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）
（検討編）

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

本書の使い方

マイナンバーカード（※）の地域住民向け領域利用に関する内容等、検討の際に利用します。

※住民基本台帳カードについても、同様に利用できます。

Ⅰ　マイナンバーカードアプリケーション搭載システムの概要

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。）は、地域住民向け領域設定システム、拡張利用領域設定システム（※1）及びオペレータ認証システムの 3 つのシステムから構成されます。

地域住民向け領域設定システムは、住民からの申込みに基づき、マイナンバーカードの空き領域設定（以下「地域住民向け領域設定」（※2）という。）やサービスの利用可否等、地域住民向け領域利用のための設定（以下「地域住民向けサービス登録」という。）を行うシステムです。

オペレータ認証システムは、システムが不正利用防止のため、生体認証等を利用して、システムを操作する権限を持つ操作者以外の操作を制限するシステムです。

※1 拡張利用領域設定システムに関しては、「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（拡張利用領域設定システム編）」を参照してください。

※2 住民基本台帳カードの場合は、「独自利用領域設定」といいます。なおカード AP 搭載システムの画面等で、「地域住民向け領域設定」を「独自利用領域設定」と表記している場合があります。

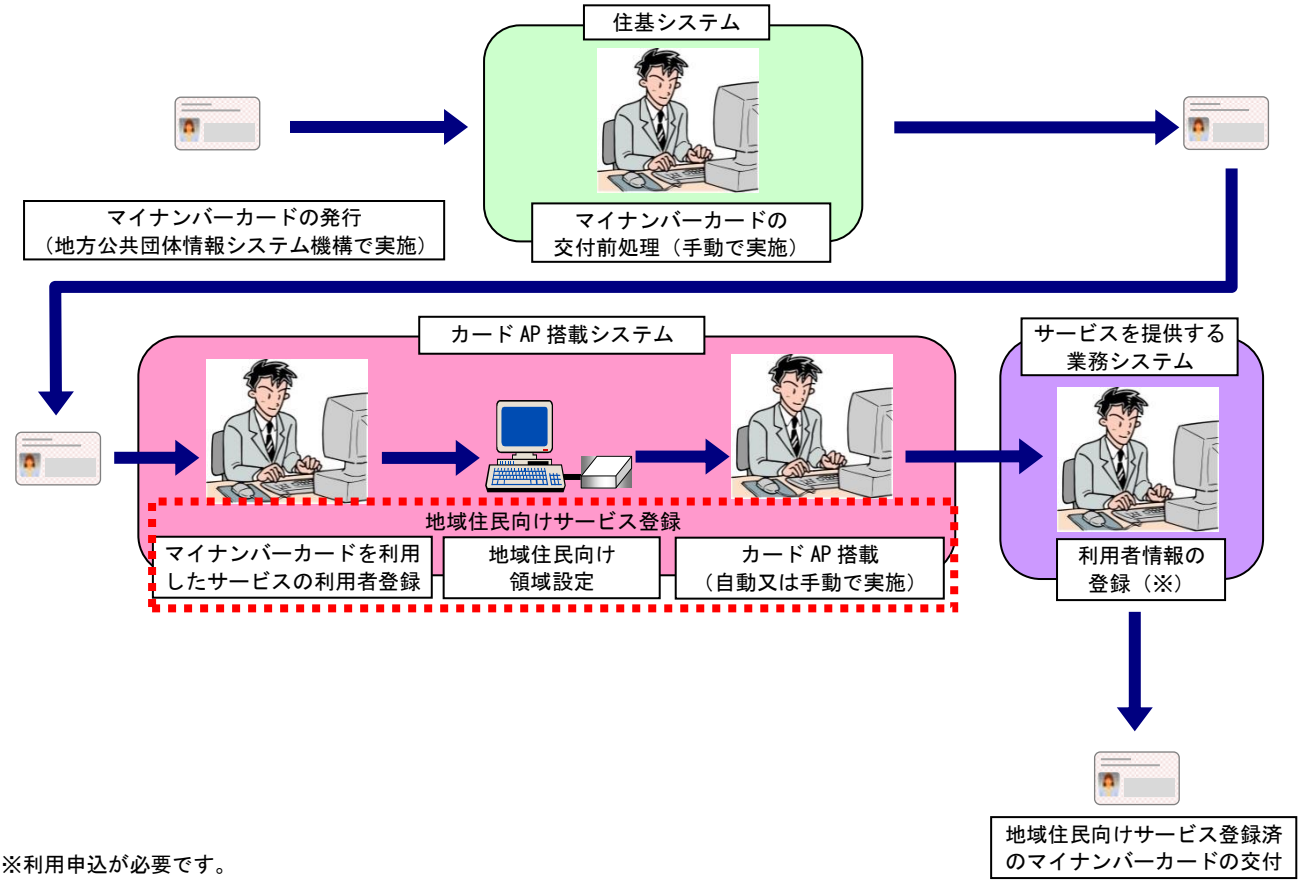
1　地域住民向け領域設定システムによる地域住民向けサービス登録

地域住民向け領域設定システムでは、マイナンバーカードについて地域住民向けサービス登録を行う他、オプションとしてカード AP 搭載システムが提供する、証明書等自動交付サービス向けのカード管理・利用者情報登録機能を利用することもできます。

実施する業務について、以下に示します。

1.1 地域住民向けサービス登録業務

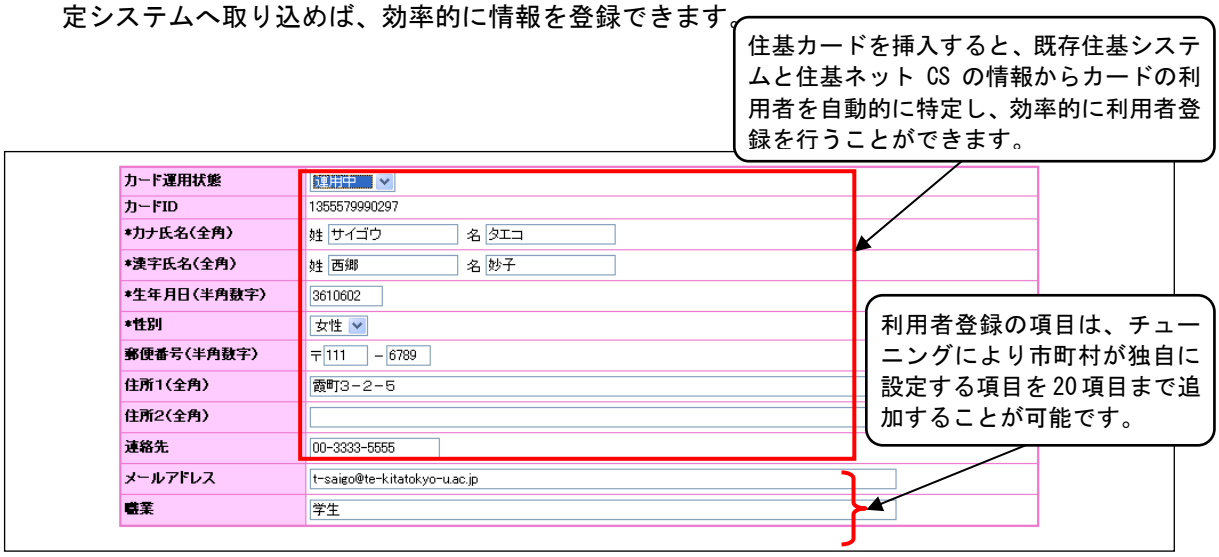
マイナンバーカードについては、地域住民向け領域設定システムでサービスの利用者の登録、地域住民向け領域設定後、カード AP を搭載し、サービスを提供する業務システムで利用者情報を登録すれば、サービス利用が可能になります。業務の流れを、以下に示します。



※利用申込が必要です。

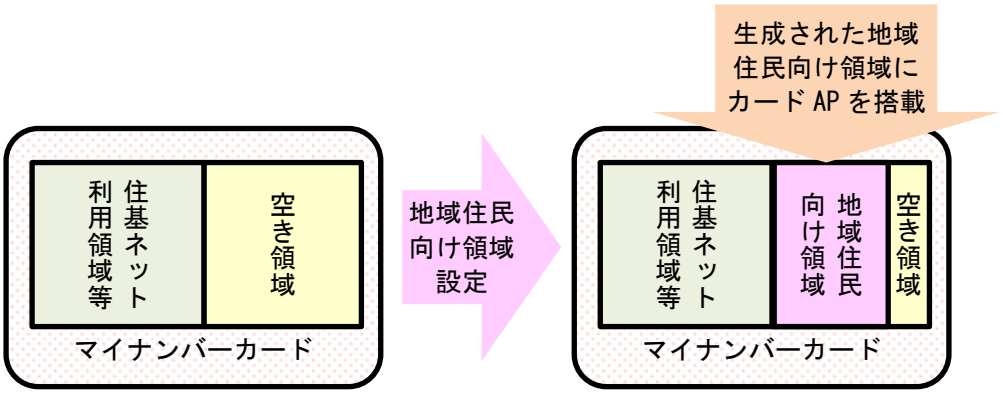
(1) 利用者登録

地域住民向け領域設定システムに利用者の情報を登録します。登録の際に、既存住基システムから住民情報（氏名・住所等）を、住基ネット CS から本人確認 4 情報を予め地域住民向け領域設定システムへ取り込めば、効率的に情報を登録できます。



