

甲府市行政情報システム更改・運用業務 システム要件書（内部情報系）

令和8年10月
甲府市

目 次

1 共通編.....	1
1.1 業務範囲.....	1
1.2 権限（職務分掌、業務ロール、承認権限 等）.....	1
1.2.1 認証方式.....	1
1.2.2 認証ID／パスワード・権限範囲.....	2
1.2.3 利用者情報連携.....	2
1.2.4 権限管理.....	2
1.2.5 異動・退職時の対応.....	2
1.2.6 関連システムとの調整.....	2
1.2.7 ログ管理.....	2
1.2.8 セキュリティ対策.....	2
1.3 市の概要.....	2
2 連携要件.....	3
2.1 業務横断データ連携.....	3
2.1.1 連携対象一覧の整理.....	3
2.1.2 シングルサインオン.....	3
2.1.3 データを抽出及び提供.....	3
2.1.4 連携方式の整理.....	3
2.1.5 連携仕様の作成支援.....	3
2.1.6 責任分界の整理.....	3
2.1.7 関連システム事業者との調整支援.....	3
2.1.8 データ変換・コード変換.....	3
2.1.9 連携エラー対応.....	3
2.1.10 連携ログ・処理結果管理.....	3
2.1.11 連携テスト支援.....	4
2.1.12 本番移行時の連携確認.....	4
2.1.13 運用開始後の連携管理.....	4
2.1.14 セキュリティ・アクセス管理.....	4
2.2 共通機能連携.....	4
3 データ移行要件.....	5
3.1 データ移行要件.....	5
3.1.1 移行要件・移行対象.....	5
3.1.2 過年度データ移行.....	5
3.1.3 履歴保持.....	5
3.1.4 抽出・変換.....	5
3.2 EUC機能.....	5
3.2.1 既存事業者との連携.....	5
3.2.2 データ抽出.....	5

3.3 移行テスト	6
3.4 本番移行	6
3.4.1 本番移行手順	6
3.4.2 本番移行及びデータ移行	6
3.4.3 終了時・次期移行	6
4 共通機能要件	7
4.1 業務システムに関する共通機能	7
4.1.1 登録機能	7
4.1.2 職員向けガイダンス	7
4.1.3 入力支援	7
4.1.4 検索	7
4.1.5 マルチウィンドウ対応	7
4.1.6 金融機関マスタ	7
4.1.7 業者マスタ	7
4.1.8 バッチ状況確認	7
4.1.9 業務機能	8
4.1.10 データ保存	8
4.1.11 メモ機能	8
4.1.12 サービス仕様	8
4.1.13 データパンチ	8
4.1.14 発行機能	8
4.1.15 権限管理	8
5 非機能要件	10
5.1 セキュリティ要件	10
5.1.1 法令	10
5.1.2 セキュリティ対応	10
5.1.3 脆弱性に対する対応	10
5.1.4 特権 I D 管理	10
5.1.5 インシデント対応	10
5.1.6 再委託先管理	10
5.1.7 外部サービス管理	11
5.2 インフラ・クラウド要件	11
5.2.1 クラウド利用時の責任分界	11
5.2.2 I S M A P 等の確認	11
5.2.3 標準的な連携方式	11
5.2.4 設置要件	11
5.2.5 回線要件	11
5.2.6 災害要件	11
5.2.7 業務端末	11
5.3 性能・可用性	12

5.3.1 性能.....	12
5.3.2 稼働時間.....	12
5.3.3 計画停止時間.....	12
5.3.4 予定外停止時間.....	12
5.3.5 RTO/RPO.....	13
5.4 運用・サポート.....	13
5.4.1 サポート範囲・対象外.....	13
5.4.2 変更管理.....	13
5.5 監査・ログ管理・運用支援.....	13
5.6 事業継続・BCP・終了時データ移管.....	13
5.6.1 事業継続性.....	13
5.6.2 リストア確認.....	14
5.6.3 契約終了時データ移管.....	14
5.6.4 データ削除・消去証明.....	14
5.6.5 引継ぎ支援.....	14

1 共通編

ここでは内部情報系で共通的な要求事項を記載する。

なお、本事業の対象業務は自治体情報システムの標準化・共通化の対象外であるが、自治体DX推進計画、地方公共団体における情報セキュリティポリシーに関するガイドライン及び政府情報システムにおけるクラウドサービスの利用に係る基本方針の考え方を踏まえ、クラウドサービスの活用を基本とする。なお、クラウド方式には、SaaS、PaaS、IaaS、プライベートクラウド等を含むものとし、特定の提供方式に限定するものではない。

