定)とする。
(2)IFDから送信されるブロックのNADが以下の状態のとき、異常NAD電文と判断し、ICカードは無応答と　なる。
－自身のアドレス値を、DADとしてもっていない。
－NADにパリティ誤りが検出された

附属書 B　基本ファイルフォーマット(規定)

この規格で規定するICカード内のメモリに構築すべき、ファイルの基本フォーマットを附属書図1に示す。なお、各ＥＦ内のデータのフォーマットについては、別途定めることとし、この規格では規定しない。

附属書図1　基本ファイルフォーマット



建設標準ＩＣカードの機能仕様解説

この解説は、本体に規定した事柄、附属書に記載した事柄及びこれらに関連した事柄を説明するもので、この規格の一部ではない。

１．規格制定の背景　　建設施工現場では、施工方法や施工資機材の多様化、品質管理の高度化が進んでいる。このため、機械・品質・出来形・資材・労務・安全等の管理に多くの情報が発生し、この処理に多くの労力を要しており、その省力化・迅速化が必要とされている。

そこで、省力化・迅速化するために情報媒体として磁気ストライプカード、メモリカード、バーコードカード、ICカードなどさまざまな種類のデータキャリアが試行され、これらの中より、情報記憶容量、さまざまな情報を管理するための独立した複数のファイル化、及び各情報に対するセキュリティ確保の点でICカードが利用され始めているが、既存のICカードは互換性がなく、互換の情報交換・伝達も困難なものとなっていた。

よって、建設事業において、共通に利用可能なICカードを提供することを目的とし、この機能仕様を規格化することとした。

なお、この規格で規定する諸特性／諸機能は、利用場面において使用される機能のみを規定したミニマム仕様として位置付けられるものである。したがって、これらに加えて、他の機能をサポートするICカードを排除するものではない。

１．１　規格制定の経過　　（社）日本建設機械化協会では、昭和63年度から「建設工事情報化委員会」を設置し、建設施工現場の情報管理の高度化手法に関する研究を行ってきた。

また、平成4年度から建設事業へICカードによる施工情報システムを普及させることを目的に、官民連帯共同研究会を発足し、３ヶ年（平成4年4月～平成6年3月）の活動を通して建設ICカード機能仕様の標準化（案）を作成した。この標準化（案）の検討に当たっては、建設業界のアプリケーションを想定し、また考慮して、国際標準（ISO）規格及び国内標準（JIS）規格に準拠した建設ICカード標準機能仕様（案）とした。これらの成果を受けて、（社）日本建設機械化協会内の情報化委員会においてこの規格を定めることとした。

１．２　この規格の位置づけ　　ICカードはセキュリティ機能が高く、多目的に利用してもセキュリティが保たれる。免許・資格などは発行主体別にパスワードを設定することも可能である。しかし、多くの発行主体を許容するとそれなりの記憶容量を必要とし、実際にユーザが利用できる記憶容量が減少する。この間でバランスを取るために、次の2段階でICカードの機能仕様を作成することとした。この規格は、前者である。

(1)利用者を7種の区分に限定して設定し、免許に関するセキュリティを少し低減させる。現行の8キロバイトのICカードに合わせたICカードに適した利用方法である。

(2)利用者の区分を事実上無制限とし、免許に関しては免許発行主体しか書込ができないようにする。この方式は現行のICカードでは実現不可能であり、今後の技術開発を待つところが大きい。今後、数年後の実現に向けて規格を作成する。

これら両規格の差はパスワードの数であり、他の機能に差はない。アプリケーションの利用上も免許・資格へのアクセス方法が変わるだけで、両方式のICカードの混在もアプリケーションで対応できると考えられる。

また、ICカードのメモリにセキュリティに関する情報を記録したり、メモリを各情報ごとにファイルとして分割するなどの発行に関する機能、及びICカードのメモリに構築される各ファイルのアクセス条件や格納データフォーマット／内容とICカード発行義務に関する情報については、（社）日本建設機械化協会において、別途定めることとし、この規格では規定しない。

２．機能仕様の概要　　ICカードの内部処理及びファイルへのデータ記憶の効率化、やファイルのセキュリティを考慮し、標準仕様として採用した機能の概要について説明する。

