

(仮称) 江東区D X推進支援センター業務運営事業委託仕様書

1 件名

(仮称) 江東区D X推進支援センター（以下「センター」という。）運営事業委託

2 事業目的

本事業は区内の中小企業及び就職を希望する区民に対して、デジタルの推進支援及びデジタル人材育成を行い、もって区内中小企業の活性化と発展を図ることを目的とする。

3 委託期間

契約締結日の翌日から令和9年3月31日

ただし、契約締結日の翌日から6月30日までは準備期間とし、7月1日から業務が円滑に始められるようにすること。

4 履行時間

(1) 開業日及び時間

月曜日から金曜日 午前9時30分～午後6時

土曜日 午前9時30分～午後5時

※ただし午前9時から午前9時30分は準備時間とすること。またセミナー等のイベントで夜間行う場合は午後9時までの開催とし、午後10時までに事務員は退室すること。

(2) 休業日

日曜日、祝日及び年末年始（12月29日～1月3日）

なお、カメラアプラザの施設管理上支障がある日は別に定める。

5 事業実施場所

カメラアプラザ内の指定の場所

（江東区亀戸2-19-1 カメラアプラザ9階）

※「レイアウト」（別紙1）参照

6 事業対象者

(1) 江東区内（以下「区内」という。）に事業所を有する、中小企業基本法第2条第1項に定める中小企業（以下「企業」という。）

(2) 就職を希望する区民（以下「就職希望者」という。）

7 事業実施項目

(1) センター管理・運営事業

①センター管理事業

- ア センターの受付事務員を常時2名以上配置すること。受付事務員はセンター利用者の受付のほか、利用者が少ない際は、センターの周知等事務を行うこと。
- イ センターの利用は会員登録制として登録情報を適切に管理することとし、登録は原則オンラインで行うこと。Web環境がない場合は電話等で会員登録を行うこと。
- ウ センターの利用は会員登録後、原則オンラインで予約を受け付けること。Web環境がない場合は電話等で予約受付を行うこと。
- エ センターの利用は、利用上限時間を設けること。利用上限時間は区と協議すること。また7事業実施項目(2)の相談室運営事業は別途相談時間を設けること。
- オ 7事業実施項目(2)から(4)までの事業を企画し運営を行うこと。また区と協議の上、仕様の範囲内で毎年1つ以上新しい要素を加えて実施すること。
- カ センターが行う事業で使用するソフトをインストールしたパソコンをセミナー用に最低20台用意すること。また事業の規模により追加でパソコンを用意すること。なお、セキュリティ対策を万全に整えること。
- キ センター利用者用のWi-fi環境を整えること。
- ク セミナーや電子看板で利用するために50インチ以上でOS内蔵の会議用ディスプレイを用意すること。
- ケ 受託者用のパソコン、コピー機、シュレッダー、電話機等、管理・運営に必要な事務機器を用意すること。
- コ センターの電源に限りがあるため電子機器の充電状態を把握し、必要に応じてモバイルバッテリーを用意すること。

②コワーキングスペース管理事業

- ア センターをコワーキングスペースとして利用可能とすること。
- イ 希望者にはパソコンを貸し出し、インストールしたソフトを利用できるよう対応すること。
- ウ 予約をしていない利用希望者に対して、空きがあれば利用できるよう対応すること。

③DX関連書籍の配架事業

- ア DX関連書籍を20冊程度配架すること。
- イ 書籍は常時配架するものとし、2か月に1回程度入れ替えを実施すること。

ウ 書籍配架用ラックを用意すること。

④センターPR事業

ア センター専用ホームページ及び各種SNSを開設し、センターの周知を図ること。

なお、ホームページについて外部サービス利用チェックリスト（別紙2）に定める機密性1の必須レベルを満たすサービスを利用することとし、選定後速やかにチェックリストを区へ提出すること。

イ 相談、セミナー、研修等の事業に関しチラシの作成やメールマガジンなどで周知を図ること。

⑤江東しごとサポートセンター※1との調整事業

ア セミナー等のセンターの事業は同フロアで事業を行っている江東しごとサポートセンターと連携し事業内容が同一にならないよう調整すること。

イ 必要に応じ就職希望者について江東しごとサポートセンターと連携し支援すること。

※1 江東しごとサポートセンターとは、人材確保を望む区内の中小企業に対し、人材紹介をはじめ、専門スタッフによる相談やアドバイス等を通じた人材の採用・育成・定着などに関するさまざまな支援サービスを提供している区の施設。

⑥総合経営相談※2との連携事業

ア 区と協議の上、区で行っている総合経営相談をセンターで実施する等、総合経営相談と連携して企業支援を行うこと。

イ 必要に応じ相談者とデジタル相談員及び経営相談員の3者で総合的な相談を行うこと。

ウ 7事業実施項目（2）から（3）の事業内容は、区で実施している総合経営相談の事業内容と同一にならないように調整すること。

※2 総合経営相談とは、区内中小企業や区内で創業する方を支援するため、専門の相談員が経営・創業・事業承継・財務・税制・労務に関する相談に対応する事業。

（2）相談室運営事業

①開業時間内に、企業の状況に応じて、適切にデジタルに関する相談対応を実施すること。

②相談はセンター内、オンライン及び区内事業所へ出張して実施すること。

③相談員は中小企業のデジタル化に詳しいものとし、常時1名以上配置すること。なお、本相談員について、区で実施している総合経営相談の経営相談員との兼務は認めない。

- ④相談は1日の相談枠と1枠当たりの時間の上限を設定の上、原則予約制とするが、予約がない時間帯に直接センターに来た相談希望者に対しても相談を行うこと。また相談員は相談枠の中でセンター設置のパソコンにインストールされたソフトの操作説明を行うこと。
- ⑤相談を実施した際は、相談記録を作成し、相談員で共有し、継続した支援を実現すること。
- ⑥相談員は相談の予約がないときに相談員の業務を提案し、実施すること。
- ⑦区と協議のうえで、相談者に対するアンケートを作成し、相談終了後にアンケート調査を実施し、その結果を区に報告すること。

(3) セミナー等運営事業

①目的・開催形式

- ア 以下の②から⑤の運営に際し、総合的なデジタル人材育成事業となるように計画すること。
- イ 以下②から④のセミナー等の定員は最大20名とすること。
- ウ 内容により、オンライン、ハイブリッドの開催を行うこと。
- エ 以下②～④について、夜間の開催を各1回は行うこと。
- オ 開催場所について、原則センターで実施するが、センター以外の場所で開催する場合の会場費は受託者が事業受託費より用意すること。

②デジタルセミナー運営事業

- ア 企業向けにデジタルに関するセミナーを月1回開催すること。

③デジタル体験会事業

- ア 企業向けにパソコンを使用してデジタル化に役立つソフト（会計ソフトなど）の操作の説明を相談室運営事業の相談枠の中ですること。
- イ 企業向けに月1回、デジタル化に役立つデジタルソフトの体験会を実施すること。具体的なソフトの内容については区と協議すること。

④デジタル研修会事業

- ア 月3回の企業及び就職希望者向けの研修会を行うこと。また就職希望者向けの研修は年間15回以上（定員の合計が300名以上）行うこと。なお、内容はマイクロソフト365の機能を中心に初心者から中・上級者の研修を行うこと。
- イ 3ヵ月に1回（1回につき複数回を1セット）の企業及び就職希望者向けのデジタルスキルの資格の取得などを目的としたデジタル人材育成のための研修会を開催すること。

⑤アンケートの実施

- 区と協議のうえで、セミナー等の開催後にアンケートを実施し、その結果を区に報告すること。

⑥その他

上記②から⑤の事業の企画、講師選定、及び募集から開催まで全ての業務を行うこと。

(4) ICT等導入支援事業※3

①相談員派遣

- ア 区からの依頼により、ICT等導入支援のための相談員を区内事業所へ派遣し、ICT等導入に係る相談支援及び事業計画策定支援を行うこと。
- イ 補助金交付申請に係る事業計画書を策定した支援利用者に対し相談員を派遣し、事業計画の内容が適当であるか確認を行うこと。
- ウ 事業計画確認後に事業計画の内容を変更しようとする支援利用者に対し相談員を派遣し、変更後の事業計画の内容が適当であるか確認を行うこと。
- エ ICT等導入を行った支援利用者に対し相談員を派遣し、フォローアップ相談を行うこと。

②派遣相談時間及び最大派遣回数（移動時間は含まない）

- ア ①アの派遣相談（相談時間約90分）：最大2回×50件=100回
- イ ①イ、ウ、エの派遣支援（相談時間約60分）：最大1回×70件=70回
- ウ 派遣相談時間は想定であるため、相談時間を大幅に超えない限り、相談を行うこと。

