

福津市マイナンバーカード交付予約・管理システムサービス業務仕様書

1 業務名

福津市マイナンバーカード交付予約・管理システムサービス業務

2 目的

マイナンバーカードを円滑に交付、管理するために以下のシステムを稼働させる。

1. 窓口の混雑を緩和することを目的に、市民が来庁日時を予約し、交付通知ができるシステムを導入する。
2. カードの交付・更新の情報を効率的かつ正確に管理することを目的に、簡単に検索及び記録できるシステムを導入する。

3 業務期間

(1) 履行期間 契約締結日の翌日から令和 10 年 3 月 31 日

(2) 使用期間 令和 7 年 8 月 1 日から令和 10 年 3 月 31 日

使用期間の 2 週間前までに本番と同じ試験環境を提供すること。ただし、これにより難しい場合には、双方協議の上で 1 週間前を限度として変更することができる。

4 基本要件

- (1) 本システムは、LGWAN-ASP(アプリケーション及びコンテンツサービス)及びクラウド方式によるサービス提供を前提とすること。
- (2) 情報セキュリティ対策を行うこと。
- (3) 以下の方法での予約が可能であること。
 - ①市民がインターネットを用いて通知はがきに記載されている番号や誕生日(月・日)等を入力し申請する。
 - ②コールセンターからインターネットを用いて予約する。
 - ③職員が LGWAN 回線を用いて予約する。
- (4) 職員が氏名や住所、マイナンバーカードの進捗状況等の個人情報を参照するときは、LGWAN 回線で行うことができるようにすること。
- (5) 予約及び管理するシステムの設定は本サービスを提供する SE 作業として実施すること。
- (6) 新しい OS(オペレーティングシステム)バージョン、スマートフォン等の新機種が市場に出てきた場合も対応可能であること。
- (7) 管理システムへのデータ入力方法は、QR コードの読み込み、CSV の取り込み、手入力に対応していること。
- (8) データインポート(CSV 等)・エクスポート(CSV 等)ができる機能を有していること。
- (9) 職員側環境として LGWAN への接続可能な回線敷設及び本サービスに接続可能な端末、

QRコード読み取り用のリーダーは当市にて用意することとする。

5 動作環境

動作環境は以下とします。

(1) 職員側、コールセンター側利用環境

- ・パソコン端末

OS: Windows 10,11

ブラウザ: Safari、Firefox、Google Chrome、Edge

- ・スマートフォン、タブレット端末

OS: iOS 10 以上、Android 8.0 以上

ブラウザ: Safari、Firefox、Google Chrome、Edge

(2) 利用者側動作環境

- ・パソコン端末

OS: Windows 10,11

ブラウザ: Safari、Firefox、Google Chrome、Edge

- ・スマートフォン、タブレット端末

OS: iOS 10 以上、Android 8.0 以上

ブラウザ: Safari、Firefox、Google Chrome、Edge

6 サービス提供時間

本サービスは原則として 24 時間 365 日の稼働とし、定期メンテナンスによるサービス停止はしないこととする。

ただし、システムメンテナンス等による停止は、30 日以上前に当市へアナウンスすることを前提に実施してもよい。

7 機能仕様

本サービスが提供するシステム機能は以下の通りとする。

7-1 利用者側機能

市民向けインターネット予約サイトは、専用アプリケーションのダウンロードを必要とせず、幅広い年齢層が操作することを前提に、ウェブアクセシビリティ（JIS 規格）の「A，AA」以上を取得し、簡便な操作性とすること。また、各種確認メールについてはシステムからの自動配信とし、配信用アドレスは事業者が用意すること。

(1) お知らせ機能

- ・自治体から市民へのお知らせ情報を表示できること。

(2) ヘルプ・FAQ

- ・ヘルプ画面、FAQ 画面に遷移するリンクが表示されていること。

(3) 来庁予約

- ・交付来庁の予約時には、通知はがきに記載されている番号と誕生日(月・日)でカードの正当性を確認できること。
- ・申請来庁の予約時には、新規発行・カード更新、再発行等の予約内容を選択できること。
- ・予約登録画面へ表示する窓口は表示・非表示の設定が行えること。
- ・予約登録画面から、簡易に予約が行えること。
- ・必要事項を入力した後、登録内容のエラーチェックを行い、エラーがなければ予約確認画面が表示されること。エラーの場合は、エラーメッセージを登録画面上に表示すること。
- ・予約登録時に受付番号とパスワードを発行し、それらの情報で予約照会が行えること。
- ・受付番号とパスワードを記載したメールを自動送信すること。
- ・予約登録時には、利用者本人以外にも複数人の予約を一括で行えること。
- ・複数人予約の場合、通知はがきに記載されている番号と誕生日(月・日)で全員分のカードの正当性を確認できること。
- ・電子証明書の更新手続きの予約が可能であること。

