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
（拡張利用領域編）
（都道府県・市区町村・行政機関等向け）

第 2.1 版

2020 年 1 月

地方公共団体情報システム機構

目　次

Ⅰはじめに

本書は、マイナンバーカードを利用した、職員証、入退館管理、図書館等の各種サービスを提供するために必要となる情報（カードアプリケーション（以下「カードAP」という。））を登録するためのシステムとして、地方公共団体情報システム機構（以下「機構」という。）が提供する「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。）の導入を検討するサービス提供主体向けの資料です。

Ⅰ章では、マイナンバーカードに確保されている領域（※）及びその利用について説明し、Ⅱ章以降で、カードAP搭載システムについて説明します。

本書は、国都道府県、市区町村、又は行政機関を対象としています。民間事業者においては、「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（民間事業者向け）」を参照してください。

本書は、カードAP搭載システムに係る概要を記しています。より詳細な資料については、以下のサイトに記載の要領に従い、機構に情報の開示を申請のうえ入手してください。

・マイナンバーカードアプリケーション搭載システム資料提供について
（https://www.j-lis.go.jp/rdd/card/bango-ap/cms_bangoap_001.html）

※本書では、主に拡張利用領域（Ⅱ章参照）を利用する場合について記載しています。地域住民向け領域（Ⅱ章参照）を利用する場合の詳細ついては、機構のホームページに掲載の、「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）」を参照してください。

Ⅱマイナンバーカードの領域利用

1　マイナンバーカードの領域について

マイナンバーカードには、住基ネットや公的個人認証等に利用する領域があらかじめ確保されています。

それら以外の領域（空き領域）として、市区町村が当該市区町村の住民のために利用することができる「地域住民向け領域」や、行政機関（※１）、都道府県、市区町村、民間事業者その他の者（以下「サービス提供者」という。）が告示（都道府県、市区町村にあっては、条例）で定め利用することができる「拡張利用領域」（ただし、市区町村が利用する領域は、「広域サービス向け領域」という。）が確保されています。

マイナンバーカードの地域住民向け領域及び拡張利用領域は、行政手続における特定の個人を識別するための番号の利用等に関する法律第十八条（以下「番号法」という。）に規定する事務の処理に利用することができます。

本書では、行政機関・都道府県・市区町村・その他の者（※２）が拡張利用領域を事務の処理に利用するために必要となる、カード AP 搭載システムについて示します。

なお、拡張利用領域を使ったサービスとしては、社員（職員）証サービス、入退館サービス、図書館サービス及びポイントサービス等が想定されます。

※１ 行政機関の保有する個人情報の保護に関する法律第二条第一項に規定する行政機関が該当します。

※２ 番号法第十八条第二号に規定する「地方公共団体」及び同法施行令第十八条第二号に規定する「行政機関、独立行政法人等又は機構」、「地方公共団体の機関」、及び「地方独立行政法人」（以下「行政機関等」という。）が該当します。

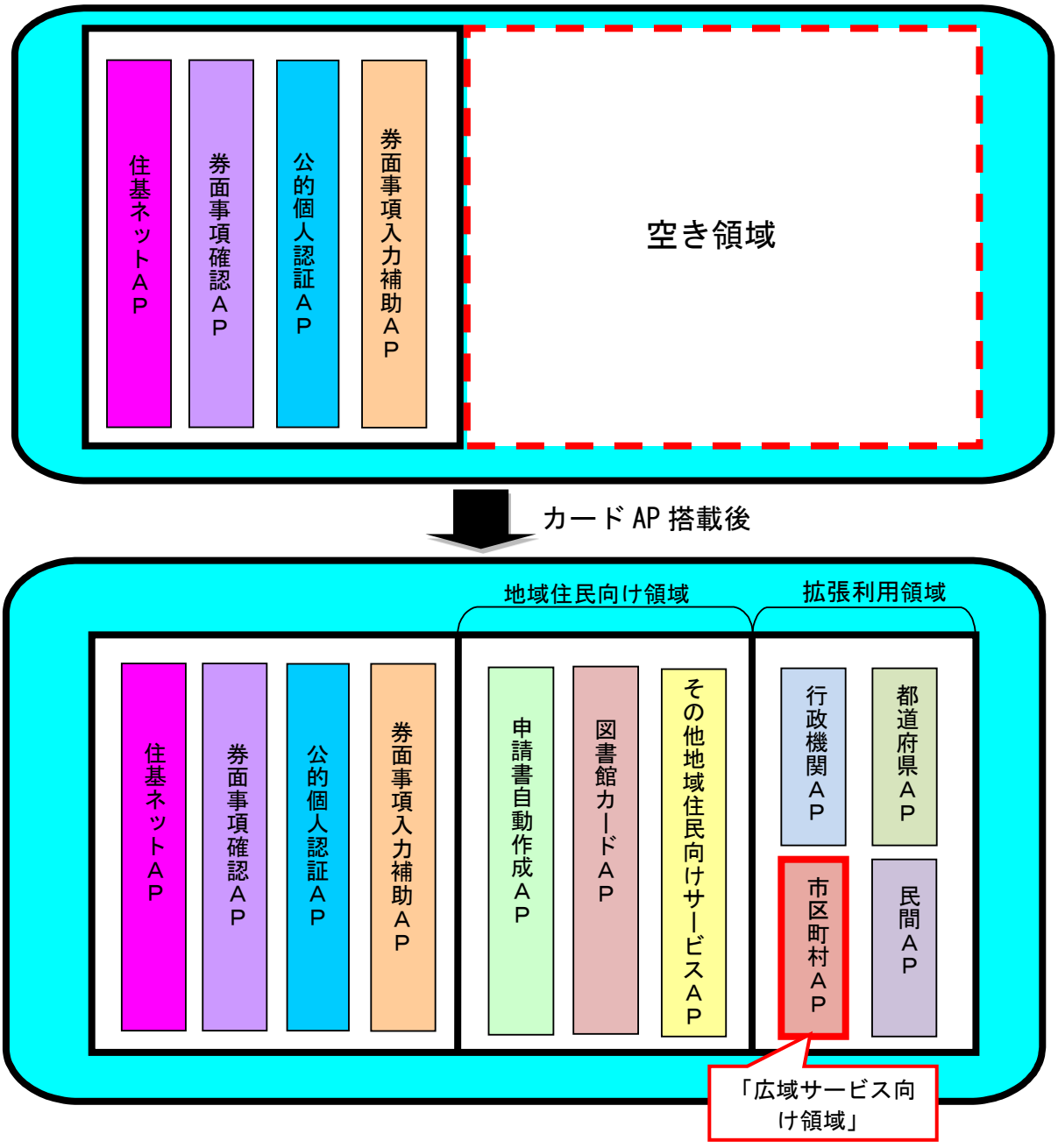
2　マイナンバーカードの領域利用のイメージ

マイナンバーカードには、複数のカード AP を搭載できます。カード AP とは、特定のサービスの提供に必要な情報を登録するもので、他の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は、標準で住基ネット AP、券面事項確認 AP、公的個人認証 AP、券面事項入力補助 AP が搭載されています。それら以外の空き領域は、地域住民向け領域、もしくは拡張利用領域として、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。

