



e2TP メッセージ仕様書

TEF950-S003-01.00.00/ja

2005 年 3 月
T-Engine フォーラム

目 次

1.	はじめに.....	1
1.1.	本仕様の概要.....	1
1.1.1.	TENeT アーキテクチャ.....	1
1.2.	本仕様書の位置付け.....	2
1.3.	規定範囲.....	2
1.4.	参照規定.....	2
1.5.	用語定義.....	2
1.6.	エンディアン.....	2
2.	e ² TP メッセージ.....	3
	本章では, e ² TP メッセージのフォーマットとその内容について説明する.	3
2.1.	e ² TP メッセージフォーマット.....	3
2.1.1.	eTRON ID.....	3
2.1.2.	メッセージタイプ.....	3
2.1.3.	スレッド ID.....	4
3.	ISO7816-4 APDU へのマッピング.....	5
3.1.	APDU フォーマット.....	5
3.2.	TENeT コマンドフォーマット.....	5
3.3.	TENeT レスポンスフォーマット.....	6
3.3.1.	通常処理時.....	6
3.3.2.	異常終了時.....	6
3.3.3.	複数メッセージを含むレスポンスフォーマット.....	7

1. はじめに

本文書は、e²TP メッセージのメッセージフォーマットおよび ISO7816-4 APDU へのマッピング方法を規定している仕様書である。

1.1. 本仕様の概要

TENeT は、モバイル環境における権利価値の安全な取引を実現するフレームワークである。TENeT 上には、IC カードと携帯端末が存在する。IC カードは、携帯端末に挿入されている状態で携帯端末上のアプリケーションから利用されることを前提とする。

アプリケーションは IC カードとメッセージを送受することで、操作命令と応答を行う。TENeT は、このメッセージ送受にメッセージパッシング形式を採用している。そのため、アプリケーションや IC カードはメッセージの送付後に、応答を待つことなく、他の相手とのやり取りが可能である。

またアプリケーションは、TENeT の分散透過的なメッセージ配送機構を利用することで、IC カードの出力メッセージに対する中継処理が不要である。

本仕様では、TENeT 上で配送されるメッセージの共通フォーマットである e²TP メッセージフォーマットを規定する。

1.1.1. TENeT アーキテクチャ

IC カード間や IC カードとアプリケーション間で分散透過的にメッセージを配送する TENeT アーキテクチャを図 1 に示す。メッセージングライブラリは、e²TP メッセージを同期（送信メッセージに対する返答メッセージを待ち受けする）もしくは非同期（メッセージの送信後、返答メッセージを待たずに処理を続行する）に送受信する。アプリケーションは、非同期メッセージ送信を行った場合には、他のイベントドリブンシステム（GUI フレームワークなど）と同様に、受信メッセージをあらかじめ登録したイベントリスナにより取得することとなる。

本アーキテクチャは、IC カードやアプリケーションが e²TP メッセージを出力すると、まずメッセージングライブラリがメッセージを受理して、宛先に対して送信する。従って、IC カードが他の IC カードを宛先として出力したメッセージはメッセージングライブラリにより直接相手先の IC カードに送信されるため、アプリケーションによる宛先の中継処理は不要となる。

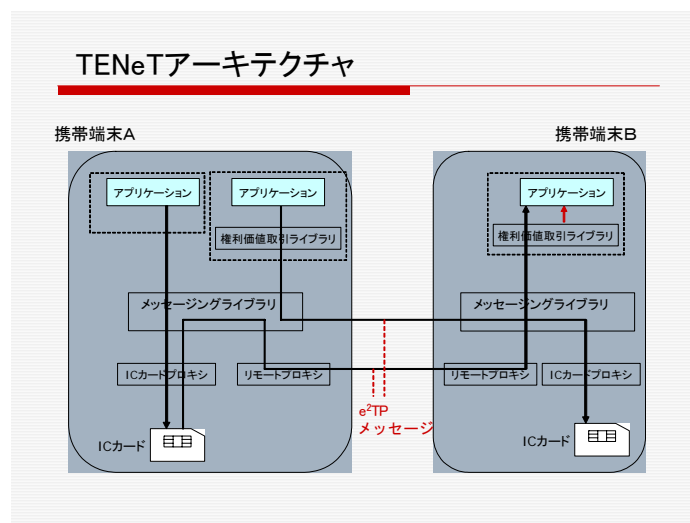


図 1 TENeT アーキテクチャ

1.2. 本仕様書の位置付け

TENeT は、権利価値取引を実現する IC カードおよびアプリケーションプログラムの相互運用性を実現するために、以下の各種仕様を規定する。

- ✚ TENeT 権利価値取引 API 仕様
アプリケーションプログラムから IC カードの権利価値を管理・流通させるための API
- ✚ TENeT メッセージング API 仕様
アプリケーションプログラムから e² TP メッセージを送受するための API
- ✚ Extended eTP (e² TP) メッセージ仕様 【本文書】
e² TP メッセージのメッセージフォーマットおよび ISO7816-4 APDU へのマッピング方式
- ✚ TENeT メッセージ仕様
TENeT 仕様 IC カードが備えるべき e² TP メッセージのメッセージセット