1.1 業務範囲

本調達は、内部情報系業務を対象とし、次に掲げる11業務に係る情報システムの構築、移行、運用及び保守を実施するものである。以下のシステムは令和11年4月の利用開始を想定する。

- ・ 共通基盤
- ・ 文書管理
- ・ 財務会計（令和10年9月利用開始想定）
- ・ 公有財産管理
- ・ 起債管理
- ・ 契約管理
- ・ 支払情報電子通知
- ・ 備品管理
- ・ 庶務事務
- ・ 人事給与
- ・ 被服貸与

各業務に係る個別要件については、別紙「業務要件書」〔個別業務編〕（内部情報系）」に定める。

また、本調達の対象には、上記各システムの提供及び運用に加え、大量印刷業務等に係る運用サービス並びにサポートデスク業務を含むものとする。各業務に係る運用要件については、別紙「D.BPO要件書（内部情報系）」に定める。

本調達により導入する各システムは、業務ごとに独立して稼働するものではなく、相互に連携する「統合内部情報システム」として構成する。統合内部情報システムにおいては、人事給与システムから連携される異動情報を共通基盤上で一元的に管理し、財務会計システム、文書管理システム、電子決裁基盤システムその他の対象システム間において、個別のメンテナンスを要することなく共通利用できる仕組みとする。

あわせて、事務効率の向上を図るため、職員、所属、役職等の情報をシステム間で同期するとともに、シングルサインオンにより各システムを利用できる統合的な利用環境を構築するものとする。

1.2 権限（職務分掌、業務ロール、承認権限 等）

1.2.1 認証方式

本調達システムは、本市が利用する認証基盤、庁内ネットワーク、職員情報等との連携を踏まえ、利

用者が適切に認証され、権限に応じてシステムを利用できる仕組みを備えること。

1.2.2 認証ID／パスワード・権限範囲

基盤連携によるSSO及び他業務データ参照に対応すること。

認証方式については、本市の現行環境及び本調達システムの構成を踏まえ、シングルサインオン、ID／パスワード認証、多要素認証その他適切な方式を協議の上整理すること。

1.2.3 利用者情報連携

職員情報、所属情報、職位、権限等について、本市が指定する情報を基に利用者管理を行えること。

1.2.4 権限管理

利用者の所属、役職、担当業務等に応じて、利用可能な機能、参照可能な情報、更新可能な範囲を制御できること。

1.2.5 異動・退職時の対応

人事異動、所属変更、退職、休職等に伴う利用者情報及び権限情報の追加、変更、停止、削除を適切に反映できること。

1.2.6 関連システムとの調整

認証基盤、人事給与システム、庁内ポータル、グループウェア等との連携が必要となる場合は、連携方式、データ項目、更新タイミング、責任分界を整理すること。

1.2.7 ログ管理

認証、ログイン、ログアウト、権限変更、利用者情報変更等について、必要なログを取得・確認できること。

1.2.8 セキュリティ対策

認証情報、利用者情報、権限情報の取扱いについて、漏えい、なりすまし、不正利用を防止するための安全管理措置を講じること。

1.3 市の概要

本市の基礎数値等概要については、本市ホームページ統計情報を参照すること。

本市／統計情報

<https://www.city.kofu.yamanashi.jp/somu-somu/shise/toke/toke.html>

本市の行政サービス及び独自制度等については、本市ホームページを参照すること。

2 連携要件

2.1 業務横断データ連携

2.1.1 連携対象一覧の整理

事業者は、本調達システムと連携する庁内外の関連システムについて、連携対象、連携目的、連携データ、連携方式、連携頻度、連携タイミング、管理主体を整理すること。

2.1.2 シングルサインオン

基盤と連携してシングルサインオンで起動すること。

2.1.3 データを抽出及び提供

他業務からの要求に応じて、必要なデータを抽出及び提供できること。

2.1.4 連携方式の整理

事業者は、現行の連携方式を踏まえ、本調達システムにおける連携方式を整理すること。連携方式は、CSV等のファイル連携、API連携、オンライン連携、外部媒体連携その他適切な方式を含めて検討すること。

