# 古平町・京極町 自治体クラウド導入事業
# サービス要件定義書

古平町・京極町自治体クラウド推進協議会

令和元年１２月

## 1. 本書の目的

古平町・京極町自治体クラウド導入事業 サービス要件定義書（以下、「本書」という。）は、古平町・京極町自治体クラウド推進協議会（以下、「甲」という。）に対して提供する自治体クラウドサービス（以下、「本サービス」という。）に関して、サービス提供事業者（以下「乙」という。）に要求する機能などの仕様の詳細を定めることを目的とする。

## 2. 業務・機能要件

本サービスにおいて提供する業務アプリケーションの業務・機能要件については、以下のとおりとする。

### 2.1. システム要件

（1）提供する業務アプリケーション（以下、「業務 AP」という。）の範囲については、別紙１「調達利用業務アプリケーション一覧」のとおりとする。
各業務 AP の処理内容については、別紙２「機能要件定義書」のとおりとする。

（2）甲への参加団体職員（以下「利用者」という。）側でシステムのデータ加工を可能とする EUC の機能等を備えること。具体的には以下の機能を提供可能であること。
・新システムで管理する全てのデータについて、利用者が任意の条件を設定して抽出し、Microsoft Excel 等による２次利用が容易な形式（CSV 形式等）に編集・変換できること。
・抽出条件・編集方法等は、反復利用や保存ができること。

（3）文字コードは、住民基本台帳ネットワークシステムで用いられる統一文字コードに対応すること。

（4）住民記録等で新たな外字文字の登録が必要となった場合は、町より字体を入手のうえ、必要な外字ファイルを作成しサーバ及び PC への登録まで実施すること。

（5）各サーバ及び端末にコンピュータウィルス対策ソフトウェアを導入し、遅滞なくコンピュータウィルスを発見し、迅速な駆除対策を行うこと。なお、ウィルス対策ソフト管理用サーバを参照することにより、パターンファイルの更新が行えること。

（6）国民健康保険市町村事務処理標準システムへ対応すること。

（7）新システムに求める機能要件書を別紙２「機能要件定義書」に示すが、代替案を含め７割以上は対応できること。

（8）SLA（Service Level Agreement）については、優先交渉権者の選定後、契約締結交渉時に甲の参加団体（以下「参加団体」という。）と協議の上、定めるものとする。
甲では、別紙７SLA 設定値に示すサービスレベル設定値（案）を想定しており、サービスレベルが満たされない場合は罰則を課すこともあると想定している。

また、SLA の考え方やサービスレベルについては企画提案書に記載すること。

### 2.2. パッケージソフトウェアの利用要件

各業務 AP の機能については、パッケージソフトウェアを活用したものであること。活用するパッケージソフトウェア製品は、国内の自治体（甲と同規模の自治体であることが望ましい）において利用実績があること。

利用に係るカスタマイズは、極力避けること。カスタマイズの内容は、パッケージソフトウェア製品のバージョンアップの際に無償サポートされる範囲とすること。

## 3. システム方式要件

### 3.1. システム全体構成要件

本サービスは、各職員の業務用端末により利用できるものであること。なお、クライアント端末の仕様は、「8.2 クライアントのソフトウェア要件（動作要件）」及び「9.2 クライアントのハードウェア要件（動作要件）」に示す。

### 3.2. 性能要件

#### 3.2.1. 前提条件

性能値を試算する際は、「4.1 データボリューム一覧」に示す現行データ件数を参考にすること。

#### 3.2.2. オンライン処理性能要件

オンライン処理の性能要件については、図表 3-1 のとおりとする。なお、各指標の保証事項については、甲乙協議のうえ、別途「古平町・京極町 自治体クラウド導入事業　サービスレベル合意書」（以下、「SLA」という。）として締結する。

図表 3-1 オンライン処理の性能要件

| 指標 | 目標値 | 備考 |
|---|---|---|
| オンライン応答時間 | 3 秒以下 | 甲の職員等の端末からデータセンター間のネットワークの負荷による影響は含めない。 |
| オンラインバッチ処理時間 | 30 分以内 | 左記の時間内で終了しない処理については、バッチ処理時間帯で実行すること。 |

#### 3.2.3. バッチ処理性能要件

本書において、バッチ処理性能要件としての具体的な指標及び数値は掲げないが、バッチ処理の遅延が、後続の処理（翌日のオンラインサービスなど）に影響を与えないような性能及び運用とすること。

4. データ要件

4.1. データボリューム一覧

設定対象データを別紙３「移行対象範囲データ一覧」に示す。本サービスの性能値の試算やデータ移行の計画の際に参考とすること。

5. ユーザインターフェース要件

5.1. 帳票一覧表

業務で使用する出力帳票については、別紙４「標準帳票一覧」から選択し、使用することとする。なお、パッケージシステムで標準搭載される帳票を基準として表示する項目が充足すればよい。

5.2. その他

その他、以下の点に考慮された画面及び帳票を提供すること。

① データの表示と入力に一貫性をもたせること。
② 利用者が効果的に情報を得ることができること。
③ 利用者が再入力や記憶する情報量を極小化すること（画面が遷移する時、必要な情報は引き継ぐなど)。
④ ユニバーサルデザインに配慮すること。

6. 外部インターフェース要件

6.1. 基本要件

本サービスの業務 AP と外部（庁内に設置しているシステム）の業務 AP 間の業務データ連携に関する基本的な要件については、以下のとおりとする。

番号法第９条第１項における別表に定められた事務及び番号法第９条第２項に基づき甲が条例で定める事務について、中間サーバ及び業務 AP 間で情報連携のための仕組みを提供すること。中間サーバとのデータ連携に関する基本的な要件については、①のとおりとする。なお、別紙５「外部システム間業務データ連携一覧」に定められた事務のうち、甲乙協議のうえ連携を実施しないこととする事務についてはこの限りではない。

