個人番号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
（都道府県・市区町村・行政機関等向け）

第 1.2 版

平成 29 年 2 月

地方公共団体情報システム機構

目　次

Ⅰ　利用領域

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、本書ではその中の、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のシステムについての内容を示します。

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、図書館サービス、ポイントサービス等があります。

※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のこと。

※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」、「地方独立行政法人」（以下「行政機関等」という。）のこと。以下この手引きにおいて同じ。

2　個人番号カードの領域利用のイメージ

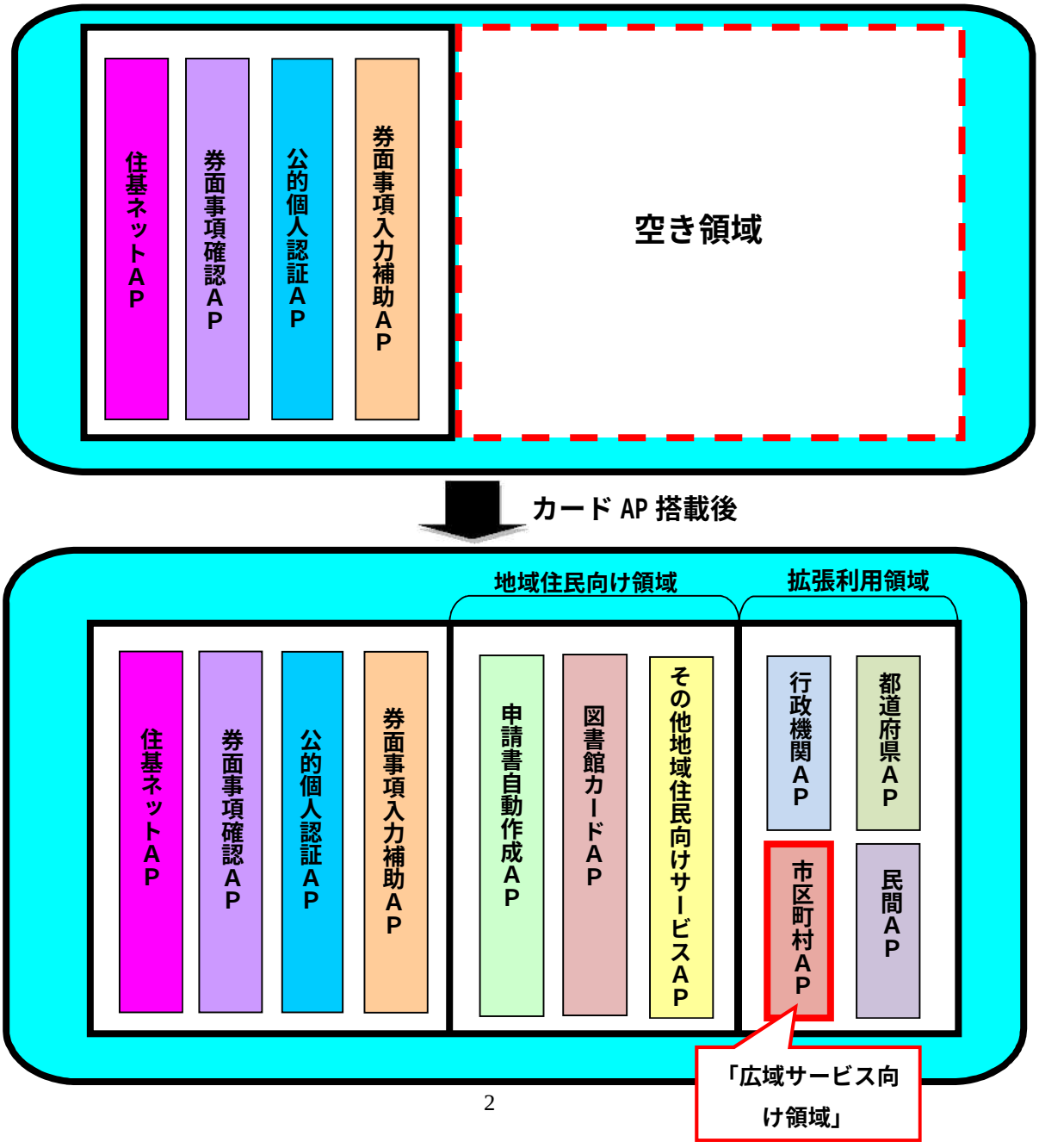
個人番号カードには、複数のカードアプリケーション（以下「カード AP」という。）を搭載できます。カード AP とは、サービスの提供に必要な情報を登録するもので、他のサービスからの利用及び参照はできません。