③派遣相談の単価

- ア 本事業における経費のうち7事業実施項目（4）②のア及びイについては、それぞれ1回当たりの単価を設定する。また単価には旅費相当分を含むものとする。
- イ 本事業における経費のうち上記ア以外の経費については、上記アの単価には含めず、10経費のうち（2）センター事業にかかる経費に含めるものとする。

※3 ICT等導入支援事業とは、事業の効率化・災害時の事業継続性の向上を目的として、ICTツール等の導入を検討する方に対し、専門的知識を有する支援員を派遣し、相談支援を実施する事業。

(5) 業務実施にかかる準備業務

①マニュアル等整備

受託者は、7事業実施項目（1）から（4）の各種業務を円滑に行うために、本仕様にに基づき区が提供する資料及びヒアリング等を通じて、本業務の内容を十分に把握したうえで、業務設計を適切に行い、準備計画及びマ

マニュアルの作成、研修等を通じて令和8年7月1日からの事業実施に備えること。

8 業務実施体制

本業務を遂行するにあたり、事業責任者及び業務従事者の要員を適正数配置し、効果的運営が可能な体制を整備し、正確で迅速な対応を行えるようにすること。また、区と必ず連絡をとれるようにすること。

9 業務執行体制等

本業務を行うにあたっては、以下の事項を遵守すること。

- (1) 受託者は、状況に応じて適正かつ柔軟に従事者を配置し、業務処理が最も効率的に行えるよう、業務執行体制を整えること。
- (2) 受託者は、業務に必要な事務処理マニュアル等を整備・適宜更新し、適正かつ効率的な事務処理の執行に努めること。
- (3) 業務従事者は、本業務の目的、性質等を十分理解し、業務を適切に処理できる能力を有する者であること。
- (4) 業務従事者は、本業務に関する知識向上に常に努め、各業務の遂行に万全を期すこと。
- (5) 責任者は、作業遂行にあたり業務従事者が独自の判断で本業務にかかる事務を行うことのないよう業務従事者の管理及び指導を適切に行うこと。
- (6) 区は受託者の業務遂行について問題があると認めた場合は、その旨を受託者に通知し、是正措置を申し出ることができる。
- (7) 区及び受託者は、業務管理上必要があると認められたときは、互いに対して業務調整会議を行うことを求めることができる。

10 経費

本事業の対象経費は下記の(1)から(11)とする。

- (1) センター職員人件費
- (2) センター事業にかかる経費
- (3) センター事業PRにかかる経費
- (4) センター職員の旅費
- (5) パソコン等機器の料金
- (6) セキュリティ対策費用
- (7) Wi-fi、電話等通信費
- (8) 区が特に認めた施設賃貸借料、工事費、備品購入費等
- (9) その他、本事業を実施するにあたって発生する経費
- (10) ICT等導入支援事業にかかる相談員派遣費用
- (11) 業務実施にかかる準備期間の対応に係る経費

※本事業の運営上の維持管理にかかる光熱水費については無償とする。但し、環境への配慮及び経費の節減に努めること。

1 1 支払い条件

単価契約による月払いとし、毎月末日以降、受託者が提出した実績報告及び完了届等による履行検査合格の後、区は請求を受けた日から30日以内に受託者に支払うものとする。なお、毎月の支払い額は下記の（１）から（３）の合計額（（１）及び（２）については7月から翌年3月までの9か月分、（３）については4月から6月までの3か月分）とする。

- （１）10経費のうち（１）から（９）について、年間の総額を業務実施期間の7月から翌年3月までの9か月で除した金額。
- （２）10経費のうち（10）について、7事業実施項目（４）③による単価に毎月の実績を乗じた金額。
- （３）10経費のうち（11）について、年間の総額を準備期間の4月から6月までの3か月で除した金額。

1 2 提供物品

- （１）区は、レイアウト（別紙1）に表示の机・椅子・ロッカーなどの備品について、事業運営中は受託者に無償で貸与する。なお、貸与備品については令和8年4月以降に設置する。
- （２）電話機やパソコン（事務用・閲覧用）・プリンター、会議用ディスプレイ、事務用品、Wi-Fi等の通信環境は受託者が事業受託費より用意すること。
- （３）備品等の管理は受託者が注意を持って行い、破損、故障等が生じた場合は、受託者の負担で処理し支払うこと。
- （４）本事業を行うための施設及び備品等を本事業以外の目的で使用してはならない。

1 3 受託者の要件

- （１）委託契約締結日より30日以内に、次に掲げる内容を記載した事業計画書を区に提出すること。
 - ①運営の基本方針（P. 2の「7事業実施項目」における年間実施計画）
 - ②運営の目標及び達成を図るための指標（利用者数等）
 - ③運営の体制（職員構成、職務分担等）
 - ④緊急時の体制
 - ⑤その他区が必要と認める事項

- (2) 委託契約終了日より30日以内に、次に掲げる内容を記載した事業報告書を提出すること。
- ①業務の実施状況
 - ②経費の支出状況
 - ③その他区が必要と認める事項
- (3) 業務処理進捗状況を常に把握し、月に1回区に報告すること。項目、様式等は区及び受託者の双方協議の上定める。
- (4) 国及び東京都の補助金の申請に必要な調査及び報告について、区が定める日時までに回答すること。
- (5) 上記(1)から(4)に加え、本業務の実施に関する調査及び報告を求められたときは、速やかにその状況を区に報告するとともに、問題がある場合は、早急に改善すること。なお、事務処理方法等について改善を要する場合は、区及び受託者の双方協議の上、決定する。
- (6) 事件・事故等が発生した場合の対応策をあらかじめ業務従事者に周知すること。
- (7) 本業務の遂行にあたり、苦情・トラブルその他イレギュラーなケースが発生したときは、責任をもって対処するとともに遅滞なく区に報告すること。
また、区への引き継ぎが必要なものは、確実に区に引き継ぐこと。
- (8) 業務に関する苦情等については、現状・原因分析と解決策及び再発防止策を講じ、区に報告すること。
- (9) 何らかの事故などにより正常な業務運営ができない状況に至ったときには、速やかに区に口頭・書面により報告し、事故報告書（発生年月日・時刻、内容、対応、原因の分析、今後における防止策）を区に提出すること。
- (10) 各業務の月次報告や業務改善検討等を行うための定例報告会を、区と行うこと。

1.4 注意事項

(1) 個人情報等保護

本事業は江東区の委託事業となることから、個人情報等の管理は、「個人情報の取扱いに関する特記条項」（別紙3-1）及び「情報セキュリティ等に係る要件及び秘密保持に関する特記条項」（別紙3-2）に基づき適切に管理すること。

主な提出書類及び履行上の条件事項は以下のとおり。

- ① 個人情報等を取り扱う責任者及び従事者の届出、秘密保持等に関する誓約書を提出すること。
- ② 個人情報等を取り扱う作業場所を特定すること。
- ③ 取り扱う個人情報（紙及び電子データ）は施錠可能な保管庫等で管理すること。

- ④業務終了後は利用した個人情報（紙及び電子データ）を速やかに区に返還又は受託者の経費負担により廃棄すること。
- ⑤利用者データベース等の個人情報の取扱いについて充分配慮すること。
この場合において、パソコン等を使用するときは、インターネット環境や他のネットワーク環境からのアクセスや関係者以外の者の不正アクセスを防止する措置を講じること。
- ⑥情報漏えい対策など必要なセキュリティ対策を施すこと。また会員登録に使用する電子申請システムが「外部サービスの利用におけるセキュリティ要件」（別紙４）に示すセキュリティ要件を満たしていること。
- ⑦作業用パソコンには個人情報漏えいにつながる業務に関係しないアプリケーションソフトをインストールしないこと。
- ⑧個人情報の提供・返却・廃棄等については書面により確認を行うこと。

（２）施設の使用

区はカメラプラザ内の指定の場所を無償提供する。また使用の際は施設の安全管理に十分留意し、施錠等を怠らないよう努め、その責を負うこと。

1 5 受託者の責務

- （１）本業務に関する記録物を作成し、広報物と併せて、法令等に定める期間適切に保管することとし、保管期間が終了した記録物の廃棄等に関しては、区と協議の上、実施すること。
- （２）本業務終了後、区検査担当者の所定の検査を受けること。