２．１　ICカードの内部処理の効率化　　作業所、通門、車載等のアプリケーション処理を速くするために、ICカード内部の処理を効率良く行うことを目的とし、以下のような機能選択を行った。

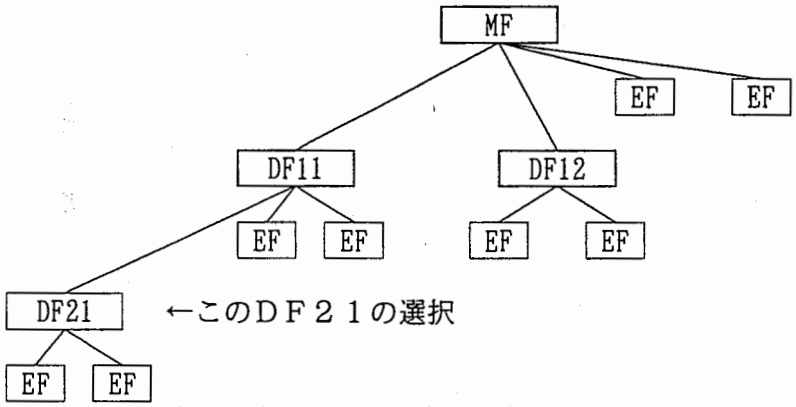
２．１．１　通信効率の向上　　日本国内では、キャラクタ伝送プロトコルよりも伝送効率と誤り処理が優れているブロック伝送プロトコルが主に従来からICカードの仕様に採用されて来ている。
　また、ISO規格として、キャラクタ伝送プロトコル（T=0）、ブロック伝送プロトコル（T=1）がIS化され、国内でのさまざまな業態でもブロック伝送プロトコル（T=1）を採用しようとしている。したがって、建設標準ICカードでは、高速通信が望まれているため、また、他の業態の動向を考慮して、ブロック伝送プロトコル（T=1）を採用した。

２．１．２　ファイルの階層化　　ファイルの階層化は、ファイル管理の容易さとファイル選択の効率化を図るためにMF（Master file）の配下に1階層のDF（Dedicated file）をもつことを必須とした。
　例えば、パソコンでデータの管理を行うときに、あるディレクトリを生成してそのディレクトリに関係するデータファイルをその配下に置くのと同様に、ＩＣカード内で車載のディレクトリ（ＩＣカードではＤＦに当る）を生成してその配下で専任者情報、稼働履歴情報等のファイルを管理することが可能となる。

２．１．３　ICカード内部アクセス処理の効率化

(1)DFの選択はDF名によるダイレクトセレクション
　DFの選択は、DF名によってDFの位置が物理的にICカード内のどこにあっても速やかに選択できるダイレクトセレクションを採用した。
　例えば、解説図1のようなファイル構造がある場合にＤＦ２１を選択するとすると、パソコンではＤＦ１１→ＤＦ２１と順に選択する必要があるが、ＩＣカードではＤＦ２１をSELECT FILEコマンドで選択することでアクセスが可能となる。ただし、この機能仕様は、ミニマム仕様としたためMFを含めて２階層を必須としているので、将来の機能拡張を鑑み採用している。

解説図1　ファイル構造



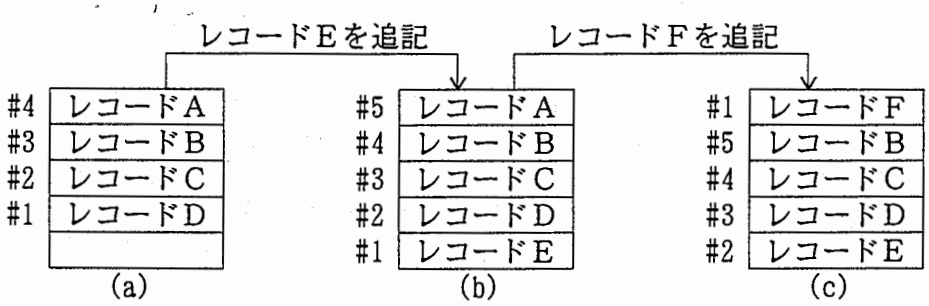
注：MF(Master File), DF(Dedicated File), EF(Elementary File)

