別紙1

業務委託概要

1 委託内容

(1) BCP 改定等支援業務

ア 計画の立案

支援全体のスケジュール及び支援内容を確認するため、実施計画書の作成及び説明を行うこと。

イ 災害時優先業務の選定

非常時優先業務に関しては、区の業務全般を洗い出し、その中から災害応急対策業務、通常業務のうち業務優先度が高いもの並びに災害発生後の他の新規発生業務及び災害復旧・復興業務を選定し、一覧としてまとめること。

ウ 目黒区業務継続計画書の改定

（ア）「市町村のための業務継続計画作成ガイド」に掲げる「業務継続計画の特に重要な6要素」を踏まえつつ、東京都業務継続計画等も参考としながら、業務継続計画の概要、想定する様々な規模の災害や危機事象における被害、非常時優先業務、業務継続のための執行体制及び執行環境並びに計画の実行性確保のための取組、訓練計画等を盛り込んだ内容とすること。

（イ） 本計画書とは別に、外部公表向けの概要版を作成すること。

（ウ） 策定した計画案について、発注者に対するレビューを実施し、承認を得ること。

エ 行動計画書の策定

行動計画書とは、BCP 発動時における職員の行動手順を明確にし、災害時等において非常時優先業務への円滑な移行や的確な業務実施に向けた具体的なプロセスを示したものである。

行動計画書には、発災時の手順書として「行動手順書」を含め、発災時の手順書として必要な要素を全て含めるとともに、可能な限り簡潔にまとめ、職員が容易に理解可能なものとすること。

行動手順書の作成に当たっては必要に応じて主管課にヒアリングを実施することとする。また、決裁権者の不在、資源の欠落及び職員の負傷等に依らず職員が自ら行動できるための手順書とすること。

策定した計画案について、発注者に対するレビューを実施し、承認を得ること。

オ 訓練計画の策定

（ア） 次年度以降に実施予定の訓練について、具体的な訓練手法を検討するとともに、発注者に提案すること。なお、ここでいう訓練とは大規模災害等の発生時を想定した非常時優先業務への移行訓練に加えて、区職員を対象とした BCP への理解促進、業務継続計画発動時おけるシミュレーション、異常発生時に各課の業務継続を可能とするための必要な知識や行動の習得等を目的とした研修を含むものとする。

（イ） 訓練計画は、継続的実施や計画の改善に繋がるような実効性の高いものとすること。また、中長期的な視点も取り入れること。

（ウ） 作成した計画案について、発注者に対するレビューを実施し、承認を得ること。

（2） ICT-BCP 策定等支援業務

ア 計画の立案

支援全体のスケジュール及び支援内容を確認するため、実施計画書の作成及び説明を行うこと。

イ 優先システムの選定

優先システムとは、非常時優先業務を実施するに当たり必要不可欠となるICT資源を指し、庁内LANやWANを構成するネットワーク及び業務用端末を含むものである。

非常時優先業務を実施するに当たり必要不可欠となるICT資源を洗い出す。その中から、システム依存度を考慮し、優先システムを選定し、一覧としてまとめること。

ウ 復旧目標の設定

（ア） 優先システムごとに目標とする対策レベルを設定すること。

（イ） 優先システムごとの目標復旧時間について設定すること。

エ 現状の課題把握

（ア） 優先システムが被害を受ける可能性を把握するため、考えられる被害状況の案（以下「リスクシナリオ」という。）を提示すること。

（イ） リスクシナリオの作成に当たっては、発注者の庁舎の状況（耐震性等）、対象システム及び対象ICT資源の状況（サーバー類の設置場所等）を踏まえて検討すること。なお、必要な情報については、発注者から提供する。

（ウ） リスクシナリオを踏まえ、優先システムにおける対策の実施状況、被害を受ける可能性について調査を行うこと。

オ リスク対策案の策定

（ア） 優先システムの脆弱性に対して、補強、代替手段などの対策案を策定すること。

（イ） リスク対応策については、費用対効果を明確にすること。

（ウ） 対策案でも対応できない残存リスクについても整理すること。

カ 目黒区ICT業務継続計画書の策定

（ア） 基本方針、想定脅威、想定脅威発生時の対応、優先システム、推進体制と役割、リスクシナリオと対策、残存リスク、復旧等に関する内容、訓練計画等、各種計画を策定し、記載すること。