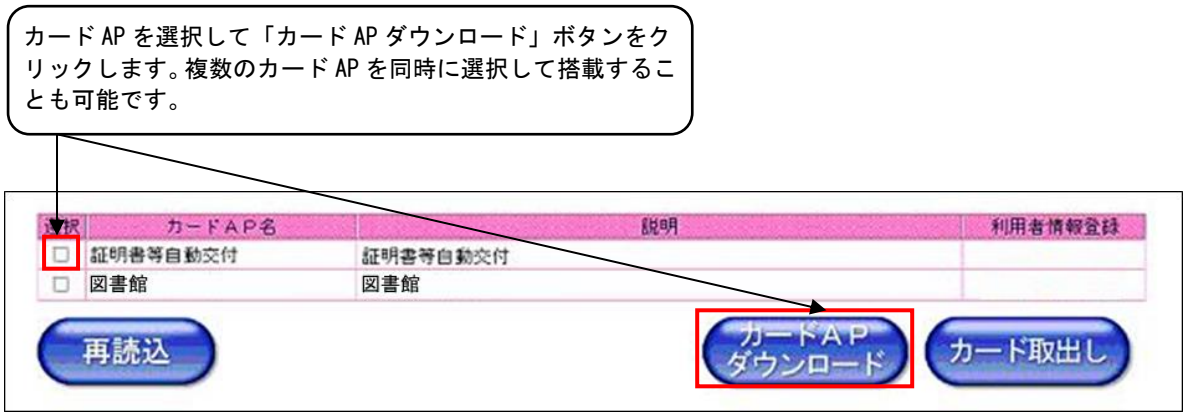
(2) 地域住民向け領域設定

マイナンバーカードの空き領域に、地域住民向け領域を生成します。地域住民向け領域設定を行うことで、カード AP 搭載が可能になります。



(3) カード AP 搭載

市町村が提供するカード AP 搭載システム及び市町村独自のサービスの中から、住民が希望する住民が希望するサービスについて、カード AP を搭載します。その後、住民からの要望によって、カード AP を追加で搭載したり、削除したりすることが可能です。



カード AP については、1 枚ずつ手動でカード AP を選択のうえ搭載する他、予め搭載する AP を選択することにより、地域住民向けサービス登録を行うすべてのマイナンバーカードに、自動的に選択したカード AP を搭載することも可能です。(この場合は上記のカード AP 搭載画面が表示されません。)

(4) 各サービスへの利用者情報の登録

搭載したカード AP を利用可能とするために、各サービスのシステムへの利用者情報の登録を行います。

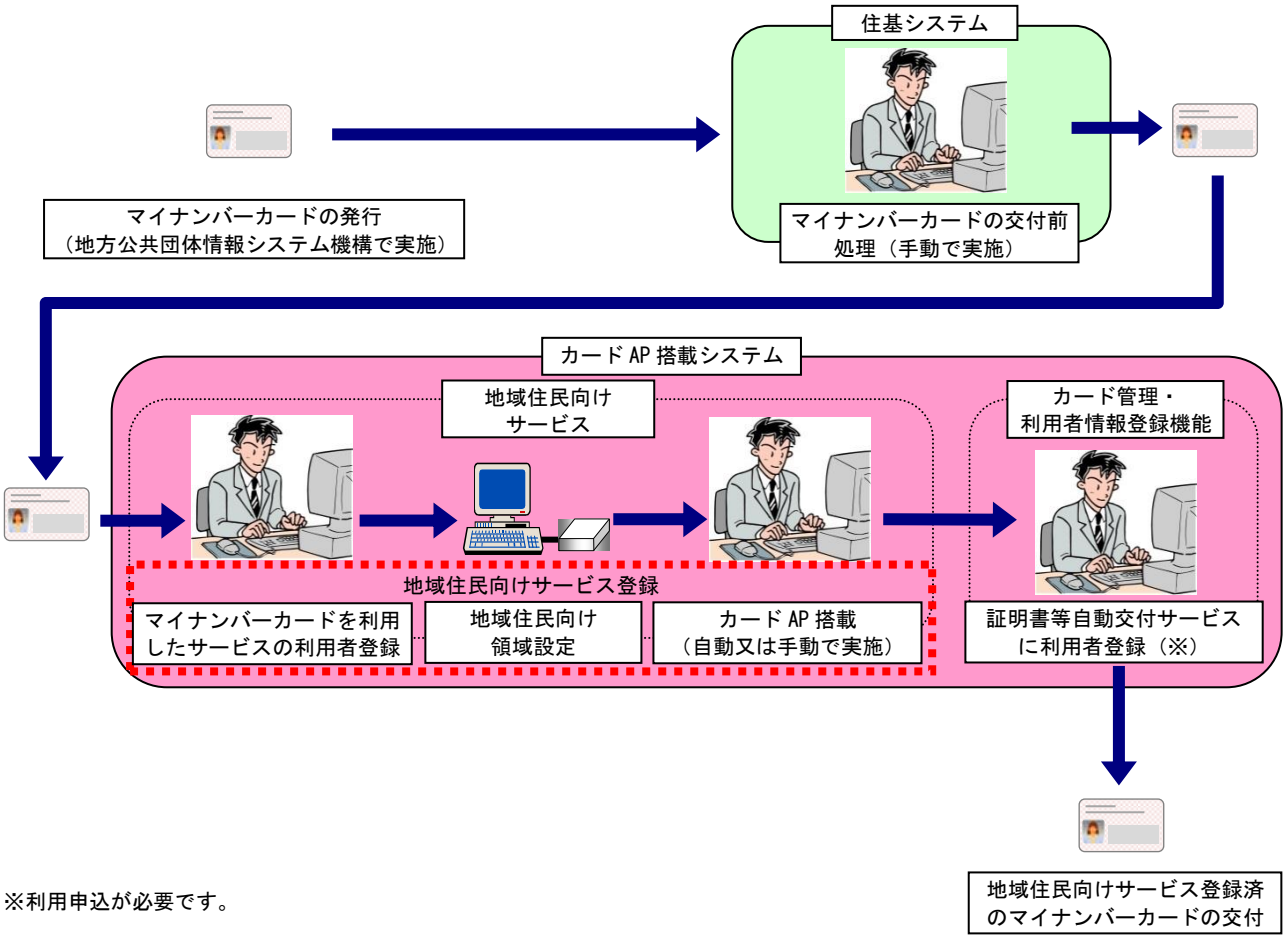
各サービスに必要な利用者情報は、カード AP 搭載システムが規定するインタフェースに準拠することにより、すでに地域住民向け領域設定システムに登録されている利用者情報を自動的に各サービスのシステムへ連携したうえで、それ以外の各サービスに必要な情報のみを手作業で入力するようにすることも可能です。

1.2 カード管理・利用者情報登録機能と地域住民向けサービス登録を組み合わせた業務

証明書等自動交付等サービス向けに提供されるカード管理・利用者情報登録機能を利用すると、証明書等自動交付システムへの利用者情報の登録を地域住民向け領域設定システムで行うことができます。

これにより、一台の端末で、マイナンバーカードの地域住民向けサービス登録、及び証明書等自動交付システムへの利用者情報登録を地域住民向け領域設定システムで一括して行うことができます。業務の流れを、以下に示します。

※本機能を利用して登録した利用者情報を、カード AP 搭載システムが規定するインタフェースに従って証明発行サーバへ連携する必要があるため、証明発行サーバの改造が必要になる場合があります。
詳細については、証明書等自動交付システムを提供する各事業者へ問合せてください。



※利用申込が必要です。

(1) 利用者登録

1.1(1)に記載の内容で、利用者登録を行います。

(2) 地域住民向け領域設定

1.1(2)に記載の内容で、地域住民向け領域設定を行います。

(3) カード AP 搭載

1.1(3)に記載の内容で、カード AP を搭載します。

(4) 証明書等自動交付サービスへの利用者登録

搭載したカード AP を利用可能とするために、証明書等自動交付サービスへの利用者情報の登録を行います。

カード管理・利用者情報登録機能を利用することにより、サービスに必要な利用者情報は、地域住民向け領域設定システムで登録することができます。

カード AP 搭載が終了したサービスに、
利用者情報を登録するために、該当の
利用者情報登録ボタンをクリックします。

証明書等自動交付システムへ登録する情報（証明書の暗証番号等）を入力します。

通常、証明書等自動交付システムへの利用者情報登録は、操作者用端末ではなく証明書自動交付システムの端末で実施します。カード管理・利用者情報登録機能を利用することにより、一連の作業として操作者用端末で利用者情報登録を実施することが可能です。

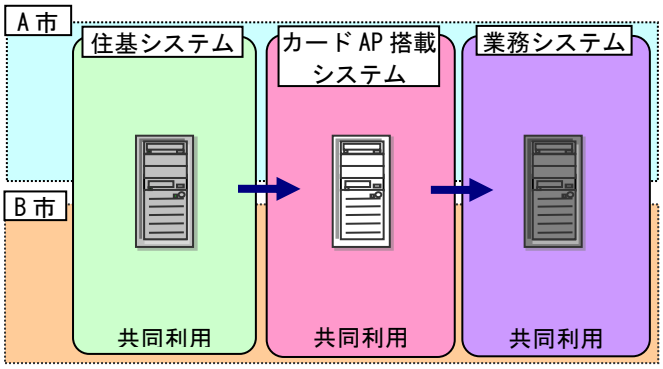
登録した情報は、地域住民向け領域設定システムから証明書等自動交付システムへ連携されます。

1.3 共同利用

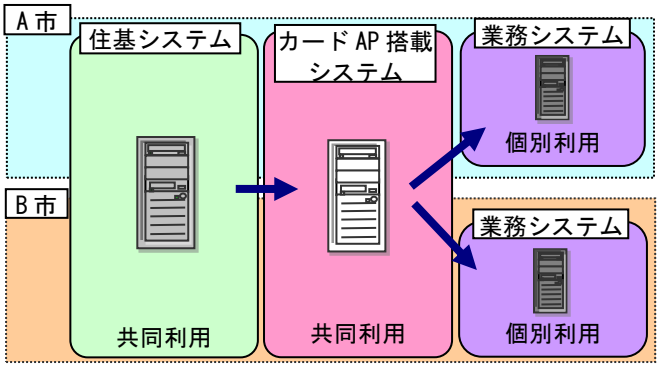
カード AP 搭載システムは、複数の市町村で共同利用できます。共同利用を実施することにより、各市町村がカード AP 搭載システムを個別に導入するよりも安価に導入が可能となります。