(4) 予約照会

- ・予約登録時に発行された、受付番号とパスワードにより、予約内容の詳細を確認できること。
- ・詳細画面には、処理状況や処理履歴も表示されること。
- ・詳細画面の内容を印刷できること。
- ・利用者が予約内容を削除することなく、詳細画面に配置された変更ボタンから予約内容を変更できること。変更した場合は、変更内容を記載したメールが自動送信されること。
- ・詳細画面に配置された取消ボタンから予約内容を削除できること。削除した場合は、削除した旨を記載したメールが自動送信されること。

(5) リマインダーメール受信

- ・予約者には、システム管理で設定したタイミングで、予約確認メールを自動送信できること。

7-2 職員側機能

画面上に市のシンボルマーク及びサービス名称を配置でき、簡便な操作・視認性が確保できていること。

(1) 交付リスト取り込み

- ・J-LIS から送付された交付対象者一覧の QR コードを読み取り、画面に表示するとともに、予約情報及びカード管理情報の基礎情報として管理できること。
- ・QR コードの重複読み込み時はエラーとなること。
- ・取り込み時には、交付窓口、発送番号を設定しカード情報に付加して管理できること。また、製造番号も開始番号を入力することで取込対象件数分の番号を自動採番して管理できること。

(2) 各種リスト取り込み

- ・本市が J-LIS のシステム等から CSV 形式で作成した更新対象者リストを取り込めること。
それにより QR コードからの交付情報と突き合わせて更新対象者等の状態を管理できること。

(3) 交付情報検索・一覧表示

- ・「製造管理番号」や「氏名」、「予約日時」などの条件で交付情報を検索し、該当する情報を一覧表示できること。
- ・一覧表示画面では、受付番号、窓口、予約日時、処理状況等での昇順・降順での並び替えができること。
- ・検索結果を全件一括 CSV 形式で出力できること。また、一覧表として EXCEL 形式で保存できること。

(4) 交付情報管理

- ・一覧表示された情報を選択し、照会、変更、削除、進捗情報登録ができること。
- ・対象交付情報に対して、交付完了日時、窓口及び申し送り事項を登録できること。
- ・対象交付情報に対して、予約日、交付窓口の変更ができること。予約情報を変更した場合は、履歴情報として管理され、変更前情報の照会ができること。
- ・対象交付情報に対して、カード発送日及び申し送り事項を登録できること。
- ・対象交付情報に対して、カード返戻日及び申し送り事項を登録できること。
- ・対象交付情報に対して、通知書返戻及び申し送り事項を登録できること。
- ・対象交付情報に対して、催告発送日及び申し送り事項を登録できること。
- ・対象交付情報に対して、カード廃棄日及び申し送り事項を登録できること。
- ・対象交付情報に対して、カード紛失日及び申し送り事項を登録できること。
- ・対象交付情報に対して、個別管理対象移行日及び申し送り事項を登録できること。
- ・対象交付情報に対して、再発行か否かを設定できること。

(5) 一括処理

- ・検索結果一覧画面から、対象を選択して「通知書送付日」「カード発送日」「交付日」の一括更新ができること。

(6) 電話予約登録(コールセンターを設置する場合、コールセンターでの利用も可能なこと)

- ・交付来庁の予約時には、通知はがきに記載されている製造管理番号でカードの正当性を確認できること。
- ・電話予約の場合は、全ての予約種別で代理人有無の登録ができること。
- ・予約登録画面では、交付窓口の選択ができること。なお、表示される窓口は受取予約(交付時来庁)、申請予約(申請時来庁)、電子証明書更新予約のそれぞれの業務が可能な窓口のみ表示されること。
- ・管理者は、権限により、予約締切日が過ぎていても予約登録ができること。
- ・管理者は、権限により、予約枠を超える予約登録ができること。
- ・登録時には、申し送り事項を入力できること。
- ・登録済みの予約情報を検索し、変更、取消ができること。

(7) 担当者管理

- ・職員及び業務従事者に対して、担当者 ID を付与し、担当者名、パスワード等を設定できること。
- ・担当者ごとに利用権限を設定できること。
- ・CSV 形式で担当者一覧情報を取り出せること。
- ・CSV 形式のデータを取り込み、一括登録、一括変更、一括削除ができること。