1 6 安全衛生

- （１）本事業の責任者及び従事者に対して、労働基準法、労働安全衛生法、労働者災害補償保険法等、労働社会保険諸法令、その他の本契約に適用される法令に基づく労働者に対する法令上の責任を負い、受託者の責任で労務管理を行い、従事者の労働災害について受託者の責任と費用で処理しなければならない。但し、カメラプラザ内の指定の場所における区の責に帰する事由による災害については、この限りではない。
- （２）カメラプラザ内の指定の場所における設備、機械、装置、通路等について、安全で衛生的な作業の遂行を損なう恐れがある場合、受託者は直ちにその旨を区に通知するものとし、区は、これに応じて速やかに安全又は衛生上、必要な措置を講じるものとする。なお、区が当該措置を講じるまでの間、受託者は、緊急措置として危険を回避するために必要な合理的措置を講じることができる。
- （３）前項の場合において、危険が重大であり、かつ、急迫しているときは、受託者は、安全が確認できるまで業務の遂行を停止することができる。
- （４）地震、火災、疫病、その他当事者の合理的支配を超える不可抗力により、

業務の全部又は一部が履行不能となった場合、受託者の責任を免除する。

1 7 危機管理

受託者の責務において、窓口業務等に関する安全対策に万全を期し、事故防止に関する必要な措置を講じること。万一、機器等の障害が発生した場合や、様々な障害、事故、災害などの緊急事態が発生した場合においても、本業務遂行に支障をきたすことがないように区と連携して十分な対応を図ること。また、事前に緊急時の体制を整備し、区に提出すること。

1 8 損害賠償責任

受託者は、故意又は過失により、区、履行場所又は第三者に損害を与えたときは、その損害を賠償しなければならない。なお、損害賠償の範囲は、区及び受託者の双方協議の上、損害額を決定する。また、本業務に際し、受託者が損害を受けた場合、区の責に帰する場合を除き、区は賠償責任を負わない。

1 9 再委託の禁止

- (1) 本業務の全てを第三者に委託してはならない。
- (2) 本業務の一部を第三者に委託する場合は、事前に区と協議しなければならない。
- (3) 区と協議の結果、本業務の一部を第三者に委託する場合は、全て受託者の責任において行うものとし、本業務に関して受託者が委託する第三者の責めに帰すべき事由により生じた損害及び増加費用については、全て受託者の責めに帰すべき事由とみなして、受託者が負担するものとする。

2 0 権利義務の帰属等

- (1) 本事業に伴って生じたホームページ及びSNS等の権利は、区に帰属するものとする。
- (2) 本事業の実施が第三者の特許権、著作権その他の権利と抵触するときは、その責任において、必要な措置を講じなければならないものとする。

2 1 業務の引き継ぎ

- (1) 本契約が終了した場合（契約解除により契約が終了した場合も含む。以下同じ。）は、本業務に関し、供用を受けた施設、機器、資料等を遅滞なく、区に返還しなければならない。なお、供用を受けたものについて、滅失・損傷等が生じた場合は、その損害を賠償するとともに、施設については、受託者の負担において原状回復するものとする。
- (2) 次期受託者に変更があった場合は、本業務の開始時に混乱をきたさないよう本契約期間中に引き継ぎ期間を設け、次期受託者が円滑に業務を行えるよ

う十分な引き継ぎを行うこと。また、ホームページ及びSNS等の管理・運営についても同様とする。その際の経費負担は受託者の負担とする。

(3) 次期受託者から業務引き継ぎにかかる端末操作研修などの依頼があった場合は、受託者と次期受託者が協議を行い、合理的な範囲で、事務計画を立案し、業務に支障をきたさないよう責任をもって対応すること。

(4) 区は、受託者が本業務の継続的な遂行が困難になったことを理由に契約を解除した場合で、当該解除の時点において成果物などが区に業務引き継ぎができる状態に至っていないときは、受託者に対して、当該成果物などの引渡しに代えて、損害の賠償を求めることができる。

2.2 その他

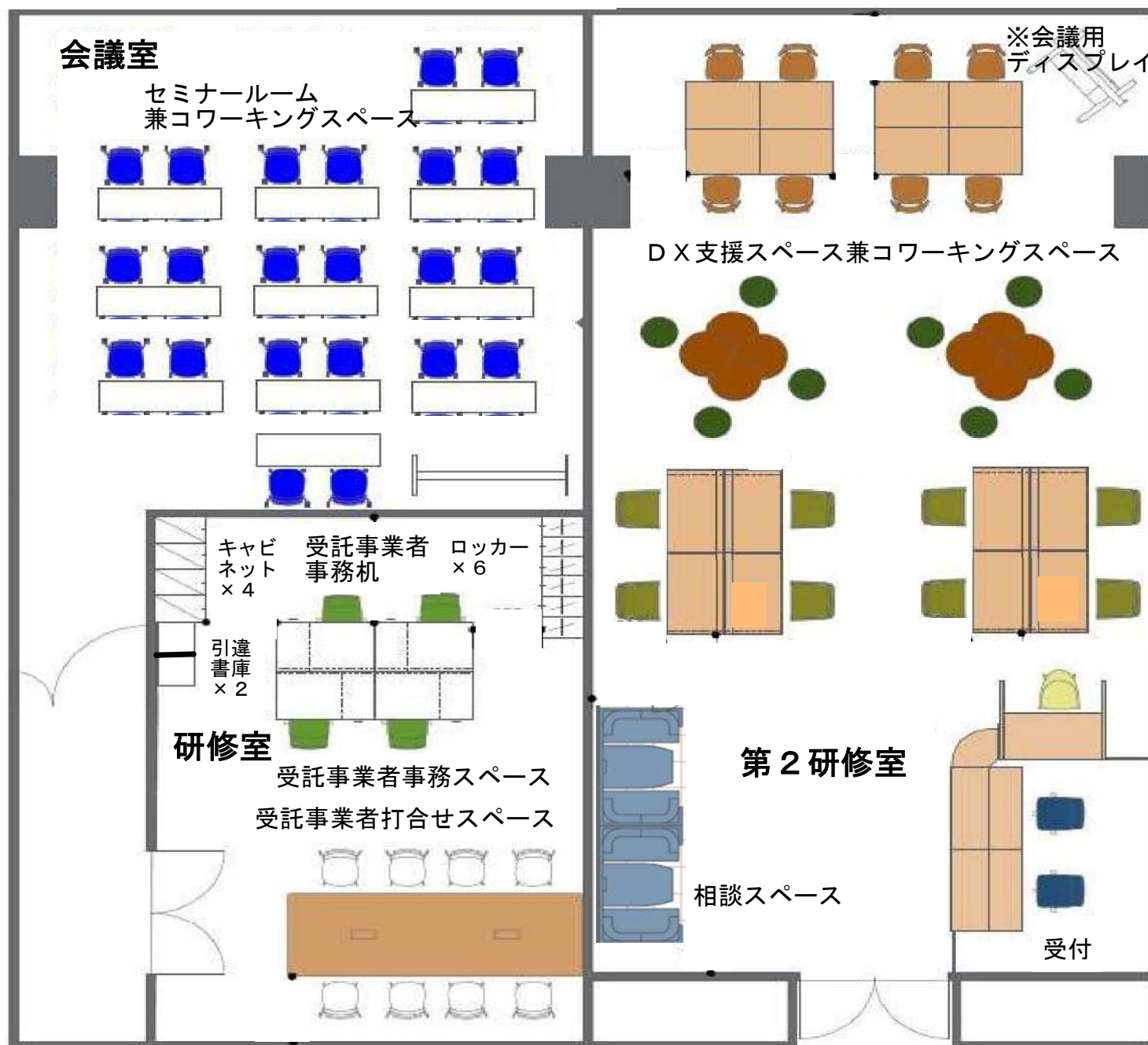
本仕様書に定めのない事項又は業務上に疑義が生じた場合は、区及び受託者の双方協議の上、決定する。

