仕　様　書

１　業務名

広島市ガバメントクラウド利用基盤（ＡＷＳ）の構築及び運用・保守業務

２　履行期間

契約締結日から令和１５年３月３１日までとする。

⑴　設計・構築業務

契約締結日から令和１０年３月３１日まで

⑵　運用・保守業務

令和１０年４月１日から令和１５年３月３１日まで

３　履行場所

広島市企画総務局行政経営部システム基盤課（広島市中区国泰寺町一丁目４番２１号)、その他本市が指定又は承認する場所

４　業務の目的

令和３年９月施行の「地方公共団体情報システムの標準化に関する法律」に基づき、標準化対象事務についてガバメントクラウドの利用に努めることとされ、さらに令和７年３月改正の「情報通信技術を活用した行政の推進等に関する法律」に基づき、情報システムの整備に当たっては、ガバメントクラウドの利用を検討し、その結果に基づく取組を行うよう努めることとされたことを踏まえ、健康福祉局健康福祉企画課が健康管理等システム及び被爆者援護システムの更新に当たってガバメントクラウド（※）を利用する事を決定した。

これを受け、本業務は、本市がガバメントクラウド（ＡＷＳ）において、効率的に標準準拠システム等を構築し運用するために必要な共通機能を、広島市ガバメントクラウド利用基盤（ＡＷＳ）として構築しその運用・保守を行うものである。

※　Ｃｌｏｕｄ　Ｓｅｒｖｉｃｅ　Ｐｒｏｖｉｄｅｒ（以下「ＣＳＰ」という。）のうち、Ａｍａｚｏｎ　Ｗｅｂ　Ｓｅｒｖｉｃｅｓ（以下「ＡＷＳ」という。）の環境（以下「ガバメントクラウド（ＡＷＳ)」という。）を利用した共同利用方式

５　広島市ガバメントクラウド利用基盤（ＡＷＳ）の基本要件

⑴　構築する場所

ア　広島市ガバメントクラウド利用基盤（ＡＷＳ）は、ガバメントクラウド（ＡＷＳ）において、本市に管理者権限が付与される利用領域（以下「広島市利用領域（ＡＷＳ）」という。）に構築し、運用・保守すること。

イ　東京リージョンをメインサイト、大阪リージョンをバックアップサイトとする。

ウ　広島市ガバメントクラウド利用基盤（ＡＷＳ）は、東京リージョンに構築すること。

エ　広島市ガバメントクラウド利用基盤（ＡＷＳ）のバックアップは、大阪リージョンに保管すること。

⑵　構成等

ア　本市では、現在、基幹系システム等を民間のデータセンターに構築したプライベートクラウドで運用しており、今後、ＡＷＳ以外のＣＳＰが提供するガバメントクラウドを利用する可能性もあるため、広島市ガバメントクラウド利用基盤（ＡＷＳ）は、概ね図１に示す構成とすること。詳細は設計において決定する。

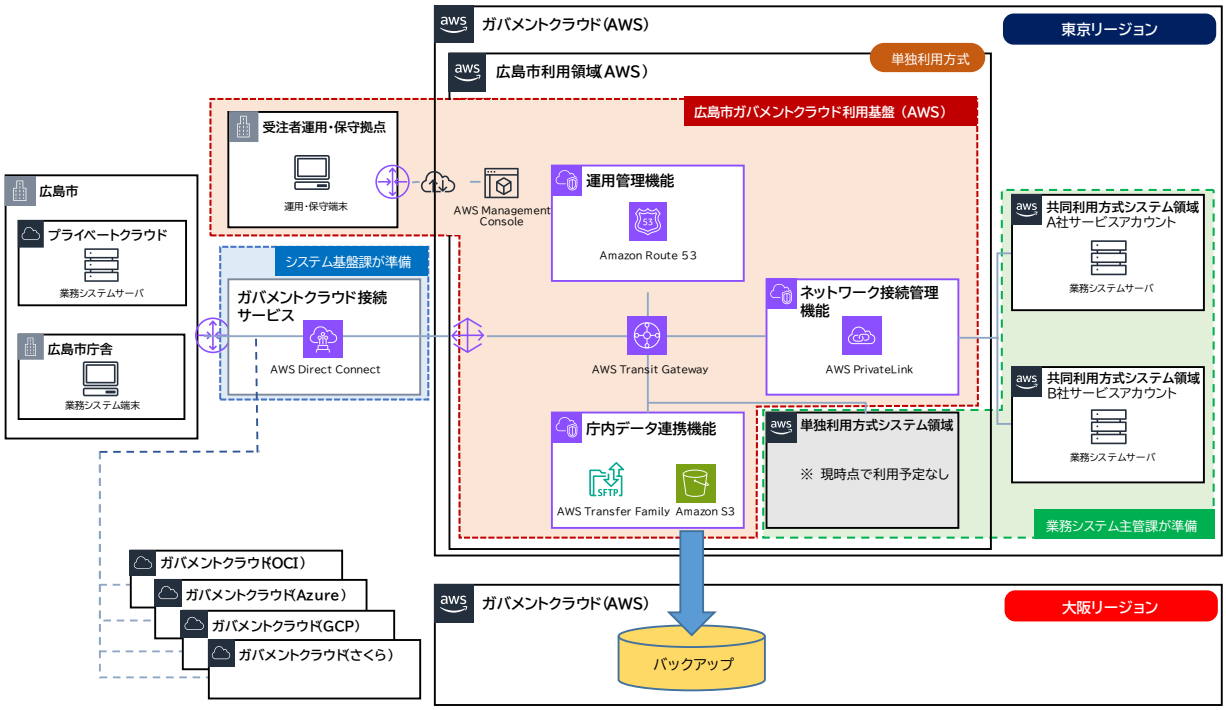

図１　広島市ガバメントクラウド利用基盤（ＡＷＳ）の概要図

イ　本市が別途準備するガバメントクラウド接続サービスと接続し、本市のプライベートクラウドにある共通基盤と、ガバメントクラウド（ＡＷＳ）の共同利用方式システム領域及び広島市利用領域（ＡＷＳ）の単独利用方式システム領域に構築する業務システムとデータ連携を行うこと。