個人番号カードは、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、地域住民向け領域や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。

下図に個人番号カードの領域利用イメージを示します。



Ⅱ　システム概要

1　個人番号カードの拡張利用領域利用

1.1　拡張利用領域の特性

拡張利用領域と地域住民向け領域には、以下の特性があります。

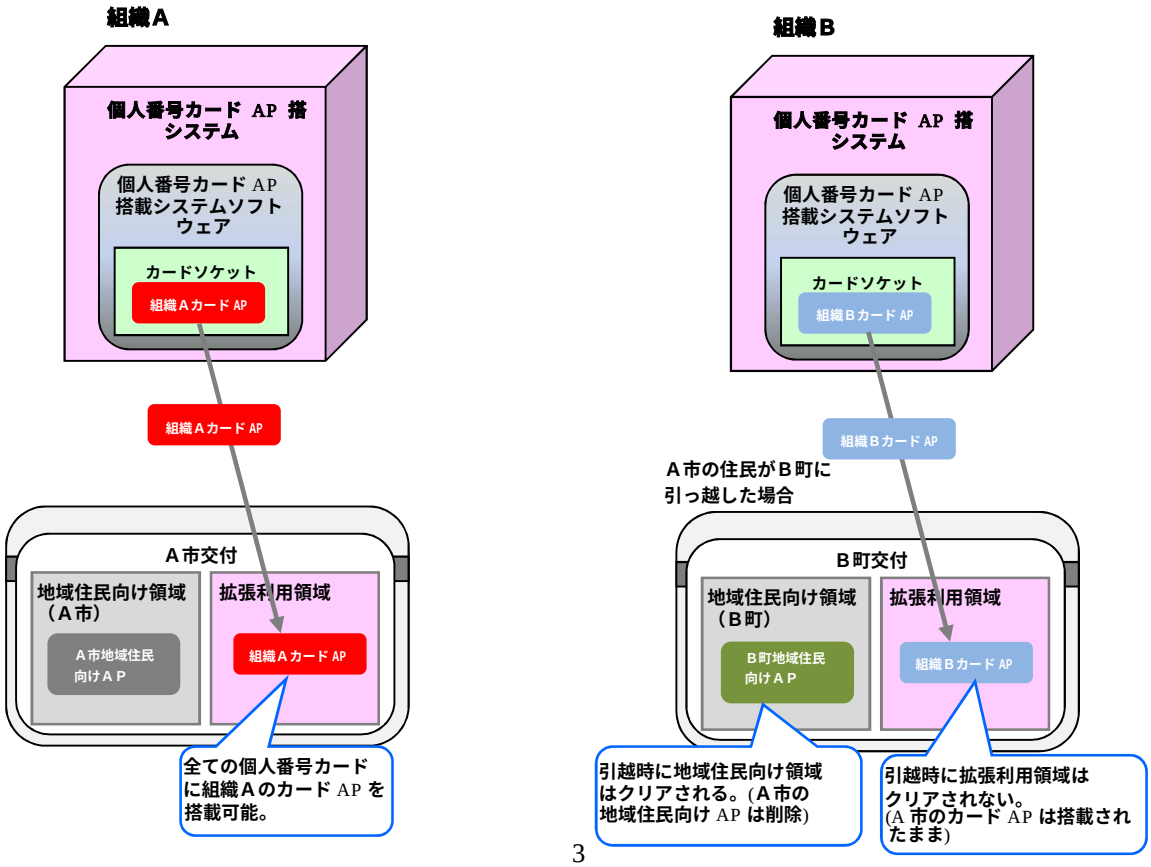
(1) 住所地以外の住民でもサービス利用が可能

地域住民向け領域は、住民住所地で発行された個人番号カードに対して、住民住所地の市区町村でのみ利用可能であり、住民住所地以外の市区町村ではカード AP の追加や削除を行うことはできませんが、拡張利用領域は、住民住所地に依存せず行政機関等においてサービスの提供が可能です。

(2) 引越後も継続してサービス利用が可能

地域住民向け領域は、引越後に、引越先にて個人番号カードの継続利用を行う場合には、搭載されていたカード AP が自動で削除されますが、拡張利用領域は継続利用を行った場合も、搭載済みのカード AP が削除されることはありません。

・個人番号カード AP 搭載システム　イメージ図



1.2　拡張利用領域の運用

個人番号カード上に存在する拡張利用領域は 1 領域であり、サービス提供者により領域を共有して利用します。個人番号カードの空き容量は有限であるため、サービス提供者においては、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してください。

1.3　拡張利用領域へカード AP を搭載するシステム

拡張利用領域にカード AP を搭載することが可能なシステムとして開発された個人番号カードアプリケーション搭載システム（以下「個人番号カード AP 搭載システム」という。）を、クラウドサービスとして、地方公共団体情報システム機構（以下「J-LIS」という。）が提供しています。

また、行政機関等は、個人番号カード AP 搭載システムを自身が管理する設備内に導入すること（以下「オンプレ」という。）も可能です。

サービス提供者におかれては、利用形態に応じた検討を行う必要があります。

サービス提供者	クラウドサービス	オンプレ
行政機関等	○（※）	○

※市区町村利用において、後述する IC カード標準システムとオンプレで同居を行う場合、クラウドサービスの利用はできません。なお、IC カード標準システムについては IC カード標準システムの導入検討の手引きをご覧ください。

1.4　拡張利用領域で利用可能なカード AP

拡張利用領域では、地域住民向け領域と同一形式のカード AP を利用することが可能です。

利用可能なカード AP は、以下の 2 種類に分類されます。

(1) IC カード標準システム準拠の標準的なカード AP