2.3 連絡先

江東区地域振興部経済課産業振興係 松田

電 話 03-3647-2332

FAX 03-3647-8442



※会議用ディスプレイは受託事業者で用意すること

本資料に記載の事務機器（会議用ディスプレイを除く）は区で準備する。
受託事業者事務スペース、セミナールーム兼コワーキングスペースは変更となる可能性がある。

【外部サービス：●●●●、業務名：●●●●、サービス利用期間：令和●●年●月●日～令和●●年●月●日、作成年月日：令和●●年●月●日】

国・非機能要件参考項目	項目	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	利用ガイドの解説	機密性3B	機密性3C	機密性2	機密性1	選択レベル	選択時の条件	レベル								備考 「利用ガイド」第4章も参照のこと	目標レベルを満たせない場合はその理由等記載	運用・保守実施状況記録 チェック欄	
								目標レベル	目標レベル	目標レベル	目標レベル			-	*	0	1	2	3	4	5				
E.1.1.1	1	サービス・事業者の信頼性	基本要件	遵守すべき規程、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	○	P13	1	1	1	1	無し	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。 [-] 遵守すべき規程やルール、法令、ガイドライン等が無い場合	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。		
G.4.3.1	2	サービス・事業者の信頼性	基本要件	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。	○	P13	2以上	2以上	1以上	1以上	各製品標準のマニュアルを利用する	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を作成する場合 [-] 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利用する	情報システムの通常の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いた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作業等)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。			
B.1.1.1	3	サービス・事業者の信頼性	基本要件	ユーザ数・ライセンスの範囲	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。 【追加】クラウドサービス上に他ベンダーが提供するソフトウェア等を導入する場合は、そのソフトウェアのクラウドサービス上におけるライセンス規定を確認する。	○	P13	1以下	1以下	0以上	0以上	特定ユーザのみ	基幹システムの場合は、重複ごとに特定のユーザが使用することを想定。 (標準システムは特定ユーザのみとする。)	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	不特定多数のユーザが利用				ライセンスの範囲を確認すること。 クラウドサービスなので、例えば登録したい方のメールアドレスを知っていれば誰でも登録することができてしまう。 そのソフトウェアのクラウドサービス上におけるライセンス規定も確認しておくこと。			
-	4	サービス・事業者の信頼性	基本要件	時刻同期	外部サービスで使用する時刻は、標準時刻(JST)と同期しているかどうか	○	P13	1	1	1	1	JST以外	クラウドサービス内における時刻同期の方法について確認し、取得するログの時刻、タイムゾーンを統一する。	仕様の対象としない	ベンダーによる提案事項	JST以外	JST								
B.1.1.2	5	サービス・事業者の信頼性	基本要件	アカウント管理	システムを事業者が構築する場合、管理者等のアカウントは適切に管理(パスワード管理や多要素認証、アクセス権限、終了時の削除など)はされている。	○	P13	1以下	1以下	0以上	0以上	特定ユーザのみ	基幹システムの場合は、重複ごとに特定のユーザが使用することを想定。 (標準システムは特定ユーザのみとする。)	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	不特定多数のユーザが利用							
-	6	サービス・事業者の信頼性	基本要件	手順書の整備	利用者(本区)が設定・操作するASPサービス、OSPサービスの管理機能について、誤操作・誤設定等を引き起こさないために必要な手順書が提供されるかを確認する。	○	P13	3以上	3以上	2以上	0以上	無し	利用開始前に手順書が提供されるかどうか	仕様の対象としない	ベンダーによる提案事項	無し	利用者が操作・設定可能な機能に限定される。	利用者が操作・設定可能な機能に限定される。	利用者が操作・設定可能な機能に限定される。	必要な手順書が適用される。					
G.4.5.1	7	サービス・事業者の信頼性	基本要件	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(図表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。	○	P13					他システムや外部システムと接続しない	庁内基幹システムとして、他システムと特などのように連携する他システムが存在しない場合。 [-] 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】 庁内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。			
-	8	サービス・事業者の信頼性	利用規模・性能	拡張性・柔軟性	利用者の増加、取り扱うデータ量の増加等による性能低下を防止するために、外部サービスのリソース等の増強を柔軟かつ迅速に行える拡張性を有しているかどうかを確認する。	○	P14	1以上	1以上	1以上	1以上	導入当時のリソース・システム構成から変更できない。	データの量、アプリケーションの数、場所の増減などでスケーラビリティまたは拡張することにより、ビジネスの需要や目的の変化に迅速に対応できる柔軟で信頼性の高いものになるか 機密性によらず、利用する外部サービスで実現する業務、サービスの規模、将来の利用者・データ量の増加予測等で判断する。	仕様の対象としない	ベンダーによる提案事項	導入当時のリソース・システム構成から変更できない。	メモリ、CPU、ディスク等の増強を容易にできる。	1に加え、利用者が追加した際、APサーバを増やすなどの追加処理を適切に実施可能なシステム構成に容易に変更できる。				将来の拡張性は、基幹系・庁内LANのシンクライアント端末を利用する場合は、拡張可能(ただし、管理面・情報漏えい等の調整が必要) 新規FAT端末を導入し利用する場合の拡張性は、端末の拡張スロット(コンピュータの機能を拡張する取付口)があり、サービスの利便性を向上させることができるかなどで判断			
B.2.1.4	9	サービス・事業者の信頼性	利用規模・性能	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・障害発生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またはシステム分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)	○	P14	3以上	3以上	3以上	3以上	規定しない	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読み取らない処理が有効な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。または代替手段がある場合 [-] コストと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況等)については、ベンダーと協議し詳細を整理する必要がある。 【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。			

C.1.2.5	サービス・事業者の信頼性	サービスの信頼性	バックアップ取得間隔	バックアップ取得時間		○	P14	4以上	4以上	1以上	1以上			バックアップを取得しない	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、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。 [注] RPOの要件が「-」される場合 [注] 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やすいように仕様が変更されること、仕様のタイミング	システム構成の変更時に、仕様のタイミング	月次で取得	週次で取得	日次で取得	同期バックアップ				
A.1.3.1	サービス・事業者の信頼性	サービスの信頼性	RPO（目標復旧時点）（業務停止時）	業務停止に伴う障害が発生した場合、バックアップしたデータから復旧システムを元の時点で復旧する必要がある目標値。 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。	システム障害発生において、障害復旧完了後、バックアップしたデータを参照してシステムを行うことを想定。 [注] 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） [注]選択レベルの時点（1営業日前の時点）での復旧では後述の入力が膨大に発生する等業務への支障が大きくなる可能性があるためである	○	P14	2以上	2以上	1以上	1以上			復旧不要	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）一時保存データからの復旧	障害発生時点（日次バックアップより6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り得る。 目標値は時間を元に定めたいクラウド	【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り得る。	
A.1.3.2	サービス・事業者の信頼性	サービスの信頼性	RTO（目標復旧時間）（業務停止時）	業務停止に伴う障害（主にハードウェア・ソフトウェア故障）が発生した場合、元々ハードウェア・ソフトウェア構成や保守体制を決定するために必要。	1営業日以上		○	P14	1以上	1以上	1以上	0以上			窓口対応等、システム停止が及ぼす影響が大いなる場合は復旧を優先しなるべく早く（復旧） （標準システムは12時間以内（レベル2以上）とする） [注]業務停止の影響がかさむ場合	仕様の対象としない	ベンダーによる提案事項	1営業日より上	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り得る。		
A.1.3.3	サービス・事業者の信頼性	サービスの信頼性	RLO（目標復旧レベル）（業務停止時）	業務停止に伴う障害が発生した場合、どこまで復旧するかレベル（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。	規定しない		○	P14	1以上	1以上	1以上	1以上			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。 （標準システムは全システム機能復旧とする） [注]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、特定の条件下で接続性が失われる機能などを指す。（例えば、住民基本台帳システムの住所発行機能だけは、障害時も提供継続する場合等。）		
E7.1.1	サービス・事業者の信頼性	サービスの信頼性	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。	取得しない		○	P14	1	1	0以上	0以上			不正なアクセスが発生した際に、「いつ」「誰か」「どこから」「何を」「どういった」と等を確認し、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、不正な操作を検出するための以下のようであることを意味している。 ・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		
-	サービス・事業者の信頼性	サービスの信頼性	データ消去方法	保存データ（事業者の複製データを含む）の消去について、実効性を確保でき、データが消去不可能となる処置を講じている。	データの復元が容易になる方法で消去している。		○	P14	1以上	1以上	1以上	1以上			サービス終了時に保存されているデータの消去については、復元不可能となる処理を実施していること。	仕様の対象としない	ベンダーによる提案事項	データの復元が容易になる方法で消去している。	データの復元ができない方法で消去している。	データの復元できない方法で消去している。	データの復元できない方法で消去している。	データの復元できない方法で消去している。			【雷ガイドライン】 クラウドサービス環境においては、データが記録されたハードウェアは、クラウドサービス事業者の所有物であり、別のクラウドサービス利用者に再利用できる可能性のあることを踏まえ、機密データは、自動的に消去することが推奨される。		
-	サービス・事業者の信頼性	サービスの信頼性	終了時の通知	保存データの返却や消去、他サービスへの移行手段（バックアップのやり直し時期事前バックアップの依頼等も含む）、利用書へこの通知方法等について定めている	サービスを終了した報告を終了日の1ヶ月前までに知らせる		○	P14	3	2	2以上	0以上			システム復旧等から終了の手続きから他の外部サービス・クラウド環境に判断	仕様の対象としない	ベンダーによる提案事項	サービス終了の報告を終了日の1ヶ月前までに知らせる	サービス終了の報告を終了日の1ヶ月前までに知らせる	サービス終了の報告を終了日の1ヶ月前までに知らせる	サービス終了の報告を終了日の1ヶ月前までに知らせる	サービス終了の報告を終了日の1ヶ月前までに知らせる					
D.1.1.2	サービス・事業者の信頼性	サービスの信頼性	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：外発生時の切り替え時間帯事前バックアップの依頼等含む。）	制約無し（必要な期間の停止が可能）		○	P14	3以上	3以上	2以上	0以上			業務が比較的少ない時間帯にシステム停止が可能。 [注]停止を増やす場合（標準システムはレベル4以上とする。）	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未満（計画停止不可）	1日（計画停止不可）	利用の少ない時間帯（復旧など）	移行のためには、システム停止が必要不可欠			【注意事項】 「レベル1」以上の制限システム上の制約によらず、移行に必要な期間のシステム停止が必要なことを示す。レベル1以上は、システム停止に関連する（業務などの）制約が存在するもので、システム停止可能時刻を示す。レベルが高くなるほど、移行によるシステム停止可能な時間幅が増え、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	サービス・事業者の信頼性	サービスの信頼性	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。	移行対象無し		○	P14							外部サービス利用開始前に移行対象範囲を明確にする。 ※新規サービス等の立ち上げ時は移行対象はなしを選択 ※システム移行には業務アプリケーションも含まれる移行がある。 [注]業務アプリケーション更新が無い場合 [注]業務アプリケーションの更新程度が高い場合	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、OS、ソフト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、ソフト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、ソフト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、ソフト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、ソフトウェアを入れ替える			【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、それぞれを考慮すること。	
D.4.1.1	サービス・事業者の信頼性	サービスの信頼性	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（クラウド移行データに含まれるRDPなどの電子帳票類を含む。）	移行対象無し		○	P14							移行前システムのデータを抽出した後、移行対象データを決定する必要があります。	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】 移行先のシステムの使用容量と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ります。		