ウ　本市が別途準備するガバメントクラウド接続サービスと接続し、本市の施設にある業務システムの端末から、ガバメントクラウド（ＡＷＳ）の共同利用方式システム領域及び広島市利用領域（ＡＷＳ）の単独利用方式システム領域に構築する業務システムが利用できること。

エ　広島市ガバメントクラウド利用基盤（ＡＷＳ）は、２４時間３６５日サービスを提供できるよう稼動すること。ただし、本市が承認した保守作業等で稼動を停止することは可能とする。

⑶　関係者との協議・調整

必要に応じて、次の関係者と、協議・調整すること。

ア　共同利用方式システム領域及び単独利用方式システム領域に、業務システムを構築し運用・保守を行う事業者

イ　業務システム主管課

ウ　ガバメントクラウド接続サービスを提供する事業者

エ　本市プライベートクラウドを構成するデータセンター、共通基盤、仮想化基盤及び庁内ＬＡＮを、それぞれ構築し運用・保守をしている各事業者

オ　デジタル庁

カ　ＣＳＰ

⑷　利用アカウント

ア　受注者には、広島市利用領域（ＡＷＳ）のうち、広島市ガバメントクラウド利用基盤（ＡＷＳ）のアカウントの利用権限を付与する。

イ　受注者は、ガバメントクラウドへの接続に必要な多要素認証（以下「ＭＦＡ」という。）に用いるハードウェアデバイスを必要数準備すること。なお、必要数には本市職員分を含めないこと。

ウ　ＣＳＰ環境の管理インターフェースへのＳＳＯに際して、アクセス元制御を実施するため、Ｇｏｏｇｌｅ社が提供するＣｈｒｏｍｅ　Ｅｎｔｅｒｐｒｉｓｅ　Ｐｒｅｍｉｕｍ（ＣＥＰ）ライセンスに関して、受注者が必要とする数を把握し、ＧＣＡＳアカウントへの紐づけ作業及びＣＥＰライセンスの管理を行うこと。

⑸　広島市ガバメントクラウド利用基盤（ＡＷＳ）を利用する業務システム

ア　共同利用方式システム領域及び単独利用方式システム領域に構築する業務システムが、新たに広島市ガバメントクラウド利用基盤（ＡＷＳ）と接続する場合は、対応すること。

イ　共同利用方式システム領域及び単独利用方式システム領域に構築する業務システムが実施する各種テストを支援するなど積極的に協力すること。

ウ　現在、健康管理等システム及び被爆者援護システムが、共同利用方式システム領域において、それぞれ令和１０年４月、令和１１年４月から利用することが決定している。

⑹　ガイドライン等の作成・支援

ア　共同利用方式 ASP 事業者、単独利用方式 ASP 事業者等が本市でガバメントクラウドを利用する際に参照するガイドラインを作成すること。

イ　ガイドラインを作成する際は、最低限、次の内容を含めること。

(ｱ)　本書の位置付け、背景・目的

(ｲ)　広島市利用領域の全体概要

(ｳ)　広島市ガバメントクラウド利用基盤（ＡＷＳ）、標準準拠システム等の責任分界点

(ｴ)　広島市ガバメントクラウド利用基盤（ＡＷＳ）の機能

(ｵ)　広島市におけるガバメントクラウド（ＡＷＳ）の利用手続（申請フロー、ルール、留意事項等）

(ｶ) 障害対応に係る事項
(ｷ) 各種申請様式　等

ウ　広島市ガバメントクラウド利用基盤（ＡＷＳ）の情報セキュリティ対策を適正に実施するため、本市において、管理体制や各種手順等を定める「情報セキュリティ実施手順」を作成するので、受注者は、必要な情報の提供などの支援を行うこと。

⑺ 構成管理

ア　ＣＳＰのマネージドサービス等を活用し、広島市ガバメントクラウド利用基盤（ＡＷＳ）におけるリソースを適切に管理するとともに、あわせて適切に構成管理を行うこと。

イ　ＩａＣ等のコード群についても各種構成管理ツールを利用し、適切に構成管理を行うこと。

ウ　本業務で作成した文書等について、適切に構成管理を行うこと。

⑻ ドキュメント管理

広島市ガバメントクラウド利用基盤（ＡＷＳ）の設定変更等を行った場合は、設計書、ガイドライン等の関連する文書等を最新化すること。

⑼ 性能管理・キャパシティ管理・コスト管理

ア　本市と協議の上、月ごとの予算と使用料金の閾値を設定し、閾値を超過した場合に本市が指定する者にメールにより通知すること。

イ　広島市ガバメントクラウド利用基盤（ＡＷＳ）のリソースの使用料金及びｖＣＰＵ利用率・ストレージ使用量・通信量等の稼動実績を、デジタル庁から提供されるツール又は受注者が整備するツール等を用いて収集・整理し、月次で報告すること。

