別紙4　周辺機器

仙台市準備品

No	機器名称	現行機種（令和7年12月時点）	次期機種予定（令和10年3月時点）	備考
1	端末	LIFEBOOK A5511/G	OS：Microsoft Windows 11（64bit） CPU：Intel Core i3 相当以上（一般的な業務用途に十分な処理性能を有すること） メモリ：4GB 以上 ディスプレイサイズ：14インチ以上 現行機種（LIFEBOOK A5511/G）と同等以上の性能を有するもの	
2	ページプリンタ	XL-C8365・XL-9322	レーザー式プリンタ カラー・白黒印刷機能を有するもの 両面印刷機能を有するもの A3、A4、B5、はがき、封筒印刷機能を有するもの 現行機種（XL-C8365・XL-9322）と同等以上の性能を有するもの	

受託者準備品

No	機器名称	現行機種（令和7年12月時点）	次期機種予定（令和10年3月時点）	備考
	（受託者準備品なし）			

別紙５

地方公共団体情報システム非機能要件の標準

【第1.2版】

令和7年9月

デジタル庁
総務省

「非機能要件の標準」について

非機能要件の標準は、「非機能要求グレード（地方公共団体版）」（平成26年3月・J-LIS作成）において、業務・システムの分類「グループ②」として示された要求グレードのうち、クラウド調達時の扱いが「○：クラウド対象と成り得る項目」とされている項目を中心に、最新の状況を鑑み、要件を修正・追加したものである。

また、「非機能要件の標準」は、地方公共団体情報システムの標準化に関する法律（令和3年法律第40号。以下「標準化法」という。）第7条及び第5条第2項第3号に定められる 地方公共団体情報システムの共通基準の1つであることから、デジタル庁が総務省と協議して定める。

1. 非機能要件の標準を用いる業務システム
   - 標準化法第2条第1項の規定に基づく「デジタル社会の実現に向けた重点計画」（令和4年6月7日閣議決定）で定める標準化対象20業務※[1]に係る地方公共団体が使用するシステム（地方公共団体情報システム）。

   ※[1] 住民基本台帳、戸籍、戸籍の附票、固定資産税、個人住民税、法人住民税、軽自動車税、印鑑登録、選挙人名簿管理、子ども・子育て支援、就学、児童手当、児童扶養手当、国民健康保険、 国民年金、障害者福祉、後期高齢者医療、介護保険、生活保護、健康管理

2. 非機能要件の標準の適用対象及び範囲
   - ガバメントクラウド、パブリッククラウド又は独自クラウド（自治体クラウド）のクラウドサービス※[2]によって提供される、IaaS、PaaSなどのクラウドサービス（以下「システム基盤」という。）を用いて構築される業務システムとする。ただし、システム基盤利用にかかるアプリケーション側の対応や主にネットワーク関連など一部の庁内環境（例：業務アプリケーションのログやセキュリティ対策、ネットワーク（庁内LAN/WAN）の通信回線や伝送機器等）についても対象に含む。

   ※[2] 「非機能要件の標準」における、ガバメントクラウド、パブリッククラウド及び独自クラウド（自治体クラウド）の定義は以下のとおりとする。
   - ガバメントクラウド：「デジタル社会の実現に向けた重点計画」等の政府方針に基づき、安全かつ合理的な利用環境としてデジタル庁が選定した複数のパブリッククラウドのこと。
   - パブリッククラウド：クラウドサービス提供事業者（CSP）がインターネット経由で不特定多数のユーザーに提供するクラウド環境のこと。
   - 独自クラウド（自治体クラウド）：自治体（又は複数の自治体）が標準準拠システムを外部のデータセンターで管理・運用するなど、特定の組織内でのみ利用されるクラウド環境のこと。

3. 非機能要件の標準の利用方法
   - ○ 各地方公共団体（本資料中「自治体」と表現することもある。）
     - ● 標準化対象20業務に係る情報システム調達等の際に、開発ベンダに対して示す非機能要件を非機能要件の標準とする。
     - ● 非機能要件の標準に従って、クラウドサービス（ガバメントクラウド、パブリッククラウド、独自クラウド（自治体クラウド））によるシステム基盤の構築や運用を要求する。
     - ● 「非機能要件の標準」の選択レベルを選択する際には、以下の点を遵守する。
       - ✓ 「選択時の条件」にプラス条件（マイナス条件）の記載がある項目は、国が示した「選択レベル」を選択するか、プラス条件（マイナス条件）の下、別のレベルを選択する。
       - ✓ 「選択時の条件」にプラス条件、マイナス条件の両方の記載がない項目は、自治体の規模や、自治体における業務の性質、リスク受容方針等に応じたレベルを選択する。
       - ✓ 次の非機能要件は、自治体の業務量に応じて具体的な値を示す。
         「B.1.1.1 ユーザ数」、「B.1.1.2 同時アクセス数」、「B.1.1.3 データ量（項目・件数）」、「B.1.1.4 オンラインリクエスト件数」、「B.1.1.5 バッチ処理件数」
       - ✓ 共同利用方式の場合は、同一の環境を利用する複数の自治体において、一律のレベルを選択する。

4. 標準化対象20業務に係る各業務システムの標準仕様と非機能要件の標準の関係
   - 各業務システムの標準仕様において、非機能要件に関して独自の厳しい要件が定められた場合には、当該標準仕様の非機能要件部分が、非機能要件の標準に優先するものとする。

【改定履歴】

版数	改定日	主な改定理由
第1.0版	令和2年9月	初版公開
第1.1版	令和4年8月	デジタル社会の実現に向けた重点計画（令和４年６月７日閣議決定）に基づき、先行事業での検証結果を踏まえて、必要な拡充等を実施
第1.2版	令和7年9月	ガバメントクラウド早期移行団体検証事業や標準準拠システムへの移行等の状況を踏まえ、自治体の規模や業務の性質、リスク受容方針等に応じて幅を持たせ得る項目について、自治体が自らの裁量でレベルを選択可能な取扱いとする等の改定を実施

「非機能要件の標準」の使用方法について

○　非機能要件の標準は、調達時に定めるべき非機能要件の項目と、行政事務の運用上、選択肢として取り得るレベル（レベル0から5までの間）を示している。

※　一方、行政事務の運用上、選択肢として取り得ないレベルについては「グレーアウト（選択できない）」としている。

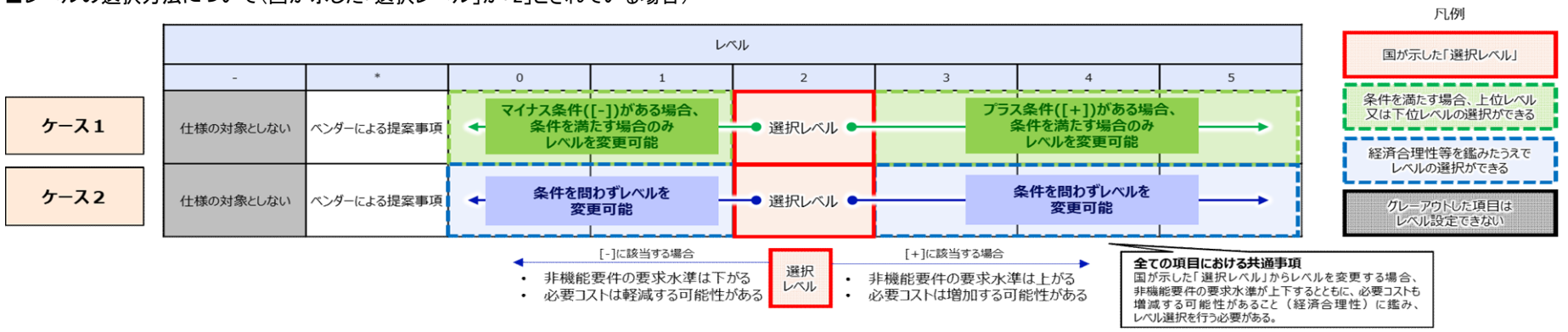
【レベル選択方法の例示】

ケース1：「選択時の条件」にプラス条件（[+]）の記載がある項目は、プラス条件を満たす場合は国が示した「選択レベル」よりもレベルを上げることができる。
また、「選択時の条件」にマイナス条件（[−]）の記載がある項目は、マイナス条件を満たす場合は国が示した「選択レベル」よりもレベルを下げることができる。
（マイナス条件（[−]）の記載がない項目は、国が示した「選択レベル」より低いレベルを選択できないことを示すため、該当レベルをグレーアウトする。）

ケース2：「選択時の条件」にプラス条件（[+]）及びマイナス条件（[−]）の両方の記載がない項目は、自治体の規模や、自治体における業務の性質、リスク受容方針等に応じて、柔軟にレベルを選択することができる。

※　注記1：いずれのケースにおいても、レベルの選択は必要であり、選択したレベルの要件は遵守する必要がある。
※　注記2：ケース1において、マイナス条件を満たし、「選択レベル」より低いレベルに選択した場合においても、「非機能要件の標準」を満たすものとする。
※　注記3：RFIやヒアリングを実施しても判断に迷う場合などには、国が示したレベルの範囲内に相当することを前提として、ベンダーに提案を求める方法も考えられる。
その場合には、「＊」を選択する。

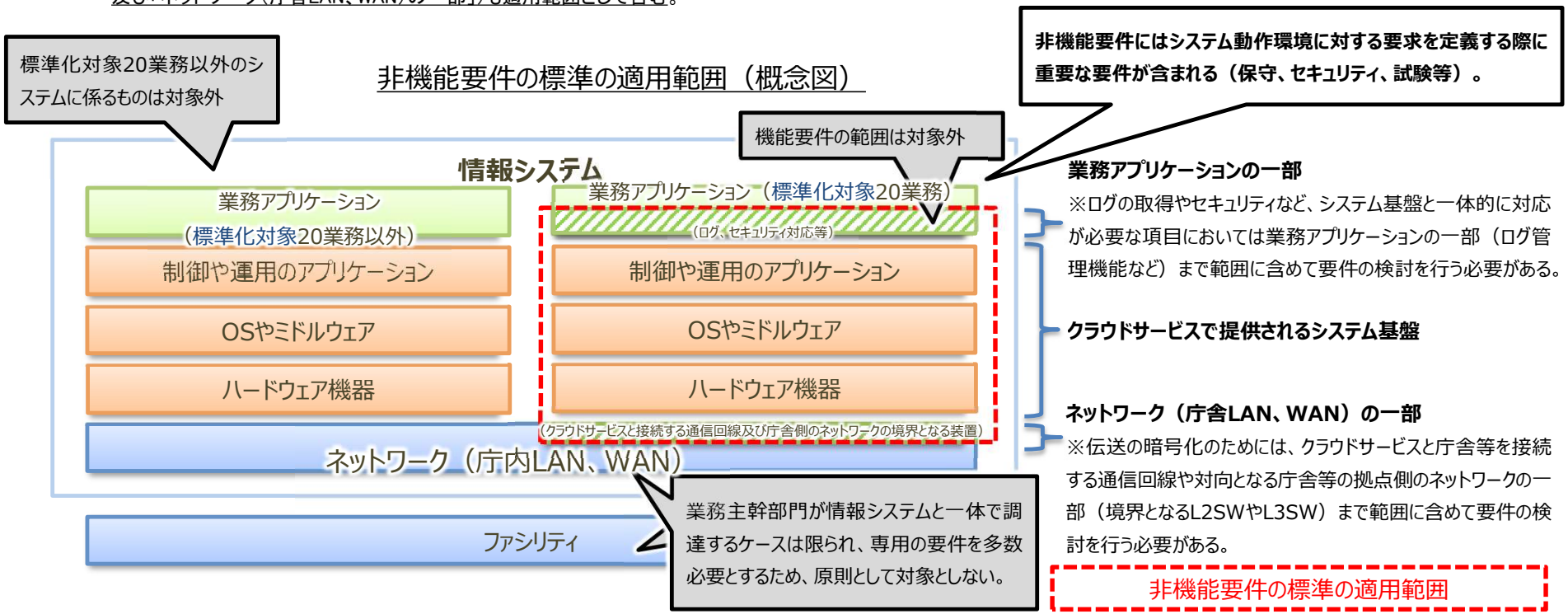
■レベルの選択方法について（国が示した「選択レベル」が「2」とされている場合）



「非機能要件の標準」の適用対象及び適用範囲

○ 非機能要件の標準の**適用対象**は、ガバメントクラウド、パブリッククラウド又は独自クラウド（自治体クラウド）のクラウドサービスを用いて提供される、標準化法第2条第1項で規定される地方公共団体情報システムとする。

○ 非機能要件の標準の**適用範囲**は、J-LIS「非機能要求グレード（地方公共団体版）」に倣い、原則として「クラウドサービス（ガバメントクラウド、パブリッククラウド又は独自クラウド（自治体クラウド））として提供されるシステム基盤」を適用範囲とする。
また、システム基盤に対するセキュリティや運用管理上の要件を定義する際に、必ずしもシステム基盤のみで実現されるとは限らないもの（「業務アプリケーションの一部」、及び「ネットワーク（庁舎LAN、WAN）の一部」）も適用範囲として含む。