2.1.5 連携仕様の作成支援

事業者は、連携データの項目、形式、桁数、コード体系、文字コード、レイアウト、送受信条件、処理タイミング等を整理し、連携仕様の作成を支援すること。

2.1.6 責任分界の整理

事業者は、連携元システム、連携先システム、ネットワーク、ファイル授受、データ加工、エラー対応等について、本市、事業者、関連システム事業者の役割分担及び責任分界を整理すること。

2.1.7 関連システム事業者との調整支援

事業者は、連携に必要な仕様確認、課題整理、対応方針案の作成、会議資料作成、議事整理等により、本市と関連システム事業者との調整を支援すること。

2.1.8 データ変換・コード変換

事業者は、連携にあたりデータ形式、コード体系、文字コード、日付形式、外字、桁数、項目名称等に差異がある場合は、変換要否、変換方法、確認方法を整理すること。

2.1.9 連携エラー対応

事業者は、連携処理におけるエラー検知、エラー内容の確認、再送、再取込、取消、二重取込防止、手動補正等の対応方法を整理すること。

2.1.10 連携ログ・処理結果管理

事業者は、連携処理の実施日時、処理件数、正常件数、エラー件数、処理結果、再処理状況等を確認

できるよう、連携ログ及び処理結果の管理方法を整理すること。

2.1.11 連携テスト支援

事業者は、関連システムとの連携について、テスト観点、テストデータ、正常系・異常系の確認内容、実施手順、判定基準を整理し、連携テストの実施を支援すること。

2.1.12 本番移行時の連携確認

事業者は、本番移行にあたり、初回連携、最終連携、差分連携、連携停止期間、連携再開手順、切替後の確認方法を整理すること。

2.1.13 運用開始後の連携管理

事業者は、本番稼働後の連携処理について、日次・月次・年次等の運用確認、エラー時対応、問い合わせ対応、関連システム変更時の影響確認方法を整理すること。

2.1.14 セキュリティ・アクセス管理

事業者は、連携データの授受にあたり、アクセス権限、認証、暗号化、送受信経路、媒体管理、ログ管理、個人情報保護等の安全管理措置を整理すること。

2.2 共通機能連携

各業務に係る個別データ連携要件については、別紙「業務要件書_〔個別業務編〕（内部情報系）」に定める。

3 データ移行要件

3.1 データ移行要件

3.1.1 移行要件・移行対象

現状データで保持されている移行対象データは、業務データ、マスタデータ、履歴データ、添付ファイル、帳票データ、設定情報等に区分し、対象範囲は「移行計画書」に定めること。

3.1.2 過年度データ移行

過年度データについては、業務継続に必要な参照・検索・帳票出力の要否を踏まえ、全件移行、参照用移行、外部保管、アーカイブのいずれとするかを業務ごとに定めること。

業務主管課の負担とならぬよう効率的かつ安全に行うこと。

3.1.3 履歴保持

移行後の履歴データの保存期間、参照方法、検索条件、ページ方針及び権限管理は、業務主管課と協議の上定めること。業務ごとに過年度データの取扱いについて指定のあるものについては、これを採用すること。

3.1.4 抽出・変換

既存システムから抽出されたデータ（既存事業者が実施）及びデータ仕様を確認し、データ移行仕様の提示、既存データの変換、移行データテスト、稼働確認等を行うこと。

3.2 EUC機能

3.2.1 既存事業者との連携

データ移行時のデータ欠如については、既存事業者、新規事業者、本市の役割分担、成果物、提出期限、再抽出条件及び照会方法を明確にし、新規事業者が主体となり業務主管課、既存事業者に協力しながら修正、追加等の作業を行うこと。

3.2.2 データ抽出

- (1) データを横断的に、リアルタイムに全件抽出することができる、汎用的かつ共通的なデータ出力機能をパッケージ機能とは別に用意すること。
- (2) 台帳・一覧系の帳票全てについて、必要なデータを全てシステムからリアルタイムにExcel出力できること。
- (3) 本市側でデータを抽出し、集計や加工等の利活用が可能となるよう、業務データの定義や構造を明示し、画面での抽出定義が可能なこと。抽出定義を保存し、再利用できること。
- (4) Excel管理を行う台帳については、システム格納項目外の独自項目を付加して管理を行っているため、これを可能にするデータベースシステムについても提案を行うこと。
- (5) データの定義や構造については、文書だけでなく、システムの把握できるような仕組みを用意すること。
- (6) 災害時支援システム等、外部のシステムへのデータの提供が都度可能となる仕組みを用意すること。

