ローコード開発ツールを活用した
電子申請受付システム構築業務委託

仕様書

令和８年１月

世田谷区　都市整備政策部　都市計画課

１．業務概要

本仕様書は、各総合支所街づくり課における各種申請等の電子化を目的として、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 kintone を基盤とし、FormBridge、kViewer、PrintCreator、gusuku Customine、kBackup のプラグインを連携させた電子申請受付システムの要件を定義する。

ローコード開発ツールによる区民・事業者からのオンライン申請受付導入により、庁内審査・決裁、帳票出力、申請状況照会、データ保全、通知等の省力化を推進し、区民・事業者サービスの向上及び職員の窓口負担軽減と処理の可視化・迅速化を図る。加えて、庁内での申請内容の情報共有をより一層推進する。

なお、本業務では、電子申請受付開始後も窓口での申請を継続して受け付ける。窓口申請分の記録方法については、別途区と受託者協議の上決定する。

２．履行場所

（１）世田谷区都市整備政策部都市計画課
　　世田谷区玉川１丁目２０番１号　２階
　　世田谷区世田谷４丁目２１番２７号　東棟４階
（２）受託者の事業所
（３）その他区が指定する場所

３．契約期間

契約締結日から令和９年３月３１日

４．業務スケジュール（予定）

令和８年	５月	契約締結、要件定義、関係課ヒアリング
	６月～１２月	設計・構築
令和９年	１月	システム動作確認
	２月	システム操作研修、システム運用開始

５．対象業務

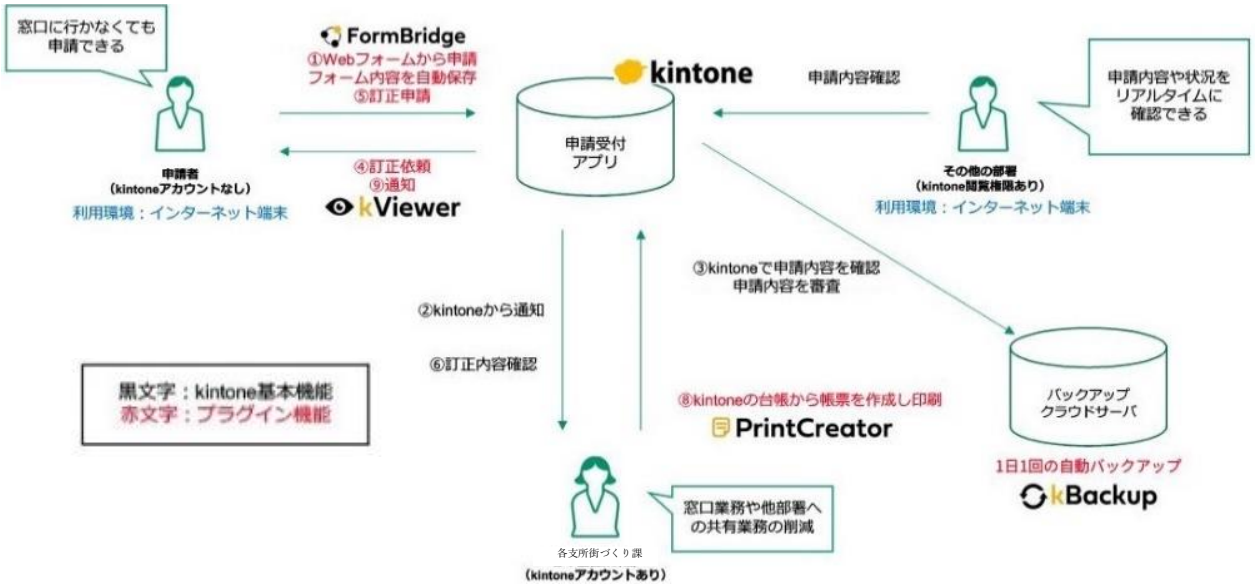
申請名	フォーム種別（数）	帳票（枚）
都市計画法第 53 条	1	1
地区計画の届出	6	0
地区街づくり計画の届出	2	2
中高層建築物等の条例に基づく届出	4	0
みどりの基本条例に基づく届出 （都市緑地法含む）	7	9
東京都風致地区条例に基づく届出	6	6
住環境の整備に関する条例に基づく届出	3	3