　また、DF名は、将来国内で登録されたAID（Application ID）を使用することで、他フィールドのICカードアプリケーションと重複する事故を防ぐばかりでなく、データ交換を可能とする道を開くものである。
　ISO規格では、ダイレクトセレクションの他にファイルID（ショートEFIDを含む）、パスリスト（MF又はカレント（その時点で選択されている）DFから目的ファイルまでのファイルIDの羅列）、暗黙的セレクション（アンサートゥリセットのあとで、自動的に指定ファイルが選択される）などがあるが、前述の実用性を考慮した。

(2)サイクリックEF（Elementary file）へのアクセス
　ファイルのどこにあってもアクセススピードの変動が少なく、取扱いが容易なレコード番号によるアクセス可能なレコードファイルを採用した。
　データ数の種類が固定しており、定期的に記録する必要のあるデータを記憶する。建設業従事者が持つICカードでは、入退情報の記録に採用している。ICカードへのデータの記録には、記憶

容量との兼ね合いで限界があり、レコードデータの追記によってファイルがいっぱいになると最旧データが上書きされるサイクリックEFを採用した。

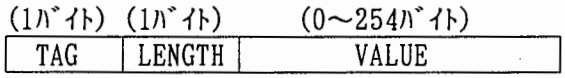
解説図2　レコード番号の付与方法



ISO規格では、レコード番号によるアクセスとレコードIDによるアクセスがあるが、後者によるアクセス処理は、前者よりも複雑であることから省略した。ファイル内のすべてのレコードデータを読出すファイルオールリードも同様な理由によって、この規格外とした。

レコードは、T（TAG:レコードID），L（LENGTH:レコードデータ長），V（VALUE:レコードデータ）で構成される簡易TLV方式を採用した。実際には、この仕様にレコードIDによるアクセスは無いので、TLV構造は必要ないと思われるが、アプリケーションでレコードデータをすべて読出した場合に、例えば、入退記録情報にどの現場での記録か識別するための識別子データとして付加することで情報の整理が容易となる。

解説図3　簡易TLVの構成



(3)二つのロジカルチャネル

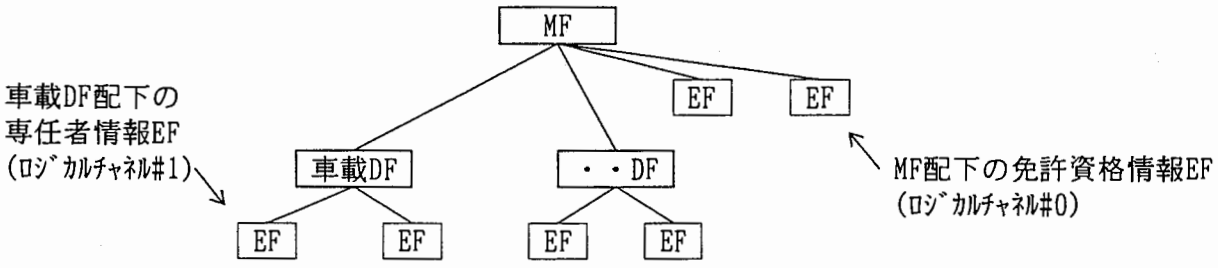
MF配下のEFとDF配下のEFとのデータをSELECT FILEコマンドを介さないでアクセス可能とするので処理効率が向上する。

建設用ICカードでは、二つのロジカルチャネルをもち、チャネル0をMFに固定し、チャネル1をSELECT FILEコマンドで選択したDFにアサインすることを可能とした。その後は、端末側からREAD/WRITE系コマンドを発行するときに、対象となるロジカルチャネルを指定すれば双方配下のEF内のデータを自由にアクセスすることが可能である。

この機能は、例えば、車載情報DF内の専任者情報データをアクセスしているときに、MFの免許資格データを必要とする場合等、同時に二つのファイルをカレント状態とすることができるので有効である。

ISO規格では、最大四つのロジカルチャネルまで設定可能であるが、現状のICカードのCPU及びRAMとの兼ね合いで実用的に二つのロジカルチャネルとした。

解説図4　ロジカルチャネルの設定方法



注：MF(Master File)，DF(Dedicated File)，EF(Elementary File)

