別冊　仕様書

令和８年度人流データ可視化システム運用保守業務
仕様書

１　業務の名称

令和８年度人流データ可視化システム運用保守業務

２　業務の目的

本業務は、当機構の事業化検討を精度向上及び効率化し、また実証的取組の効果を数値化するため、GNSS 人流データを活用した人流の現況把握・分析を可能とする人流データ可視化システム（以下、「人流可視化システム」という）に関するシステムの運用及び保守を行うことを目的とする。

３　業務履行期間

契約締結翌日から令和 12 年３月 31 日まで。

ただし、本仕様書４(1)に記載する業務は令和９年１月 31 日まで。また、本仕様書４(2)①、(3)及び(4)に記載する業務は令和 12 年１月 31 日まで。

４　調達内容

令和５年度人流データ可視化システム構築業務（以下、「前回業務」という。）で構築した機能及び提供・供与する各種サービス及びソフトウェア等の運用保守をすること。

(1)　前回業務受注者からの引継ぎ要件

受注者は、令和９年１月 31 日までに、前回業務受注者から別紙１に示すシステム要件を満たす人流可視化システムの運用保守に必要な情報について引継ぎを受けること。不明な点がある場合には、機構に照会する等、常に機構と密な連絡を取り、作業を行うこと。前任者から人流可視化システムを引き継ぎ、受注者の責任と負担により、本システムを令和９年２月１日より利用可能な状態にすること。受注者は作業の実施にあたり、事前に「５.(1)プロジェクト計画書」を提出するものとする。なお、令和９年２月１日以降は、前任者からの引継ぎを受けることができない。

(2)　運用及び保守業務

①　運用業務要件

受注者は、本調達サービスの運用に係る各種問い合わせ及び調査依頼等の稼働支援業務に応じること。

イ　運用方針

（イ）　利用可能時間は平日 24 時間とする。

（ロ）　メンテナンスの実施日は平日・休日を問わない。事前の利用者への周知方策

についても確保すること。

（ハ） 可用性に係る要件は、利用停止許容時間を24時間程度とする。なお、稼働率は98.5%以上を目標とすること。

（ニ） 本システムの運用に必要となる管理者及び一般ユーザー用マニュアルの更新を適宜実施すること。

（ホ） 機構に代わってシステムの運用のために必要なクラウドサーバーを調達すると共に、クラウドサービスを利用するに当たり、機構と協議の上、特権アカウントや一般アカウント等のアカウント全体構成を策定し、適切にアカウントの管理、払い出し及び権限付与を行うこと。

なお、現在使用しているクラウドサーバーはGoogle Cloud Platformであり、スペックは以下のとおり。

・Cloud Run CPU:2 メモリ:4GiB

・Cloud Functions vCPU:1 メモリ:2GB

・Cloud SQL vCPU:4 メモリ:32GB SSDストレージ:200GB バックアップ：400GB

・Cloud Storage:200GB

・BigQuery

・Cloud Armor（WAF）

（ヘ） (2)①(ホ)にて調達するクラウドサーバーの利用料(インフラ費用)に係り、以下の対応をすること。

a 本業務を通じてシステムの非機能要件（別紙１「３ システムの非機能要件」参照）を明示し、毎月の利用量及び利用料金の確定後、前月分の利用しているクラウドサービス（インスタンスタイプ等）及び単価（契約形態も含む)、利用実績、実施した作業内容、対応すべき、または、解決した課題等を記載した月次報告書を作成し、機構に報告すること。なお、証跡のために、利用しているクラウドサービス（インスタンスタイプ等）及び単価（契約形態も含む)、利用実績が確認可能な画面を報告書に添付する、または、画面へのアクセス可能な権限を機構に付与すること。

これらのレポートについては、キックオフ・納品・機構要求等のその他機構の指定する必要な時点においても提出すること。

b インフラ費用を含む運用及び保守費用全般に変更が発生する場合、根拠と共に機構に情報提示をすること。

ロ 運用支援体制

（イ） 本調達クラウドサービス、ライセンス等に関して、アフターサービス等の提供及び各種相談、問い合わせの受付等を行う体制を確保すること。

（ロ） 対応時間帯については、平日の10：00～17：00までとする（年末年始は除く)。

（ハ） 対応方法については、管理者と受注者の電話又は電子メールでのやり取りとする。

ハ 技術サポート

（イ） 本調達全般の質問に対する回答、助言を行うこと。

（ロ） 本調達全般の問題発生時における迅速な原因調査、対策、報告を行うこと。

（ハ） 本調達サービス等のソフトウェアのバグ及びバージョンアップ、セキュリティアップデート等の情報提供を行うこと。

（ニ） その他、本調達サービス等を適正かつ効率的に使用するために機構が依頼する支援に対する回答、助言を行うこと。

（ホ） 本調達サービス等の利用にあたり一般ユーザーからの依頼に応じて打合せを実施すること。（15 地区程度）

ニ バックアップ・リストア

（イ） 業務運用の継続に影響を与えない最低限のシステムイメージ、データのバックアップを取得すること。

（ロ） バックアップの取得は自動化、リストアに関しては、手動での実施とする。

② 保守業務要件

受注者は以下の保守内容に対応すること。

イ 本調達サービス等に関する機能保証及び各種装置の円滑な稼働に障害が生じた場合の調整等を行うこと。

ロ 本調達で受注者が運用保守するソフトウェアのバグについては、機構と速やかに調整の上、受注者の責めに帰すべき事由によるものについては受注者の負担で対応すること。その他の場合の対応範囲及び費用負担については機構と協議の上決定すること。

