第３部対応

項番	頁	区分	コメント内容	修正案など	対応方法
1	―	―	共通コマンドは利用フェーズと発行フェーズとで分離すべき。 付属書の位置づけが明確でない。	発行系コマンドを付属書とするのではなく、 ３部 共通コマンド ４部 発行系コマンド のようにしてはいかがでしょうか。	「まえがき」に附属書は必須ではない参考仕様である旨を明記します。なお、発行系コマンドについては、現行の通り、附属書に載せることにします。
2	1	C	附属書の位置付けが不明確	序文に附属書の位置付けを記述する。	「まえがき」に附属書は必須ではない参考仕様である旨を明記します。
3	4	R	ﾃﾝﾌﾟﾚｰﾄの定義がほしい。	EMV では、「構造型ﾃﾞｰﾀｵﾌﾞｼﾞｪｸﾄのﾊﾞﾘｭｰ部」と定義されている。	テンプレートとは、JIS X 6307 の定義の通り、「構造化されたデータオブジェクトの値フィールド」です。用語の定義として追加します。
4	7 等	C	「RFU」という意味が広く使われているため、ISO で RFU となっている所と、この仕様で RFU としているところが区別できない。		ご指摘に区別を明確にするため、ISO で RFU となっているところは RFU と記述し、この仕様で RFU とするところは、「本仕様で留保」と記載します。
5	30	R	6.2.2(3)キーの組合せ論理 ・JICSAPV1.1 カードでもJICSAPV2.0 対応システムで使用できるようにご検討お願いします。	「カード識別子ファイル内の仕様書バージョン等を参照することで上位装置がシステムを切り替えて対応する」等を追記することを提案します。	上位装置側は必ずしも JICSAP1.1 と JICSAP2.0 の両方に対応する必要はないと判断しています。両者の混在を想定するシステムの場合は、当然のことながら上位装置側で両者に対応するシステムが必要となります。これはシステム開発者の判断で行われるべきと考えます。

6	32、33	R	6.3.セキュリティステータスの管理方法にて、規則2と規則3の最後に(オプション)とあるが、これでは規則2/3全体がオプションと読めてしまう。	(オプション)表示を外す	備考にプラットフォーム型、ネイティブ型の注意事項を記述しているので、規則１、規則２、規則３の（オプション）の記述は削除します。	
7	34	R	6.4 セキュアメッセージング ・セキュアメッセージングフレームがJICSAPV1.1 と互換性がありません。上位装置がフレームを切替えて対応できるようにするべきと考えます。	・「カード識別子ファイル内の仕様書バージョン等を参照することで上位装置がフレームを切り替えて対応する」等を追記することを提案します。	上位装置側は必ずしもJICSAP1.1とJICSAP2.0の両方に対応する必要はないと判断しています。両者の混在を想定するシステムの場合は、当然のことながら上位装置側で両者に対応するシステムが必要となります。これはシステム開発者の判断で行われるべきと考えます。	
8	34 ～ 41	R	6.4 セキュアメッセージング ・「認証」のみ機能を使用する場合には、セキュアレスポンスAPDUを暗号化するのか平文のままかの区別ができないと考えます。NMDA 共通コマンド仕様書（H12.12.5 ）にレスポンスディスクリプタを定義するべきと考えます。		本仕様では、セキュアメッセージングの機能を「暗号かつ認証のみ」に限定しており、レスポンスAPDUがデータを伴う場合は、必ず暗号化されることになります。	
9	34 ～ 41	R	6.4 セキュアメッセージング ・NMDA 共通コマンド仕様書（H12.12.5 ）に規定されているレスポンスディスクリプタがありません。レスポンスディスクリプタを定義するべきと考えます。		レスポンスディスクリプタの機能は必ずしも必要ではないと判断し、実装上の負荷を軽減させることを優先しました。	
10	42	R	6.4.5.主な機能の説明にて、「元の暗号対照データが8の倍数である」とあるが、暗号アルゴリズムによりブロック長が異なるため、必ずしも8の倍数とは限らない。	「元の暗号対象データがブロック暗号の単位の倍数である」に修正	ご指摘通り修正します。	

