

マイナンバーカードアプリケーション搭載システム  
導入検討の手引き  
(地域住民向け領域設定システム編)  
(基礎編)

第 2.0 版

平成 29 年 7 月

地方公共団体情報システム機構

## 目 次

I	地域住民向け領域の利用について	2
1	地域住民向け領域利用の基本的な考え方	2
2	マイナンバーカードの領域利用のイメージ	3
3	マイナンバーカードアプリケーション搭載システムの利用	4
II	「カード AP 搭載システム」の概要	5
1	システムのコンセプト	5
2	運用面の特徴	6
2.1	カード運用状態による利用制限	6
2.2	地域住民向けサービスの利用と停止	6
2.3	住民情報入力作業の省力化	6
2.4	共同利用	7
2.5	チューニング	8
2.6	市町村独自サービスの追加	9
2.7	引越継続及び外国人への対応	9
2.8	住基ネット CS との連携機能に係る暗号方式への対応	9
2.9	カード AP 搭載システムのログイン認証方式の追加	9
3	提供できるサービス	10
3.1	証明書等自動交付サービス	10
3.2	図書館サービス	11
4	提供できる地域住民向けサービスとカード AP 搭載システムの関係	12
III	セキュリティ対策	13
1	個人情報保護のための施策	13
1.1	制度面からの対策	13
1.2	技術面からの対策	13
1.3	運用面からの対策	13
2	セキュリティ対策概要	14
2.1	カード AP 搭載システムでのセキュリティ対策	14
2.2	市町村にて検討すべきセキュリティ対策	16

## 本書の使い方

マイナンバーカード（※）の地域住民向け領域の利用に関する内容等、導入の検討前に利用します。

※住民基本台帳カード（以下「住基カード」という。）についても、同様に利用できます。

# I 地域住民向け領域の利用について

## 1 地域住民向け領域利用の基本的な考え方

マイナンバーカードには、住基ネット上の利用領域のほかに、公的個人認証サービスのための利用領域等が確保されています。これら以外の領域は、市町村が独自利用を行うための領域（以下「地域住民向け領域」(※)という。)として確保できます。市町村は、条例の定めるところにより、この地域住民向け領域を活用した様々なサービス（以下「地域住民向けサービス」という。）を提供できます。

※住基カードについては、「独自利用領域」となります。

地域住民向けサービス例を以下のとおり想定しています。

- ①印鑑登録証明
- ②証明書自動交付
- ③図書館カード
- ④公共施設予約
- ⑤申請書自動作成
- ⑥検診・健康診断等
- ⑦避難者確認
- ⑧各種ポイント
- ⑨救急支援
- ⑩地域通貨
- ⑪その他（スポーツ施設予約・病院診察カード等）

※総務省「マイナンバー制度とマイナンバーカード」サイトの「マイナンバーカードの普及促進に関する取組状況(サービス別)」より。[http://www.soumu.go.jp/kojinbango\\_card/03.html](http://www.soumu.go.jp/kojinbango_card/03.html)

## 2 マイナンバーカードの領域利用のイメージ

マイナンバーカードには、複数のカードアプリケーション（以下「カード AP」という。）を搭載できます。カード AP とは、地域住民向けサービスの提供に必要な情報を登録するもので、それぞれの地域住民向けサービス専用利用されます。他の地域住民向けサービスからの利用及び参照はできません。