ウ　報告の中では、ネットワーク、サーバ、サービス等の区分ごとの内訳を明確にするとともに、ＣＳＰが提供するツールから得られる情報等を参考に、広島市ガバメントクラウド利用基盤（ＡＷＳ）の構成やコストが最適化されるよう改善提案を行うこと。

⑽ その他

ア　デジタル庁から運用管理補助者が実施すべきとして通知があり、追加で実施すべき業務が発生した場合などは、本市と受注者で協議の上、対応を決定すること。

イ　契約締結後、本市が実施するデジタル庁へのガバメントクラウド利用申請に必要な情報を本市に提供するとともに、申請資料の作成を支援すること。

ウ　環境構築においては、原則、ＣＳＰのマネージドサービスを利用することとし、次のような運用作業の負担軽減に繋がる構成とするよう配慮すること。

(ｱ) 継続的なリソースモニタリング及びリソース使用量に応じた広島市ガバメントクラウド利用基盤（ＡＷＳ）の最適化
(ｲ) アクセス管理や監視（ログ、死活、ネットワーク、稼動状況等）の利用
(ｳ) その他情報セキュリティ対策、バックアップ運用等

６　ハードウェア要件

⑴ デジタル庁が示す「ガバメントクラウド利用における推奨構成ＡＷＳ編」を踏まえて、広島市ガバメントクラウド利用基盤（ＡＷＳ）に必要な広島市利用領域（ＡＷＳ）のリソースを設計すること。

⑵ ⑴の設計を基に本市の承認の下、広島市利用領域（ＡＷＳ）のリソースを使用して、環境設定

などの必要な作業を行い、広島市ガバメントクラウド利用基盤（ＡＷＳ）を構築すること。

⑶　ガバメントクラウド（ＡＷＳ）とガバメントクラウド接続サービス以外に、必要なハードウェアを整備し運用・保守すること。

７　ソフトウェア要件

ガバメントクラウド（ＡＷＳ）とガバメントクラウド接続サービス以外に、必要なソフトウェアを整備し運用・保守すること。

８　ネットワーク要件

⑴　ネットワーク管理

ア　広島市利用領域（ＡＷＳ）のネットワークを適切に管理すること。なお、業務システム内部のネットワークについては、業務システム事業者が管理する。

イ　本市が提供する利用可能なＣＩＤＲ情報を基に、広島市利用領域（ＡＷＳ）のＣＩＤＲ体系を確立し、これに則って運用等すること。

ウ　本市の施設のフロントオフィスシステムネットワークに接続した業務システムの端末から、広島市ガバメントクラウド利用基盤（ＡＷＳ）を経由して、共同利用方式システム領域及び単独利用方式システム領域に設置している業務システムが利用できるようネットワークの環境を構築及び運用・保守をするとともに管理すること。

⑵　ネットワーク接続管理機能

ア　本市が別途準備するガバメントクラウド接続サービスと接続し、本市のプライベートクラウド等の本市の施設、ＡＷＳ以外のＣＳＰが提供するガバメントクラウド等と適切な通信を行うこと。

イ　本市からの申請を受けて、本市が別途準備するガバメントクラウド接続サービスと接続し、本市のプライベートクラウド等の本市の施設、ＡＷＳ以外のＣＳＰが提供するガバメントクラウド等と適切な通信が適切に行えるよう設定の追加、変更、削除などの管理を行うこと。

⑶　受注者運用・保守拠点との接続

ア　広島市利用領域（ＡＷＳ）のＡＷＳ　Ｍａｎａｇｅｍｅｎｔ　Ｃｏｎｓｏｌｅ（以下「管理コンソール」という。）へは、インターネット経由で接続すること。

イ　管理コンソールへの接続に当たっては、「広島市情報セキュリティポリシー」等を遵守すること。

ウ　本市が許可した端末のみが、広島市ガバメントクラウド利用基盤（ＡＷＳ）の管理コンソールに接続できるようにすること。

エ　インターネット経由から広島市ガバメントクラウド利用基盤（ＡＷＳ）へのアクセスは、管理コンソールだけとすること。

９　機能要件

⑴　アカウント管理

ア　広島市利用領域（ＡＷＳ）におけるアカウントの管理方法及び単独利用方式システム領域に業務システムを構築し運用・保守を行う事業者等に対してアカウントを払い出す際のルールを

策定すること。

イ　広島市利用領域（ＡＷＳ）のアカウントの払い出しを行うこと。

ウ　単独利用方式システム領域に、業務システムを構築し運用・保守を行う事業者に対してアカウントの払い出し、ユーザ情報及び権限情報の管理を適切に行うこと。

エ　受注者が利用しているアカウントについて、ユーザ情報及び権限情報の管理を行うこと。

オ　アカウントの払い出しを行う上で、本市からデジタル庁に対して申請が必要となるため、デジタル庁に報告する申請内容の準備・作成の支援を行うこと。

⑵　運用管理機能（名前解決及び時刻同期）

ア　広島市利用領域（ＡＷＳ）内で名前解決、時刻同期が行えること。

イ　名前解決機能は、ＣＳＰのマネージドサービスを利用すること。

ウ　時刻同期機能は、ＣＳＰのマネージドサービスを利用すること。

⑶　庁内データ連携機能

ア　「地方公共団体情報システム共通機能標準仕様書」の庁内データ連携機能に準拠したファイル連携が行えること。

イ　データ保管領域はオブジェクトストレージで構成し、ＡＷＳ　Ｔｒａｎｓｆｅｒ　Ｆａｍｉｌｙ等のＣＳＰのマネージドサービスを利用してＳＦＴＰで接続できるようにすること。詳細な要件については、「地方公共団体情報システム共通機能標準仕様書」の機能要件、「ファイル連携に関する詳細技術仕様書」等を参照すること。