本システムで電子申請化の対象とする業務は、上記の７業務を基本とする。

帳票数及びフォーム数は、区と協議のうえ確定する。また、受託者との詳細打合せにおいて申請内容の整理等を行い、最終的に業務数を削減する場合がある。削減にあたっては、機能要件・業務要件を満たすことを前提とし、成果物一覧・工程表・見積内訳を調整のうえ、契約内容に反映する。また、契約金額は、実質作業量に応じて適正化（減額または再算定）を行う。

６．システム構成（概要）

（１）システム構成



・kintone（申請管理／決裁／情報共有）
・FormBridge（申請フォーム）
・kViewer（申請者認証／申請状況照会／閲覧・修正／修正依頼／帳票の交付）
・PrintCreator（帳票作成）
・gusuku Customine（採番等申請管理等の台帳管理円滑化）
・kBackup（定期データの保全）

（２）業務フロー

①申請前認証

・申請者は、電子申請フォーム（FormBridge）にアクセスする前に、メールアドレスを入力して認証を行う。

②申請フォーム入力・送信

・認証済みの申請者が FormBridge の電子申請フォームに必要事項を入力し送信。

③受付通知

・申請完了後、FormBridge の自動返信メールで受付通知。通知にて申請内容確認。
・kViewer 上で審査状況「受付中」と表示。

④収受確認

・職員が、kintone 上で必要図書等が揃っているか確認を行う。必要図書が揃っている場合は、kintone のプロセス管理で「受付」にステータス変更し収受番号の採番を行う。

・不足図書等がある場合は、申請者と職員が kViewer 上で不足図書のやり取りを行う。

⑤kintone 登録・審査開始

・kintone に申請データが登録され、職員が図面および申請内容を kintone 上で確認し、審査を開始。

・kintone のプロセス管理で「審査中」にステータス変更。

・kViewer 上で「審査中」と表示。

・紙での申請がある場合、職員がその内容を kintone に入力。

⑥修正依頼・やり取り

・申請者と職員が kViewer 上で修正依頼や確認のやり取りを行う。

⑦承認プロセス

・審査完了後、申請内容が承認者に通知され、承認プロセスが開始。

・kintone のプロセス管理で「承認待ち」にステータス変更。

・kViewer 上で「決裁中」と表示。

・承認者がコメントを追加し、必要に応じて取下げや差戻しを実施。

⑧決裁完了・通知

・すべての操作は kintone に履歴として記録。

・最終的な決裁が行われ、結果が kViewer 上で「決裁完了」と表示。

・職員が申請者に対し、メールまたは電話で結果を通知。

⑨帳票出力・提供

・申請内容は PrintCreator を通じて帳票として出力。

・帳票は電子保管または印刷。

・申請者に対し、決裁書類の一部帳票を kViewer を通じて交付。

⑩データ保全

・kintone に登録されたデータを、１日１回夜間自動的にバックアップを行う。

・職員が誤って削除してしまったデータを、マウス操作により特定のタイミングのデータに戻す。

７．機能要件

実施機能は機能設計を経て決定するものとする。

（１）申請受付（FormBridge）

・専用フォームを作成（条件分岐・入力制御・必須チェック等）。

・ファイル添付（図書、図面、写真）と容量制御。

・下書き保存・再開、入力途中の自動保存。

・受付番号の自動採番、申請内容全体を示した送信完了メールの自動送信。
・アクセス制御（認証導線を設置)。

（２）申請データ管理等（kintone）
・申請アプリ、審査台帳、帳票出力用データテーブル等を設計。
・部署、役職に応じたアクセス権限、フィールド単位の閲覧・編集制御。
・承認の標準ワークフロー（担当→係長→審査係長→課長→部長等)、取下げ・差戻し・意見追記に対応。
・ステータス管理の設定。
・レコード履歴・操作ログ（閲覧・登録・ダウンロード）を取得。
・検索、集計、ダッシュボードで業務 KPI（件数、処理日数、未処理件数等）を可視化。
・アクセス権を有する者同士で情報を共有。