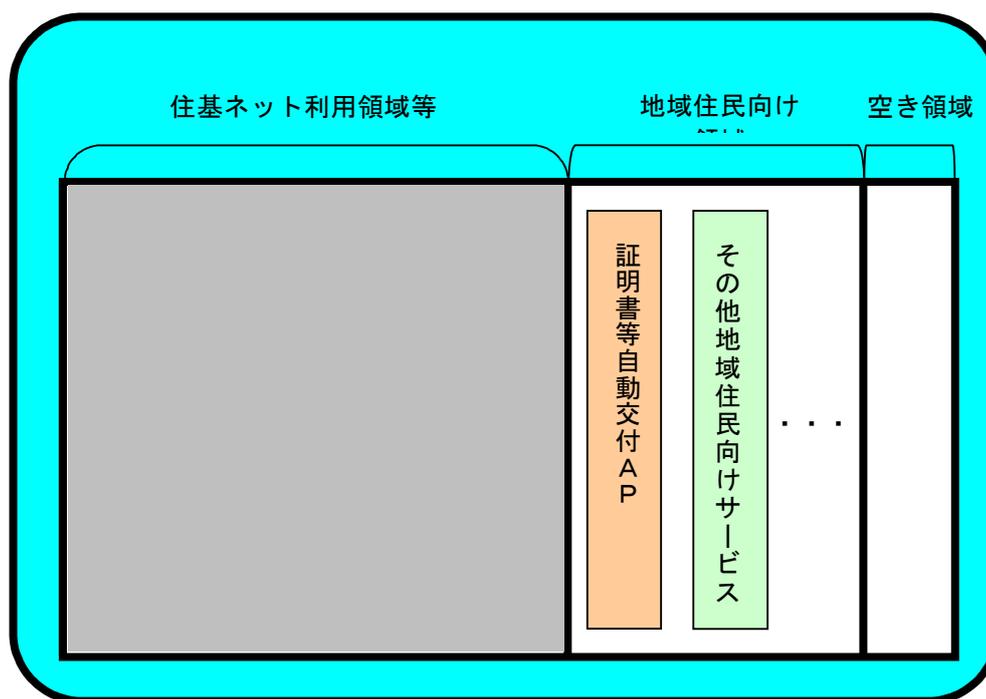
マイナンバーカードには、交付時に住基ネット利用領域等が確保されますが、それ以外の領域は、地域住民向け領域として、地域住民向けサービスの提供に必要な情報を登録するためのカード AP を搭載できます。

地域住民向けサービスを提供するためには、地域住民向け領域に、地域住民向けサービスの提供に必要なカード AP を搭載しなければなりません。

地域住民向け領域には、様々な地域住民向けサービスのカード AP を搭載することが可能です。ただし、搭載するカード AP の数は、交付するマイナンバーカードのメモリ容量により異なります。