ウ　データ連携に当たっては、認証・認可、通信経路の暗号化、保存データの暗号化を行うこと。

エ　本市からの申請を受けて、庁内データ連携機能のバケットの作成、変更、削除等の管理、権限設定などを行うこと。

オ　共同利用方式システム領域及び単独利用方式システム領域に構築する業務システム等が、データ連携を行うために必要となる作業等を行うこと。

⑷　セキュリティ管理

ア　広島市ガバメントクラウド利用基盤（ＡＷＳ）のセキュリティリスクを低減させるための指針の策定、予防対策等を行うこと。

イ　広島市ガバメントクラウド利用基盤（ＡＷＳ）の各種サービスにおいて、クラウドサービス利用における責任共有モデル上、サービス利用者の責任範囲とされるものについて、脆弱性対応を適宜実施すること。

ウ　セキュリティに関するマネージドサービス（ＡＷＳ　Ｓｅｃｕｒｉｔｙ　Ｈｕｂ／Ａｍａｚｏｎ　ＧｕａｒｄＤｕｔｙ等）を活用し、ＣＳＰのベストプラクティスに従ったセキュリティ対策が実施されていることを確認するとともに、当該サービスからアラートが発報された場合は、そのアラートの内容に従い、設定変更等の必要な作業を実施すること。

エ　デジタル庁によるテンプレートの変更があった場合に、本市と協議の上、変更されたテンプレートを速やかに適用すること。

⑸　システム監視

ア　広島市ガバメントクラウド利用基盤（ＡＷＳ）の各種サービスの稼動状況を一元的に常時監視すること。

イ　死活監視に加え、リソースの利用状況やスループット等のパフォーマンスの状況を一元的に

常時監視すること。

ウ　障害発生を検知した際に、自動で障害状況等を通知すること。

⑹　バックアップ・リストア管理

ア　広島市ガバメントクラウド利用基盤（ＡＷＳ）のシステム障害等に備え、バックアップを取得すること。

イ　東京リージョンで取得したバックアップデータを大阪リージョンへコピーして保管すること。

ウ　東京リージョンで大規模障害等が発生した場合は、東京リージョンの復旧を待った後、大阪リージョンのバックアップデータから復元させることを基本とするが、東京リージョンが長期間復旧しない場合は、本市の指示に従い、大阪リージョンにＩａＣにより復元させること。

エ　障害が発生した場合に、広島市ガバメントクラウド利用基盤（ＡＷＳ）をＩａＣにより迅速に復旧できることを前提にバックアップすること。

オ　広島市ガバメントクラウド利用基盤（ＡＷＳ）の設定変更の都度、バックアップを取得すること。

⑺　ログ管理

ア　広島市利用領域（ＡＷＳ）内でのシステム障害やインシデント対応に備え、広島市ガバメントクラウド利用基盤（ＡＷＳ）で導入する各種サービスのログを一元的に収集、保存、管理すること。

イ　各種ログの分析を行い、本市の求めに応じて状況等を報告すること。

⑻　テンプレート適用管理

ア　本市と協議の上、必要に応じて、デジタル庁から提供される「サンプルテンプレート」を基に、セキュリティや運用の適切性を踏まえた本市独自のテンプレート（以下「独自テンプレート」という。）を作成すること。

１０　非機能要件

「別紙　非機能要件一覧」の要件を満たすこと。

１１　サービスレベル合意（ＳＬＡ）

⑴　受注者は、本システムの利用期間を通して安定したサービスを本市が受けられることを目的とし、本システムの利用開始前に本市とＳＬＡ（Ｓｅｒｖｉｃｅ　Ｌｅｖｅｌ　Ａｇｒｅｅｍｅｎｔ）を締結し、受注者はその遵守と継続的なサービス品質の改善に努めること。

⑵　ＳＬＡは「別紙　非機能要件一覧」を満たすものとし、締結されたＳＬＡに基づき、サービス品質を維持すること。

１２　業務の内容

⑴　プロジェクト管理

受注者は、本業務が適切に実施されるよう、全ての工程におけるプロジェクト管理を徹底すること。具体的には、各作業の進捗状況の把握、課題・問題点の早期発見と解決策の検討、本市への迅速な状況報告等を行うこと。

ア　委託業務実施計画書の作成

(ｱ)　契約締結日から１０日以内に広島市委託契約約款第６条に規定する委託業務実施計画書を作成し、本市の承認を得ること。

(ｲ)　委託業務実施計画書には、作業方法、現場責任者の氏名・連絡先、業務従事者の氏名・連絡先、役割分担、過去の業務従事実績、作業実施体制、実施スケジュールを記載し、作業体制及び全体スケジュールを明確にすること。

(ｳ)　委託業務実施計画書を変更する必要があるときは、本市の承認を得た上で計画を変更し、変更後の委託業務実施計画書を提出すること。

(ｴ)　委託業務実施計画書は、電子データにて本市に提出すること。

イ　誓約書等の作成

契約締結後、速やかに次の資料を作成し、本市の承認を得ること。

- 本市の情報の秘密保護に関する誓約書
- 現場責任者選任届
- 業務着手届
- 作業場所に関する届出

ウ　Ｗｏｒｋ　Ｂｒｅａｋｄｏｗｎ　Ｓｔｒｕｃｔｕｒｅ（以下「WBS」という。）の作成

委託業務実施計画書の提出後、速やかにプロジェクトの詳細タスクを記したＷＢＳを作成し、提出するとともに、定義したスケジュールに基づき進捗状況を管理すること。

エ　委託業務実施報告書等の作成

(ｱ)　契約書に定める支払期終了時に、完了した業務の業務履行完了日、提出した成果物の一覧を記述した委託業務実施報告書を提出すること。

(ｲ)　次の管理項目でプロジェクトに関する各種管理を行うとともに、定期的（月１回以上）に本業務の進捗状況に関する報告書（以下「進捗報告書」という。）を作成した上で、定例会で報告すること。