２．１．４　ショートEF-IDによるEFの選択　　読み書き処理速度向上のために、EF選択機能（ショートEFIDによるEF指定）と読取り機能又は、書込み機能を一つのコマンドとする方式を採用した（ただし、レコードファイルへのアクセスではレコード番号１～２５５まで、またバイナリファイルではファイルの先頭から相対アドレス１～２５５までの範囲で処理が可能）。

また、PIN（パスワード),/KEY（鍵）データ比較処理速度の向上のために、前述のショートEFIDと同様に、PIN/KEYの格納場所の指定とチェック機能を一つのコマンドで行う方式を採用した。

- VERIFY（パスワードのチェック機能）
- INTERNAL AUTHENTICATION（ICカードの真偽性チェック又は、アプリケーションファイルの真偽性チェック）
- EXTERNAL AUTHENTICATION（端末の真偽性チェック又は、ホストコンピュータの真偽性チェック）

２．２　ICカードのファイルへのデータ記憶の効率化　　多くのデータを記憶可能とするため、ICカードのファイルはその目的に応じて各種のデータを効率良く記憶できるように、ファイル形式の一つとしてトランスペアレントファイルを選択した。

２．２．１　トランスペアレントファイル（バイナリファイル）　　レコードファイルへのアクセスに比べると処理速度はやや落ちるが、データ長の異なった様々なデータを限られたICカードのファイルに効率良く記憶するには、トランスペアレントファイルが有効である。

トランスペアレントのファイルは、各ファイルごとに1番地から始まる番地指定によってアクセスする。データを読出すときには、その番地と必要なデータ数を指定し、また、データを書込むときには、その番地と書込みデータを指定することで処理が行われる。

レコードファイルとトランスペアレントファイルは、1枚のICカードの中に混在することが可能である。

２．３　ICカード内のファイルセキュリティの確保　　ICカード内のファイルセキュリティの確保のため、以下のような機能を採用した。

２．３．１　アクセス条件の種類とアクセスキーの組合せについて　　この規格では、カードに対してアクセスするコマンドの機能を分類したアクセス種別として、各ファイルに対し、以下のアクセス種別ごとのアクセス条件を設定が可能である。

解説表1　各EFのアクセス種別

ファイル	アクセス種別
データEF	読出し系、及び書換え系
キーEF	書換え系、及びロック解除系

なお、キーEFに設定可能なロック解除系については、パスワードのロック解除機能を想定したものであり、この規格では、その機能の詳細については、規定しない。

解説表2　各コマンドのアクセス種別

コマンド名及び機能	アクセス種別		
	読出し系	書換え系	ロック解除系
READ BINARY	○		
UPDATE BINARY		○	
READ RECORD(S)	○		
APPEND RECORD		○	
UPDATE RECORD		○	
SELECT FILE			
VERIFY			
INTERNAL AUTHENTICATE			
EXTERNAL AUTHENTICATE			
GET CHALLENGE			
CHANGE PIN		○	
ロック解除機能			○

○：アクセス条件が設定可能なアクセス条件（空欄は、設定不可）

また、各アクセス条件情報として、7種のアクセスキーの組合せ(OR条件)、及びキーの照合を必要としない“フリーアクセス”条件の設定を可能とする。

例えば、7種すべてのアクセスキーを設定する場合には、解説表3のように設定が可能であり、また、書換え系、ロック解除系にも同様な設定がなされることとなる。この場合に、発行者パスワード、所持者パスワード、作業所パスワード、通門パスワード、免許パスワード、車載パスワードと建退共パスワード（「建退共」とは、(特)建設業・清酒製造業・林業退職金共済組合を略したものであり、以下「建退共」という。）の7種7個のパスワード、又は、発行者パスワード、所持者パスワード、作業所パスワード、通門パスワード、免許パスワード、車載パスワードと建退共のアクセスキーをEXTERNAL AUTHNTICATEコマンドの照合によるものとペアとなるINTERNAL AUTHNTICATEコマンド用のパスワードも必要となり、パスワードは7種8個となる。

解説表3　各アクセス種別のアクセス条件の設定例

読出し系						
発行者	所持者	作業所	通門	免許	車載	建退共

なお、パスワードとして、MF配下のパスワード及びDF配下のパスワードを合計して、8個を登録可能なこととする。したがって、この規格の規定では、EXTERNAL AUTHNTICATE、INTERNAL AUTHNTICATEコマンドを使用するものを一組設定すると、アクセスキー7種、パスワード8個が最大となる。