11	43	C	セキュリティ環境の内、一時的データ要素は、RAM に置かれることが一般的と思われるが、プラットフォーム型 OS の場合、同一アプリの選択で RAM 内容がクリアされてしまうことがある。	プラットフォーム型 OS の場合は、同一アプリ選択時にもカレント SE がリセットされても良いことを明記	ご指摘通り修正します。	
12	43 等	Q	6.5 セキュリティ環境中ではセキュリティ環境の設定手順は規定しない、となっているが、これは具体的にどう言う意味か？セキュリティ環境を設定するコマンドは定義されているが、これはセキュリティ環境の設定手順とは異なるのか。		セキュリティ環境を設定するコマンドがオプションである旨明記します。	
13	45	Q	セキュリティ環境のデータ要素の表は、ISO7816-8 を参考にしているが、ISO の表から、HASH のアルゴリズム識別子に関する表記が削除されているのはなぜか		ハッシュ関数はアプリケーションごとに一つに決まる（暗黙的選択）ものと判断し、ハッシュ関数の識別子を削除しました。	
14	48	Q	7.共通コマンドで拡張 Lc/Le は必須か？		拡張 Lc/Le は，JavaCard などの場合実現が難しいため, 必須とはしません.	
15	48	R	ケース 4 のコマンドフォーマットにて、Le が 1 or 3 となっている	1 or 2 に修正	修正いたします.	
16	49	R	クラスバイトの符号化において、b2b1 が b”00”固定となっているが、ロジカルチャネルは少なくとも 1 チャネルのサポートが必要であるため、2 チャネル以上となる場合もあり、この時チャネルを表すことができない。	bxx に変更する。	修正いたします.	

17	51	Q	SELECT FILE コマンドの応答である FCI に関して、「応答可能なデータオブジェクトは以下の通り」とあるが、ここにあるデータオブジェクト以外は出力できないのか？ この表現だとその下に定義されるデータオブジェクト以外を排除しているように取れてしまう。		Tag= “84”および Tag= “85”で定義するデータオブジェクト以外のデータオブジェクトを FCI として含んで良いと考えています。このような主旨の記述になるよう修正致します。	
18	51	R	7.4.1 SELECT FILE ・使用条件及びセキュリティ条件に「第８章参照のこと。」とありますが、第８ 章が添付されていません。ご確認お願いします。		6 章の誤りです．修正いたします．	
19	54	R	7.4.2 VERIFY ・Lc が、他コマンド群では３ バイト表記を認めている仕様に対し、１ バイト表記のみとした理由を追記するべきと考えます。ご検討お願いします。		VERIFY の Lc を１バイトとしたのは、照合鍵の長さを 1～16 バイトと想定していたためです。理由が明確になるよう記述を修正致します。	
20	55 等	C	SW6986 カレントファイルがない、SW6A82 アクセス対象ファイルがない、において、ファイル種別を IEF、WEF などのように規定しているが、ISO ではすべて File not find であるため、これに従い、ファイルがないとしても良いのではないか		SW:6986 および SW:6A82 の意味を「ファイルがない」に修正いたします．	