拡張利用領域でサービスを提供するためには、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。なお、拡張利用領域内のカード AP は、利用者の希望により随時に搭載や削除が可能です。

以下に、マイナンバーカードの領域利用イメージを示します。



3　空き領域の特性

地域住民向け領域及び拡張利用領域には、以下の特性があります。

(1) 領域の利用対象者

地域住民向け領域は、住民票のある市区町村で発行されたマイナンバーカードに対して、その市区町村でのみ利用可能であり、住民票のない市区町村や、国都道府県、行政機関等ではカードAPの追加や削除を行うことができません。

一方、拡張利用領域は、住民票の有無にかかわらず、市区町村や、国都道府県、行政機関等でもカードAPの追加や削除を行えます。

住民票のある市区町村で交付されたマイナンバーカードへのカードAPの搭載・削除の可否

	国都道府県	市区町村		行政機関等
		住民票あり	住民票なし	
地域住民向け領域	×	○	×	×
拡張利用領域	○	○	○	○

○：カードAPの追加や削除が可能　×：カードAPの追加や削除が不可

※マイナンバーカード上に存在する地域住民向け領域及び拡張利用領域は、それぞれ1領域ずつであり、サービス提供者により領域を共有して利用します。マイナンバーカードの空き容量は有限であるため、カードAPにおいて必要以上に領域を確保したり、不必要な数を搭載したりすることが無いよう留意する必要があります。

(2) 引越継続利用

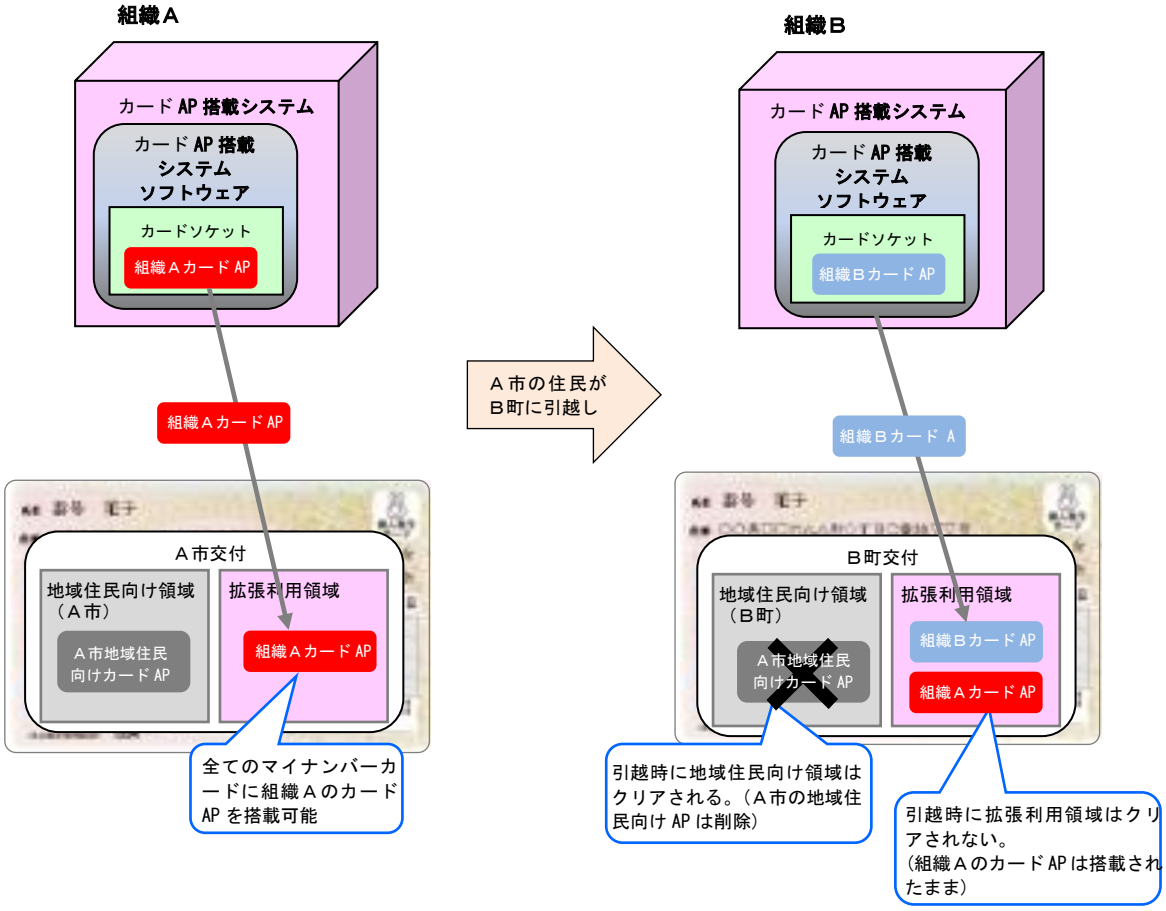
地域住民向け領域に搭載されたカードAPは、引越先にてマイナンバーカードの継続利用手続きを行う際に自動的に削除されます。

一方、拡張利用領域に搭載されたカードAPは、引越先にて継続利用手続きを行う際に削除されません。

転出の際の処理

領域	転出の際の処理
地域住民向け領域	転出の際にカードAPが自動的に削除される
拡張利用領域	転出しても搭載したカードAPが削除されない

引越継続利用のイメージ



III　システム概要

機構にて提供するカードAP搭載システムにより、拡張利用領域（※）にカードAPを搭載できます。

なお、職員証、入退館管理、図書館等のサービスそのものを提供するためのシステム（以下「業務システム」という。）については、サービス提供者にて別途準備（改修）する必要があります。

※カードAP搭載システムにより、地域住民向け領域にもカードAPを搭載できます。詳細については、機構のホームページに掲載の「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）」を参照してください。

1 機能概要

※各機能の詳細については、情報開示の申請（Ⅳ１(1)参照）後に機構より提供される、詳細資料に含まれる手引書等を参照してください。

(1) オペレーター認証

カードAP搭載システムは、システム操作者が適正な権限保有者であることを確認するための認証機能及び操作可能範囲を制限する権限管理機能を有しています。

なお、システム操作者の認証方式については、生体認証、もしくはID・パスワードによる認証のいずれかを選択可能です。

(2) カードAP管理

サービス提供者からの申請に基づいて複数のカードAPの登録が可能です。

また、サービス提供者において、登録された複数のカードAPから端末機の操作者が所属する利用機関ごとにダウンロードすることができるカードAPの設定を行えます。

(3) カードAPダウンロード・削除

対象のマイナンバーカードについて、カードAPのダウンロードと削除を行うことが可能です。複数カードAPから都度ダウンロードするカードAPを選択する方式のほか、予め自動で搭載するカードAPを設定しておき、都度カードAPの選択をしない方式も利用可能です。