２．３．２　ファイルセキュリティの独立性とファイル間で共有されるセキュリティ　　個人情報、免許資格情報、車載情報等のICカード内ファイルのアプリケーション提供者が異なる場合が考えられるため、ICカード内のファイルのセキュリティは、ファイルごとに独立して設定可能であり、あるファイルに対して、他のファイルのセキュリティ変更によって、脅かすことの無いことが前提である。

例えば、データEFはデータを記録するエリアとそのエリアを管理する管理エリアから構成されており、その管理エリア内にセキュリティを確保するためのアクセス条件をもつ。アクセス条件には読出し系／書換え系の2種類のアクセス種別にアクセス条件が分れることになる。つまり、あるキーを照合した場合、当該データEFの内容を“読出せるが書換えはできない”、“読出し、書換え共にできる”というようなアクセス条件が設定可能となる。そして、この例では各アクセス種別のアクセスキーの組合せが、3種（発行者パスワード、所持者パスワード、作業所パスワードのOR条件）で構成されている。

解説表4　データEFのアクセス条件

読出し系			書換え系		
発行者	所持者	作業所	発行者	所持者	作業所
●	●		●		

●…照合要

この場合、

読出し系：発行者キー又は所持者キーの照合が必要となる。つまり、どちらかの照合で読出し可能となる。

書換え系：発行者キーの照合が必要となる。したがって所持者キーの照合では、書換えは不可能となる。

この状態で、VERIFYコマンドによって“所持者キー(例えば9876)”を照合した場合を以下に示す。

解説表5　データEFのアクセス条件

読出し系			書換え系		
発行者	所持者	作業所	発行者	所持者	作業所
●	○		●		

○…照合済み

表に示すように、読出し系のアクセス条件として要求されている所持者キーが照合されているため、データの読出しが可能となる。

なお、書換え系のアクセス条件として要求されているキーは未だ照合されていないため、データの書換えは不可能となる。

また、どのキーも照合されていない状態において、VERIFYコマンドで“発行者キー(例えば1234)”を照合した場合を以下に示す。

解説表6　データEFのアクセス条件

読出し系			書換え系		
発行者	所持者	作業所	発行者	所持者	作業所
○	●		○		

○…照合済み

解説表に示すように、読出し系及び書換え系のアクセス条件として要求されている発行者キーが照合されているため、データの読出し／書換えが共に可能となる。

つまり、“発行者はデータの書換えは可能であるが、所持者は不可能となる”というアクセス条件が実現されたことになる。

このようなアクセス条件をそれぞれのEFに設定可能であり、格納データに必要なセキュリティに従って、読出し系／書換え系それぞれのアクセス主体の構成を変えることが可能である。

上記のように、互いの契約によってセキュリティの条件が揃えば、異なったアプリケーション提供者が同一のファイルを参照する機能をもつ必要がある。例えば、車載情報DF内のデータをアクセスするために車載情報DF下のパスワード照合したときに、MF下の免許資格ファイルへのアクセス条件が車載情報DF下のパスワード照合によってアクセス可能となっていれば、他のパスワードを照合すること無くアクセスすることが可能となる（ただし、アクセス条件の設定次第で免許資格ファイルへのアクセスが不可能とすることもできる）。

２．３．３　外部装置によるICカード機能の認証とICカードによる外部装置機能の認証に関する機能採用　　金銭に関係するアプリケーションを想定すると、ICカード内に記憶したパスワードの照合（VERIFYコマンド）よりもセキュリティ性の高い機能として、暗号化アルゴリズムを使用した外部装置によるICカード機能の認証とICカードによる外部装置機能の認証に関する機能を採用した。

・外部装置によるICカード機能の認証

外部装置によるICカード機能の認証とは、外部装置(又は外部装置に対し、操作者がキーボード

等でキー入力した場合を考えると、外部装置と操作者を1つの系として適用されるカード外部環境)が既知としている認証キーをICカードが所有しているか否かを、ICカードから出力される認証用データに基づいて外部装置によって判断する認証である。

例えばICカード内にシステム固有のデータを記憶させておき、システム利用開始時にリードコマンドなどによって直接該データを読出し、これをシステム側でチェックする方法によって容易に等価なことは実現できる。