ハ その他詳細については、機構と協議・調整すること。

ニ 別紙２に定める情報セキュリティ対策の履行状況確認結果について、3 か月毎に運用保守会議を開催し、下記に関する確認状況及び今後の対応について報告すること。ただし、運用保守会議開催時期および責任の所在にかかわらず、セキュリティ対策上の問題が生じた場合には、機構と速やかに報告の上、対応方法を検討すること。

(3) システム管理業務

上記(2)②ニに記載の、情報セキュリティ対策の履行状況確認において、分析の精度に影響を及ぼすおそれのあるセキュリティ上の問題が確認された場合、ソフトウェアのバグ対応等に係るバージョンアップ、セキュリティのアップデート、またライセンス等のアップデート作業を実施すること。

(4) 人流データの調達

別紙３に示す要件を満たす人流データの調達及び本システムへの入力を行うこと。（15 地区程度）

(5) 後任者への引継ぎ要件

業務終了後、受注者と別の者（以下、「後任者」という）が人流可視化システムの

運用保守等を行う場合には、後任者が運用・保守等業務を滞りなく行えるよう、後任者に対し確実に引継ぎを行うこと。引継ぎは、対象システムの業務に影響を与えないよう、受注者の負担において実施すること。引継ぎにおいては、少なくとも以下の事項を実施すること。

① システム運用保守に係るドキュメントの提供及び説明

② システム構成、運用手順及び保守手順に関する説明及び実機を用いたデモンストレーションの実施

③ クラウド環境、各種サービス及びアカウントに係る設定情報並びに権限移管に必要な対応

④ その他、一般的な引継ぎ業務として必要な事項であって機構が合理的に必要と認める事項

なお、上記以外の追加対応については機構と受注者が協議の上決定するものとする。

5　工程管理

(1)　受注者はプロジェクト計画書（作業内容、工程表、体制表に関する内容が記載されている簡易なドキュメント）を契約締結後 7 日以内に提出し、機構の承認を得ること。

(2)　提出したスケジュールに対し、その後の定期的な進捗報告等のプロジェクト管理を行うこと。

6　納品物

(1)　共通事項

①　受注者は、納入する際に指定のドキュメントを CD-ROM 等の媒体により日本語で提供すること。また、提出予定のドキュメントを一覧にまとめ提出すること。

②　CD-ROM 等の媒体に保存する形式は、Microsoft Office 形式若しくは PDF 形式とする。ただし、機構が別形式での提出を求めた場合はこの限りではない。

(2)　工程管理に関するドキュメント

①　プロジェクト計画書

②　議事録

(3)　システムに関するドキュメント

①　要件定義書

②　システム設計書

③　システム構成図

④　試験仕様書

(4)　システム保守・運用に関するドキュメント

①　運用・保守計画書

②　運用・保守手順書

(5)　操作マニュアルに関するドキュメント

① ユーザー向けシステム利用マニュアル
② 管理者向けシステム利用マニュアル
(6) その他のドキュメント（必要部数）
① その他関連ドキュメント

7 納品検査

受注者は、業務請負契約書第９条に基づき機構が必要と認める検査等について対応すること。納品検査は、受注者立ち会いの上で、機構が総合動作状態、書類等の納品検査を実施するものとする。

8 知的財産権について

(1) 本業務の実施に当たり作成・変更等が行われたプログラムや設計書、マニュアル等の著作権（著作権法 第21条から第28条で定められた権利を含む）及び納品物の所有権については、受注者が本業務実施以前から権利を保有している等の理由により、あらかじめ書面にて権利譲渡不可能と示されたもの以外は、当機構に帰属するものとする。
(2) 本業務の実施に当たり発生した権利について、受注者は著作人格権を行使しないものとする。
(3) 本業務の実施に当たり発生した権利について、今後、二次的著作物が作成された場合等であっても、受注者は原著作物の著作権者としての権利を行使しないものとする
(4) 本業務の実施に当たり作成・変更等が行われたプログラムや設計書、マニュアル等に第三者が権利を有する著作物が含まれる場合、受注者は当該著作物の使用に必要な費用負担・使用許諾契約等についての一切の手続を行うこと。なお、この場合、受注者は事前に当機構の承認を得ることとし、当機構は受注者が行った当該使用許諾契約の範囲で当該著作物を使用する。
(5) 本業務の実施に当たり第三者との間で著作権の権利侵害について争いが生じた場合は、当該争いの原因が当機構の責めに帰すべき場合を除き、受注者の責任及び負担において一切の処理を行うこと。当機構は争いの事実を知った場合は受注者に通知し、必要な範囲内で協力措置を実施する。