- 進捗管理
- 問合せ管理
- 成果物管理
- 変更管理
- 情報セキュリティ管理
- リスク課題管理
- 品質管理
- コミュニケーション管理
- 貸与物等管理

オ　プロジェクト管理を円滑に行うため、次の要件を満たすＳａａＳ型のプロジェクト管理ツールを導入し、本市と受注者間のコミュニケーション手段として活用してもよいこととする。

(ｱ)　ＩＳＭＡＰクラウドサービスリストに登録のあるＳａａＳ、又はＩＳＭＡＰクラウドサービスリストに登録されたＩａａＳ若しくはＰａａＳ上に構築されたＳａａＳであること。

(ｲ)　プロジェクト管理ツールの開発元がＩＳＯ／ＩＥＣ　２７０１７及びＩＳＯ／ＩＥＣ２７０１８を取得していること。

(ｳ)　プロジェクト管理ツールの提供に係るセキュリティ統制について、以下のいずれかにより第三者評価を確認できること。

・　ツール開発元が、ＡＩＣＰＡ　ＳＯＣ２/ＳＯＣ３の監査フレームワーク又は経済産業省が策定した「情報セキュリティサービス基準（情報セキュリティ監査サービス）」に基づく第三者機関が評価したレポートを保有していること。

・　ツール開発元が利用するクラウド基盤（ＩａａＳ/ＰａａＳ）が、ＡＩＣＰＡ　ＳＯＣ２/ＳＯＣ３等の第三者機関の評価を受けていること、かつ、ツール開発元がアプリケーション層及び運用面のセキュリティ統制に関する説明資料を提示できること。

(ｴ)　プロジェクト管理ツールで扱う情報資産の保管場所が日本国内に限定されること。

(ｵ)　プロジェクト管理ツールにかかる経費は全て受注者が負担すること。

(ｶ)　プロジェクト管理ツールの認証は、多要素認証であること。

カ　会議体の開催

(ｱ)　表１に記載する会議体を開催すること。表１に記載のない会議体であっても、調整先関係者との調整などで必要とされるものがある場合は、積極的に提案し開催すること。なお、議題の重要度に応じて、開催方式（対面・リモート）を選択すること。

表１　会議体

会議体	開催頻度	目的	出席者
キックオフ会議	１回	本業務開始時に、本業務全体に関する進捗管理、課題管理、リスク管理等について確認を行う。	・本市（責任者含む） ・受注者（責任者含む）
定例会議	月１回以上	本業務全体に関する進捗管理、課題管理、リスク管理等について報告、協議を行う。	・本市 ・受注者
個別検討会議	週次	作業内容、個別の課題・リスク等について協議を行う。	・本市 ・受注者
稼動判定会議	本番稼動開始前	全ての設計・構築の作業が完了し、本番稼動を開始するかどうか判定を行う。	・本市（責任者含む） ・受注者（責任者含む）
ステアリングコミッティ	必要に応じて開催	本業務の遂行に重大な影響を及ぼす課題、リスク、仕様変更、スケジュール変更等について協議し、対応方針及び意思決定を行う。	・本市（責任者含む） ・受注者（責任者含む）

(ｲ)　受注者は、会議に必要な書類等を会議の５開庁日前を目途に作成し、事前に本市担当職員へ送付すること。なお、会議終了後は、会議内容を議事録に取りまとめ、会議終了後５開庁日までに本市へ報告し、その承諾を得ること。

(ｳ)　会議開催に当たっては、本市職員の負担を加味し、複数の会議を同日開催するなど、効率的に運営するための施策を講じること。

キ　課題管理

(ｱ)　会議等で取り上げた課題については、議事録とは別に課題管理表にまとめること。

(ｲ)　課題管理表は、受注者が対応・回答すべきもの、本市が対応・回答すべきものに分け、それぞれ対応・回答期限を明記すること。

(ｳ)　課題は期限内に対応すること。もし期限内に対応できないものがあれば、本市の承認を得た上で対応期限を変更すること。

ク　リスク管理

(ｱ)　業務の遂行に影響を及ぼすリスクを識別し、リスク管理一覧として管理すること。

(ｲ)　識別したリスクは定期的に状況を確認し本市に報告するとともに、必要に応じて対策を講じること。

ケ　品質管理

(ｱ)　受注者は、委託業務実施計画書を本市が承認した後、速やかに品質管理計画表を作成し提出すること。

(ｲ)　品質管理計画表には、本システムの品質を保証するためのテスト実施計画や成果物の品質を評価するための品質管理指標、各品質管理指標に対する目標値、品質評価・分析方法、報告タイミング等を定義すること。