3.3 移行テスト

- (1) 移行テストは、少なくとも事前検証、リハーサル、本番移行の各段階で実施し、件数一致、項目一致、業務確認、エラー残件、性能影響を確認すること。
- (2) 移行後は、移行元件数と移行先件数、主要項目、金額、ステータス、履歴、関連データの整合性を確認し、業務主管課の確認を受けること。
- (3) 現状データ全件移行、変換、テスト、修正を行うこと。

3.4 本番移行

3.4.1 本番移行手順

本番移行に当たっては、移行作業の手順、実施体制、判定基準、切戻し条件及び切戻し手順、再移行手順、暫定運用方法、影響範囲の確認方法並びに報告・連絡手順を定めること。

3.4.2 本番移行及びデータ移行

- (1) 本番移行時に重大な不整合又は移行失敗が発生した場合は、あらかじめ定めた判定基準及び手順に基づき、切戻し、再移行又は暫定運用等の必要な対応を実施するとともに、影響範囲を確認し、速やかに本市へ報告すること。
- (2) 業務に必要なデータは、既存システムからの移行もしくは入力等、必要な手法によって全件移行すること。
- (3) データ移行作業は原則として事業者で実施すること。

3.4.3 終了時・次期移行

契約終了時又は次期更改時に、本市が保有するデータを標準的な形式で抽出・提供できること。

4 共通機能要件

4.1 業務システムに関する共通機能

以下の項目に規定する機能を有すること。また、以下に明示がなくとも、行政向けシステムにおいて一般的に必要と判断される機能を備えること。サービス要件書及び「業務要件書_〔個別業務編〕（内部情報系）」にこれらとは異なる記載がある場合には、そちらの条件を優先する。

4.1.1 登録機能

必須情報が入力されていない状態でも一時保存ができること。

4.1.2 職員向けガイダンス

職員向けガイダンスポップアップ画面やG U I の柔軟なカスタマイズなどの機能を有すること。

4.1.3 入力支援

- (1) 日付入力支援機能（西暦・和暦の入力支援、カレンダー入力など）を備えること。
- (2) 処理した履歴を保持し（直近の10件程度）、処理対象者を簡単に呼び出せること。

4.1.4 検索

- (1) 法人の電話番号、法人名又は代表者名、登記年月日、法人の略称や通称で検索ができること。
- (2) 口座情報から検索ができること。
- (3) 数字、アルファベットは大文字小文字の関係なく検索ができること。
- (4) 検索履歴を保持し（直近の10件程度）、検索履歴から再度検索ができること。

4.1.5 マルチウィンドウ対応

- (1) 複数のメニューを同時に立ち上げて処理できること。
- (2) 複数の業務を同時に立ち上げて処理できること。

4.1.6 金融機関マスタ

金融機関マスタを提供し、常に最新の状態を維持するようメンテナンスを行うこと。

4.1.7 業者マスタ

- (1) 指定医療機関、指定介護機関、指定事業所など、業務ごとに使用する業者マスタを管理できること。
- (2) 業者コードは自動及び任意で付番できること。

4.1.8 バッチ状況確認

- (1) 業務主管課で行うバッチ処理に関して、進捗状況や詳細結果が一覧で確認できること。
- (2) 実行情報、結果情報は保持すること。

4.1.9 業務機能

本共通機能項目は、各業務システムに対して共通して使用する基本機能を掲載したものである。基本機能の共通化により、業務の効率化及び市民サービスの均一化を図る。

4.1.10 データ保存

- (1) 特に指定が無い限り、データは移行データや履歴も含め、システム内に全件保持し続けること。
- (2) データをシステム外にパージする場合は、個別に文書による承認を得ること。パージしたデータは閲覧・抽出のできるシステムを用意すること。

4.1.11 メモ機能

- (1) メモ(備考欄)機能については、過去の入力情報を削除することなく管理及び閲覧ができること。
- (2) 各通知書、納付書等へメモの記入スペースを設けるとともに、メモの記入ができること。
- (3) メモの有無を画面上で容易に確認することができること。

4.1.12 サービス仕様

- (1) 本市の業務を理解し、システムを効率的に利用できる業務方法を提案すること。
- (2) 他団体の事例を踏まえ、条例・規則等の変更も含め、業務の効率的な実施手法についての提案を行うこと。
- (3) 外部ツール等を活用し、データの利活用に際しシステム変更が不要なシステムであること。