（３）申請状況照会等（kViewer）
・申請者が受付番号・認証情報により自身の申請状況を照会可能。
・不足書類の提出・修正依頼への回答受付、提出履歴の確認。
・一部帳票の電子交付。

（４）帳票出力（PrintCreator）
・kintone データテーブルから帳票を PDF で作成。
・許可・不許可・決裁文書・通知書等をテンプレート化。

（５）データ保全（kBackup）
・１日１回の自動バックアップ。
・誤操作や不正改ざん発生時の迅速なリストア手順を整備。

（６）自動処理（gusuku Customine）
・申請種別・入力値・審査状況に応じたステータス自動更新。
・フィールドをカテゴリごとにタブで分割表示。
・フィールドの表示・非表示、編集不可、必須制御。
・受付番号を自動で発番。
・選択肢の階層化により、住所等届出入力項目選択を効率化。
・レコード一覧画面に代表的な検索ボックスを追加。
・条件に応じて文字色・背景色の変更による期限超過・未対応アラートの表示。

８．非機能要件

（１）セキュリティ
・通信および蓄積データの暗号化、強固なアクセス制御（多要素認証、権限管理)。
・監査ログ（システムログ／アプリケーションログ）の取得と改ざん防止。
・データセンターは国内拠点、電源・空調の冗長化、24/365 監視、入退室管理。
・ISMS（ISO/IEC 27001）等の第三者認証、必要に応じて ISMAP 同等の水準を確認。
・脆弱性情報の監視とアップデート適用、ペネトレーションテスト等の実施。

・不正アクセス対策、データ及びアカウント漏洩・改ざん・消去防止、マルウェア対策等、セキュリティ対策に万全を期したシステム環境を持続。
・クラウドサービスを管理者として利用する際の適切なアクセス制御。
・IP アドレス制限によるアクセス制御。

（２）可用性
・計画停止を除き、稼働率 99.99% を目標。
・冗長構成により障害ポイントを最小化、バックアップと組み合わせた迅速復旧。

（３）操作性
・ノーコード／ローコードによるドラッグ＆ドロップ操作で項目追加・変更・削除が可能。
・運用開始後もフォームやステータス設定を庁内で変更可能。

（４）利用者数
・各総合支所（世田谷・北沢・玉川・砧・烏山）街づくり課・烏山総合支所駅周辺整備担当課職員１３０名、都市計画課職員３名、その他関係課１０名程度。将来的にユーザー数を拡大可能な実績のあるサービスであること。

９．委託範囲

本業務は、電子申請受付システムの構築および導入支援を目的とし、以下の業務範囲を含むものとする。

（１）設計・開発
①フォーム設計：FormBridge を用いた申請フォームの構築、入力制御、公開設定。
②kintone アプリ設計：テーブル・フィールド定義、条件分岐、プロセス管理設定。
③帳票テンプレート整備：PrintCreator による帳票レイアウト設計、PDF 出力設定。
④ワークフロー設定：申請・承認・差戻し・取下げのフロー設計。
⑤gusuku Customine 設定：フィールド制御、ステータス更新、集計設定。
⑥kViewer 公開設定：kViewer を用いた認証及び申請者との情報交換を行う公開ページの設定、テンプレート設計、通知設定、アクセス制御。

（２）導入支援
①総合テスト支援：テスト仕様書作成、テスト実施、結果報告。
②問い合わせ窓口対応：導入期間中の技術的問い合わせ対応（メール・チャット等）。
③軽微な設定変更：導入後の初期調整（フィールド追加、通知条件変更等）。

（３）マニュアル作成
①操作手順書：申請者・承認者・管理者向け操作手順書。
②運用手順書：日常運用、帳票出力、通知管理、設定変更手順。
③バックアップ復旧手順書：kBackup によるバックアップ設定、リストア手順、障害時対応。

（４）職員研修
①管理者研修：３時間、ハイブリッド形式（対面＋オンライン）、録画配布。

②一般職員研修：２時間、ハイブリッド形式、FAQ・教材配布。
③研修成果物:研修計画書、教材(スライド・演習資料・各ツール別の操作研修資料)、FAQ 集、録画、実施報告書。