また、番号に依らない業務 AP と外部（庁内に設置しているシステム）の業務 AP 間の業務データ連携に関する基本的な要件については、②のとおりとする。

① 中間サーバとのデータ連携方式

中間サーバとの連携方式には、オンラインで即時連携を行う「Webサービス連携」及び一括で非同期処理を行う「サーバ間XMLデータ連携」とすること。

Web サービス連携及びサーバ間 XML データ連携については、「情報提供ネットワークシ

ステム等の外部インターフェイス仕様書」（内閣官房）、「中間サーバ・ソフトウェアの外部インターフェイス仕様書」（総務省）等を参照すること。

② 業務 AP 間の業務データ連携方式

業務 AP 間の業務データ連携方式は、ファイル伝送またはメッセージ交換とすること。ただし、同一事業者内の業務 AP 間についてはこの限りでない。

メッセージ交換及びファイル伝送については、「自治体クラウド開発実証に係る標準仕様書（平成２２年度版）」（平成２３年３月 地方公共団体情報システム機構）（以下、「自治体クラウド標準仕様書」という。）の「4.5 業務データ連携」を参照すること。ただし、自治体クラウド標準仕様書の文中の「都道府県域 DC」を「本サービス」と読み替えること。

③ セキュア通信

業務 AP の業務データ連携の通信として通信時の認証と通信内容の秘匿化を考慮すること。仕様については、自治体クラウド標準仕様書の「4.5 業務データ連携 4.5.1.2 要件一覧（B）セキュア通信機能」のとおりとする。

④ ファイル伝送

庁内のシステムとのファイル伝送（ファイル送信、ファイル受信）が行えること。
仕様については、自治体クラウド標準仕様書の「4.5 業務データ連携 4.5.1.2 要件一覧（D）オフサイトのファイル伝送、（E）オフサイトへのアクセスが制限される場合のファイル送信のとおりとする。（ただし、（E）については、自治体クラウド標準仕様書の文中の「都道府県域 DC」を「本サービス」と読み替えること。）

⑤ 送受信ログの記録

業務データ連携時の送受信のログを記録すること。仕様については、自治体クラウド標準仕様書の「4.5 業務データ連携 4.5.1.2 要件一覧(G)送受信ログの記録」のとおりとする。

⑥ 連携データ形式の定義

交換するメッセージや伝送するファイルのデータ項目やコード内容を、業務 AP 間で共通化すること。なお、業務データの提供元の事業者が、提供先のシステム運用・保守事業者及び甲と協議のうえ、共通化を行うものとする。

共通化に際し、「地域情報プラットフォーム標準仕様書」（APPLIC-0002-2016）の「自治体業務アプリケーションユニット標準仕様」の「インターフェース仕様」、「項目セット辞書」、「コード辞書」及び本書の「14.データ移行（サービスの変更・終了時）要件」の「移行データ標準レイアウト」を参照し、データ項目やコード設計のリファレンス（辞書）として活用すること。

6.2. 詳細要件

本サービスと中間サーバを含む外部システム間で連携を行うデータについては、別紙５「外部システム間業務データ連携一覧」のとおりとする。

乙は、連携を実施するにあたり、特定個人情報ファイルについて個別の事務に紐づいていることに加え、特定個人情報の利用が事務単位であり業務 AP 単位ではないことを十分に理解し、甲が制定した情報連携のための条例内容と整合性をとること。

7. ネットワーク要件

乙は、セキュアなネットワークを介して本サービスを提供すること。

個人情報、個人番号及び特定個人情報（以下、「個人情報等」という。）及び機密情報を取り扱う情報システムと接続する外部ネットワーク（※1）についても、上記と同等のネットワークを使用すること。また、送受信される情報の暗号化を行うこと。

乙は、乙の施設内及び外部ネットワークについて、本書の各要件及び SLA を実現可能なネットワーク構成とすること。

参加団体の施設への接続におけるアクセス回線については、乙が整備する。なお、本サービスの利用及び「3.2 性能要件」の実現に必要な接続ルータ及びアクセス回線に関する要件を参加団体に提示すること。

（※１）参加団体の施設とその外部とを結ぶネットワークの総称で、参加団体が契約する通信回線は除く。

8. ソフトウェア要件

8.1. サーバ等のソフトウェア要件

本書の各要件及び SLA を実現可能なソフトウェアを利用すること。また、本書の各要件及び SLA を実現可能なソフトウェア保守を行うこと。

8.2. クライアントのソフトウェア要件（動作要件）

本サービスを利用する職員等の端末（クライアント）のソフトウェア仕様は、図表 8-1 のとおりである。

図表 8-1 クライアントのソフトウェア仕様

| 項　目 | 仕　様 | 備　考 |
|---|---|---|
| OS | Microsoft Windows10 Professional (64bit) | |
| Web ブラウザ | Microsoft InternetExplorer 11 | |
| OA ソフト | Microsoft Word 2016 以降<br>Microsoft Excel 2016 以降<br>Adobe Reader DC | |

9. ハードウェア要件

9.1. サーバ等のハードウェア要件

本書の各要件及びSLAを実現可能なハードウェアを利用し、保守を行うこと。

9.2. クライアントのハードウェア要件（動作要件）

本サービスを利用する職員等の端末（クライアント）のハードウェア仕様は、別紙「業務機器類調達仕様書」のとおりである。

10. 情報セキュリティ要件

10.1. 基本要件

乙は、本サービスを提供するにあたり、乙の規定する「情報セキュリティポリシー」及び「個人情報等の取り扱いに関する特記仕様書」を遵守すること。また、ISO/IEC 27017に準拠すること。