(8) マスタ管理

- ・交付対象の窓口情報を管理できること。
- ・窓口ごとに、交付用・申請用などの対象となる業務、基準となる交付可能な曜日や時間帯、処理単位の所要時間、予約可能件数が設定できること。
- ・窓口ごとに、有効開始日時、終了日時を設定でき、対象外の日時は予約できないこと。
- ・窓口ごとに設定されている曜日、時間、可能件数をもとに、1 年分の予約可能枠を一括設定できること。一括設定した後は、個別に枠数を変更できること。
- ・窓口は 10 か所以上の登録が可能であること。
- ・窓口ごとに予約期限の設定が行えること。予約締切日が土日祝日にあたる場合は、その前日を予約期限として設定できること。
- ・窓口ごとに予約画面への表示・非表示の設定が行えること。

(9) システム管理

- ・システム全般の初期値や諸元値(セッションタイムアウト、メール文面、画面ヘッダーロゴ、パスワード設定ルールなど)の設定ができること。
- ・受付番号の設定ルールや、何日前まで予約可能かを設定する日数を保持できること。
- ・担当者に付与する権限として、どのメニューを使用できるかの権限ルールを設定できること。
- ・予約者へのお知らせ情報を設定できること。公開開始日、終了日の設定ができ、市民側の画面には自動的に表示が制御できること。
- ・職員側、及び業務従事者側の操作ログ情報を閲覧できること。
- ・職員側、及び業務従事者側の機能を利用する前に、ID、パスワードによる認証を行い、権限に応じたメニューのみ表示されること。
- ・ログイン後は任意のタイミングでログアウトできること。また一定時間無操作の場合は自動的にログアウトされること。
- ・ログインしている担当者は自身のパスワードを変更できること。

(10) データ取り込み・出力(カード管理)

- ・本市が保有するカード管理簿(Access)データをシステムに取り込めること(受託事業者においてレイアウトを指定し、本市職員において変換する)。
- ・システム導入時に本市職員が行う、現行のカード管理簿(Access)から移行するデータの作成及びセットアップ作業のサポートを行うこと。
- ・必要に応じて CSV 形式でカード管理に関する全てのデータを出力できること。

8 情報セキュリティ対策

(1) 運用にかかわるセキュリティ対策

- ①行政事務処理作業における必要な情報のみを公開し、特に設定ファイルや個人情報を含む機密情報を格納したファイルを公開しないこと。
- ②必要最低限なアクセスのみ許可するよう、適切なアクセス制御を実施していること。
- ③担当者操作ログは、担当者 ID、操作日時、操作内容について、管理者の求めに応じて、出力・提出できること。

(2) ソフトウェアセキュリティ対策

- ①WEB アプリケーションに想定される攻撃手法(Dos や SQL インジェクション)への対策を講じていること。
- ②WEB アプリケーションを構成するソフトウェア(フレームワークなど)の脆弱性の収集に努め、脆弱性が公開された際には、システムへの影響を検証し、可能な限りセキュリティ対策を実施すること。
- ③第三者による不正使用・改竄等を未然に防ぐ対策を講じていること。

(3) ネットワークセキュリティ対策

- ①ルーターやファイアウォールにより、不要な通信を遮断していること。また、開放しているポート番号を把握し、不必要なポートを閉塞していること。
- ②必要に応じて、ネットワークセキュリティ機器を導入していること。
- ③侵入防止／侵入検知対策を行っていること。

- ・IDS(Intrusion Detection System)不正侵入検知装置
- ・IPS(Intrusion Prevention System)不正侵入防止装置
- ・WAF(Web Application Firewall)不正侵入防止装置

- ④ウィルス対策を行っていること。

WEB サーバと内部処理を行っているサーバのそれぞれ別のアンチウィルスソフトを用いて、2重の対策を実施していること。

- ⑤通信ログ管理を行っていること。

ファイアウォールなどのネットワーク機器の通信ログを記録し、不正アクセスや攻撃の兆候が見られる場合には、速やかに必要な対策を講じること。

9 システムのセキュリティ対策

(1) ガイドライン

下記のガイドラインの最新版の要件を満たしていること。また委託期間中に版が更新された場合は速やかに対応すること

- ①「クラウドサービス提供における情報セキュリティ対策ガイドライン（第3版）」
- ②「安全なウェブサイトの作り方」改訂第7版 独立行政法人情報処理推進機構セキュリティセンター(IPA)