共同利用の形態は、下図に示すとおりで、住基ネット CS や業務システムの運用単位には依らず様々な運用形態に対応することが可能です。

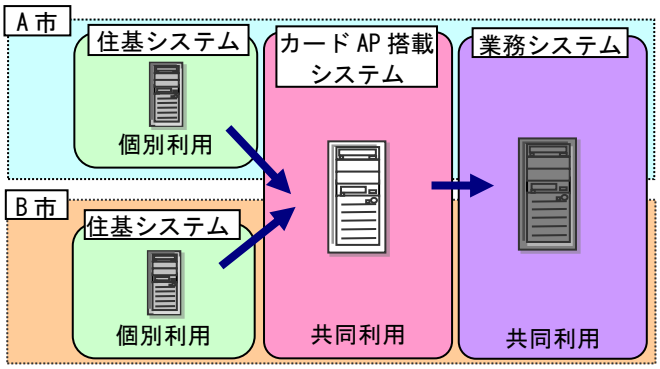
パターン 1：すべてを共同利用



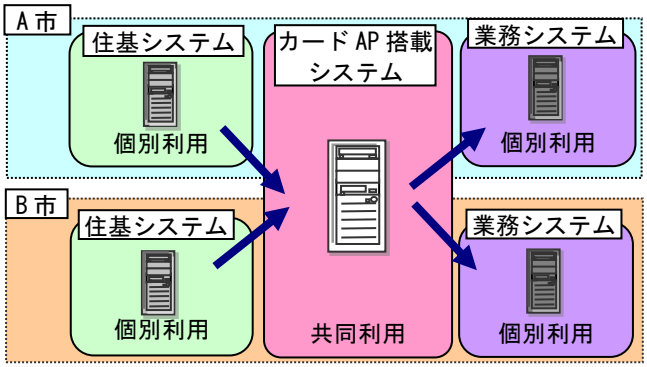
パターン 2：住基システム及びカード AP 搭載システムを共同利用



パターン 3：カード AP 搭載システム及び業務システムを共同利用

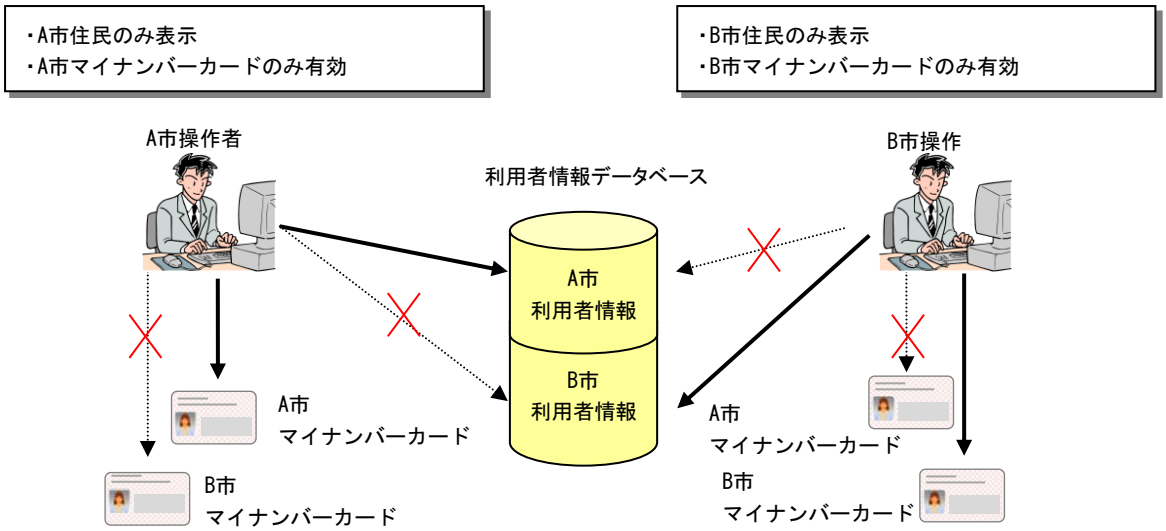


パターン４：カード AP 搭載システムを共同利用



(1) 住民情報アクセス制限

共同利用した際に、それぞれの市町村の情報は、当該市町村以外からアクセスできないよう、アクセス権限が設定できます。



2　オペレータ認証システムによる不正使用等の悪用防止

市町村操作者等の業務システムへの操作に際して、特定の操作者以外の操作を制限したり、操作できる機能を限定したりすることができます。これを「操作者の権限チェック」といいます。

また、業務システムの情報登録及び参照時は、ネットワーク上での盗聴防止のため、暗号化します。併せて、操作しているシステムが、正しいカード AP 搭載システムの業務システムであることを確認します。この 2 つを「通信の暗号化と通信相手チェック」といいます。

各業務システムは、「操作者の権限チェック」と「通信の暗号化と通信相手チェック」の組み合わせにより、市町村内部の不正使用等の悪用防止対策を施し、安全に運用できます。各業務システムの安全な運用をサポートするシステムがオペレータ認証システムです。

操作者の権限チェックでは、「オペレータ ID・パスワードによる認証方式」に加え、「生体認証方式」のあわせて 2 通りの方式が利用できます。

2.1 操作者の権限チェック

(1) 操作者の権限チェックの概要

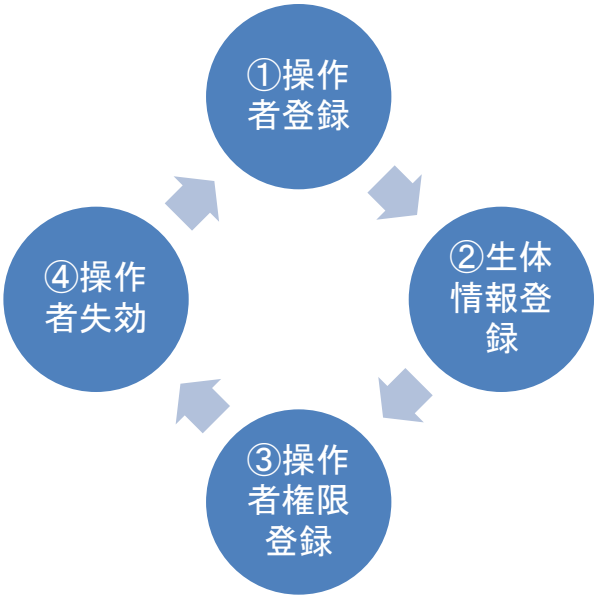
操作者の権限チェックでは、「生体認証方式」又は「オペレータ ID 及びパスワードによる認証方式」の 2 通りの方式を利用できます。

生体認証方式では、操作者の生体情報を事前登録します。この作業は、各業務システムの操作者を識別する情報を登録・管理する部門（運用管理部門）で行うことを想定しています。

操作者のなりすまし等に対するセキュリティを確保するために、生体認証方式の導入を推奨します。

(2) 生体認証方式における操作者の権限チェックの特徴

操作者の権限は、以下の 4 つのプロセスからなる流れとなります。



①操作者登録

運用管理部門は、カード AP 搭載システムの運用準備作業として、操作者の名前、所属等の操作者管理情報及び操作者に利用可能な業務システムを対応付ける操作者権限情報を入力し、操作者を一意に識別する「オペレータ ID」を登録します。

②生体情報登録

運用管理部門は、オペレータ ID に対応する生体情報を事前登録します。

③操作者権限登録

業務システムの管理者は、操作者を一意に識別するオペレータ ID に対し、業務ごとの「業務内 ID」を対応付けます。「業務内 ID」は、業務システムごとの業務権限とのセットであり、業務システムで登録します。