J-LIS では、行政機関等の費用・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、行政機関等の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、J-LIS に資料提供申込後、別途開示するカード 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。

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。

個人番号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 J-LIS が用意します。カード AP アダプタを用いることで、行政機関等は独自カード 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行政機関等は、別途 J-LIS に対し、「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、以上の方法によらす、独自のカード AP を作成することも可能です。

2　個人番号カード AP 搭載システムの概要

2.1　機能概要

(1) オペレーター認証

個人番号カード 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。

操作者の認証においては、生体認証と 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

行政機関等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、行政機関等において、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

操作対象の個人番号カードに対して、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(オンプレの場合)

個人番号カードに対してカード AP を搭載する際に、個人番号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

個人番号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。

2.2　オンプレ利用における補足

(1) 重要情報の保護

個人番号カード AP 搭載システムでは、個人番号カードの操作のために必要な鍵情報を取扱うため、行政機関等側で十分なセキュリティ対策を行う必要があります。

(2)　IC カード標準システムとの並行運用

個人番号カード AP 搭載システムは、現在行政機関等に導入されている IC カード標準システムとの同居構成をオンプレで行うことが可能です。ただし、IC カード標準システムとの同居構成時は以下の制約がありますので、留意ください。

<IC カード標準システム同居時の制約事項>

- IC カード標準システムで連携している住基ネット CS のカード運用状況連携データを個人番号カード AP 搭載システム側で利用することはできません。
- 地域住民向け領域と拡張利用領域の両方に同一 AID のカード AP をダウンロードすることはできません。