1.3. 規定範囲

本文書は、e²TP メッセージのメッセージフォーマットおよび e²TP メッセージの IC カード入出力時の ISO7816-4 APDU へのマッピング方式を規定する。

1.4. 参照規定

ISO/IEC Integrated circuit(s) cards with contacts

- Part4: Interindustry commands for interchange, ISO/IEC 7816-4: 1995(E).

1.5. 用語定義

本文書で用いる共通の用語を表 1 に定義する。

用語	意味
B	Byte の略 バイトを示す
MSB	Most Significant Bit の略. バイト配列の最上位ビットを示す

1.6. エンディアン

e²TP メッセージ上のすべての数値について、エンディアンとしてネットワークエンディアン（ビッグエンディアン）を用いる。

2. e²TP メッセージ

本章では、e²TP メッセージのフォーマットとその内容について説明する。

2.1. e²TP メッセージフォーマット

TENeT は、IC カード間の分散処理をアプリケーションプログラムから容易に利用するために、IC カード間や IC カードとアプリケーションプログラム間で分散透過的にメッセージを送受するための機構を備えている。TENeT では、この機構を用いて配送するメッセージを e²TP (extended eTRON Transfer Protocol) メッセージと呼ぶ。e²TP メッセージのフォーマットを表 2 に示す。

format 値の先頭 1 バイトが e²TP メッセージフォーマットのバージョンである。本仕様の仕様バージョンは 10h である。format 以外の値は仕様バージョンが 10h の時に規定される値である。

DestID と SrcID はメッセージの宛先と送信元を示す識別子である。メッセージングライブラリはこの SrcID を宛先としてメッセージを配送する。

DATA 部には「TENeT メッセージ仕様書」で規定される TENeT メッセージが入力される。IC カードはメッセージタイプによりメッセージを識別して、そのメッセージの内容である DATA に対して処理を行う。

スレッド ID とメッセージタイプおよび eTRON ID については、以下の節で詳細を説明する。

表 2 e²TP メッセージのフォーマット

	内容	サイズ (バイト)	意味
Format	フォーマット	4	e ² TP メッセージフォーマットのバージョンを表す 先頭 1B: 仕様バージョン(10h) 残り 3B: 予約領域(000000h)
DestID	宛先 eTRON ID	16	メッセージの宛先の eTRON ID
SrcID	送信元 eTRON ID	16	メッセージの送信元の eTRON ID
ThreadID	スレッド ID	20	メッセージの関係を示す ID
MessageType	メッセージタイプ	2	仕様毎に定めるメッセージの種別
LEN	データ長	2	ルーティングヘッダが付与されるメッセージのデータ長
DATA	データ	LEN	TENeT メッセージ

2.1.1. eTRON ID

eTRON IDは、eTRON/16で定義されている16バイトの識別子である。TENeTは、eTRON IDを利用して、内部的にeTRON IDの前者12バイトを「domain」、後者4バイトを「port」と分割する。

TENeT上の各ICカードは、固有のdomainを持つ。ICカードはport=0を自身の値としており、ICカードのeTRON IDは「domain|0」となる。

portは、アプリケーションからの要求に応じて、ICカードが一意に払い出す。アプリケーションは、ICカードのdomainとportを連結した値である「domain|port」を自身の識別子として取得する。携帯端末に追加・削除されるアプリケーションが固有のeTRON IDを持つことは運用上非効率であるため、必要時に一意な識別子を付与することで運用上の対処としている。

portは「使い捨て」にされるため、いつかはportの払い出しを行うことができなくなる危険もあるが、1つのdomain当たりで約40億個のportを割り当てることができる。すなわち、1秒に1回のIDの払い出しを行っても、portを使い切るには約136年かかり、事実上portを使い果たすことはない。

2.1.2. メッセージタイプ

メッセージタイプは、「TENEt メッセージ仕様書」で規定された TENEt メッセージを分類する 2 バイトの値である。メッセージタイプの内訳は、上位 1 バイトが基本/交換メッセージを表す大分類、下位 1 バイトが基本/交換メッセージのメッセージを表す小分類である。それぞれの分類の詳細を表 3 と表 4 に示す。