これにより操作者は、一つのオペレータ ID で複数の業務システムを利用でき、業務システムの管理者は、操作者それぞれの利用範囲を制限できます。

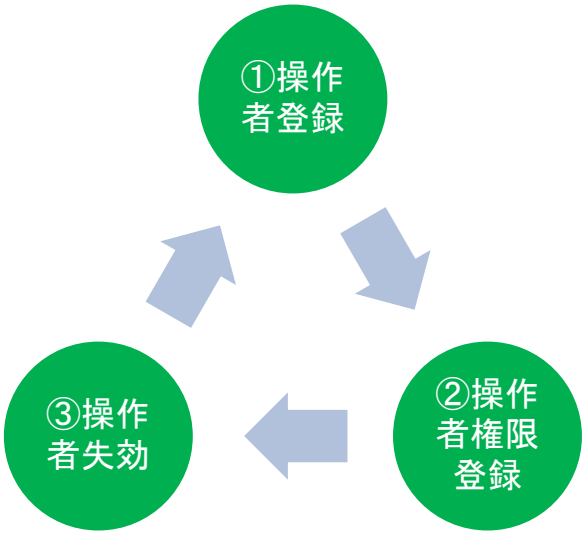
操作者権限のイメージについては、(4) を参照してください。

④操作者失効

運用管理部門は、操作者の権限を失効する場合に操作者の登録情報を削除します。

(3) ID・パスワードによる認証方式における操作者の権限チェックの特徴

操作者の権限は、以下の 3 つのプロセスからなる流れとなります。



①操作者登録

(2)①に記載のとおりです。

②操作者権限登録

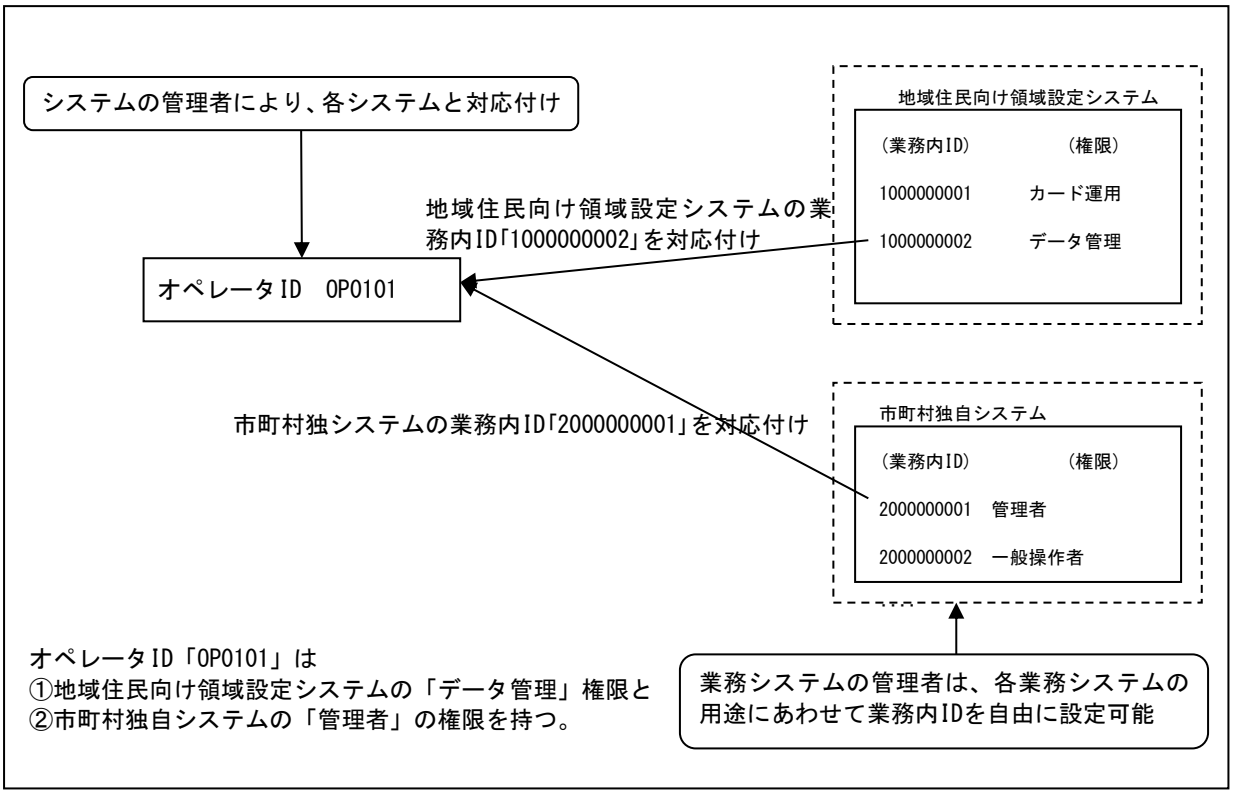
(2)③に記載のとおりです。

③操作者失効

(2)④に記載のとおりです。

(4) 操作者権限のイメージ

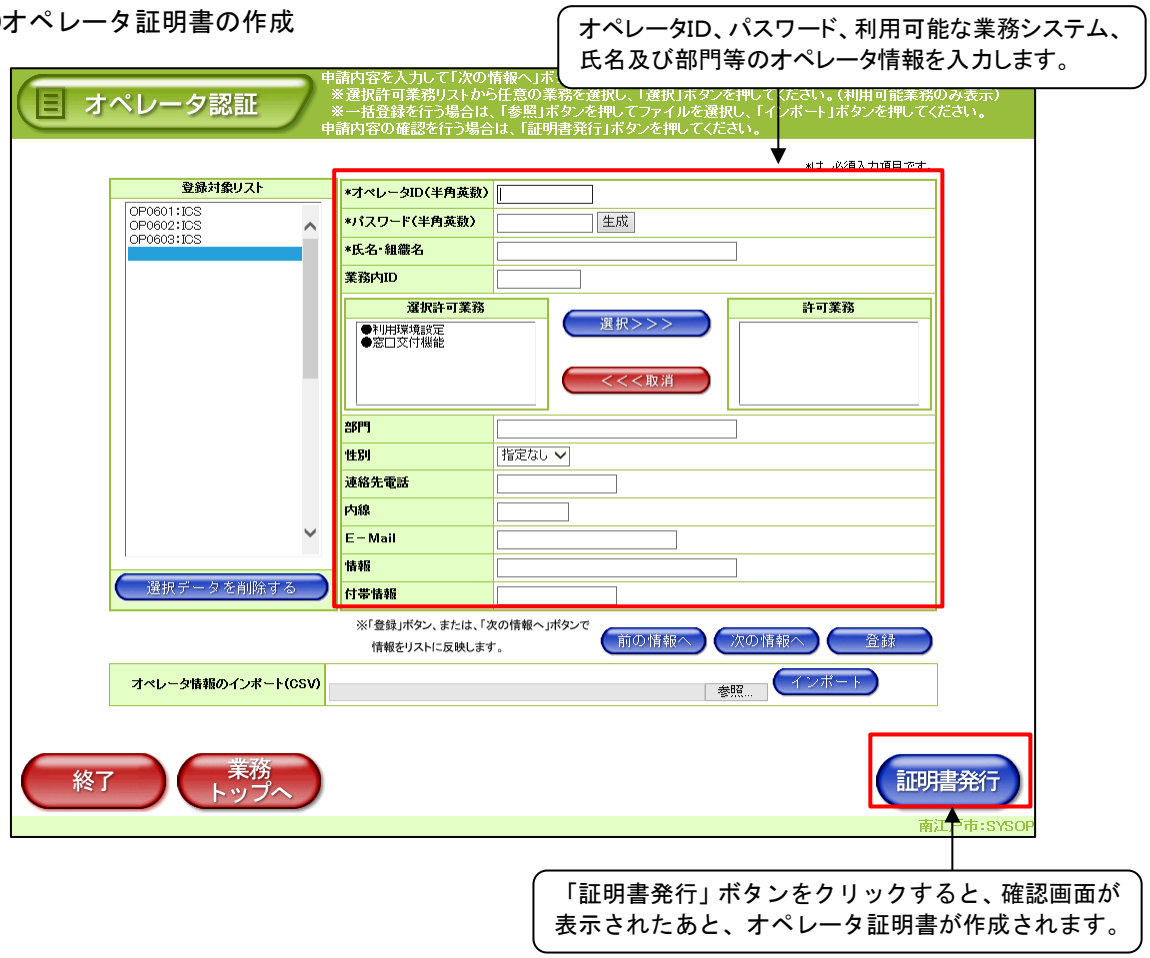
操作者権限のイメージを、以下に示します。



(5) 操作者の権限登録

操作者の権限登録では、利用可能な業務システム等、操作者の権限に基づいた電子証明書（以下「オペレータ証明書」という。）を作成します。オペレータ証明書の作成後、採用する認証方式に応じて必要な手順を実施します。

①オペレータ証明書の作成



②オペレータ証明書作成後の手順

操作者の権限チェックを生体認証方式で行う場合、各操作者に対して、生体情報を事前に登録する必要があります。上記①でオペレータ情報を登録し、電子証明書（オペレータ証明書）を作成後、生体認証装置を用いて生体情報を取得します。