(ｳ)　受注者は品質管理計画表に基づき、各工程における品質状況を本市が判断できるよう、進捗報告書やテスト結果報告書に取りまとめた上で報告すること。

(ｴ)　設計書等のドキュメントの提出に当たっては、受注者内で十分な品質確認（レビュー）を実施すること。

(ｵ)　本市で確認（レビュー）が必要なドキュメントについては、事前に確認の観点や判断すべき事項を明確にした上で、十分な説明を行うこと。

(ｶ)　レビューで受けた指摘は適時レビュー指摘事項一覧表に記録するとともに、工程終了時にはレビュー結果報告書に取りまとめて提出すること。

コ　本市からの資料提供

(ｱ)　本業務の実施に当たり必要と思われる資料及びデータは、本市が提供する。

(ｲ)　受注者は、本市から提供された資料及びデータを本契約に基づく業務を処理する目的のためのみに用いるものとし、本市の許可なくして複写又は複製してはならない。

(ｳ)　本業務が終了したとき、本市の求めがあったとき、又は本業務に必要がなくなったときは、本市から提供された資料及びデータ（本市の許可を得て複写・複製したものも含む。）を本市に返却すること。

⑵　設計・構築業務

ア　基本設計

(ｱ)　本仕様書の要件を基に基本設計を行うこと。

(ｲ)　基本設計書を作成し本市の承認を得ること。

(ｳ)　本書に示した要件に加え、関係各課へヒアリングを実施して構築に当たり必要な詳細な要件を調査・分析すること。

(ｴ)　システム設計の前提となるＳＬＡを提案し、本市の承認を得ること。

イ　概要設計

(ｱ)　基本設計書を基に概要設計を行うこと。

(ｲ)　概要設計書を作成し本市の承認を得ること。

ウ　詳細設計

(ｱ)　概要設計書を基に詳細設計を行うこと。

(ｲ)　詳細設計書を作成し本市の承認を得ること。

エ　構築

(ｱ)　詳細設計を基に構築や設定を行うこと。

(ｲ)　本市が、別途、調達するガバメントクラウド接続サービスの回線敷設作業が令和９年２月までに完了するため、通信回線事業者がその後に実施する疎通確認テストに協力すること。

(ｳ)　デジタル庁から配布される必須適用テンプレート及び独自テンプレートを適用し環境構築を行うこと。

(ｴ)　設計内容どおり運用が行えることを確認するため、テスト計画書を作成し、テストを実施すること。

(ｵ)　テスト完了後は、テスト結果報告書を提出し、本市の承認を得ること。

(ｶ)　運用・保守業務を開始する前に、設計・構築業務が完了し、運用が開始できる状態にあることを判断するための稼動判定会議を実施すること。

(ｷ)　本番環境リリース計画書を作成し、本市の承認を得た上で、本番環境のリリースに係る作業を実施すること。なお、必要に応じてリハーサルを行うなど、安全なリリースに資する取組を行うこと。

(ｸ)　本番環境リリース作業完了後は、リリース結果報告書を作成し、本市の承認を得ること。

⑶　運用・保守業務

ア　詳細設計書を基に運用・保守を実施すること。

イ　広島市ガバメントクラウド利用基盤（ＡＷＳ）において、クラウドサービス利用における責任共有モデル上、サービス利用者の責任範囲とされるものについて保守作業を行うこと。

ウ　保守作業は、原則として、本市と協議の上、ガバメントクラウドを利用している標準準拠システム等が稼動していない時間帯に、当該標準準拠システム等の稼動に影響を与えない方法で行うこと。

エ　受注者が実施する保守作業に加えて、ＣＳＰが実施する保守・メンテナンスにおいて標準準拠システム等の稼動に影響を及ぼす可能性がある場合は、事前に本市に報告すること。

オ　システム構成のベストプラクティスを提案するツール（ＡＷＳ　Ｔｒｕｓｔｅｄ　Ａｄｖｉｓｏｒ等）を活用し、当該ツールが提案する推奨構成の内容を定期的に確認し、その結果を踏まえて本市の承認を得た上で、必要な設定変更等を行うこと。

⑷　障害対応

ア　広島市ガバメントクラウド利用基盤（ＡＷＳ）内で障害（セキュリティに関するアラートやインシデントへの措置を含む。）を検知した場合は、あらかじめ定めた障害連絡ルート・方法に基づき、関係者へ連絡するとともに、関係者と協力して適切な復旧対応を行うこと。

イ　共同利用方式システム領域及び単独利用方式システム領域で生じた不具合について、本市からの求めに応じ、原因調査を実施するなど、不具合の解消のために積極的に協力すること。

⑸　問合せ対応

ア　本市職員からの広島市ガバメントクラウド利用基盤（ＡＷＳ）に関する問合せや、ネットワーク等の技術的な相談を受け付け、対応すること。

イ　問合せ対応は、原則、開庁日の８：３０～１７：１５までとする。ただし、障害発生時にあっては、２４時間３６５日対応すること。

ウ　問合せの対応状況を管理し、分析をした結果とともに月次で報告すること。

１３　成果物

⑴　成果物は、作成途中の案を随時提出するなど、本市と協議しながら作成すること。作成に当たり、本市の関係部署等と調整を行う必要が生じた場合には、本市と協議した上で、必要な資料を作成すること。

