世田谷区新 BOP 学童クラブ利用手続き業務委託　業務説明書

1　業務の目的

世田谷区新　BOP　学童クラブ利用手続きにおいて、現行のオンライン申請システムを見直し、区担当課、各児童館、各新 BOP の事務処理について、一層の効率化を図るとともに、新 BOP 学童クラブ利用児童の保護者の各種申請における利便性向上に寄与することを目的とする。

2　委託業務期間

契約締結日から令和11年3月31日まで

※良好な履行状況及び予算配当を条件として、単年度ごとに令和11 年度まで随意契約を締結する予定がある。

3　前提条件

（1）業務実施にあたっての原則について

①受託者は関係法令を遵守し、本業務を適切に実施すること。

②受託者は、世田谷区新 BOP 学童クラブの制度趣旨及び公共性を十分に理解し、区民等に対して丁寧に対応すること。

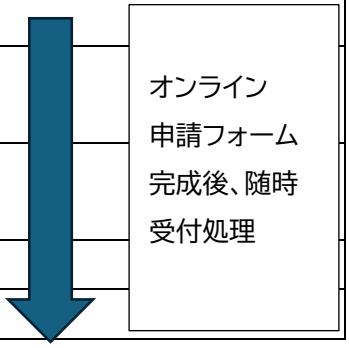
③受託者は、説明書（別紙含む）の記載事項を遵守すること。

④受託者は、世田谷区やその他関係機関からの制度情報の収集に努めたうえで業務を実施すること。

⑤受託者は、業務の繁閑に応じて柔軟な対応が求められることから、履行体制にかかる人員配置については、適宜、区と協議し、必要な人材確保に努め業務を実施すること。

（2）事業スケジュールについて

令和8年　7月～	業務設計
令和8年　9月	各種オンライン申請フォーム案完成
令和8年　10月	新 BOP 学童クラブ児童募集案内周知開始 随時オンライン申請フォーム稼働
令和8年　11月2日 ～令和8年12月15日	令和9年4月一斉受付（一次）
令和9年1月15日 ～令和9年2月10日	令和9年4月一斉受付（二次）
令和9年1月末	一次分決定通知発送
令和9年3月上旬	二次分決定通知発送



（3）　履行体制について

受託者は、本業務を遂行するにあたり、以下のとおり、管理責任者、現場責任者、従事者を配置すること。

管理責任者

①　受託者は、業務の統括を担う者として、本業務に従事する者の中に、常時1名以上の管理責任者を配置すること。

② 管理責任者の業務範囲は、以下に掲げるものとする。

ア 本業務の全体統括に関すること（進行管理、履行状況確認、業務報告）

イ 契約全般に関すること

ウ 区と受託者間の全体調整に関すること

エ 区と受託者間の連絡調整に関すること

オ その他、本業務全体の調整に関すること

③ 管理責任者は、本委託業務と同規模かつ類似の業務において、従事経験を有し、かつ責任者等の管理・監督業務の経験またはそれに準じる業務の経験を有する者をもって充てることとする。

現場責任者

① 受託者は、各現場における業務の統括を担う者として、履行場所にて本業務に従事する者の中に、常時1名以上の現場責任者を配置すること。

② 現場責任者の業務範囲は、以下に掲げるものとする。

ア 本業務の現場統括に関すること（進行管理、履行状況確認、業務報告）

イ 円滑に業務を実施する体制を整えること（業務分析、マニュアル作成、従事者への教育など）

ウ 従事者の適正な配置および指導に関すること

エ 業務遂行に伴う従事者の安全管理に関すること

オ 緊急時における従事者の安全確保に関すること

カ 区と従事者の円滑な連携の支援に関すること

キ 各業務の統括に関すること（履行状況確認、業務報告）

ク 従事者の現場における体制管理及び指揮監督に関すること

ケ 従事者相互の連携に関すること

コ 現場における個人情報保護に関すること

③ 現場責任者は、本委託業務と同規模かつ類似の業務において、従事経験を有し、かつ責任者等の管理・監督業務の経験またはそれに準じる業務の経験を有する者をもって充てることとする。

従事者

① 受託者は、業務を遂行するにあたり、あらかじめ従事者を定めること。

② 従事者は、本事業に従事する上記管理責任者及び現場責任者以外の者とする。

③ 区は、業務履行にあたる従事者の選任が不適当と認めた場合、受託者に変更など必要な措置を講ずることを求めることができる。

（4）新 BOP 学童クラブ利用手続き申請システムについて

①新 BOP 学童クラブ利用手続き業務に係る事務処理を円滑に行うため、利用者（保護者）、区担当課並びに各児童館および新 BOP 等の各拠点において、申請情報をネットワーク上で閲覧・処理可能なシステムを構築し、その運用支援業務を実施こと。

②システム構築にあたっては、ゼロからプログラムを書く従来の開発方法に比べて短期間で柔軟に業務システムの構築が可能であるローコード開発ツール（サイボウズ株式会社製 kintone）を基盤とした新 BOP 学童クラブ利用手続き申請システムを構築すること。また、当該システムへのアクセスについては、グローバル IP アドレスによる接続元制限（IP アドレス制限）等を設定すること。

③構築するシステムは、別紙1の階層ごとに閲覧権限を指定できること。なお、閲覧権限の詳細は別途区が指定する。

④本利用手続き業務における申請者情報について、区が管理する学童クラブ管理システムへ登録・更新するためのデータを区指定の拡張子で区に提供すること。

(5)事務センター業務について

①新 BOP 学童クラブ利用手続き業務について、申請の受付、審査等を行う事務センターを区庁舎外に設置し、運用すること。

4 業務の概要

(1)新 BOP 学童クラブ利用手続き申請システムに関する業務

(2)書類確認関連業務

(3)審査業務

(4)不備対応業務

(5)書類の発送準備業務

5 業務の詳細

(1)新 BOP 学童クラブ利用手続き申請システムに関する業務

①受託者はサイボウズ株式会社の kintone を基盤とした BOP 学童クラブ利用手続きに係る申請フォーム(以下※を参照)を区と協議のうえ構築すること。システム構築場所は、原則受託者事務所とし別紙2「情報セキュリティ対策基準(抜粋版)」及び別紙3「電算処理の業務委託契約の特記事項」を遵守した環境とする。区の庁内作業が必要な場合は、期間と人数を提示すること。

※現在稼働している申請フォームは以下(ⅰ)～(ⅷ)のとおり。

(ⅰ)入会申請

(ⅱ)延長利用申請

(ⅲ)延長利用辞退申請

(ⅳ)退会申請

(ⅴ)退会日変更申請

(ⅵ)利用料減免申請

(ⅶ)証明書交付申請

(ⅷ)取り下げ申請(入会・延長・減免・減免(長期欠席)