（イ） 本計画を次年度以降推進していく上での維持管理方針についても具体的に示し、将来の情報システム更改等を想定し、メンテナビリティ（保守性）に重点を置き、維持管理が容易に行えるよう構成すること。

（ウ） 本計画書とは別に、外部公表向けの概要版を作成すること。

（エ） 策定した計画案について、発注者に対するレビューを実施し、承認を得ること。

キ　行動計画書の策定

行動計画書とは、ICT-BCP 発動時における職員の行動手順を明確にし、優先システム復旧に向けた具体的なプロセスを示したものである。

行動計画書には、発災時の手順書として「行動手順書」を含め、発災時の手順書として必要な要素を全て含めるとともに、可能な限り簡潔にまとめ、職員が容易に理解可能なものとすること。

行動手順書は、発災時に優先システムが使用できなくなった状況を想定し、窓口業務を継続して実施するための復旧手順を含むものとし、その作成に当たっては必要に応じて主管課にヒアリングを実施することとする。また、決裁権者の不在、資源の欠落及び職員の負傷等に依らず職員が自ら行動できるための手順書とすること。

策定した計画案について、発注者に対するレビューを実施し、承認を得ること。

ク　運用手順書の策定

（ア）運用手順書とは、目黒区ICT業務継続計画書の内容に沿って、ICT-BCP の対象となる優先システムなどについて、分析作業や更新作業を行う手順を示したものである。運用手順書に基づいて、定期的に目黒区ICT業務継続計画の見直しを行うことで実効的・実践的な計画とすることを想定している。

（イ）運用手順書についても、目黒区ICT業務継続計画書及び行動計画書等の策定内容に沿って内容の見直しを行うとともに、分かりやすく、理解しやすいものとすること。

（ウ）策定した手順書案について、発注者に対するレビューを実施し、承認を得ること。

ケ　訓練計画の策定

（ア）次年度以降に実施予定の訓練について、具体的な訓練手法を検討するとともに、発注者に提案すること。なお、ここでいう訓練とは障害発生時を想定した障害訓練に加えて、区職員を対象としたICT-BCP への理解促進、ICT-BCP 発動時おけるシミュレーション、異常発生時に各課の業務継続を可能とするための技能習得等を目的とした研修を含むものとする。

（イ）訓練計画は、継続的実施や計画の改善に繋がるような実効性の高いものとすること。また、中長期的な視点も取り入れること。

（ウ）作成した計画案について、発注者に対するレビューを実施し、承認を得ること。

（3）BCP 改定及びICT-BCP 策定等支援業務共通

ア　パブリックコメント実施支援

意見募集結果の取りまとめ支援やパブリックコメントの実施により目黒区業務継続計画書及び目黒区ICT業務継続計画書に反映すべき事項があった場合には、必要に応じて更新すること。

（4）BCP 及び ICT-BCP 訓練の実施及び見直し（令和9年度・10年度）

BCP 及び ICT-BCP の実効性を高めるため、以下のとおり、訓練の実施及び見直しを行うこと。

ア BCP

1(1)オで策定した訓練計画に沿って当区職員を対象とした机上訓練、実働訓練を実施すること。なお、業務プロセス、業務分掌及び体制の変更があった場合には、必要に応じて1(1)オで策定した訓練計画を更新すること。

訓練後は、訓練結果を踏まえた課題や見直し事項を整理し、訓練計画書に反映すること。

イ ICT－BCP

1(2)ケで策定した訓練計画に沿って当区職員を対象とした机上訓練、実働訓練を実施すること。なお、システム構成、業務プロセス、業務分掌及び体制の変更があった場合には、必要に応じて1(2)ケで策定した訓練計画を更新すること。

訓練後は、訓練結果を踏まえた課題や見直し事項を整理し、訓練計画(行動手順書等)に反映すること。

2 プロジェクト管理

(1)プロジェクト計画書の策定

業務全体のプロジェクト管理方法、体制、計画(作業ごとの詳細スケジュール含む。)等を具体的に記載したプロジェクト計画書について、契約確定の日から2週間以内に作成及び提出し、発注者の承認を得ること。なお、おおむね半年に1度、発注者に対して進捗状況の報告(中間報告及び最終報告)を行うこと。

