＜サービス仕様書＞

１．業務名

箕面市マイナンバーカード交付予約・管理サービス

本サービスの引渡しを受けた時からこの契約及び本サービス仕様書の定めに基づき、本サービスを使用することができる。

２．業務期間

本業務の利用期間は、令和 6 年 7 月 1 日から令和 9 年 3 月 31 日までとする。

なお、令和 6 年 6 月 1 日から令和 6 年 6 月 30 日まではサービスの構築、テスト運用、操作研修等の準備期間とする。

３．テスト環境

テスト運用にあたっては、本番環境と同じテスト環境を用意すること。なお、テスト環境は本番環境の利用開始後も継続して使用できること。

４．サービス提供時間

本サービスは原則として 24 時間 365 日の稼働とする。

ただし、システムメンテナンス等による計画停止は、30 日以上前に当市へ連絡することを前提に実施することとする。なお、定期的な計画停止は実施しないこととする。

５．基本要件

（１）本サービスは、LGWAN-ASP 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）職員側環境として、LGWAN へ接続可能な回線及び本サービスに接続可能な端末、QR コードリーダは当市にて用意するものとする。

（３）新しい OS のバージョン、新しいブラウザのバージョンやスマートフォンなどの新機種が市場に出てきた場合も対応可能であること。

６．機能

別添「機能一覧」のとおり。

７．情報セキュリティ対策

（１）運用に係る情報セキュリティ対策

①行政事務処理作業における必要な情報のみを公開し、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必要最低限のアクセスのみ許可するよう、適切にアクセス制御を実施していること。

③ユーザ ID・操作日時・操作内容についての操作ログを、求めに応じて出力及び提出できること。

（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）の脆弱性の収集に務め、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第三者による不正利用・改ざん等を未然に防ぐ対策を講じていること。

（３）ネットワークのセキュリティ対策

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。

④WEB サーバと内部処理サーバにそれぞれ別のアンチウイルスソフトを用いて 2 重のウイルス対策を行っていること。

⑤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。

（４）システムのセキュリティ対策

①以下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、契約期間中に版が更新された場合は速やかに対応すること。

・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）

・安全なウェブサイトの作り方
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）

・TCP/IP に係る既知の脆弱性に関する調査報告書　最新版
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脆弱性対策情報データベースサイトを日次で確認し、必要に応じて速やかに対策を講じること。

③内閣官房情報セキュリティセンター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。

④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に実施すること。

⑤予約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。

８．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

①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。

②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。また、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、データの消失を最低限にすることができること。

③二重化されたデータベースをさらにもう一つ複製データベースとして設置し、最新のデータベース更新データを常に二重化されたデータベースと複製データベースに反映することにより、二重化されたデータベースに障害が発生した場合は複製データベースから障害発生時点に復旧できること。

（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。

９．データセンター

（１）システムを設置するデータセンターは国内のデータセンターであること。

（２）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（ティア４）のデータセンターに準拠していること。

（３）震度Ⅵ相当に耐えうる構造となっていること。

（４）外壁、屋根や防水対策を行い、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。

（５）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。

（６）電力会社から特別高圧受電により安定供給された受電設備を有すること。

（７）７２時間相当の燃料をデータセンター内で蓄積し、長時間運転が可能な設備であること。

（８）通信ケーブル専用の地下トンネルなど、インフラダウンを回避する設備を有すること。

１０．保守・運用サポート

（１）障害発生時の保守受付窓口を設けること。障害発生時には、24 時間 365 日の障害対応を行い、迅速な復旧に努めること。

（２）当市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い合わせや質問に対し、ヘルプデスクを設け、迅速な対応が取れること。なお、問い合わせ受付は、平日（祝祭日及び年末年始 12 月 29 日～1 月 3 日以外）の 9 時から 17 時とする。
（３）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。
（４）緊急時には、指定された緊急連絡先に一斉に緊急連絡を送信する仕組みを有すること。
（５）保守運用作業に伴う停止（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。また、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。
（６）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。

１１．事業者の要件
（１）プライバシーマーク、ISO9001（品質マネジメントシステム）、情報セキュリティマネージメントシステム適合性評価制度（ISMS）における認証を取得していること。
（２）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。

１２．再委託
（１）業務の全部又は一部を第三者に委任し、又は請け負わせ（以下「再委託等」という。）ないこと。ただし、事前に以下の①から③の事項を書面で市に通知し、市の承認を得て再委託等を行う場合は、この限りではない。
①再委託等の受任者又は下請負人の名称
②再委託等の業務の内容
③その他市が必要とする事項
（２）指名停止措置を受けている者（ただし、民事再生法（平成 11 年法律第 225 号）の規定による再生手続開始の申立て又は会社更生法（平成 14 年法律第 154 号）の規定による更生手続開始の申立てをしたことにより指名停止の措置を受けたものを除く）若しくは指名除外の措置を受けている者又は第 24 条第２項第 12 号に該当する者を再委託等の受任者又は下請負人としないこと。
（３）業務上知り得た個人情報の保護及び業務上使用したデータの適正な取扱いその他当該第三者が遵守すべき事項として市が定めた内容を記載した誓約書を、当該第三者のすべての者に提出させること。

－　以上　－