

公的分野における連携ＩＣカード技術仕様（改定）

平成16年3月12日

公的分野における
ＩＣカードの普及
に関する関係府省
連絡会議申し合せ

行政機関が発行するＩＣカードに関して、平成13年12月25日に当連絡会議において申し合わせた「公的分野における連携ＩＣカードの運用指針」（以下「運用指針」という。）に基づき、カードシステムの技術仕様について以下の通り定めるものとする。

1．基本的考え方

- 1) 平成13年7月27日の当連絡会議において、「住民基本台帳カードのスペックをベースとして連携ＩＣカードの基本的スペック」とすることを申し合わせており、財団法人地方自治情報センターにおいて定められた「住民基本台帳ネットワークシステム住民基本台帳カード仕様書」を基に、連携ＩＣカードの運用を円滑に進め、複数のカード発行者がそれぞれ発行したいずれのカードの上でも、複数の連携アプリケーションの実行が可能となるよう、仕様の見直し・追加を行い、カードシステムの技術仕様（以下、「技術仕様」という。）として定めるものとする。
- 2) 技術仕様は、別表のとおり、カード発行者、連携アプリケーション供給者の作成する要求仕様（以下「要求仕様」という。）において必ず準拠すべき「必須仕様」、要求仕様において引用することが望ましい「推奨仕様」、要求仕様作成時に仕様作成者が参考とすることができる「参照情報」の三種類の情報に分類し、カードの物理仕様、電気的特性及びプロトコル、機能仕様、カード運用システム、セキュリティの各編から構成する。

2．タスクフォースの設置

- 1) 運用指針1．にいう連携ＩＣカード発行者及び運用指針5．にいう運用指針を準用して連携ＩＣカードとしてＩＣカードを発行する者（以下「発行府省等」という。）が実装仕様の策定にあたってより具体的な規定を必要とする場合、ITの進捗によっ

て技術仕様の見直しが必要となる場合に迅速に対応するため、技術ワーキンググループの中に更に詳細に必要な仕様を規定するためのタスクフォースを設置し、引き続き検討を進めるものとする。

- 2) タスクフォースは、住民基本台帳カードを担当する総務省自治行政局、IT装備都市研究事業を担当する経済産業省及び発行府省等から構成され、適宜、検討結果は技術ワーキンググループを通じて連絡会議に報告することとする。なお、タスクフォースには、知見を有する外部の専門家が参画することを妨げない。
- 3) 発行府省等は、ICカードを発行、運用するに先立ち、タスクフォースにおいて先行する連携ICカードシステムとの互換性、マルチアプリケーション動作の確認を行わなければならない。なお、確認の方法についてもタスクフォースにおいて具体的なアプリケーションに則して検討を行う。

3 . 技術仕様の改定

技術仕様は、2 . 3)の確認の結果、技術仕様の見直し、追加が必要となる場合に改定を行う他、IT技術の進歩に対応するため、二年ごとに、内閣官房、総務省自治行政局、及び経済産業省を中心として技術仕様の改定の必要性について検討を行うこととする。なお改定する場合には、旧仕様との互換性について考慮することとする。また、上記以外でも、関連法令の改廃への対応やセキュリティ対応など至急の改定を要する場合には、適宜改定を行うこととする。

なお、以下の点について引き続きタスクフォースにおいて検討を行うこととする。

- ・ カードの外形について：SIMカード等の普及状況を踏まえて検討。
- ・ 券面表記について：偽造、変造の発生状況及びそれらの技術状況に応じた機能強化の必要性について検討。
- ・ 不揮発性メモリの容量の下限について：市場動向、技術動向を踏まえて検討。
- ・ 機能仕様について：ICカードに搭載されたICチップの機械語で動作するアプリケーション型のサービスにおける、マルチプラットフォームでの互換性を確保する方法について、具体的なアプリケーションに則して検討。
- ・ セキュリティの強化について：技術動向を踏まえて検討。あわせて、リーダライタのセキュリティについても検討。