なお、本サービスの提供に必要な設備等の情報資産（※2）については、乙の管理責任のもとで構築・運用されるため、これらの情報資産は、「10.2 詳細要件」を踏まえ、乙の情報セキュリティポリシーに基づき、情報セキュリティ対策を計画・実施するものとする。

（※２）本サービスの構成要素（本サービスの提供に用いるハードウェア、ソフトウェア、通信機器・回線、建物等の固定資産）及び構成要素を介する情報

10.2. 詳細要件

10.2.1. 組織・運用

10.2.1.1. 情報セキュリティのための組織

① 内部組織

乙は、従業員（※3）に対する秘密保持又は守秘義務についての要求を明確にし、文書化すること。当該文書は、定期的又は本サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。

乙は、情報セキュリティ対策における具体的な実施基準や手順等を明確化し、文書化すること。当該文書は、定期的又は本サービスの提供に係る重大な変更が生じた場合（組織環境、業務環境、法的環境、技術的環境等）に見直しを行うこと。

② 外部組織（データセンタを含む）

外部組織（※4）が関わる業務プロセスにおける、情報資産に対するリスクを識別し、適切な対策を実施すること。

情報資産へのアクセスが可能となる外部組織との契約においては、想定される全てのアクセスについて、その範囲を規定すること。

（※3）乙に所属し、本サービスの提供に携わる者で経営陣を除く者。派遣社員、アルバイト等を含む。

（※4）乙からサービスの一部を委託された企業等、本サービスの提供にあたり契約関係のある組織の総称。

10.2.1.2. 連携事業者に関する管理

① 連携事業者から組み込むサービスの管理

連携事業者（※５）が提供するサービスについて、事業者間で合意された情報セキュリティ対策及びサービスレベルが、連携事業者によって確実に実施されることを担保すること。

連携事業者が提供するサービスの運用に関する報告及び記録を常に確認し、レビューすること。また、定期的に監査を実施すること。

（※5）自らのサービスに他のサービスを組み込むことにより、本サービスを提供する際に、他のサービスを提供する事業者。

10.2.1.3. 従業員に係る情報セキュリティ

① 雇用期間中

本サービスに係る従業員に対して、情報セキュリティポリシーに関する意識向上のための適切な教育・訓練を実施すること。

本サービスに係る従業員が、甲の情報セキュリティポリシーもしくは本サービス提供上の契約に違反した場合の対応手続きを備えること。

② 雇用の終了又は変更

本サービスに係る従業員の雇用が終了又は変更となった場合のアクセス権や情報資産等の扱いについて、実施すべき事項や手続き、確認項目等を明確にすること。

10.2.1.4. 法令等の遵守

個人情報等、機密情報、知的財産など、法令又は契約上適切な管理が求められている情報については、利用可否範囲（対象区画・施設、利用が許可される者等）の明示、認可手続きの制定、監視、警告等により、認可されていない目的のための情報システム及び情報処理施設の利用を行わせないこと。

10.2.1.5. ユーザサポートの責任

① 乙への責任

本サービスの提供に支障が生じた場合には、その原因が連携事業者に起因するものであったとしても、本仕様書に基づき、乙が、その責任において一元的にユーザサポートを実施すること。

10.2.2. 物理的・技術的対策

10.2.2.1. アプリケーション、プラットフォーム（※7)、サーバ・ストレージ（※8)、ネットワークに共通する情報セキュリティ対策

（※7）認証、決済等の付加的機能を提供する、本サービスで提供されるアプリケーションの基盤。

（※8）本サービスを提供する際に利用するアプリケーション等を搭載する機器及びアプリケーション上の情報を蓄積・保存するための装置の総称。なお、付随する OS 等の基盤ソフトウェア、蓄積されているデータ・ログ等の情報を含む。

10.2.2.2. アプリケーション、プラットフォーム、サーバ・ストレージ

① アプリケーション、プラットフォーム、サーバ・ストレージの運用・管理

ア 稼働率及び定期保守時間の規定

乙は、本サービスを利用者に提供する時間帯を定め、この時間帯における本サービスの稼働率を規定すること。なお、提供する時間帯については、「12.3 ①サービス提供時間」を満たすこと。また、稼働率に関する保証事項については、甲及び利用者での協議のうえ、別途 SLA として締結する。

アプリケーション、プラットフォーム、サーバ・ストレージについても、定期保守時間を規定すること。

イ 容量・能力の予測

乙は、本サービスの提供に用いるアプリケーション、プラットフォーム、サーバ・ストレージに対し、利用状況の予測に基づいて設計した容量・能力等の要求事項を記録した文書を作成し、保存すること。

ウ 利用状況等の記録

乙は、利用状況、例外処理及び情報セキュリティ事象の記録（ログ等）を取得し、記録（ログ等）の保存期間を明示すること。

利用者の利用状況の記録（ログ等）の保存期間は、3 ヶ月以上とする。

例外処理及び情報セキュリティ事象の記録（ログ等）の保存期間は、5 年以上とする。

② アプリケーション、プラットフォーム、サーバ・ストレージの情報セキュリティ対策

ア ウィルス等に対する対策

乙は、本サービスの提供に用いるプラットフォーム、サーバ・ストレージ（データ・プログラム、電子メール、データベース等）についてウィルス等に対する対策を講じること。

10.2.2.3. ネットワーク

10.2.2.3.1 外部ネットワーク　（※9）からの不正アクセス防止

① 権限の割当、使用の制限

乙は、本サービスの情報システム管理者及びネットワーク管理者の権限の割当及び使用を制限すること。

② ユーザ認証

乙は、利用者及び管理者（情報システム管理者、ネットワーク管理者等）等のアクセスを管理するための適切な認証方法、特定の場所及び装置からの接続を認証する方法等により、アクセス制御となりすまし対策を行うこと。