特に基本/交換における各メッセージの小分類は、下位 1 バイトの MSB で通常メッセージとエラーメッセージを分類、b6 以下の値で TENEt メッセージを分類している。

表 3 メッセージタイプの上位 1 バイトの分類

大分類	b7	b6	b5	b4	b3	b2	b1	b0	16 進表記
TENEt メッセージ仕様	0	x	x	x	x	x	x	x	-
基本	0	0	0	0	0	0	0	0	00h
交換	0	0	0	0	0	0	0	1	01h
(RFU)	0			(その他の値)					-
任意	1	x	x	x	x	x	x	x	-

※ MSB が 1 の時は、メッセージタイプは AP が任意に使用することが可能である。

表 4 メッセージタイプの下位 1 バイトの分類 (通常/エラー)

大分類	b7	b6	b5	b4	b3	b2	b1	b0
通常メッセージ	0	x	x	x	x	x	x	x
エラーメッセージ	1	x	x	x	x	x	x	x

※ MSB が 0 の時は、メッセージタイプは通常メッセージに用いる。

※ MSB が 1 の時は、メッセージタイプはエラーメッセージに用いる。

2.1.3. スレッド ID

アプリケーションや IC カードは、入出力する一連の e²TP メッセージをメッセージをスレッド ID により対応付ける。

スレッド ID はアプリケーションによって生成される値である。アプリケーションから IC カードに対して操作を要求する際に、その要求を一意に識別するための ID としてスレッド ID を付与する。このスレッド ID はアプリケーション単位で一意であればよいため、アプリケーションは操作要求ごとに一意である識別子 serial を自身の ID に連結した値「domain|port|serial」をスレッド ID とする。

たとえば、アプリケーションから IC カードに送付するファイル生成メッセージについて、ファイル生成メッセージと、IC カードから送付される応答メッセージに同一のスレッド ID を付与することで、アプリケーションはメッセージの送付と応答を対応付けることができる。

また、交換制御ではアプリケーションが IC カードに交換を支持すると、アプリケーションと IC カード間でメッセージが複数回数やり取りされる。上記と同様にすべてのメッセージに同一のスレッド ID を持たせることで、アプリケーションは一連のメッセージとして識別できる。

3. IS07816-4 APDU へのマッピング

本章では、2章で定義した e²TP メッセージを、IC カードへの入出力形式である APDU フォーマットへマッピングする方法を説明する。

3.1. APDU フォーマット

IC カードのハードウェアやメッセージフォーマットの国際標準仕様として IS07816-4 がある [IS07816-4]。この IS07816-4 に準拠した IC カードは、APDU (Application Protocol Data Unit) フォーマットに従ったメッセージのみを受理する。図 1 に APDU のフォーマットを示す。CLA と INS の値は IS07816-4 で規定された共通コマンドを分類する。P1 と P2 は共通コマンドで利用するパラメータである。

Header				Body		
CLA (1B)	INS (1B)	P1 (1B)	P2 (1B)	Lc (1B)	Data (可変長)	Le (1B)

図 1 APDU フォーマット

e²TP メッセージは、IS07816-4 準拠ではない独自規定のフォーマットである。TENEt は、IS07816-4 準拠の IC カードが e²TP メッセージを受理できるように、IC カードとのやり取りに IS07816-4 の Envelope コマンドを用いる。Envelope コマンド/レスポンスは、RoutingHeader の値は IS07816-4 の規定値を付与して、Body 部の DATA 内に 2.1 節で規定した e²TP メッセージを含む形となる。(図 2 参照)

3.2. TENEt コマンドフォーマット

3.1 節で述べた IS07816-4 Envelope コマンドフォーマットを図 2 に示す。e²TP メッセージは APDU フォーマットの Body 部に格納される。Envelope コマンドの規定値を表 5 に示す。

Header				Body		
CLA (1B)	INS (1B)	P1 (1B)	P2 (1B)	Lc (3B)	Data (可変長)	Le (2B)

C-APDUは、常に Case4拡張とする

Message						
RoutingHeader						Payload
FORMAT (4B)	DestID (16B)	SrcID (16B)	ThreadID (20B)	Message Type(2B)	LEN (2B)	DATA (可変長)

図 2 コマンドフォーマット

表 5 コマンドフォーマット規定値

パラメータ	値
CLA	00h (固定値)
INS	C2h (固定値)
P1	00h (固定値)
P2	00h (固定値)
Lc	Body 内の” Data” 部の長さ
Data	e ² TP メッセージ
Le	0000h (固定値)