(2)プロジェクト管理

プロジェクト計画書に基づき、以下に示す事項を含む本委託に係るプロジェクト管理を行うこと。

ア 進捗管理

各タスクの状況把握及びスケジュール管理を行うため、次の要件を満たす進捗管理を実施すること。

(ア)WBS(Work Breakdown Structure)を作成し、作業工程ごとに必要な成果物及び作業タスクを明確にすること。

(イ)プロジェクトの進捗状況を WBS 等により、定量的に管理すること。

(ウ)計画から遅れが生じた場合は、原因を調査し、要員追加や担当者変更等の体制見直しも考慮した改善策を提示し発注者の承認を得た上で、実施すること。

イ 課題管理

プロジェクト遂行中に発生した各種課題を一元的に管理するため、次の要件を満たす課題管理を実施すること。

(ア)課題の内容、発生日、優先度、解決予定日、担当者、対応状況、対応策、対応結果、解決日等の情報を一元的に管理すること。

(イ)対応状況を確認及び報告し、課題の経過状況を発注者と共有することで、迅速な解決に取り組むこと。

ウ　リスク管理

プロジェクトの円滑な進行を阻害するプロジェクト内外のリスクを特定し、対応策の検討、実施状況等を管理するため、次の要件を満たすリスク管理を実施すること。

（ア）プロジェクトの遂行に影響を与えるリスクを特定し、その発生要因、発生可能性、影響度及びリスク軽減策を整理すること。また、定期的にリスクを監視及び評価し、その結果を発注者と共有することで、リスクによる影響の抑制に努めること。

（イ）リスクの発生に備え、緊急対応時の体制及び計画を整備し、発注者の承諾を得ること。

エ　品質管理

プロジェクトの運営管理及び成果物の品質を保証するため、次の要件を満たす品質管理を実施すること。

（ア）作業工程ごと及び納入成果物ごとに品質評価基準等を設定し、評価結果を発注者に報告し、承諾を得ること。

（イ）検証、品質改善策の検討及び実施を管理する体制を構築するとともに、品質改善のための各種取組が、プロジェクト計画書に定められた手続に則って実施されていることを確実に確認・報告すること。

オ　変更管理

プロジェクトの成果物の構成及び変更の履歴を管理するため、次の要件を満たす構成・変更管理を実施すること。プロジェクトの進捗や成果物の品質に影響を及ぼすような大規模な仕様追加・変更が発生した場合には事前に発注者に報告し、承諾を得ること。

（ア）成果物の変更の履歴を管理する構成管理対象を特定し、適切に管理すること。

（イ）変更履歴を管理するだけではなく、構成管理対象は品質低下対策のため、最新版や特定時点の版を、いつでも提供できる仕組みを確立すること。

（ウ）仕様や構成管理対象の変更について、定期的に監査及び評価し、問題があった場合には、発注者に報告すること。

カ　コミュニケーション管理

プロジェクトに係る全ての参画者による円滑かつ効率的なコミュニケーションを可能とするため、次の要件を満たすコミュニケーション管理を実施すること。

（ア）作業工程ごとにおける各種作業に関する打合せ、成果物等のレビューのほか、プロジェクトの進捗状況・課題等に関する報告を行う会議（打合せ）を開催すること。

（イ）打合せについては、内容、対象者等を明確にすること。併せて、打合せの頻度及び参加者は、発注者と受託者の協議により決定するものとする。ただし、少なくとも月に1回以上開催することとし、発注者側の各担当及び受託者側の調査・支援要員が出席することを前提とする。

（ウ）打合せが開催される都度、原則として5開庁日以内に議事録を提示し、発注者の承認を得ること。打合せについては、発注者の要求に応じて議事録を提示し、発注者の承認を得ること。

（エ）受託者は、コミュニケーションの方法として、オンライン会議、対面会議、電子メール、発注者が指定し受託者が利用可能なコミュニケーションツール及び電話等に対応すること。

電話による問合せ対応時間は、目黒区の休日を定める条例（平成元年目黒区条例第 1 号）第1条第1項各号に規定する目黒区の休日を除く、午前 9 時から午後 5 時までを基本とすること。