21	57	R	7.4.3 GET CHALLENGE ・(6)特記事項の「～次に任意のコマンドが実行されるまで～」については、例えば「乱数取得→外部認証ファイル選択→外部認証（カレントＥＦ指定)」ができないという解釈もありえるため、該当コマンドは列記した方がよいと考えます。	・ Get Cahllenge 、 External Authenticate 、Select file（MF 、DF)、その他該当するコマンドを列記することを提案します。	現行の記述のままとします。 例示された処理は、「外部認証ファイル選択→乱数取得→外部認証（カレント EF 指定)」で代用可能であり、現行仕様で問題はないと考えます。	
22	62	R	7.4.5 INTERNAL AUTHENTICATE ・コマンドAPDU 内ではLc は1 バイト表記、表中では1 バイトor3 バイトと記載されています。誤記と考えますので修正をお願いします。	・表中のLc を1 バイトor3 バイトと修正することを提案します。	ご提案のとおり修正いたします.	
23	62	R	7.4.5 INTERNAL AUTHENTICATE ・ISO/IEC7816-4(1995.9.1)及びNMDA 共通コマンド仕様書（H12.12.5 ）では、Le は1バイトor2 バイトとなっていますが、ご確認お願いします。	・Le は1 バイトor2 バイトと修正することを提案します。	ご提案のとおり修正いたします.	
24	71	R	READ_RECORD のレスポンスにおいて、短縮 Le フィールドの場合複数読出しができない、と取れる	短縮 Le フィールドの場合も複数読出しが可能とする	「使用条件」の「複数レコード読み出しを指定した場合～」の項目を削除し, レスポンスメッセージの欄は短縮 Le でも複数読み出しが可能と記述を修正します. (V1.1 から変更なしとする)	
25	71	R	7.4.9 READ RECORD(S) ・コマンドAPDU 表の備考欄に‘ 00 ’はカレントレコードを示すと記載されていますが、JICSAPV2.0 では5.4.1(3)レコード参照方式でカレントレコードについて説明がありません。追記した方がよいと考えます。ご検討お願いします。	・「ライトレコード及びアペンドレコードしたレコードがカレントレコードとなる。」と追記することを提案します。	カレントレコードは本仕様では規定外の機能と位置付けています。従って、コマンド APDU 表の備考欄は「本仕様では留保」と記述します。	

26	71	C	READ RECORD(S)ｺﾏﾝﾄﾞの P1 の備考にｶﾚﾝﾄﾚｺｰﾄﾞに関する記述がある。	ｶﾚﾝﾄﾚｺｰﾄﾞに関する記述を削除。	コマンド APDU 表の備考欄は「本仕様では留保」と記述します。	
27	74	C	WRITE RECORD ｺﾏﾝﾄﾞの「定義および適用範囲」と「使用条件およびｾｷｭﾘﾃｨ条件」にﾚｺｰﾄﾞﾎﾟｲﾝﾀに関する記述がある。	ﾚｺｰﾄﾞﾎﾟｲﾝﾀに関する記述を削除。	ご指摘の通り修正します。	
28	74	R	7.4.10 WRITE RECORD ・定義及び適用範囲にレコードポインタの記述があります。削除する必要があると考えます。ご検討お願いします。	・レコードポインタの記述を削除することを提案します。	ご指摘の通り修正します。	
29	77	R	7.4.11 APPEND RECORD ・使用条件及びセキュリティ条件で、「可変長レコードの場合、創生時と同じサイズ以下のレコードのみ書込み可能」とありますが、創生時の定義が不明確です。ファイル創生時に、アペンドする可変長レコードのサイズも確定してしまうというようにも解釈できます。定義を明確にして戴きたいと考えます。	・「可変長レコードの場合、創生時と同じサイズ以下のレコードのみ書込み可能」の行を削除することを提案します。	創生時とはファイル創生時を意味し、可変長レコードの最大サイズがファイル創生時に確定すると考えています。但し、この制約は附属書 I の CREATE FILE コマンドによってファイルを創生した場合の制約であるので、下線部を追記します。「可変長レコードの場合、創生時と同じサイズ以下のレコードのみ書込み可能(附属書 I に示す CREATE FILE コマンドによってファイルを創生した場合の制約)」	