3.3. TENEt レスポンスフォーマット

IC カードが Envelope コマンドを処理して出力するレスポンスのフォーマットを示す。レスポンスはメッセージが通常に処理された場合、および APDU コマンドの Header 部の値が不正であった場合で異なる。それぞれのレスポンスフォーマットを示す。

3.3.1. 通常処理時

通常のレスポンスフォーマットを図 4 に示す。パラメータである SW1, SW2 の規定値を表 6 に示す。

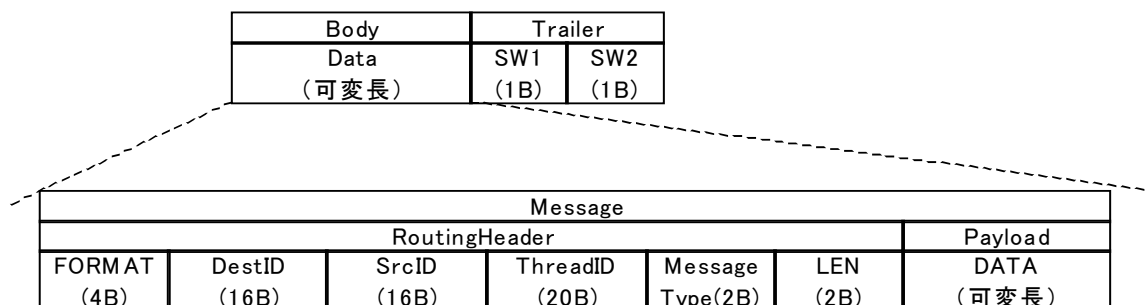


図 4 レスポンスフォーマット (通常終了時)

表 6 レスポンスフォーマット規定値

パラメータ	値
Data	TENEt メッセージ
SW1	90h (固定値)
SW2	00h (固定値)

3.3.2. 異常終了時

Envelope コマンドの Header や Lc と Le の不一致などの RoutingHeader の不正による異常終了時のレスポンスフォーマットを図 5 に示す。パラメータである SW1, SW2 の規定値を表 7 に示す。

Trailer	
SW1 (1B)	SW2 (1B)

図 5 レスポンスフォーマット (異常終了時)

表 7 異常終了時の規定値

内容	値	備考
LEN, Lc, Le エラー	6700h	LEN, Lc 又は Le 値が不正
コマンド実行条件を満足しない	6985h	Personalize 未完了
CLA エラー	6E00h	C-APDU の CLA が不正
INS エラー	6D00h	C-APDU の INS が不正
P1-P2 エラー	6A86h	C-APDU の P1 又は P2 が不正
Ver エラー	6AA0h	RoutingHeader の Version が不正
SrcID エラー	6AA1h	RoutingHeader の SrcID が不正
DestID エラー	6AA2h	RoutingHeader の DestID が不正
LEN エラー	6AA3h	RoutingHeader の LEN が不正
(TBD)	(TBD)	(TBD)

3.3.3. 複数メッセージを含むレスポンスフォーマット

TENeT は、処理の結果を複数の相手に同時送付する場合がある。この場合は、図 6 の通り、複数のメッセージをレスポンスメッセージの Body 部に接続して出力する。本フォーマットにより出力される複数メッセージの相手先への到着順序はメッセージの格納順とは限らない。

本フォーマットの利用は IC カードからの出力時のみ可能であり、IC カードに対するアプリケーションからのメッセージ入力時には禁止である。

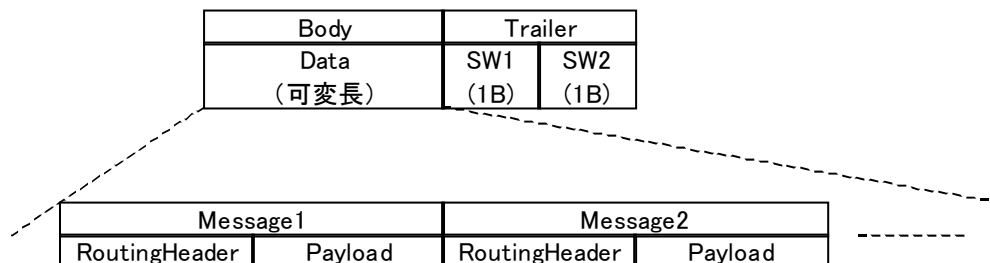


図 6 複数メッセージを含むレスポンスフォーマット

[参考文献]

- ✓ 「TENEt メッセージ仕様書」, T-Engine フォーラム, 2005.