(4) 利用者管理

マイナンバーカードに対してカードAPを搭載する際に、マイナンバーカードに紐付く利用者情報(氏名等)を登録することが可能です。（※）この機能により登録したデータは利用者情報連携機能により外部システムへ連携することが可能です。

(5) カード障害切り分け

マイナンバーカード操作時にエラーが発生した場合、当該カードの障害発生状況を確認することが可能です。

(6) カード一時停止等のステータスのオンライン提供

カード AP を格納したカードを紛失した場合には、マイナンバーカード所持者が、個人番号カードコールセンターに紛失等の届出を行えば、サービス提供者の業務システムにおいても、オンラインでそのステータスの提供を受けることができます。(※)

※拡張利用領域のみを利用している場合は、１日１回連携されます。なお、サービス提供者が直接業務システムに失効情報を登録することで、即時でステータス情報を更新できます。

2　利用形態

カード AP 搭載システムは、クラウドサービスとしての利用、もしくはオンプレ形態での利用が可能です。

サービス提供者は、利用形態に応じた検討を行う必要があります。

2.1 クラウドサービスとしての利用

機構が提供するクラウドサービスに接続のうえ、カード AP 搭載システムを利用する形態です。サービス提供者は、必要な台数の端末機（IC カードリーダ／ライタも含む）及び回線を準備することにより、カード AP 搭載システムを利用できます。

カード AP 搭載システムのメンテナンスやバージョンアップは機構にて実施するため、常に最新バージョンのカード AP 搭載システムを安全且つ低コストで利用できます。(※)

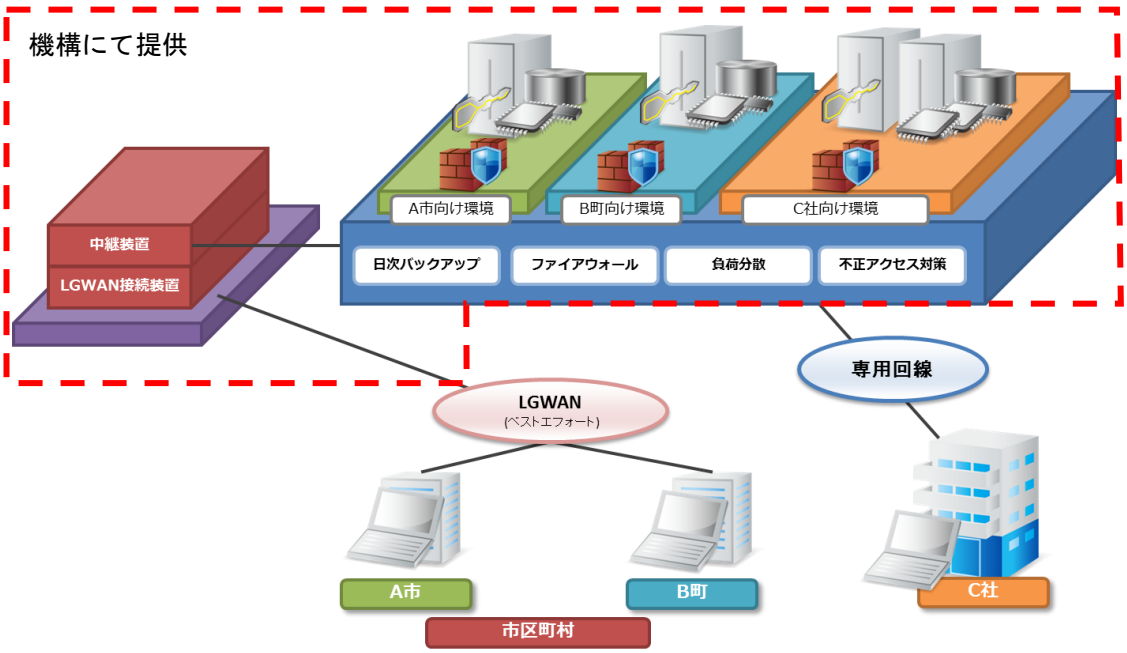
※費用の詳細については、「VI1 イニシャルコスト」及び「VI2 ランニングコスト（年間経費）」を参照してください。

クラウドサービスとしての利用にあたり、以下を実施する必要があります。

(1) クラウドサービスとの接続

機構が指定する閉域網回線サービスを契約し、カード AP 搭載等に係る端末機(サービス提供者にて用意)と接続する必要があります。端末機の詳細については、情報開示の申請（Ⅳ１(1)参照）後に機構より提供される「機器調達仕様書」を参照してください。

クラウドサービスのイメージ



(2) 業務システムの改修

クラウドサービスは、カード AP のダウンロードまでを行います。標準カード AP の場合は、カード AP ダウンロード時にカード AP 内に利用者 ID が付番されますので、業務システム（職員証サービス、図書館サービス、ポイントサービス等のシステム）にて利用者 ID と利用者情報の紐付け登録をする機能を用意する必要があります。（※）

なお、独自カード AP の場合は、業務システムにて利用者 ID の付番とカード AP 内に利用者 ID の書き込みを行う必要があります。

（業務システムに要求されるインタフェース等の詳細については、情報開示の申請（Ⅳ 1 (1)参照）後に機構より提供される、詳細資料に含まれる仕様書等を参照してください。）

※このための改修を容易にするツール（カード AP アクセスモジュール）を機構より提供しています。

2.2 オンプレ形態での利用

カード AP 搭載システムをサービス提供者が管理する設備内に導入し、運用する形態です。2.1（2）に記載のとおり、業務システムの改修も併せて実施します。

市区町村が地域住民向け領域にカード AP を搭載する場合は、オンプレ形態で利用する必要があります。

なお、オンプレ形態で利用する場合は、以下の点に留意する必要があります。

(1) 重要情報の保護

カード AP 搭載システムでは、マイナンバーカードの操作のために必要な鍵情報を取扱うため、サービス提供者側で十分なセキュリティ対策を行う必要があります。

(2) セキュリティパッチの適用

機構では、半年に１回程度、カード AP 搭載システムに対して最新のセキュリティパッチを適用し、動作検証を実施のうえ、そのパッチリストを公開しています。オンプレでカード AP 搭載システムを利用している場合は、最新のパッチリストに従い、カード AP 搭載システムの機器について定期的にセキュリティパッチを適用する必要があります。(※)