（※9）乙の情報処理施設とその外部とを結ぶネットワークの総称で、乙とLGWAN間、乙と連携事業者間、保守管理用回線等を指す。甲が契約する通信回線は除く。

10.2.2.3.2 外部ネットワークにおける情報セキュリティ対策

① 情報交換の実施基準・手順等の整備

乙は、外部ネットワークを利用した情報交換において、情報を盗聴、改ざん、誤った経路での通信、破壊等から保護するため、情報交換の実施基準・手順等を備えること。

② 通報

乙は、外部ネットワークの障害を監視し、障害を検知した場合は管理責任者に通報すること。

10.2.2.4. 建物、電源（空調等）

本サービスの提供に用いるサーバ・ストレージ、情報セキュリティ対策機器等の情報システムが設置されている建物（情報処理施設）については、日本データセンター協会規定のデータセンターファシリティスタンダードTier3以上であること。

情報処理施設の詳細について、別紙「データセンター要件確認書」の項目について充足しているか回答すること。

10.2.2.5. その他

10.2.2.5.1. 機密性・完全性を保持するための対策

① 電子データの原本性確保

乙は、電子データの原本性確保を行うこと。

② 個人情報等の取扱い

個人情報等は関連する法令に基づいて適切に取り扱うこと。

10.2.2.5.2. 乙の運用管理端末における情報セキュリティ対策

乙は、運用管理端末に、許可されていないプログラム等のインストールを行わせないこと。

従業員等が用いる運用管理端末の全てのファイルのウィルスチェックを行うこと。

乙は、技術的ぜい弱性に関する情報（OS、その他ソフトウェアのパッチ発行情報等）を定期的に収集し、必要に応じて、パッチによる更新を行うこと。

10.2.2.5.3. 媒体の保管と廃棄

① 媒体の保管管理

乙は、紙、磁気テープ、光メディア等の媒体の保管管理を適切に行うこと。

② 機器及び媒体の廃棄

乙は、機器及び媒体を正式な手順に基づいて廃棄すること。

## 11. 初期導入要件

### 11.1. 初期導入要件

#### 11.1.1. 初期導入実施計画の作成

乙は初期導入（設定のための要件定義・設計、カスタマイズに伴う設計・開発（改修）を含む）の実施体制と役割、詳細な作業内容、作業スケジュール、開発環境、導入方法、導入ツール等に関する初期導入実施計画を作成の上、初期導入を実施すること。

#### 11.1.2. 開発環境

業務 AP のカスタマイズ等に必要な開発環境は乙が整備すること。なお、開発環境の整備にかかる費用は、乙の負担とする。

#### 11.1.3. 導入方法

本サービスの利用開始期限や品質を適切に確保するため、本サービスの特性等に応じた導入手法及びプロジェクト管理手法に基づき初期設定を行うこと。

### 11.2. テスト要件

#### 11.2.1. テスト実施計画の作成

乙はテスト体制と役割、詳細な作業内容、作業スケジュール、テスト環境、テストツール、合否判定基準などに関するテスト実施計画を作成の上、テストを実施すること。

#### 11.2.2. テスト環境

単体テスト及び結合テストについては、開発環境においてテストを実施すること。

総合テストについては、開発環境及び検証環境又は本番環境において実施すること。

検証環境又は本番環境におけるテストは、開発環境におけるテスト終了後に行うこと。

受入テスト及び運用テストについては、検証環境又は本番環境において実施すること。

11.2.3. テスト方法

単体テスト、結合テスト、総合テスト、受入テスト及び運用テストにおけるテスト実施方法は図表 11-1 のとおりとする。なお、各テストについては、初期設定やカスタマイズの内容等に応じて、必要な範囲で実施すること。

各テストにおけるテスト項目については、乙が検討し、利用者の承認を受けること。

図表 11-1 テスト方法

| テスト工程 | 利用者の役割 | 甲の役割 | テスト内容 |
|---|---|---|---|
| 単体テスト | 監理 | 実施 | 作成（カスタマイズ）したプログラムを対象としたテストを行う。 |
| 結合テスト | 監理 | 実施 | 作成（カスタマイズ）したプログラムに係るプログラム間のテストを行う。 |
| 総合テスト | 監理 | 実施 | 初期設定に係るシステム機能全体のテスト（機能、性能、セキュリティ及び運用機能等）を行う。 |
| 受入テスト | 実施 | 支援 | 総合テストのテスト項目の一部を甲が実施する。 |
| 運用テスト | 支援 | 実施 | 運用・保守要領及び運用・保守実施計画等に基づき、運用が行えることを確認する。 |

11.2.4. テストデータ

現行システムのデータについては、機密度の高いデータ項目や個人情報等に係るデータ項目が含まれるため提供しない。乙は、本サービスのデータの特性を踏まえた擬似データを作成し、各テストに使用すること。