②オンライン申請システムは誰もが見やすく、利用しやすい仕組みを構築するとともにパソコンだけでなく、スマートフォン・タブレット等で容易に申請できるようにすること。

③区民が一般的に利用することが想定される端末機 OS にて操作可能なシステムを構築すること。

④申請フォームにおける項目の詳細やインターフェイスについては、区と受託者が協議のうえ決定すること。

⑤書類審査を行うにあたって必要となる手続きを把握しやすい画面構成であること。

⑥二重申請を防止するためのチェック機能を有すること。

⑦申請ステータス(審査状況、返戻状況等)など、申請から審査完了までのステータス管理が可

能であること。

⑧区から提供を受けた審査基準に基づき審査を行い、当該申請における審査内容を区及び受託者がシステム上で確認できること。

⑨申請者自身が申請内容及び申請に係る審査状況の閲覧が可能なシステムを構築すること。

⑩申請者から紙で申請された内容をスキャニング画像化してシステムにアップロードし、管理することが可能であること。

⑪システムの管理項目について、区が指定した条件によってデータを抽出することができ、かつ、当該データを CSV 形式で出力することが可能な機能を有すること。

（2）書類確認関連業務

①申請受付及び点検

ア 紙による申請の受付及び点検

・受領した紙申請書に受領印を押印する。

・確認書等及び受領した申請書類等でスキャニングを行い、画像データ化すること。これらのデータは、新 BOP 学童クラブ利用手続きシステム（以下、「システム」という。）に取込み、申請内容をシステムに反映すること。また、画像データは、区及び受託者が随時システム上で閲覧できる状態で管理すること。なお、データ形式は JPEG または PDF とする。

・確認書等の記載内容とシステムに反映された情報に相違がないか、複数の担当者によるチェックを必ず実施すること。

・受領した確認書等については、件数確認を行ったうえで、区へ報告すること。

イ オンラインによる申請の受付及び点検

・オンライン申請に係る申請情報の点検についても、システム等を十分に活用し、必要な対応を行うこと。

（3）審査業務

① 紙による申請の審査

・受託者は、上記（2）①でシステムに取込んだ申請情報及び画像データを確認し、申請内容の記入不備及び提出物の不足がないか一次審査を行う。審査は、区が提供する審査基準に基づき行い、審査結果はシステムに記録する。なお、審査基準に照らしても判断に迷う場合は、随時区の指示を仰ぐものとする。

・一次審査後は、必ず別の者が二次審査を行い、審査結果はシステムに記録すること。なお、二次審査においても確認項目は上記審査基準に基づくものとする。

② オンラインによる申請の審査

・受託者は、申請者がオンライン申請により入力した申請情報及び添付した画像データを確認し、申請内容に入力不備がないか及び添付画像との照合による一次審査を行う。審査は審査基準に基づき行い、審査結果はシステムに記録を行うものとする。なお、審査基準に照らしても判断に迷う場合は、随時区の指示を仰ぐものとする。

・一次審査後は、必ず別の者が二次審査を行い、審査結果はシステムに記録すること。なお、二次審査においても確認項目は上記審査基準に基づくものとする。

（4）不備対応業務

① 申請者への追加書類提出依頼

・受託者は、申請者に不足する資料（以下、「追加書類」という。）の提出依頼を行う。
不備の内容が、申請者当の記入した文字が難読であるなど、申請者への確認内容が軽微な場合においては、区と協議のうえ受託者が申請者に架電、メール送信等を利用して不足する情報の確認を行うことも可能とする。

② 追加書類受領時の審査

・受託者は、追加書類を受領した場合は、上記（3）同様に審査・記録を行うものとする。

③ 再審査後の不備対応

・再審査の結果、内容に不備がある場合、受託者は区の提供する様式に基づき、審査にあたり不足する情報及び資料を記載した不備連絡文書（以下「不備連絡文書」という。）を作成し、区の指定する書類を同封のうえ、申請者等宛てに発送する。不備連絡文書の発送後、区が定める期日までに申請者等から追加書類の提出がない場合は、区との協議により申請者へ架電またはメール送信等により督促及び補正することも可能とする。

④ 3（1）、（2）、（4）①～③の対応記録をシステムに記録し、受託者及び区が情報共有をリアルタイムに確認できる状態となるよう管理すること。なお、記録に不備がないか、リーダー等の管理者による確認を必ず行うこと。

（5）書類の発送準備業務

・受託者は、4月一斉受付時の「新 BOP 学童クラブ入会承認通知書」「新 BOP 学童クラブ延長利用承認通知書」を区が指定する封用に封入すること。

6 プロジェクト管理

（1）区への報告等

①本業務を推進するためのマススケジュール、WBS、作業フローを区と協議のうえ作成し、全体の進捗管理を行う。受託者は区に作業進捗を定期報告する。

②本業務を推進するための課題について、受託者にてまとめ、区に適宜報告する。区は報告を受けた課題について、受託者と協議のうえ、対応方針を決定する。

③遅延が発生している作業または遅延が想定される作業について、把握次第速やかに区に報告し、区及び受託者にて進捗回復の検討を行う。

（2）区及び事務従事者への操作説明及び対象者向けマニュアルの提供

①システムの操作方法について、区及び受託者が配置した従事者へ操作説明を実施する。

②システムの操作方法について、区より問い合わせがあった場合、適宜対応する。

③システムの操作方法について、マニュアルを作成し、対象者に提供する。

（3）システム運用保守

①システムのバージョンアップ、不具合修正は、受託者が対応すること。

②サーバーのハードウェアに不具合が生じた場合または定期メンテナンス等の保守作業が発生した場合

には、原則としてハードウェア保守事業者と共に立会い、保守作業支援を行うこと。

③区との連絡窓口は、土・日曜日及び国民の祝日に関する法律で規定する日を除く午前 9 時から午後 5 時まで受け付けることとし、問い合わせを受け付け、障害等の状況に応じて、迅速に対応を行うこと。

7 業務委託料

受託者に支払う経費は毎月の検査合格後、受託者の請求に基づき支払うものとする。

8 研修

業務の遂行に必要となる研修は、受託者の責任において実施することとし、業務開始後においても必要に応じて実施すること。相談対応等に当たっては、基本的なビジネスマナーを遵守し、相談者等の置かれている状況等について十分配慮した対応を心掛けるよう、従事者に徹底すること。なお、区はその研修に立ち会うことができる。

9 連絡体制

受託者は、区から管理責任者へ迅速に緊急連絡・業務報告・事務連絡等が行えるよう、連絡体制・連絡手段を確保し、区あて報告すること。

10 履行状況の報告

受託者は、区と定期的な連絡会議等を実施し、履行状況について区に報告しなければならない。また、区から求めがある場合には、受託した業務の履行状況等について書面等により報告しなければならない。なお、障害対応時の報告は速やかに行うものとする。

11 事故対応

(1)受託者は、事業の中断を引き起こすような災害発生等を想定し、早期復旧を図るための事業継続計画(BCP)を業務開始前に策定すること。

(2)落雷や電力会社の施設・設備の電気事故等による緊急停電、定期的なメンテナンス、計画停電などの影響を受けることなく業務が継続できるよう、必要な体制を整備すること。なお、復旧までに時間を要するような場合において、受託者の別拠点へ一時的に業務移管を行うことは可とする。この場合において、受託者は、当該別拠点及び一時的な業務体制について、区の承諾を得るものとする。

(3)業務の過程で発生したシステム破損等については、受託者の負担において、対応すること。

(4)万一事故が発生した場合は、受託者は直ちに区に通知するとともに、遅滞なくその状況を、書面をもって報告し、対応について区と協議し、その決定に基づき処理しなければならない。