⑵　表２の成果物を作成し、本市に納品すること。成果物は、本市と協議の上、統合又は分割してもよいものとする。

表２　成果物一覧

業務	成果物	内容	納品時期
プロジェクト管理	委託業務実施計画書	プロジェクトを運営するための計画書	契約締結後１０日以内／運用・保守業務開始前
	業務工程表（スケジュール表）	進捗管理を行うためのマスタスケジュール（大日程）、WBS（中日程）	実施計画書提出後速やかに
	管理資料	プロジェクトを運営するための各種書類（進捗管理表、品質管理表、リスク課題管理表、変更管理表、問合せ管理表等）	随時
	会議資料・議事録	本業務で実施した会議で使用した資料及び議事録	随時
	実施報告書	業務履行完了に当たり、実施結果等を記述した文書	契約書に定める支払期終了時
設計・構築業務	ネットワーク構成図	広島市利用領域（AWS）のネットワーク構成図	工程終了後速やかに
	基本設計書	機能要件／非機能要件に対する実現方法や制約事項、システム設計の根拠となるＳＬＡ等を記載した設計書	
	概要設計書	機能設計、画面設計、帳票設計、連携データ設計、データベース設計、コード設計、ファイル設計、システム構成、処理方式、運用設計等を記載した設計書	
	詳細設計書	プログラム設計、システム環境設	

業務	成果物	内容	納品時期
		計、運用詳細設計等を記載した設計書	
	テスト計画書・結果報告書	環境構築において実施する各種テストの計画書及びその結果を記載した報告書	
	本番環境リリース計画書・結果報告書	本業務で構築する環境等についてのリリース計画書及びその結果を記載した報告書	
	稼動判定資料	広島市ガバメントクラウド利用基盤（ＡＷＳ）の本番稼動可否の判断に必要な内容を取りまとめた各種資料	
	ガイドライン・各種様式	ガバメントクラウドを利用する上での広島市におけるルール、手順等を記載したガイドライン及び各種申請様式	
運用・保守業務	月次報告書	運用・保守業務の状況等を記載した報告書	月次
	改善提案書	広島市ガバメントクラウド利用基盤（AWS）の利用状況を分析して、サービス利用の改善内容を取りまとめた提案書	随時
	障害報告書	障害の発生内容（発生日時、障害事象等）、対応内容（対応日時、原因等）等を記述した文書	随時（障害復旧後、３日以内）
	改版した設計書等	運用・保守業務において改版した設計書等	随時

⑶　本仕様書で成果物として定義していないドキュメント等については、契約締結後、本市と受注者で協議の上、実施計画書において定めるものとする。

⑷　契約期間中は、媒体破損、データ不良等による納品物の再作成及び修正を保証できるように、受注者の責任において納品した成果物の複製物を保管すること。

⑸　納品形態は、Ｍｉｃｒｏｓｏｆｔ　Ｏｆｆｉｃｅ製品（Ｗｏｒｄ・Ｅｘｃｅｌ・ＰｏｗｅｒＰｏｉｎｔ）、ＰＤＦ形式のいずれかで作成された成果物を本市が指定する方法で納品すること。

⑹　記録媒体に書き込む際は、最新の定義ファイルが適用されたウイルス対策ソフトによりチェックを行い、ウイルスが含まれていないことを確認すること。

⑺　成果物の納品場所は、本市が指定する場所とする。

⑻　受注者は、この契約により作成される成果物等の著作権（著作権法（昭和４５年法律第４８

号）第２１条から第２８条までに規定する権利をいう。）を成果物等の引渡し時に本市に無償で譲渡するものとする。また、受注者は、いかなる場合も著作者人格権を行使しないものとする。

⑼　受注者は、本市に対し、成果物等が第三者の著作権その他の権利を侵害していないことを保証するものとする。また、成果物等について第三者から著作権その他の権利の侵害等の主張があったときは、受注者はその責任においてこれに対処するものとし、損害賠償等の義務が生じたときは、受注者がその全責任を負うものとする。

１４　実施体制等

⑴　実施体制

ア　受注者は本業務を確実に履行できるよう、表３の要件を満たす要員を配置することに加えて、履行期間中に、AWSが認定するAWS Certified Solutions Architect － Professional（SAP）試験合格による資格を有する要員を１名以上配置すること。

表３　実施体制

役割名	詳細	
統括業務責任者（広島市委託契約約款における現場責任者）	役割	本業務の統括的なマネジメントを行う。
	要件	・　本市からの要求事項に対して、事業者として迅速に判断ができること。 ・　次のいずれかの要件を満たすこと。 ・　（独）情報処理推進機構が実施する情報処理技術者試験（プロジェクトマネージャー）に合格していること。 ・　米国プロジェクトマネジメント協会が認定するPMP（Project Management Professional）試験合格による資格を有すること。 ・　PeopleCertが認定するPRINCE2(PRojects IN Controlled Environments,②nd version）のPractitioner試験に合格していること。
業務遂行責任者	役割	・　本業務を遂行するために必要な全体的な管理を行う。 ・　各チームのリーダーを支援するとともに、チームを跨ぐ横断的な調整を行う。 ・　本業務と関係するステークホルダーとの調整を行う。
	要件	・　次のいずれかの要件を満たすこと。 ・　（独）情報処理推進機構が実施する情報処理技術者試験（プロジェクトマネージャー）に合格していること。 ・　米国プロジェクトマネジメント協会が認定するPMP（Project Management Professional）試験合格による資格を有すること。