項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	利用ガイドの解説[2]	選択レベル		本市の選択レベル		選択時の条件	[+][-]条件[3]	レベル								備考 「利用ガイド」第4章も参照のこと
													-	*	0	1	2	3	4	5	
C.1.2.2	運用・保守性	通常運用	外部データの利用可否	外部データによりシステムのデータが復旧可能かどうか確認するための項目。 外部データとは、当該システムの範囲外に存在する情報システムの保有するデータを指す（例：住民基本4情報については、住基ネットの情報がある等）。	○		2	システムの復旧に外部データを利用できない	2	システムの復旧に外部データを利用できない	全データを復旧するためのバックアップ方式を検討しなければならないことを想定。		仕様の対象としない	ベンダーによる提案事項	外部データによりシステムの全データが復旧可能	外部データによりシステムの一部のデータが復旧可能	システムの復旧に外部データを利用できない				【注意事項】 外部データによりシステムのデータが復旧可能な場合、システムにおいてバックアップ設計を行う必要性が減るため、検討の優先度やレベルを下げて考えることができる。 外部に同じデータを持つ情報システムが存在するため、本システムに障害が発生した際には、そちらから抽出したデータによって情報システムを復旧できるような場合は、国が示した「選択レベル」からレベルを下げることが考えられる。
C.2.3.5	運用・保守性	保守運用	OS等パッチ適用タイミング	OS等パッチ情報の展開とパッチ適用のポリシーに関する項目。 OS等は、サーバー及び端末のOS、ミドルウェア、その他のソフトウェアを指す。 脆弱性に対するセキュリティパッチなどの緊急性の高いものは速やかに適用する。	○	P29	4	緊急性の高いパッチは速やかに適用し、それ以外は定期保守時に適用を行う	4	緊急性の高いパッチは速やかに適用し、それ以外は定期保守時に適用を行う	緊急性の高いパッチを除くと、定期保守時にパッチを適用するのが一般的と想定。 [-]外部と接続することが全くない等の理由で緊急対応の必要性が少ない場合（リスクの確認がとれている場合）。 [+]外部と接続することがある等の理由で緊急対応の必要性が高い場合（リスクの確認がとれている場合）。	○	仕様の対象としない	ベンダーによる提案事項	パッチを適用しない	障害発生時にパッチ適用を行う	定期保守時にパッチ適用を行う	緊急性の高いパッチは速やかに適用し、それ以外は障害対応時等適切なタイミングで適用を行う	緊急性の高いパッチは速やかに適用し、それ以外は定期保守時に適用を行う	新規のパッチがリリースされるたびに適用を行う	【注意事項】 リリースされるパッチの種類（個別パッチ／集合パッチ）によって選択レベルが変わる場合がある。 セキュリティパッチについては、セキュリティの項目でも検討すること（E.4.3.4）。 また、マイナンバー利用事務系のOSについては最新のパッチを速やかに適用すること。 なお、パッチを適用する際には事前検証を実施した上で速やかに適用することが望ましい。 【外部とは】 インターネットに接続した環境又は閉域環境の条件を満たさない環境。閉域環境とは「L2SW/L3SWによる通信経路の限定を行い、かつ、ファイアウォールによる通信プロトコルの限定等を行うことで必要な通信に制限をしている環境」を指す。
E.1.1.1	セキュリティ	前提条件・制約条件	遵守すべき規程、ルール、法令、ガイドライン等の有無	ユーザが遵守すべき情報セキュリティに関する規程やルール、法令、ガイドライン等が存在するかどうかを確認するための項目。 なお、遵守すべき規程等が存在する場合は、規定されている内容と矛盾が生じないよう対策を検討する。 （例） ・情報セキュリティに関する法令 ・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（総務省） ・その他のガイドライン ・その他のルール	○		1	有り	1	有り	セキュリティポリシー等を遵守する必要があることを想定。		仕様の対象としない	ベンダーによる提案事項	無し	有り					【注意事項】 規程やルール、法令、ガイドライン等を確認し、それらに従い、セキュリティに関する非機能要求項目のレベルを決定する必要がある。
E.2.1.1	セキュリティ	セキュリティリスク分析	リスク分析範囲	システム開発を実施する中で、どの範囲で対象システムの脅威を洗い出し、影響の分析を実施するかの方針を確認するための項目。 なお、適切な範囲を設定するためには、資産の洗い出しやデータのライフサイクルの確認等を行う必要がある。 また、洗い出した脅威に対して、対策する範囲を検討する。	○		1	重要度が高い資産を扱う範囲	1	重要度が高い資産を扱う範囲	重要情報が取り扱われているため、脅威が現実のものとなった場合のリスクも高い。そのため、重要度が高い資産を扱う範囲に対してリスク分析する必要がある。 [+] 情報の移動や状態の変化が大きい場合	○	仕様の対象としない	ベンダーによる提案事項	分析なし	重要度が高い資産を扱う範囲	対象全体				【レベル1】 重要度が高い資産は、各自治体の情報セキュリティポリシーにおける重要度等に基づいて定める（重要度が最高位のものとする等）。
E.4.3.4	セキュリティ	セキュリティリスク管理	ウィルス定義ファイル適用タイミング	対象システムの脆弱性等に対応するためのウィルス定義ファイル適用に関する適用範囲、方針及び適用のタイミングを確認するための項目。	○	P30	2	定義ファイルリリース時に実施	2	定義ファイルリリース時に実施	ウィルス定義ファイルは、ファイルが公開されるとシステムに自動的に適用されることを想定。 [-]ウィルス定義ファイルが、自動的に適用できない場合（例えばインターネットからファイル入手できない場合）。	○	仕様の対象としない	ベンダーによる提案事項	定義ファイルを適用しない	定期保守時に実施	定義ファイルリリース時に実施				【注意事項】 定義ファイルを適用する際には事前検証を実施した上で速やかに適用することが望ましい。 最新のウィルス定義ファイル適用時に、ウィルス検索エンジンのアップデートも検討すること。

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	利用ガイドの解説[2]	選択レベル		本市の選択レベル		選択時の条件	[+][-]条件[3]	レベル								備考 「利用ガイド」第4章も参照のこと
													-	*	0	1	2	3	4	5	
E.5.1.1	セキュリティ	アクセス・利用制限	管理権限を持つ主体の認証	資産を利用する主体（利用者や機器等）を識別するための認証を実施するか、また、どの程度実施するのかを確認するための項目。 複数回、異なる方式による認証を実施することにより、不正アクセスに対する抑止効果を高めることができる。 なお、認証するための方式としては、ID/パスワードによる認証や、ICカード認証、生体認証等がある。	○	P31	3	複数回、異なる方式による認証	3	複数回、異なる方式による認証	攻撃者が管理権限を手に入れることによる、権限の乱用を防止するために、認証を実行する必要がある。		仕様の対象としない	ベンダーによる提案事項	実施しない	1回	複数回の認証	複数回、異なる方式による認証			【注意事項】 管理権限を持つ主体とは、情報システムの管理者や業務上の管理者を指す。 認証方式は大きく分けて「知識」、「所持」及び「存在」を利用する方式がある。 機器等（データ連携サーバ等）は多要素認証の対象としない。
E.5.2.1	セキュリティ	アクセス・利用制限	システム上の対策における操作制限	認証された主体（利用者や機器など）に対して、資産の利用等を、ソフトウェアにより制限するか確認するための項目。 例）ソフトウェアのインストール制限や、利用制限等、ソフトウェアによる対策を示す。	○		1	必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみ許可する。	1	必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみ許可する。	不正なソフトウェアがインストールされる、不要なアクセス経路（ポート等）を利用可能にしている等により、情報漏洩の脅威が現実のものとなってしまうため、これらの情報等への不要なアクセス方法を制限する必要がある。 （操作を制限することにより利便性や、可用性に影響する可能性がある）		仕様の対象としない	ベンダーによる提案事項	無し	必要最小限のプログラムの実行、コマンドの操作、ファイルへのアクセスのみ許可する。					【注意事項】 利用者に応じて適切に、実行可能なプログラム、コマンド操作、アクセス可能なファイルを設定・管理すること。
E.6.1.1	セキュリティ	データの秘匿	伝送データの暗号化の有無	暗号化通信方式を使用して伝送データの暗号化を行う。 インターネットに直接接続せず、内部ネットワークのみに接続する情報システムの伝送において、悪意のある攻撃から重要なデータを保護するための対策。	○	P31	2	すべてのデータを暗号化	2	すべてのデータを暗号化	インターネットに直接接続せず、内部ネットワークのみに接続する情報システムを想定。 [-] インターネットに接続していない①を満たす閉域環境における伝送データにおいて、以下の②③双方の条件も満たす場合 ①L2SW/L3SWによる通信経路の限定を行い、かつ、ファイアウォールによる通信プロトコルの限定等を行うことで必要な通信に制限していること。 ②通信ログを取得していること。 ③インシデント管理及び対応を行うこと。	○	仕様の対象としない	ベンダーによる提案事項	無し	一部のデータを暗号化（自治体の判断により暗号化対象とする伝送データを選定する）	すべてのデータを暗号化			【注意事項】 本項番の「暗号化」は「ハッシュ化」等も含む。 暗号化方式等は、国における評価の結果をまとめた「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」を勘案して決定する。 （CRYPTREC暗号リスト：http://www.cryptrec.go.jp/list.html）。
E.6.1.2	セキュリティ	データの秘匿	蓄積データの暗号化の有無	ファイル・フォルダを暗号化するソフトウェアや、データベースソフトウェアの暗号化機能を使用して暗号化を行う。	○	P32	3	すべてのデータを暗号化	3	すべてのデータを暗号化	蓄積するデータについては、第三者に漏洩した場合でも、内容の判読ができないようすべてのデータの暗号化を実施する。		仕様の対象としない	ベンダーによる提案事項	無し	認証情報のみ暗号化	重要情報を暗号化	すべてのデータを暗号化			【レベル1】 認証情報のみ暗号化とは、情報システムで重要情報を取り扱うか否かに関わらず、パスワード等の認証情報のみ暗号化することを意味する。 【注意事項】 本項番の「暗号化」は「ハッシュ化」等も含む。 暗号化方式等は、国における評価の結果をまとめた「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)」を勘案して決定する。 （CRYPTREC暗号リスト：http://www.cryptrec.go.jp/list.html）。 システム利用開始時点からの全データを暗号化すること。

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	利用ガイドの解説[2]	選択レベル		本市の選択レベル		選択時の条件	[+][-]条件[3]	レベル								備考 「利用ガイド」第4章も参照のこと
													－	＊	0	1	2	3	4	5	
E.7.1.1	セキュリティ	不正追跡・監視	ログの取得	不正を検知するために、監視のための記録（ログ）を取得するかどうかの項目。 なお、どのようなログを取得する必要があるかは、実現する情報システムやサービスに応じて決定する必要がある。 また、ログを取得する場合には、不正監視対象と併せて、取得したログのうち、確認する範囲を定める必要がある。	○		1	必要なログを取得する	1	必要なログを取得する	不正なアクセスが発生した際に、「いつ」「誰が」「どこから」「何を実行したか」等を確認し、その後の対策を迅速に実施するために、ログを取得する必要がある。		仕様の対象としない	ベンダーによる提案事項	取得しない	必要なログを取得する					【注意事項】 取得対象のログは、不正な操作等を検出するための以下のようなものを意味している。 ・ログイン/ログアウト履歴（成功/失敗） ・操作ログ ・セキュリティ機器の検知ログ ・通信ログ ・DBログ ・アプリケーションログ 等
E.7.1.3	セキュリティ	不正追跡・監視	不正監視対象（装置）	サーバ、ストレージ、ネットワーク機器、端末等への不正アクセス等の監視のために、ログを取得する範囲を確認する。 不正行為を検知するために実施する。	○		1	重要度が高い資産を扱う範囲	1	重要度が高い資産を扱う範囲	脅威が発生した際に、それらを検知し、その後の対策を迅速に実施するために、監視対象とするサーバ、ストレージ、ネットワーク機器、端末等の範囲を定めておく必要がある。 [+]システム全体の監視が必要な場合	○	仕様の対象としない	ベンダーによる提案事項	無し	重要度が高い資産を扱う範囲	システム全体				
E.10.1.1	セキュリティ	Web対策	セキュアコーディング、Webサーバの設定等による対策の強化	Webアプリケーション特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。Webシステムが攻撃される事例が増加しており、Webシステムを構築する際には、セキュアコーディング、Webサーバの設定等による対策の実施を検討する必要がある。	○	P32	1	対策の強化	1	対策の強化	オープン系の情報システムにおいて、データベース等に格納されている重要情報の漏洩、利用者への成りすまし等の脅威に対抗するために、Webサーバに対する対策を実施する必要がある。		仕様の対象としない	ベンダーによる提案事項	無し	対策の強化					
E.10.1.2	セキュリティ	Web対策	WAFの導入の有無	Webアプリケーション特有の脅威、脆弱性に関する対策を実施するかを確認するための項目。 WAFとは、Web Application Firewallのことである。	○	P33	0	無し	0	無し	インターネットに直接接続せず、内部ネットワークのみに接続する情報システムを想定。		仕様の対象としない	ベンダーによる提案事項	無し	有り					【注意事項】 インターネットに接続したWebアプリケーションを用いる場合は、国が示した「選択レベル」からレベルを上げることが考えられる。