しかしデータ伝送路上に現れる該データを盗聴し、偽造カード内に該データを忍ばせておき、システムのリードコマンドに呼応してこれを出力すれば、システムはこの時点では正常な(システムに使用するに相応しい)カードであると判断してしまう。

この理由からカードから出力される確認用データは、出力ごとに異なるデータであり、かつこれを受信した外部装置は何らかの手段を講じて、この異なるデータから常に1つの特定データを導出して(又はこれと等価な方法によって)、検査する方法が望ましい。

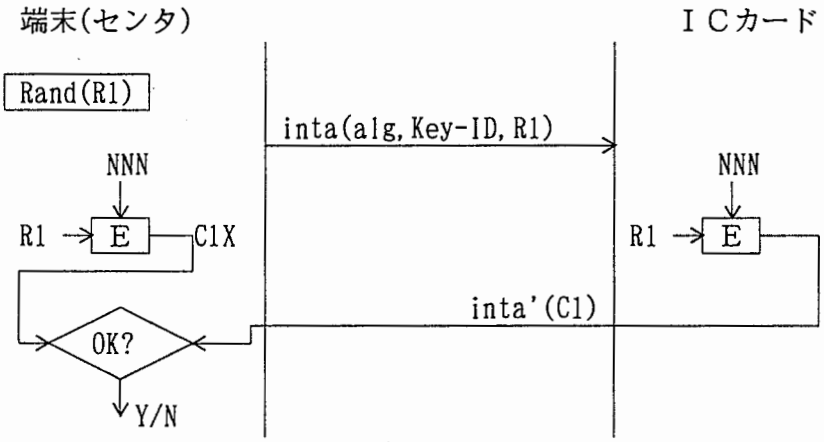
このため時刻変化するパラメタを用いて該確認用データにある種の演算処理を施した後、カードが演算データを出力する方法がある。このとき該パラメタをカードに通知しなければならないので、演算データと該パラメタを入手した場合、これらから容易に確認用データが類推できるものであると、やはり前述の問題が発生する。

これを回避するために、演算処理として暗号ロジックを採用する方法が考えられる。この実現手段が、この節でのべる外部装置によるカードの認証である。

ICカード認証フローを図11.2に示す。

なお、図中のKey-IDとは、使用するキーを特定するIDであり、この規格で規定するShort EF-IDに相当する。

解説図5　端末によるICカード機能の認証手順フロー



手順

Step 1：端末(又はセンタ)は、乱数（Rand(R1)）を生成する。

Step 2：intaiコマンドによって、認証に必要なアルゴリズム（alg）、キーデータを指示するキーデータのID（Key-ID）、及びStep 1で生成した乱数を通知する。

Step 3：ICカードはこれを受信すると、指定されたアルゴリズム及びキーデータで、乱数（Rand(R1)）を暗号化し、結果をC1とする。

Step 4：Step 3で算出したC1を、intaiコマンドのレスポンスとして端末に通知する。

Step 5：端末は、これを受信すると、自身で同様な方法によって算出したC1XとC1とを比較して、一致すれば端末はICカードが正当であると判断する。

・ICカードによる外部装置機能の認証

ICカードによる外部装置機能の認証とは、ICカードが既知としている認証キーを外部装置(又は前記したカード外部環境)が所有しているか否かを、外部装置から入力される確認用データに基づいてICカードによって判断する認証である。

これに類似する機能としてVERIFYコマンドによるキーの内部照合処理があげられる。このコマンドの場合、照合対象となるキーデータはそのままの形でデータ伝送路上に現れる。このため伝送路上を盗聴することによって、容易にキーデータが不当外部者に漏洩してしまう。