オンライン会議の実施に当たっては、発注者が指定するツール（Microsoft Teams）を使用すること。

（カ）受託者は、丁寧で分かりやすいコミュニケーションを行うこと。また、クラウドやネットワーク等に関する知識がほとんどない業務担当者から詳しい職員まで幅広い知識レベルの者を想定し、相手に応じて適切な会話を行うこと。

キ　セキュリティ管理

各作業工程におけるセキュリティに関する事故及びその未然防止のため、定期的にチェックリスト等による点検を行うこと。

2　機密情報の保護

別紙1－1「機密情報の取扱いに関する標準特記仕様書」のとおり

3　成果物の提出

本業務で作成した成果物は、発注者と調整の上で必要な時期に提出し、それらを取りまとめた納品物として、次の項目を期限内に納品すること。

※電子データによる成果品は、修正可能な形式（ワードやエクセル）とし、メンテナビリティ（保守性）に留意すること。

※下記（1）及び（2）については、区民にわかりやすく読み手の興味を惹くデザイン・構成及び色彩におけるアクセシビリティや音声ガイダンスの導入等多様性に配慮し、冊子に用いるイラスト等は地域福祉の視点に配慮したものとし、受託者オリジナルのものを作成することする。

（1）目黒区業務継続計画改定

ア　目黒区 BCP 業務継続計画書（基本計画書）

（ア）素案

・電子データで1部

（イ）完成版

・電子データで1部

・A4 判／両面4色刷り／あじろ綴じ製本／1部

イ　行動計画書（行動手順書含む。）

電子データで1部

ウ 訓練計画

電子データで1部

エ 外部公表向けの概要版

(ア)素案

・電子データで1部

・A4 判／両面 4 色刷り／中綴じ正本製本／500部

(イ)完成版

・電子データで1部

・A4 判／両面 4 色刷り／中綴じ正本製本／500部

(2)目黒区ICT業務継続計画策定

ア 目黒区ICT業務継続計画書(基本計画書)

(ア)素案

・電子データで1部

(イ)完成版

・電子データで1部

・A4 判／両面4色刷り／あじろ綴じ製本／1部

イ 行動計画書(行動手順書含む。)

電子データで1部

ウ 運用手順書

電子データで1部

エ 訓練計画

電子データで1部

オ 概要版

(ア)素案

・電子データで1部

・A4 判／両面 4 色刷り／中綴じ正本製本／500部

(イ)完成版

・電子データで1部

・A4 判／両面 4 色刷り／中綴じ正本製本／500

(3)本業務の進捗管理

ア 議事録

(4)その他、本業務において作成した資料等

4 業務体制

(1)プロジェクト管理者

プロジェクト管理者は、プロジェクト全ての運営管理及び成果物の品質に係る責任を持つ者である。

プロジェクト管理者に求める要件は、国内の自治体に係る BCP や ICT-BCP の策定・改定におけるプロジェクト管理者の経験を有すること。

(2)プロジェクトリーダー

プロジェクトリーダーは、それぞれの業務において、主体となって区と調整し、担当タスクについて責任を持つ者である。

プロジェクトリーダーに求める要件は、国内の自治体に係る BCP や ICT-BCP の策定・改定におけるプロジェクトリーダーの経験を有すること。

(3)プロジェクトメンバー

プロジェクトメンバーは、プロジェクト管理者又はプロジェクトリーダーの指示を受け、本業務委託の目的に沿って、業務を円滑、迅速かつ確実に遂行する者である。

プロジェクトメンバーに求める要件は、プロジェクトメンバーのうち1名以上は国内の自治体に係る BCP や ICT-BCP の策定・改定におけるプロジェクトメンバーとしての経験を有すること。

(4)体制変更

本業務を担当する主たる者は、原則として委託期間中変更しないこととする。

やむを得ず変更する場合は、変更予定の1か月前までに発注者に報告すること。

また、体制を変更する場合は、受託者の責任においてその内容及び修正済のドキュメント一式を他の要員に引き継ぐこと。

5 その他

(1) 本業務はすべて受託者で行い、業務の一部であっても発注者の同意なく再委託は行わないこと。また、不測の事態発生時に業務が滞ることのないように人員を配置すること。