9 特記事項

(1) ソフトウェアのライセンス登録が必要な場合は、機構の指示に従い受注者が代行し登録を行い、かつ登録の証明を示すライセンス書等を一式にし、機構へ納めること。また、契約期間内でのライセンス登録情報の変更、ライセンス登録の継続等についても、機構の指示に従い作業を行うこと。
(2) 本調達価格には、要求仕様及びそれに係る費用を含むものとする。
(3) 仕様書に記載の無い事項等、疑義が生じたときは、その都度機構担当者と協議すること。
(4) 関係各所との打合せに必要な資料は、随時、機構担当者と協議の上作成すること。

(5)　法令及び条例等の関係法令を遵守すること。
(6)　本業務の履行上知り得た情報等を第三者に漏らさないこと。
(7)　本業務の完了は、成果品を提出し、検査に合格した時点とする。なお、検査合格後であっても、誤りが発見された場合には速やかにこれを訂正すること。
(8)　暴力団員等による不当介入を受けた場合の措置について
①　業務の履行に際して、暴力団員等による不当要求又は業務妨害（以下「不当介入」という。）を受けた場合は、断固としてこれを拒否するとともに、不当介入があった時点で速やかに警察に通報を行うとともに、捜査上必要な協力を行うこと。
②　①により警察に通報を行うとともに、捜査上必要な協力を行った場合には、速やかにその内容を記載した文書により発注者に報告すること。
③　暴力団員等による不当介入を受けたことにより、工程に遅れが生じる等の被害が生じた場合は、発注者と協議を行うこと。
(9)　受注者は、作業の全部又は主体的部分を一括して第三者に委託又は請け負わせてはならない。作業の一部を第三者へ委託する場合、機構の承認を得ること。

10　セキュリティ要件

業務にあたっては、別紙２に示すセキュリティ要件書を遵守すること。

11　生成 AI 利用に関する取扱い

本業務における生成 AI　の取扱いについては、別紙４「受注者等が生成 AI を利用する場合における取扱いについて」を参照すること。なお、本業務において、発注時点で個人情報等（仕様書別紙４に定める氏名等及び同意取得個人情報を除く。）、第三者の秘密情報及び利用権限のない著作物等以外に発注者が指定する生成 AI　へ　の入力等禁止情報はない。

12　遵守事項

政府機関統一基準等関連ガイドラインを理解した上で、別紙５に定めるとおりセキュリティ関連規程及び個人情報保護規程を遵守し、システムの構成や特性に応じ情報の機密性・完全性・可用性を各々適切に確保し取組を行うこと。また、契約締結時に規程等が改正されている場合は、改正後の規程等を遵守すること。

以　上

別紙－１

令和８年度人流データ可視化システム運用保守業務

システム要件書

目次

１　システムの全体像
１－（１）機能全体像
１－（２）機能を活用した業務の流れ

２　システムの機能要件
２－（１）用語定義
２－（２）データの基礎加工
２－（２）－①　滞在/移動判定
２－（２）－②　移動手段判定
２－（２）－③　道路 ID 付与
２－（２）－④　地区内の在住/在勤判定
２－（３）エリア等定義
２－（３）－①　エリアの指定
２－（３）－②　道路の指定
２－（３）－③　道路情報の追加
２－（４）可視化
２－（４）－①　地区の基礎理解１：地区内人量
２－（４）－②　地区の基礎理解２：地区内通行者量
２－（４）－③　地区来訪者の居住地理解
２－（４）－④　指定エリアの来訪者理解
２－（４）－⑤　指定道路の通行者理解
２－（４）－⑥　指定エリア外行動理解
２－（４）－⑦　２エリア間行動理解
２－（５）可視化に関わる制御
２－（６）データダウンロード
２－（７）その他ツールユーザー向け機能
２－（７）－①　エリア設定の保存・読み込み
２－（７）－②　ツールユーザー向けガイド
２－（８）管理者向け機能
２－（８）－①　ツールユーザーの作成・編集・削除
２－（８）－②　データ登録
２－（８）－③　データ削除