12 運搬責任

(1)業務委託にかかわる書類、用品、資料及び納品すべき物品等の運搬が必要な場合には、受託者の責任で行うものとする。また、その物品等を区に受け渡す場合は、受領印及び確認印を押印した送付書または納品書を作成し、区、受託者双方で保管するものとする。

(2)個人情報を含む物品を運搬については、必ずセキュリティ便で行うものとし、契約期間中は常に使える

ようにしておくこと。なお、セキュリティ便とは、個人情報保護が施されており、かつ、受託者の作業場所と区の納品場所を直送で運搬するサービスを指す。

13 個人情報及び特定個人情報の保護

（1）受託者および従事者は、世田谷区個人情報保護条例に基づき、別紙3「電算処理の業務委託契約の特記事項」を遵守すること。

（2）この秘密の保持については、本契約終了後についても同様とする。

14 情報保護に関する義務

受託者は、善良なる管理者の注意義務と個人情報に関する法令ならびに条例等を遵守し、業務上知り得た事項について、他に漏洩し、または利用してはならない。

また、受託者において、業務用パーソナルコンピュータの管理・運営及び個人情報の保護について統括する現場責任者を定め、区へ通知するとともに、従事者に対し、次に掲げる基準を守ることを義務付けること。

（1）履行場所は、区が、管理責任者または現場責任者を通じて指定する場所に限ること。

（2）履行場所への入退出は、区が管理責任者または現場責任者を通じて許可した従事者のみに限ること。

（3）受託者は、業務履行に当たり使用した電算端末機、紙台帳に登載されている情報及びこの契約を履行するために用いた資料及びその結果等について、履行場所以外へ持ち出してはならない。

（4）受託者は、受託業務完了後は、区の指示により提出または廃棄を要するものを除き、区より受領したデータ及び紙台帳資料等を速やかに区に返却するとともに、作成したメモ等の記録を受託者の責任で断裁処分等、利用不能な状態にしなければならない。

（5）受託者は、区が別に廃棄を指示した機密古紙について、溶解処理にて廃棄を行い、そのすべてを溶解処理したことを証明する書類を作成し、溶解処理後１週間以内に区へ提出すること。

（6）受託者は、電子データの完全消去について、「消去証明書」を作成し、消去後１週間以内に提出すること。

15 契約不適合の保証

検査終了後1年の間に、受託者の行った作業内容に契約の内容に適合しないものがあった場合には、区は受託者に対して当該不適合の補修を求め、若しくは不適合の補修とともに区が実際に被った損害額を賠償請求できるものとする。

16 損害賠償

（1） 受託者は、従事者による事件・事故等が発生した場合は、直ちに区に報告すること。

（2） 業務を履行する上で、区または第三者に損害又は損失を及ぼしたときは、区の責に帰する場合を除き、受託者がその責を負うものとする。

（3） 業務を履行しないことにより、区または第三者に損害又は損失を及ぼしたときは、区の責に帰する場合を除き、受託者がその責を負うものとする。

17 権利の帰属

受託者が作成する作成物件の著作権は、契約金額の支払いをもって区に帰属する。但し、受託者が従前から有していた著作権、その他一切の権利は受託者に留保されるものとし、区は当該契約に基づいて自己利用するために必要な範囲で、これらを著作権法に従い利用できるものとする。業務の履行に関し新たに著作した成果物の著作権は区に帰属する。この場合も受託者が従前から有していた著作権、その他一切の権利は受託者に留保されるものとする。

18 契約形態

本契約の履行において必要な資材、作業場所等にかかる一切の費用は、区が提供するものを除き、受託者が支払いを行うものとし、その費用は契約金額に含まれるものとする。

19 再委託の扱い

(1)受託者は、業務の一部を第三者に再委託することができる。その場合、区に書面をもって事前に通知し、承諾を得ること。

(2)再委託をする場合は、再受託者にも本契約の内容を遵守させ、受託者は上記業務の管理監督義務を負うものとする。

(3)再受託者が区にとって不利益となる事象を発生させた場合、そのすべての責任を受託者が負うこと。

20 その他

(1)障害を理由とする差別の解消の推進に関する特記事項

受託者は、本業務の実施にあたり「障害を理由とする差別の解消の推進に関する法律」(平成 25 年法律第 65 号)を遵守するとともに、区が定めた「障害を理由とする差別の解消の推進に関する法律の施行に当たっての世田谷区の基本方針」及び「世田谷区における障害を理由とする差別の解消の推進に関する職員対応要領」に準じた取扱いをすること。なお、当該基本方針及び要領については、世田谷区ホームページ(https://www.city.setagaya.lg.jp/02083/2843.html)を参照すること。

(2)本仕様書の内容に疑義が生じた場合及び仕様書に記載のない事項は、区及び区契約事務担当と協議のうえ、決定する。

21 担当

世田谷区子ども・若者部児童課

電話 5432-2308 FAX5432-3016

住所 〒154-8504 世田谷区世田谷4－21－27

アクセス権限等
①受託事業者及び世田谷区児童課は全ての閲覧権限及び管理者権限を持つ

②児童館は管轄の新BOP分の閲覧権限を持つ

③新BOPは所属の新BOP分のみの閲覧権限を持つ

児童館名	新BOP名
01_池尻児童館	2_三宿小新BOP
	4_太子堂小新BOP
	9_多聞小新BOP
	28_池尻小新BOP
02_若林児童館	1_若林小新BOP
	22_山崎小新BOP
	31_城山小新BOP
03_弦巻児童館	12_駒沢小新BOP
	21_弦巻小新BOP
	25_三軒茶屋小新BOP
	27_松丘小新BOP
04_野沢児童館	13_旭小新BOP
	14_中里小新BOP
	18_駒繋小新BOP
	23_中丸小新BOP
05_上町児童館	5_桜小新BOP
	10_世田谷小新BOP
06_桜丘児童館	6_桜丘小新BOP
	29_笹原小新BOP
07_代田児童館	19_池之上小新BOP
	65_下北沢小新BOP
08_松沢児童館	11_松沢小新BOP
	15_松原小新BOP
	26_赤堤小新BOP

09_代田南児童館	7_代沢小新BOP
	24_代田小新BOP

10_等々力児童館	36_八幡小新BOP
	37_奥沢小新BOP
	38_尾山台小新BOP
	40_東玉川小新BOP
	42_九品仏小新BOP
	47_玉堤小新BOP