(2) 受託者は、貸与を受けた資料等の取扱に十分注意し、本業務終了後、速やかに発注者に返却するものとする。なお、業務処理上作成した資料等の文書一切を抹消、焼却、切断など復元不可能な状態にして処分するものとする。

(3) 労働基準法をはじめ関係法令を遵守し、業務を履行しなければならない。

(4) 本仕様書に記載されていない事項又は仕様について疑義が生じた場合は、その都度協議の上、誠意をもって実施すること。

以　上

別紙1－1

機密情報の取扱いに関する標準特記仕様書

（基本的事項）

第1条　受注者は、この契約による事務の実施に当たり、個人情報（特定個人情報を含む。以下同じ。）を取り扱うときは、その保護の重要性を認識し、個人の権利利益を侵害することのないよう、個人情報の保護に関する法律（平成15年法律第57号）（特定個人情報を取り扱う場合は、行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）を含む。）その他の関係法令を遵守し、個人情報の漏えい、滅失又は毀損の防止その他の個人情報の安全管理のために必要かつ適切な措置を講じなければならない。

2　受注者は、この契約による事務の実施に当たっては、目黒区情報セキュリティ基本方針を遵守し、機密情報（個人情報のほか、この契約に基づき発注者から提供を受ける技術情報及び行政の運営上の情報のうち、秘密である旨を示された機器等の情報資産（メモ及びバックアップ等を含む。）をいう。以下同じ。）を適正に取り扱わなければならない。

（秘密保持義務）

第2条　受注者は、この契約による事務により知り得た機密情報をいかなる理由があっても第三者に漏らしてはならず、この旨を当該事務に従事する者（以下「従事者」という。）へ周知徹底しなければならない。この契約が終了し、又は解除となった後においても同様とする。

（書面主義の原則）

第3条　受注者は、この仕様書に定める事項により通知、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。

（個人情報保護方針の公表）

第4条　受注者は、この契約による事務において個人情報を取り扱う場合は、個人情報の保護に関する法律等の法令に基づき、個人情報保護方針を公表していなければならない。

参考：個人情報保護方針の公表項目

1　取得する個人情報の利用目的
2　保有個人データに関する事項
3　開示等の請求に応じる手続
4　問い合わせ及び苦情の窓口
5　オプトアウトにより個人情報を第三者へ提供する場合は、次に掲げる事項
・第三者への提供を利用目的とすること
・第三者に提供される個人データの項目
・第三者への提供の手段又は方法
・本人の求めに応じて第三者への提供を停止すること
6　個人情報を共同利用する場合は、次に掲げる事項
・利用する者の名称
・利用目的
・利用する個人情報の項目

（情報セキュリティ及び個人情報保護に関する認証等）

第4条の2　受注者は、この契約による事務の履行のために機密情報を取り扱う場合において、発注者の指定があるときは、次に掲げるいずれかの認証制度の認証を取得していなければな

らない。

（1）ISMS（ISO/IEC27001（JIS Q 27001））認証取得

（2）プライバシーマーク（JIS Q 15001）取得

（3）その他発注者が適当と認める認証取得

（クラウドサービスに関する認証等）

第4条の3　受注者は、この契約による事務の履行のために利用するクラウドサービス（有料、無料にかかわらず、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。）で機密情報を取り扱う場合であって、発注者の指定があるときは、次に掲げるいずれかの認証制度の認証を取得し、又は内部統制評価制度による審査を受けていなければならない。