0.5.1.1	20	サービス・事業者の信頼性	サービスの信頼性	移行のユーザ/ベンダー作業分組	移行作業の作業分組。			○	P14	1	1	1	1		実施していない	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、レベルに関連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分けを行うことが望ましい。 【レベル】 共同で移行作業を実施する場合、ユーザ/ベンダーの作業分組を規定すること。特に移行対象データに関する作業は、取り分けることには注意すること。					
-	21	サービス・事業者の信頼性	事業者の信頼性	受託者は、情報セキュリティに関して十分な知識がある。	本システム・サービスを提供する要員に対し情報セキュリティに関する教育や定期的な知識等の習熟状況を確認すると同時にセキュリティ確保のための対策が取られているかどうか			○	P15	2	2	2	2		実施していない	情報セキュリティに関して十分な知識を備えていること。 または、社内での研修等を受講し、最新情報を取得していること。 【-】定期的な研修等で知識をアップデートしていく仕組み等がない場合	仕様の対象としない	ベンダーによる提案事項	実施していない	実施している（配属時）	年1回以上定期的に実施している。											
0.1.3.1	22	サービス・事業者の信頼性	事業者の信頼性	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処置に発動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まない。「E.7.1 不正監視」で別途検討すること。			○	P15	3以上	3以上	2以上	1以上		監視を行わない	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。 （標準システムはレベル4（レベル3に加えてリソース監視を行う）以上とする。） 【-】障害時は管理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る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の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要素となる。					
0.6.3.1	23	サービス・事業者の信頼性	事業者の信頼性	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。		△	P15	1以上	1以上	1以上	1以上		インシデント管理について規定しない	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。 【-】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	インシデント管理について規定しない	既存のインシデント管理のプロセスに使う	新規にインシデント管理のプロセスを規定する												
0.6.4.1	24	サービス・事業者の信頼性	事業者の信頼性	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。		△	P15	1以上	1以上	1以上	0以上		問題管理について規定しない	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。 【-】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	問題管理について規定しない	既存の問題管理のプロセスに使う	新規に問題管理のプロセスを規定する												
0.6.2.1	25	サービス・事業者の信頼性	事業者の信頼性	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。			○	P15	1以上	1以上	1以上	0以上		問い合わせ対応窓口の設置について規定しない	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 【-】問い合わせ対応窓口を設置する必要がない場合 【+】コストと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	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ある。					
-	26	サービス・事業者の信頼性	事業者の信頼性	第三者認証・監査	第三者認証を取得している。			○	P15	2以上	2以上	1以上	1以上		ISMSなどの第三者認証を取得していない。	利害関係のない第三者によって評価されていることとシステムへの信頼性が向上。また、機密性の高い情報資産への管理体制、サイバー攻撃への対策という観点から、政府が求めるセキュリティ要求を満たしているクラウドサービスを利用しているかの確認	仕様の対象としない	ベンダーによる提案事項	ISMSなどの第三者認証を取得していない。	ISMS/ISO/IEC27010の認証を取得していない。	ISMS/ISO/IEC27017を	ISMS/ISO/IEC27010の認証	ISMS/ISO/IEC27018を				ISO/IEC 27018 個人情報を含むクラウドサービスに特化した情報セキュリティに関する認証 ISO/IEC 27017 クラウドサービスに特化した情報セキュリティ					
-	27	サービス・事業者の信頼性	事業者の信頼性	ISMAP登録	政府情報システムのためのセキュリティ評価制度（ISMAP）に登録している。			○	P15	1	1	0以上	0以上		ISMAPへの登録がない	ISMAPへの登録がない	仕様の対象としない	ベンダーによる提案事項	ISMAPへの登録がない	ISMAPへの登録がある							ASP(Application Service Provider)は、インターネット上でサービスを提供するものです。この範囲のサービスを提供する事業者と、ISMAPへの登録という説明は仕様対象ではないので注意してください。 また、SaaS(Software as a Service)もASPとはほぼ同義で使われることもあります。概念的に2つに区別されることもあります。 シングルテナント （1顧客に対して1環境を用意すること） マルチテナント （複数の顧客に対して1環境を用意すること） マルチテナントの場合、複数の顧客が同じ環境を利用するので、暗号化処理やテナント間のアクセス制限などが出来ているか確認してみてください。					
-	28	サービス・事業者の信頼性	事業者の信頼性	第三者認証・監査	第三者認証を取得していないなら、監査報告があるか。			○	P15	1	1	0以上	0以上		第三者による監査報告がされていない	SOC報告書などによって、クラウドサービスの内部統制の有効性が担保されているかどうか確認する	仕様の対象としない	ベンダーによる提案事項	第三者による監査報告が実施されている	第三者による監査報告が実施されている							ASPを利用する場合は、ASPが利用するCSPの状況を確認するようにしてください。					

E.10.1.1	29	サービス・事業者の信頼性	セキュリティ対策	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のを確認するための項目。Webシステムが構築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が必要がある。									無し	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、利用者のな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	対策の強化有り					
															[-] 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								
C.2.3.5	30	サービス・事業者の信頼性	セキュリティ対策	OS等パッチ適用タイミング	OS等パッチ情報の把握とパッチ適用のポリシーに関する項目。 OS等は、サーバ及び端末の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即時に適用する。										緊急性の高いパッチを除くこと、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）。	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の応用時に適用し、それ以外は随時適切なタイミングで適用を行う	緊急性の高いパッチは即時に適用し、それ以外では定期保守時のみ適用を行う	新規のパッチがリリースされるとすぐに適用すること。	【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。 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送やかに適用すること。 なお、事前検証なくパッチを適用しなければならないというわけではない。
E.4.3.4	31	サービス・事業者の信頼性	セキュリティ対策	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、方針並び適用のタイミングを確認するための項目。										定義ファイルを採用しない	ウィルス定義ファイルは、ファイルが開閉されるときシステムに自動的に適用されることを想定。	仕様の対象としない ベンダーによる提案事項	定義ファイルを採用しない	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】 事前検証なく定義ファイルを適用しなければならぬというわけではない。 最新版のウィルス定義ファイル適用時に、ウイルス検索エンジンのアップデートも検討すること。	
E.10.1.2 E.3.1.2	32	サービス・事業者の信頼性	セキュリティ対策	Webアプリケーション診断の有無	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。									不要	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。 [-] 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	仕様の対象としない ベンダーによる提案事項	不要	実施					
E.2.1.1	33	サービス・事業者の信頼性	セキュリティ対策	リスク分析範囲	システム開発を実施の中で、どの範囲を対象システムの脅威を見出し、影響の分析を実施するかを決定するための項目。 なお、適切な範囲を設定するためには、資産の見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。									分析なし	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にリスクが高い。そのため、重要度が低い資産を扱う範囲に対してリスク分析をする必要がある。 [-] 重要情報の漏洩等の脅威が存在しない(あるいは許容可能)場合 [-] 情報の移動や状態の変化が大きき場合	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、各団体の情報セキュリティポリシーにおける重要等級に基づいて定める（重要度が最も高いものとする等）。		
E.6.1.1	34	サービス・事業者の信頼性	セキュリティ対策	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。									無し	情報の盗聴・改ざん等を防止している、専用線やVPN接続によるサブスクリプションSSL/TLSによる通信の暗号化がされているかどうか。	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る	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な情報を取り扱う否かに関わらず、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】 本項の「暗号化」は「ハッシュ化」等も含む。 ガバナンスクラウド及びISMAPクラウドサービスに登録されているクラウドサービスについては、ISMAPの認証過程で通信のセキュリティ対策の実装を確認しているため、クラウドサービス内の伝送データの暗号化は必須ではない。 暗号化方式等は、国における評価の結果をまとめた、「電通政府における調査のために参照すべき暗号化リスト(CRYPTREC暗号化リスト)」を勘案して決定する。（CRYPTREC暗号化リスト： http://www.cryptrec.go.jp/list.html ）。		
E.6.1.2	35	サービス・事業者の信頼性	セキュリティ対策	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適切に暗号化を行う。（※暗号管理機能をクラウドサービス提供者が提供するものを活用する場合、鍵の生成から廃棄に至るまでのライフサイクルにおける仕組みに関する内容を確認し、リスクが十分に低減する。）									無し	蓄積するデータについては、第三者に漏洩しないようすべてのデータの暗号化を実施する。 ※外都サードパーティの管理対象機器等における蓄積データの暗号化（本区コールセンターが保有）	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る	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な情報を取り扱う否かに関わらず、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、「電通政府における調査のために参照すべき暗号化リスト(CRYPTREC暗号化リスト)」を勘案して決定する。（CRYPTREC暗号化リスト： http://www.cryptrec.go.jp/list.html ）。		
E.7.1.3	36	サービス・事業者の信頼性	セキュリティ対策	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。									無し	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	無し	重要度の高い資産を扱う範囲	システム全体				