11.2.5. 受入テストの支援

乙は、甲と協議のうえ、受入テスト仕様書の作成支援を行うこと。

受入テストの実施支援（テストへの立会い、操作補助など）を行うこと。

受入テスト結果報告書の作成支援を行うこと。

11.3. システム移行要件

11.3.1. 移行実施計画の作成

乙は、移行実施体制と役割、詳細な作業内容、作業スケジュール、移行環境、移行方法、移行ツール等に関する移行実施計画を作成の上、システム移行を実施すること。

11.3.2. 移行方法

以下の作業を含め本サービスへの移行に必要な作業を実施すること。

① 利用者より、現行システムから抽出した移行データの提供を受ける。
② 移行データの調査（現行システムのファイル・データレイアウトの調査、外字利用の調査、不備データの調査など）を行うこと。
③ 移行データの整備（不備データの指摘、本サービスで追加されるデータ項目への値設定など）を行うこと。
④ 移行データに不足があった場合は、町村担当者、現行業者、受託者にて協議した上で対応方針を決定すること。
⑤ 移行リハーサル（移行データの検証、移行時間の測定など）の実施後、移行を行い、移行結果の検証を行うこと。
⑥ 移行データのうち２以上の業務システムにおいて、総務省から公開されている「中間標準レイアウト」を用いてデータ移行すること。（対象とする業務については、参加団体ごとに異なっていても構わない。）

11.3.3. 移行対象データ

移行対象のデータについては、以下のとおりとする。

① 現行システムで管理されているデータ全てとすること。
② 紙台帳等のシステム化されていない情報は、原則として、移行対象としないが、当該情報を移行する場合は、利用者がシステムへの入力を行う。

11.3.4. 稼動当初のサポート

稼動当初の最低１ヶ月間、オペレータもしくは操作についてのサポート要員を各団体１名以上配置すること。また、その際の体制や対応方法について提案すること。

11.4. 教育・研修要件

11.4.1. 教育・研修実施計画の作成

乙は、職員等及び運用要員等への教育・研修の実施体制と役割、作業内容、作業スケジュール、教育・研修環境、教育・研修方法などに関する教育・研修実施計画を作成の上、教育・研修を実施すること。

なお、乙の運用要員等への教育・研修は、乙の責任において本サービスの利用に支障がないように実施すること。

11.4.2. 教育・研修環境

乙は、教育・研修用のシステム環境を用意すること。なお、原則として、研修に必要な会議室及び機器（端末、プリンタなど）は甲及び利用者のものを利用する。

11.4.3. 教育・研修方法

乙の職員等への教育・研修の方法については、図表 11-2 のとおりとする。

図表 11-2 教育・研修方法

| 教育・研修の内容 | 対象者 | 方式 | 回数 |
|---|---|---|---|
| システム操作研修（業務 AP ごと） | 業務担当者 | 個別指導 | 1 回 |
| システム管理研修（業務 AP 共通） | システム管理担当者 | 集合研修 | 1 回 |

11.4.4. 教育・研修用教材の作成

「11.4.3 教育・研修方法」に示した研修に必要な操作マニュアル及び運用・保守要領などの資料の作成、必要部数のコピーなどを行うこと。

11.4.5. 教育・研修の実施報告

「11.4.3 教育・研修方法」に示した教育・研修の実施の完了報告を行うこと。

11.5. その他の作業要件

11.5.1. 作業場所

利用者との打合せ、受入テスト及び研修など利用者等が関わる作業については、原則として、甲の参加団体の施設（会議室など）で実施すること。

その他の初期導入のための作業については、原則として、参加団体の事業所内で実施すること。

11.5.2. 会議体

11.5.2.1. 定例報告会

原則として、月に 1 回、作業状況の報告会を実施すること。ただし、緊急を要する報告に関しては必要に応じて実施すること。

11.5.2.2. レビュー

初期導入の各工程において、乙の社内で適正なレビューを実施するとともに、必要に応じて、利用者のレビューを受けること。

11.5.2.3. 会議の進行、議事録の作成及び懸案事項などの管理

各会議の進行、議事録の作成及び懸案事項などの管理は乙が行うこと。

## 12. 運用・保守要件

### 12.1. 運用・保守要領の作成

乙は本サービスで行う運用・保守作業内容を記載した運用・保守要領を作成すること。

運用・保守要領として以下の内容を定義すること。

図表 12-1 運用・保守要領

| 要領 | 内　容 |
|---|---|
| 文書管理要領 | 本サービスの運用において作成及び入手した文書の管理方法について定める。 |
| 情報セキュリティ対策要領 | 個人情報保護法、番号法及び情報セキュリティポリシーなどに準拠して、必要な対策を定める。 |
| 進捗管理要領 | 運用・保守作業の進捗管理に必要な事項を定める。 |
| システム操作管理要領 | システム操作の管理に必要な事項（運用スケジュール、システム操作マニュアル、作業指示書等）を定める。 |
| サービス指標管理要領 | サービス指標の実績値の管理に必要な事項を定める。 |
| 性能管理要領 | 性能管理に必要な以下の事項を定める。<br>・CPU 等機器の負荷状況の監視方法<br>・ディスク等記憶媒体の空き容量、使用量の監視方法<br>・ハードウェア、ソフトウェア等の死活監視方法<br>・ネットワークの性能、死活監視方法<br>・電源、空調等設備の監視方法 等 |
| 保守要領 | 保守に必要な以下の事項を定める。<br>・保守スケジュール（ソフトウェアのバージョンアップ、ハードウェア定期保守等）<br>・保守対応時間帯（24 時間対応等）<br>・保守対象のソフトウェア及びハードウェア<br>・保守作業の内容（パッチ、部品交換等） 等 |
| 課題問題管理要領 | 本サービスの運用における課題・問題の管理に必要な事項（管理項目等）を定める。 |
| 変更管理要領 | ソフトウェア、仕様書、各種マニュアル等の変更に必要な事項を定める。 |
| 構成管理要領 | 本サービスの構成要素の定期的な棚卸手順等、構成管理に必要な事項を定める。 |
| データ管理要領 | データの授受、保存、バックアップ及び保管の方法及び手順を定める。 |
| 設備管理要領 | 情報システムを設置する建物、関連設備等の管理に必要な事項を定める |
| 障害対策要領 | 障害対策に必要な以下の事項を定める。<br>・損失分析、影響範囲<br>・復旧目標時間、復旧目標時点及び復旧優先順位<br>・障害対策計画 |
| 運用保守要領の改訂手順 | 運用・保守要領を変更する必要が生じた場合の手順を定める。 |