（５）運用開始後の初期サポート
①稼働初月の伴走支援:運用開始後 1 か月間の技術支援、設定調整、問い合わせ対応。

１０．業務体制
受託者は本業務を提供するにあたり、以下の条件を満たすこと。
（１）プロジェクト管理者は、PMI（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）の資格、またはこれと同等の能力があると認められる者を配置すること。
（２）プロジェクト管理者又はメンバーにおいて、過去３カ年以内に、東京都内の自治体において本委託業務で使用するクラウドサービスを利用したシステム設計・開発に関する実績を有する者を配置すること。
（３）プロジェクト管理者又はメンバーにおいて、本委託業務で使用するクラウドサービスに関する認定資格の有資格者を配置すること。
（４）問い合せ対応窓口は、HDI サポートセンター国際認定の資格を有すること。また、対応時間は年末年始を除く平日 9：00-17：30 とすること。

１１．業務の実施にあたっての遵守事項
（１)機密保持、資料の取扱い
履行にあたっては、別紙１「情報セキュリティ対策基準（抜粋版)」、別紙２「電算処理の業務委託契約の特記事項」、別紙３「個人情報を取り扱う業務委託契約の特記事項」を遵守すること。
（２)法令等の遵守
本業務の遂行に当たっては、以下の法令等を遵守し履行すること。
①地方自治法（昭和 22 年法律第 67 号）
②著作権法（昭和 45 年法律第 48 号）
③個人情報保護に関する法律（平成 15 年法律第 57 号）
④世田谷区財務規則
⑤世田谷区個人情報保護条例
⑥その他関係法令及び諸規則
（３)その他文書、標準への準拠
①アプリケーション・コンテンツの作成規程
・提供するアプリケーション・コンテンツに不正プログラムを含めないこと。
・提供するアプリケーションに脆弱性を含めないこと。
・実行プログラムの形式以外にコンテンツを提供する手段がない限り、実行プログラムの形式でコンテンツを提供しないこと。

・電子証明書を利用するなど、提供するアプリケーション・コンテンツの改ざん等がなく真正なものであることを確認できる手段がある場合には、それをアプリケーション・コンテンツの提供先に与えること。
・提供するアプリケーション・コンテンツの利用時に、脆弱性が存在するバージョンのＯＳやソフトウェア等の利用を強制するなどの情報セキュリティ水準を低下させる設定変更を、ＯＳやソフトウェア等の利用者に要求することがないよう、アプリケーション・コンテンツの提供方式を定めて開発すること。
・サービス利用にあたって必須ではない、サービス利用者その他の者に関する情報が本人の意思に反して第三者に提供されるなどの機能がアプリケーション・コンテンツに組み込まれることがないよう開発すること。

②資料の貸与

・区は、本業務において必要と認める資料を受託者に貸与するものとする。受託者は、その保管及び取り扱いについては、亡失、汚損、破損等のないよう万全の注意を払うものとし、使用後速やかに返却するものとする。
・資料の借用について受託者は、その都度区に対して借用書を提出するものとする。区が貸与する資料に関して、受託者は、第三者に情報が漏れることのないよう取扱いと保管に留意し、本業務の目的以外に使用しないこと。また、本業務上必要であっても発注者の承諾なくして複写してはならない。

（４）規程改正への対応

別紙１「情報セキュリティ対策基準（抜粋版）」の改正があった場合は、別途、担当部署から改正後の当該基準を提供するので、受託者は本業務に関する影響分析を行うこと。

１２．成果物

（１）成果物品

①要件定義書

・業務概要、目的
・ツール構成と役割分担
（kintone、FormBridge、kViewer、PrintCreator、gusuku Customine、kBackup）
・機能要件
・非機能要件

②画面遷移図

・申請者・承認者・管理者の画面フロー

③データ設計書

・テーブル・フィールド定義（kintone アプリ）
・条件分岐一覧（フォーム制御、通知、ワークフロー）
・gusuku Customine によるフィールド制御仕様