4.1.13 データパンチ

データパンチは決められたスケジュールに沿って運用を行うこと。データパンチ用原票については、原紙となるため取扱いには十分に注意し、受領や返却などの受け渡しについてはドキュメントにより確実に行うこと。

役割分担：業務主管課	データパンチ用原票の整理・分類・並び替え・補記 データパンチ後の確認・修正
事業者	データパンチ用原票の受領及び返却 データパンチ実施 データパンチ不可項目の情報伝達

4.1.14 発行機能

- (1) 通知にはカスタマーバーコード、電子公印、文書管理番号を印字できること。
- (2) 文書管理番号の自動採番が行えること。
- (3) 印刷イメージや印刷対象などを確認するなど、無駄な印刷物の排除ができること。
- (4) 決裁欄については、決裁運用に合わせた設定ができること。

4.1.15 権限管理

- (1) 職員番号、パスワードを設定及び管理ができること。また、システム操作権限（メニュー操作、バッチ起動、帳票出力）を操作者ごとに設定できること。
- (2) パスワードが定期的に変更されていない場合に通知する機能を有し、パスワード変更やアカウン

トロックなどの設定が行えること。

- (3) 複数業務を跨った権限や、参照できるデータの範囲を限定する権限など、本市の運用に合わせた設定が可能なこと。

5 非機能要件

5.1 セキュリティ要件

5.1.1 法令

事業者は、本業務の遂行に当たり、本市の情報セキュリティポリシー、関係法令、国の標準ガイドライン類及び本仕様書の定めを踏まえ、必要なセキュリティ対策を講じること。

5.1.2 セキュリティ対応

- (1) 事業期間を通じて、その時点において有効と判断される技術的・業務的及び組織的なセキュリティ対策を講じ、不正なアクセス、ソフトウェア、システム利用、情報の漏えい、改ざん、滅失又は毀損を防止する仕組みを備えること。
- (2) 事業者は、パスワードその他の認証、権限管理、アクセス制御、操作記録、ログ管理その他必要なセキュリティ管理を実施し、必要に応じて設定内容の確認、変更及び見直しを行うこと。
- (3) 不正なデータの出力・持ち出し又は不適切な利用を防止するための管理策を備えること。
- (4) 不正なアクセスまたはシステム利用があった場合に、その事実を確認し、必要な範囲で記録、調査及び報告ができる仕組みを備えること。
- (5) 特定データの操作、保存、移動、出力等について、必要に応じて追跡及び確認ができるようにすること。事業者は、外部システム又は別システムとの間でデータを授受する場合には、情報の機密性、完全性及び可用性を確保するため、適切な方法により安全に実施すること。

5.1.3 脆弱性に対する対応

- (1) 事業者はセキュリティ上の脆弱性又はそのおそれを把握した場合には、速やかに本市に報告するとともに、その影響範囲及び対応方針について本市と協議すること。
- (2) 事業者は、セキュリティ修正プログラムの適用、設定変更、不要なサービスの停止、アクセス権限の見直しその他必要な対策について、システムの安定稼働への影響を考慮したうえで、適切な時期及び方法により実施すること。
- (3) 事業者は、セキュリティ対応の実施状況、発生したインシデント又はそのおそれ、対応状況、残存リスク及び今後の対応方針について、本市へ適時報告すること。

5.1.4 特権ID管理

特権IDを利用する作業は、事前承認、利用者、利用日時、利用目的、操作内容、作業結果を記録し、本市が確認できる状態で管理すること。

5.1.5 インシデント対応

インシデントの分類、初動対応、報告期限、影響範囲特定、復旧、再発防止策、本市への報告内容を明確化すること。

5.1.6 再委託先管理

再委託については、本調達に係る業務の一部を第三者に実施させる場合を対象とし、再委託する業務の範囲、再委託先、実施体制、取り扱う情報、責任関係及びセキュリティ対策等を明示した上で、本市

