自治体窓口 DXSaaS
要件定義書

令和Ｘ年ＸＸ月

第Ｘ.Ｘ版

目次

1. 概要
1.1. サービスの範囲

2. 機能要件
2.1. 業務機能・帳票要件
2.1.1. 業務の一覧
2.1.2. 要求機能
2.1.3. 使用性・操作性要件
2.2. 情報システム間連携要件
2.2.1. 各業務システム→本システムとの連携
2.2.2. マイナポータルとの連携

3. 非機能要件
3.1. 前提条件
総務省とデジタル庁で公開している「地方公共団体情報システム非機能要件の標準」をベースとする。

3.1.1. システム稼働時間
各自治体の窓口開庁時間は稼働していること。

3.1.2. システム利用者

3.1.3. システム利用環境

3.2. ネットワーク要件
ガバメントクラウド接続サービスを経由で接続を想定してるが、それ以外の接続方法でも良い。

3.3. クラウドサービス要件
ガバメントクラウドの CSP のうち、どこに構築するかは指定しない。

3.4. ユーザービリティ及びアクセシビリティ要件

3.5. 性能・拡張性事項

要素	要件
オンライン応答時間	3 秒以内とすること。なお、自治体のネットワークの影響については除外とする。
バッチ処理	オンライン業務開始前までに、すべてのバッチ処理が終了できるように、構築すること。

要素	要件
チューニング	データ量、利用者の増加に対して、システムパフォーマンスが劣化しないように、適宜チューニングが行えるように構築すること。
キャパシティ	同時接続数、負荷に応じてスケールすること。

3.6. 可用性要件

要素	要件
サービス提供時間	24/365(計画停止除く)
サービス稼働率	年間のシステム稼働率は 99.9%を目標とすること
RPO（目標復旧地点）	平常時、営業停止を伴う障害が発生した際には、障害発生地点（日次バックアップ＋アーカイブからの復旧）までのデータ復旧を目的とすること。
冗長化	サーバ単一障害等でも業務が継続可能なように、複数の地域を跨いで設置すること。 複数のサーバに対して負荷分散を行うこと。 DB サーバを有する場合は、サーバ障害等でも業務が継続可能なように構成すること。
計画停止予定通知	事前通知を７日前まで行うこと。

3.7. 完全性要件

要素	要件
バックアップ方法	システムへの負荷を考慮し、最適となるようにバックアップの方法及び頻度が設定されていること。その際に、バックアップ処理によりシステムの性能要件を損なうことのないようなシステムを構築すること。
バックアップ対象	トランザクションデータ、マスタデータ、システム・ソフトウェア設定情報等、システムのリカバリに必要な各データのバックアップが取得できる機能を設けること。
バックアップ 保管期間	バックアップデータは業務上の必要性を考慮した保管期間で保存できるように構築すること。
復元	各バックアップデータ、ジャーナル等により、障害直前のデータを復元できるように構築すること。
監視	監視対象の設定や、異常状態の定義等、監視が実施できるように構築すること。（具体的な対象の設定や、異常状態の定義は受託後に本市と決定すること）
障害発生通知	30 分以内
復旧回復時間	12 時間以内

3.8. 上位互換性要件

3.9. 中立性要件

3.10. 情報セキュリティ要件

要素	要件
個人情報保護・データ保護	保有するデータは、各自治体の個人情報保護条例の対象であり、物理的セキュリティ、技術的セキュリティ、人的セキュリティにおいて万全の対策を講じること。
機密性の確保	サービス環境内外からの不正な接続及び侵入、行政情報資産の漏えい、改ざん、消去、破壊、不正利用等を防止するための対策を講じること。
利用者の認証	ID/パスワード等により利用者の識別を行う機能を設けること。 システムへのアクセス制御を行う機能を設けること。 アクセスを許可されたユーザーに対しての権限管理を行う機能を設けること。
ログ	システムログ及びアプリケーションログを取得し、取得したログの漏えい、改ざん、消去、破壊等を防止できる機能を設けること。 なお、ログの収集・一元管理・一定期間中の保存が可能であり、GUIツールで検索・統計分析・編集・プリント出力等を可能とする最低限の監査系機能を設けること。 現段階で想定している監査系機能は以下の通りである。 ・システム利用監査証跡（データ更新時／データ参照時） ・印刷監査（帳票印刷時、画面ハードコピー取得時） ・出力監査（サーバから端末へのファイルのダウンロードやサーバ間のファイルのファイル転送時）
暗号化	通信及び蓄積データに対して全て暗号化を行う機能を設けること。
ウィルス対策	以下の不正プログラム対策を講じること。 ・定時スキャン設定のみならず、個別ファイルをアクセスする都度スキャンが可能な機能を設けること。 ・データ送受信時にウィルスチェックが可能な機能を有すること。 ・最新のエンジン及びパターンファイルの自動更新が可能な機能を有すること。 ・常時監視機能の設定が可能であること。 ・各機器へのエンジン及びパターンファイルの配布状況管理機能を有すること。 ・ウィルス感染・検疫・駆除の一元監視機能を有すること。 ・検知時のアクションとして、システム管理者に対する通報と、ユーザーに対する通知が可能な機能を有すること。

要素	要件
設計	サーバから端末に攻撃の糸口になり得る情報を送信しないように情報システムを構築すること。
セキュリティパッチ	・適用にあたっては、本システムへの影響や、適用しても問題がないか確認した上で速やかに適用すること