(3)　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、カード所持者が各行政機関等にその旨の届出を行い、行政機関等が業務システムにてサービス停止の登録を行う必要があります。

将来的には、カード所持者が、J-LIS のコールセンターに紛失等の届出を行えば行政機関等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ることとなる予定です。（平成 29 年度よりサービス提供予定）

3　クラウドサービスの概要

(1) クラウドサービスとの接続

クラウドサービスの利用にあたっては、J-LIS の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(行政機関等にて用意)と接続されている必要があります。端末機の詳細については、J-LIS に資料提供申込後、別途開示する「機器調達仕様書」を参照してください。

(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、行政機関等における業務システム（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。※

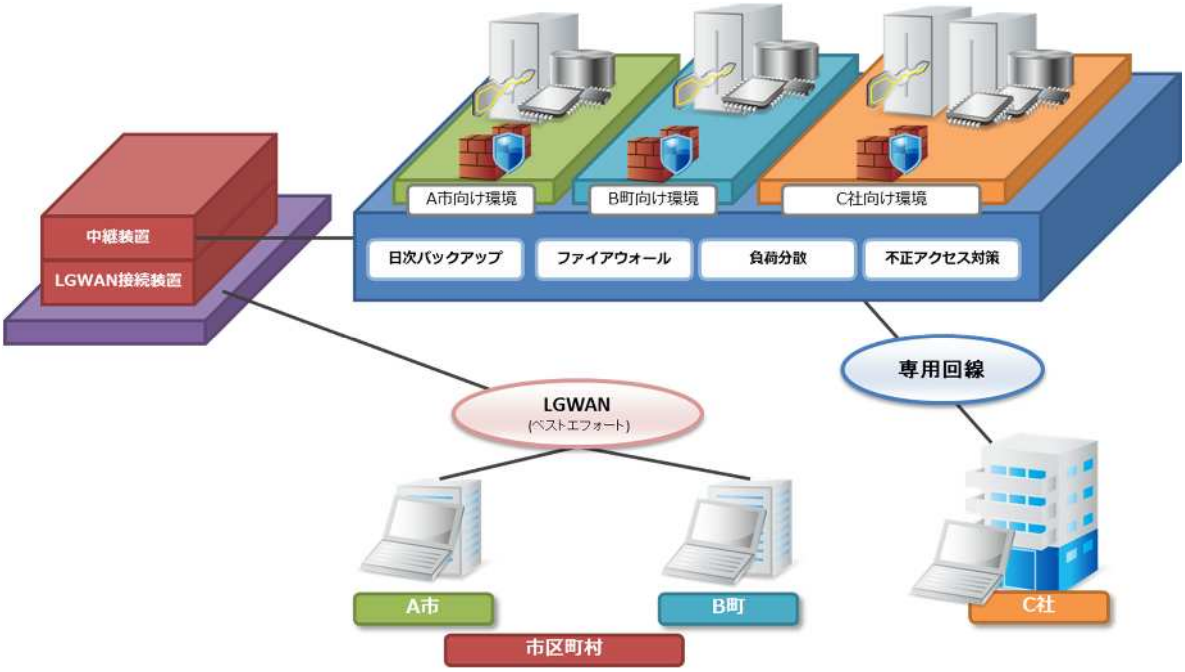
独自カード AP の場合は、業務システムにて利用者 ID の付番とカード AP 内に利用者 ID の書き込みを行ってください。

※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 J-LIS で有しており、行政機関等の要望に応じて提供することが可能です。

(3) 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 を格納したカードの紛失等があった場合には、カード所持者が各行政機関等にその旨の届出を行い、行政機関等が業務システムにてサービス停止の登録を行う必要があります。

将来的には、カード所持者が、J-LIS のコールセンターに紛失等の届出を行えば行政機関等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ることとなる予定です。（平成 29 年度よりサービス提供予定）