11_玉川台児童館	34_京西小新BOP
	41_桜町小新BOP
	43_瀬田小新BOP

12_森の児童館	33_玉川小新BOP
	46_中町小新BOP

13_深沢児童館	39_東深沢小新BOP
	44_等々力小新BOP

14_上用賀児童館	45_用賀小新BOP

15_新町児童館	32_深沢小新BOP

16_船橋児童館	20_経堂小新BOP
	56_船橋小新BOP
	63_希望丘小新BOP

17_喜多見児童館	61_喜多見小新BOP

18_成城さくら児童館	51_砧小新BOP
	52_明正小新BOP

19_山野児童館	59_山野小新BOP

20_祖師谷児童館	49_塚戸小新BOP
	50_祖師谷小新BOP

21_鎌田児童館	35_二子玉川小新BOP
	57_砧南小新BOP

22_烏山児童館	53_烏山北小新BOP
	58_給田小新BOP
	62_武蔵丘小新BOP

23_上北沢児童館	17_上北沢小新BOP
	54_八幡山小新BOP

24_上祖師谷ぱる児童館	48_烏山小新BOP
	60_千歳小新BOP

25_粕谷児童館	55_芦花小新BOP
	64_千歳台小新BOP

委託先事業者等公開用抜粋版

情報セキュリティ対策基準

【留意事項】
　本基準（委託先事業者等公開用抜粋版）は、区における情報システム構築等の外部委託案件に関し、情報セキュリティ対策の側面から外部委託事業者が遵守すべき内容を示すものである。
　文中には、「情報システム管理者は」というように職員が主語となっている内容であっても、実質的には「外部委託事業者に伝達のうえ情報システムに実装させることにより遵守すべき事項」等が存在する。
　以上を踏まえ、情報システム構築等の受託者においては、当該受託事案と関連のある記載事項全てを考慮した情報セキュリティ対策を講じること。

施行日：平成 24 年 11 月 21 日

世田谷区

改訂履歴

年月日	版番号	改訂理由・内容
平成 24 年 11 月 21 日	1.1	初版発行
平成 28 年 1 月 1 日	1.2	ポリシー改定を反映
平成 31 年 4 月 1 日	1.3	情報セキュリティ対策基準改定を反映
令和 2 年 4 月 1 日	1.4	情報セキュリティ対策基準改定を反映
令和 4 年 6 月 16 日	1.5	情報セキュリティ対策基準改定を反映
令和 5 年 4 月 1 日	1.6	情報セキュリティ対策基準改定を反映
令和 5 年 12 月 22 日	1.7	情報セキュリティ対策基準改定を反映
令和 7 年 4 月 1 日	1.8	情報セキュリティ対策基準改定を反映

目次

1　目的

本対策基準は、基本方針に定める情報セキュリティを確保するために遵守するべき行為及び判断等の基準を定め、情報資産を適切に取扱うことにより、安定的かつ継続的な行政サービスの提供を維持することを目的とする。

2　省略

3　適用範囲

(1)行政機関の範囲

対策基準が適用される行政機関は、区長部局、行政委員会、議会事務局とする。これらの対象行政機関で、情報資産に接する全ての職員（再任用職員及び会計年度任用職員を含む。以下同じ。）をいう。

(2)情報資産の範囲

本対策基準が対象とする情報資産は次のとおりとする。（ただし、教育委員会における学校教育に用いるものを除く。）

・ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

・ネットワーク及び情報システムで取り扱う情報（これらを印刷したものを含む。）

・情報システムの仕様書及びネットワーク図等のシステム関連文書

情報資産の種類	情報資産の例
ネットワーク	通信回線、通信ケーブル、ルータ等の通信機器
情報システム	サーバ、パソコン、モバイル端末、汎用機、複合機、オペレーティングシステム、ソフトウェア等
これらに関する施設・設備	コンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル等
電磁的記録媒体	サーバ、端末、通信機器等に内蔵される電磁的記録媒体と、USBメモリ、外付けハードディスクドライブ、DVD-R、磁気テープ等の電磁的記録媒体
ネットワーク及び情報システムで取り扱う情報	ネットワーク、情報システムで取り扱うデータ（これらを印刷した文書を含む。）

システム関連文書	システム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図等

4　省略

5　省略

6　情報システム全体の強靭性の向上

(1) マイナンバー利用事務系

ア　マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。ただし、マイナンバー利用事務系と他の領域を通信する必要がある場合は、通信経路の限定(MAC アドレス又は IP アドレス)及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。また、この場合においてもインターネットと接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された接続先については、この限りではなく、LGWAN を経由して、インターネットとマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。

イ　情報のアクセス及び持ち出しにおける対策

①情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない。

②情報の持ち出し不可設定

原則として、USB メモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

ウ　マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの扱い

マイナンバー利用事務系の端末・サーバ等と専用回線により接続されるガバメントクラウド上の情報システムの領域については、マイナンバー利用事務系として扱い、他の領域とはネットワークを分離しなければならない。

エ　マイナンバー利用事務系と接続されるクラウドサービス上での情報資産の取扱い

マイナンバー利用事務系の情報システムをガバメントクラウドにおいて利用する場合は、その情報資産の機密性を考慮し、暗号による対策を実施する。その場合、暗号は十分な強度を持たなければならない。

また、クラウドサービス事業者が暗号に関する対策を行う場合又はクラウドサービス事業者が提供する情報資産を保護するための暗号機能を利用する場合、クラウドサービス事業者が提供するそれらの機能や内容について情報を入手し、その機能について理解に努め、必要な措置を行わなければならない。

(2)LGWAN 接続系

ア　LGWAN 接続系とインターネット接続系の分割

LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータを LGWAN 接続系に取り込む場合は、次のいずれかの実現方法等により、無害化通信を図らなければならない。

①危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

②インターネット環境で受信したインターネットメールの本文のみを LGWAN 接続系に転送する方式

③インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式

イ　LGWAN 接続系と接続されるクラウドサービス上での情報システムの扱い

LGWAN 接続系の情報システムをクラウドサービス上へ配置する場合は、その領域を LGWAN 接続系として扱い、マイナンバー利用事務系とネットワークを分離し、専用回線を用いて接続しなければならない。

(3)インターネット接続系

①インターネット接続系においては、通信パケットの監視、及びふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見及び対処並びに LGWAN への不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

②都及び区市町村におけるインターネットとの通信を集約する自治体情報セキュリティクラウドに参加するとともに、関係省庁や東京都等と連携しながら、情報セキュリティ対策を推進しなければならない。

③業務の効率性・利便性の向上を目的として、インターネット接続系に主たる業務端末と入札情報や職員の情報等重要な情報資産を配置する場合、必要な情報セキュリティ対策を講じた上で、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施しなければならない。

④インターネット接続系に住民の個人情報を保存しないこと。業務上、やむを得ずインターネット接続系に保存が必要な場合は一時的なものとし、必要が無くなり次第直ちに削除すること。

7　物理的対策

(1)機器の取付け等

情報システムは、原則として次の措置を講じた上で設置しなければならない。ただし、設置場所の制約等により設置することができない事項にあっては、CISO 補佐の指定した取扱いを行うものとする。

ア　機器の取付け

情報システムに係る装置の取付けを行う場合は、火災、水害、埃、振動、温及び湿度等の影響をできる限り排除した場所に設置すると共に、施錠するなど容易に取り外すことができないような措置を講じなければならない。また、重要性の高い情報資産（重要性分類Ⅰ、Ⅱ等）を取扱うシステムは、災害時でも被害の程度が低いと想定される安全な場所に設置しなければならない。

ウ　機器の電源

①サーバ等の機器の電源については、当該機器を適正に停止するまでの間に十分な電力を供給する装置等を備え付けるように努めなければならない。

②落雷等による過電流に対してサーバ等の機器を保護するための措置を講じるように努めなければならない。

エ　通信ケーブル等の配線

①配線は、損傷や情報の傍受等を受けることがないように適正な措置を講じなければならない。

②情報化基盤管理者及び情報システム管理者は、通信ケーブル及び電源ケーブルの損傷などの報告に対して適正に対応しなければならない。

③情報化基盤管理者及び情報システム管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置するなど適正に管理しなければならない。