1　クラウド調達時の扱い　　○：クラウドの対象と成り得る項目　　△：クラウドの対象となる場合がある項目　　－：通常クラウドの対象とならない項目
なお、本項目でクラウド調達に必要な項目を網羅している訳ではない。

2　利用ガイドの解説　　Pxx：利用ガイドのメトリクス詳細説明ページ

3　[+][-]条件　　○：レベルの変更に条件がある項目

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	利用ガイドの解説[2]	選択レベル		本市の選択レベル		選択時の条件	[+][-]条件[3]	レベル								備考 「利用ガイド」第4章も参照のこと
													－	＊	0	1	2	3	4	5	
A.1.3.1	可用性	継続性	RPO（目標復旧地点）（業務停止時）	業務停止を伴う障害が発生した際、バックアップしたデータなどから情報システムをどの時点まで復旧するかを定める目標値。 バックアップ頻度・バックアップ装置・ソフトウェア構成等を決定するために必要。	○	P35	2	1営業日前の時点（日次バックアップからの復旧）	2	1営業日前の時点（日次バックアップからの復旧）	システム障害時において、障害復旧完了後、バックアップデータを使用したリストアを行うことを想定。 [-] データの損失がある程度許容できる場合（復旧対象とするデータ（日次、週次）によりレベルを選定） [+]選択レベルの時点（1営業日前の時点）での復旧では後追い入力が膨大に発生する等業務への支障が大きいことが明らかである場合	○	仕様の対象としない	ベンダーによる提案事項	復旧不要	5営業日前の時点（週次バックアップからの復旧）	1営業日前の時点（日次バックアップからの復旧）	障害発生時点（日次バックアップ+一時保存データからの復旧）			【注意事項】 RLOで業務の復旧までを指定している場合、業務再開のために必要なデータ整合性の確認（例えば、バックアップ時点まで戻ってしまったデータを手修正する等）は別途ユーザが実施する必要がある。
A.1.3.2	可用性	継続性	RTO（目標復旧時間）（業務停止時）	業務停止を伴う障害（主にハードウェア・ソフトウェア故障）が発生した際、復旧するまでに要する目標時間。 ハードウェア・ソフトウェア構成や保守体制を決定するために必要。	○	P35	2	12時間以内	2	12時間以内	窓口対応等、システム停止が及ぼす影響が大きい機能の復旧を優先しなるべく早く復旧する。 [-] 業務停止の影響が小さい場合 [+] 運用の実現性を確認した上で、業務への支障が大きいことが明らかである場合	○	仕様の対象としない	ベンダーによる提案事項	1営業日以上	1営業日以内	12時間以内	6時間以内	2時間以内		【注意事項】 RLOで業務の復旧までを指定している場合、業務再開のために必要なデータ整合性の確認（例えば、バックアップ時点まで戻ってしまったデータを手修正する等）は別途ユーザが実施する必要がある。 目標復旧時間をSLAに定めていないクラウドサービスを利用する場合は、CSPがSLAで示す稼働率を元に業務停止時間の最大値を算出し、RTOを検討することが考えられる。
A.1.3.3	可用性	継続性	RLO（目標復旧レベル）（業務停止時）	業務停止を伴う障害が発生した際、どこまで復旧するかのレベル（特定システム機能・すべてのシステム機能）の目標値。 ハードウェア・ソフトウェア構成や保守体制を決定するために必要。	○	P36	2	全システム機能の復旧	2	全システム機能の復旧	すべての機能が稼働していないと影響がある場合を想定。 [-] 影響を切り離せる機能がある場合	○	仕様の対象としない	ベンダーによる提案事項	規定しない	一部システム機能の復旧	全システム機能の復旧				【レベル1】 一部システム機能とは、特定の条件下で継続性が要求される機能などを指す。（例えば、住民基本台帳システムの住民票発行機能だけは、障害時も提供継続する場合やコンビニにおいて証明書発行が可能な場合等。）
A.1.4.1	可用性	継続性	システム再開目標（大規模災害時）	大規模災害が発生した際、どれ位で復旧させるかの目標。 大規模災害とは、火災や地震などの異常な自然現象、あるいは人為的な原因による大きな事故、破壊行為により生ずる被害のことを指し、情報システムに甚大な被害が発生するか、電力などのライフラインの停止により、システムをそのまま現状に修復するのが困難な状態となる災害をいう。	○	P37	2	一ヶ月以内に再開	2	一ヶ月以内に再開	電源及びネットワークが利用できることを前提に、遠隔地に設置された予備機とバックアップデータを利用して復旧することを想定。機能は、業務が再開できる最低限の機能に限定する。また、復旧までの間、バックアップデータから必要なデータをCSV等で自治体が利用できる形式で提供（※）する。 ※住民記録システム等、住民の安否確認に必要なデータを持つシステムについては、発災後72時間以内に、必要なデータを自治体が利用できる形式で提供すること。 [-] 運用の実現性を確認した上で、一定の再開期間を許容できる場合 [+] 人命に影響を及ぼす、経済的な損失が甚大など、安全性が求められる場合でベンダーと合意できる場合	○	仕様の対象としない	ベンダーによる提案事項	再開不要	数ヶ月以内に再開	一ヶ月以内に再開	一週間以内に再開	3日以内に再開	1日以内に再開	【注意事項】 目標復旧レベルについては、業務停止時に規定されている目標復旧水準を参考とする。
A.1.5.1	可用性	継続性	稼働率	明示された利用条件の下で、情報システムが要求されたサービスを提供できる割合。 明示された利用条件とは、運用スケジュールや、目標復旧水準により定義された業務が稼働している条件を指す。その稼働時間の中で、サービス中断が発生した時間により稼働率を求める。 一般的にサービス利用料と稼働率は比例関係にある。	○	P38	3	99.5%	3	99.5%	ガバメントクラウド又はパブリッククラウド、独自クラウドのいずれにおいても、保守要員による運用保守作業と各クラウドサービスで提供される運用保守サービス等（SLA等）を活用し、運用の実現性及び業務への影響を考慮した上で稼働率を設定すること。 また、自治体がその他受注者との取り決め項目として明示することで適合するものとする。 [-] 運用の実現性を確認した上で、業務停止が許容できる場合 [+] 運用の実現性を確認した上で、業務への支障が大きいことが明らかである場合	○	仕様の対象としない	ベンダーによる提案事項	規定しない	95%	99%	99.5%	99.9%	99.99%	【レベル】 稼働時間（バッチ処理等を含む運用時間）を平日のみ1日当たり12時間と想定した場合。 99.99%・・・・年間累計停止時間17分 99.9%・・・・・年間累計停止時間2.9時間 99.5%・・・・・年間累計停止時間14.5時間 99%・・・・・・年間累計停止時間29時間 95%・・・・・・年間累計停止時間145時間

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	利用ガイドの解説[2]	選択レベル		本市の選択レベル		選択時の条件	[+][−]条件[3]	レベル								備考 「利用ガイド」第4章も参照のこと
													−	＊	0	1	2	3	4	5	
B.1.1.1	性能・拡張性	業務処理量	ユーザ数	情報システムの利用者数。利用者は、庁内、庁外を問わず、情報システムを利用する人数を指す。 性能・拡張性を決めるための前提となる項目であると共にシステム環境を規定する項目でもある。また、パッケージソフトやミドルウェアのライセンス価格に影響することがある。	○		1	上限が決まっている	1	上限が決まっている	基幹系システムの場合は、業務ごとに特定のユーザが使用することを想定。		仕様の対象としない	ベンダーによる提案事項	特定ユーザのみ	上限が決まっている					【注意事項】 標準準拠システムにおけるメトリクス「ユーザ数」を検討する際は、レベルを選択した後にユーザ数を特定するのではなく、利用用途を踏まえてユーザ数の数値化をした上でレベルを特定する。 例1） 標準準拠システムの利用者は、一意のユーザ（ユーザA（担当課）、ユーザB（情報システム部門））であり、当分変更の余地はないため2名分を想定（レベルは「0:特定ユーザのみ」となる） 例2） 標準準拠システムの利用者は、担当分担や組織変更などの利用人数変更を考慮し、最大15名分あれば十分と想定（レベルは「1:上限が決まっている」となる） 数値化された内容によっては、用意するクラウドサービスについて高コストなものが求められる可能性があるため、精緻な数値化を行うとともに、要求する数値（レベル）の必要性を十分に検討する必要がある。 なお、ベンダーとの調整において、当該項目の数値化を要しない等の整理が行われた場合においては、必ずしも数値化を要するものとしない。 この場合、自治体は「＊:ベンダーによる提案事項」を選択し、ベンダーの提案事項を踏まえ検討する。
B.1.1.2	性能・拡張性	業務処理量	同時アクセス数	同時アクセス数とは、ある時点で情報システムにアクセスしているユーザ数のことである。 パッケージソフトやミドルウェアのライセンス価格に影響することがある。	○		1	同時アクセスの上限が決まっている	1	同時アクセスの上限が決まっている	特定のユーザがアクセスすることを想定。		仕様の対象としない	ベンダーによる提案事項	特定利用者の限られたアクセスのみ	同時アクセスの上限が決まっている					【注意事項】 標準準拠システムにおけるメトリクス「同時アクセス数」を検討する際は、レベルを選択した後に同時アクセス数を特定するのではなく、以下のように、利用用途を踏まえて同時アクセス数の数値化をした上でレベルを特定する。 例1） 標準準拠システムの同時アクセスは、特定の業務担当者のみが利用し、同時に最大2名がアクセスすることを想定 （レベルは「0:特定利用者の限られたアクセスのみ」となる） 例2） 標準準拠システムの同時アクセスは、業務の繁忙期などを鑑み、15名利用者がいる前提で、最大10名の同時アクセスが発生することを想定 （レベルは「1:同時アクセスの上限が決まっている」となる） 数値化された内容によっては、用意するクラウドサービスについて高コストなものが求められる可能性があるため、精緻な数値化を行うとともに、要求する数値（レベル）の必要性を十分に検討する必要がある。 なお、ベンダーとの調整において、当該項目の数値化を要しない等の整理が行われた場合においては、必ずしも数値化を要するものとしない。 この場合、自治体は「＊:ベンダーによる提案事項」を選択し、ベンダーの提案事項を踏まえ検討する。
B.1.1.3	性能・拡張性	業務処理量	データ量（項目・件数）	情報システムで扱うデータの件数及びデータ容量等。性能・拡張性を決めるための前提となる項目である。	○		0	すべてのデータ件数、データ量が明確である	1	主要なデータ件数、データ量のみが明確である	要件定義時には明確にしておく必要がある。		仕様の対象としない	ベンダーによる提案事項	すべてのデータ件数、データ量が明確である	主要なデータ件数、データ量のみが明確である					【レベル1】 主要なデータ量とは、情報システムが保持するデータの中で、多くを占めるデータのことを言う。 例えば、住民記録システムであれば住民データ・世帯データ・異動データ等がある。 なお、適切な構成でクラウドサービスを利用することで、拡張性を容易に確保することが考えられる。 【注意事項】 レベル0は標準準拠システムにおいて取り扱うすべてのデータ件数やデータ量が特定できている場合に選択する。 レベル1は標準準拠システムにおいて取り扱うすべてのデータ件数やデータ量を特定することが困難な場合（少なくとも主要なデータの件数やデータ量は明確になっている場合）に選択する。 レベル1の場合は、明確になっていないデータ件数やデータ量を考慮すると、システム設計中や運用中において、データ件数やデータ量が変わり得る。将来的なデータ容量枯渇やパフォーマンスなどの観点を考慮した構成の検討、および継続的なデータ件数やデータ量の監視を行う必要がある。 全部のデータ量が把握できていない場合は、国が示した「選択レベル」からレベルを上げることが考えられる。 数値化された内容によっては、用意するクラウドサービスについて高コストなものが求められる可能性があるため、精緻な数値化を行うとともに、要求する数値（レベル）の必要性を十分に検討する必要がある。 なお、ベンダーとの調整において、当該項目の数値化を要しない等の整理が行われた場合においては、必ずしも数値化を要するものとしない。 この場合、自治体は「＊:ベンダーによる提案事項」を選択し、ベンダーの提案事項を踏まえ検討する。