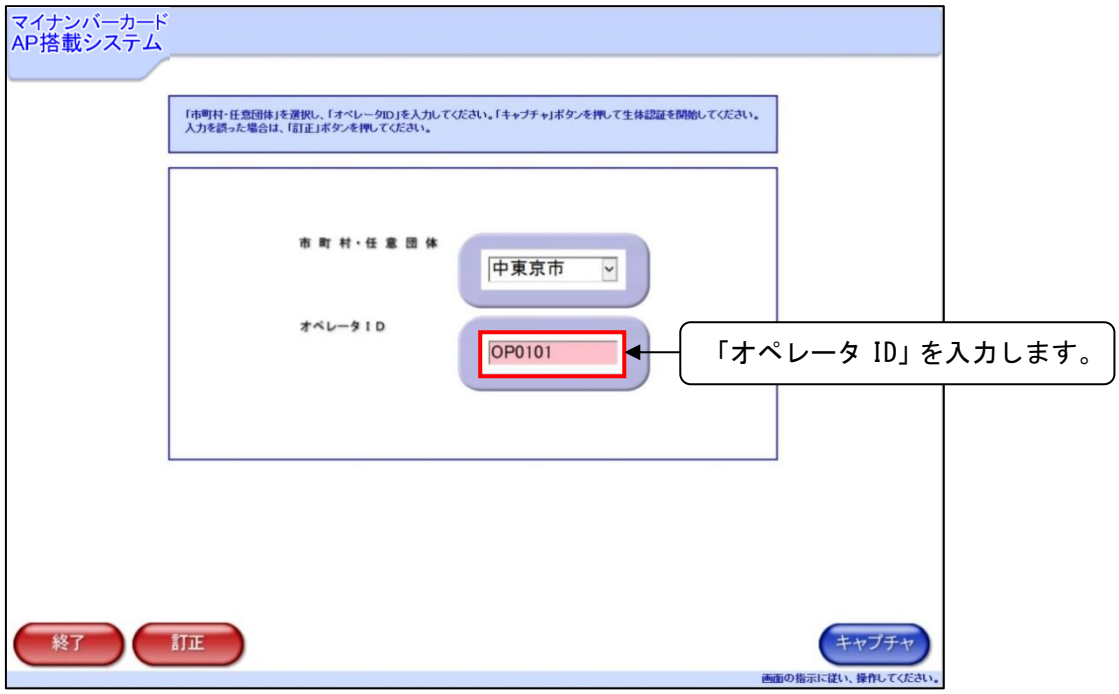
なお ID・パスワードによる認証方式の場合は、実施する必要がありません。

(6) 操作者の権限チェックにおける運用

操作者の権限チェックは、操作者等が業務システムの操作を開始するときに行われます。採用する認証方式により、以下の手順を実施します。

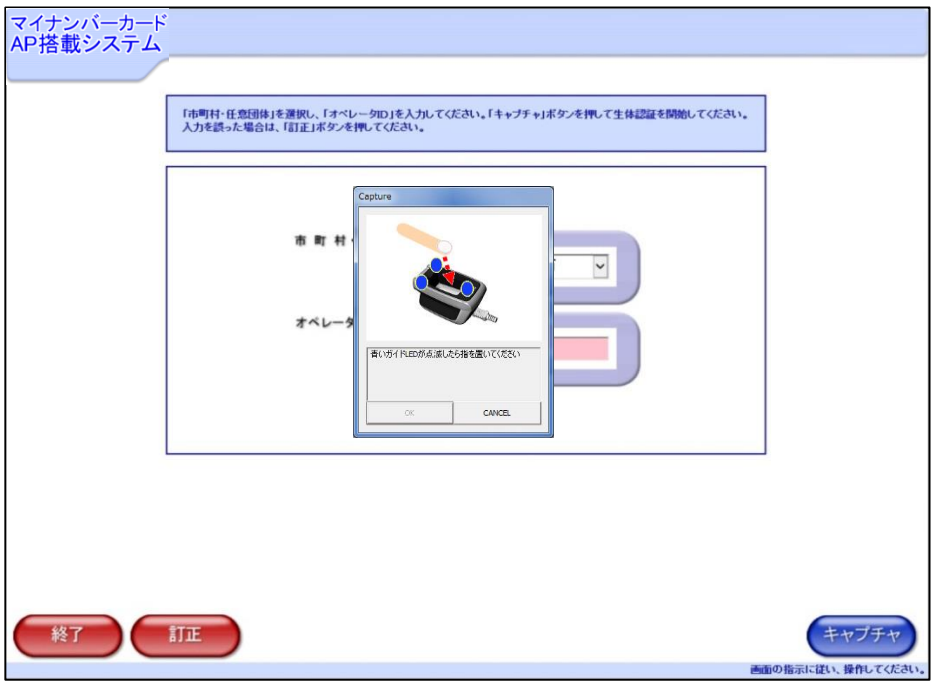
①生体認証方式の場合

（A）生体情報照合画面で、操作者のオペレータ ID を入力します。

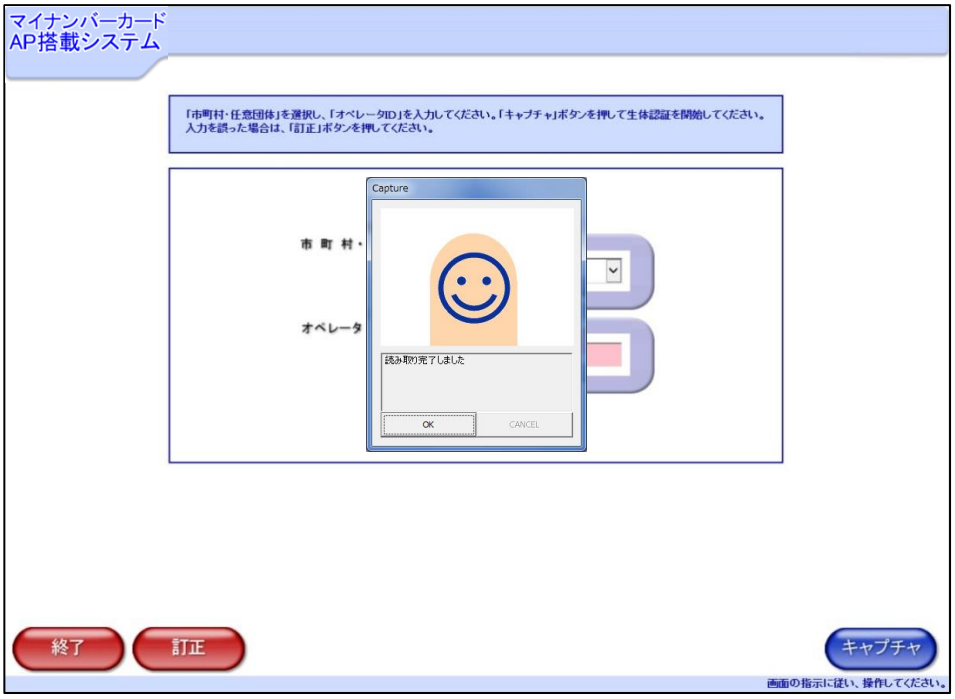


※共同利用を実施している場合は、市町村・任意団体も設定します。

（B）登録した指を生体認証装置に置きます。



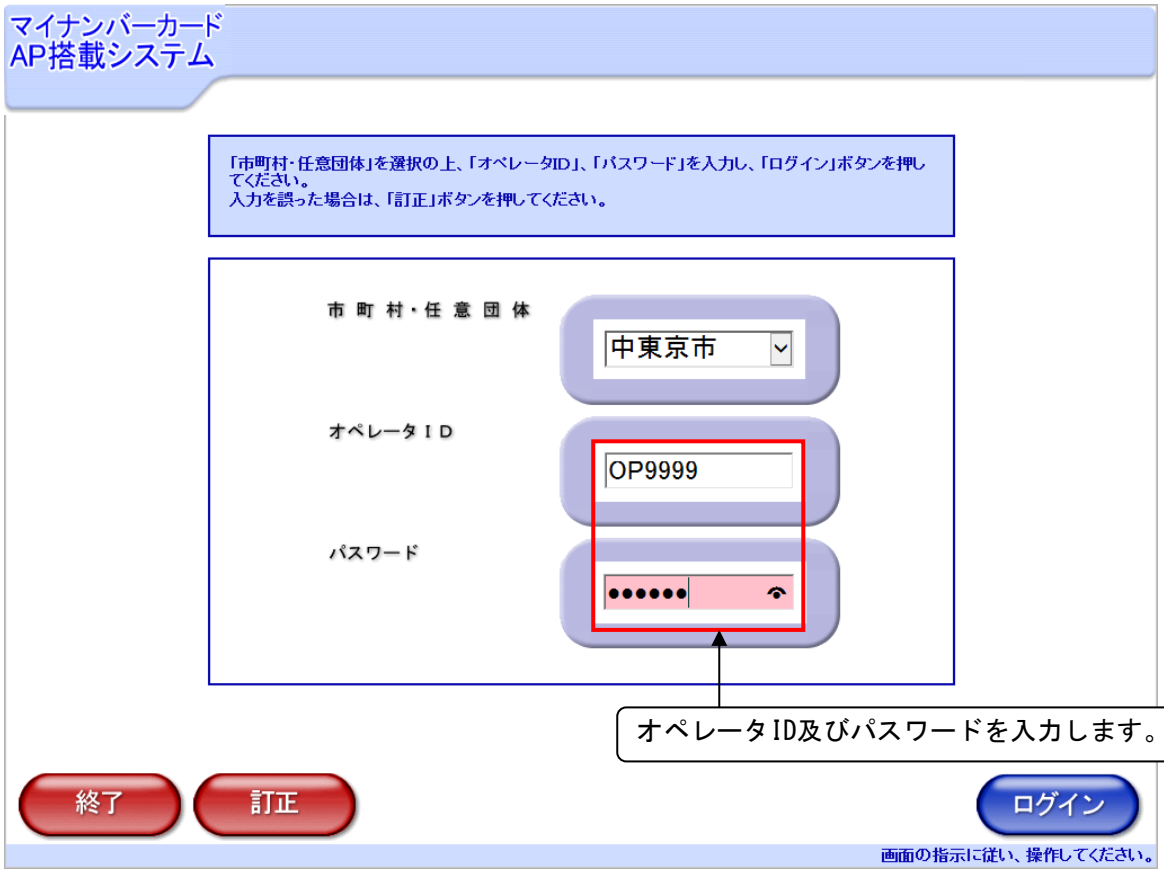
（C）生体情報が読み込まれます。



（D）操作者権限が確認された場合には、利用可能な業務システムを含む操作者用トップ画面が表示されます。

②ID・パスワードによる認証方式の場合

（A）操作者用ポータルメニューログイン画面にて、操作者のオペレータ ID 及びパスワードを入力します。



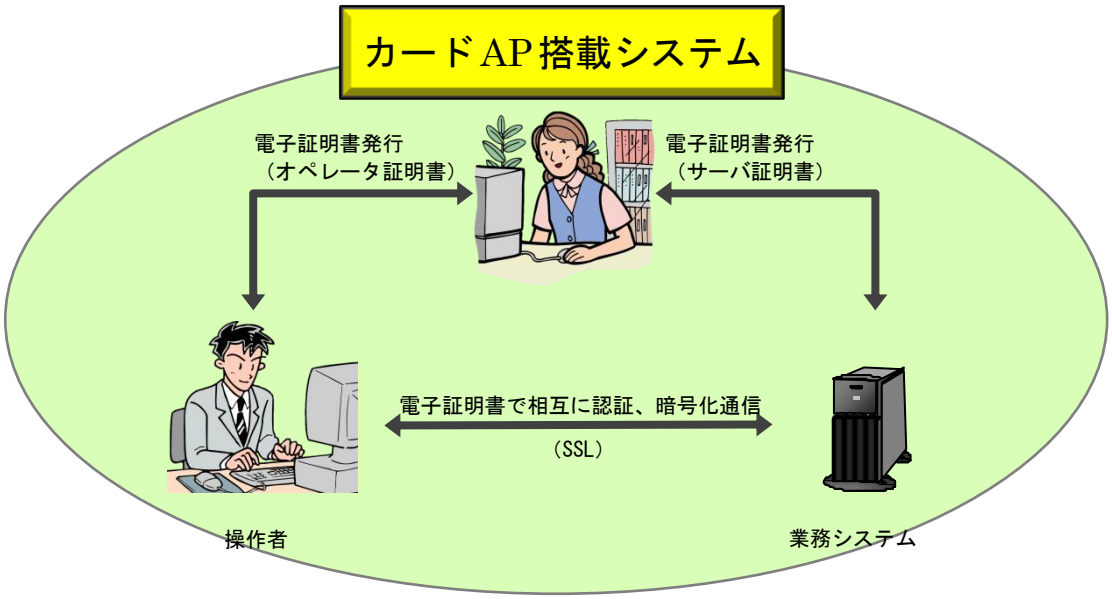
※共同利用を実施している場合は、市町村・任意団体も設定します。

（B）操作者権限が確認された場合には、利用可能な業務システムを含む操作者用トップ画面が表示されます。（画面については、①（D）を参照してください。）

2.2 通信の暗号化と通信相手のチェック

(1) 通信の暗号化と通信相手チェックのコンセプト

通信の暗号化と通信相手チェックは、SSL の技術を用いて実現しています。SSL は、インターネット及びイントラネット上の認証・暗号の仕組みとして実用化され、普及している技術のひとつです。



生体認証方式による認証方式の場合において、通信相手のチェックは、操作者側と業務システム側の両方で SSL を用いて相互に相手を認証します。その結果、双方が相手を正しいと認識したとき、暗号用の鍵を交換し、業務システムに情報を登録・参照する際に、ネットワーク上で盗聴されないように通信の暗号化を行います。