（1）クラウドセキュリティ認証制度

（ISMS導入組織の場合）

ア　ISMSクラウドセキュリティ（ISO/IEC 27017）認証取得

イ　パブリッククラウド上における個人情報保護（ISO/IEC 27018）認証取得

ウ　プライバシー情報マネジメントシステム（ISO/IEC 27701）認証取得

（サービス単位での場合）

・　クラウド情報セキュリティ監査（CS）ゴールドマーク又はシルバーマーク（JASA クラウドセキュリティ推進協議会）取得

（発注者が重要な情報システムとして特に指定したものの場合）

ア　日本国政府情報システムのためのセキュリティ評価制度（ISMAP）認証取得

イ　アメリカ合衆国政府機関におけるクラウドセキュリティ認証制度（FedRAMP）認証取得

（2）内部統制評価制度

ア　受託業務に係る内部統制の保証報告書（SOC2）（日本公認会計士協会 IT7 号）

イ　受託業務に係る内部統制の保証報告書（SOC3）（日本公認会計士協会 IT2 号）

ウ　業務全般にかかるシステムの内部統制の保証業務（SysTrust）審査報告書（日本公認会計士協会 IT2 号）

エ　電子商取引認証局に対する保証業務（WebTrsuts）審査報告書（日本公認会計士協会 IT3 号）

（データセンターに関する情報セキュリティ対策）

第4条の4　受注者は、この契約による事務の履行のために利用するデータセンターで機密情報を取り扱う場合は、次に掲げる条件を満たすものを利用しなければならない。

（1）データセンターファシリティスタンダード（日本データセンター協会（JDCC））ティア3以上又はこれと同等レベルの安全性及び可用性の高さに関するサービス品質を保証するもの。

（2）個人情報を含むデータは日本国内にあること。

（収集の制限）

第5条　受注者は、この契約による事務の履行のために機密情報を収集するときは、その業務の

目的を達成するために必要な範囲で、適法かつ公正な手段によって収集しなければならない。

（管理体制等の通知）

第6条　受注者は、この契約の締結後、次の文書を発注者に直ち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機密情報保護に関する社内規程又は基準

（2）次の内容を含む従事者名簿

ア　機密情報取扱いの責任者及び機密情報を取り扱う者の氏名、責任、役割及び事務執行場所

イ　機密情報に係る記録媒体の授受に携わる者の氏名並びに事務執行場所

ウ　この契約による事務に関する緊急時連絡先一覧

（3）この契約による事務に関する実施スケジュールを明記した文書

2　受注者は、この契約による事務の履行のために特定個人情報を取り扱う場合においては、この契約の締結後、次の文書を発注者に直ち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）この契約による事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24条の3の事項を証するもの。）

（2）この契約による事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条の4の事項を証するもの。）

3　受注者は、この契約による事務の履行のためにクラウドサービスを利用する場合においては、この契約の締結後、クラウドサービスの利用に係るリスク対策文書（第24条の5の事項を証するもの）を発注者に直ち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。

4　受注者は、前3項の規定により、発注者に届け出た従事者以外の者に、この契約による事務に係る機密情報を取り扱わせてはならない。

（再委託の制限等）

第7条　受注者は、この契約による事務の履行について、機密情報を取り扱う事務の全部又は一部を第三者（受注者の子会社（会社法（平成17年法律第86号）第2条第3号に規定する子会社をいう。）を含む。以下同じ。）に委託（以下「再委託」という。）してはならない。ただし、再委託をする事業者の名称及び所在地、再委託の内容及び理由並びに再委託をする事業者の機密情報に係る安全管理措置の状況等必要な事項を発注者に書面で提出し、その承諾を得た場合はこの限りではない。

2　前項ただし書の規定により再委託を受けた事業者は、この契約を受注した事業者とみなしてこの仕様書の規定が適用されるものとする。

3　受注者は、第1項ただし書の規定により再委託をする場合は、発注者に対し再委託をする業務

に関する報告を行うとともに、再委託をする業務に関する全ての行為について、発注者に対し全ての責任を負うものとする。

（目的外使用及び外部提供の禁止）

第8条　受注者は、この契約による事務で取り扱う機密情報を当該事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。

第9条　受注者は、発注者がこの契約による事務での使用を目的として受注者に提供し、又は貸与する機器等の情報資産を、当該事務以外の目的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。

（複写及び複製等の制限）

第10条　受注者は、この契約による事務で取り扱う機密情報について、発注者の承認を得ずに複写、複製又は加工してはならない。当該事務を実施する上でやむを得ず複写、複製又は加工するときは、あらかじめ発注者に通知し、その承認を得なければならない。この場合において、当該事務の終了後（当該事務の終了後、引き続き発注者と受注者と当該事務に係る契約を締結する場合を除く。）、受注者は、直ちに複写、複製又は加工した機密情報を消去し、再生又は再使用できない状態にするとともに、機密情報を消去した日時、担当者及び処理内容を発注者に報告しなければならない。