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	利用ガイドの解説[2]	選択レベル		本市の選択レベル		選択時の条件	[+][−]条件[3]	レベル								備考 「利用ガイド」第4章も参照のこと
													−	＊	0	1	2	3	4	5	
B.1.1.4	性能・拡張性	業務処理量	オンラインリクエスト件数	単位時間ごとの業務処理件数。性能・拡張性を決めるための前提となる項目である。	○		0	処理ごとにリクエスト件数が明確である	0	処理ごとにリクエスト件数が明確である	要件定義時には明確にしておく必要がある。		仕様の対象としない	ベンダーによる提案事項	処理ごとにリクエスト件数が明確である	主な処理のリクエスト件数のみが明確である					【レベル1】 主な処理とは情報システムが受け付けるオンラインリクエストの中で大部分を占めるものを言う。 例えば、住民記録システムの転入・転出処理などがある。 なお、適切な構成でクラウドサービスを利用することで、拡張性を容易に確保することが考えられる。 【注意事項】 レベル0は標準準拠システムにおいて処理ごとのリクエスト件数を特定できている場合に選択する。 レベル1は標準準拠システムにおいて処理ごとにリクエスト件数を特定することが困難な場合（少なくとも主要な処理のリクエスト件数は明確になっている場合）に選択する。 レベル1の場合は、明確になっていないオンラインリクエスト件数を鑑み、将来的なパフォーマンスなどの観点を考慮した構成の検討、および継続的なリクエスト件数の監視を行う必要がある。 全部のオンラインリクエスト件数が把握できていない場合は、国が示した「選択レベル」からレベルを上げることが考えられる。 数値化された内容によっては、用意するクラウドサービスについて高コストなものが求められる可能性があるため、精緻な数値化を行うとともに、要求する数値（レベル）の必要性を十分に検討する必要がある。 なお、ベンダーとの調整において、当該項目の数値化を要しない等の整理が行われた場合においては、必ずしも数値化を要するものとしない。 この場合、自治体は「＊:ベンダーによる提案事項」を選択し、ベンダーの提案事項を踏まえ検討する。
B.1.1.5	性能・拡張性	業務処理量	バッチ処理件数	バッチ処理により処理されるデータ件数。性能・拡張性を決めるための前提となる項目である。	○		0	処理単位ごとに処理件数が決まっている	1	主な処理の処理件数が決まっている	要件定義時には明確にしておく必要がある。		仕様の対象としない	ベンダーによる提案事項	処理単位ごとに処理件数が決まっている	主な処理の処理件数が決まっている					【レベル1】 主な処理とは情報システムが実行するバッチ処理の中で大部分の時間を占める物をいう。 例えば、人事給与システムや料金計算システムの月次集計処理などがある。 なお、適切な構成でクラウドサービスを利用することで、拡張性を容易に確保することが考えられる。 【注意事項】 バッチ処理件数は単位時間を明らかにして確認する。 全部のバッチ処理件数が把握できていない場合は、国が示した「選択レベル」からレベルを上げることが考えられる。 レベル0は標準準拠システムにおいて処理ごとの処理件数を特定できている場合に選択する。 レベル1は標準準拠システムにおいて処理ごとに処理件数を特定することが困難な場合（少なくとも主要な処理の処理件数は明確になっている場合）に選択する。 レベル1の場合は、明確になっていないオンライン処理件数を鑑み、将来的なパフォーマンスなどの観点を考慮した構成の検討、および継続的な処理件数の監視を行う必要がある。 数値化された内容によっては、用意するクラウドサービスについて高コストなものが求められる可能性があるため、精緻な数値化を行うとともに、要求する数値（レベル）の必要性を十分に検討する必要がある。 なお、ベンダーとの調整において、当該項目の数値化を要しない等の整理が行われた場合においては、必ずしも数値化を要するものとしない。 この場合、自治体は「＊:ベンダーによる提案事項」を選択し、ベンダーの提案事項を踏まえ検討する。
B.2.1.4	性能・拡張性	性能目標値	通常時オンラインレスポンスタイム	オンラインシステム利用時に要求されるレスポンス。 システム化する対象業務の特性を踏まえ、どの程度のレスポンスが必要かについて確認する。アクセスが集中するタイミングの特性や、障害時の運用を考慮し、通常時・アクセス集中時・縮退運転時ごとにレスポンスタイムを決める。具体的な数値は特定の機能又はシステム分類ごとに決めておくことが望ましい。（例：Webシステムの参照系/更新系/一覧系など）	○	P39	3	3秒以内	3	3秒以内	管理対象とする処理の中で、通常時の照会機能などの大量データを扱わない処理がおおむね目標値を達成できれば良いと想定。 [−] 遅くても処理出来れば良い場合、又は代替手段がある場合 [+] 運用の実現性を確認した上で、業務への支障が大きいことが明らかである場合	○	仕様の対象としない	ベンダーによる提案事項	規定しない	10秒以内	5秒以内	3秒以内	1秒以内		【注意事項】 すべての処理に適用するわけではなく、主な処理に適用されるものとする。 測定方法、調達範囲外の条件（例えばネットワークの状態等）については、ベンダーと協議し詳細を整理する必要が有る。 【レベル4】 1秒以内とした場合には、用意するハードウェアについて高コストなものを求める必要があるため、その必要性を十分に検討する必要がある。

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	利用ガイドの解説[2]	選択レベル		本市の選択レベル		選択時の条件	[+][−]条件[3]	レベル								備考 「利用ガイド」第4章も参照のこと
													−	*	0	1	2	3	4	5	
B.2.1.5	性能・拡張性	性能目標値	アクセス集中時のオンラインレスポンスタイム	オンラインシステム利用時に要求されるレスポンス。 システム化する対象業務の特性を踏まえ、どの程度のレスポンスが必要かについて確認する。アクセスが集中するタイミングの特性や、障害時の運用を考慮し、通常時・アクセス集中時・縮退運転時ごとにレスポンスタイムを決める。具体的な数値は特定の機能又はシステム分類ごとに決めておくことが望ましい。（例：Webシステムの参照系/更新系/一覧系など）	○	P40	2	5秒以内	2	5秒以内	管理対象とする処理の中で、ピーク時の照会機能などの大量データを扱わない処理がおおむね目標値を達成できれば良いと想定。 [−] 遅くても処理出来れば良い場合、又は代替手段がある場合 [+] 運用の実現性を確認した上で、業務への支障が大きいことが明らかである場合	○	仕様の対象としない	ベンダーによる提案事項	規定しない	10秒以内	5秒以内	3秒以内	1秒以内		【注意事項】 すべての処理に適用するわけではなく、主な処理に適用されるものとする。測定方法、アクセス集中時の条件については、ベンダーと協議し詳細を整理する必要が有る。 【レベル4】 1秒以内とした場合には、用意するハードウェアについて高コストなものを求める必要があるため、その必要性を十分に検討する必要がある。
B.2.2.1	性能・拡張性	性能目標値	通常時バッチレスポンス遵守度合い	バッチシステム利用時に要求されるレスポンス。 システム化する対象業務の特性を踏まえ、どの程度のレスポンス（ターンアラウンドタイム）が必要かについて確認する。更に、アクセスが集中するタイミングの特性や、障害時の運用を考慮し、通常時（※）・ピーク時・縮退運転時ごとに遵守度合いを決める、具体的な数値は特定の機能またはシステム分類ごとに決めておくことが望ましい。 （例：日次処理/月次処理/年次処理など） ※「通常時」とは、運用保守期間のうち、繁忙期間（住基業務であれば転入・転出の多い年度末・年度当初、個人住民税業務であれば確定申告時期・当初課税時期等）及び想定量を超える処理が発生した期間を除いた期間をいう。	○		2	再実行の余裕が確保できる	2	再実行の余裕が確保できる	管理対象とする処理の中で、通常時のバッチ処理を実行し、エラーが発生するなどして処理結果が不正の場合、再実行できれば良いと想定。		仕様の対象としない	ベンダーによる提案事項	遵守度合いを定めない	所定の時間内に収まる	再実行の余裕が確保できる				【注意事項】 再実行をしない場合又は代替手段がある場合は、国が示した「選択レベル」からレベルを下げることが考えられる。
B.2.2.2	性能・拡張性	性能目標値	アクセス集中時のバッチレスポンス遵守度合い	バッチシステム利用時に要求されるレスポンス。 システム化する対象業務の特性を踏まえ、どの程度のレスポンス（ターンアラウンドタイム）が必要かについて確認する。更に、アクセスが集中するタイミングの特性や、障害時の運用を考慮し、通常時・ピーク時・縮退運転時ごとに遵守度合いを決める、具体的な数値は特定の機能又はシステム分類ごとに決めておくことが望ましい。 （例：日次処理/月次処理/年次処理など）	○		2	再実行の余裕が確保できる	2	再実行の余裕が確保できる	管理対象とする処理の中で、ピーク時のバッチ処理を実行し、エラーが発生するなどして処理結果が結果が不正の場合、再実行できる余裕があれば良いと想定。 ピーク時に余裕が無くなる場合にはサーバ増設や処理の分割などを考慮する必要がある。		仕様の対象としない	ベンダーによる提案事項	遵守度合いを定めない	所定の時間内に収まる	再実行の余裕が確保できる				【注意事項】 再実行をしない場合又は代替手段がある場合は、国が示した「選択レベル」からレベルを下げることが考えられる。
C.1.1.1	運用・保守性	通常運用	運用時間（平日）	業務主管部門等のエンドユーザが情報システムを主に利用する時間。（サーバを立ち上げている時間とは異なる。）	○	P40	1	定時内での利用（1日8時間程度利用）	1	定時内での利用（1日8時間程度利用）	開庁時間を定時と想定。 ※住民記録システム等、開庁時間の定時内において常時利用するシステムにおいては、選択レベル未満のレベルを採用することは想定されない [−] 不定期に利用する情報システムの場合 [+]定時外も頻繁に利用される場合、頻繁ではないが計画された稼動延長がある場合	○	仕様の対象としない	ベンダーによる提案事項	規定無し（不定期利用）	定時内での利用（1日8時間程度利用）	繁忙期は定時外も頻繁に利用（1日12時間程度利用）	定時外も頻繁に利用（1日12時間程度利用）	24時間利用		【注意事項】 情報システムが稼働していないと業務運用に影響のある時間帯を示し、サーバを24時間立ち上げていても、それだけでは24時間無停止とは言わない。 一般的に、クラウドサービスにおいては、仮想サーバやコンテナなど、サービス起動時間に対して費用が発生する。運用時間を必要最低限に留め、サービスを停止させることでクラウドにかかるコストの削減が見込まれる。
C.1.1.2	運用・保守性	通常運用	運用時間（休日等）	休日等（土日/祝祭日や年末年始）に業務主管部門等のエンドユーザが情報システムを主に利用する時間。（サーバを立ち上げている時間とは異なる。）	○	P40	1	定時内での利用（1日8時間程度利用）	1	定時内での利用（1日8時間程度利用）	休日等の窓口開庁がある場合を想定。 [−] 休日の窓口開庁や休日出勤がない場合 [+] 定時外も頻繁に利用される場合	○	仕様の対象としない	ベンダーによる提案事項	規定無し（原則利用しない）	定時内での利用（1日8時間程度利用）	定時外も頻繁に利用（1日12時間程度利用）	24時間利用			【注意事項】 一般的に、クラウドサービスにおいては、仮想サーバやコンテナなど、サービス起動時間に対して費用が発生する。運用時間を必要最低限に留め、サービスを停止させることでクラウドにかかるコストの削減が見込まれる。
C.1.2.5	運用・保守性	通常運用	バックアップ取得間隔	バックアップ取得間隔	○	P41	4	日次で取得	4	日次で取得	全体バックアップは週次で取得する。しかし、RPO要件である、1日前の状態に戻すためには、毎日差分バックアップを取得しなければならないことを想定。 [−] RPOの要件が[−]される場合 [+] RPOの要件が[+]される場合	○	仕様の対象としない	ベンダーによる提案事項	バックアップを取得しない	システム構成の変更時など、任意のタイミング	月次で取得	週次で取得	日次で取得	同期バックアップ	【注意事項】 「全体バックアップ」の「全体」は「データの全体」を指し示す。