④情報化基盤管理者、情報システム管理者は、自ら又は情報システムの担当者及び契約により操作を認められた外部委託事業者等以外の者が配線を変更及び追加できないよう必要な措置を講じなければならない。

8　人的対策

情報資産の人的対策は、次に掲げるところにより実施するものとする。

(7)認証情報の管理

ウ　ID の取扱い

職員は、自己の管理する ID に関し、次の事項を遵守しなければならない。

①自己が利用している ID は、他人に利用させてはならない。

②共用 ID を利用する場合は、共用 ID の利用者以外に利用させてはならない。

エ　パスワードの管理

職員は、自己の保有するパスワードに関して、次の事項を遵守しなければならない。

①パスワードは、他者に知られないように管理すること。

②パスワードを秘密にし、パスワードの照会等には一切応じないこと。

③パスワードのメモの不用意な作成や、端末等の本体及びその周辺へのメモの貼り付けなどにより、パスワード流出の機会を作らないこと。

④パスワードは十分な長さとし、文字列は、想像しにくいものとすること。

⑤情報システム又はパスワードに対する危険の恐れがある場合は、速やかにパスワードを変更すること。

⑥複数の情報システムを取扱う職員は、パスワードをシステム間で共有しないこと。

⑦仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更すること。

⑧サーバ、ネットワーク機器及び端末等にパスワードを記憶させないこと。

⑨職員の間でパスワードを共有しないこと。ただし、ID の共用を指定されている場合はパスワードを共有できることとするが、この場合のパスワードは定期的に変更し、パスワードを再利用しないこと。

9　技術的及び運用における対策

情報資産の技術的及び運用における管理等は、次に掲げるところにより実施するものとする。

(1)コンピュータ及びネットワークの管理

イ　バックアップ

情報化基盤管理者及び情報システム管理者は、重要性の高い情報資産を取扱うシステム等に記録された情報については、冗長化措置にかかわらず、その重要度に応じて期間を設定し、定期的にバックアップを取らなければならない。

エ　情報システム仕様書等の管理

情報化基盤管理者及び情報システム管理者は、ネットワーク構成図及び情報システム仕様書等については、記録媒体にかかわらず業務上必要とする者のみが閲覧できるよう、適正に保管しなければならない。

オ　ログ及びシステム変更記録等の管理

①情報化基盤管理者及び情報システム管理者は、あらかじめ項目や保存期間等を定めて取得することとしたログ及び情報セキュリティの確保に必要な記録を全て取得し、一定期間保存しなければならない。

②情報化基盤管理者及び情報システム管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適正にログを管理しなければならない。
③情報化基盤管理者及び情報システム管理者は、定期的にログ等を分析及び監視しなければならない。
④情報化基盤管理者及び情報システム管理者は、基幹システム等、特に重要な情報を取り扱う情報システム及びネットワークについては、取得したログを定期的に点検若しくは分析する機能又は仕組みを設け、必要に応じて悪意ある第三者等からの不正侵入及び不正操作等の有無について点検又は分析しなければならない。なお、外部サービス提供者が収集し、保存する記録（ログ等）に関する保護（改ざんの防止等）の対応について、ログ管理等に関する対策や機能に関する情報を確認し、記録（ログ等）に関する保護が実施されているのか確認しなければならない。
⑤情報化基盤管理者及び情報システム管理者は、重要性分類Ⅱ以上の情報を取り扱う外部サービスの利用において、監査及びデジタルフォレンジックに必要となる外部サービス提供者の環境内で生成されるログ等の情報（デジタル証拠）について、外部サービス提供者から提供されるログ等の監視機能を利用して取得することで十分では無い場合は、外部サービス提供者に提出を要求するための手続を明確にしなければならない。

カ　障害記録

情報化基盤管理者及び情報システム管理者は、職員から報告のあった情報及びシステムの障害に対する処理並びに問題等を障害記録として体系的に記録し、常に活用できるように保存しなければならない。

ソ　電子署名　・暗号化

職員は、外部に送るデータについて区で定めるパスワード等による暗号化、共有リンク方式による等、セキュリティを考慮して、送信しなければならない。必要に応じて、電子署名を実施したうえで送信することが望ましい。
また、区で定めた方法で、暗号のための鍵を管理しなければならない。

（2)アクセス制御

ア　アクセス制御等

情報化基盤管理者及び情報システム管理者は、利用者がその権限を超えて情報システムを利用することができないように必要最小限の範囲で適切に設定する等、システム上制限しなければならない。

イ　利用者登録

①情報化基盤管理者及び情報システム管理者は、利用者の登録、変更、抹消、登録情報の管理、異動又は世田谷区外への出向等の職員及び退職者における

利用者 ID の取扱い等については、定められた方法にしたがって適正に行わなければならない。
②情報システムのアクセスに必要な利用者登録・変更は、情報化基盤管理者又は情報システム管理者に対する申請により行う。
③職員は、業務上必要がなくなった場合は、利用者登録を抹消するよう、情報化基盤管理者又は情報システム管理者に通知しなければならない。
⑤情報化基盤管理者及び情報システム管理者は、利用者に必要以上のアクセス権限が付与されていないか定期的に確認しなければならない。
ウ　管理者権限
①情報化基盤管理者及び情報システム管理者は、管理者権限等の特権 ID を利用する者を必要最小限にし、当該 ID のパスワードの漏えい等が発生しないよう、当該 ID 及びパスワードを厳重に管理しなければならない。
④情報化基盤管理者及び情報システム管理者は、特権 ID 及びパスワードの変更について、外部委託事業者に行わせる場合は、厳重に管理しなければならない。
⑤情報化基盤管理者及び情報システム管理者は、特権 ID 及びパスワードについて、人事異動の際のパスワードの変更、及び入力回数制限等のセキュリティ機能を強化しなければならない。
⑥情報化基盤管理者及び情報システム管理者は、特権 ID を初期設定以外のものに変更しなければならない。
オ　ログイン時の表示等
情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン･ログアウト時刻の表示等により、正当な権限を持つ職員がログインしたことを確認できる仕組みがある場合、これを有効に活用しなければならない。
カ　管理者によるパスワードの管理方法
パスワードの管理方法は次に掲げるとおりとする。
①情報化基盤管理者及び情報システム管理者は、職員のパスワードに関する情報を厳重に管理しなければならない。
②情報化基盤管理者及び情報システム管理者は、職員のパスワードについて、定期的にその妥当性について調査を行わなければならない。
③情報化基盤管理者及び情報システム管理者は、第三者に知られることのないよう、暗号化等パスワードの取扱いに注意しなければならない。
④情報化基盤管理者及び情報システム管理者は、職員に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更させることが可能なシステムとするよう努めなければならない。