の承認を得ること。

5.1.7 外部サービス管理

外部サービスの利用については、利用するサービスの内容、取り扱う情報、責任分界、セキュリティ対策、障害・サービス終了時の対応及び監査対応の可否等を明示すること。

5.2 インフラ・クラウド要件

5.2.1 クラウド利用時の責任分界

クラウドサービスを利用する場合は、クラウド事業者、事業者、本市の責任分界、障害時連絡、ログ取得、バックアップ、復旧、セキュリティ対応の役割を明確にすること。

5.2.2 I S M A P等の確認

クラウドサービスを利用する場合は、I S M A P等の公的な安全性評価制度への登録状況、データ所在、監査対応可否を踏まえて提案すること。

5.2.3 標準的な連携方式

他システム連携は、標準仕様、公開A P I、C S V等の一般的なデータ形式、標準的な認証・連携方式を優先し、特定製品に依存する方式を採用する場合は理由と代替策を示すこと。

5.2.4 設置要件

サーバ設置場所（バックアップやテスト環境、開発環境も含む）や作業拠点（開発や運用アウトソーシングも含む）は、事業者が用意すること。

5.2.5 回線要件

- (1) 回線については、B C P対策も含め、事業者が用意すること。1 G b p s以上の速度を確保すること。
- (2) BCP 対応として、庁舎内サーバールームへのバックアップ設置の提案を行うこと。

5.2.6 災害要件

災害時に主要データを参照できる代替手段を確保すること。

5.2.7 業務端末

- (1) 業務に必要な端末の提供として、人事給与については端末18台、レーザープリンタ4台（内カラープリンタ1台）、及びその他必要な周辺機器を確保し、本市の指定に従い配置すること。その他の業務については本市が調達した端末で行うものとする。
- (2) 端末はノート型（15.6インチ以上）のものを用意すること。E x c e l、W o r dを利用できるライセンスを用意すること。
- (3) 一人一台端末とのディスプレイの共有など、デスクトップの省スペース化に関する提案を行うこと。
- (4) 修理や部品交換など、メンテナンスや増強が容易な端末を提案すること。

5.3 性能・可用性

5.3.1 性能

- (1) 通常想定される業務実施に支障の出ない性能を維持すること。
- (2) 業務仕様書に個別の記載がある場合を除き、検索、照会、登録、更新、画面遷移等の主要なオンライン処理について、ネットワーク等の影響を排した条件で、通常時3秒以内、アクセス集中時5秒以内を基本目標とする。
- (3) 帳票出力については、印刷指示から印刷開始まで10秒以内を基本目標とする。
- (4) 前各号の性能目標を適用する対象処理、アクセス集中時の条件、測定条件、測定頻度及び測定方法については、サービス要件書及びモニタリングに係る規定との整合を図った上で、本市と協議し決定すること。
- (5) 通常検索・定型集計を対象とし、大量抽出・非定型集計は対象外又は別基準とする。
- (6) 性能調査測定の手法・プロセスについて具体的に示し、甲府市の承認を得ること。

5.3.2 稼働時間

- (1) 事業関連図書で特に指定する場合を除き、稼働時間は、土曜日と祝祭日、および12月30日から1月3日を除く全ての日で原則7:30～24:00とする。また、業務時間は、土曜日と祝祭日、および12月30日から1月3日を除く全ての日で原則8:30～17:15とする。
- (2) 但し、この他に本市が事業者と事前の協議を行い稼働する時間を含むものとする。
- (3) 稼働時間・業務時間については、事業者の提案により延長する場合もある。

5.3.3 計画停止時間

- (1) メンテナンス等により予定されたシステムの計画停止時間の総計は、年間総稼働時間の1%以下であること。また、一回の停止時間については、本市の承認を得て決定すること。
- (2) 稼働時間内に、職員もしくは市民の利用に何らかの影響のある機能等が計画的にかつ正常に使用できない場合を、計画停止とみなす。
- (3) 稼働時間外における停止時間は、計画停止時間に含まない。
- (4) 計画停止時は、障害対応計画書によりシステム停止予定時間を明らかにした上で本市の承認を得ること。

5.3.4 予定外停止時間

- (1) 予定外のシステム停止時間の総計は、総稼働時間の0.5%以下であること。
- (2) 稼働時間内に、職員もしくは市民の利用に何らかの影響のある機能等が予定されずにかつ正常に使用できない場合を、予定外停止とみなす。
- (3) 復旧のために稼働時間内に影響を与えた部分を除き、稼働時間外における停止時間は、予定外停止時間に含まない。
- (4) システムが計画通りの性能を維持するための諸条件について明示し、あらかじめ必要な措置をとること。
- (5) 性能の想定に際し前提となる端末性能、配置、使用方法、ネットワーク条件等について明示すること。対応可能な最大端末数等についても明示すること。