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	利用ガイドの解説[2]	選択レベル		本市の選択レベル		選択時の条件	[+][−]条件[3]	レベル								備考 「利用ガイド」第4章も参照のこと
													−	*	0	1	2	3	4	5	
C.4.3.1	運用・保守性	運用環境	マニュアル準備レベル	運用のためのマニュアルの準備のレベル。	○		2	情報システムの通常運用と保守運用のマニュアルを提供する	2	情報システムの通常運用と保守運用のマニュアルを提供する	運用をユーザが実施することを想定。 [−]通常運用に必要なオペレーションのみを説明した運用マニュアルのみ作成する場合、又はユーザーによる運用を想定していない場合 [+] ユーザ独自の運用ルールを加味した特別な運用マニュアルを作成する場合	○	仕様の対象としない	ベンダーによる提案事項	各製品標準のマニュアルを提供する	情報システムの通常運用のマニュアルを提供する	情報システムの通常運用と保守運用のマニュアルを提供する	ユーザのシステム運用ルールに基づくカスタマイズされたマニュアルを提供する			【レベル】 通常運用のマニュアルには、サーバ・端末等に対する通常時の運用（起動・停止等）にかかわる操作や機能についての説明が記載される。保守運用のマニュアルには、サーバ・端末等に対する保守作業（部品交換やデータ復旧手順等）にかかわる操作や機能についての説明が記載される。 障害発生時の一次対応に関する記述（系切り替え作業やログ収集作業等）は通常運用マニュアルに含まれる。バックアップからの復旧作業については保守マニュアルに含まれるものとする。 なお、クラウドサービス上でのメンテナンス（一部サービスの提供終了や廃棄を含む）への対応に関するマニュアルについても想定される。
C.4.5.1	運用・保守性	運用環境	外部システムとの接続有無	情報システムの運用に影響する他システムや外部システム（自治体が管理に関わらないシステム）との接続の有無に関する項目。	○		1	他システムと接続する	1	他システムと接続する	庁内基幹系システムとして、住基と税などのように連携する他システムが存在することを想定。 [−] データのやり取りを行う他システムが存在しない場合 [+] 外部システムに接続して、データのやり取りを行う場合	○	仕様の対象としない	ベンダーによる提案事項	他システムや外部システムと接続しない	他システムと接続する	外部システムと接続する				【注意事項】 庁外の民間クラウド等で稼動する場合でも、内部ネットワークで接続する場合は庁内のシステムと位置づけること。 また、接続する場合には、そのインターフェース（接続ネットワーク・通信方式・データ形式等）について確認すること。
C.5.2.2	運用・保守性	サポート体制	保守契約（ソフトウェア）の種類	保守が必要な対象ソフトウェアに対する保守契約の種類。	○		2	アップデート	2	アップデート	ソフトウェアがバージョンアップした場合に、ベンダーがアップデートすることを想定。 [−] アップデート権を必要としない場合、かつ、バージョンアップの要否を都度検討し、必要な場合に応じて別契約によりバージョンアップを行う場合	○	仕様の対象としない	ベンダーによる提案事項	保守契約を行わない	問い合わせ対応	アップデート				
D.1.1.2	移行性	移行時期	システム停止可能日時	移行作業計画から本稼働までのシステム停止可能日時。（例外発生時の切り戻し時間や事前バックアップの時間等も含むこと。）	○		4	利用の少ない時間帯（夜間など）	4	利用の少ない時間帯（夜間など）	業務が比較的少ない時間帯にシステム停止が可能。		仕様の対象としない	ベンダーによる提案事項	制約無し（必要な期間の停止が可能）	5日以上	5日未満	1日（計画停止日を利用）	利用の少ない時間帯（夜間など）	移行のためのシステム停止不可	【注意事項】 基幹業務システムにおいては、システム停止可能な日や時間帯が極めて限定的である。長期のシステム停止期間においても、システム停止可能日とその時間帯をあらかじめ定めておく必要がある。 なお、レベル5の「移行のためのシステム停止不可」は、一般的に並行稼働する複数システム間の移行において可能であり、移行作業に要する人的コストや必要機器等を考慮すると、移行リスクは低減できるが必要コストの負担が大きくなる可能性に留意すること。 停止可能日・時間を増やす場合は、国が示した「選択レベル」からレベルを下げることが考えられる。 【レベル】 レベル0は情報システムの制約によらず、移行に必要な期間のシステム停止が可能なことを示す。レベル1以上は、システム停止に関わる（業務などの）制約が存在する上での、システム停止可能日時を示す。レベルが高くなるほど、移行によるシステム停止可能な日や時間帯など、移行計画に影響範囲が大きい制約が存在することを示している。
D.3.1.1	移行性	移行対象（機器）	設備・機器の移行内容	移行前の情報システムで使用していた設備において、新システムで新たな設備に入れ替え対象となる移行対象設備の内容。	○	P44	3	移行対象設備・機器のシステム全部を入れ替える	3	移行対象設備・機器のシステム全部を入れ替える	業務アプリケーションも含めた移行がある。		仕様の対象としない	ベンダーによる提案事項	移行対象無し	移行対象設備・機器のハードウェアを入れ替える	移行対象設備・機器のハードウェア、OS、ミドルウェアを入れ替える	移行対象設備・機器のシステム全部を入れ替える	移行対象設備・機器のシステム全部を入れ替えて、さらに統合化する		【レベル】 移行対象設備・機器が複数あり、移行内容が異なる場合には、それぞれ合意すること。 【注意事項】 業務アプリケーション更改が無い場合は、国が示した「選択レベル」からレベルを下げることが考えられる。 業務アプリケーションの更改程度が大きい場合は、国が示した「選択レベル」からレベルを上げることが考えられる。
D.4.1.1	移行性	移行対象（データ）	移行データ量	旧システム上で移行の必要がある業務データの量（プログラム、移行データに含まれるPDFなどの電子帳票類を含む）。	○	P45	*	ベンダーによる提案事項	*	ベンダーによる提案事項	移行前システムのデータを抽出した上で、移行対象データを決定する必要がある。		仕様の対象としない	ベンダーによる提案事項	移行対象無し	1TB未満	10TB未満	10TB以上			【注意事項】 データベースの使用量をそのまま使用すると、ログデータなど移行には必要のないデータも含まれる場合がある。

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	利用ガイドの解説[2]	選択レベル	本市の選択レベル	選択時の条件	[+][−]条件[3]	レベル								備考 「利用ガイド」第4章も参照のこと
											−	*	0	1	2	3	4	5	
D.5.1.1	移行性	移行計画	移行のユーザ/ベンダー作業分担	移行作業の作業分担。	○		1 ユーザとベンダーと共同で実施	1 ユーザとベンダーと共同で実施	移行結果の確認等、一部を自治体職員が実施する形態を想定。 [+] 標準仕様準拠のシステムから標準仕様準拠のシステムに移行する場合	○	仕様の対象としない	ベンダーによる提案事項	すべてユーザ	ユーザとベンダーと共同で実施	すべてベンダー				【注意事項】 最終的な移行結果の確認は、レベルに関係なくユーザが実施する。なお、ユーザデータを取り扱う際のセキュリティに関しては、ユーザとベンダーで取り交わしを行うことが望ましい。 ベンダーに移行作業を分担する場合については、既存システムのベンダーと新規システムのベンダーの役割分担を検討する必要がある。 【レベル1】 共同で移行作業を実施する場合、ユーザ/ベンダーの作業分担を規定すること。特に移行対象データに関しては、旧システムの移行対象データの調査、移行データの抽出/変換、本番システムへの導入/確認、等について、その作業分担を規定しておくこと。
F.1.1.1	システム環境・エコロジー	システム制約/前提条件	構築時の制約条件	構築時の制約となる庁内基準や法令、各地方自治体の条例などの制約が存在しているかの項目。 例） ・政府機関の情報セキュリティ対策のための統一基準 ・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（総務省） ・個人情報保護法などシステムに関連する法令 ・ISO/IEC27000系 など	○		1 制約有り	1 制約有り	庁内規約などが存在する場合を想定。		仕様の対象としない	ベンダーによる提案事項	制約無し	制約有り					【注意事項】 情報システムを開発する際に、機密情報や個人情報等を取り扱う場合がある。これらの情報が漏洩するリスクを軽減するために、プロジェクトでは、情報利用者の制限、入退室管理の実施、取り扱い情報の暗号化等の対策が施された開発用環境を整備する必要が生じる。 また運用予定地での構築が出来ず、別地に環境設定作業場所を設けて構築作業を行った上で運用予定地に搬入しなければならない場合や、逆に運用予定地でなければ構築作業が出来ない場合なども制約条件となる。
F.1.2.1	システム環境・エコロジー	システム制約/前提条件	運用時の制約条件	運用時の制約となる庁内基準や法令、各地方自治体の条例などの制約が存在しているかの項目。 例） ・政府機関の情報セキュリティ対策のための統一基準 ・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（総務省） ・個人情報保護法などシステムに関連する法令 ・ISO/IEC27000系 など	○		1 制約有り	1 制約有り	設置に関して何らかの制限が発生するセンターやマシンルームを前提として考慮。ただし条件の調整などが可能な場合を想定。		仕様の対象としない	ベンダーによる提案事項	制約無し	制約有り					

1 クラウド調達時の扱い　○：クラウドの対象と成り得る項目　△：クラウドの対象となる場合がある項目　－：通常クラウドの対象とならない項目
なお、本項目でクラウド調達に必要な項目を網羅している訳ではない。

2 利用ガイドの解説　Pxx：利用ガイドのメトリクス詳細説明ページ

3 [+][−]条件　○：レベルの変更に条件がある項目

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	利用ガイドの解説[2]	選択レベル		本市の選択レベル		選択時の条件	[+][-]条件[3]	レベル								備考 「利用ガイド」第4章も参照のこと
													－	＊	0	1	2	3	4	5	
A.3.1.1	可用性	災害対策	復旧方針	地震、水害、テロ、火災などの大規模災害時の業務継続性を満たすための代替の機器として、どこに何が必要かを決める。	○	P48	2	同一の構成で情報システムを再構築	2	同一の構成で情報システムを再構築	災害発生後に調達したハードウェア等を使用し、同一の構成で情報システムを再構築することを想定 [-] 運用の実現性を確認した上で、限定された構成等で情報システムを再構築することが許容できる場合 [+] 運用の実現性を確認した上で、可用性を高めたい場合	○	仕様の対象としない	ベンダーによる提案事項	復旧しない	限定された構成で情報システムを再構築	同一の構成で情報システムを再構築	限定された構成をDRサイトで構築	同一の構成をDRサイトで構築		【レベル】 レベル1及び3の限定された構成とは、復旧する目標に応じて必要となる構成（例えば、冗長化の構成は省くなど）を意味する。 【注意事項】 データセンター等の庁舎外にサーバを設置する場合は、庁舎がDRサイトの位置づけとなる場合もある。 DR（Disaster Recovery）サイトとは、災害などで業務の続行が不可能になった際に、緊急の代替拠点として使用する施設や設備のこと。
A.3.2.1	可用性	災害対策	保管場所分散度（外部保管データ）	地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、データ・プログラムを運用サイトと別の場所へ保管する。	○		2	1ヶ所（遠隔地）	2	1ヶ所（遠隔地）	遠隔地1ヶ所 [+] 運用の実現性を確認した上で、可用性を高めたい場合	○	仕様の対象としない	ベンダーによる提案事項	外部保管しない	1ヶ所（近隣の別な建物）	1ヶ所（遠隔地）	2ヶ所（近隣の別な建物と遠隔地）	2ヶ所（遠隔地）		【注意事項】 ここで遠隔地とは、主系サーバ等の設置場所と同時被災の恐れがない遠隔地であり、庁舎等の利用場所から見ての遠隔地では無い。 A.3.2.2（保管方法（外部保管データ））と合わせて考慮し、整合するようにレベルを選択すること。
A.3.2.2	可用性	災害対策	保管方法（外部保管データ）	地震、水害、テロ、火災などの大規模災害発生により被災した場合に備え、データ・プログラムを運用サイトと別の場所へ保管するための方法。	○	P49	1	媒体による外部保管（バックアップ）、またはネットワーク経由でストレージへのリモートバックアップ	1	媒体による外部保管（バックアップ）、またはネットワーク経由でストレージへのリモートバックアップ	A.3.2.1と同じ拠点へのリモートバックアップを想定。 [+]媒体での外部保管とネットワーク経由でストレージへの遠隔保管による運用（バックアップ）の両方を必要とする場合	○	仕様の対象としない	ベンダーによる提案事項	外部保管（バックアップ）しない	媒体による外部保管（バックアップ）、またはネットワーク経由でストレージへのリモートバックアップ	媒体による外部保管（バックアップ）及びネットワーク経由でストレージへのリモートバックアップの兼用				【注意事項】 A.3.2.1（保管場所分散度(外部保管データ)）と合わせて考慮し、整合するようにレベルを選択すること。 近年のランサムウェアによるセキュリティインシデントが多発していることに鑑みると、リモートバックアップに加えて媒体による外部保管（バックアップ）を取得することも考えられる。
C.1.2.3	運用・保守性	通常運用	データ復旧の対応範囲	データの損失等が発生したときに、どのようなデータ損失に対して対応する必要があるかを示す項目。	○	P50	1	障害発生時のデータ損失防止	1	障害発生時のデータ損失防止	障害発生時に決められた復旧時点（RPO）へデータを回復できれば良い。 [+] 職員の作業ミスなどによって発生したデータ損失について運用の実現性を確認した上で業務への支障が起きることは明らかな場合	○	仕様の対象としない	ベンダーによる提案事項	バックアップを取得しない	障害発生時のデータ損失防止	職員の作業ミスなどによって発生したデータ損失防止				【注意事項】 職員が一度正常に処理したデータについては、回復するデータには含まれない。
C.1.3.1	運用・保守性	通常運用	監視情報	情報システム全体、あるいはそれを構成するハードウェア・ソフトウェア（業務アプリケーションを含む）に対する監視に関する項目。 監視とは情報収集を行った結果に応じて適切な宛先に発報することを意味する。本項目は、監視対象としてどのような情報を発信するべきかを決定することを目的としている。 セキュリティ監視については本項目には含めない。「E.7.1 不正監視」で別途検討すること。	○	P51	4	レベル3に加えてリソース監視を行う	4	レベル3に加えてリソース監視を行う	夜間の障害時にも、管理者に状況を通知し、すぐ対処が必要なのかどうかを判断するため、詳細なエラー情報まで監視を行うことを想定。 [-] 障害時は地方公共団体の情報システム管理者又は地方公共団体より運用業務を委託され管理権限を保持する事業者がすぐに情報システムにアクセスできるため、詳細なエラー情報まで監視する必要がない場合 [+] 通常よりも処理が集中されることが予想できパフォーマンス監視が必要な場合	○	仕様の対象としない	ベンダーによる提案事項	監視を行わない	死活監視を行う	レベル1に加えてエラー監視を行う	レベル2に加えてエラー監視（トレース情報を含む）を行う	レベル3に加えてリソース監視を行う	レベル4に加えてパフォーマンス監視を行う	【レベル】 死活監視とは、対象のステータスがオンラインの状態にあるかオフラインの状態にあるかを判断する監視のこと。 エラー監視とは、対象が出力するログ等にエラー出力が含まれているかどうかを判断する監視のこと。トレース情報を含む場合は、どのモジュールでエラーが発生しているのか詳細についても判断することができる。 リソース監視とは、対象が出力するログや別途収集するパフォーマンス情報に基づいてCPUやメモリ、ディスク、ネットワーク帯域といったリソースの使用状況を判断する監視のこと。 パフォーマンス監視とは、対象が出力するログや別途収集するパフォーマンス情報に基づいて、業務アプリケーションやディスクの入出力、ネットワーク転送等の応答時間やスループットについて判断する監視のこと。 【運用コストへの影響】 エラー監視やリソース監視、パフォーマンス監視を行うことによって、障害原因の追求が容易となったり、障害を未然に防止できるなど、情報システムの品質を維持するための運用コストが下がる。 また、定期報告会には、リソース監視結果、パフォーマンス監視結果の報告は必須ではない。