※最新のパッチリストに記載のセキュリティパッチを適用していない場合は、不具合等が生じた際に機構に問合せても、原因の究明に至らない場合あります。

(3) システム更新計画の検討

機構では、最新バージョンの OS について、適切な時期に動作検証を実施のうえ、サポート対象としています。一方、ソフトウェアベンダでサポートの終了したバージョンについては、カード AP 搭載システムにおいてもサポート対象外となります。(※) オンプレでカード AP 搭載システムを利用する場合は、OS のライフサイクルも考慮のうえ、システムの更新計画を検討する必要があります。

※サポート対象外のバージョンの OS を利用している場合は、不具合等が生じた際に機構に問合せても、原因の究明に至らない場合あります。

3 利用可能なカード AP

地域住民向け領域及び拡張利用領域に搭載するカード AP は、同一形式のものを利用できます。利用可能なカード AP は、以下の２種類に分類されます。

(1)標準的なカード AP

機構では、サービス提供者の費用・工数を削減するために、標準的なカード AP(以下「標準カード AP」という。) を提供しています。標準カード AP は、３種類あり、サービスの性質に応じ、選定することが可能です。

アプリケーション仕様の詳細については、情報開示の申請 (Ⅳ１(1)参照) 後に機構より提供される、カード AP の種類ごとのカードアプリケーション仕様書を参照してください。

標準カード AP 一覧

カード AP の種類	概要
タイプＡ（レコード型）	利用者識別情報等をレコード形式で記録し、当該領域を読み出すにあたり、認証と PIN（パスワード）による照合が必要なアプリケーションです。厳密な認証が必要とされるケースに適しています。

タイプＣ（共通カード AP 型）	利用者識別情報等を記録し、認証不要で読み出すことが可能なアプリケーションです。ポイントカード等の本人性確認が不要な業務シナリオに適しています。
タイプＤ（バイナリ型）	利用者識別情報等をバイナリ形式で記録し、当該領域を読み出すにあたり、認証と PIN（パスワード）による照合が必要なアプリケーションです。また、読み出しにあたりカードとの通信の暗号化が必須となります。システム側の読み出し実装が複雑になりますが、カードとの通信経路でインターネットなどを利用しており中間者攻撃が想定されるケースに適しています。

＜参考＞

カード AP の種類	PIN（パスワード）	相互認証	データの 暗号化が可能な範囲
タイプＡ	あり （システム固定の PIN を利用することも可能）	あり	③（https 等で暗号化）
タイプＣ	なし	なし	③（https 等で暗号化）
タイプＤ	あり （システム固定の PIN を利用することも可能）	あり	①（標準で暗号化） ②（標準で暗号化） ③（https 等で暗号化）

(2) 独自カード AP

標準カード AP の利用が適さないシステムにおいては、サービス提供者が独自のカード AP（以下「独自カード AP」という。）を作成し利用することが可能です。

マイナンバーカードは複数のカード製造事業者が存在し、それぞれに搭載するチップが異なることから、カード AP もチップ毎に製造を行う必要があります。そのため、共通の実装でチップ毎のカード AP を作成可能なツールとして、カード AP アダプタを機構にて提供します。カード AP アダプタを用いることで、サービス提供者は独自カード AP の作成に必要なインプットデータを１つ作成するだけで簡単に独自カード AP を作成することができます。

独自カード AP を作成することを希望するサービス提供者は、別途機構に対し、情報開示の申請（Ⅳ１(1)参照）後に機構より提供される「カード AP アダプタインプット情報作成手引書」を参照のうえ、「カード AP 登録依頼書」にて申請してください。

また、上記の方法によらず、独自のカード AP を作成することも可能です。

Ⅳ　システム導入手順及びスケジュール

カード AP 搭載システムの標準的な導入手順、導入スケジュールを以下に示します。

1　導入手順

(1) 情報開示の申請

カード AP 搭載システムの導入を検討しているサービス提供者は、以下のサイトに記載の要領に従い、資料提供申込書及び機密保持誓約書を提出してください。承諾後、機構から開示資料をダウンロードする際に使用する ID・パスワードを発行します。

・マイナンバーカードアプリケーション搭載システム資料提供について
（https://www.j-lis.go.jp/rdd/card/bango-ap/cms_bangoap_001.html）

(2) プロジェクトチームの発足

カード AP 搭載システムを導入する場合には、導入のためのプロジェクトチームを発足し、導入計画等を策定します。

(3) サービス内容の検討と調査

カード AP 搭載システムを利用したサービス内容について検討し、現在行っている業務への影響を調査・分析します。なお、カード AP は、単独利用のみならず、複数のサービス提供者で、共同利用することも可能です。「Ⅷ参考資料　利用及び申請のパターンイメージ」をご覧ください。

(4) 導入要件の確認及び導入スケジュールの作成

カード AP 搭載システムを利用するための導入要件の確認を行います。

また、全体の作業項目を確認し、導入スケジュールを作成します。

(5) 条例等の制定や改正

番号法第十八条に基づきマイナンバーカードを事務の処理に利用する場合は、条例等の制定が必要です。

また、具体的な運用に関し、必要に応じて条例、施行規則等の制定や改正が必要です。

(6) システム利用申込書の提出

カード AP 搭載システムを導入する場合は、機構へ「マイナンバーカードアプリケーション搭載システム サービス利用申込書」（以下「サービス利用申込書」という。）及び「マイナンバーカードアプリケーション搭載システム 使用許諾契約書」（クラウドの場合は、「カード AP

アクセスモジュール 使用許諾契約書」）の提出が必要になります。オンプレの場合、ソフトウェア等の提供まで約１ヶ月と想定されます。なお、申込受付状況によっては、ソフトウェア等の提供時期が前後することがあります。クラウドの場合は、サービス利用申込書が受理された後、クラウドサービス利用申込書を提出する必要があります。

(7) クラウドサービス利用申込書の提出（クラウドの場合）

クラウドサービスとして利用する場合は、別途機構が定める利用約款に基づいて、「マイナンバーカードアプリケーション搭載システム クラウドサービス利用申込書」（以下「クラウドサービス利用申込書」という。）を提出します。

(8) カード AP の用意

標準カード AP を利用する場合は、カード AP 登録依頼書を機構に提出します。その後、機構にて AID の採番、カード AP の提供を行います。

また、独自カード AP を製造する場合は、機構が AID の採番、カードアダプタを使用してカード AP の製造を行いますので、カード AP アダプタに登録する情報（インプットデータ）を記入した上でカード AP 登録依頼書を提出してください。

(9) 業務運用・システム運用設計

サービス開始後の業務運用設計（業務フロー、運用体制・時間）及びシステム運用設計（セキュリティ要件等、バックアップ・監視等の機能要件定義）を行います。

(10) システム設計

運用に即したチューニング設計、マスタデータ等の設計を行います。

(11) ネットワークや機器等の調達

規模及びサービスに対応したネットワーク、機器構成を決定し、機器、ネットワークを調達します。

(12) 機器及びネットワークの設定

機器の設置・設定、必要なネットワークに接続します。

オンプレ形態での導入の場合は、サーバ機器等の構築・設定も必要になります。

(13) カード AP 登録

クラウドサービスとしての利用の場合、カード AP の登録は、カード AP 登録依頼書に基づいて機構にて行います。

また、オンプレ形態の場合は、サービス提供者にてカード AP の登録を行います。

(14) 動作確認試験

クラウドサービスへの接続確認、カード AP 搭載システムの動作確認、及びサービス提供者が定めた業務運用手順等の確認を実施し、試験終了後、機構に総合試験手引書（総合試験チェックリスト）（以下、「総合試験チェックリスト」という）を提出します。