12.2. 運用・保守計画の作成

乙は、運用・保守実施体制と役割、詳細な作業内容、作業スケジュール、運用・保守環境、運用方法、運用ツール等に関する運用・保守実施計画を作成の上、運用・保守を実施すること。

12.3. 運用要件

乙が実施する運用業務の内容については、以下のとおりとする。

12.3.1 運用管理

① システムの本稼動前までに、運用計画書を作成し参加団体の了承を得ること。
② 運用計画書に基づいた運用管理を行い参加団体に対して毎月の定期報告及び随時の報告を行うこと。
③ 全参加団体共同での定期報告を行うこと。
④ 運用計画書の年度更新及び必要に応じた改定を行うこと。
⑤ 本事業全体の運用監視を行い、運用に不備あるときはこれを改善すること。
⑥ 参加団体にはソフトウェアを利用させるのみであること。物理サーバーあるいは仮想マシンそのものの操作権限を参加団体に付与することなく運用できること。

12.3.2. サービス提供時間

① オンラインサービス提供時間については、年末年始・祝日を除く月～金 8:30～18:00 とする。
② 土曜日、日曜日及び祝日についても、事前申請等をすることで、サービス提供を行うものとする。
③ システムの提供時間終了時にシステムが利用されている場合に終了待機などの排他制御が行えること。

12.3.3. 監視

① サーバ及びネットワーク機器の死活監視（随時）、性能監視（随時）、プロセス監視（随時）、ログ監視（随時）、セキュリティ監視（随時）、警告内容の確認（随時）、エスカレーション（随時）を行うこと。
② 電源、空調等設備の監視の警告内容の確認（随時）、エスカレーション（随時）を行うこと。
③ 各処理の異常状態を警告通知できること、通知の手法としてメールもしくはポップアップ機能を使用できること。メールは複数のメールアドレスを設定できること。
④ 稼動実績について、稼動統計を作成し定期報告を行うこと。

12.3.4. パフォーマンス

① 検索結果表示や帳票出力についてのレスポンスタイムは３秒以内、移動処理については１０秒以内とすること。処理に際しては、利用者にストレスを与えず業務に支障をきたさないレスポンスタイムを提供すること。

② 万一、品質・性能が満たされない事象が発生した場合は、速やかに参加団体へ報告し、速やかに問題の解決を行うこと。

12.3.5. バッチ処理

① バッチ処理の起動は自動化でき、業務システム単位で設定ができること。

② バッチ処理はマルチタスク処理で行えること。

③ 同時起動できない処理がある場合には利用者に適切に通知し必要な制御を行うこと。

④ バッチ処理の起動、終了を利用者にメッセージ通知すること。

12.3.6. バックアップ管理

① バックアップデータ保管場所については、サーバー機器専用室と同等以上のファシリティ要件を充足していること。

② バックアップデータの遠隔地保管場所、データ伝送を「企画提案書」に記載すること。

③ バックアップ（日次)、バックアップ確認及び実施結果の記録（日次)、記録媒体交換・保管（月次）を行うこと。

④ バックアップの管理世代数は、5 世代以上とし、必要なデータをリストアできる状態で維持管理が行われること。

12.3.7. セキュリティ管理

セキュリティ管理については、別表８「セキュリティ要求項目」の通りとする。

また、事業者は「企画提案書」においてセキュリティの対策について明記すること。

12.3.8. ログ管理

利用者の情報システム管理者によるログ参照ができること。

12.3.9. 障害対応

① 障害への対応方法を提案すること。

② 業務や住民 業務や住民 サービスに影響を与える障害発生時おいては、障害発生を 10 分以内に検知し、障害検知時から 10 分以内に障害が影響する参加団体へ通知すること。また、回復予定時間については、障害検知時から 90 分以内に障害が影響する参加団体へ通知すること。

③ 障害発生時等について以下時間内に対応すること。（大規模災害、停電時を除く）

ア 異動処理、証明書発行書等で住民の被る影響が大きい障害、印刷不良、操作方法不明等で窓口において直ぐに対応する必要があるのもの。[10 分以内]

イ データ不整合等で日次更新・データ連携に影響するもの。[2 時間以内（ただし、日次更新等処理までの時間が 2 時間に満たない場合は、日時更新等処理までの時間）]

ウ 上記に該当しないもので日次更新・データ連携に影響のしないもの。[当日中]
なお、業務主管課担当者と協議の上、翌日対応で問題がないと判断した場合はこの限りでない。

エ 操作方法についての問合せで上記以外のもの。[24 時間以内]

- リカバリポイントについては、アプリケーションまたはハードウェアが停止する直前までのデータを極力復旧し、データの検証を行うこと。障害発生後、停止に至るまでの間に行われた異動等に関して不整合等の問題が確認された場合は、乙の責任においてデータ入力を行い、利用者業務主管課担当者の承認を得ること。
- 想定の範囲内の災害により機器を破損しサービス停止に至った場合には乙の責任において迅速に代替データセンターを確保するなどしてサービスを再開すること。　また、データの復旧は乙が保証すること。なお、本仕様書で想定している範囲を超えた自然災害による損害については、甲・乙で協議の上、住民の不利益にならないようデータを復旧するものとする。