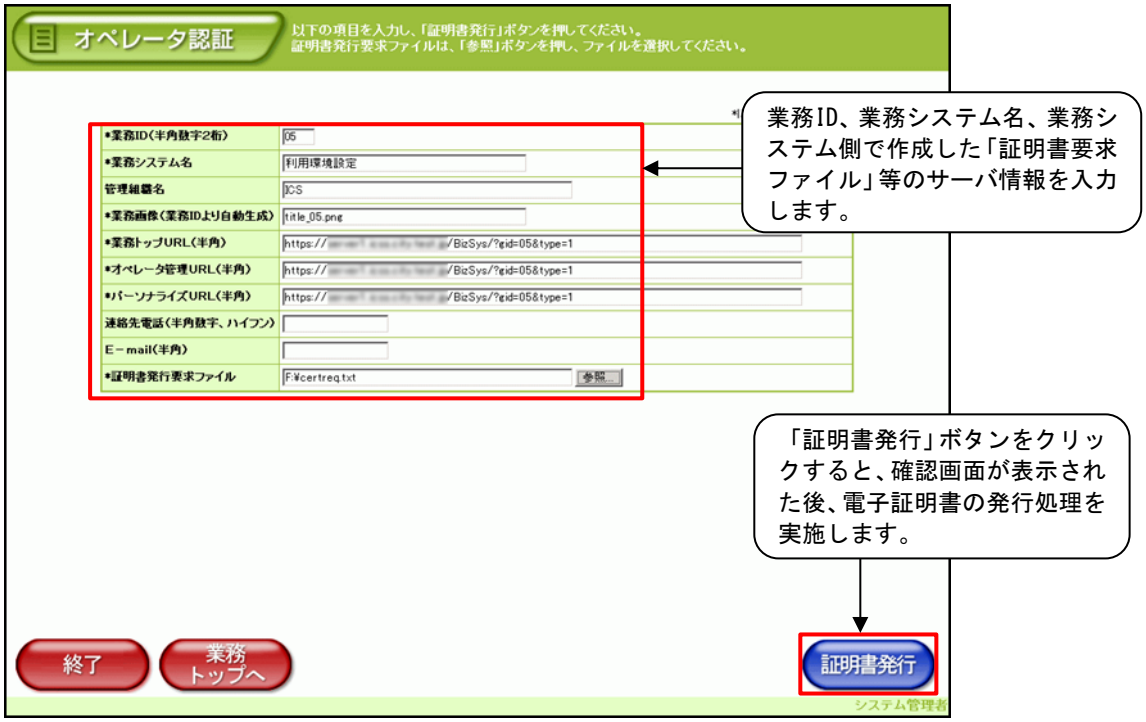
具体的には、まず業務システムのサーバにはサーバ証明書と呼ばれる電子証明書を格納します。操作者側及び業務システム側でそれぞれの通信相手の電子証明書を検証して相互認証します。

オペレータ ID・パスワードによる認証方式の場合の通信チェックでは、操作者側から業務システム側を認証する、片側の認証となります。業務システム側から操作者側の認証は、オペレータ ID に対応するパスワードが正しいかどうかをチェックすることにより行います。

(2) サーバ証明書の発行

サーバ情報に基づいてサーバ証明書を発行します。発行されたサーバ証明書は、ダウンロードできますので、それを業務システムのサーバに格納します。なお、サーバ証明書の発行は、市町村が独自に準備したシステムに対して行うことも可能です。

①業務システムのサーバ情報を入力します。



②業務システムのサーバ証明書を取得します。

③ダウンロードしたサーバ証明書を業務システムサーバに格納します。

(3) 共同利用

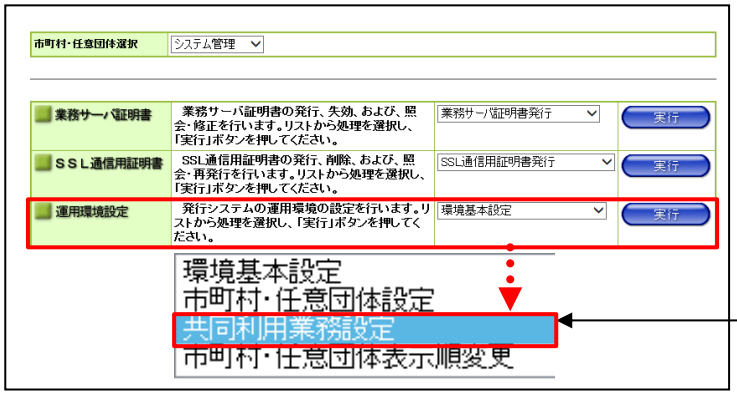
通常、市町村ごとに行う必要がある操作者の登録・権限作業を、システム管理者が一括して実施ことができます。

また、操作者情報の移行機能を提供します。

(4) 業務システムの共同利用設定

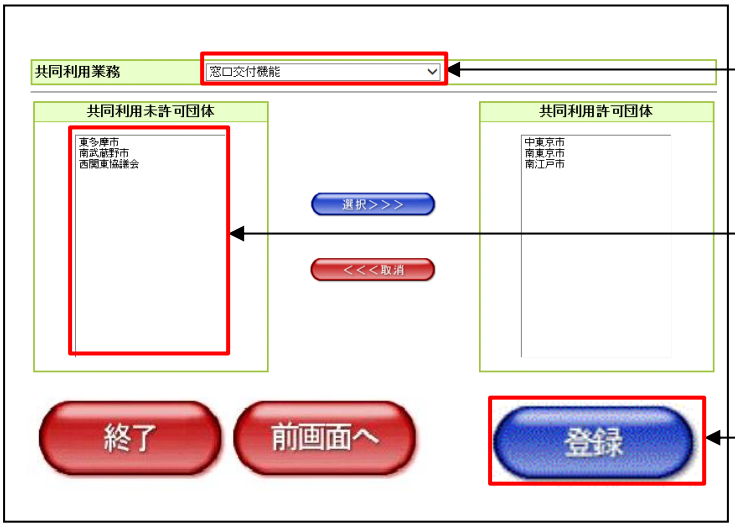
共同利用する業務システムを団体ごとに設定します。これにより、権限を持たない操作者のアクセスを制限でき、高いセキュリティレベルを保つことができます。