④ワークフロー設計書
・申請、承認、差戻し、取下げフロー
・kintone プロセス管理設定
・gusuku Customine によるステータス一括更新仕様
⑤帳票設計・テンプレート
・Excel/Word テンプレート（申請書・承認書など）
・PrintCreator 設定（レイアウト、出力条件、PDF 命名規則）
・帳票出力の自動化設定（Webhook 連携など）
⑥FormBridge 設計・公開設定書
・フォーム構成・入力制御・公開設定
・通知設定・バリデーション仕様
⑦kViewer 設計書
・認証設定
・テンプレート設計（一覧・詳細ビュー）
・通知設計・アクセス制御
⑧PrintCreator 設計書
・帳票テンプレート一覧（背景 PDF 含む）
・出力条件・レイアウト設計
・PDF 命名規則・保存先設計
・自動出力設定（Webhook、時間指定）
⑨gusuku Customine 設計書
・導入プラグイン一覧と目的
・フィールド制御仕様（表示/非表示、入力制限）
・ステータス更新＋設定
・集計サポート＋設定（一覧画面での合計・平均表示）
・UI 制御（表示/非表示、入力制限）
⑩kBackup 設計書
・バックアップ対象アプリ一覧
・実行頻度・保存先・保持期間
・リストア手順（全体・個別）
・障害時対応フロー・セキュリティ設定
⑪テスト仕様書・結果報告書
・機能別テストケース（各ツール含む）
・テスト実施記録・不具合対応履歴
⑫操作手順書・運用手順書
・申請者・承認者・管理者向け操作手順
・gusuku Customine 操作手順
・PrintCreator 帳票出力手順

・kBackup バックアップ・リストア手順

⑬研修資料一式

・研修計画書・教材（スライド・演習資料）

・FAQ 集・録画・実施報告書

・各ツール別の操作研修資料

（kintone、FormBridge、kViewer、PrintCreator、gusuku Customine、kBackup）

⑭プロジェクト計画書

⑮システム構成図

⑯セキュリティ設定書

⑰業務実施報告書

⑱電子申請受付アプリ

※正式な成果物については契約締結後に区と受託者協議のうえ決定する。

（２）納品方法

①～⑰の電子データ　ＣＤ－Ｒ等　１部

・電子データの形式等については担当課の指示に基づき納品すること。

・納品する電子データの著作権は区へ譲渡すること。

・成果品等本委託に関わる電子データを、外部媒体を用いて区に提出する際には事前にウイルスチェックを実施し、セキュリティの安全確認を行うこと。また、提出にあたっては、チェック方法や日時等について提出媒体表面に記載（プリント）すること。

（３）納品場所

世田谷区都市整備政策部都市計画課

〒１５４―８５０４　世田谷区世田谷４丁目２１番２７号　本庁舎東棟４階

１３．成果物の取扱いに関する事項

（１）知的財産権の帰属

①本業務における成果物の原著作権及び二次的著作物の著作権（著作権法第 21 条から第 28 条に定める全ての権利を含む。）は、受託者が本調達の実施の従前から権利を保有していた等の明確な理由によりあらかじめ提案書にて権利譲渡不可能と示されたもの以外は、全て区に帰属するものとする。

②区は、成果物について、第三者に権利が帰属する場合を除き、自由に複製し、改変等し、及びそれらの利用を第三者に許諾することができるとともに、任意に開示できるものとする。また、受託者は、成果物について、自由に複製し、改変等し、及びこれらの利用を第三者に許諾すること（以下「複製等」という。）ができるものとする。ただし、成果物に第三者の権利が帰属するときや、複製等により区がその業務を遂行する上で支障が生じるおそれがある旨を契約締結時までに通知したときは、この限りでないものとし、この場合には、複製等ができる範囲やその方法等について協議するものとする。

③納品される成果物に第三者が権利を有する著作物（以下「既存著作物等」という。）が含まれる場合には、受託者は、当該既存著作物等の使用に必要な費用の負担及び使用許諾契約等に関わる一切の手続を行うこと。この場合、本業務の受託者は、当該既存著作物の内容について事前に区の承認を得ることとし、区は、既存著作物等について当該許諾条件の範囲で使用するものとする。なお、本仕様に基づく業務に関し、第三者との間に著作権に係る権利侵害の紛争の原因が専ら区の責めに帰す場合を除き、受託者の責任及び負担において一切を処理すること。この場合、区は係る紛争等の事実を知ったときは、受託者に通知し、必要な範囲で訴訟上の防衛を受託者に委ねる等の協力措置を講じるものとする。