３　システムの非機能要件

３－（１）サーバー環境

３－（２）利用環境

３－（３）セキュリティ

３－（４）サービス提供時間

４　データ等に関する要件

４－（１）人流データ

４－（２）地図等のデータ

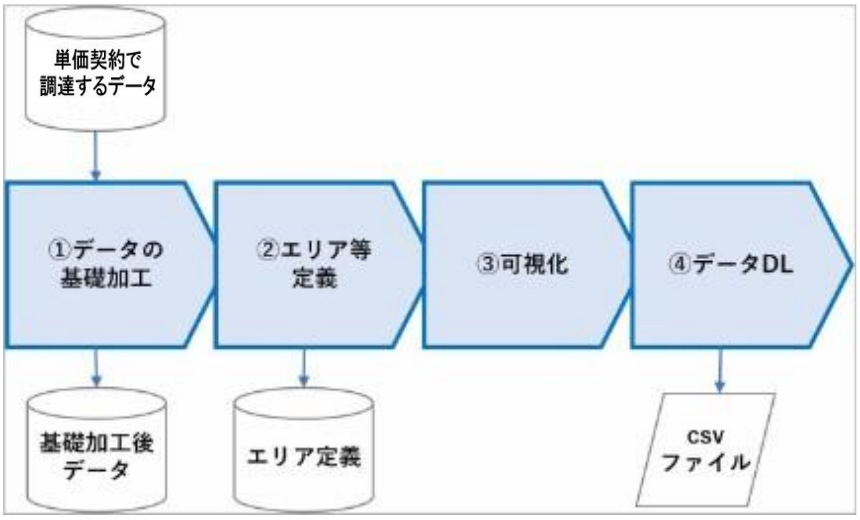
１　システムの全体概要

１－（１）　機能全体像

本システムは、GNSS 人流データを調達し、当機構の事業化検討の精度向上及び効率化に向けて人流の現況把握・分析を可能とするもの。

機能は主に以下の要素から構成される。

■主な処理フロー



① データの基礎加工

調達したローデータに対し、滞在/移動の判定や移動手段判定等の基礎加工を行う機能

② エリア等定義

可視化の対象となるエリアや道路を選択するための機能

③ 可視化

加工後のデータ及びエリア定義のデータを用い、様々な可視化を行う機能

④ データ DL

可視化されたデータを csv 形式等でダウンロードする機能

上記以外にも管理者向け機能なども存在する（詳細は２章以降参照）

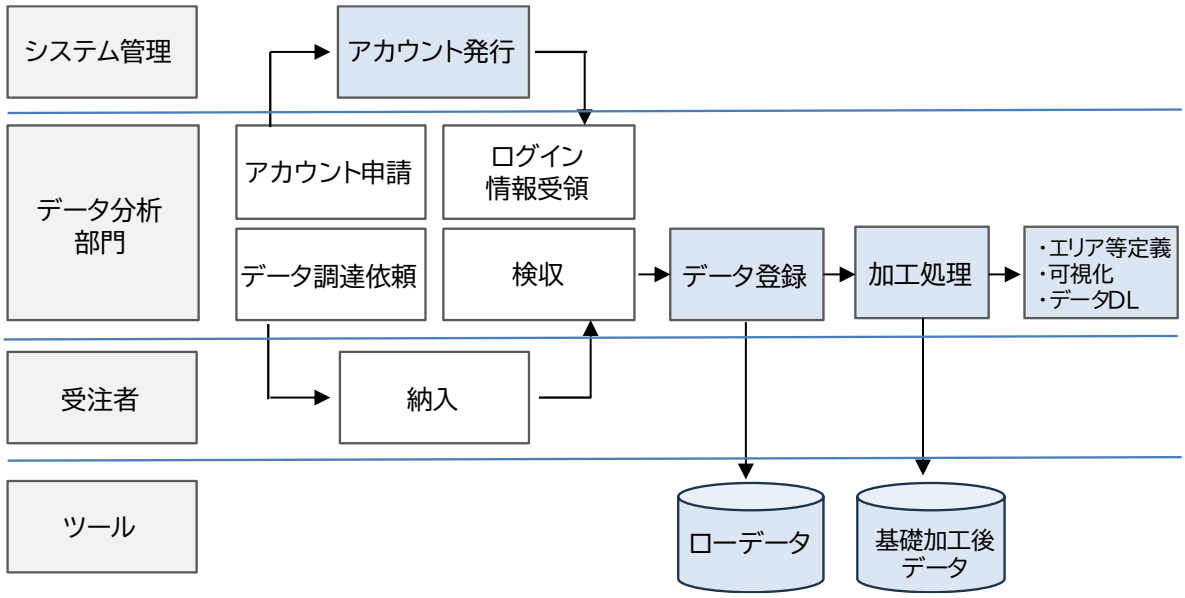
１－（２） 利用までの主な業務の流れ

本システムの利用に関わるのは「データ分析部門」と「システム管理部門」の２つ。

データ分析部門からのアカウント申請（メール等）を受け、アカウントを発行する流れと、データ分析部門による単価契約に基づいたデータ調達の流れがそれぞれ存在。

アカウント情報にもとづきシステムにログインし、データを登録・基礎加工を行ったうえで、各種エリア等の定義/可視化/データ DL などを行う。

■想定する流れ



２　システムの機能要件

２－（１）　用語定義

本要件書では、以下のように用語を定義する。

[エリア定義関連]

- 地区：データ分析の対象となる地理的範囲全体のこと。人流データ調達の際に、中心点の緯度・経度及び半径にて、具体的な範囲を定める。
- エリア：地区を、データ分析において考慮する単位に分割したもの。単一の施設の場合もあれば、複数の施設が含まれる街区の場合もある。

[人流データ関連]

- ユーザー：調達する人流データに含まれるスマートフォンユーザーのこと（人流可視化ツールの利用者は「ツールユーザー」と表記し、区別する）
- 拡大係数：人流データにもとづくユーザーカウント等から実際の滞在人数等を計算する（拡大推計を行う）際に用いる係数

[地図・道路関連]

- 道路ネットワークデータ（道路ＮＷデータ）：道路を線分で表現したデータ
- 道路ＩＤ：道路の各線分に割り振られたＩＤ

２－（２）　データの基礎加工

調達する人流データ（※4－(1)に詳述）に対し、以下に示す加工処理機能を具備すること。

２－（２）－①　滞在/移動判定

イ　処理概要

- ユーザーの位置情報ログが一定範囲内に一定時間止まっていた場合に滞在とみなす。

ロ　判定上の留意点

- 判定のためのパラメータについては、調達可能性がある社（※４―（１）に詳述）のいずれかの位置情報ログで検証を行い、適切な値を決定すること。

ハ　判定結果

- 各位置情報ログに対して、滞在/移動のフラグを付与すること。

２－（２）－②　移動手段判定

イ　処理概要

- 「移動」判定されたログに対し、電車・車・徒歩の区分を行う。

ロ　判定上の留意点

・ 電車判定においては別途整備する路線データ（※４―（２）に詳述）にもとづく。
・ 判定のためのパラメータついては、調達可能性がある社（※４―（１）に詳述）のいずれかの位置情報ログで検証を行い、適切な値を決定すること。