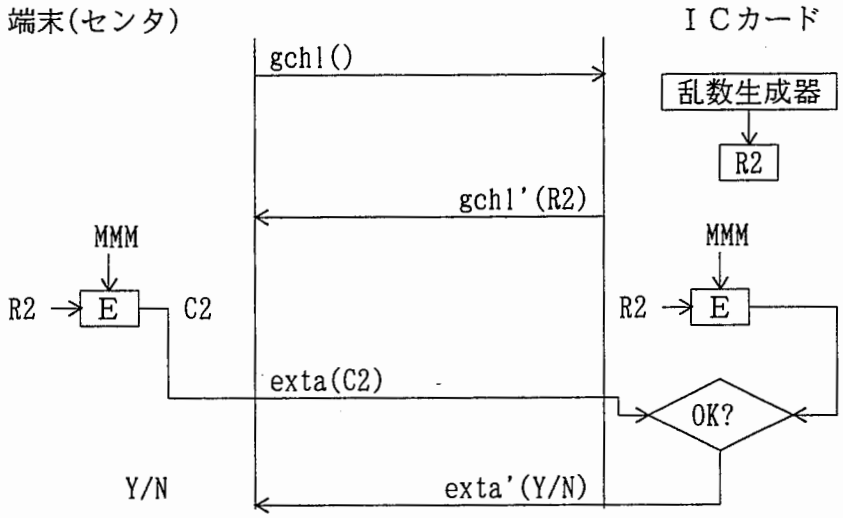
このため照合対象のデータが常にことなる形態で伝送路上をとおり、カード側でこの異なるデータから常に1つの特定データを導出し(又はこれと等価な方法によって)検査する方法が望ましい。

これを実現する手段が、ICカードによる外部装置の認証である。

外部装置認証フローを図11.3に示す。

なお、図中のKey-IDとは、使用するキーを特定するIDであり、この規格で規定するShort EF-IDに相当する。

解説図6　ICカードによる外部装置機能の認証手順フロー



exta/exta':external authenticateコマンド／レスポンス
E:DESアルゴリズム

手順

Step 1：まず端末(又はセンタ)は、gchliコマンドによって乱数を要求する。

Step 2：ICカードはこれを受信すると、乱数（Rand(R2)）を生成し、gchliコマンドのレスポンスとして、これを端末に返送する。

Step 3：次に端末は、既知とする、認証に必要なアルゴリズム（alg）、及びキーデータで、乱数（Rand(R2)）を暗号化し、結果をC2とする。

Step 4：Step 3で算出したC2、算出に使用したアルゴリズム（alg）、及びキーデータを指示するIDを、extaiコマンドでICカードに通知する。

Step 5：ICカードはこれを受信すると、自身で同様な方法によって算出したC2XとC2とを比較して、一致すればICカードは端末が正当であると判断する。そしてこの結果を、extaiコマンドのレスポンスとして端末に通知する。

・認証とアクセス条件

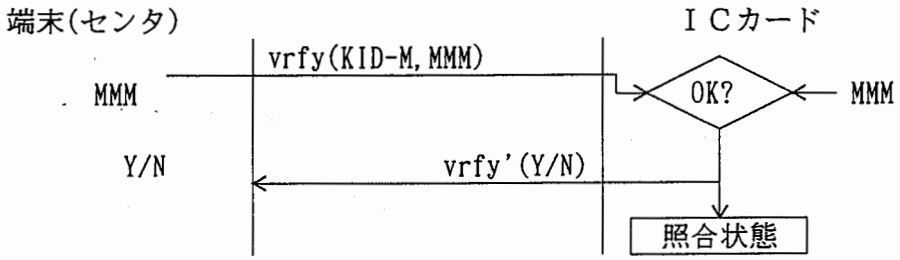
前述したように、“外部装置認証”のプロセスには、ICカード内部照合処理が含まれている。この照合の対象となるキーデータは、ICカードによって“内部認証キー”として識別されるキーがパラメタとして使用される。