30	80	R	7.4.12 UPDATE RECORD ・使用条件及びセキュリティ条件で「可変長レコードの場合､創生時と同じサイズ以下のレコードのみ書込み可能」とありますが､創生時の定義が不明確です｡この場合の創生時と同じサイズとはアップデートしようとしているレコードのサイズと読み取れます｡正しいかどうか判断しかねるため定義を明確にして戴きたいと考えます。	・「創生時と同じサイズ」を「追記したレコードと同じサイズ」に変更することを提案します。	可変長レコードを扱う EF の場合，創生時にその EF で扱うことができる１レコードの最大長を指定し,領域を確保する必要があり，その最大長の範囲内で UPDATE を行う必要があるという趣旨の記述です｡但し、この制約は附属書Ｉの CREATE FILE コマンドによってファイルを創生した場合の制約であるので､下線部を追記します。「可変長レコードの場合､創生時と同じサイズ以下のレコードのみ書込み可能(附属書 I に示す CREATE FILE コマンドによってファイルを創生した場合の制約)」	
31	86	R	7.4.14.GET_DATA コマンドのステータスワードにおいて、6400 は不要	SW6400 の行を削除	SW:6400 は必要と判断します。	大日本印刷株式会社 BF 事業部 IC カード本部 荒井 尚 ［ＮＩＣＳＳ］
32	89	R	7.4.14.PUT_DATA コマンドのステータスワードにおいて、6400 が必要	SW6400 の行を追加	追加いたします.	大日本印刷株式会社 BF 事業部 IC カード本部 荒井 尚 ［ＮＩＣＳＳ］
33	91 94 96 98	R	7.5.1 CHANGE REFERENCE DATA 7.5.2 DEACTIVATE FILE 7.5.3 ACTIVATE FILE 7.5.4 RESET RETRY COUNTER ・ISO/IEC7816-9 （2000.9.1 ）を前提としているためCLA 、INS が異なっています｡上位装置がコマンドを切替えて対応できるようにするべきと考えます。ご検討お願いします。	・「カード識別子ファイル内の仕様書バージョン等を参照することで上位装置がコマンドを切り替えて対応する」等を追記することを提案します。	JICSAP1.1 と JICSAP2.0 の互換性についての指摘を思われますが、上位装置側は必ずしも JICSAP1.1 と JICSAP2.0 の両方に対応する必要はないと判断しています｡両者の混在を想定するシステムの場合は､当然のことながら上位装置側で両者に対応するシステムが必要となります｡これはシステム開発者の判断で行われるべきと考えます。	株式会社トーキン ＩＣ カード事業推進部 佐藤博美 大日本印刷株式会社 BF 事業部 IC カード本部 荒井 尚 ［ＮＩＣＳＳ］ 大日本印刷株式会社 BF 事業部 IC カード本部 荒井 尚 ［ＮＩＣＳＳ］

34	111	Q	7.6.5.GENERATE PUBLIC KEY PAIR コマンドにおいて、カレント IEF に必ず鍵ペアが入っている必要があるか？		Create File(IEF)に於いては、キーデータを設定することを前提としています.また、IEF は設定系のアクセスモードは定義されていません。よって、規格書には以下の文章を GENERATE PUBLIC KEY PAIR の(2)使用条件に追記します。 「IEF に鍵ペアが設定されていない状態に於いて、本コマンドを実行した場合の動作について、本仕様では規定しない」	
35	114	Q	JICSAP オリジナルコマンドとして GET SESSION KEY コマンドが定義されているが、ISO7816-8 のセキュリティ関連コマンド群で同様の機能は実装できる。 JICSAP オリジナルコマンドを作成した理由は何か。		本コマンドのように、生成したデータを暗号化し、かつ署名を付けて返すようなコマンドは ISO7816-8 には規定されていないと考えています。	
36	114	R	7.6.6 GET SESSION KEY ・NMDA 共通コマンド仕様書（H12.12.5）では INTERNAL AUTHENTICATE により本機能が実現されてます。上位装置がコマンドを切替えて対応できるようにするべきと考えます。ご検討お願いします。	・「カード識別子ファイル内の仕様書バージョン等を参照することで上位装置がコマンドを切り替えて対応する」等を追記することを提案します。	NMDA 仕様と JICSAP2.0 との共存を想定する場合は、ご指摘のようにカードの種別を上位装置側で認識し、コマンドを切り替える必要があります。しかしながら、このような対応は両者の共存を図るシステムにのみ必要であるため、システム開発者の判断で行うものと考えています。	