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	利用ガイドの解説[2]	選択レベル		本市の選択レベル		選択時の条件	[+][-]条件[3]	レベル								備考 「利用ガイド」第4章も参照のこと
													－	＊	0	1	2	3	4	5	
C.5.9.1	運用・保守性	サポート体制	定期報告会実施頻度	保守に関する定期報告会の開催の要否。	○		3	四半期に1回	4	月1回			仕様の対象としない	ベンダーによる提案事項	無し	年1回	半年に1回	四半期に1回	月1回	週1回以上	【注意事項】 業務ごとの定期報告会の頻度を指す。 また、障害発生時に実施される不定期の報告会は含まない。 保守に関する報告事項が予め少ないと想定される場合、国が示した「選択レベル」からレベルを下げることが考えられる。 保守に関する報告事項が予め多いと想定される場合、国が示した「選択レベル」からレベルを上げることが考えられる。
C.5.9.2	運用・保守性	サポート体制	報告内容のレベル	定期報告会において報告する内容の詳しさを定める項目。	○		3	障害及び運用状況報告に加えて、改善提案を	3	障害及び運用状況報告に加えて、改善提案を	障害発生時など改善提案が必要な場合を想定		仕様の対象としない	ベンダーによる提案事項	無し	障害報告のみ	障害報告に加えて運用状況報告を行う	障害及び運用状況報告に加えて、改善提案を行う			
C.6.2.1	運用・保守性	その他の運用管理方針	問い合わせ対応窓口の設置有無	ユーザの問い合わせに対して単一の窓口機能を提供するかどうかに関する項目。	○	P52	1	ベンダーの既設コールセンターを利用する	1	ベンダーの既設コールセンターを利用する	サポート契約を締結するベンダーの既設コールセンターが問い合わせ対応窓口となることを想定		仕様の対象としない	ベンダーによる提案事項	問い合わせ対応窓口の設置について規定しない	ベンダーの既設コールセンターを利用する	ベンダーの常駐等専用窓口を設ける				【注意事項】 ここでは、ユーザとベンダー間における問い合わせ窓口の設置の有無について確認する。問い合わせ対応窓口機能の具体的な実現方法については、別途に具体化する必要が有る。 問い合わせ対応窓口を設置する必要がない場合は、国が示した「選択レベル」からレベルを下げることが考えられる。 運用の実現性を確認した上で、常駐作業員がいないと適切な保守・運用ができないと考えられる場合は、国が示した「選択レベル」からレベルを上げることが考えられる。
C.6.3.1	運用・保守性	その他の運用管理方針	インシデント管理の実施有無	システムで発生するインシデントの管理を実施するかどうかを確認する。インシデント管理の実現方法については、有無の確認後に具体化して確認する。	△		2	ベンダーに委託し、既存のインシデント管理のプロセスに従う	2	ベンダーに委託し、既存のインシデント管理のプロセスに従う	運用管理業務のうちインシデントに対する管理として求める内容。		仕様の対象としない	ベンダーによる提案事項	インシデント管理について規定しない	自治体において実施し、既存のインシデント管理のプロセスに従う	ベンダーに委託し、既存のインシデント管理のプロセスに従う	ベンダーに委託し、新規にインシデント管理のプロセスを規定する			【注意事項】 運用管理契約を行わない場合は、国が示した「選択レベル」からレベルを下げることが考えられる。 新たにプロセスを作成する必要がある場合（既存のプロセスを見直す場合を含む）は、国が示した「選択レベル」からレベルを上げることが考えられる。
C.6.4.1	運用・保守性	その他の運用管理方針	問題管理の実施有無	インシデントの根本原因を追究するための問題管理を実施するかどうかを確認する。問題管理の実現方法については、有無の確認後に具体化して確認する。	△		2	ベンダーに委託し、既存の問題管理のプロセスに従う	2	ベンダーに委託し、既存の問題管理のプロセスに従う	運用管理業務のうち問題管理に対する管理として求める内容。		仕様の対象としない	ベンダーによる提案事項	問題管理について規定しない	自治体において実施し、既存の問題管理のプロセスに従う	ベンダーに委託し、既存の問題管理のプロセスに従う	ベンダーに委託し、新規に問題管理のプロセスを規定する			【注意事項】 運用管理契約を行わない場合は、国が示した「選択レベル」からレベルを下げることが考えられる。 新たにプロセスを作成する必要がある場合（既存のプロセスを見直す場合を含む）は、国が示した「選択レベル」からレベルを上げることが考えられる。
C.6.5.1	運用・保守性	その他の運用管理方針	構成管理の実施有無	リリースされたハードウェアやソフトウェアが適切にユーザ環境に構成されているかを管理するための構成管理を実施するかどうかを確認する。構成管理の実現方法については、有無の確認後に具体化して確認する。	△		2	ベンダーに委託し、既存の構成管理のプロセスに従う	2	ベンダーに委託し、既存の構成管理のプロセスに従う	運用管理業務のうち構成管理に対する管理として求める内容。 [-]運用管理契約を行わない場合 [+]新たにプロセスを作成する必要がある場合（既存のプロセスを見直す場合を含む）	○	仕様の対象としない	ベンダーによる提案事項	構成管理について規定しない	自治体において実施し、既存の構成管理のプロセスに従う	ベンダーに委託し、既存の構成管理のプロセスに従う	ベンダーに委託し、新規に構成管理のプロセスを規定する			
C.6.6.1	運用・保守性	その他の運用管理方針	変更管理の実施有無	ハードウェアの交換やソフトウェアのパッチ適用、バージョンアップ、パラメータ変更といったシステム環境に対する変更を管理するための変更管理を実施するかどうかを確認する。変更管理の実現方法については、有無の確認後に具体化して確認する。	△		2	ベンダーに委託し、既存の変更管理のプロセスに従う	2	ベンダーに委託し、既存の変更管理のプロセスに従う	運用管理業務のうち変更管理に対する管理として求める内容。		仕様の対象としない	ベンダーによる提案事項	変更管理について規定しない	自治体において実施し、既存の変更管理のプロセスに従う	ベンダーに委託し、既存の変更管理のプロセスに従う	ベンダーに委託し、新規に変更管理のプロセスを規定する			【注意事項】 運用管理契約を行わない場合は、国が示した「選択レベル」からレベルを下げることが考えられる。 新たにプロセスを作成する必要がある場合（既存のプロセスを見直す場合を含む）は、国が示した「選択レベル」からレベルを上げることが考えられる。
C.6.7.1	運用・保守性	その他の運用管理方針	リリース管理の実施有無	承認された変更が正しくシステム環境に適用されているかどうかを管理するリリース管理を実施するかどうかを確認する。リリース管理の実現方法については、有無の確認後に具体化して確認する。	△		2	ベンダーに委託し、既存のリリース管理のプロセスに従う	2	ベンダーに委託し、既存のリリース管理のプロセスに従う	運用管理業務のうちリリース管理に対する管理として求める内容。		仕様の対象としない	ベンダーによる提案事項	リリース管理について規定しない	自治体において実施し、既存のリリース管理のプロセスに従う	ベンダーに委託し、既存のリリース管理のプロセスに従う	ベンダーに委託し、新規にリリース管理のプロセスを規定する			【注意事項】 運用管理契約を行わない場合は、国が示した「選択レベル」からレベルを下げることが考えられる。 新たにプロセスを作成する必要がある場合（既存のプロセスを見直す場合を含む）は、国が示した「選択レベル」からレベルを上げることが考えられる。
D.1.1.1	移行性	移行時期	システム移行期間	移行作業開始から本稼働までのシステム移行期間。	○		4	2年未満	4	2年未満	年度を跨いで移行を進める必要がある。		仕様の対象としない	ベンダーによる提案事項	システム移行無し	3ヶ月未満	半年未満	1年未満	2年未満	2年以上	【注意事項】 期間短縮の場合は、国が示した「選択レベル」からレベルを下げることが考えられる。 さらに長期期間が必要な場合は、国が示した「選択レベル」からレベルを上げることが考えられる。

項番	大項目	中項目	メトリクス（指標）	メトリクス説明	クラウド調達時の扱い[1]	利用ガイドの解説[2]	選択レベル		本市の選択レベル		選択時の条件	[+][-]条件[3]	レベル								備考 「利用ガイド」第4章も参照のこと
													－	＊	0	1	2	3	4	5	
D.1.1.3	移行性	移行時期	並行稼働の有無	移行作業から本稼働までのシステムの並行稼働の有無。	○		1	有り	1	有り	移行のためのシステム停止期間が少ないため、移行時のリスクを考慮して並行稼働は必要。		仕様の対象としない	ベンダーによる提案事項	無し	有り					【レベル1】 並行稼働有りの場合には、その期間、方法等を規定すること。 【注意事項】 移行のためのシステム停止期間が確保可能であり、並行稼働しない場合、国が示した「選択レベル」からレベルを下げることが考えられる。
E.3.1.2	セキュリティ	セキュリティ診断	Webアプリケーション診断実施の有無	Webアプリケーション診断とは、Webサイトに対して行うWebサーバやWebアプリケーションに対するセキュリティ診断のこと。	○		1	実施	1	実施	内部ネットワーク経由での攻撃に対する脅威が発生する可能性があるため対策を講じておく必要がある。		仕様の対象としない	ベンダーによる提案事項	不要	実施					【注意事項】 内部犯を想定する必要がない場合、インターネットに接続したWebアプリケーションを用いない場合、国が示した「選択レベル」からレベルを下げることが考えられる。

1　クラウド調達時の扱い　　○：クラウドの対象と成り得る項目　　△：クラウドの対象となる場合がある項目　　－：通常クラウドの対象とならない項目
なお、本項目でクラウド調達に必要な項目を網羅している訳ではない。

2　利用ガイドの解説　　Pxx：利用ガイドのメトリクス詳細説明ページ

3　[+][-]条件　　○：レベルの変更に条件がある項目

行政情報の取扱いに関する特記仕様書

1　行政情報

(1) 行政情報の範囲

この契約において，「行政情報」とは，仙台市行政情報セキュリティーポリシー第１章（２）⑧に定めるものをいい，仙台市（以下「発注者」という。）が貸与したもののほか，受注者が収集し，又は作成したもの（成果物，成果物の途中にあるもの等）も含むものとする。