なお、地域住民向け領域内のカード AP は、マイナンバーカードの交付後、住民の希望により随時に搭載や削除が可能です。

下図にマイナンバーカードの領域利用イメージを示します。



### 3 マイナンバーカードアプリケーション搭載システムの利用

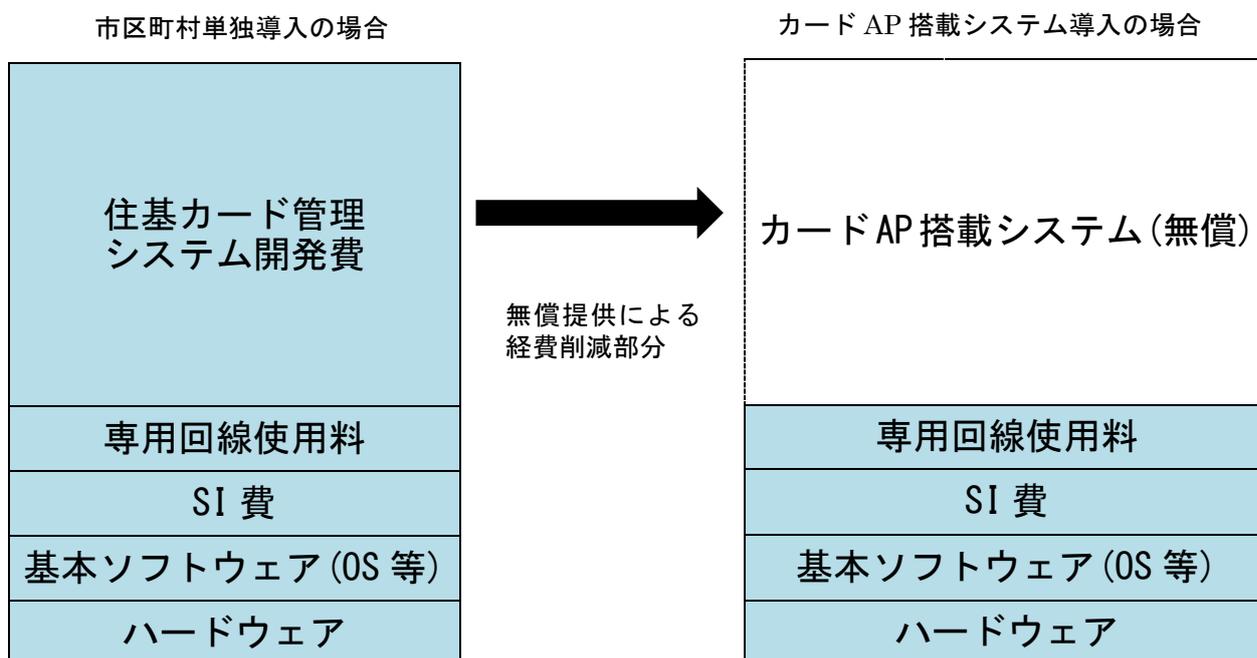
上記の①、②、及び③の地域住民向けサービスについては、市町村において地域住民向けサービスを容易に提供することが可能なシステムとして、地方公共団体情報システム機構（以下「J-LIS」という。）がマイナンバーカードアプリケーション搭載システム（以下「カード AP 搭載システム」という。）を、希望する市町村に対し無償で提供しています。

カード AP 搭載システムを利用することにより、これまで財源やマンパワーの不足等の理由から地域住民向けサービスの導入を見送っていた市町村においてもマイナンバーカードを利用した地域住民向けサービスを容易に提供することができます。

このような地域住民向けサービスを利用できるシステムを、市町村単独で導入した場合とカード AP 搭載システムを利用した場合の経費のメリットについては、以下の比較表を参考にしてください。

## 比較表

### カード AP 搭載システムを導入することによる経費のメリット



※どちらの場合にも稼働後のランニングコストは必須です。

## II 「カード AP 搭載システム」の概要

### 1 システムのコンセプト

(1) すべての種類のマイナンバーカード（※）に対応

市町村合併等により、ひとつの市町村で異なるベンダのマイナンバーカードが混在する場合でも、システムとして対応できます。

(2) 市町村の業務の実状に適切に対応

プログラムの変更（カスタマイズ）を行うことなく、パラメータの設定により、画面レイアウトの変更、帳票様式の変更、データベース項目の追加ができます。

パラメータの設定は、市町村の操作者により、簡単にできます。

(3) 複数の市町村での共同利用にも配慮

マイナンバーカードを交付する市町村での地域住民向けサービス提供だけでなく、他の市町村と共同利用することもできます。

(4) 市町村独自システムの開発が容易

市町村独自サービスを提供するシステム（以下「市町村独自システム」という）を構築する際に、カード AP 搭載システムと連携すれば、安価かつ容易に開発できます。

※地域住民向け領域の容量には、制限があります。詳細はカードベンダにお問い合わせください。

## 2 運用面の特徴

### 2.1 カード運用状態による利用制限

カード AP 搭載システムでは、住基ネット GS と連携することにより、マイナンバーカードの運用状態に基づき、運用中のカードでのみ、カード AP の搭載及び地域住民向けサービスの提供を行います。