（機密情報の持出制限）

第11条　受注者は、この契約による事務開始前までに当該事務で機密情報を取り扱う事務執行場所及び機密情報の管理状況について、発注者に報告しなければならない。

2　受注者は、事前の発注者の承諾なく、この契約による事務で取り扱う機密情報を事務執行場所から持ち出してはならない。

3　受注者は、発注者の施設、事務執行場所等から機密情報を持ち出す必要がある場合には、暗号化、パスワード設定等の保護対策、鍵付きのケース等に格納する等機密情報の紛失や不正利用を防止するための安全管理措置及び運搬に当たってのセキュリティ便の使用等の紛失リスクの低減対策等を事前に発注者に協議しなければならない。

4　受注者は、実際に機密情報の持出しを行う場合には、運搬、保管・管理、廃棄等の各段階におけるその保護対策の状況、安全管理措置の状況等（以下「情報セキュリティ管理状況」という。）に関する記録及び適正な状況であることの確認を行った記録を残さなければならない。

（物的セキュリティ対策）

第12条　受注者は、この契約による事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、磁気、紫外線、直射日光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。

第13条　受注者は、この契約による事務に係る発注者が運用する情報システムのサーバ等を区の施設外に設置する場合は、発注者の承認を得なければならない。

2　受注者は、前項のサーバ等について、定期的に情報セキュリティ対策状況について確認すると

ともに、発注者から要請があった場合は、その結果を発注者に報告しなければならない。

第14条　受注者は、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、発注者のサーバ管理施設その他の発注者の管理区域に立ち入る場合において発注者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。

第15条　受注者は、この契約による事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、又は従事者が事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）

第16条　受注者は、この契約による事務において、発注者に提出した情報セキュリティ及び機密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。

2　受注者は、情報セキュリティ対策について疑義がある場合、遵守することが困難な点等がある場合は、速やかに発注者に報告し、代替策について協議しなければならない。

第17条　受注者は、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。

第18条　受注者は、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）従業者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。）。

第19条　受注者は、従事者に対して、情報セキュリティ及び機密情報保護に関する教育並びに緊急時対応のための訓練を計画的に実施し、発注者にその教育の実施状況等を報告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）

第20条　受注者は、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、発注者が指定する期間保存しなければならない。

第21条　受注者は、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。

第22条　受注者は、情報システム等に記録された重要度の高い機密情報について、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発注者に通知し、承認を得なければならない。

第23条　受注者は、情報システムの開発及び導入に当たり、開発及び導入前に発注者と協議の上、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。

第24条　受注者は、この契約による事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、発注者と協議の上、修正プログラムを適用しなければならない。また、不正プログラム対策を行い、不正プログラム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。

第24条の2　受注者は、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。

第24条の3　受注者は、この契約による事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。

第24条の4　受注者は、この契約による事務に使用する情報システムにおいて特定個人情報を取り扱う場合は、定期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、ソフトウエ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。

第24条の5　受注者は、この契約による事務において利用するクラウドサービスで機密情報を取り扱う場合は、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。

（その他のセキュリティ対策）

第25条　受注者は、この契約による事務に関し、発注者より機密情報を受領した場合は、預かり証を発注者に対して交付しなければならない。

2　前項の場合において受注者は、当該機密情報を適切に管理するため、機密情報の受領日時、受領者名、受領した機密情報の種類等の記録簿を作成するとともに、発注者から要請があった場合は、速やかに当該記録簿を発注者に提示しなければならない。

第26条　受注者は、機密情報を電子メール、ファイル交換サービス等で送受信する場合は、事前に暗号化、パスワード設定等の保護対策を発注者に協議するとともに、実際に保護対策を講じなければならない。

2　受注者は、機密情報を郵送等で送付する場合は、送付状況を追跡できるサービスを活用する等の対策を講じなければならない。

3　受注者は、やむを得ず機密情報を使送する場合は、施錠可能なケースにより運搬する等の保護対策を講じるとともに、事前に運搬ルートを発注者に協議し、その運搬ルートを遵守しなけれ

ばならない。

第27条　受注者は、この契約による事務で取り扱う機密情報について、厳格にアクセス制御を行うとともに、当該機密情報を施錠可能な金庫、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、機密情報の取扱いには十分注意し、機密情報の紛失並びに情報の改ざん、漏えい等の防止に努めなければならない。