(2) 行政情報の取扱い

この契約において，行政情報の取扱いとは，行政情報に関する収集，記入，編集，加工，修正，更新，検索，入力，蓄積，変換，合算，分析，複写，複製，保管，保存，搬送，伝達，出力，消去，廃棄などの一切の行為をいう。

2　行政情報の適正な取扱い

(1) 秘密の保持

受注者は，この契約の履行に関して知り得た秘密を他人に漏らしてはならない。

(2) 再委託の禁止

受注者は，業務の処理を他に委託し又は請け負わせてはならない。ただし，発注者の書面による承諾を得た場合は，この限りでない。

(3) 委託目的以外の使用及び第三者への提供の禁止

① 受注者は，この契約による事務に関して知り得た行政情報をみだりに他人に知らせ，又は不当な目的に使用してはならない。この契約が終了し，又は解除された後においても同様とする。

② 受注者は，その使用する者に対し，在職中及び退職後においてもこの契約による事務に関して知り得た行政情報をみだりに他人に知らせ，又は不当な目的に使用してはならないことなど，行政情報の取り扱いに関して必要な事項を周知しなければならない。

(4) 複写及び複製の禁止又は制限

受注者は，発注者の指示又は承諾があるときを除き，この契約による事務を処理するために発注者から貸与された行政情報が記録された資料等を複写し，又は複製してはならない。

(5) 事故発生時における報告義務

受注者は，行政情報を記録している媒体に滅失，盗難，改ざんその他の事故が発生したときは，直ちに，当該事故の経緯及び被害状況を調査し，必要な措置を講じ，速やかに発注者に報告し，発注者の指示に従うものとする。契約が終了し，又は解除された後においても同様とする。

(6) 行政情報の消去等

受注者は，この契約が終了し，又は解除された際には，この契約の履行に供した行政情報を記録した記録媒体については，①または②の方法により適切に措置するものとし，③の方法で報告する。

① 米国国立標準技術研究所が規定する方式，又はそれと同等以上の品質を定義した方式に準拠したデータ消去ソフトを用い，当該行政情報が記録された記録媒体のデータ消去を行うこと。

(a) データ消去の回数は，準拠する消去方式が求める回数以上とする。

(b) データ消去の実施後は，行政情報を記録していた媒体（シリアル番号または製造番号，型式などが判別できるもの）ならびに適切にデータ消去が完了したことを示す画面表示を，証拠資料として写真撮影すること。

② データ消去ソフトによる行政情報の消去が行い難い場合は，米国国立標準技術研究所が規定する方式，又はそれと同等以上の品質を定義した方式に準拠した方法により，物理破壊また

は暗号化技術を利用した消去を行うものとする。

(a)　物理破壊には磁気によるデータ消去を含むものとする。

(b)　磁気によるデータ消去は，米国国家安全保障局が規定する最新の方式により行うこと。

(c)　特殊機材等，代替性に乏しく高額製品であり，物理破壊を実施する機会費用が大である場合は，当該製品の製造会社等が推奨する方法により実施すること。但し，当該製造会社等が推奨する方法の妥当性・合理性について確認できる書証等の提供を受けるものとする。

(d)　データ消去の実施後は，行政情報を記録していた媒体（シリアル番号または製造番号，型式などが判別できるもの）を，証拠資料として写真撮影すること。

③ 以下の起算日から 5 営業日以内に「データ消去報告書」を本市に提出すること。

	庁舎外に持ち出して①または②を実施	左記以外の場合
起 算 日	庁舎外への持ち出し日	①または②の実施日

(a)　報告書には，記録媒体名（型式）や台数，消去実施日，方法（方式）などを明記し，証拠写真を添付すること。

(b)　データ消去の対象となる記録媒体が多数におよび，5 営業日を超える場合は，別途「データ消去計画書」を作成し，適切に工程管理を行うこと。

(c)　記録媒体の処理数が大量にあることに伴い，上記(b)の計画期間が長期（1 か月以上）に及ぶ場合は、データ消去が完了したものより順次「データ消去報告書」を提出するものとする。

3　立会い及び実地調査

(1) 作業への立会い

①　受注者は，この契約の履行に係る行政情報の取扱いの作業について，発注者が立会いを求める場合は，これを拒否してはならない。

ただし，受注者自身の情報保護措置に支障をきたす等の正当な理由がある場合は，その理由を明示して，発注者の立会いを拒否することができる。

②　発注者は，①のただし書きにより，作業への立会いを拒否された場合は，受注者に対して作業状況の報告を求めることができる。

(2) 行政情報の取扱いに関する調査

①　発注者は，この契約の履行に係る行政情報の取扱いの状況について，受注者の作業場所その他の施設について，定期又は不定期に調査を行うことができる。

この契約が終了し，又は解除された場合においては，この契約の履行に係る行政情報の取扱いに関する事項に限り，受注者に対して調査を行うことができる。

②　受注者は，①の調査を拒否してはならない。

ただし，受注者自身の情報保護措置に支障をきたす等の正当な理由がある場合は，その理由を明示するとともに，この契約の履行に係る行政情報の取扱いが適正であることを証明したときに限り，発注者の調査を拒否できる。

4　契約解除及び損害賠償

(1) 契約解除

発注者は，受注者が本特記仕様書に定める義務を履行しない場合は，本特記仕様書に関連する委託業務の全部又は一部を解除することができる。

(2) 損害賠償

受注者は，(1) の規定により契約が解除されたことにより発注者に損害を及ぼしたときは，その損害を賠償しなければならない。

別記

個人情報等の取扱いに関する特記仕様書

1　定義

（1）個人情報

個人情報の保護に関する法律第2条第1項(仙台市議会における業務を委託する場合にあっては，仙台市議会の個人情報の保護に関する条例第2条第1項）に規定する個人情報をいう。

（2）死者情報

死者に関する情報であって，当該情報に含まれる氏名，生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ，それにより，特定の個人を識別することができることとなるものを含む。）をいう。

（3）個人情報等

個人情報及び死者情報を総称していう。

2　個人情報等の適正な取扱い

（1）個人情報等の取扱い

この契約において，「個人情報等の取扱い」とは，個人情報等に関する収集，記入，編集，加工，修正，更新，検索，入力，蓄積，変換，合算，分析，複写，複製，保管，保存，搬送，伝達，出力，消去，廃棄等の一切の行為をいう。

（2）個人情報等の適正な取扱いに関する規定の遵守

受注者は，この契約の履行に伴う個人情報等の取扱いについて，個人情報の保護に関する法律又は仙台市議会の個人情報の保護に関する条例及び仙台市死者情報保護事務取扱要綱の趣旨に則り，業務委託契約書に規定する個人情報等の保護に関する事項を遵守しなければならない。

（3）個人情報等の取扱いについての再委託の禁止

受注者は，この契約の履行に伴う個人情報等の取扱いについて，再委託をしてはならない。
ただし，特別な事情があると発注者が認めた場合はこの限りではない。

（4）個人情報等の適正な取扱いの確保に関する調査票の遵守

受注者は，発注者に提出した個人情報等の適正な取扱いの確保に関する調査票に記載した事項を遵守しなければならない。

3　個人情報等の取扱いを行う場所及び作業内容

（1）作業場所及び作業内容

個人情報等の取扱いを行う場所（以下「作業場所」という。）及び作業内容は，別紙「個人情報等の取扱いに係る作業場所及び作業内容に関する届」のとおりとする。

（2）届の提出等

受注者は，「個人情報等の取扱いに係る作業場所及び作業内容に関する届」を，個人情報等の取扱いに係る作業の開始前までに発注者に提出しなければならない。

（３）作業場所等の変更

受注者は，作業場所又は作業内容について変更しようとする場合は，変更の理由を付して発注者に書面で申し入れ，変更後の作業場所又は作業内容について，発注者による事前の調査及び承認を受けなければならない。

なお，作業場所の変更には，別の場所への切替えのほか，区画，部屋等の仕切りの変更，設備の改造等を含む。

４　個人情報等の取扱いに係る体制

（１）管理監督者

①　管理監督者とは，個人情報等保護責任者及び，作業責任者をいう。

②　個人情報等の取扱いに係る作業の管理監督者は，別紙「個人情報等の取扱いに係る管理監督者に関する届」（以下「管理監督者届」という。）のとおりとする。

（２）作業従事者

個人情報等の取扱いに係る作業従事者は，別紙「個人情報等の取扱いに係る作業従事者に関する届」（以下「作業従事者届」という。）のとおりとする。

（３）誓約書

受注者は，管理監督者及び作業従事者に対して，個人情報等の取扱いに関する遵守事項を周知し，社内において，個人情報等の適正な取扱いに関して誓約書に押印させ，提出させなければならない。

（４）届等の提出等

受注者は，管理監督者届，作業従事者届及び誓約書の写しを，個人情報等の取扱いに係る作業の開始前までに発注者に提出しなければならない。

（５）管理監督者又は作業従事者に関する変更等

①　受注者は，管理監督者又は作業従事者について変更し，追加し，又は減少させようとする場合は，変更等の理由を付して発注者に書面で申し入れ，管理監督者又は作業従事者の変更等について，発注者の事前の承認を受けなければならない。

管理監督者又は作業従事者に関する事項（役職，氏名，経歴，資格，作業内容，所属，身分その他個人情報等の保護に関して重要な事項）について変更しようとする場合も同様とする。

②　①による管理監督者又は作業従事者の変更等にあたっては，申入れの書面に，変更後の管理監督者届，作業従事者届及び誓約書（誓約書については，変更又は追加された管理監督者又は作業従事者の分に限る。）を添付しなければならない。

（６）第三者による個人情報等の取扱いの禁止等

①　受注者は，（４）の届に記載した者又は（５）の発注者の承認を受けた者以外の個人及び法人その他の団体（以下「第三者」という。）に，個人情報等の取扱いを行わせてはならない。

②　受注者は，この契約の履行において，第三者に個人情報等の取扱いを行わせる必要があると判断するときは，その理由を付して発注者に書面で申し入れ，当該第三者による個人情報等の取扱いについて，発注者の事前の承認を受けなければならない。

５　個人情報等の受渡し，搬送

（１）個人情報等の受渡し

①　受注者は，個人情報等の受渡し（納品，貸与品の返却に伴うものを含む。以下同じ。）について，

その日時，場所，担当者，内容，数量等の必要な事項を計画として定め，当該計画を記載した書面を発注者に提出しなければならない。

② 発注者及び受注者は，現に個人情報等の受渡しを行う場合には，その日時，場所，担当者，内容，数量等の必要な事項について記録した書面を作成し，受渡し完了後に発注者と受注者双方の署名，押印等をもって確認するものとする。

（2）個人情報等の搬送

① 受注者は，個人情報等の搬送について，その日時，経路，担当者，荷物の梱包状況，使用車両，交通手段等の必要な事項を計画として定め，当該計画を記載した書面を発注者に提出しなければならない。

② 発注者及び受注者は，現に個人情報等の搬送を行う場合には，その日時，経路，担当者，荷物の梱包状況，使用車両，交通手段等の必要な事項について記録した書面を作成し，搬送完了後に発注者と受注者双方の署名，押印等をもって確認するものとする。

（3）計画の変更等

受注者は，個人情報等の受渡し及び搬送に関する計画を変更しようとする場合は，変更後の計画を記載した書面を発注者に提出しなければならない。

（4）計画を記載した書面等の統合

個人情報等の受渡し及び搬送に関する計画を記載した書面（変更に係るものを含む。）及び現に個人情報等の受渡し及び搬送を行う場合の記録の書面は，発注者と受注者の協議により，これらの書面の全部若しくは一部又はこの契約の履行に係る他の書面と統合して作成し，使用することができる。

6 個人情報等の保護に関する計画

（1）人的，物理的及び技術的な保護に関する措置の計画

受注者は，個人情報等の取扱いにあたっての人的，物理的及び技術的な保護に関する以下の措置について具体的な計画を定め，当該計画を記載した書面を発注者に提出し，事前に発注者の承認を受けなければならない。

・個人情報等の保護，適正な取扱いに関する遵守事項の周知（周知文の配付，掲示等）
・個人情報等の保護に関する研修等の実施
・管理監督者の作業への立会い・監督等の体制の整備（管理監督者の人数，立会い時間，作業の開始・終了，休憩時間の監督体制等）
・作業場所等における管理監督者及び作業従事者の表示（名簿の作成，掲示等）
・管理監督者，作業従事者，訪問者等第三者の識別（識別票の携行，名札の着用等）
・作業場所で従事している者の把握（出欠の表示等）
・作業分担の周知・確認（作業分担表の作成，掲示，配付等）
・作業従事者の入替わり・交代の手順（入替わり・交代に要する時間，業務の引継ぎ・確認等）
・作業場所への出入の管理（守衛，ＩＤカード等による入室権限の確認等）
・作業場所の施錠の管理（施錠者・開錠者の指定，鍵の保管方法等）
・作業に使用する機器類（主にパソコン，外付けドライブ等の情報機器等）の限定・特定（種類・性能，台数等の確認，複数業務の同時並行処理の禁止等）
・持込み・持出し品等の管理（出入者，許可者，日時，目的，持出し・持込み物品の記録等）
・個人情報等の保管方法（耐火保管庫の設置・利用，保管庫の鍵の管理等）
・個人情報等の管理方法（保管場所からの持出し，返却方法等）
・個人情報等の不正な複製，複写等の防止（持ち運び型の電磁的記録媒体への記録・複製の権限管理，紙媒体の複写の権限管理等）