### 2.2 地域住民向けサービスの利用と停止

カード AP 搭載システムでは、地域住民向けサービスの利用開始及び停止手続きを、円滑に進められます。

#### (1) 地域住民向けサービスの利用開始手続き

市町村の操作者は、住民からの地域住民向けサービス利用の申込みに基づき、地域住民向け領域へのカード AP の搭載及び業務システムへの利用登録をします。

#### (2) 地域住民向けサービスの停止手続き

市町村の操作者は、マイナンバーカード紛失の届出等により、利用している地域住民向けサービスを停止します。

### 2.3 住民情報入力作業の省力化

#### (1) 既存住基システムからの情報の取込み

カード AP 搭載システムでは、既存住基システムから住民情報を取り込むことができるため、操作者が、住民情報を入力する必要がありません。取り込む方法には、オフラインと中継サーバを使用するオンラインの 2 種類があります。

#### (2) 各業務システムへの情報伝達

カード AP 搭載システムでは、利用者の情報として、住民情報を管理します。これらの情報は、必要に応じて、地域住民向けサービスの提供を行うシステムにオンラインで伝達できます。

## 2.4 共同利用

### (1) システムの共同利用

カード AP 搭載システムでは、ハードウェア、OS、ミドルウェア、アプリケーション及びカード AP を、複数市町村で共同利用できるため、各市町村で、導入・運用コストの低減が図れます。

### (2) 登録情報の共同利用

カード AP 搭載システムでは、複数市町村で各システムに登録されるマスタ情報等を共同利用できるため、住民への広域的な地域住民向けサービスの提供やシステムの管理が一元化されることによる操作者の利便性向上が図れます。

## 2.5 チューニング

カード AP 搭載システムは、各市町村の業務の実状により、市町村の操作者が、容易にチューニングできます。

チューニングは、パラメータ等の設定で行い、DB 項目の追加や帳票レイアウトの変更のほか、画面の色、フォント、ボタン文言、タイトルガイダンスの文言、説明文等の変更ができます。

利用環境設定

下記のメニューの中から、利用する業務のボタンを押してください。

タイトルガイダンスの変更ができます。

背景色の変更ができます。

カード運用	カードを運用するための、利用者情報登録及びカードAPのダウンロード/削除を行うメニューです。	利用者管理	実行
データ管理	外部システムからのデータ(カード運用情報、住民情報)取り込み及び利用者情報のファイル出力を行うメニューです。	利用者管理 カードAPダウンロード カードAP削除 カード内AP一覧参照 カード障害切り分け	実行
オペレータ管理	オペレータ認証システムへの業務内IDの登録削除及び業務内IDの新規登録/権限の変更/削除を行うメニューです。	オペレータID管理	実行
システム設定	基本システムの初期設定及び環境設定を行うメニューです。システムの初期設定時のみ利用します。	独自利用領域キー登録	実行

説明文の変更ができます。

ボタン文言の変更ができます。

終了

中東京市: OP0501

## 2.6 市町村独自サービスの追加

市町村は、カード AP 搭載システムが提供する地域住民向けサービスの他に、市町村独自サービスを追加できます。

市町村独自システムを開発する際に、カード AP 搭載システムが規定するインタフェースに準ずることとで、カード AP 搭載システムが提供する地域住民向けサービスと同様の運用ができます。

また、カード AP アクセスモジュール（カード AP 内の情報を簡易に読み書きできるソフトウェア）を利用すれば、容易に市町村独自システムにマイナンバーカードとのインタフェースを追加できます。

なお、市町村独自システムを開発する際に、カード AP 搭載システムが規定するインタフェースに準じない場合においても、地域住民向け領域にカード AP をダウンロード及び削除できます。

## 2.7 引越継続及び外国人への対応

カード AP 搭載システムは、マイナンバーカードの引越継続利用に対応しており、他市で発行したマイナンバーカードを引越後も継続して条例利用が可能です。※

また、外国人住民に対して発行されたマイナンバーカードも条例利用が可能です。

※IC カード標準システム Ver7.2.1（引越継続未対応のバージョン）以前で地域住民向け領域設定を行った住基カードについては、カード AP 搭載システムで引越継続利用を行うことはできません。