-	37	サービス・事業者の信頼性	セキュリティ対策	OS・ミドルウェア層への攻撃対策	外部脅威に対する要件の確認。（OSやWebサーバーの脆弱性を狙った攻撃を防ぐ）														IPS/IDSなどを導入していない	サイバー攻撃（マルウェア感染、パフファオーパーバロー攻撃など）を防ぐ	仕様の対象としない	ベンダーによる提案事項	IPS/IDSなどを導入していない	IPS/IDSなどを導入していない							IPS(不正侵入防止システム)： 有 ・ 無 IDS(不正侵入検知システム)： 有 ・ 無			
-	38	サービス・事業者の信頼性	セキュリティ対策	Webアプリケーション層への攻撃対策	Webアプリケーションの仕組みは年々複雑化している。様々なアプリケーションやシステムとの連携で思いがけない脆弱性が見つかる場合もある。														WAFを導入していない	Webアプリケーションのセキュリティ対策	仕様の対象としない	ベンダーによる提案事項	WAFを導入していない	WAFを導入している										
E5.1.1	39	サービス・事業者の信頼性	セキュリティ対策	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。														実施しない	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。 ※レベルは、外部サービスの認証時に多要素認証が求められることが望ましいが、事業者・区役とも管理権限を行使する際、利用する端末等にログインする際に個人を特定する形で多要素認証があり、外部サービスの認証によって管理権限を行使できる場合も可とする。ただし、この場合その端末利用ログから外部サービスに接続していること	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。		
E5.2.1	40	サービス・事業者の信頼性	セキュリティ対策	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等、利用制限等、ソフトウェアによる対策を示す。														無し	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になってしまうため、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） [-] 重要情報等への攻撃の拠点とならない端末等に関しては、運用による対策が有効	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。				
以下は、標準システムは、機密性3B記載の目標レベルの順守が原則。標準システム以外のシステムで外部サービスを利用する場合、本区から目標レベルは提示しないが事業者が提供するサービスレベルを提示してもらうこと。また、提示されたサービスレベルが事業者の主旨や取り扱う情報等を鑑みたとに必要なレベルに達していないと判断した場合は事業者とサービスレベルの調整を行うこと。																																		
A1.4.1	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、どこ迄で復旧させるかの目標。 大規模災害とは、火災や地震などの偶発的な自然現象。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が、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稼働に修復するのが困難な状態となる災害をいう。														再開不要	電源及びネットワーク、アプリケーションを設置するインフラ（サーバ・バックアップ等）が利用できるときを前提に、遠隔地に設置された予備機とバックアップデータ等を利用して、復旧するまで必要な期間を想定。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C/S等で自治体が利用できる形式で提供（B）する。 ※住居記録システム等、住居の安全確認に必要なデータを持つシステムについては、発災後7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。 [-] 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に求める場合	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。					
A15.1	A.15.1	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、サービス中断が生じた時間により稼働率を求める。一般的にサービス利用率と稼働率は比例関係にある。														規定しない	ベンダーのサポート観点から、直で2時間稼働の場所にあることを想定。1回当たり6時間程度停止する故障を年間2回まで許容する。 [-] コストと地理的条件的実現性を確認した上で、業務への支障が大きいために明らかである場合 [-] 地理的条件から実現困難な場合、業務停止が許容できる場合。	仕様の対象としない	ベンダーによる提案事項	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6日当たり12時間と想定しうる場合。 99.9%・・・年間累計稼働時間17分 99.9%・・・年間累計稼働時間20時間 99.9%・・・年間累計稼働時間45時間 99%・・・年間累計稼働時間20時間 95%・・・年間累計稼働時間145時間					
A3.1.1	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高めるための代替の機器として、どこに何が必要かを定める。														復旧しない	災害発生後に関連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 [-] コストと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	指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	指定された構成で情報システムを再構築	同一の構成でDRサイトを構築	【レベル】 レベル1及び3の指定された構成とは、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、災害などで業務の継続が不可能になった際に、緊急の代替拠点となること。						
A3.2.1	A.3.2.1	可用性	災害対策	保管場所分散（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。														外部保管しない	遠隔地1ヶ所 [-] コストと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（遠隔地の別な建物と遠隔地）	2ヶ所（遠隔地）	【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、災害などで業務の継続が不可能になった際に、緊急の代替拠点となること。						
A3.2.2	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。														外部保管しない	A3.2.1と同じ観点へのリモートバックアップを想定。 [-] 媒体での外部保管のみによる運用を許容できる場合	仕様の対象としない	ベンダーによる提案事項	外部保管しない	媒体による外部保管のみ	ネットワーク経由でストレージへのリモートバック				【注意事項】 A3.2.1（保管場所分散（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。					