37	附 C-1	Q	今後、IPA/TAO 等により識別子が規定され、この体系が現在のものと全く異なった場合に、どうすべきか？ 特に既出のカードは全く互換性が取れない。		現時点では IPA/TAO で暗号アルゴリズム識別子が規定されていません。今後、IPA/TAO で検討がなされ、本仕様とは異なる体系となる可能性がありますが、その際には上位装置側のシステムで切り替え等の対応を行って頂きたいと考えています。	
38	附 C-1	C	「楕円暗号」は一括りになっているが、非常に多岐にわたるため、1Byte のモードだけでは細かいバージョンを表現しきれない可能性がある。		モードのバイト数の拡張を可能とする方向で検討します。	
39	G2	C	ｾｷｭｱﾒｯｾｰｼﾞﾝｸﾞの CCS の計算において、CBC ﾓｰﾄﾞへの入力が１ﾌﾞﾛｯｸのみの場合もあるが、付属書 G では、１ﾌﾞﾛｯｸの場合の処理方法の説明がない。	図 G-4 として、１ﾌﾞﾛｯｸの場合の処理方法を追加する。	ご指摘通り修正します。	
40	附 属 書 I-2	R	I-1 CREAT FILE ・表I-3 の可変長レコード構造の②可変長レコードにおける「全レコード長の総和」とは T1L1V1 T2L2V2 T3L3V3 ・・・TnLnVn の総和という意味でしょうか。その場合、「×全レコード数」という表現は適切でないと考えます。ご検討お願いします。	・「全レコード数」を「0x0001固定」に変更することを提案します。	表 I-3 のフィールド名： 「レコード構造または D0 構造」 →「ファイルサイズ」と修正します。また、「ファイルサイズ」（修正後）の意味欄：②可変長レコード構造のとき、 最大レコード長||全レコード数に変更いたします。ここで、ファイルサイズ＝最大レコード長×全レコード数となります。	
41	I-5	R	I-2 DELETE FILE ・IEF 削除処理の説明に「削除した領域は、再利用可能である」の記述がありません。追加するべきと考えます。ご検討お願いします。	・「削除した領域は、再利用可能である」と追記することを提案します。	（iii）IEF 削除処理に、「削除した領域は、再利用可能である」を追加します。	

42	I-5	R	I-2 DELETE FILE ・CLA がOxh と記載されていますが、コマンドの性質上、8xh が適切と考えます。誤記ではないでしょうか。ご検討お願いします。	・CLA を「0x 」から「8x 」に変更することを提案します。	ISO/IEC7816-9 に規定されるDELETE FILE の機能に準拠していると考えられるため、CLA=0X にて問題ないと考えます。修正は不要と考えます。	
43	I1 ～ I3	C	CREATE FILE ｺﾏﾝﾄﾞのﾊﾞﾘｭｰ部の具体的な設定方法が不明。 例えば、IEF 創生時のﾊﾞﾘｭｰ部の場合（表 I-4)、EF-ID やｷｰｻｲｽﾞはそれぞれに TLV で置くのか否か、等。	1)ｺﾏﾝﾄﾞ APDU の説明箇所において、ﾊﾞﾘｭｰ部の意味が「FCP ﾃﾝﾌﾟﾚｰﾄ相当の情報」とだけ書かれているので、「付属書 E 参照」を追加。 2)TLV 形式にするのであれば、未定義のタグ値を決める。	バリュー部を、ＤＦクリエイト、ＥＦクリエイト、ＩＥＦクリエイトのそれぞれに図示します。	
44	I2	C	表 I-3 において、「全ﾚｺｰﾄﾞ長の総和×全ﾚｺｰﾄﾞ数」という表現はおかしいのでは？　また、そのﾌｨｰﾙﾄﾞ名も適当でない。	ﾌｨｰﾙﾄﾞ名を「ﾌｧｲﾙｻｲｽﾞ」とし、意味を「全ﾚｺｰﾄﾞ長の総和」等とする。	表 I-3 のフィールド名： 「レコード構造または DO 構造」 →「ファイルサイズ」と修正します。また、「ファイルサイズ」（修正後）の意味欄：「②可変長レコード構造のとき、 最大レコード長||全レコード数」に変更いたします。 さらに、（修正後）の意味欄：「③DO 構造のとき、 全容量」 に変更いたします。	
45	I3	C	表 I-4 において、ｷｰｻｲｽﾞが TLV 全体の長さか、V のみの長さかを明確にする必要がある。		注に下記を追記します。 「設定されるＫｅｙ長は、ヴァリュー部のみとする」	
46	5 7	C	「ＦＣＰ」は、「ファイル制御情報パラメタ」「ファイル制御パラメタ」どちらが正しいのか。		FCP は JIS を参照し、「ファイル制御パラメタ」とします。	