## 2.8 住基ネット CS との連携機能に係る暗号方式への対応

カード AP 搭載システムサーバは、住基ネット CS とカード運用状況等のデータ連携を行っていますが、その連携機能において電子政府推奨暗号リストに則った暗号方式に対応しています。

※電子政府推奨暗号リスト：<http://www.cryptrec.go.jp/list.html>

## 2.9 カード AP 搭載システムのログイン認証方式の追加

カード AP 搭載システムのログイン認証機能（オペレータ認証機能）においては、従来の ID・パスワードによる認証方式に加え、生体認証方式（指紋による認証）にも対応しています。

### 3 提供できるサービス

カード AP 搭載システムを利用し、次のような地域住民向けサービスを提供できます。

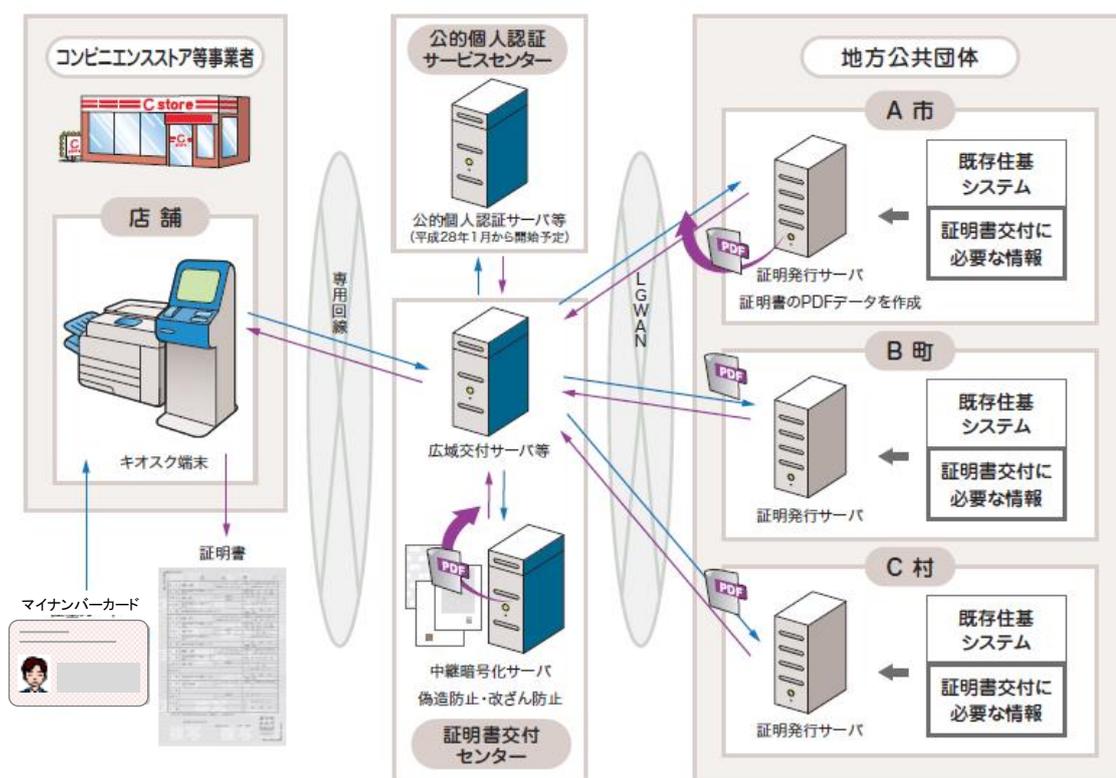
#### 3.1 証明書等自動交付サービス

##### (1) コンビニ交付サービス

コンビニ交付サービスは、コンビニエンスストア等でのキオスク端末を利用し、住民票の写し、印鑑登録証明書、その他の各種証明書（以下「各種証明書」という。）を交付するものです。また、市町村が受付窓口の時間外や土曜、日曜及び祝日等にも、利用者は希望する時に自由に各種証明書を受け取ることができます。（年末年始を除く 6:30 から 23:00 まで利用可能です。）