ハ 判定結果

・ 各位置情報ログに対して、移動手段区分を付与すること。

２－（２）－③ 道路 ID 付与

イ 処理概要

・ 移動手段区分が「徒歩」「車」と判定されたログに対し、道路との距離等にもとづく判定により移動している道路の特定を行う。

ロ 判定上の留意点

・ 判定に際しては、別途整備する道路ネットワーク（以下、道路ＮＷ、※４―（２）に詳述）と各位置情報ログのとの距離判定を行い、距離が最短となる道路を選定する方法を基本とする。

ハ 判定結果

・ 各位置情報ログに対して、道路ＩＤを付与すること。

２－（２）－④ 地区内の在住/在勤判定

イ 処理概要

・ 調達する人流データに存在するユーザー居住地/勤務地の緯度・経度情報にもとづき、ユーザーの居住地/勤務地が地区内であるかを判定する。

ロ 判定上の留意点

・ 「地区」は、中心点の緯度・経度及び半径（m）にて指定される。

ハ 判定結果

・ 各位置情報ログに対して、在住・在勤それぞれのフラグを付与すること。

２－（３） エリア等定義

地区内において特定場所を集計対象、可視化対象とするためのエリア設定に関する機能として、以下の処理を具備すること。

２－（３）－① エリアの指定

- ツールユーザーが画面上に表示された地図をみながら、マウス操作等により、ポリゴン（多角形）、円、長方形の３種類の方法で、エリアを指定し、保存ができること。
- 町丁目を指定してエリアを設定し、保存ができること。

２－（３）－② 道路の指定

- ツールユーザーが画面上に表示された地図をみながら、マウス操作等により、ポリゴン（多角形）、円、長方形の３種類の方法で、道路 ID 群を選択できること。
- なお、道路 ID 群の選択については、上記３種類の方法による範囲指定により、当該範囲に含まれる道路 NW データ（線分データ）をツールユーザーが確認し、必要に応じて線分の追加・削除を個別に行ったうえで対象を確定するなど、意図する道路 ID 群の選択が容易になっている機能の実現が望ましい。

２－（３）－③ 道路情報の追加

- ツールに取り込んだ道路 NW データに対し、道路の追加・削除を行えること。
- 追加・削除を行う際には、ツールユーザーが地図及び道路 NW データを視覚的に確認しながら、追加・削除をマウス操作等により行えるようにすること。
- システムに初期登録されている既存道路 NW データに対し、道路の削除を行えること。

２－（４）　可視化

以下、①～⑦の可視化要件を実現するようなデータ加工、及び集計・描画処理を具備すること。なお、①～⑦は必ずしも可視化メニューの構成を表すものではなく、要件整理の枠組みに過ぎない。また、「イメージ」として表示している描画要素もあくまで参考情報としての位置づけとする。

画面の構築に際しては、調達可能性がある社（※４―（１）に詳述）のいずれかの位置情報ログを利用した可視化を行い、表現等を決定すること。

２－（４）－①　地区の基礎理解１：地区内人量

人流データの調達対象とした地区全体を俯瞰し、地区内のどこに、どんな人が、どの程度の量、存在するかを可視化する。

イ　可視化要素

- 人数（拡大推計値及び色分布図）
- 性別・年代分布
- 地区内居住者/勤務者/来街者比率

ロ　可視化・絞り込みの切り口

- 時間帯別
- 日にち（複数日を選択可能）
- 性別・年代（地図表示対象の絞り込み）
- 地区内居住者/勤務者/来街者（地図表示対象の絞り込み）
- 平日、休日別
- エリア