役割名	詳細	
		・　ＰｅｏｐｌｅＣｅｒｔが認定するＰＲＩＮＣＥ２（ＰＲｏｊｅｃｔｓ　ＩＮ　Ｃｏｎｔｒｏｌｌｅｄ　Ｅｎｖｉｒｏｎｍｅｎｔｓ，②ｎｄ　ｖｅｒｓｉｏｎ）のＰｒａｃｔｉｔｉｏｎｅｒ試験に合格していること。 ・　ＡＷＳでの設計・構築・運用の実務経験を１年間以上有すること。
チームリーダー	役割	・　チーム内のメンバー管理、進捗、課題、問題等に対して、マネジメントを行い、チーム内のタスクを円滑に推進する。 ・　業務遂行責任者や他チームとの調整を行う。 ・　本市との窓口を担当する。
	要件	・　ＡＷＳが認定するＡＷＳ　Ｃｅｒｔｉｆｉｅｄ　Ｓｏｌｕｔｉｏｎｓ　Ａｒｃｈｉｔｅｃｔ　－　Ａｓｓｏｃｉａｔｅ(ＳＡＡ)以上の試験合格による資格を有し、かつ、ＡＷＳの設計・構築・運用の実務経験を１年間以上有すること。 ・　本業務内で他の役割を兼務しないこと。ただし、チームリーダーとして、複数のチームを兼務することは許容する。
チームメンバー	役割	チームリーダーの指示の下、担当領域における業務を遂行する。
	要件	・　本業務が確実に遂行できる体制とすること。 ・　チームメンバーの半数以上が、ＡＷＳが認定するＡＷＳ　Ｃｅｒｔｉｆｉｅｄ　Ｃｌｏｕｄ　Ｐｒａｃｔｉｔｉｏｎｅｒ（ＣＬＦ）以上の試験合格による資格を有し、かつ、ＡＷＳの設計・構築・運用の実務経験を１年間以上有すること。 ・　本業務内で他の役割を兼務しないこと。ただし、チームメンバーとして、複数のチームを兼務することは許容する。

⑵　作業場所と利用環境

ア　インターネット経由で管理コンソールに接続して行う場合は、デジタル庁が示す「ガバメントクラウドリスクアセスメント」及び「ガバメントクラウド利用における推奨構成」に記載されているものと同様の方式で行い、また同様のセキュリティ対策を行うこと。

イ　受注者の作業場所と利用環境は、「ガバメントクラウドリスクアセスメント」に記載されているものと同様のセキュリティ対策を行い、これに加えて「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」等に記載されるマイナンバー利用事務系のネットワークに求められるセキュリティ要件等を満たせるようにすること。

ウ　受注者の拠点は、上記の要件に加え、広島市情報セキュリティポリシー等にある必要な情報セキュリティ対策や、地震対策や津波到達外立地、津波への対策等のＢＣＰ対策が講じられていること。

１５　スケジュール

図２のスケジュールに従い本業務を実施すること。

① ガバメントクラウド接続サービス回線敷設作業完了に伴う疎通確認テスト
② 健康管理等システム及び被爆者援護システムの構築作業開始に伴う接続作業

図２　スケジュール

１６　その他特記事項

⑴　契約終了時の対応

ア　本業務の契約履行期間の満了、全部若しくは一部の解除、又はその他契約の終了事由の如何を問わず、本業務において構築した環境等の継続利用に必要となる構成情報、監視や権限等の設定情報、運用手順書、その他の成果物及び必要な情報について、本業務の一環として後継の事業者に引継ぎを行うこと。

イ　受注者は、前項に基づく引継ぎが完了した後、本業務に係る情報のうち本市が指定するものについては、本市の指示に従い消去すること。

ウ　前項の情報消去の対象には、本業務の実施のために受注者が使用した端末、記憶媒体、受注者が管理するプロジェクト管理ツール・クラウドストレージ等に保存された本業務に係る情報も含むものとする。情報の消去後はその結果を本市へ報告すること。なお、当該情報の消去に当たっては、復元が困難な方法により行うこと。

エ　引継ぎに係る具体的な内容及び方法は、別途協議の上決定するものとする。

オ　本業務の終了後に、本市が新たな広島市ガバメントクラウド利用基盤（ＡＷＳ）へ移行する際は、移行対象データについて、本市が指定するデータ形式、フォーマットで出力すること。

⑵　仕様書の解釈

本仕様書及び添付書類に定めのない事項及び解釈の相違があった場合において、本業務の履行に際し必要な事項が発生した場合は、原則として本市の解釈によるものとする。本市の解釈により難いと本市及び受注者が認める場合は、本市と協議の上、対応するものとする。

⑶　経費に係る留意事項

本業務の実施に当たっては、付帯して発生する作業、ライセンス料等、必要となる一切の費用

は入札金額に含めることとし、別途本市に請求は行わないこと。

⑷　本業務の履行に当たっては、法令等の定め、デジタル庁等の国から提示される関連ドキュメントのほか、次の規程等についても内容を十分に理解し遵守すること。

ア　「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」を基にした広島市情報セキュリティポリシー

イ　広島市個人情報の保護に関する法律施行条例

ウ　広島市個人情報の保護に関する法律施行条例施行規則　等

広島市ガバメントクラウド利用基盤（AWS）の構築及び運用・保守業務　仕様書

別紙　非機能要件一覧

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		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	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	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	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	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	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。
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	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	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	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	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		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	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	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	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	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		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）	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	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	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	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%	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
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	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。

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		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.1.1.2	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	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。	○		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。
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。	○		1	主な処理のリクエスト件数のみが明確である	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	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。

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	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.1.1.5	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。	○		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
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	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。
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	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	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	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	3 定時外も頻繁に利用（1日12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	3 24時間利用	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	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。

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		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.1.2.5	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	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。
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。	○		3	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	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	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	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）	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
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	0	移行対象無し	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	0	移行対象無し	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。
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。	○		2	すべてベンダー	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	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。

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		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	
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	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		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	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）	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	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	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	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。
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。	○		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、改善提案を行う	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	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。

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		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.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	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	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	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	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	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	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。
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。	○		0	無し	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	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　ー：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