試験時に使用するカードについては、各カードベンダからすべてのカード種別（現在２種類）を機構が借用し、機構からサービス提供者に貸出を行う予定です。

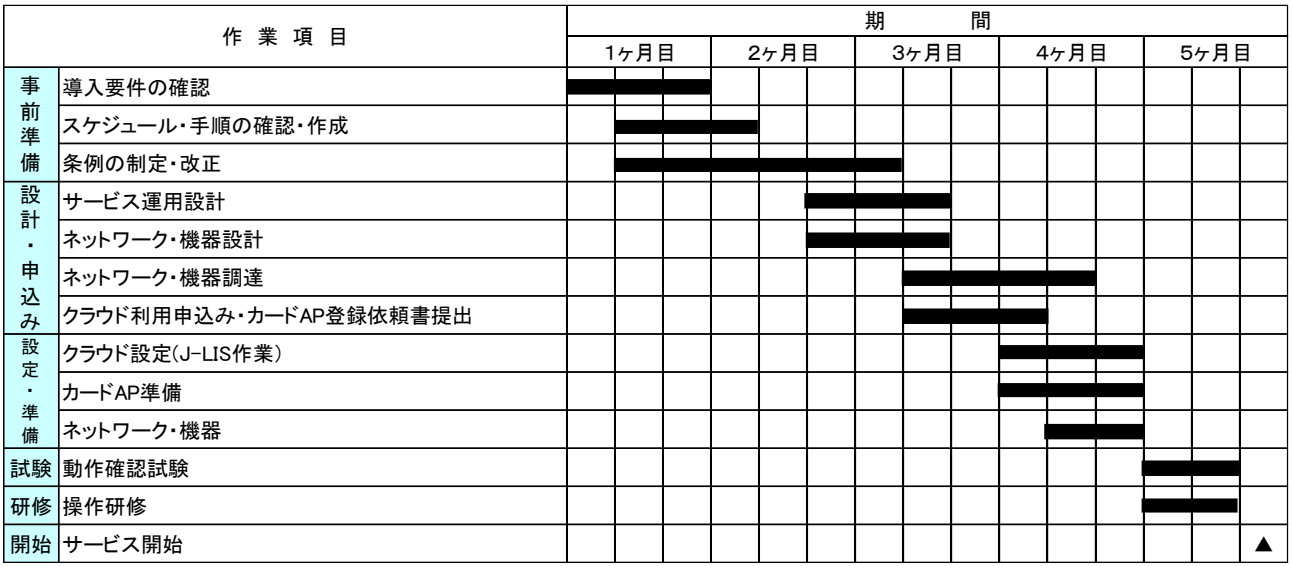
(15) 研修

導入するサービスの運用マニュアルを整備し、サービス提供者側で操作研修等を行います。

2　導入スケジュール

2.1　クラウドサービスとしての利用の場合

サービス開始までの標準的なスケジュールを以下に示します。なお、クラウドサービス利用申込書は、サービス開始日の２ヶ月半以上前に提出してください。

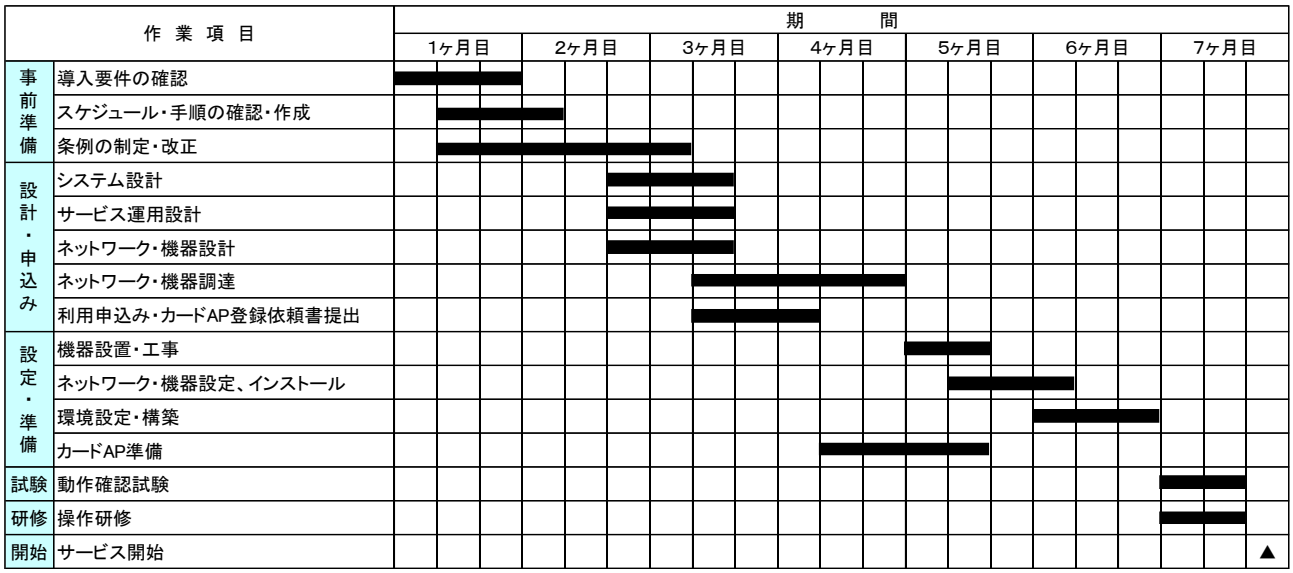


項番	作業項目		作業内容
1	事前準備	導入要件の確認	・導入するための各種要件確認 ・仕様・機能の理解 ・プロジェクトチーム発足
2		スケジュール・手順の確認・作成	・全体作業項目の確認 ・導入スケジュールの調整・作成
3		条例の制定・改正	・マイナンバーカード利用条例等の制定・改正
4	設計・申込み	サービス運用設計	・業務運用設計（業務詳細フロー、職員の作業分担、運用体制、時間） ・システム運用設計（セキュリティ要件、バックアップ・監視等の機能要件）
5		ネットワーク・機器設計	・トラフィックの確認 ・新規敷設、既設ネットワーク利用、クラウドサービスとの接続に必要なネットワーク構成（LAN・回線等）の詳細設計 ・端末台数等の把握
6		ネットワーク・機器調達	・設計、仕様よりネットワーク、機器の調達