ハ　可視化形態

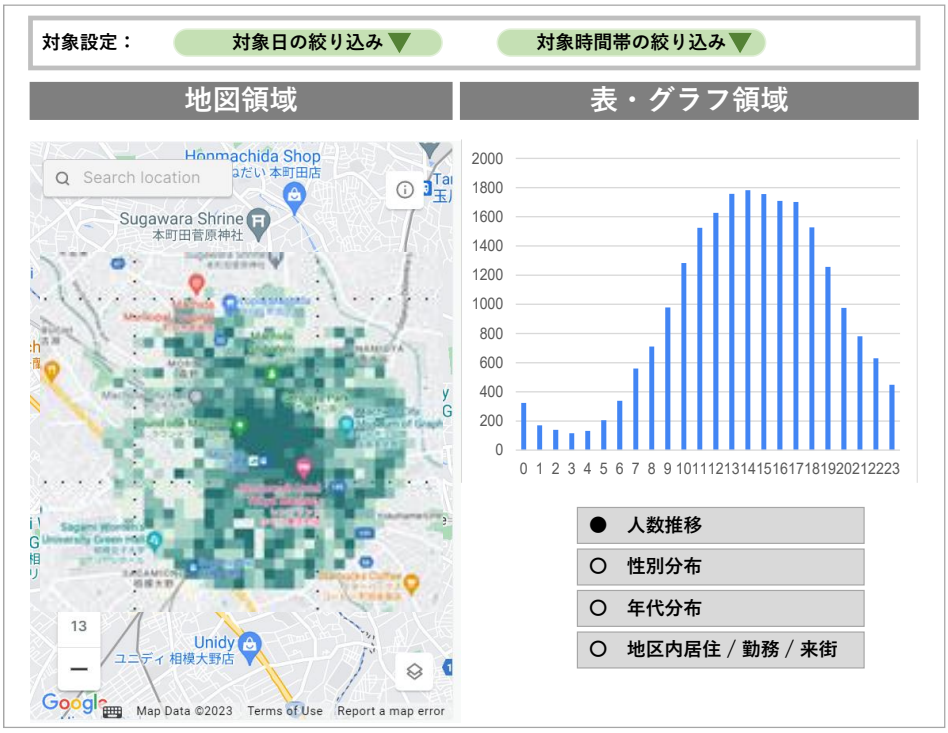
[表・グラフ表現]

- 時間帯別平均人数推移
  - ➢　内訳として、性別分布、年代分布、地区内居住者/勤務者/来街者分布

[地図表現]

- 単位面積あたりの人の量に関する分布図
- 色の濃淡や色分けで人の量の多寡を表現したタイル形式
- 地図の縮尺にあわせ、表示するタイルサイズも動的に変更

［イメージ図］


対象設定：
対象日の絞り込み
対象時間帯の絞り込み
地図領域
表・グラフ領域
Search location
Sugawara Shrine
本町田菅原神社
Unidy
ユニディ 相模大野店
Map Data ©2023
Terms of Use
Report a map error
2000
1800
1600
1400
1200
1000
800
600
400
200
0
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23
人数推移
性別分布
年代分布
地区内居住 / 勤務 / 来街

２－（４）－②　地区の基礎理解２：地区内通行者量

人流データの調達対象とした地区全体を俯瞰し、地区内の道路ごとの人流を可視化する（車等での移動者、歩行者）

イ　可視化要素

・ 道路 NW に割り付けられた人数をベースとした色分布図

ロ　可視化・絞り込みの切り口

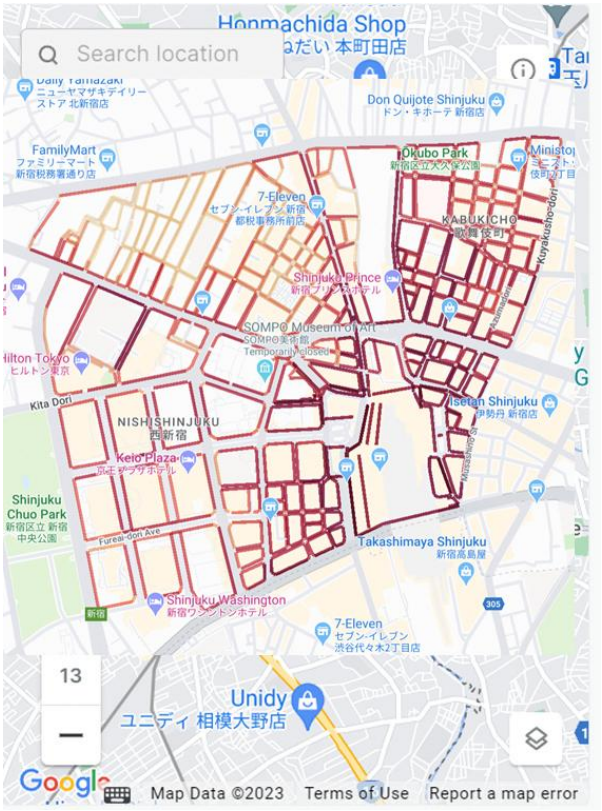
・ 時間帯別
・ 日にち（複数選択）
・ 移動手段
・ 地区内居住者/勤務者/来街者（地図表示対象の絞り込み）
・ 平日、休日別
・ エリア