つまり間接的に該キーを暗号化して照合することと等価になる。

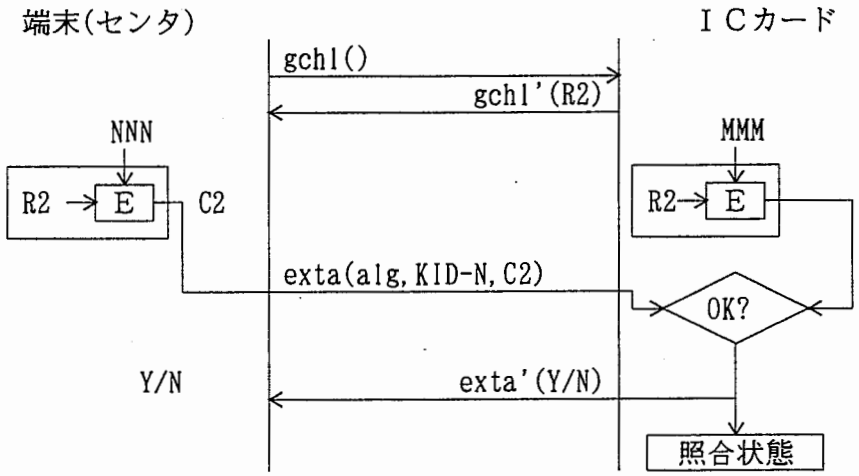
下図を用いて、説明する。

なお、図中のKIDとは使用するキーを特定するIDであり、この規格で規定するShort EF-IDに相当する。

解説図7　verifyコマンドによる照合状態の確立



解説図8　EXTERNAL AUTHENTICATEコマンドによる照合状態の確立



図示するように、EXTERNAL AUTHENTICATEコマンドの機能は、指定されたキーに暗号化処理を施す以外は、VERIFYコマンドの照合処理と等価な機能をもっている。

したがって、この規格で規定するICカードは、EXTERNAL AUTHENTICATEコマンドによる認証処理結果(認証状態：照合状態の一種)を、ファイルのアクセス条件に加えることができることとする。

また、必要に応じて、外部装置認証用キーに対して不一致回数上限値を設定することによって、キーの自動ロックを施すことが可能である。

なお、外部装置とICカードとの認証を行うため、キーデータが2つ必要であり、メモリ容量を圧迫することとなる。そのため、各アプリケーションに設定するセキュリティの高さを考慮した設定が必要となる。

２．３．４　パスワード変更機能の採用　　パスワード変更機能は、建設事業従事者本人のプライバシー保護のため、本人の手に渡った後、各自が本人のパスワードを希望するパスワードに変更できるように機能を採用した。

また、他にセキュリティの確保として、例えば、本人以外のパスワードでも発行時点では仮のパスワードを使用しておき、建設事業従事者に渡るときにはアプリケーションで使用ができるように実際のパスワードに変更するものである。

また、全国一斉に行うことが前提となるが定期的なパスワード変更を行うことで、より高いパスワードによるセキュリティが確保される。

ただし、この機能はISO規格で規定されていない機能である。

２．４　コマンド　　ISO規格で規定されているコマンドのいくつかは、他のコマンドで代用可能であり、また、ミニマム仕様と位置付けるために建設のアプリケーションでは使用しないと思われるコマンドについては、この規格では規定しなかった。

また、逆に、ISO規格では規定されていないパスワード更新機能として、CHANGE PINコマンドを機能

追加した。

解説表7に建設標準ICカード仕様とISO/IEC 7816-4 (2nd CD:1993) で提案されているコマンドとの比較表を示す。

解説表7 建設標準ICカード仕様とISO/IEC 7816-4 (2nd CD:1993) とのコマンド比較表

コマンド名	建設標準	ISO/IEC 7816-4	この仕様に不採用の理由
READ BINARY	○	○	
WRITE BINARY		○	建設のアプリケーションでは使用しないため
UPDATE BINARY	○	○	
ERASE BINARY		○	UPDATE BINARYコマンドで代用可能なため
READ RECORD(S)	○	○	
WRITE RECORD		○	建設のアプリケーションでは使用しないため
APPEND RECORD	○	○	
UPDATE RECORD	○	○	
GET DATA		○	書込み系コマンドで代用可能なため
PUT DATA		○	読取り系コマンドで代用可能なため
SELECT FILE	○	○	
VERIFY	○	○	
INTERNAL AUTHENTICATE	○	○	
EXTERNAL AUTHENTICATE	○	○	
GET CHALLENGE	○	○	
MANAGE CHANNEL		○	SELECTE FILEコマンドで代用可能なため
CHANGE PIN	○		

○：標準仕様として規定されている（空欄は、標準仕様として規定されていない）

また、各コマンドの処理ステータスコードのトラップ順位については、ICカード内のプログラム容量がアプリケーション側のシステムに比べ限られている
ため、トラップ順位を規制されることによる処理の負担はプログラム容量を圧迫するものであり、ICカードの機能削減につながる問題である。したがって、各コマンドの処理ステータスコードのトラップ順位は、この規格では規定しないこととした。