【別紙４】非機能要件一覧

項番	内容
（１）ユーザーインターフェース	
1-1	窓口支援システムを利用する既存クライアント端末は、追加ライセンス費用無しで増設できること。
1-2	入力画面において、選択可能な項目については、チェックボックス・プルダウン等を使用することで入力低減が図られていること。
1-3	入力画面において、IMEの切替を項目に合わせて自動で切り替えることで入力低減が図られていること。
1-4	通常の業務において、リクエストの99.9%以上を平均3秒以内に応答すること。 （ただし、複雑な検索や抽出処理を除く）
1-5	データ容量やユーザ数が増加しても処理速度が低下しないよう、十分なキャパシティを備えること。
1-6	バッチ処理はオンライン業務に影響を与えない仕組み又は時間帯で処理すること。
（２）セキュリティ	
2-1	クラウドサービスを利用する場合、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたサービス、またはガバメントクラウド（AWS等）を利用すること。
2-2	利用するクラウドサービスのデータセンターは、日本国内に立地されていること。 また、バックアップやデータの保管についても日本国内で行われること。
2-3	クラウド内はウイルス対策ソフトによるウイルス対策を行うこと。 また、パターンファイル公開後は可及的速やかに適用すること。
2-4	当該システムを構成するサーバ機器やサービス等については稼働監視を行い、障害発生時は速やかに本市へ通知すること。
2-5	本市マイナンバー利用事務系ネットワークとデータセンターの接続は、IP-VPNの構築等により、マイナンバー利用事務系ネットワークと同等のセキュリティを確保すること。 また、FW等で第三者からの不正接続を防止すること。
2-6	日次でシステムバックアップ及びデータバックアップを取得すること。
2-7	ユーザ単位でログ（参照・更新・削除・印刷等）を取得できること。 また、本市からの求めがあった場合は、保守運用の一環としてログを提供すること。
2-8	当該システムに関する保守運用を行う際のログを取得し保管すること。 また、本市からの求めがあった場合は、保守運用の一環としてログを提供すること。
2-9	各種ログは1年以上保存し、改ざんや消失に対する予防措置を講じること。
2-10	入力・表示された個人情報について、クライアント端末内にデータを残さないこと。
2-11	ISO/IEC 27001、ISO/IEC 27017のいずれかを取得していること。 また、プライバシーマーク等の認証取得状況を提示すること。
2-12	情報セキュリティ対策について、受託者従業員に対し研修を実施していること。
2-13	将来的に当該システムの契約が終了となった場合は、移行に向けて蓄積されたデータをcsv形式で出力できること。 また、受託者の責任でデータを破棄すること。