①共同利用業務設定を選択します。



共同利用業務設定を選択します。

②共同利用する業務システムに団体を対応付けます。



業務システムを選択します。

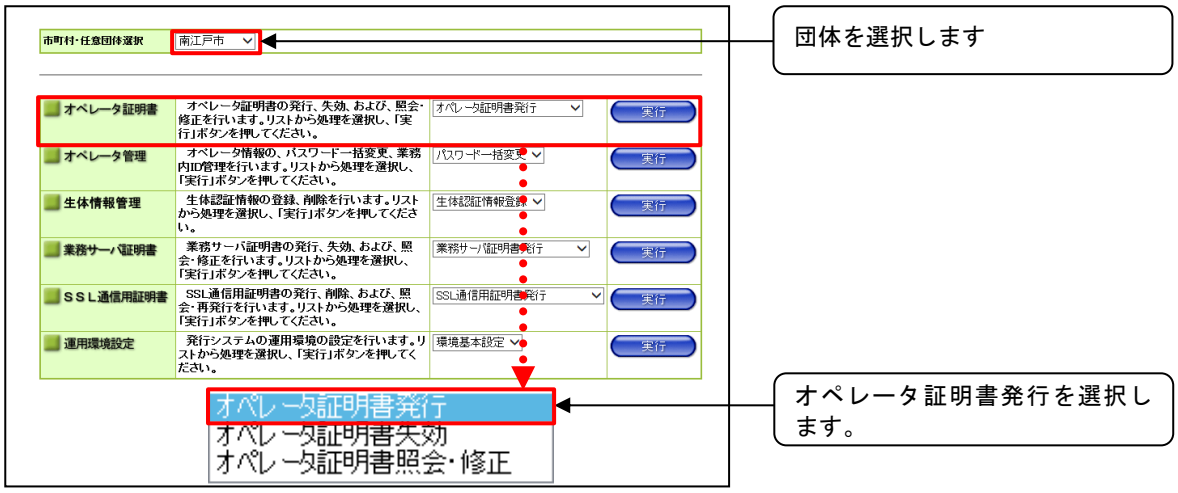
共同利用を許可する団体を選択します。

「登録」ボタンをクリックすると、情報が登録されます。
サーバ情報入力画面で入力した内容を確認します。

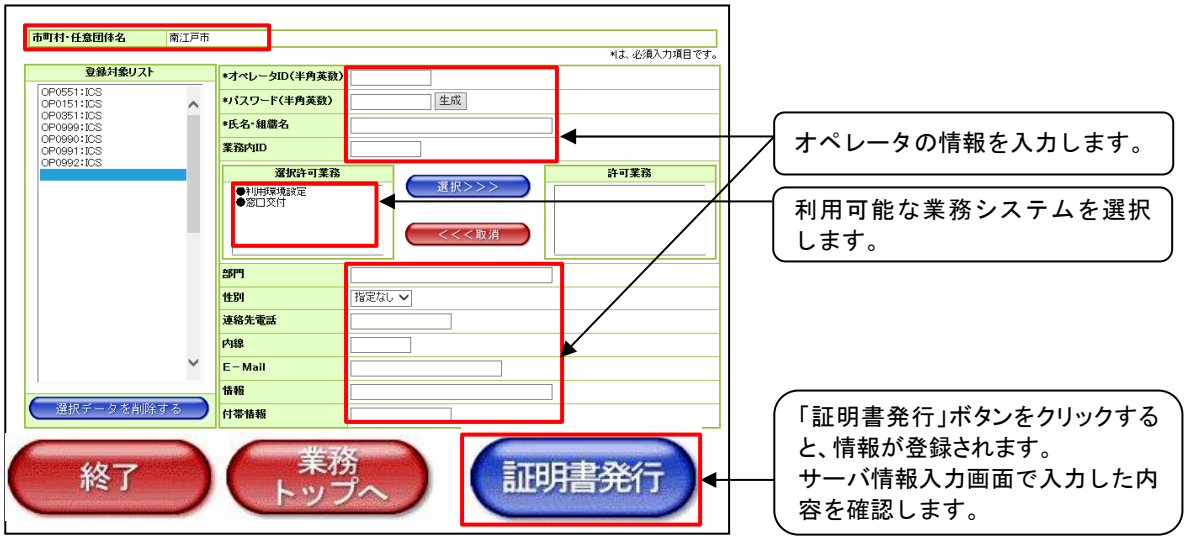
(5) 操作者の登録

システム管理者が一括して共同利用の各団体の操作者を登録でき、操作者ごとに権限を設定できます。

①オペレータ証明書発行を選択します。



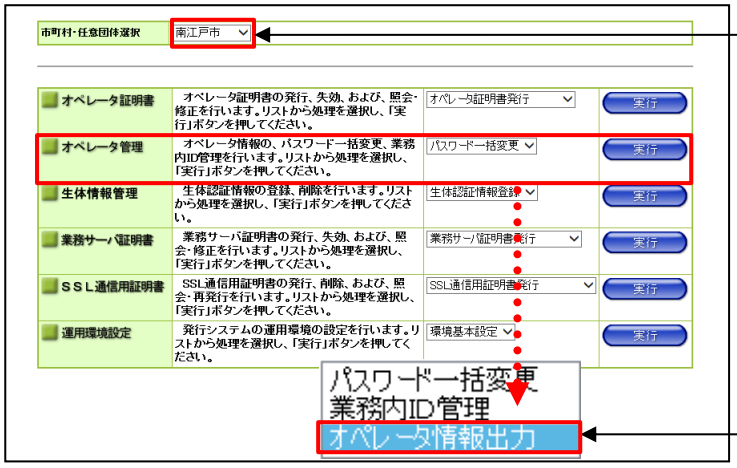
②共同利用する業務システムに団体を対応付けます。



(6) 操作者情報の移行

操作者情報を特定の団体から別の団体へ一括して移行することができます。

①オペレータ情報出力を選択します。



団体を選択します。

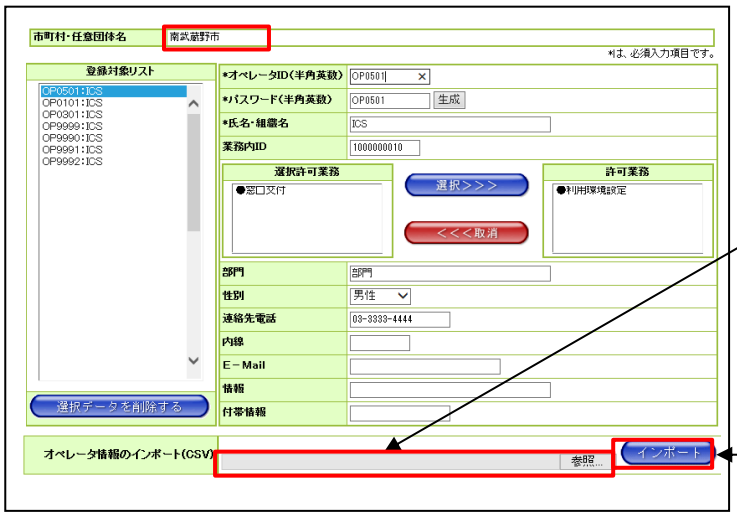
オペレータ情報出力を選択します。

②オペレータ情報を出力します。

出力条件を設定できます。

「ファイル出力」ボタンをクリックすると、情報がCSVファイルで出力されます。

③オペレータ情報を別の団体に移行します。



オペレータ情報を出力したCSVファイル名を指定します。

「インポート」ボタンをクリックすると、オペレータ情報が展開されます。
サーバ情報入力画面で入力した内容を確認します。

II システムの概要

1　証明書等自動交付システム

1.1 証明書等自動交付システムの概要

証明書等自動交付システムは、住民が、コンビニエンスストア等に設置されているキオスク端末及び支所や駅前等のブースに設置されている自動交付機に自身のマイナンバーカードを認証させ、暗証番号を入力するだけで簡単に住民票の写しや印鑑登録証明書等の各種証明書の交付を受けることが出来るシステムです。

証明書等自動交付システムを導入することにより、以下のような便益を得ることが可能です。

- 窓口営業時間外の証明書等の交付
- 申請書への記入等請求手続きの簡略化
- 窓口での待ち時間短縮
- 操作者稼動の軽減
- 広域エリアの証明書等の交付（コンビニ交付を導入した場合）

1.2 証明書等自動交付システムの各サービス

(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。コンビニ交付により、土日・時間外や通勤・通学圏内での証明書等の交付等システム・機能拡張に取り組む市町村も増えています。（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の概要

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、住民は、自動交付機を自ら操作して、証明書等の申請から交付まで受けられます。

なお、カード AP 搭載システムでは証明書等自動交付システムについて、以下のインタフェースを規定しています。

- 証明書等自動交付システムとマイナンバーカード間
- 証明発行サーバと地域住民向け領域設定システム間（カード管理・利用者情報登録を利用する場合）

市町村において証明書等自動交付システムを導入するためには、自動交付機を提供する事業者から、上記インタフェースに順ずる自動交付機や証明発行サーバ等を調達し、システム構築を行う必要があります。詳細については、各事業者に問合せてください。

なお証明発行サーバについては、コンビニ交付サービスとの兼用が可能です。

また各事業者が提供する自動交付機の仕様にもよりますが、一般的に自動交付機は、以下のような機能を有します。

①利用者の認証機能
②料金徴収機能
③運用監視機能
④待ち受け画面表示機能　等

市町村は各自動交付機の機能やサイズ、価格等を比較・考慮し、自動交付機を選定することが可能です。

2　図書館システム

2.1 図書館システムの概要

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受けることを可能とします。

これは、市区町村の図書館システム側に住基カード内又はマイナンバーカードの情報を読み取る機能等を組み込むことにより、一枚のマイナンバーカードで、マイナンバーカードの交付を受けた市区町村の図書館ばかりでなく、複数の市町村の図書館システムにおいて、サービスの提供を受けることが可能となります。(※)

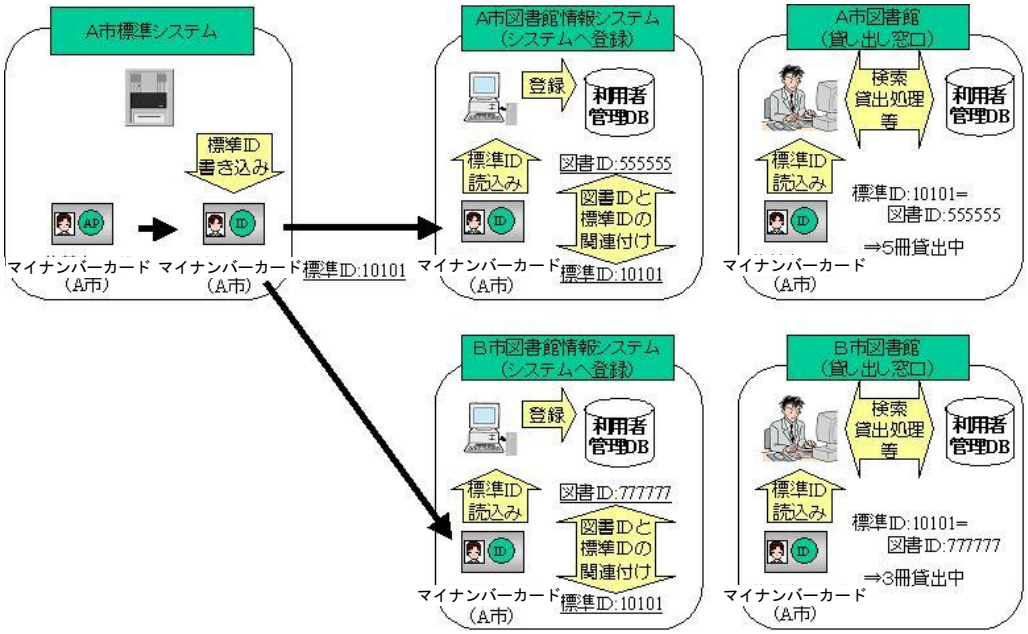
※カード AP 搭載システムが規定するインタフェースに準拠した図書館システムで利用者登録を行えば、利用できるようになります。

2.2 図書館システムの特徴

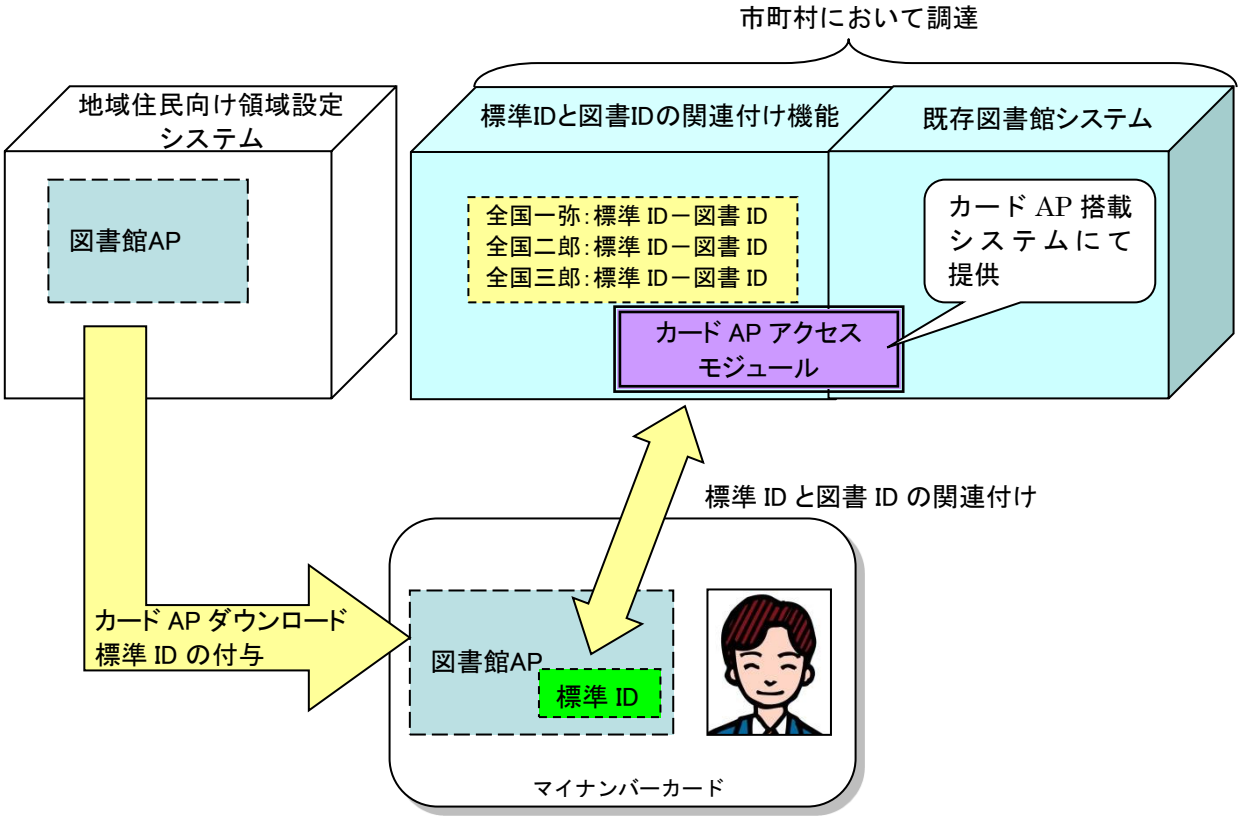
各市町村の既存の図書館システムと同じように、利用者番号(図書 ID)は、各市町村で附番し、それを既存の図書館システムで管理します。