別表

平成 16 年 3 月 12 日改定

		必須仕様	推奨仕様	参照情報
カードの物理仕様	カードのインターフェース	非接触近接型インターフェース (JIS X 6322-1:2001) を有する		
	一般的物理特性	JIS X 6301:1998 ID1 に準拠する		
	材質	非塩ビ系の素材を使用する		
	寸法	JIS X 6301:1998 ID1 に準拠する ただし、エンボスについては規定しない		
	追加物理的特性	JIS X 6322-1:2001 に準拠する 動的曲げ強さ及び動的ねじれ強さの試験条件は、JIS X 6303:2000 4.2.9 及び JIS X 6303:2000 4.2.10、試験方法は JIS X6305-1:2003 参照		
	券面	券面印刷には複数の偽造防止機能を施す 統一マークを施す 券面の情報付与領域には、情報保護機能を施す	各アプリケーションの固有のマークを施す 顔写真を有する	連携 IC カード券面の偽造防止技術ハンドブック (H14.7)
	不揮発性メモリの容量の下限		不揮発性メモリ容量の下限値は 32KB 以上とする	
電気的特性及びプロトコル	電力伝送	JIS X 6322-2:2001 に準拠する ただし、最小動作磁界は 4.0A / m (rms) とする	据置型及び開放型リーダライタを使用する場合は、近接型通信インタフェース実装規約書第 1.1 版 (NMDA H13.7) 8. に準拠する	住民基本台帳カード対応については、住民基本台帳ネットワークシステム近接型通信インタフェース実装規約書第 1.12 版 (H14.4) 6.
	信号インターフェース	JIS X 6322-2:2001 に規定される B 型の信号インターフェースに準拠する		
	初期化及び衝突防止	JIS X 6322-3:2001 に規定される B 型の初期化及び衝突防止に準拠する	推奨仕様 据置型及び開放型リーダライタを使用する場合は、近接型通信インタフェース実装規約書第 1.1 版 (NMDA H13.7) 12. に準拠する	住民基本台帳カード対応については、住民基本台帳ネットワークシステム近接型通信インタフェース実装規約書第 1.12 版 (H14.4) 10.
	伝送プロトコル	JIS X 6322-4:2002 に準拠する	据置型及び開放型リーダライタを使用する場合は、近接型通信インタフェース実装規約書第 1.1 版 (NMDA H13.7) 13. に準拠する	参照情報 住民基本台帳カード対応については、住民基本台帳ネットワークシステム近接型通信インタフェース実装規約書第 1.12 版 (H14.4) 11.

	必須仕様	推奨仕様	参照情報	
カードの機能仕様	カードのアーキテクチャ	住民基本台帳カード仕様書第2.3版(H15.7)第4章 1.1、または、住民基本台帳カードType 仕様書第2.0版(H15.1)序章2.5に準拠する		
	プラットフォーム仕様	住民基本台帳カード仕様書第2.3版(H15.7)第4章 2.1.1、または、住民基本台帳カードType 仕様書第2.0版(H15.1)第2章に準拠する カード種別判定機能を実現する下記のプラットフォーム共通コマンドを規定する・ファイル選択コマンド SELECT FILE:JIS X 6306:1995 に準拠する	カード種別判定機能を実現する 下記のプラットフォーム共通コマンドを規定する 照合 認証系コマンド INTERNAL AUTHENTICATE:JIS X 6306:1995 に準拠する オブジェクト データアクセスコマンド GET DATA:ISO/IEC7816-4 に準拠する	住民基本台帳カード仕様書第2.3版(H15.7)第5章
	アプリケーション機能仕様	データ型(ファイル型)サービスを利用する場合は、下記コマンドセットを規定する 照合 認証系コマンド VERIFY,GET CHALLENGE,EXTERNAL AUTHENTICATE:JIS X 6306:1995 に準拠する レコードアクセス系コマンド READ RECORD(S),APPEND RECORD,UPDATE RECORD:JIS X 6306:1995 に準拠する WRITE RECORD,ERASE ALL RECORDS,UPDATE RECORD:JICSAP Ver2.0(H13.7)に準拠する 鍵ファイル管理運用コマンド UNLOCK KEY,CHANGE KEY:JICSAP Ver1.1(H10.7)に準拠する 又は CHANGE REFERENCE DATA,RESET RETRY COUNTER:JIS X 6300-8:2001 に準拠する PK コマンド COMPUTE DIGITAL SIGNATURE,VERIFY DIGITAL SIGNATURE,VERIFY CERTIFICATE:JIS X 6300-8:2001 に準拠する	アプリケーションサイズの上限は5KBとする	JICSAP 外部端子付きICカード仕様 Ver1.1(H10.7) JICSAP ICカード仕様 V2.0 (H13.7)第3部 JICSAP:日本ICカードシステム利用促進協議会

		必須仕様	推奨仕様	参照情報
カード運用システム	プレーヤの定義	NICSS 要件書 Ver1.20(H13.4) / NICSS 参照仕様 Ver1.00(H13.4) / NICSS 運用ガイドライン Ver1.00 (H13.4) に準拠する NICSS 次世代 ICカードシステム研究会		
	アプリケーションの管理			
	カード発行・停止・更新			
	APダウンロード削除・停止			
	サービス利用			
	カード運用状態通知			
	ホットリスト			
セキュリティ	物理仕様	耐タンパ性を有する		
	暗号処理	公開鍵の暗号処理機能を有する	RSA1024bit 同等以上の強度を持った暗号機能を有する	
	セキュリティポリシー	ISO/IEC15408 の EAL 4以上の保障レベルを有する ISO17799 に準拠するセキュリティポリシーを策定し運用する 国の行政機関については、「情報セキュリティポリシーに関するガイドライン」(平成12年7月18日情報セキュリティ対策推進会議決定)に基づき、所要の措置を講じる		