ハ　可視化形態

［地図表現］

・ 道路 NW あたりの通行者量に関する分布図
・ 線の色の濃淡や色分けで通行者量の多寡を表現

【イメージ図】



２－（４）－③　地区来訪者の居住地理解

人流データの調達対象とした地区来訪者の居住地分布を地図・グラフに可視化する。

イ　可視化要素

・ 居住地の分布図（地区外も含む）
・ 居住地ランキング（市区町村単位）

ロ　可視化・絞り込みの切り口

・ 日にち（複数日を選択可能）
・ エリア
・ 地区内居住者/勤務者/来街者（地図表示対象の絞り込み）
・ 平日、休日別

ハ　可視化形態

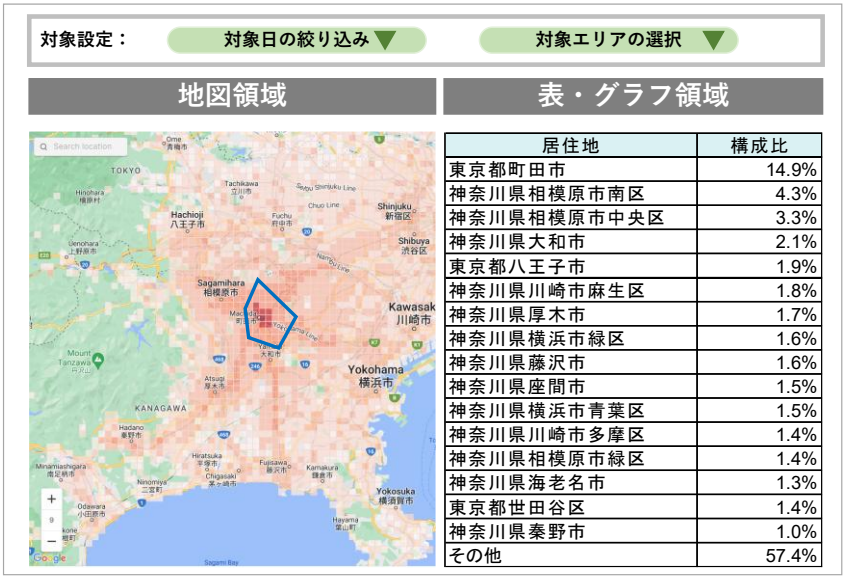
[表・グラフ表現]

・ 居住地ランキング（市区町村単位）

[地図表現]

・　単位面積あたりの居住者の量に関する分布図
・　色の濃淡や色分けで人の量の多寡を表現したタイル形式
・　地図の縮尺にあわせ、表示するタイルサイズも動的に変更

【イメージ】



居住地	構成比
東京都町田市	14.9%
神奈川県相模原市南区	4.3%
神奈川県相模原市中央区	3.3%
神奈川県大和市	2.1%
東京都八王子市	1.9%
神奈川県川崎市麻生区	1.8%
神奈川県厚木市	1.7%
神奈川県横浜市緑区	1.6%
神奈川県藤沢市	1.6%
神奈川県座間市	1.5%
神奈川県横浜市青葉区	1.5%
神奈川県川崎市多摩区	1.4%
神奈川県相模原市緑区	1.4%
神奈川県海老名市	1.3%
東京都世田谷区	1.4%
神奈川県秦野市	1.0%
その他	57.4%

２－（４）－④　指定エリアの来訪理解

地区のうち、2－(3)で定義される特定のエリアにフォーカスし、エリア内にどんな人が存在するかを可視化する。

イ　可視化要素

(イ)人数（拡大推計値）
(ロ)性別・年代分布
(ハ)地区内居住者/勤務者/来街者比率
(ニ)滞在時間分布
(ホ)来訪時移動手段分布

ロ　可視化・絞り込みの切り口

・　時間帯別
　　※上記「イ　可視化要素」の（イ）、（ロ）、（ハ）を対象とする。
・　日にち（複数選択）
・　エリア

・　地区内居住者/勤務者/来街者（地図表示対象の絞り込み）
・　平日、休日別

ハ　可視化形態

[表・グラフ表現]

・　時間帯別平均人数推移
　➢　内訳として、性別分布、年代分布、地区内居住者/勤務者/来街者分布
・　滞在時間分布
・　来訪時移動手段分布

[地図表現]

・　特になし。（選択されたエリアが表示されており、データ表示は無しの想定）

[イメージ図]



２－（４）－⑤　指定道路の通行者理解

　地区のうち、特定の道路・道路群にフォーカスし、道路をどんな人が通過しているかを可視化する。

イ　可視化要素

・　人数（拡大推計値）
・　性別・年代分布
・　移動手段分布（車、徒歩）
・　地区内居住者/勤務者/来街者比率

ロ　可視化・絞り込みの切り口

・　時間帯別
・　日にち（複数選択）
・　道路

・ 地区内居住者/勤務者/来街者（地図表示対象の絞り込み）
・ 平日、休日別

ハ　可視化形態

[表・グラフ表現]

・ 時間帯別平均人数推移
  ➢ 内訳として、性別分布、年代分布、移動手段分布、地区内居住者/勤務者/来街者分布

[地図表現]

・ 特になし。（選択された道路が表示されており、データ表示は無しの想定）

[イメージ図]



２－(４)－⑥ 指定エリア外行動理解

地区内の特定エリア（主エリア）に来訪している人が、どのような経路で来訪しているのか、来訪前後にどのエリアを移動・滞在しているのかを可視化する。

イ　可視化要素

(イ)来訪者のエリア外の行動履歴（同日、前後 30 分/前後 60 分）
(ロ)周辺道路（複数）移動者の比率（経路 A と B で３：４等）
(ハ)追加で保存リストより選択されたエリア（副エリア）への訪問率（同日または１か月）

ロ　可視化・絞り込みの切り口

- 日にち（複数選択）
- 主エリア
- 評価対象とする経路　　※イ可視化要素(ロ)のみ
- 移動手段　　※イ可視化要素(ロ)のみ
- 評価対象とする副エリア　※イ可視化要素(ハ)のみ