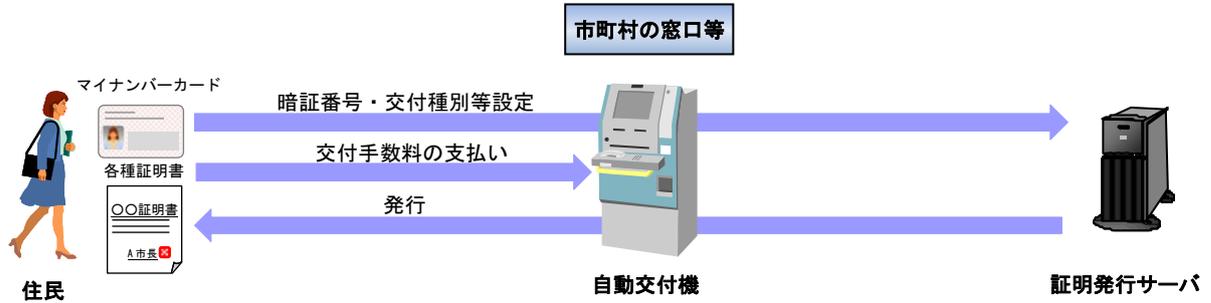
コンビニ交付サービスを地域住民向けサービスとして実施する場合は、カード AP 搭載システムを導入する必要があります。

コンビニ交付サービスの詳細については、「住民票の写し等証明書交付サービス（コンビニ交付）導入検討の手引き」を参照してください。



(2) 自動交付機によるサービス

当サービスは、自動交付機を利用して、各種証明書を交付するものです。自動交付機を設置すれば、市町村受付窓口の営業時間外や非営業日にもサービス提供できるため、住民は、都合の良い時に証明書等を受け取れます。



### 3.2 図書館サービス

当サービスは、マイナンバーカードを図書館カードとして利用し、図書館の窓口サービスを提供するものです。住民は、マイナンバーカードを交付された市町村の図書館に加え、複数の市町村にまたがって図書館での窓口サービスを受けられます。



## 4 提供できる地域住民向けサービスとカード AP 搭載システムの関係

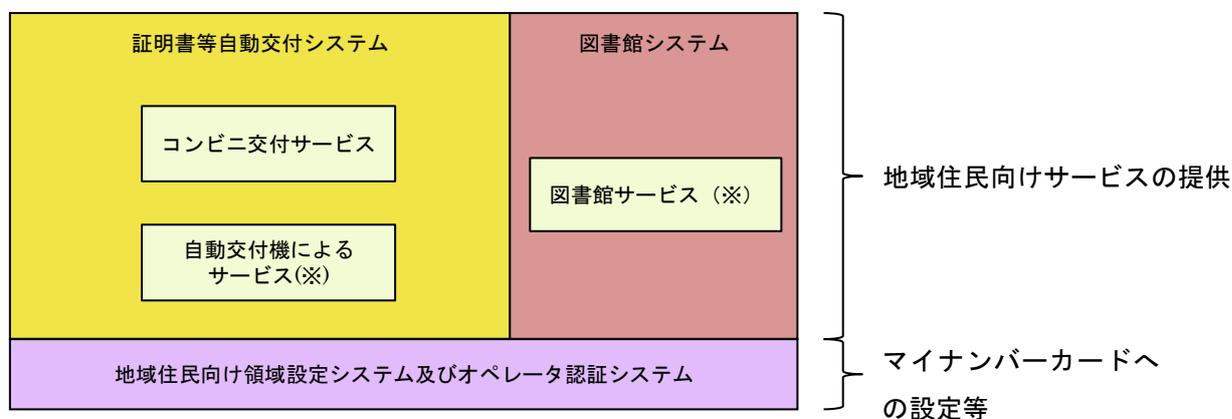
カード AP 搭載システムが提供する地域住民向けサービスは、前章で記載した以下の3つで、下図のとおり、地域住民向け領域設定システム、オペレータ認証システム及び各業務システムが動作します。