47	5	R	「主ファイル」の説明で、「ファイル識別子で選択されなくても良い。」とあるが判りづらい。	暗黙のうちに選択されているのか、本当に指定せず直接ＤＦを選択してもよいのか、説明を追加したほうが良い。	p5 の用語の定義では、「・・・主ファイルはファイル識別子で選択されなくてもよい」は削除します。 MF は原則として活性化直後にカレントになるものと考えています。但し、プラットフォーム型ではカレントにならなくても良いとしています。(5.5 参照) また、MF を選択したい場合もあると考え、オプションですが、ファイル識別子による選択も可としています。
48	6	C	「レコード番号」の説明で、レコード番号が出てくる。	「レコード番号」→「番号」に変更	ご指摘の通り修正します。
49	9	R	図 5-1 に 2 レベルのＤＦも記述しておいた方が、論理的に判りやすい。検討をお願いしたい。	１レベルの下に 2 レベルのＤＦも記述する。	2 レベルの DF は必須としないので、現行の図 5-1 の通りとします。
50	9	R	「根幹」の用語定義をお願いしたい。本文と備考で使われる意味が異なっているように思えるため		ご指摘の内容を踏まえ、5.1 の備考の記述を修正します。
51	9	R	5.2 (1)　備考 JAVA カード仕様では、SELECT FILE の仕様では、このコマンドでは、先に 1 レベルの DF 名を全てチェックする。この動作と DF 名のユニーク性で不整合が発生する。	プラットフォーム型でも、フル DF 名はカード内で唯一でなければならない。	ご指摘の通りです。p9 5.2(1)の備考の記述を修正します。
52	11	C	表 5-1 に ISO で規定している ATR ファイル等の EF-ID も追記して欲しい。		表 5-1 の注釈として、「上記以外で ISO でリザーブされるファイル ID は ISO/IEC 7816-4,8,9 参照」を追記します。

53	23	Q	TLV の形状と Tag の値が記述してあるが、この図からは、本当に区別できるか不明である。	TLV の構造をチェックするための方法について、追記する。	BER-TLV 用 DO-WEF のデータオブジェクト形式に以下の記述を追記します。 備考：T の欄に示すタグの値は、その範囲内で連続したすべての値が有効ではない。詳細は附属書 B 参照。 TLV 構造のチェック方法は製造者依存と考えています。
54	23	C	タグ長が 1Ｂと２Ｂを混在させることの可否を記述することを検討して欲しい。		タグフィールドの長さが 1B と 2B の混在は可能と考えます。
55	29	C	－　親 DF 直下の に追記	「－　1 レベルのＤＦを親 DF とする直下の」と修正	「1 レベルの DF 直下の IEF-ID 指定」と修正します。
56	25	Q	「IC カードの電気的活性化後は、すべての論理チャネルのカレント DF は MF とする」となっているが、暗黙のうちにＭＦをアクセスする IC カード仕様になっていると解釈して良いか。		原則として「IC カードの電気的活性化後は、すべての論理チャネルのカレント DF は MF とする」としていますが、備考にプラットフォーム型 IC カードの場合は、IC カードの電気的活性化後、論理チャネルのカレント DF は必ずしも MF でなくてもよいと記述しています。
57	51	C	7.4.1(1) － DF の選択～。DF 選択の後、 の一部修正	－ DF の選択～。DF が選択された直後、	現行の記述のままで良いと判断します。
58	52	C	(4)(ⅱ)データ部 テンプレート TLV の記述で、FCI は FCP と FMD の情報（テンプレート）を包含すると読める。 　7816-4 の 5.1.5 Table１	ＦＣＩ＝”6F”の中にＦＣＰ＝”62”テンプレートが含まれるので、 “6F”L_0”62”L_1”84”L_2DF 名”85”L_3容量 となるのではないか	ISO/IEC 7816-4 について、タグ “6F”にて、FCP および FMD を送れると解釈しています。できるだけ省略するという観点から、FCP のタグ “62”を省略しています。また、EMV 仕様でもタグ “62”を省略しています。