・防犯（守衛による巡視，機械による監視等）
・防火（防火責任者の指定等）
・物品紛失，盗難等の防止（端末等のワイヤー固定，外部記録媒体等の物品の数量管理等）
・個人情報等への不正なアクセスの防止（ＩＤ・パスワードによる権限確認，アクセス記録の作成・保管，ネットワークからの独立等）
・個人情報等の送信防止（電子メール等による個人情報等の送信の防止等）
・個人情報等の改ざん・破壊・漏えい等の防止（ウィルスチェックの実施，作業機器への不要なソフトウェアの導入禁止等）
・事故・障害による被害の拡大防止（バックアップの適切な取得，バックアップの保管方法，補助電源の設置等）
・事故・障害発生時の緊急連絡体制の整備（発注者・受注者・その他の関係者等の連絡網の作成，周知等）
・作業状況の報告（作業日報の作成，定期的又は発注者の要求に応じた作業状況の報告等）
・作業上不要な情報の消去，廃棄等（消去・廃棄方法の指定とその確認・記録等）
・契約の終了・解除又は発注者の指示による貸与品の返却，成果品の納品，複写物等の消去・廃棄等（返却・納品・消去・廃棄方法の指定とその確認・記録等）

（２）受注者の工夫等
① （１）の措置の事項は例示であって，受注者が，この契約の履行にあたり特に必要とされる措置又は受注者の工夫による保護の措置について計画することを妨げない。
② 受注者は，（１）の措置について，これらを複合的に実施し，個人情報等の保護をより確実なものとしなければならない。

（３）計画の変更等
受注者は，個人情報等の保護に関する計画を変更しようとする場合は，変更後の計画を記載した書面を発注者に提出し，事前に発注者の承認を受けなければならない。

（４）計画の是正等
① 発注者は，受注者の提出した計画を記載した書面（変更に係るものを含む。）について，個人情報等の保護に関する措置として不十分な点があると認めるときは，受注者に是正を求めることができる。
② 受注者は，発注者による是正の要求に対して，速やかに対応しなければならない。

7 立会い，実地調査等

（１）作業への立会い
① 受注者は，この契約の履行に係る個人情報等の取扱いの作業について，発注者が立会いを求める場合は，これを拒否してはならない。
ただし，受注者自身の情報保護措置に支障をきたす等の正当な理由がある場合は，その理由を明示して，発注者の立会いを拒否することができる。
② 発注者は，①のただし書きにより，作業への立会いを拒否された場合は，受注者に対して作業状況の報告を求めることができる。

（２）個人情報等の取扱いに関する調査
① 発注者は，この契約の履行に係る個人情報等の取扱いの状況について，受注者の作業場所その他の施設について，定期又は不定期に調査を行うことができる。
この契約が終了し，又は解除された場合においては，この契約の履行に係る個人情報等の取扱

いに関する事項に限り，受注者に対して調査を行うことができる。

② 受注者は，①の調査を拒否してはならない。

ただし，受注者自身の情報保護措置に支障をきたす等の正当な理由がある場合は，その理由を明示するとともに，この契約の履行に係る個人情報等の取扱いが適正であることを証明したときに限り，発注者の調査を拒否できる。

（３）個人情報等の取扱いに関する改善指導

①発注者は，（２）に規定する調査により，受注者の個人情報等の取扱いに不適切な点を認めたときは，受注者に対して，必要な是正措置をとるべきことを請求することができる。

②受注者は，発注者による是正措置の請求に対して，速やかに対応しなければならない。

特定個人情報等の取扱いに関する特記事項

第 1 条（特定個人情報等の保護に関する法令等の遵守）

受託者は、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号。以下「番号法」という。）、個人情報保護委員会が定める特定個人情報の適正な取扱いに関するガイドライン（以下「ガイドライン」という。）に基づき、本特定個人情報等の取扱いに関する特記事項（以下「特記事項」という。）を遵守しなければならない。また、これらのほか、個人情報の保護に関する法律（平成 15 年法律第 57 号）及び仙台市議会の個人情報の保護に関する条例（令和 5 年仙台市条例第 29 号）並びに仙台市死者情報保護事務取扱要綱（令和 5 年 3 月 24 日総務局長決裁）の趣旨に則り、特記事項を遵守しなければならない。

第 2 条（責任体制の整備）

受託者は、特定個人情報及び個人番号（以下「特定個人情報等」という。）の安全管理について、内部における責任体制を構築し、その体制を維持しなければならない。

第 3 条（作業責任者等の届出）

1　受託者は、特定個人情報等の取扱いに係る作業責任者及び作業従事者を定め、書面により発注者に報告しなければならない。
2　受託者は、特定個人情報等の取扱いに係る作業責任者及び作業従事者を変更する場合の手続を定めなければならない。
3　受託者は、作業責任者を変更する場合は、事前に書面により発注者に申請し、その承認を得なければならない。
4　受託者は、作業従事者を変更する場合は、事前に書面により発注者に報告しなければならない。
5　作業責任者は、特記事項に定める事項を適切に実施するよう作業従事者を監督しなければならない。
6　作業従事者は、作業責任者の指示に従い、特記事項に定める事項を遵守しなければならない。

第 4 条（取扱区域の特定）

1　受託者は、特定個人情報等を取り扱う場所（以下「取扱区域」という。）を定め、業務の着手前に書面により発注者に報告しなければならない。
2　受託者は、取扱区域を変更する場合は、事前に書面により発注者に申請し、その承認を得なければならない。
3　受託者は、発注者が指定した場所へ持ち出す場合を除き、特定個人情報等を定められた場所から持ち出してはならない。

第 5 条（教育の実施）

1　受託者は、特定個人情報等の保護、情報セキュリティに対する意識の向上、特記事項における作業従事者が遵守すべき事項その他本委託業務の適切な履行に必要な教育及び研修を、作業従事者全員に対して実施しなければならない。

2　受託者は、前項の教育及び研修を実施するに当たり、実施計画を策定し、実施体制を確立しなければならない。

第 6 条（守秘義務）

1　受託者は、本委託業務の履行により直接又は間接に知り得た特定個人情報等を第三者に漏らしてはならない。契約期間満了後又は契約解除後も同様とする。

2　受託者は、本委託業務に関わる作業責任者及び作業従事者に対して、秘密保持に関する誓約書を提出させなければならない。

第 7 条（再委託）

1　受託者は、本委託業務を第三者へ委託（以下「再委託」という。）してはならない。

2　受託者は、本委託業務の一部をやむを得ず再委託する必要がある場合は、再委託先の名称、再委託する理由、再委託して処理する内容、再委託先において取り扱う情報、再委託先における安全性及び信頼性を確保する対策並びに再委託先に対する管理及び監督の方法を明確にした上で、業務の着手前に、書面により再委託する旨を発注者に申請し、その承認を得なければならない。

3　前項の場合、受託者は、再委託先に本契約に基づく一切の義務を遵守させるとともに、発注者に対して、再委託先の全ての行為及びその結果について責任を負うものとする。

4　受託者は、再委託先との契約において、再委託先に対する管理及び監督の手続及び方法について具体的に規定しなければならない。

5　受託者は、再委託先に対して本委託業務を委託した場合は、その履行状況を管理・監督するとともに、発注者の求めに応じて、管理・監督の状況を発注者に対して適宜報告しなければならない。

第 8 条（派遣労働者等の利用時の措置）

1　受託者は、本委託業務を派遣労働者、契約社員その他の正社員以外の労働者に行わせる場合は、正社員以外の労働者に本契約に基づく一切の義務を遵守させなければならない。

2　受託者は、発注者に対して、正社員以外の労働者の全ての行為及びその結果について責任を負うものとする。

第 9 条（特定個人情報等の管理）

受託者は、本委託業務において利用する特定個人情報等を保持している間は、ガイドラインに定める各種の安全管理措置を遵守するとともに、次の各号の定めるところにより、特定個人情報等の管理を行わなければならない。

一　個人番号を取り扱う事務、特定個人情報等の範囲及び同事務に従事する作業従事者を明確化し、取扱規程等を策定すること。

二　組織体制の整備、取扱規程等に基づく運用、取扱状況を確認する手段の整備、情報漏えい等事案に対応する体制の整備、取扱状況の把握及び安全管理措置の見直しを行うこと。

三　事務取扱担当者の監督・教育を行うこと。

四　特定個人情報等を取り扱う区域の管理、機器及び電子媒体等の盗難等の防止、電子媒体等の取扱いにおける漏えい等の防止、個人番号の削除・機器及び電子媒体等の廃棄を行うこと。

五　アクセス制御、アクセス者の識別と認証、外部からの不正アクセス等の防止、情報漏えい等の防止を行うこと。

第 10 条（提供された特定個人情報等の目的外利用及び第三者への提供の禁止）

受託者は、本委託業務において利用する特定個人情報等について、本委託業務以外の目的で利用してはならない。また、第三者へ提供してはならない。

第 11 条（受渡し）

受託者は、発注者受託者間の特定個人情報等の受渡しに関しては、発注者が指定した手段、日時及び場所で行った上で、発注者に特定個人情報等の預り証を提出しなければならない。

第 12 条（特定個人情報等の返還又は廃棄）

1　受託者は、本委託業務の終了時に、本委託業務において利用する特定個人情報等について、発注者の指定した方法により、返還又は廃棄を実施しなければならない。

2　受託者は、本委託業務において利用する特定個人情報等を消去又は廃棄する場合は、事前に消去又は廃棄すべき特定個人情報等の項目、媒体名、数量、消去又は廃棄の方法及び処理予定日を書面により発注者に申請し、その承諾を得なければならない。

3　受託者は、特定個人情報等の消去又は廃棄に際し発注者から立会いを求められた場合は、これに応じなければならない。

4　受託者は、本委託業務において利用する特定個人情報等を廃棄する場合は、当該情報が記録された電磁的記録媒体の物理的な破壊その他当該特定個人情報等を判読不可能とするのに必要な措置を講じなければならない。

5　受託者は、特定個人情報等の消去又は廃棄を行った後、消去又は廃棄を行った日時、担当者名及び消去又は廃棄の内容を記録し、書面により発注者に対して報告しなければならない。

第 13 条（定期報告及び緊急時報告）

1　受託者は、発注者から、特定個人情報等の取扱いの状況について報告を求められた場合は、直ちに報告しなければならない。

2　受託者は、特定個人情報等の取扱いの状況に関する定期報告及び緊急時報告の手順を定めなければならない。

第 14 条（監査及び検査）

1　発注者は、本委託業務に係る特定個人情報等の取扱いについて、本契約の規定に基づき必要な措置が講じられているかどうか検証及び確認するため、受託者及び再委託先に対して、監査又は検査を行うことができる。

2　発注者は、前項の目的を達するため、受託者に対して必要な情報を求め、又は本委託業務の処理に関して必要な指示をすることができる。

第 15 条（事故時の対応）

1　受託者は、本委託業務に関し特定個人情報等の漏えい等の事故（番号法違反又はそのおそれのある事案を含む。）が発生した場合は、その事故の発生に係る帰責の有無に関わらず、直ちに発注者に対して、当該事故に関わる特定個人情報等の内容、件数、事故の発生場所、発生状況等を書面により報告し、発注者の指示に従わなければならない。

2　受託者は、特定個人情報等の漏えい等の事故が発生した場合に備え、発注者その他の関係者との連絡、証拠保全、被害拡大の防止、復旧、再発防止の措置を迅速かつ適切に実施するために、緊急時対応計画を定めなければならない。

3　発注者は、本委託業務に関し特定個人情報等の漏えい等の事故が発生した場合は、必要に応じて当該事故に関する情報を公表することができる。

第 16 条（契約解除）

1　発注者は、受託者が本特記事項に定める義務を履行しない場合は、本特記事項に関連する委託業務の全部又は一部を解除することができる。

2　受託者は、前項の規定による契約の解除により損害を受けた場合においても、発注者に対して、その損害の賠償を請求することはできないものとする。

第 17 条（損害賠償）

受託者の故意又は過失を問わず、受託者が本特記事項の内容に違反し、又は怠ったことにより、発注者に対する損害を発生させた場合は、受託者は、発注者に対して、その損害を賠償しなければならない。