III　システム導入手順

個人番号カード 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

個人番号カード 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、資料提供申込書、機密保持誓約書を提出してください。承諾後、J-LIS 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。

(2) プロジェクトチームの発足

個人番号カード 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

個人番号カード 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、複数の行政機関等で、共同利用することも可能です。「VII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

個人番号カード 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個人番号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

個人番号カード AP 搭載システムを導入する場合は、J-LIS へ「個人番号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「個人番号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）

クラウドサービスを利用する場合は、別途 J-LIS が定める利用約款に基づいて、「個人番号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 J-LIS に提出します。その後、J-LIS 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、J-LIS 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 J-LIS にて行います。

また、オンプレの場合は、行政機関等にてカード 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、個人番号カード AP 搭載システムの動作確認、行政機関等が定めた業務運用手順等の確認を実施し、試験終了後、J-LIS 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 J-LIS が借用し、J-LIS から行政機関等に貸出を行う予定です。

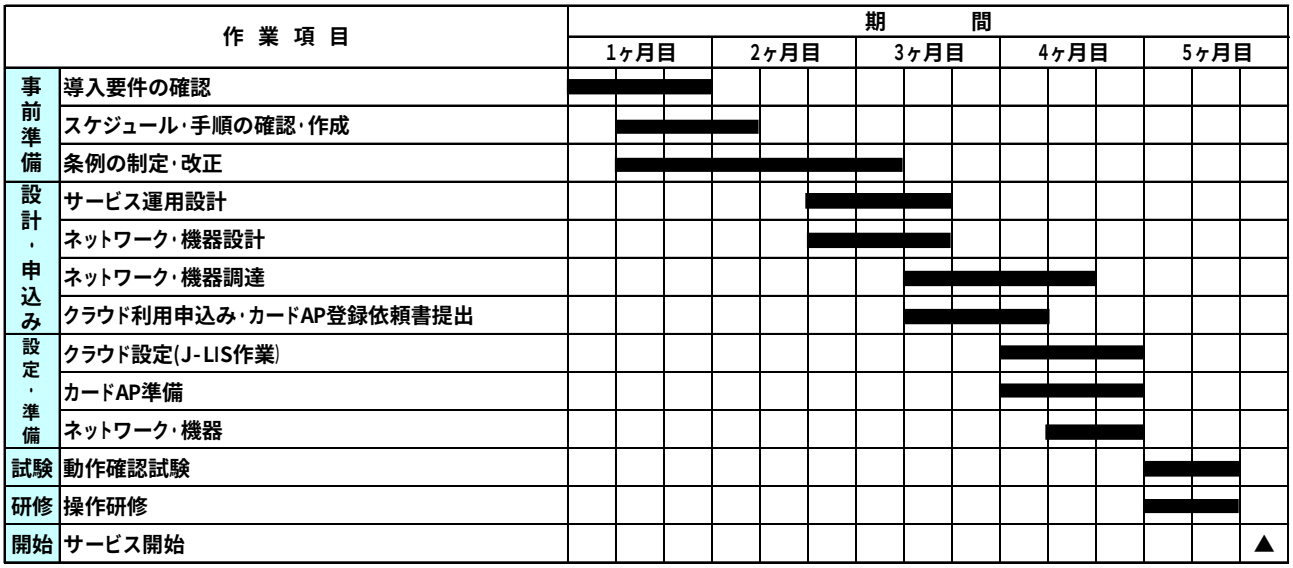