第28条　受注者は、この契約による事務が終了したときは、発注者より受領し、又は受注者が当該事務を遂行する中で記録・作成した機密情報や機密情報に当たらない機器等の情報資産を速やかに発注者に返却しなければならない。

2　前項のほか、発注者に返却が不可能な機密情報又は発注者に返却をすることによりかえって機密情報が紛失する可能性がある場合には、発注者の了承のもと、機密情報及び情報資産を復元できないような処置をした上で廃棄し、日時、担当者及び処理内容を発注者に報告し、廃棄した記録を遅滞なく提出しなければならない。

3　この契約による事務を遂行していく中で、発注者から受領した機密情報を保持しておく必要性が乏しい場合については、前項と同様とする。

第29条　受注者は、機密情報の作成業務を終了したときは、直ちに当該機密情報を発注者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。

（電子情報処理機器の修理又は廃棄）

第30条　受注者は、この契約による事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「電子情報処理機器」という。）を修理又は廃棄する場合は、事前に当該電子情報処理機器に保存されている機密情報を消去し、再生又は再使用できない状態にするとともに、機密情報を消去した日時、担当者及び処理内容を発注者に速やかに報告しなければならない。

2　前項の場合は、次に掲げる措置を行うものとし、受注者はその旨を発注者に事前に報告するものとする。ただし、当該措置を行うことが困難な場合には、発注者に協議し、承認を得るものとする。

（1）記録装置の物理的又は電磁的な破壊

（2）発注者が指定する場所で、発注者の職員の立会いの下における当該電子情報処理機器に保存されている機密情報を消去し、再生又は再使用できない状態にする措置

（3）発注者が指定する場所で、発注者の職員の立会いの下における記録装置の物理的又は電磁的な破壊

（委託業務の報告）

第31条　受注者は、発注者に対し、機密情報の情報セキュリティ管理状況及びこの契約による事務の状況を定期的及びこの契約による事務の終了後に報告するものとする。ただし、発注者が必要と認めるときは、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）

第32条　受注者は、機密情報の情報セキュリティ管理状況について、発注者の求めに応じて報告するものとする。

2　発注者は、受注者によるこの契約による事務の履行に伴う機密情報の取扱いについて、必要があると認めるときは、受注者に対して必要な指示を行うことができる。

3　発注者が必要に応じて監査又は検査を実施する場合は、受注者は受け入れなければならない。

第33条　受注者は、発注者が必要とする場合は、業務執行場所へ発注者の職員の立入りを認めるものとする。

（緊急時の対応）

第34条　受注者は、この契約による事務において、事務上のトラブル、災害、事故、電子情報処理機器の不良、故障及び破損等が発生した場合は、速やかに発注者にその状況について報告し、発注者の指示に従わなければならない。

第35条　受注者は、この契約による事務について次に掲げる事象が発生した場合は、速やかに、発注者にその状況を具体的に報告するとともに、発注者と協議の上、事故処理を行うものとする。

（1）機密情報の紛失

（2）機密情報の破壊

（3）機密情報の改ざん

（4）機密情報の漏えい

（5）不正アクセス

（6）情報セキュリティ基本方針及びこの仕様書に定める事項の違反

（7）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

（契約の解除）

第36条　発注者は、受注者の責に帰すべき理由により、この契約による事務の履行に関し前条各号に掲げる事象が発生したときは、この契約を解除することができる。

（サービスレベルの保証）

第37条　受注者は、この契約による事務のサービスレベルについて、事前に発注者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。

（損害賠償）

第38条　受注者は、この仕様書に定める事項に違反し、又はこの仕様書に定める事項を履行しなかったことにより、発注者又は第三者に損害が生じた場合には、発注者又は第三者に対しこれを賠償するものとする。

（公表措置）

第39条　発注者は、受注者がこの契約による事務の履行により知り得た機密情報の紛失、漏えい、滅失、毀損及び改ざん等の事故を発生させたときは、その事実を公表することができる。

（疑義等）

第40条　この仕様書に定める事項について疑義が生じたとき又は定めのない事項については、発注者及び受注者双方協議の上定める。

以　　上