カード AP 搭載システムは、利用者情報登録や、マイナンバーカードへの地域住民向け領域設定、カード AP 搭載・削除といった、地域住民向けサービスを利用するための設定や、カード AP 搭載システムを操作するオペレータの管理等を行うシステムです。

業務システムは、地域住民向け領域設定システムで設定したマイナンバーカードに対して、コンビニ交付サービスや、図書館サービス等の地域住民向けサービスを提供するためのシステムです。

なお、自動交付機によるサービス及び図書館サービスについては、インターフェースのみを規定していますので、これら地域住民向けサービスを提供する場合は、市町村において、既存のシステムを当該インターフェースに合わせて改修するか若しくは事業者の提供するシステムを別途調達するかの対応を行なう必要があります。

- ① コンビニ交付サービス
- ② 自動交付機によるサービス
- ③ 図書館サービス



※ インターフェースのみ規定

## III セキュリティ対策

### 1 個人情報保護のための施策

カード AP 搭載システムでは、住民の個人情報を取り扱うことから、個人情報の保護を重要な課題としています。このため、個人情報保護に関する国際基準（以下「OECD8 原則」という。）を踏まえた上で、制度・技術・運用の 3 つの側面から個人情報を保護する対策を講じています。

#### ※ OECD8 原則

個人のプライバシー保護を目的として OECD が理事会勧告として 1980 年に採択したもので、8 原則とは、①収集制限、②データ内容、③目的明確化、④利用制限、⑤安全保護、⑥公開、⑦個人参加、⑧責任のそれぞれの原則です。

#### 1.1 制度面からの対策

- カード AP 搭載システムに記録される個人情報は、行政機関の保有する電子計算機処理に係る個人情報保護に関する法律に基づき取り扱います。

#### 1.2 技術面からの対策

- ネットワークからの不正アクセス及び情報漏えいを防止します。
- カード AP 搭載システムでは、認証技術を用いマイナンバーカード内へ安全に情報を搭載します。また、オペレータ認証システムにより、不正なシステム利用及びデータ利用を防止します。さらに、不正操作を発見あるいは追跡するための記録を保持します。
- 地域住民向け領域に搭載されたアプリケーションを利用する際、本人の暗証番号を設定し、なりすまし行為等の不正を防止します。

#### 1.3 運用面からの対策

カード AP 搭載システムは、以下に示す項目について、運用管理規程等を策定するための方針を示しています。方針に従って市町村にて運用面での具体的なセキュリティ対策を策定のうえ実施してください。

- サーバ装置、端末又はネットワーク等の機器についての盗難又は不正利用の防止に係る規定
- マイナンバーカード、帳票又は媒体の保管及び使用に係る規定
- ウィルス対策やログの監査に係る規定 等

これらの詳細について知りたい場合は、J-LIS に資料提供申込を行ってください。

## 2 セキュリティ対策概要

### 2.1 カード AP 搭載システムでのセキュリティ対策

カード AP 搭載システムにて実施しているセキュリティ対策の概要を以下に示します。セキュリティ対策の詳細について知りたい場合は、J-LIS に資料提供申込を行ってください。