- (6) システム構築時の検証により、あらかじめ検証を行い、検証結果について本市の承認を得ること。
- (7) 運用管理期間内の使用ハードウェア容量・クラウド領域・必要性能について予測を行い、十分な容量及び性能をあらかじめ確保しておくこと。
- (8) ハードウェア、サーバ関連設備、クラウド領域、システム領域等、サービス仕様と業務仕様を満たすために必要なレベルまでは、事業者負担で必要な調達・作業・検査・メンテナンス等を行うこと。なお、ハードウェア等の資産を本市は原則保有せず、また、サービス仕様等を満たすことができれば、ハードウェア等は新品である必要も最新である必要も無い。
- (9) あらかじめサービスの利用量やリソースの使用量についての予測を行い、運営管理期間中における計画を立案しておくこと。

5.3.5 RTO/RPO

- (1) 障害・災害時のRTO（復旧目標時間）及びRPO（復旧時点）を、業務重要度に応じて設定すること。
- (2) 必要な可用性、耐障害性、拡張性、運用効率性を確保できる構成とする。クラウド・SaaSの場合は仮想化方式に限定しない。

5.4 運用・サポート

5.4.1 サポート範囲・対象外

サポート対象は本調達対象システム及び本業務に関する問い合わせとし、制度判断、対象外システム、端末・ネットワーク障害等は対象外又は別窓口連携とすること。

5.4.2 変更管理

設定変更、帳票変更、連携条件変更、運用手順変更等を行う場合は、変更内容、影響範囲、承認者、実施時期、費用負担を記録し、本市の承認を得ること。

5.5 監査・ログ管理・運用支援

- (1) 認証ログ、操作ログ、管理者操作ログ、データ出力ログ、連携ログ、障害ログを取得し、保存期間、保管場所、閲覧権限、検索・提出方法を明示すること。
- (2) 特定データの操作、保存、移動等、どのクライアントでどのような操作が行われたか検出できる仕組みを備えること。
- (3) 外部記録装置の接続と処理内容を詳細に記録し、後日の調査を可能とすること。
- (4) 出力データの暗号化やパスワード保護について、セキュリティポリシーやガイドライン等に沿った適切な処置が行えること。
- (5) 基幹業務系ネットワーク、内部情報系ネットワーク、インターネット系ネットワークを跨って業務情報を交換する仕組みを備えること。

5.6 事業継続・BCP・終了時データ移管

5.6.1 事業継続性

- (1) 事業の完了時、及び破綻時において、サービスの継続性を確保するための計画を策定し、最新の状態を維持すること。

- (2) 本事業の完了時、及び事業者が破綻した場合、構成企業や製品提供元が破綻した場合等、事業やサービスの継続に支障を来たす場合を想定し、具体的な対応方法を策定しておくこと。なお、対策に要する費用は原則本事業の範囲内であることに留意すること。
- (3) 災害時におけるサービス継続を確保し、継続計画を策定・実施すること。実施内容は常に確認・検証が可能であること。
- (4) 大規模災害によりシステムが損壊した場合、発生時から①1週間以内、②1ヶ月以内、③1ヶ月以降、に分類し、それぞれのフェーズにおけるサービスの提供方法を策定すること。
- (5) 少なくとも、①及び②のフェーズにおける事業継続計画の策定及び復旧対策の検討・準備については、本事業の範囲内とする。また、③においては、災害発生前と同等の業務レベルを維持できるサービスを提供するために必要な具体的な対策を示し、想定費用を積算すること。なお、想定を超える激甚災害その他の不可抗力により、インフラの再調達、大規模な復旧作業その他通常の事業継続対策の範囲を超える対応が必要となった場合は、本市と事業者が協議の上、その対応内容及び費用負担を決定するものとする。

5.6.2 リストア確認

定期的に復元確認を実施し、結果を報告すること。

5.6.3 契約終了時データ移管

契約終了時又は事業者変更時に、業務データ、設定情報、ログ、運用資料を一般的に利用可能な形式で提供すること。

5.6.4 データ削除・消去証明

移管完了後、事業者環境に残存するデータを復元困難な方法で削除し、削除結果を報告すること。

5.6.5 引継ぎ支援

次期事業者への引継ぎに必要な資料提供、質疑対応、移行支援を行うこと。