項番	作業項目		作業内容
7	設計・申込み	利用申込み･カードAP依頼	・サービス利用申込書の作成・提出 ・カードAPアクセスモジュール 使用許諾契約書の作成・提出 ・クラウドサービス利用申込書の作成・提出 ・カードAP登録依頼書の作成・提出
8	設定・準備	クラウド設定（機構作業）	・機構にてクラウドサービス利用申込書に基づいてクラウド設定
9		カードAP準備	・標準カードAPの場合、機構にてAIDの採番、カードAPの提供 ・独自カードAPの場合、サービス提供者がインプットデータを作成した上で、機構にてAIDの採番、カードAPの準備
10		ネットワーク・機器設定	・ネットワーク機器の設置工事及びネットワーク敷設工事 ・クラウドサービスへの接続 ・システムを利用する機器の設定
11	試験	動作確認試験	・クラウドサービスへの接続確認試験 ・システム動作確認試験 ・業務運用試験 ・総合試験チェックリストの提出
12	研修	操作研修	・操作研修・運用指導等
13	開始	サービス開始	・サービスの開始

2.2　オンプレ形態の場合

サービス開始までの標準的なスケジュールを以下に示します。



項番	作業項目		作業内容
1	事前準備	導入要件の確認	・導入するための各種要件確認 ・仕様・機能の理解 ・プロジェクトチーム発足
2		スケジュール・手順の確認・作成	・全体作業項目の確認 ・導入スケジュールの調整・作成
3		条例の制定・改正	・マイナンバーカード利用条例等の制定・改正
4	設計・申込み	システム設計	・運用に即したチューニング設計 ・設定項目、移行項目、DB、マスタデータの設計
5		サービス運用設計	・業務運用設計（業務詳細フロー、職員の作業分担、運用体制、時間） ・システム運用設計（セキュリティ要件等、バックアップ・監視等の機能要件）

項番	作業項目		作業内容
6	設計・申込み	ネットワーク･機器設計	・トラフィックの確認 ・性能要件からサーバ、端末機、周辺機器、ネットワーク機器（ルータ・ハブ・ファイアウォール等）のスペック、必要台数等システム構成設計、構成の詳細設計、搭載設計等 ・新規敷設、既設ネットワーク利用、関係機関との接続に必要なネットワーク構成（LAN・回線等）の詳細設計 ・設置場所を含めた全体のネットワーク設計 ・新規敷設、既設ネットワーク利用、関係機関との接続に必要なネットワーク構成（LAN・回線等）の詳細設計 ・システム導入に関する電源、空調、ブース、配線等の詳細設計
7		ネットワーク･機器調達	・設計、仕様よりネットワーク、サーバ等機器の調達
8		利用申込み･カードAP依頼	・サービス利用申込書の作成・提出 ・カードAP搭載システム 使用許諾契約書の作成・提出 ・カードAP登録依頼書の作成・提出
9	構築・準備	機器設置・工事等	・ネットワーク機器の設置工事及びネットワーク敷設工事 ・導入予定のサーバ、端末等の機器の搬入、組立て、初期調整 ・電源、空調、ブース、配線等の工事
10		ネットワーク・機器設定､インストール	・システムのインストール、環境設定作業 ・ネットワーク環境設定、ミドルウェア・カードAPインストール、基本的な設定項目の初期設定、初期チューニング
11		環境設定・構築	・サーバ、クライアントそれぞれについて設定 ・マスタデータの作成及びDBへの登録 ・チューニング作業、設定登録
12		カードAP準備	・標準カードAPの場合、機構にてAIDの採番、カードAPの提供 ・独自カード AP の場合、サービス提供者がインプットデータを作成した上で、機構にてAIDの採番、カードAPの準備
13	試験	動作確認試験	・システム動作確認試験 ・業務運用試験
14	研修	操作研修	・操作研修・運用指導等
15	開始	サービス開始	・サービスの開始

Ⅴ　システム運用

カード AP 搭載システムの運用について以下に示します。

機構では、カード AP 搭載システムの使用に関する問合せを受付け、機能を正常に維持し、円滑に稼動させるためのサポートを行います。

なお、技術者の現地派遣による支援は、行っていません。

<table>
<tr><th>項　目</th><th colspan="2">クラウドサービス</th><th>オンプレ</th></tr>
<tr><td>サービス提供時間</td><td colspan="2">8:00AM から 22:00 まで
年末年始（12 月 29 日から１月３日まで）を除く。</td><td>サービス提供者の運用方針に従って策定</td></tr>
<tr><td>システム問合せ対応</td><td colspan="3">業務運用システムにて対応（平日 9:00AM から 18:00 まで）</td></tr>
<tr><td rowspan="2">障害発生時対応</td><td>クラウド側で検知</td><td>サービス提供者登録連絡先に連絡</td><td rowspan="2">業務運用システムにて対応
（平日 9:00 AM から 18:00 まで）</td></tr>
<tr><td>サービス提供者側で検知</td><td>クラウド側に連絡</td></tr>
<tr><td>メンテナンス時対応</td><td colspan="2">計画メンテナンスの場合、10 営業日前までにサービス提供者登録メールアドレスに連絡</td><td></td></tr>
<tr><td>※サービス提供者における端末機及びネットワーク機器等の障害等対応</td><td colspan="3">サービス提供者において機器の保守事業者と調整</td></tr>
</table>

Ⅵ　費用の概算

カードAP搭載システムの導入・運用に係る費用の概算を以下に示します。なお、想定される最小構成での概算費用のため、実際の費用については各ベンダへお問合せください。

1　イニシャルコスト

）

項番	項　　目	概算費用（※）		支払い先	内容
		クラウドサービス	オンプレ		
1	サーバ機器	－	120 万～	機器調達先	機器調達仕様に基づく機器調達及びバックアップシステム導入
2	端末機器	20 万/台	20 万/台	機器調達先	端末機、IC カードリーダ・ライタ、ワイヤーロック等備品
3	ネットワーク関連機器	20 万～	30 万～	機器調達先	小型 L3 スイッチ、L2 スイッチ導入の場合（同一拠点内にサーバ/端末機設置を想定）
4	ソフトウェア関連	－	100 万～	機器調達先	Windows Server、Oracle Database、バックアップソフトウェア、ウイルス対策ソフト
5	導入 SI 作業	－	350 万～	導入 SI ベンダ	ネットワーク設定及び端末機構築、サーバ構築(オンプレの場合)
6	業務システム改修	100 万～	100 万～	業務システムベンダ等	カード AP 内の利用者 ID を業務システムに登録するための改修費
7	ネットワーク回線設定料	６万～	－	クラウド事業者	（クラウド）閉域回線を敷設する際の設定料。LGWAN 回線を使用する場合は不要。 （オンプレ）同一拠点に設置の場合。回線設置場と利用拠点から離れている場合は別途費用発生。
8	クラウドサービス初期構築	40 万～	－	クラウド事業者	クラウド環境の構築、設定費
		10 万		機構	
合計		196 万～	720 万～		