  また、乙及びその従業員または従業員の親族等の被災状況により必要な場合は、復旧に要する期間を参加団体と協議することができる。障害復旧後、乙は原因の分析と再発防止策を参加団体に報告すること。
- 乙は、事故または災害あるいは誤操作等により参加団体のシステム及びデータを損壊または消失させたときに、バックアップから復元・復旧させるために要する時間をベンチマークテスト等により把握し、ダウンタイム／アップタイム等を予め参加町村へ通知するものとする。

12.3.10. バージョンアップ等

① バージョンアップや法制度改正によるプログラムリリース、セキュリティパッチの適用や配布について、システムの運用に支障のないように実施できること。

② バージョンアップや法制度改正、セキュリティパッチの適用について、極力プログラム改修が発生しない仕組みが考慮されていること

12.3.11. 問い合わせ窓口

① 参加団体の各業務主管課から、システムに関する問い合わせを受け付ける窓口を設けること。

② 問い合わせ窓口は障害等の一次受付窓口を兼ねること。

③ 問い合わせ窓口は本庁業務稼働時間（8：30～18：00）は電話またはメール、FAXによる受付を行い、それ以外の時間帯においてもメールによる受付が行えること。

④ なお、選挙時の対応等特別な業務に対しては業務稼働時間外であっても柔軟に対応すること

12.3.12. 稼働当初のサポート

稼働当初は、最低1カ月間オペレータもしくは操作のサポート要員を利用者ごと1名以上配置すること。人数については各参加団体の状況に応じた対応をすること。また、その際の体制や対応方法について提案すること。

12.3.13. 運用時のサポート

① 安定稼働後においても、月1回以上参加団体を訪問し、運用状況やスケジュール、課題の改善方法等を確認すること。現地訪問する担当者の体制は乙が提案すること。

② 年次処理やそれに類するもの及び不定期に発生する処理（選挙・申告相談会場設営等）の実施時には現地に立ち合うこと。

③ 障害発生を検知した場合、問題の一次切り分けは乙が行うこと。なお、現地から各参加団体の担当者の確認作業により収集できる情報が、問題の切り分けに資すると判断される場合には、乙は、参加団体の担当者の協力を求めることができる。

12.4. 保守要件

乙が実施する運用業務の内容については、以下のとおりとする。

① アプリケーション保守

プログラム不具合調査・プログラム修正・動作確認（随時）を行うこと。

② ソフトウェア保守

本書の各要件を実現可能なソフトウェア保守を行うこと。

③ ハードウェア保守

本書の各要件を実現可能なハードウェア保守を行うこと。

12.5. 業務運用について

「12.3 運用要件」及び「12.4 保守要件」の業務以外の業務運用（業務に係るデータ入力、帳票出力等）については、本サービスに含めないものとする。

13. 運用施設・設備要件

13.1. 施設要件

乙のデータセンター等については、別紙「データセンター要件確認書」に概ね充足すること。

13.1.1. 立地条件

データセンター等は日本国内に存在すること。

可能な限り災害の影響を受けない場所に施設が存在すること。（過去に液状化被害を受けた地域でないこと。水害の恐れが少ないことが、市町村等のハザードマップ（国土交通省の公開する「洪水氾濫危険区域図」等）で確認できること。）

13.1.2. 建物条件

13.1.2.1. 耐震性

・建物は、震度 6 強までの地震に耐えられるものであること。建築基準法に基づいた免震又は耐震等の構造上の安全性を配慮した設計・施工が行われていること。

13.1.2.2. 火災予防

・建物は、揮発物等爆発の危険性が高いものを取り扱う施設から離れた火災の被害を受けるおそれの少ない場所に設置されていること。

13.1.2.3. 落雷被害予防

・建物は、落雷の被害を受けるおそれの少ない場所に設置されていること。
・雷サージ等による電気設備機器の破損を防止できるような構造になっていること。

13.1.2.4. 水害予防

・電気設備が収納されるエリア（機械室等）には、外部からの水の浸入を防止する措置が講じられていること。

13.2. 設備要件

13.2.1. 電源設備

13.1.2.1. 商用電源

① 電力会社より特別高圧ループ受電方式、もしくはマルチスポット方式等により複数系統で受電し、冗長化対策が講じられていること。

② 電源は、異なる変電所から 2 系統以上で受電していることが望ましい。

③ 受変電設備は、本サービスを停止せずに法定点検や工事等を行うことが可能であること。

13.1.2.2. 予備電源

① 停電時に本サービスを運用するために十分な容量を持つ非常用自家発電設備が設置され、修理・点検に備えること。電力会社での送電系統に障害が発生したことを想定し、予備電源として 24 時間以上の発電機用燃料を備蓄していること。