(15) 研修

導入するサービスの運用マニュアルを整備し、行政機関等側で操作研修等を行います。

2　導入スケジュール　イメージ

2.1　クラウドサービス利用の場合

想定されるスケジュールは次のとおりです。なお、クラウドサービス利用申込みは、サービス開始の 2 ヶ月半以上前に提出してください。

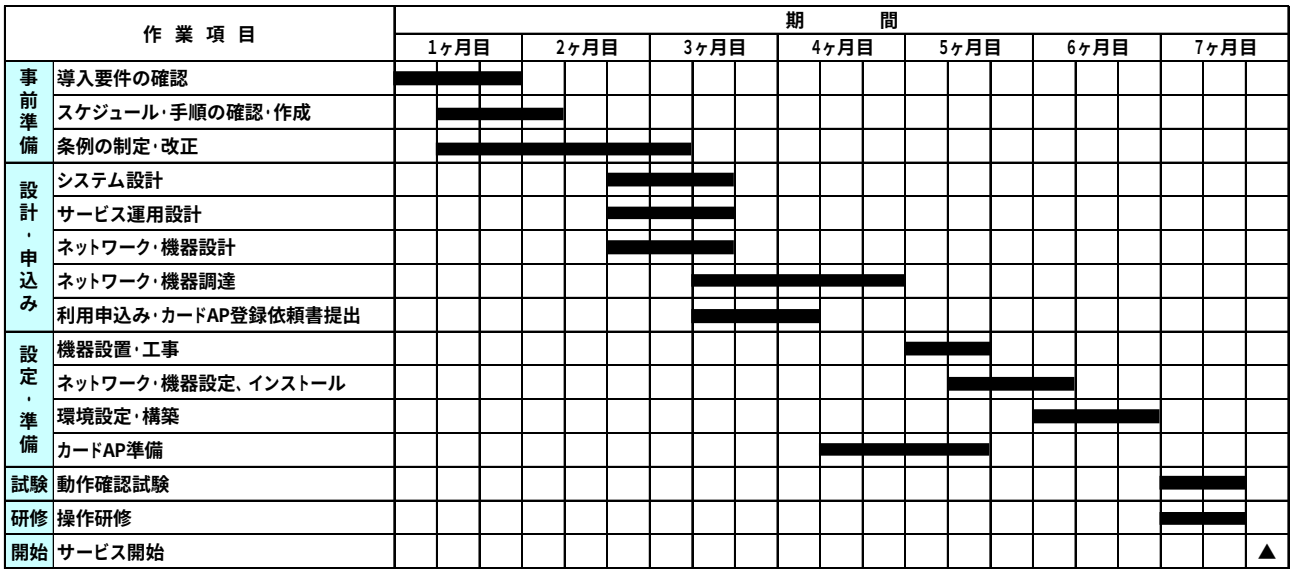


項番	作業項目		作業内容
1	事前準備	導入要件の確認	・導入するための各種要件確認 ・仕様・機能の理解 ・プロジェクトチーム発足
2		スケジュール・手順の確認・作成	・全体作業項目の確認 ・導入スケジュールの調整・作成
3		条例の制定・改正	・個人番号カード利用条例等の制定・改正
4	設計・申込み	サービス運用設計	・業務運用設計（業務詳細フロー、職員の作業分担、運用体制、時間） ・システム運用設計（セキュリティ要件、バックアップ・監視等の機能要件）
5		ネットワーク・機器設計	・トラフィックの確認 ・新規敷設、既設ネットワーク利用、クラウドサービスとの接続に必要なネットワーク構成（LAN・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（J-LIS作業）	・J-LIS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、J-LISにてAIDの採番、カードAPの提供 ・独自カード AP の場合、行政機関等がインプットデータを作成した上で、J-LIS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　オンプレの場合

想定されるスケジュールは次のとおりです。



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	・個人番号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 ・個人番号カード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、J-LISにてAIDの採番、カードAPの提供 ・独自カード AP の場合、行政機関等がインプットデータを作成した上で、J-LIS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

Ⅳ　システム運用

個人番号カード AP 搭載システムの運用について以下に示します。

J-LIS では、個人番号カード AP 搭載システムの使用に関する問合せをメールで受付け、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については、サポートの対象外です。