⑤情報化基盤管理者及び情報システム管理者は、認証情報の不正利用を防止するための措置を講じなければならない。
キ　接続時間の制限
管理者権限によるネットワーク及び情報システムへの接続については、必要最小限の接続時間に制限しなければならない。
(3)システム開発、導入、保守等
ア　情報セキュリティ要求事項の分析及び明示
情報システム管理者は、情報システムの開発及び保守に関する情報セキュリティ要求事項を分析し、明確に定めなければならない。
イ　情報システムの調達
①情報システムの調達
(a)情報化基盤管理者及び情報システム管理者は、システム開発、導入、保守等の調達にあたっては、一般に公開する調達に関する仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。
(b)情報化基盤管理者及び情報システム管理者は、機器及びソフトウェアを購入等する場合、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。
②情報システムの受託事業者への対応
(a)新たな情報システムの開発を外部委託事業者等に委託する場合には、導入前のセキュリティ検証要求事項等を定めなければならない。
(b)情報システム管理者は、情報システムの受託事業者に対して名札等を着用させるとともに、必要に応じて身分証明書等の提示を求め、従事者の確認を行わなければならない。
ウ　情報システムの開発
①情報システムの開発における責任者及び作業者の特定
(a)情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。
(b)情報システム管理者は、システム開発案件に関するルールを定めなければならない。
②システム開発における責任者、作業者の ID の管理
(a)情報システム管理者は、システム開発の責任者及び作業者が使用する ID を管理し、開発完了後、開発用 ID を削除しなければならない。
(b)情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。
③システム開発に用いるハードウェア及びソフトウェアの管理
(a)情報システム管理者は、システム開発の責任者及び作業者が使用するハ

ードウェア及びソフトウェアを特定し、それ以外のものを利用させてはならない。
④ウェブアプリケーションの開発時の対策
情報システム管理者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講じなければならない。
(b)情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。
エ　開発と移行
①情報システム管理者は、重要なシステムについて、システム開発、保守及びテスト環境と、システム運用環境を分離しなければならない。
②情報システム管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。
③情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。
④情報システム管理者は、システム開発・保守に関連する資料及びシステム関連文書を適切に整備・保管しなければならない。
⑤情報システム管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。
オ　テスト
①情報システム管理者は、新たにシステムを導入する際には、既に稼働しているシステムに接続する前に十分な試験を行わなければならない。
②情報システムのオペレーティングシステムやソフトウェアを変更する場合には、その手続を定め技術的なレビュー及びテストを実施し、悪影響がないことを確認しなければならない。
③情報システム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。
④情報システム管理者は、システムの最終検証等の必要やむを得ない場合を除いて、個人情報及び機密性の高い情報資産を、テストデータに使用してはならない。
⑥情報システム管理者は、試験結果を CIO 補佐及び情報化基盤管理者へ報告するとともにその試験結果を厳重に保管しなければならない。
⑦情報システム管理者は、業務システムに誤ったプログラム処理が組み込ま

れないよう、不具合を考慮したテスト計画を策定し、確実に検証が実施されるよう、必要かつ適切に委託事業者の監督を行わなければならない。

カ　暗号による管理策

情報化基盤管理者及び情報システム管理者は、情報の機密性を保護するため、特に取扱いに慎重を要する電子データが不正アクセスにさらされないよう、必要に応じて暗号化技術を使用するように努めなければならない。暗号化技術を使用する際には、適用される法令及び規制、適用性や管理技術を十分に調査しなければならない。

ク　機器の修理及び廃棄

①電磁的記録媒体を有する機器について、外部委託事業者等に修理又は廃棄させる場合には、情報資産が復元できない状態で行わなければならない。

(4)不正プログラム対策（コンピュータウイルス対策）

ウ　情報システム管理者の措置事項

情報システム管理者は、次の事項を遵守しなければならない。

①サーバ及びパソコン等のウイルスチェックを行うこと。

②ウイルスチェック用のパターンファイルは常に最新のものに保つこと。

③ウイルスチェック用のソフトウェアは、常に最新の状態に保つこと。

(5)不正アクセス対策

ア　情報化基盤管理者及び情報システム管理者の措置事項

情報化基盤管理者及び情報システム管理者は、次の対策を講じなければならない。

①使用終了又は使用される予定のないデータの出入口（ポート）を長期間空けた状態のままにしてはならない。

②サーバ及びクライアント上の不要なサービスについて、機能を削除又は停止しなければならない。

③不正アクセスによるウェブページ書換え防止を確実にするために、データの書換え記録を保存し、情報化基盤管理者及び情報システム管理者が確認できるようにしなければならない。

(6)技術的脆弱性の管理

情報基盤管理者及び情報システム管理者は、情報システムの脆弱性に対し速やかに対応するために、以下の管理策を実施しなければならない。

ア　技術的脆弱性情報の取得

情報基盤管理者及び情報システム管理者はサーバ装置、端末及び通信回線装置等におけるセキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

イ　技術的脆弱性への対応
①情報基盤管理者及び情報システム管理者は技術的脆弱性情報の取得により判明した情報を、重要性及び影響範囲等を基に、速やかに関係者に通知しなければならない。
②通知を受けた関係者はその指示に従い、速やかに対策を講じなければならない。
(7)情報システムの管理
ア　情報システムの監視
①情報セキュリティに関する事案を検知するため、情報化基盤管理者及び情報システム管理者は、常に情報システムの監視を行わなければならない。
②上記の監視により得られた記録については、消去や改ざん等されないように適正な措置を講じ、定期的に安全な場所に保管するとともに、これらの記録の正確性を確保するため、正確な時刻の設定の措置を講じなければならない。
③外部と常時接続するシステムについては、ネットワーク侵入監視装置等を設置し、監視を行わなければならない。
⑦情報化基盤管理者及び情報システム管理者は、定期的に新たな脅威の情報を収集し、必要に応じて情報システムにおける監視の対象や手法を見直さなければならない。

１０　危機管理対策

情報資産への侵害等に対する危機管理対策については、次に掲げるところにより実施するものとする。
(1)緊急時対応計画の策定
CISO 又は情報セキュリティ委員会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合における体制、運用、証拠保全、被害拡大の防止及び復旧等の適切な措置を迅速かつ円滑に実施し、再発防止の措置を講じるために、緊急時対応計画を以下のとおり定める。
ア　関係者の連絡先及び緊急時対応マニュアル
①情報化基盤管理者及び情報システム管理者は、情報システムごとに緊急連絡先名簿、緊急時対応マニュアルを整え、全ての職員に対し緊急時の対応方法について周知しなければならない。
②情報化基盤管理者は、緊急時における情報収集及び区民への情報提供を行うことができるように体制を整え、情報提供に努めなければならない。

イ　発生した事案に係る報告すべき事項
①セキュリティに関する事案を発見した者は、次の項目について速やかにCISO補佐に報告しなければならない。
(a)事案の状況
(b)事案が発生した原因として、想定される行為
(c)確認した被害・影響範囲（事案の種類、損害規模、復旧に要する額等）
(d)ログ等
ウ　事案への対処
③情報システム管理者は、次の事項が発生し情報資産保護のために情報システムの停止がやむを得ないと判断した場合には、情報システムを停止しなければならない。その際、情報システム管理者は、緊急時対応マニュアルに基づき対応しなければならない。
(a)コンピュータウイルス等不正プログラムが、情報資産に深刻な被害を及ぼしているとき。
(b)災害等により電源を供給することが危険又は困難なとき。
(c)その他情報資産に係る重大な被害が想定されるとき。
④情報化基盤管理者及び情報システム管理者は、事案に係るシステムのアクセス記録及び経過記録等を保存しなければならない。
⑤情報化基盤管理者及び情報システム管理者は、事案に係る証拠保全を実施するとともに、再発防止の暫定措置を講じた後、早期に復旧に努めなければなければならない。復旧後、必要と認められる期間、再発監視を行わなければならない。