59	52	C	(4)(ⅱ)データ部 容量の単位を示す。	単位は、Byte。	追記します。
60	58	C	(6)特記事項 「次に任意のコマンドが実行されるまで」 の修正	次の任意のコマンドが実行されるまで	ご指摘の通り修正します。
61	A-2	C	エディトリアル 4行　「無かったので、」 ７行　先頭の「同様に」	文が冗長になるので 「無かった。このため、」 削除	ご指摘の通り修正します。
62	B-1	C	表 B-1 で表中記載と備考で矛盾していると思われます。確認下さい		（b8b7）= “10”は、「テンプレート内でだけ使用する」ものですが、例外として、ファイル制御情報とセキュアメッセージングにおいては、テンプレート外で使用する、という意味です。この記述は JIS X 6307 の通りです。
63	G-1	C	G.2　　３行目 ～８バイト）とキーA	「～８バイト」をキーA」に修正	ご指摘通り修正します。
64	附属書Ⅰ	R	コマンド一覧か、目次をつけて貰いたい。		コマンド一覧を追加します。
65		R	プラットフォーム型とネイティブ型の違いをもっと明確に記述してほしい	解説ではなく、附属書または、本文のどこかに挿入する	プラットフォーム型とネイティブ型の違いについては附属書 A に記載しています。
66		C	CLA で”8X”を使用しているが、他の仕様(例えば EMV)との整合性をとって欲しい。	整合性の確認できている仕様範囲を追記する。	ISO/IEC 7816 シリーズで定義されないコマンドを CLA：“8X”としています。これらの仕様については EMV 仕様に対して阻害しないよう配慮しています。

67	40	C	CCS を計算する際に、コマンドヘッダ部分を含めているが、この時のCLA はセキュアメッセージング対応を示す b3-4 は立っているのか。 （JICSAP1.1 ではこのビットは 1 と規定してある) この場合､各々のケースでの図において、正確には最初の「CH 部」とCCS を算出する元となる(またそれ以降の)「CH 部」は別のものとなる。 　これを明記して欲しい(例えば後者の標記を「CH'部」とするなど)。		「CH 部」と「CH'部」を区別して表記します。「CH'部」を CLA の b4,b3 を「SM 適用」に設定したものとします。
68	45	C	Q&A の項番 13 では、HASH アルゴリズムは DF 内で 1 種類のため､表から外したとあるが、 　複数の証明書が一つのアプリ(DF)に来て、それぞれ異なる HASH アルゴリズムを 　サポートしていた場合はどうなるのか。		JICSAP でハッシュ関数をひとつに決めたわけではなく、JICSAP としての考え方は、 ・ひとつのアプリで使用するハッシュ関数はひとつ ・それが何であるかはアプリが知っている ・したがって､ハッシュ関数を識別する必要はない という場合をサポートしようというものです。 もちろん､ひとつのアプリが複数のハッシュを使うことを禁止しているわけではありません。（その実現方法は JICSAP では規定していません。）
69	73	C	7.4.10.WRITE RECORD 書き込み長さの制限(附属書 I にしたがった創生を行なった場合､その長さに従う)がない。		書込み長さの制限を追記します。

70	I-3	C	附属書 C　暗号アルゴリズム識別子国際登録機関登録番号は随時変更され得るので、IPA 等の HP にて確認すべきことを明記して欲しい。		ご指摘の注意事項を追記します。
71	114	C	GET SESSION KEY の拡張の意味があるか?		ご指摘の通り、Lc の拡張は不要と判断します。Lc：1or3 は、Lc：1 に修正します。

注１．部：仕様書の部
注２．区分：C （コメント）、Q （質問）、R （要望）
注３．続く２ 枚目はフリーフォーマットとします。