B1.1.3	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、性能・拡張性を決めるための前提となる項目である。	○	-	0	0	0	0	すべてのデータ件数、データ量が明確である	要件定義時には明確にしておく必要がある。 【レベル1】 【1】全てのデータ量が把握できている場合	仕様の対象としない	ベンダーによる提案事項	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、データ量のみのみ明確である							【レベル1】 主要なデータ量は、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ものを言う。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・移動データ等がある。 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。
B1.1.4	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。 ※種数の集約に関連するバッチ処理であれば、利用対象から漏れてもよい	○	-	-	-	*	*	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。 【1】全てのオンラインリクエスト件数が把握できていない場合	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のみが明確である	主な処理のリクエスト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記入・転出の履歴などがある。 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。
B1.1.5	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。	○	-	-	-	*	*	処理単位ごとに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。 【1】全てのバッチ処理件数が把握できていない場合	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	【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。 【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ものを言う。例えば、人事給与システムや税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。						
C5.2.2	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	保守が必要対象ソフトウェアに対する保守契約の種類。	○	-	2	2	2	2	保守契約を行わない	ソフトウェアがバージョンアップした場合には、ベンダーがアップデートすることを想定。 【1】アップデート権を必要としない場合	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						
C5.9.1	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以上	3以上	*	*	無し	【1】保守に関する報告事項が予め少ないと想定される場合 【1】後述に関する報告事項が予め多いと想定される場合	仕様の対象としない	ベンダーによる提案事項	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】 継続ごとの定期報告会の頻度を指す。報告会発生時に実施される不定期の報告会は含まない。
C5.9.2	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	3	*	*	無し	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	障害報告に追加して運用状況報告を行って、改善提案を						
C6.5.1	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。構成管理の実施方法については、資産の確認後に具体化して確認する。	△	-	1	1	1	1	構成管理について規定しない	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。 【1】運用管理契約を行わない場合 【1】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	既存の構成管理のプロセスに使う	新規に構成管理のプロセスを規定する						
C6.6.1	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バッチ適用、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。変更管理の実施方法については、資産の確認後に具体化して確認する。	△	-	1	1	1	1	変更管理について規定しない	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。 【1】運用管理契約を行わない場合 【1】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	変更管理について規定しない	既存の変更管理のプロセスに使う	新規に変更管理のプロセスを規定する						
C6.7.1	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。リリース管理の実施方法については、資産の確認後に具体化して確認する。	△	-	1	1	1	1	リリース管理について規定しない	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。 【1】運用管理契約を行わない場合 【1】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	リリース管理について規定しない	既存のリリース管理のプロセスに使う	新規にリリース管理のプロセスを規定する						
D1.1.1	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	4	3	3	システム移行無し	年度を跨いで移行を進める必要がある。 【1】期間短縮の場合 【1】さらに長期期間が必要な場合	仕様の対象としない	ベンダーによる提案事項	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			
D1.1.3	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	0	1	1	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が必要。 【1】移行のためのシステム停止期間が短く必要であり、並行稼働しない場合	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。
F1.1.1	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。 ・J-SOX法 ・ISO/IEC27000系 ・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） ・FISC ・プライバシーマーク ・構築実施場所の制限など	○	-	1	1	1	1	制約無し	庁内規約などが存在する場合を想定。 【1】法や条例の制約を受けない場合、もしくは業界などの標準や取り決めがない場合	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（重要な制約のみ適用）	制約有り（すべての制約を適用）						【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、情報利用者の制約、入退室管理の実施、取り扱い情報の符号化等の対策が施された開発環境を整備する必要がある。 また運用予定地での機密が流出する、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。
F1.2.1	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。 ・J-SOX法 ・ISO/IEC27000系 ・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） ・プライバシーマーク ・リモートからの運用の可否など	○	-	1	1	1	1	制約無し	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。 【1】設置センターのポリシーや共同運用など運用に関する方式が制約となっている場合	仕様の対象としない	ベンダーによる提案事項	制約無し	制約有り（重要な制約のみ適用）	制約有り（すべての制約を適用）						

(別紙 3 - 1) ※乙を受託者、甲を江東区とする。

個人情報の取扱いに関する特記条項

(個人情報保護法等の遵守)

第 1 条 乙は、個人情報の保護に関する法律のほか、甲の定める江東区個人情報の保護に関する法律施行条例施行規則並びに情報セキュリティポリシー及び情報セキュリティ実施手順に基づき、個人情報の取扱いに関する特記条項（以下「特記条項」という。）を遵守しなければならない。

(責任体制の整備)

第 2 条 乙は、個人情報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。

(作業責任者等の届出)

第 3 条 乙は、個人情報の取扱いに係る作業責任者及び作業従事者を定め、業務の着手前に書面により甲に報告しなければならない。

2 乙は、個人情報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 乙は、作業責任者を変更する場合は、事前に書面により甲に申請し、その承認を得なければならない。

4 乙は、作業従事者を変更する場合は、事前に書面により甲に報告しなければならない。

5 作業責任者は、仕様書及び特記条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、仕様書及び特記条項に定める事項を遵守しなければならない。

(作業場所の特定)

第 4 条 乙は、個人情報を取り扱う場所（以下「作業場所」という。）を定め、業務の着手前に書面により甲に報告しなければならない。

2 乙は、作業場所を変更する場合は、事前に書面により甲に申請し、その承認を得なければならない。

3 乙は、甲の事務所内に作業場所を設置する場合は、作業責任者及び作業従事者に対して、乙が発行する身分証明書を常時携帯させ、事業者名が分かるようにしなければならない。

(教育の実施)

第 5 条 乙は、個人情報の保護、情報セキュリティに対する意識の向上、仕様書及び特記条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 乙は、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。

(守秘義務)

第 6 条 乙は、本委託業務の履行により直接又は間接に知り得た個人情報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 乙は、本委託業務にかかわる作業責任者及び作業従事者から、秘密保持に関する誓約書（甲に対する誓約書をいう。以下単に「誓約書」という。）を徴取し、これを甲に提出しなければならない。

（再委託）

第7条 乙は、本委託業務の全部の委託をしてはならない。

- 2 乙は、甲の書面による許諾を得た場合に限り、本委託業務の一部の委託（以下「再委託」という。）をすることができる。
- 3 乙は、前項の許諾を得ようとするときは、次の事項を明確にした上で、事前に、書面により再委託をする旨を甲に申請しなければならない。
- (1) 再委託を受ける者の名称
 - (2) 再委託をする理由
 - (3) 再委託をして処理する内容
 - (4) 再委託を受ける者において取り扱う個人情報
 - (5) 再委託を受ける者における安全性及び信頼性を確保する対策
 - (6) 再委託を受ける者が当該再委託に係る業務の全部又は一部の委託をすることの有無
 - (7) 再委託を受ける者に対する管理及び監督の方法
- 4 乙は、第2項の規定により再委託をしたときは、再委託を受けた者に本契約に基づく一切の義務を遵守させるとともに、甲に対し、再委託を受けた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。
- 5 乙は、第2項の規定により再委託をしたときは、乙と再委託を受けた者との契約において、再委託を受けた者に対する乙の管理及び監督の手段及び方法を具体的に規定しなければならない。
- 6 乙は、第2項の規定により再委託をしたときは、その履行につき管理及び監督をするとともに、甲の求めに応じ、管理及び監督の状況を甲に対し適宜報告しなければならない。
- 7 乙は、第2項の規定により再委託をしたときは、再委託を受けた者に、当該再委託に係る業務にかかわる作業責任者及び作業従事者から誓約書を徴取させなければならない。
- 8 前項の誓約書は、乙が、再委託を受けた者から受け取り、甲に提出しなければならない。

（派遣労働者等の利用時の措置）

第8条 乙は、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 乙は、甲に対して、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。

（個人情報の管理）

第9条 乙は、本委託業務において利用する個人情報を保持している間は、次の各号の定めるところにより、個人情報の管理を行わなければならない。

- (1) 施錠が可能な保管庫又は施錠若しくは入退室管理の可能な保管室で厳重に個人情報を保管

すること。

- (2) 甲が指定した場所へ持ち出す場合を除き、個人情報を定められた場所から持ち出さないこと。
- (3) 個人情報を電子データで持ち出す場合は、電子データの暗号化処理又はこれと同等以上の保護措置を施すこと。
- (4) 事前に甲の承認を受けて、業務を行う場所で、かつ、業務に必要な最小限の範囲で行う場合を除き、個人情報を複製又は複写しないこと。
- (5) 個人情報を移送する場合、移送時の体制を明確にすること。
- (6) 個人情報を電子データで保管する場合、当該データが記録された媒体及びそのバックアップの保管状況並びに記録されたデータの正確性について、定期的に点検すること。
- (7) 個人情報を管理するための台帳を整備し、個人情報の利用者、保管場所その他の個人情報の取扱いの状況を当該台帳に記録すること。
- (8) 個人情報の紛失、漏えい、改ざん、破損その他の事故（以下「個人情報の漏えい等の事故」という。）を防ぎ、機密性、完全性及び可用性の維持に責任を負うこと。
- (9) 作業場所に、私用パソコン、私用外部記録媒体その他の私用物を持ち込んで、個人情報を扱う作業を行わせないこと。
- (10) 個人情報を利用する作業を行うパソコンに、個人情報の漏えいにつながると考えられる業務に関係のないアプリケーションをインストールしないこと。

（提供された個人情報の目的外利用及び第三者への提供の禁止）

第10条 乙は、本委託業務において利用する個人情報について、本委託業務以外の目的で利用してはならない。また、甲に無断で第三者へ提供してはならない。

（個人情報の受渡し等）

第11条 乙は、甲乙間の個人情報の受渡しに関しては、甲が指定した手段、日時及び場所で行った上で、甲に個人情報の預り証を提出しなければならない。

- 2 本委託業務において電子計算組織の運用又は保守をする場合は、乙は、業務の着手前に、接続又は操作をすることができる情報の種類及び範囲並びに接続又は操作の方法について甲の指示を受けるものとする。

（個人情報の返還、消去又は廃棄）

第12条 乙は、本委託業務の終了時に、本委託業務において利用する個人情報について、甲の指定した方法により、返還、消去又は廃棄を実施しなければならない。

- 2 乙は、本委託業務において利用する個人情報を消去又は廃棄する場合は、事前に消去又は廃棄すべき個人情報の項目、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甲に申請し、その承諾を得なければならない。
- 3 乙は、個人情報の消去又は廃棄に際し甲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 乙は、本委託業務において利用する個人情報を消去又は廃棄する場合は、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個人情報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 乙は、個人情報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、書面により甲に対して報告しなければならない。