② 非常用自家発電設備の発電能力は本サービス機器の稼働に必要な電力を供給可能なこと。

③ 無給油で連続運転が可能な時間が経過した後も、優先的に燃料供給が受けられる契約を、燃料供給会社と結んでいること。

④ 非常用自家発電機の運転中であっても、安全に給油が可能な構造であること。

13.1.2.3. 空気調和設備

① 機械室及びデータ保管室の温度は 20℃から 26℃に適切に保たれていること。

② 機械室及びデータ保管室の湿度は 35%から 65%に適切に保たれていること。

③ 機械室及びデータ保管室の空気調和設備は、機械室及びデータ保管室ごとに冗長構成（N+1 以上）であること。

④ 空気調和設備用の電源回路は 2 系統化方式を採用していること。

⑤ 空気調和設備は、24 時間 365 日連続して稼動可能であること。

⑥ 空気調和設備は、電力会社からの電源供給が停止した場合でも、24 時間以上連続して運転が可能であること。

⑦ 空気調和設備の配管、ダクト類は、圧力の変動や火災による機器の損傷を防止するため耐圧性、耐火性に優れた材質を使用し、さらに不燃材で被覆されていること。

⑧ フィルタに使用する断熱材は不燃性とし、火災時の煙や有毒ガスから人命の保護を図るとともに、設備の損傷防止を考慮していること。

⑨ 空気調和設備が水冷式の場合は、漏水防止措置を講じるとともに、漏水のおそれがある場所には漏水感知機が設置されていること。

⑩ 空調設備が設置された室については、温度及び湿度並びに空調設備の作動状況の常時検知監視が行われていること。

13.2.3. 防火設備

① 建築基準法に規定する耐火建築物であること。

② 建築基準法に則った延焼防止対策が実施されていること。

③ 機械室及びデータ保管室に、消火設備としてコンピュータ設備に被害を与えないガス消火設備を有していること。

④ 機械室及びデータ保管室に、煙感知器設備が設けられており、火災の早期発見が可能なこと。

⑤ 運用要員が常駐する場所においては、運用要員の健康を損なわない消火設備（消火器等）が設置されていること。

13.2.4. 機械室及びデータ保管室

機械室及びデータ保管室は物理的に隔離された管理区域であり、地階以外であること。ただし 1 階の場合は地上高が 150㎝ 以上であること。セキュリティ上、外部からの識別侵入が容易にできないように無窓の外壁にする等の対策が施されていること。

電源ケーブルは、フロア内分電盤（PDF）からラックまで冗長化されていること。

13.2.5. ラック設備

① サーバが収容されるラックは、免震対策又は耐震対策が採られていること。

② 震度 6 強までの揺れに対応できること。

③ 施錠が可能なこと。

13.2.6. 防犯設備

13.2.6.1. 施設入退館管理

① 入退室管理と入退館管理は異なる管理体制であること。

② 施設への入退館管理は、24 時間 365 日警備員による入退者の監視・管理を実施していること。

③ 入館者の PC や電子記録媒体の持込、持出の管理が申請管理されていること。

④ 施設への入館においては、あらかじめ定められた申請者からの事前申請制とし、すべての入館者が明らかにされていること。

⑤ 施設の入り口から、機械室及びデータ保管室に至るまで、3 回以上の入室者の確認箇所が設けられ、不審者が容易に立ち入りできない対策が講じられていること。

⑥ 無許可車両が不用意に立ち入られぬよう管理されていること。

13.2.6.2. 機械室及びデータ保管室入退室管理

① 機械室及びデータ保管室の各出入口には入退室管理を行う設備を設置すること。

② 入退室の状況について常に入退室管理により把握できること。

③ 不要な機械室及びデータ保管室への入室ができないよう入室可能な機械室及びデータ保管室を制限できる入退室管理の仕組みを有すること。

④ 入退室の状況の管理は、以下の機能を有すること。

1. 個人識別機能（暗証番号、個人認証カード、生体認証等）
2. アクセス者、日時、鍵、アクセスの記録機能
3. 扉の自動施錠、解錠機能

⑤ 入退室が確認できる監視カメラが設置されていること。

⑥ 機械室及びデータ保管室等の扉・枠・錠は、耐火性の優れたもので十分な強度を有すること。

⑦ 機械室及びデータ保管室には、外部に直接面した窓、扉などは設置されていないこと。

13.2.6.3. ラック防犯設備

サーバラックの鍵は、施設により管理され、本人確認作業後に開錠及び施錠を実施すること。

13.2.6.4. 不正侵入監視

① 施設の主要な出入口は、赤外線センサーや監視カメラ等により常時監視し、不正な侵入の有無が 24 時間監視及び録画されていること。

② 監視カメラ用のモニター及び録画装置は、機械室及びデータ保管室以外のセキュリティ対策が施された場所に設置すること。

13.2.7. 運用要員室

運用要員室への入退については、IC カード等で室内への入退管理を実施していること。
機械室及びデータ保管室と同一建物又は隣接する建物内に設置されていること。

14. サービスの終了時の業務について

乙は、本業務の終了に際し、甲及び次期事業者となる者に対して業務の円滑な引継ぎに必要な作業を支援することとする。また本業務の契約終了に伴う撤去は、乙が実施し、それに係る費用は乙が負担すること。その際には原状回復を基本とし、データの消去及び消去済の証明書を提出すること。

なお、業務の引継ぎに係る具体的な内容については、甲・乙が協議の上、決定するものとする。

14.1. 契約終了時のデータ抽出費用

本業務の終了に際し、甲は乙には既存データの抽出を委託する。その際には総務省が示す「中間標準レイアウト仕様」に準じたレイアウトとすること。また、中間標準レイアウトの対象外の業務システムや定義されていない項目は、乙のレイアウトとすること。レイアウト説明書やコード表等を、データと共にに提出することとし、それに係る費用を想定して提案価格見積書に記載すること。この費用については価格点の採点対象とする。

前提条件

① 上記レイアウトにて、電子ファイル（CSV 等）形式で提出すること。
② 抽出を行うデータについては、システムの全データ、全項目を対象とする。
③ ファイルレイアウト表やコード表等のドキュメントも提出すること。
④ データ提供は２回とするが、データ移行スケジュールは概ね６カ月を想定し、データ及びドキュメントについての問い合わせの対応を行うこと。

14.2. 移行データの提供方法

乙は、移行データを、電子媒体（CD-R、DVD-R、USB メモリ等）により提供すること。

15. 秘密保持

本業務により知り得た情報（周知の情報を除く）は、システムの提案、契約、構築、運用の目的以外に使用せず、契約終了後においても機密として保持し、第三者に開示もしくは漏えいしてはならない。

以　上