#### (1) システムのセキュリティ対策

項番	対策	内容
1	ログイン認証	システムを操作する操作者及び住民の正当な権限の有無を確認します。 正当な権限を持たない者による操作や、保護すべき情報資産に対する不正アクセスからシステムを保護します。 生体認証方式、操作者識別カードによる認証方式、又は ID・パスワードによる認証方式のうちのいずれかを導入します。
2	停止措置	マイナンバーカード紛失時及び盗難時における「なりすまし」によるマイナンバーカード不正使用を防止します。 住民からマイナンバーカード紛失、盗難の届出があった場合に、そのマイナンバーカードに対するサービス提供を停止します。 また、サービス利用 ID・パスワードの不正使用を防止するため、住民からマイナンバーカード紛失・盗難の届出があった場合に、該当サービス利用 ID に対するサービス提供を停止します。
3	個人情報取得の制限	カード AP 搭載システムに登録された住民情報のシステム横断的な収集及び関連付け並びに目的外利用を防止します。業務システムごとに固有の情報を管理することで、別システムからの個人情報の取得を制限します。
4	住民情報アクセス制限	複数市町村でカード AP 搭載システムを共同利用する際に、各市町村で参照・登録できる住民情報を制限できます。参照可能な住民情報を自団体住民のみと設定します。
5	監査・故障解析ログ取得	システム稼働時に、情報資産に対するアクセス履歴やシステムの稼働状況を記録します。不正操作の発見あるいは追跡に利用します。

#### (2) 地域住民向け領域のセキュリティ対策

項番	対策	内容
1	アプリケーション ファイアウォール	カード AP 間の不正アクセスを防止します。各カード AP へのアクセスを、それと一対の業務システムに制限します。
2	暗証番号設定とロック（停止状態）	カード AP ごとに暗証番号を設定することで、本人以外の不正利用を防止します。暗証番号の入力を数回（※）間違えると、カード AP をロック（停止状態）し、一時的に利用停止状態とします。

項番	対策	内容
3	相互認証	不正カードや不正システムからのアクセスを防止するため、カード AP と業務システムの間で相互認証します。カード AP とそれと一対の業務システムとの間でのみ、相互にアクセスできます。
4	独自利用領域キーの設定	第三者による地域住民向け領域の不正利用を防止します。マイナンバーカード、カード AP 搭載システムの双方に電子的な鍵を設定し、合致する場合にのみ、地域住民向け領域の設定、カード AP の搭載・削除等ができます。

※窓口交付機能においては3回（固定値）ですが、証明発行サーバ側でそれより少ない回数でロックするように設定されている場合は、それに従います。

### (3) 通信データのセキュリティ対策

項番	対策	内容
1	通信相手の認証	ネットワーク上での通信相手のなりすましを防止します。サーバ証明書によるサーバ認証と暗証番号やサービス利用 ID・パスワードによる利用者認証をします。
2	通信データの暗号化	ネットワーク上の盗聴、改ざんを防止します。端末とサーバ間の通信を暗号化します。
3	電子記録媒体内データに対する暗号化	電子記録媒体にてデータ交換を行う際の盗聴、改ざんを防止します。住基ネット CS から受け渡される電子記録媒体の情報を暗号化し、第三者からの盗聴、改ざんを防止します。

## 2.2 市町村にて検討すべきセキュリティ対策

市町村にて検討すべきセキュリティ対策を下表に示します。

### (1) ネットワークのセキュリティ対策

項番	対策	内容
1	専用回線の採用	カード AP 搭載システムで使用するネットワーク回線は、盗聴、なりすまし、改ざん等の防止のため、専用回線を利用し、閉じたネットワークの構築を前提とします。
2	ファイアウォールの設置	ネットワークを介した不正行為や不正侵入に対して、カード AP 搭載システムを保護するファイアウォールを設置し、アクセス制御します。

### (2) その他のセキュリティ対策

項番	対策	内容
1	運用管理規程	機器、帳票、媒体等の取扱いを規定した運用管理規程等の運用面のセキュリティ対策を実施します。 運用管理規程は、カード AP 搭載システムのセキュリティを確保するために、市町村がそれぞれの現状に基づき規定し、遵守します。
2	物理的侵入対策	技術面と同様に、入退出管理に代表される物理面のセキュリティ対策も実施します。 物理的な不正侵入への対策は、カード AP 搭載システムのセキュリティを確保するために、市町村がそれぞれの現状に基づいた対策を立案し、講じます。