(定期報告及び緊急時報告)

- 第13条** 乙は、甲から、個人情報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 乙は、個人情報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。

(監査及び検査)

- 第14条** 甲は、本委託業務に係る個人情報の取扱いについて、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、乙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 甲は、前項の目的を達するため、乙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。

(事故時の対応)

- 第15条** 乙は、本委託業務に関し個人情報の漏えい等の事故が発生した場合は、その事故の発生に係る帰責の有無にかかわらず、直ちに甲に対して、当該事故にかかわる個人情報の内容、件数、事故の発生場所、発生状況を書面により報告し、甲の指示に従わなければならない。

- 2 乙は、個人情報の漏えい等の事故が発生した場合に備え、甲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 甲は、本委託業務に関し個人情報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。

(契約解除)

- 第16条** 甲は、乙が特記条項に定める義務を履行しない場合は、特記条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 乙は、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、甲に対して、その損害の賠償を請求することはできないものとする。

(損害賠償)

- 第17条** 乙の故意又は過失を問わず、乙が特記条項の内容に違反し、又は怠ったことにより、甲に対する損害が発生させた場合は、乙は、甲に対して、その損害を賠償しなければならない。

情報セキュリティ等に係る要件及び秘密保持に関する特記条項

(情報セキュリティポリシー及び情報セキュリティ実施手順の遵守)

第1条 受託者（以下、「乙」という）は、本契約に基づく業務（以下、「本業務」という）の遂行にあたり、江東区（以下、「甲」という）の定める情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

(責任体制の整備)

第2条 乙は、本業務の遂行にあたり、ISMS（ISO/IEC 27001）等の認証取得等、情報セキュリティにおける責任体制を構築し、その体制を維持しなくてはならない。

(作業責任者及び作業従事者の特定)

第3条 乙は、本業務における情報セキュリティの管理に関する責任者（以下「作業責任者」という。）を選任し、氏名・役職・連絡先を業務の着手前に甲に報告しなければならない。

2 乙は本業務に従事する作業従事者を定め、氏名・所属を業務の着手前に甲に報告しなければならない。

3 乙は、甲に報告した作業従事者を変更する場合は、その旨を甲に報告しなければならない。

(作業場所の指定)

第4条 乙は、甲の事務所以外で本業務を遂行する場合は、情報セキュリティ上の管理対策が講じられている区域（以下、「要管理対策区域」という）にて作業を実施しなくてはならない。

2 乙は、本業務を甲の事務所内で遂行をする場合は、作業責任者及び作業従事者に対して、身分証明書を常時携帯させ、事業者名が分かるようにしなければならない。

(情報漏えい防止のための技術的安全管理措置に関する取り決め)

第5条 乙は、本業務の遂行にあたり、個人情報、その他の機密情報の漏えい、滅失、不正アクセス等を防止するための技術的安全管理措置を講じなければならない。

2 乙は、乙指定作業場所で業務を遂行するにあたり、情報資産の盗難・紛失防止対策を講じなくてはならない。

(アクセスを許可する情報の種類と範囲、アクセス方法)

第6条 甲は、乙が本業務の遂行に必要とする情報の種類・範囲を明示し、乙は定められた情報以外の情報へアクセスしてはならない。また、定められた情報以外の情報を利用してはならない。

2 乙は、本業務の遂行にあたり必要とする情報にアクセスする場合、甲が指定する方法でアクセスしなくてはならない。

(教育の実施)

第7条 乙は、情報セキュリティに関する必要な教育を、作業従事者全員に対して実施しなければならない。

(提供された情報の目的外利用及び第三者への提供の禁止)

第8条 乙は、甲の指示又は承諾があるときを除き、本業務に係る情報を当該業務以外の目的に利用し、又は第三者に提供してはならない。

(守秘義務)

第9条 乙は、本業務の履行を通じて直接又は間接に知り得た事項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 本業務における守秘義務は、甲に報告した作業責任者及び作業従事者を対象とする。

(再委託)

第10条 乙は、本契約業務の全部の委託をしてはならない。乙は、甲の許諾を得た場合に限り、本契約業務の一部の委託をすることができる。

(情報資産の返還、消去、廃棄等)

第11条 乙は、本業務の契約期間満了後、本業務において利用する情報資産について、甲の指定した方法により、返還、消去又は廃棄を実施し、甲に報告しなければならない。

(定期報告及び緊急時報告義務)

第12条 乙は、甲から、本業務における情報セキュリティ対策の履行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。また、乙は、本業務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。

(監査又は検査)

第13条 甲は、本業務における情報セキュリティ対策について、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、乙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。

(インシデント発生時の公表)

第14条 乙は、本業務に関し情報セキュリティインシデントが発生した場合は、その事故の発生に係る帰責の有無にかかわらず、直ちに甲に対して報告し、甲の指示に従わなければならない。

2 甲は、本業務に関し情報セキュリティに関する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。

(損害賠償)

第15条 乙の故意又は過失を問わず、乙が情報セキュリティポリシーを遵守しなかったことにより甲に対する損害を発生させた場合は、乙は、甲に対して、その損害を賠償しなければならない。

外部サービスの利用におけるセキュリティ要件

No	セキュリティ対策
1	受託者は情報セキュリティに関して十分な知識があること。
2	ライセンス違反等がないよう必要な数だけアカウントを準備すること。
3	利用する端末にセキュリティ対策（ユーザ認証・ウィルス対策・デバイス管理・Web フィルタリング等）を行っていること。
4	外部サービスを利用する端末に機微なデータが保存されない対策を行っていること。
5	利用する端末を外部に持ち出す場合、Free Wi-Fi への接続禁止等の措置が講じられていること。
6	外部サービスを提供するシステム・利用する端末のリソースに不足がなく、将来の拡張性があること。
7	外部サービスで使用する時刻は、標準時刻と同期していること。
8	都区市町村情報セキュリティクラウドへの接続及び LGWAN を利用する場合は、それらの帯域を圧迫しないこと。
9	システムのレスポンス（応答時間）は許容範囲内であること。
10	ユーザが特別な知識を必要とせず、直感的に利用できるシンプルなデザインの画面や操作性となっていること。
11	サービスの稼働率は、サービス停止の頻度や時間等がシステムとして許容範囲内であること。
12	SLA（サービス品質保証）を締結できること
13	データのバックアップ及びリストアができること。 （バックアップのタイミング：日次）
14	障害発生時にシステム及びデータの復旧方法や復旧時間等の目標を定めていること。
15	システム及びネットワークが冗長化されていること。
16	インシデント等の検証に必要なログを提供できること。
17	OS やアプリケーション等のバージョンアップや設定変更、パッチ適用、脆弱性診断等を行い、実施状況を報告すること。
18	サービス終了時に保存データ（事業者の複製データも含む）を消去する際は、実効性を確保でき、データが復元不可能となる処置を講じること。
19	サービス終了時は利用者アカウントや管理者アカウント等を削除できること。
20	第三者認証（ISMAP 登録や ISO27017 による認証等）や情報セキュリティ監査の結果等を有していること。
21	システムを事業者が構築する場合、事業者内において適切なセキュリティ管理体制（職員の資格取得や研修等）がとられていること。
22	重要な操作（仮想化されたデバイスのインストールや変更・削除、バックアップ・リストア、サービス終了時など）に関して、手順が文書化されていること。

23	システムを事業者が構築する場合、管理者等のアカウントは適切に管理（パスワード管理や多要素認証、アクセス権限、終了時の削除など）されていること。
24	再委託や第三者の外部サービス利用がある場合、上記No.21と同様に再委託先等の情報セキュリティ対策を実施していること。
25	データはすべて国内に保存されること。 (データが保存されているサーバは国内に設置されていること)
26	データセンターの防災対策や入退室管理・監視体制が整っており、サービス利用において安全な設備になっていること。
27	事業者または区がインシデントを検知した際、区 CSIRT への連絡・報告体制が取れていること。
28	サービスのサポート体制や窓口、受付時間がサービス利用において十分なものになっていること。
29	情報の盗聴、改ざん等を防止するため、専用回線・VPN 接続によるサービス利用、または TLS による通信の暗号化がされていること。
30	サービス提供側にファイアウォールなどによる外部・内部からの不正アクセスを防止措置が施されていること。
31	サービス提供側に IPS/IDS や WAF による不正通信やマルウェアの発見・遮断措置が施されていること。
32	盗難・改ざん等の防止のため、保存されたデータは暗号化されていること。
33	不必要なアクセスがされないよう、情報資産・機能に対して、各利用者に必要最低限のアクセス権のみ付与すること。
34	ID/PW による認証を行うこと。