１１　省略

１２　法令遵守

(1)適用法令の識別
職員は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令や契約上の要求事項を遵守し、これに従わなければならない。
・地方公務員法（昭和２５年法律第２６１号）
・著作権法（昭和４５年法律第４８号）
・不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）
・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）
・サイバーセキュリティ基本法（平成２６年法律第１０４号）
・個人情報の保護に関する法律（平成１５年法律第５７号）

・世田谷区個人情報保護条例（令和５年３月条例第３号）

(2)知的所有権

著作権、意匠権、商標等の知的所有権に関わる物件の使用及びソフトウェア製品の使用許諾契約をする場合には、法的制限事項に適合するように実施しなければならない。

(3)個人情報の保護

個人情報を取扱う職員は、情報セキュリティポリシーのほか、世田谷区個人情報保護条例（令和５年３月条例第３号）も遵守し、その定めに基づいた対策を講じなければならない。

１３　省略

１４　委託による運用

(1)外部委託事業者の選定基準

①情報化管理者は、外部委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

②情報化管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、委託事業者を選定しなければならない。

１５　省略

１６　省略

１７　評価・見直し

(1)監査

ア　実施方法

CISO は、情報セキュリティ監査責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、毎年度及び必要に応じて監査を行わせなければならない。外部委託事業者等への監査についても同様とする。

電算処理の業務委託契約の特記事項
（兼電算処理の個人情報を取り扱う業務委託契約の特記事項）

（秘密保持義務）

1　受託者は、当該委託契約（業務内容に保守委託を伴う賃貸借契約等を含む。以下同じ。）に係る電算処理業務（以下「委託業務」という。）により知り得た個人情報その他の情報（以下「情報」という。）を、いかなる理由があっても第三者に漏らしてはならず、この旨を委託業務に従事する者（以下「従事者」という。）へ周知徹底しなければならない。また、契約期間満了後も、同様とする。

（書面主義の原則）

2　受託者は、本特記事項により通知、報告、提出等が求められている事項については、特段の定めがない限り、書面により行うものとする。

（管理体制等の通知）

3　受託者は、当該委託契約の締結後直ちに、以下の文書を区に提出しなければならない。提出後に内容の変更があった場合も、同様とする。

（1）情報セキュリティ及び個人情報保護に関する社内規程又は基準
（2）以下の内容を含む従事者名簿
　① 電算処理の責任者及び電算処理を行う者の氏名、責任、役割及び業務執行場所
　② 委託業務において個人情報を取り扱う者の氏名、責任、役割及び個人情報の授受に携わる者の氏名並びに業務執行場所
　③ 委託業務に関する緊急時連絡先一覧
（3）委託業務に係る実施スケジュールを明記した文書
（4）委託業務において使用する情報システムのネットワーク構成図（特定個人情報ファイル（コンピュータ等で検索することができるよう体系的に構成した情報の集合物であって、個人番号をその内容に含むもの。以下同じ。）を取り扱う場合のみ。第 23 項の事項を証するもの。）
（5）委託業務において使用する情報システムのセキュリティ仕様書（特定個人情報ファイルを取り扱う場合のみ。第 24 項の事項を証するもの。）
（6）クラウドサービス（有料、無料に関わらず、民間事業者等がインターネット上で提供する情報処理サービスで、約款への同意及び簡易なアカウントの登録等により当該機能が利用可能となるサービスのこと。以下同じ。）利用に係るリスク対策文書（委託業務においてクラウドサービスを利用する場合のみ。第 25 項の事項を証するもの。）

（再委託の禁止）

4　受託者は、委託業務の全部又は一部を、他の者に再委託してはならない。ただし、附属業務でやむを得ず再委託する必要があるときは、受託者は、再受託者（委託先の子会社（会社法（平成 17 年法律第 86 号）第 2 条第 1 項第 3 号に規定する子会社をいう。）である場合も含む。以下同じ。）に当該委託契約及び本特記事項を遵守させ、かつ、再受託者にかかる再委託の内容及び第3項に規定する事項を、区に事前に書面をもって通知し、その承認を得なければならない。

　再受託者も、委託業務の全部又は一部を、他の者に更に再委託してはならない。附属業務でやむを得ず更に再委託する必要があるときは、再委託と同様の条件と手続きにより、区の承認を得なければならない。更に再委託が繰り返される場合も同様とする。

（目的外使用等及び複写等の禁止）

5　受託者は、委託業務で取り扱う情報を委託業務の目的以外に使用してはならない。また、第三者に提供してはならない。

6　受託者は、区が委託業務での使用を目的として受託者に提供し、又は貸与する情報及び情報資産（世田谷区電子計算組織の運営に関する規則（平成16年世田谷区規則第47号）第2条第9号に規定する情報資産をいう。以下同じ。）を、委託業務以外の目的に使用してはならない。

7　受託者は、委託業務で取り扱う情報及び情報資産について、業務上必要なバックアップを取得する場合を除き、区の承認を得ずに複写してはならない。委託業務を実施する上でやむを得ず複写するときは、あらかじめ区に通知し、その承認を得なければならない。この場合において、委託業務の終了後、受託者は、直ちに複写した電磁的記録の消去及び印刷物の廃棄を行い、使用できない状態にするとともに、消去又は廃棄した日時、担当者及び処理内容を区に報告しなければならない。

8　受託者は、区の事前の承諾なく、委託業務で取り扱う情報及び情報資産を区の事業所または受託者の事業所から持ち出してはならない。

（物的セキュリティ対策）

9　受託者は、委託業務に使用する情報システムに係る装置の取付けを行う場合は、できる限り、火災、水害、埃、振動、温度、湿度等の影響を受けない場所に設置するものとし、施錠等容易に取り外すことができないよう必要な措置を講じなければならない。

10　受託者は、委託業務に係る区が運用する情報システムのサーバ等を区庁舎外に設置する場合は、区の承認を得なければならない。また、定期的に当該サーバ等への情報セキュリティ対策状況について確認するとともに、区から要請があった場合は、その結果を区に報告しなければならない。

11　受託者は、その従事者に名札等の着用及び身分証明書等の携帯を義務付け、区の情報システム室その他の区の管理区域に立ち入る場合において区から求められたときは、身分証明書等を提示するよう指導しなければならない。

12　受託者は、委託業務で使用するパソコン等の盗難を防止するため、当該パソコン等をセキュリティワイヤーで固定し、又は従事者が業務執行場所を離れる間において施錠可能なロッカー等に収納させるなどの措置を講じなければならない。