③「TCP/IP に係る既知の脆弱性に関する調査報告書」改訂第5版 独立行政法人情報処理推進機構セキュリティセンター(IPA)

(2) 脆弱性の対策

- ①毎日、脆弱性対策情報データベース(JVNIpedia)サイトを確認し、必要に応じて速やかに対策を講じること。
- ②内閣官房情報セキュリティセンター(NISC)からセキュリティに関する情報提供があった場合、内容を確認し、必要な対策を速やかに講じること。
- ③セキュリティ専門会社によるセキュリティ診断を定期的実施すること。
- ④利用者側のインターネット回線は、安全性の高いEV-SSL 証明書を取得し、https 通信で通信経路を暗号化すること。

10 障害対策

(1) 冗長化

システム及びネットワークはすべて冗長化し、片方の機器に障害が発生してももう片方の機器で縮退運転を継続できる方式とし、サービス停止に至らない対策を講じること。

(2) バックアップ

- ・定期的にデータの自動バックアップを行う仕組みを用意すること。サーバ障害時にも速やかに復旧できる対策を講じること。
- ・バックアップデータは最低 1 日前までの状態には復旧できるようにすること。

直近のバックアップから障害発生時までの受付情報についても、別途、一時的に保持することにより、データの消失を最小限にすることができること。

(3) 無停電電源装置

データベースが保存されるサーバなどの機器類には、無停電電源装置(UPS)を付加し、不慮の停電や落雷等に備えること。停電時には、自動的にシャットダウン処理を行い、データの消失等を未然に防ぐこと。

11 データセンタについて

- ・システムを設置するデータセンタは国内のデータセンタであること。また、日本データセンタ協会が制定する推奨基準項目をクリアした、最高レベルである“ティア4”のデータセンタに準拠していること。
- ・震度VI相当(50～100年に一度の大規模地震)に耐えうる構造となっていること。
- ・外壁、屋根は防水対策を行い開口部についても地盤面から嵩上げを行っていること。また、地域危険度や地震、火災、水害といった各種の災害対策を考慮し、優れた立地条件のもとで運用されていること。
- ・建築基準法に適合した耐火建築物であり、外壁の窓等の開口部についても防火措置を講じていること。ハロン消火設備、自動火災報知設備、延焼防止対策(排煙設備防火区画整備)、高感度煙感知システムを設置し、館内の諸設備の集中監視を実施していること。

と。

12 保守・サポートについて

(1) 障害発生時の保守受付窓口

障害発生時の保守受付窓口を設けること。24 時間 365 日の障害対応を必要とし、迅速な復旧に努めるものとする。

(2) 障害発生時等の対応

障害発生時の対応を迅速に行なうため、リモートアクセスによる保守作業を行なえるものとする。リモートアクセスにより解決できない場合は、オンサイト保守を実施する。

ヘルプデスク

担当部署からの電話・メール・FAX 等での、システム操作に関する問合せや質問に対し、ヘルプデスクを設け、迅速な対応が取れること。なお、問い合わせ受付時間は、平日 9 時から 17 時とし、祝日及び年末年始 12 月 29 日～1 月 3 日は対象外とする。

(3) 報告体制の整備

- ・インターネット回線を用いて、運用状況や障害発生時の復旧状況を確認できる仕組みを有すること。
- ・緊急時にリアルタイムに電話やメールにて指定された緊急連絡先に一斉に緊急連絡を通知する仕組みを有すること。

(4) 定期保守運用

- ・保守運用作業にともなう停止（定期的かつ計画された停止を除く）を行うことなく、24時間 365日サービスを利用できること。
- ・サービスを停止することなく新機能のリリース、定期バックアップを行うことができること。

(5) 運用監視/セキュリティ監視

- ・セキュリティが確保された監視場所で、24時間365日専門の監視要員が運用監視、セキュリティ監視を行うこと。
- ・運用監視ソフトによりサーバ機器、ネットワーク機器、時刻同期等について障害監視、パフォーマンス監視、リソースの監視を行うこと。異常が発生した場合は、保守担当者に即時通知されること。緊急度の高いレベルの障害発生時はオペレータによる緊急連絡を行うこと。

13 事業者要件

- ・プライバシーマーク及び、情報セキュリティマネジメントシステム (ISMS) 適合性評価制度における認証を取得していること。
- ・ISO27017 (クラウドサービスセキュリティ) の認証を取得していること。

以上