④プログラムに関する権利（著作権法第 21 条から第 28 条に定める全ての権利を含む。）及び成果物の所有権は、区から受託者に対価が完済されたとき受託者から区に移転するものとする。

⑤受託者は区に対し、一切の著作者人格権を行使しないものとし、また、第三者をして行使させないものとする。

⑥受託者は使用する画像、デザイン、表現等に関して他者の著作権を侵害する行為に十分配慮し、これを行わないこと。

（２）契約不適合責任

①本業務における成果物等について、種類、品質又は数量が契約書、本調達仕様書その他合意された要件（以下「契約書等」という。）の内容に適合しないもの（以下「不適合」という。）である場合、その不適合が区の責に帰すべき事由による場合を除き、受託者は自己の費用で、区の選択に従い、その修補、代替物の引渡し又は不足分の引渡しによる履行の追完（以下、手段を問わず総称して「履行の追完」という。）をすること。なお、受託者は如何なる場合であっても、区の選択と異なる方法で履行の追完をする場合は、区の事前の承諾を受けること。

②受託者は、その具体的な履行の追完の実施方法、完了時期、実施により発生する諸制限事項について、区と協議し、承諾を得てから履行の追完を実施するものとし、完了時には、その結果について区の承諾を受けること。

③受託者が区から相当の期間を定めた履行の追完の催告を受けたにもかかわらず、その期限内に履行の追完を実施しない場合、区は、その不適合の程度に応じて代金の減額を請求することができる。ただし、次に掲げる場合、受託者に対して履行の追完の催告なく、直ちに代金の減額を請求することができる。

・履行の追完が不能であるとき。
・受託者が履行の追完を拒絶する意思を明確に表示したとき。
・本業務の性質又は契約書等の内容により、特定の日時又は一定の期間内に履行をしなければ契約をした目的を達することができない場合において、受託者が履行の追完をしないでその時期を経過したとき。
・前 3 号に掲げる場合のほか、前項の催告をしても履行の追完を受ける見込みがないことが明らかであるとき。

④受託者は、成果物について検査合格をした日を起算日として１年間、成果物の不適合（ただし、数量の不適合を除く）を理由とした責任を負うものとする。

（３）検査

①本業務の受託者は、「成果物」について、納品期日までに区に内容の説明を実施して検査を受けること。

②検査の結果、成果物に不備又は誤り等が見つかった場合には、直ちに必要な修正、改修、交換等を行い、変更点について区に説明を行った上で、指定された日時までに再度納品すること。

１４．その他

（１）本仕様書に定めのない事項については、区及び受託者双方協議の上決定する。

（２）本業務において使用する以下のローコード開発ツール等のライセンスについては、区が別途調達し、受託者に供与するものとする。対象ライセンスは以下のとおりとする。

・kintone
・FormBridge（プロフェッショナル）
・kViewer（プロフェッショナル）
・PrintCreator（プロフェッショナル）
・gusuku Customine
・kBackup（プレミアム）

本業務において使用するkintone等は、いずれもSaaS型クラウドサービスであり、ライセンスに基づき利用されるものである。委託者は、受託者が本業務遂行に必要な範囲でkintone環境にアクセスできるよう、当該ライセンスを一時的に供与するものとする。

受託者は、委託者が指定するアカウントによりログインし、申請フォームの作成・設定等を行う。

業務完了後、受託者は当該ライセンスの利用を終了し、委託者は当該アカウントのパスワード変更またはアカウントの無効化等により、受託者によるログインを不可とする措置を講じるものとする。

なお、当該ライセンスは委託者が契約・管理するものであり、受託者はこれを業務目的以外に利用してはならない。また、クラウドサービスの性質上、データの保管・管理は委託者の責任において行われるものとし、受託者は業務遂行に必要な範囲を超えてデータにアクセス・保存・複製等を行ってはならない。