※単位は円（千円単位は切上げ）税抜きで記載しています。

※費用については最小構成時の参考価格です。

※業務システムベンダとの調整等、追加作業がある場合は、上記以外にも費用が発生することがあります。

2　ランニングコスト（年間経費）

項番	項　　目	概算費用（※）		支払い先	内容
		クラウドサービス	オンプレ		
1	機器保守	10 万～	50 万～	機器調達先	
2	サーバ等保守運用	－	70 万～	導入 SI ベンダ	
3	ソフトウェア更新費用	－	50 万	導入 SI ベンダ	年に１度システムのバージョンアップをする場合
4	コロケーション費用	－	60 万	コロケーション事業者	月５万円を想定（１ラック 25 万円/月の１/５）
5	ネットワーク回線使用料	19 万～	－	クラウド事業者	（クラウド）閉域回線を敷設する際の回線料。LGWAN 回線を使用する場合は不要。 （オンプレ）同一拠点に設置の場合。回線設置場と利用拠点から離れている場合は別途費用発生。
6	クラウド利用料	39 万～	－	クラウド事業者	クラウド基盤利用料等
7	サポート料	91 万	91 万	機構	サポート料（カード AP 搭載システムのソフトウェア・サービスの提供（アプリケーション保守費用を含む)、機能改善、問合せ対応等） （クラウド）パッチ適用、バージョンアップ （オンプレ）パッチ提供、バージョンアップツールの提供
合計		159 万～	321 万～		

※単位は円（千円単位は切上げ）税抜きで記載しています。

※費用については最小構成時の参考価格であり、変動する可能性があります。

※サポート料は、クラウドサービス利用初年度については、利用開始月からの月割計算となります。

VII セキュリティ対策等

サービス提供者が行うべきセキュリティ対策は以下のとおりです。

1　カードAP搭載システムのセキュリティ対策

項番	対策	内容
1	オペレーター認証	システムの操作者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。 認証方式は、生体認証方式又は ID・パスワードによる認証方式のうちのいずれかを採用していること。
2	停止措置	マイナンバーカードの紛失時及び盗難時における「なりすまし」による不正使用を防止します。 マイナンバーカードの運用状況データの連携を行うことにより、住民からの紛失、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すること。 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の紛失・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すること。
3	アクセスログ管理	不正行為の検知、発生原因の特定のために、システムのアクセスログを記録します。
4	暗証番号設定とロック（停止状態）	カードAP側で照合機能を保有する場合、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。
5	相互認証	カードAP側で内部認証/外部認証機能を保有する場合、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。

2　クラウドサービスとしての導入時のセキュリティ対策

2.1 クラウドサービスのセキュリティ対策（機構において実施している対策）

項番	対策	内容
1	個人情報の不保持	個人情報を保持しません。サービス提供者側の業務システムで保持している個人情報と紐付けを行い、サービスを提供します。
2	通信のなりすまし防止	ネットワーク上での通信相手のなりすましによる不正を防止するために、サーバ証明書によるサーバ認証等を行います。
3	通信回線の暗号化	通信回線に対する盗聴行為、情報漏えいを防止するため、通信回線を暗号化します。
4	閉域網の採用	クラウドで使用するネットワーク回線は、外部と通信を行う機器のネットワークと、内部のネットワークを通信回線上、分離します。
5	物理的侵入対策	クラウドサービスのサーバルームには入室ができない対策を講じます。
6	不正プログラム対策	サーバ類には不正プログラム対策ソフト等の導入により、不正プログラムの感染防止の対策を行います。
7	不正監視	外部からの不正アクセスを検知する機能を備えます。また、大量アクセス、機器異常による過負荷状態を検知する機能を備えます。

2.2 サービス提供者側で必要と考えられるセキュリティ対策（参考）

項番	対策	内容
1	運用管理規程	機器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すること。 運用管理規程は、セキュリティを確保するために、サービス提供者がそれぞれの現状に基づき規定し、遵守すること。
2	アクセス権管理	利用範囲を利用者の職務に応じて制限し、アクセス権の割り当てを適切に設計し管理を行うこと。
3	通信経路の分離	利用端末はインターネットへの接続環境と分離し、クラウドサービスとの接続は専用回線とすること。
4	物理的保護	機器のワイヤーロック、ディスプレイの盗み見防止等に代表される物理面のセキュリティ対策を実施すること。
5	不正プログラム対策	導入機器には、不正プログラム対策ソフト等の導入により、不正プログラムの感染防止の対策を行うこと。
6	利用端末構築	機器調達仕様書に示すソフトウェア以外や他システムを導入せず、カード AP 搭載システム専用の端末とし、ソフトウェア及びハードウェアの脆弱性の有無を確認の上、導入すること。
7	脆弱性対策	導入機器について、脆弱性の有無を確認し導入し、導入後も更新を定期的に行うこと。
8	システムの構成管理	構築時の情報システムの構成（ハードウェア、ソフトウェア）が記載された文書（機器管理台帳等）を作成するとともに文書どおりの構成とし、変更が生じた場合には随時更新すること。

3　オンプレ形態での導入時に必要と考えられるセキュリティ対策（参考）

項番	対策	内容
1	運用管理規程	導入機器、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すること。 運用管理規程は、セキュリティを確保するために、サービス提供者がそれぞれの現状に基づき規定し、遵守すること。
2	アクセス権管理	利用範囲を利用者の職務に応じて制限し、アクセス権の割り当てを適切に設計し管理を行うこと。
3	通信のなりすまし防止	ネットワーク上での通信相手のなりすましを防止するために、サーバ証明書によるサーバ認証等を行います。
4	通信回線の暗号化	通信回線に対する盗聴行為、情報漏えいを防止するため、通信回線を暗号化すること。
5	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、システムを保護するファイアウォールを設置し、アクセス制御すること。
6	閉域網の採用	カードAP搭載システムで使用するネットワーク回線は、外部と通信を行う機器のネットワークと、内部のネットワークを通信回線上、分離すること。
7	通信経路の分離	利用端末はインターネットへの接続環境と分離すること。
8	物理的保護	入退出管理、機器のワイヤーロック、ディスプレイの盗み見防止等に代表される物理面のセキュリティ対策を実施すること。 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、サービス提供者がそれぞれの現状に基づいた対策を立案し、講ずること。
9	不正プログラム対策	サーバ、端末等には不正プログラム対策ソフト等の導入により、不正プログラムの感染防止の対策を行うこと。
10	利用端末構築	機器調達仕様書に示すソフトウェア以外や他システムを導入せず、カードAP搭載システム専用の端末とし、ソフトウェア及びハードウェアの脆弱性の有無を確認の上、導入すること。
11	脆弱性対策	導入機器について、脆弱性の有無を確認し導入し、導入後も更新を定期的に行うこと。
12	不正監視	外部からの不正アクセスを検知する機能を備えること。また、大量アクセス、機器異常による過負荷状態を検知する機能を備えること。
13	外部委託における対策	システム構築を外部委託する場合、委託元が意図しない変更、情報窃取等が行われないよう対策を講じること。