（人的セキュリティ対策）
13　受託者は、委託業務において、区に提出した情報セキュリティ及び個人情報保護に関する社内規程又は基準を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに区に報告し、代替策について協議しなければならない。
14　受託者は、情報及び情報資産を適切に保管するものとし、パソコン等により情報及び情報資産を使用する場合は、第三者に使用され、又は閲覧されることがないように、離席時にパスワードロック又はログオフ等を行わなければならない。
15　受託者は、従事者に情報システムの保守又は運用業務に関し、次の事項を遵守させなければならない。
（1）自己が利用している ID は、他人に利用させないこと（ID の共用を指定されている場合は除く。）。
（2）共用 ID を利用する場合は、共用 ID の利用者以外の者に利用させないこと。
（3）パスワードを秘密にし、パスワードの照会等には一切応じないこと（パスワード発行業務を除く。）。
（4）パスワードのメモの不用意な作成等により、パスワード流出の機会を作らないこと。
（5）パスワードは、十分な長さとし、想像し難い文字列とすること。
（6）複数の情報システムを取り扱う場合は、パスワードを情報システム間で共有しないこと。
（7）パソコン等のパスワードの記憶機能を利用しないこと。
（8）社員間でパスワードを共有しないこと（ID の共用を指定されている場合を除く。）。
16　受託者は、従事者に対して、情報セキュリティに関する教育及び緊急時対応のための訓練を計画的に実施しなければならない。

（技術的及び運用におけるセキュリティ対策）
17　受託者は、情報システムの保守又は運用業務を遂行するに当たり、情報システムの変更記録、作業日時及び実施者を記録するとともに、各種アクセス記録及び情報セキュリティの確保に必要な記録を全て取得し、一定期間保存しなければならない。
18　受託者は、アクセスログ等を取得するサーバについて、正確な時刻設定を行わなければならない。自動的にサーバ間の時刻同期が可能な場合は、その措置を講じなければならない。
19　受託者は、情報システム等に記録された重要性の高い情報について、定期的にバックアップを取得しなければならない。また、バックアップの取得前にその手法を区に通知し、承認を得なければならない。
20　受託者は、情報システムの開発及び導入に当たり、開発及び導入前に区と協議の上、情報セキュリティに係る検証事項を定め、検証を実施しなければならない。
21　受託者は、委託業務に使用する情報システムがネットワークに接続されている場合は、不正アクセスを防ぐため、常にセキュリティホールの発見に努め、メーカー等からのセキュリティ修正プログラムの提供があり次第、情報システムへの影響を確認し、区と協議の上、修正プログラムを適用しなければならない。また、ウィルスチェックを行い、ウィルスの情報システムへの侵入及び拡散を防止しなければならない。
22　受託者は、情報システムを開発する場合は、システム開発及びテスト環境と、本番運用環境を分離しなければならない。
23　受託者は、委託業務において特定個人情報ファイルを取り扱う場合は、当該特定個人情報ファイルをインターネットから物理的又は論理的に分離された環境にて取り扱わなければならない。
24　受託者は、委託業務に使用する情報システムにおいて特定個人情報ファイルを取り扱う場合は、定期に及び必要に応じ随時に当該情報システムのログ等の分析を行うなど不正アクセス等を検知する仕組みを講じるとともに、当該情報システムの不正な構成変更（許可されていない電子媒体、機器の接続等、ソフトウェアのインストール等）を防止するために必要な措置を講じなければならない。
25　受託者は、委託業務においてクラウドサービスを利用する場合は、当該クラウドサービスの利用に伴い想定される情報セキュリティ上のリスクを回避するために必要な措置を講じなければならない。（例：当該クラウドサービス提供事業者が公表している情報セキュリティ対策内容の確認、受託者が従業員に付与するクラウドサービス用 ID の適切な付与管理、クラウドサービス上に記録した情報が第三者に提供される場合についての確認、サービス利用終了時のデータの取扱い条件の確認、等）

（データのセキュリティ対策）
26　受託者は、委託業務に関し、区より情報及び情報資産を受領した場合は、預かり証を区に対して交付しなければならない。また、当該情報及び情報資産を適切に管理するため、情報及び情報資産の受領日時、受領者名、受領した情報及び情報資産の種類等の記録簿を作成するとともに、区から要請があった場合は、速やかに当該記録簿を区に提示しなければならない。
27　受託者は、委託業務に係る重要度の高い情報及び情報資産を運搬する場合は、可能な限り暗号化、パスワード設定等の保護対策を行い、鍵付きのケース等に格納する等、情報及び情報資産の滅失や不正利用を防止するための処置を講じなければならない。また、重要度の高い情報を電子メール等で送受信する場合は、暗号化、パスワード設定等の保護対策を行わなければならない。
28　受託者は、委託業務で取り扱う情報及び情報資産を施錠可能な金庫、ロッカー等に適切に保管する等善良な管理者の注意をもって当たり、情報及び情報資産の取扱いには十分注意し、情報及び情報資産の滅失、毀損及び漏えいの防止に努めなければならない。
29　受託者は、委託業務が終了したときは、区より受領した情報及び情報資産を速やかに区に返却しなければならない。また、返却が不可能な場合は、区の了承のもと、バックアップデータを含む電磁的記録の消去及び印刷物の廃棄を行い、使用できない状態にする（電算処理機器を廃棄する場合は復元できない状態にする）とともに、消去又は廃棄した日時、担当者及び処理内容を区に報告しなければならない。
30　受託者は、情報資産の作成業務を終了したときは、直ちに当該情報資産を区があらかじめ指定した職員に引き渡さなければならない。

（電算処理機器の廃棄）
31　受託者は、委託業務で使用しているサーバ、パソコン等の機器（以下これらを「電算処理機器」という。）を廃棄する場合は、事前に当該電算処理機器に保存されている情報及び情報資産を消去、復元できない状態にした上で廃棄

しなければならない。

（委託業務の報告）

32　受託者は、区に対し、委託業務の状況を定期的に報告するものとする。ただし、必要があるときは、その都度報告するものとする。

（監査、施設への立入検査の受入れ）

33　受託者は、情報及び情報資産の情報セキュリティ管理状況について、区の求めに応じて報告するものとする。また、区が必要に応じて監査又は検査を実施する場合は受け入れなければならない。なお、再受託者及び更に再委託が繰り返される場合も同様とする。

34　受託者は、区が必要とする場合は、業務執行場所へ区の職員の立入りを認めるものとする。

（緊急時の対応）

35　受託者は、委託業務において、業務上のトラブル、災害、事故、電算処理機器の不良、故障及び破損等が発生した場合は、直ちに区にその状況について報告し、区の指示に従わなければならない。

36　受託者は、委託業務について次に掲げる事象が発生した又は発生したおそれがある場合は、直ちに、区にその状況を具体的に報告しなければならない。

（1）情報及び情報資産の滅失
（2）情報及び情報資産の毀損
（3）情報の漏えい
（4）不正アクセス
（5）情報セキュリティポリシーの違反
（6）前各号に掲げるもののほか、情報セキュリティに悪影響を及ぼす事象

（サービスレベルの保証）

37　受託者は、委託業務のサービスレベルについて、事前に区と合意している場合は、そのサービスレベルを保証するものとする。

（契約解除及び損害賠償）

38　受託者が、法令及び本特記事項に違反した場合、区は、この契約を解除することができる。ただし、債務の不履行がこの契約及び取引上の社会通念に照らして軽微であるときは、この限りでない。また、受託者は、本特記事項に違反し、又は本特記事項を履行しなかったことにより、区に損害が生じた場合には、区に対しこれを賠償するものとする。