（２）ネットワーク要件

本件にて区職員が使用する端末のネットワークは、総務省の「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（令和７年３月版）」におけるインターネット接続系である。

（３）システム開発環境

本業務における kintone アプリの開発・テストは、区が契約する kintone サービス上の開発・テスト環境で実施し、開発環境で対応できない作業については、委託者と協議のうえ区の承認を得て本番運用環境を使用することとし、利用に際しては区のセキュリティポリシーを遵守すること。

（４）業務終了後のデータ削除・返却

委託業務の完了後、委託事業者は本業務において取得・保存したすべての個人情報及び関連データについて、以下のいずれかの方法により適切に処理を行うものとする。

ア　データ削除

・委託事業者は、保存、取得したされた個人情報を復元不可能な方法により完全に削除すること。

・削除方法には、暗号化されたデータの物理的破壊、セキュアな消去ツールの使用等を含む。

・削除完了後、削除証明書または削除報告書を提出すること。

イ　再委託先の対応

・委託事業者が再委託を行っている場合、再委託先に対しても同様の削除措置を講じること。

・再委託先からの削除報告も併せて提出すること。

１５．支払い

検査合格後、請求に基づき支払う（１回)。

１６．附属文書

（１）別紙１ 情報セキュリティ対策基準（抜粋版）

（２）別紙２ 電算処理の業務委託契約の特記事項

（３）別紙３ 個人情報を取り扱う業務委託契約の特記事項

１７．本件担当

都市整備政策部都市計画課調整係　電話 03-6432-7147

委託先事業者等公開用抜粋版

別紙 1

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。

別紙２
20230401

電算処理の外部委託基準

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。

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、この契約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。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、この契約の締結後直ちに、以下の文書を委託者に提出しなければならない。

（１）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　個人情報を取り扱う者の氏名、責任及び役割

②　委託業務において個人情報の授受に携わる者の氏名及び業務執行場所

③　緊急連絡先一覧

（３）委託業務に係る実施スケジュールを明記した文書

（再委託の禁止）

４　受託者は、この契約による業務を第三者に再委託してはならない。ただし、当該業務の全部又は一部についてやむを得ず第三者に委託する必要があるときは、あらかじめ再委託する業者名、再委託の内容を委託者に通知し、委託者の承諾を得なければならない。また、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。）にも、この契約を遵守させなければならない。

（目的外使用及び外部提供の禁止）

５　受託者は、個人情報を委託者の指示する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。

（複写及び複製の禁止）

６　受託者は、個人情報の全部又は一部を委託者の許可なく複写し、又は複製してはならない。

７　委託者の許可を受けて複写又は複製したときは、委託業務の終了後直ちに当該複写物又は複製物を利用できないよう処分又は委託者へ提出しなければならない。

（安全管理措置の実施）

８　受託者は、委託業務において、委託者に提出した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。

９　受託者は、従事者に対して、個人情報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。

10　受託者は、個人情報の授受、保管及び管理について、善良な管理者の注意をもって当たり、個人情報の漏えい、滅失、毀損等（以下「漏えい等」という。）の事故を防止しなければならない。

（委託終了時における個人情報の消去及び媒体の返却）

11　受託者は、委託業務が終了したときは、直ちに、委託業務に使用した個人情報の消去及び個人情報が記録された媒体の返却をしなければならない。

（委託業務の報告）

12　受託者は、委託者に対し、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）

13　受託者は、委託者が必要とする場合、監査又は検査を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。

14　受託者は、委託者が必要とする場合は、業務執行場所へ委託者の職員の立入りを認めるものとする。

（個人情報の漏えい等の対応）

15　受託者は、個人情報の漏えい等が生じたとき、又は漏えい等が生じたおそれがあるときには直ちに委託者に対して通知するとともに、遅滞なくその状況について書面をもって委託者に報告し、委託者の指示に従わなければならない。

（契約解除及び損害賠償）

16　受託者が、個人情報の取扱いについて法令及び本特記事項に違反した場合、委託者は、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、受託者が、個人情報の取扱いにつき法令及び本特記事項に違反したことにより、委託者に損害が生じた場合には、これを賠償するものとする。