サービス提供者で必要と考えられるセキュリティ対策は、以下のとおりです。

＜通知カード及び個人番号カードに関する技術的基準より抜粋＞

第９　個人番号カードの条例等利用領域等の利用

１　法第 18 条の条例等に規定する事務以外の事務の処理への利用の禁止等

(1) 法第 18 条の条例等に規定する事務以外の事務の処理への利用の禁止

個人番号カードの半導体集積回路に、住民基本台帳ネットワークシステムに係るアプリケーション、券面事項確認アプリケーション、券面事項入力補助アプリケーション、公的個人認証サービスアプリケーション又は条例等利用アプリケーション以外のアプリケーションを搭載してはならないこと。また、個人番号カードに貼り付けた磁気テープを利用する場合その他の電磁的方法により必要な事項を記録して利用する場合においても、法第 18 条の条例等に規定する事務以外の事務の処理に利用してはならないこと。

(2) 条例等利用領域管理システム等の導入

個人番号カードの半導体集積回路を法第 18 条の条例等に規定する事務の処理に利用する場合は、法第 18 条各号に掲げる者は、条例等利用領域に条例等利用アプリケーションのみを安全かつ確実に搭載する等の運用及び管理を行うシステム等を導入すること。また、当該システム等は、法第 17 条第３項に規定する措置を講じた個人番号カードの半導体集積回路に、条例等利用アプリケーションを搭載できるものとすること。

２　個人番号カードの領域間の独立性の確保

(1) 基本利用領域等と条例等利用領域間の独立性の確保

個人番号カードの半導体集積回路を法第18条の条例等に規定する事務の処理に利用する場合は、住民基本台帳ネットワークシステム又は券面事項確認アプリケーション、券面事項入力補助アプリケーション若しくは公的個人認証サービスアプリケーションに係るシステムが条例等利用領域に情報を記録し、又は当該領域の情報を読み取ることができない措置を講ずること。

また、条例等利用アプリケーションに係るシステムが基本利用領域、券面事項確認利用領域、券面事項入力補助領域又は公的個人認証サービス利用領域に情報を記録し、又は公的個人認証サービス利用領域に記録された情報を読み取ることができない措置を講ずること。

(2) 複数の条例等利用領域間の独立性の確保

個人番号カードの半導体集積回路を複数の法第18条の条例等に規定する事務の処理に利用する場合は、それぞれの条例等利用アプリケーションに係るシステムがそれぞれの条例等利用領域以外の領域に情報を記録し、又は当該領域に記録された情報を読み取ることができない措置を講ずること。

３　条例等利用アプリケーションにおける個人情報の保護

(1) 法第 18 条の条例等に規定する事務の処理に応じた個人情報保護措置の実施

個人番号カードの半導体集積回路を法第18条の条例等に規定する事務の処理に利用する場合は、暗証番号、発行前の不正使用を防止するための情報、相互認証を行うための情報又はアクセス権限の制御その他の個人情報の適切な管理のために必要な措置を講ずること。

(2) 必要最小限の個人情報の記録

個人番号カードの条例等利用領域内には、特に必要性が認められる場合を除き、条例等利用アプリケーションに係るシステムへアクセスするための利用者番号等以外の個人情報を記録しないこと。この場合において、当該利用者番号等には、住民票コードを使用しないこと。

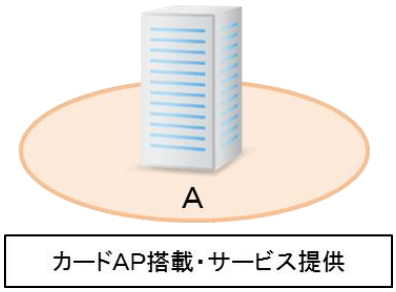
(3) 希望するアプリケーションの搭載等

法第 18 条第２号に掲げる者は、条例等利用アプリケーションの全部又は一部の個人番号カードへの搭載を希望する者に限って、当該アプリケーションを当該希望する者の個人番号カードに搭載するほか、個人番号カードに貼り付けた磁気テープ等を利用する場合においても、個人番号カードに貼り付けた磁気テープ等の利用を希望する者に限ってその利用を行うこと。また、法第 18 条第１号に規定する市町村の機関は、同条の規定により個人番号カードを利用する場合には、利用を希望する者に限ってその利用を行うこと。

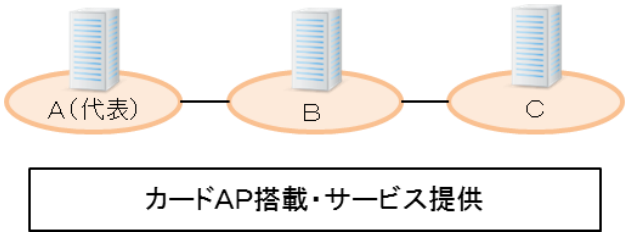
VIII 参考資料

利用及び申請のパターンイメージ

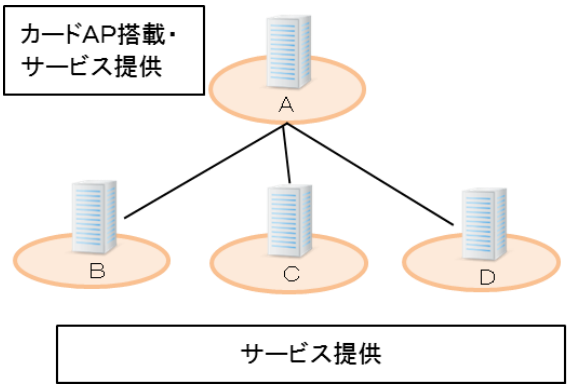
1　単独でサービスを提供する場合



2　サービスを共同で利用する場合



3　カード AP 搭載・サービス提供を行う代表とサービス提供のみ行う支所の申請の場合



上記 3 パターンいずれの場合でも下記の資料の提出が必要です。

パターン	提出書類
クラウド	・マイナンバーカードアプリケーション搭載システム サービス利用申込書 ・マイナンバーカードアプリケーション搭載システム クラウドサービス利用申込書 ・カード AP アクセスモジュール 使用許諾契約書 ・カード AP 登録依頼書
オンプレ	・マイナンバーカードアプリケーション搭載システム サービス利用申込書 ・マイナンバーカードアプリケーション搭載システム 使用許諾契約書 ・カード AP 登録依頼書

備考

カード AP 搭載システムの利用申請を行う場合は、代表者がその他のサービス提供者の申請内容を取りまとめた上で申し込みを行う。