<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">8:00～22:00
年末年始（12 月 29 日～1 月 3 日）を除く。</td><td>行政機関等の運用方針に
従って策定</td></tr>
<tr><td>システム問合せ対応</td><td colspan="3">メール（平日 9:00～18:00）にて対応</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>行政機関等登録連絡先に連絡</td><td rowspan="2">メール
（平日 9:00～18:00）にて対応</td></tr>
<tr><td>行政機関等側で検知</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
行政機関等登録メールアドレスに連絡</td><td></td></tr>
<tr><td>※行政機関等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">行政機関等において機器の保守事業者と調整</td></tr>
</table>

Ⅴ　費用の概算

個人番号カードAP搭載システムの導入・運用に係る費用の概算を示します。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ベンダへお問合せください。

1　イニシャルコスト

（円）

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	7 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		J-LIS	
合計		197 万～	720 万～		

※千円単位は切上げ

※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）

（円）

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	20 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	42 万～	－	クラウド事業者	クラウド基盤利用料等
7	サポート料	98 万	98 万	J-LIS	サポート料（個人番号カード 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		170 万～	328 万～		

※千円単位は切上げ

※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。

VI セキュリティ対策等

行政機関等が行うべきセキュリティ対策は次のとおりです。

1　個人番号カード 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	個人番号カード紛失時及び盗難時における「なりすまし」による個人番号カード不正使用を防止します。 個人番号カード運用状況データの連携を行うことにより、住民から個人番号カード紛失、盗難の届出があった場合に、その個人番号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、住民から個人番号カード紛失・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（J-LIS 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、個人番号カード 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　オンプレで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	個人番号カード 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、個人番号カード 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、個人番号カード 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。

行政機関等で必要と考えられるセキュリティ対策は、次のとおりです。

＜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

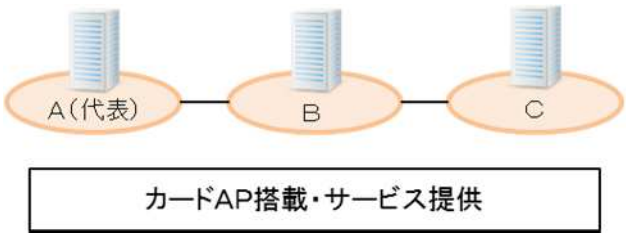
法第 18 条第２号に掲げる者は、条例等利用アプリケーションの全部又は一部の個人番号カードへの搭載を希望する者に限って、当該アプリケーションを当該希望する者の個人番号カードに搭載するほか、個人番号カードに貼り付けた磁気テープ等を利用する場合においても、個人番号カードに貼り付けた磁気テープ等の利用を希望する者に限ってその利用を行うこと。また、法第 18 条第１号に規定する市町村の機関は、同条の規定により個人番号カードを利用する場合には、利用を希望する者に限ってその利用を行うこと。

Ⅶ　参考資料

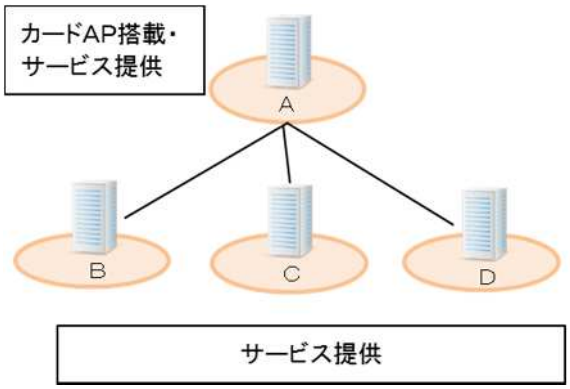
利用及び申請のパターンイメージ

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	個人番号カード AP 搭載システム　サービス利用申込書 個人番号カード AP 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	個人番号カード AP 搭載システム　サービス利用申込書 個人番号カード AP 搭載システム　使用許諾契約書 カード AP 登録依頼書

備考

個人番号カード AP 搭載システムの利用申請を行う場合は、代表者がその他の行政機関等の申請内容を取りまとめた上で申し込みを行う。