カード AP 搭載システムで、マイナンバーカードのカード AP 内に、市町村コードと各市町村で附番する一意の番号（乱数）により、全国で一意となる番号（標準 ID）を書き込み、マイナンバーカード内の標準 ID と図書館システムの管理する図書 ID を関連付けることで、サービス提供が可能となります。

これにより、マイナンバーカードを交付し、マイナンバーカード内に標準 ID を書き込んだ市町村ばかりでなく、その他の市町村における図書館システムでも、この関連付けを登録することで、サービス提供が可能となります。


A市標準システム
標準ID
書き込み
AP
ID
マイナンバーカード
（A市）
マイナンバーカード
（A市）
標準ID:10101
A市図書館情報システム
（システムへ登録）
登録
利用者
管理DB
標準ID
読込み
図書ID:555555
図書IDと
標準IDの
関連付け
マイナンバーカード
（A市）
標準ID:10101
A市図書館
（貸し出し窓口）
検索
貸出処理
等
利用者
管理DB
標準ID
読込み
標準ID:10101=
図書ID:555555
⇒5冊貸出中
マイナンバーカード
（A市）
B市図書館情報システム
（システムへ登録）
登録
利用者
管理DB
標準ID
読込み
図書ID:777777
図書IDと
標準IDの
関連付け
マイナンバーカード
（A市）
標準ID:10101
B市図書館
（貸し出し窓口）
検索
貸出処理
等
利用者
管理DB
標準ID
読込み
標準ID:10101=
図書ID:777777
⇒3冊貸出中
マイナンバーカード
（A市）

マイナンバーカードを利用して図書館のサービスを受けるための、関連付けの機能については、市町村の図書館システムで実現する必要がありますが、現在、多くの図書館システムベンダでは、この機能を付加しているところです。マイナンバーカードを活用した図書館サービスの提供を検討される市区町村は、図書館システムベンダ及び地方公共団体情報システム機構（以下「J-LIS」という。）に問合せてください。



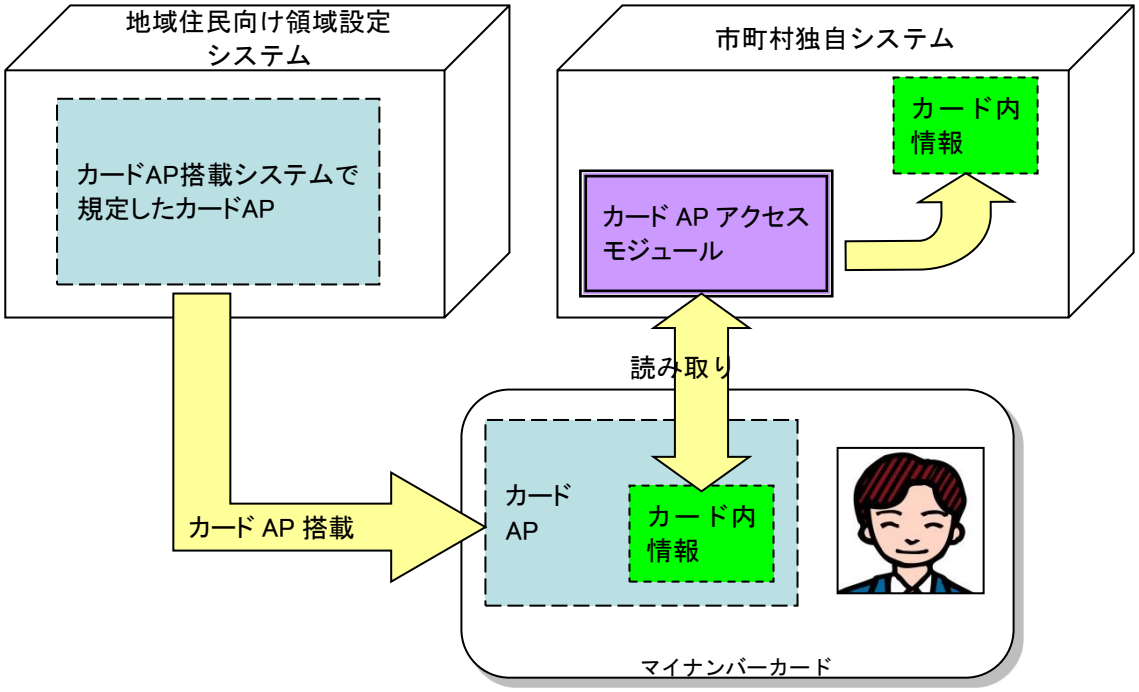
※カード AP アクセスモジュールとは、カード AP 搭載システムの機能として提供しているカード AP 内の情報を簡易に読み込むことができるソフトウェアです。

3　市町村独自システムの開発

カード AP 搭載システムが提供する 3 つのシステムのほか、カード AP アクセスモジュールを利用して、市町村独自システムを導入することができます。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拠することで、カード AP 搭載システムが提供する各システムと同様の運用を行うことができます。

また、市町村独自システムを開発する際に、カード AP 搭載システムの以下の機能と連携を行うことが可能です。

(1) カード AP 搭載システムが提供するカード AP 内の情報を簡易に読み書きできるソフトウェア(カード AP アクセスモジュール)を利用することが可能です。カード AP アクセスモジュールを利用することにより、より簡易に市町村独自システムを開発することが可能です。



※　カード AP アクセスモジュールの提供方法等、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) カードAP搭載システムが提供する地域住民向け領域設定システムとのレプリケーションを利用することができます。レプリケーションを行うことにより、利用者の登録作業を軽減できます。また、地域住民向け領域設定システムで更新された利用者情報の更新を随時行うことにより、利用者情報を常に最新の状態で保持することが可能になります。

(3) カードAP搭載システムが提供するオペレータ認証システムの業務ログイン認証を利用することができます。オペレータ認証使用することにより、カードAP搭載システムと同様のセキュアなログイン認証を行うことが可能になります。

III　システム構成

1　概要

カードAP搭載システムは、運用面及び保守面の観点より、業務システムごとに独立したシステムで構成されています。独立したシステムで構成することには、以下のような利点があります。

- 業務システム毎に異なる利用状況に対し、柔軟なシステムの拡張が可能
- 特定の業務システムで発生した故障が他の業務システムへ影響しない
- 特定の業務システムにおけるメンテナンスのためのシステム停止が他の業務システムへ影響しない
- データベースや各業務システムを実行する環境において、業務ごとに異なる運用形態をサポートすることが可能

1.1 システムごとの機器構成

(1) カードAP搭載システムの機器構成

カードAP搭載システムは、地域住民向け領域設定システムとオペレータ認証システムを同一サーバに格納した、1台のサーバにより構成されます。

(2) 証明書等自動交付システムの機器構成

証明書等自動交付システムは、証明発行端末（証明書自動交付機等）及び証明発行サーバ等から構成されます。また、証明発行サーバは、既存住民情報システムと連携します。

証明書等自動交付システムにおいて、カードAP搭載システムは、マイナンバーカードとのインタフェースを規定しています。

したがって、証明発行端末の機能、既存住民情報システムとのインタフェース及びマイナンバーカードの運用情報（停止、廃止等）を取得するインタフェース等は、開発元の事業者によって異なります。

(3) 図書館システムの機器構成

図書館システムにおいて、カードAP搭載システムは、マイナンバーカードとのインタフェースのみを規定しています。したがって、図書館システムの機能（標準IDと図書IDを関連付ける機能等）は、開発元の事業者によって異なります。

※機器構成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。

1.2 信頼性

カードAP搭載システムにおいて、サーバ装置、ネットワーク機器（ファイアウォール、ルータ、ハブ）等の冗長構成（信頼性）については、代替機を設置し、故障発生時に代替機へ切り替えることを前提としています。代替機は、必要に応じ、市町村にて準備してください。

クラスターシステム等による縮退、切り替え運転については、サポートしていません。

また、カードAP搭載システムでは、無停電電源装置（UPS）の設置を推奨しています。

1.3 拡張性

カードAP搭載システムにおいて、サーバ装置、ネットワーク機器（ファイアウォール、ルータ、ハブ）等の拡張性については、各装置のCPU、メモリ、ディスク増設及び高スペックの機器へ更改することを前提としています。

負荷分散装置（ロードバランサー）等による高負荷への対応は、サポートしていません。

2　ネットワーク構成

(1) 庁内ネットワーク

カードAP搭載システムでは、サーバ機器及び各種端末の設置セグメントを柔軟に変更することが可能です。共同利用に伴い、LGWAN 等のセキュリティが確保されたネットワークを介して、各サーバが異なるドメインに存在するような環境にも対応しています。

ネットワーク構成の検討に際しては、各市町村のセキュリティポリシーに従い、設計を行ってください。