ハ　可視化形態

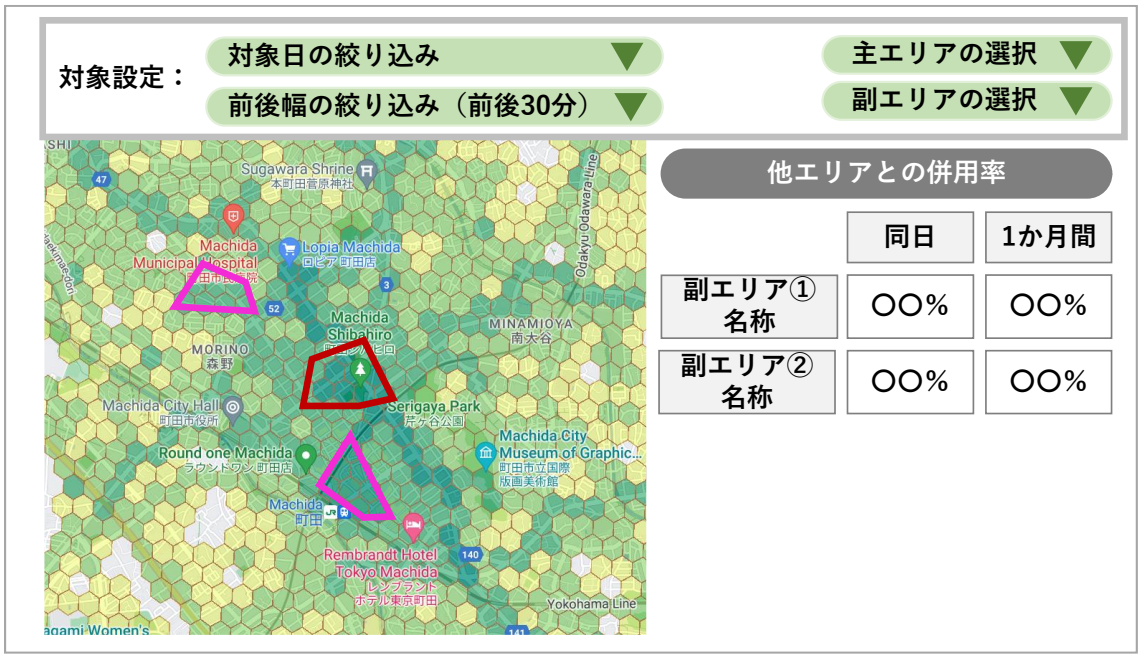
[表・グラフ表現]

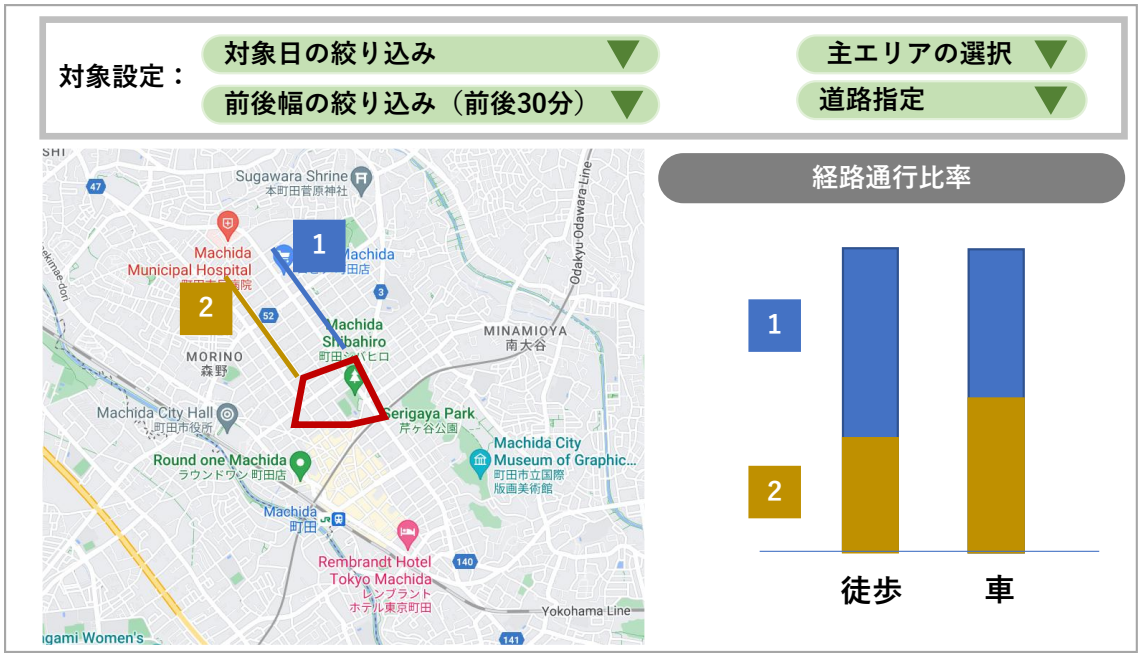
- 主エリア来訪者の副エリアへの来訪率（期間全体 / 同日回遊）
- 経路通行比率
- 地区内居住者/勤務者/来街者（地図表示対象の絞り込み）
- 平日、休日別

[地図表現]

- 来訪者の主エリア外の行動履歴（同日 / 前後 30 分/前後 60 分、地区外含む）
  - 単位面積あたりの人の量に関する分布図
  - 色の濃淡や色分けで人の量を表現
  - 地図の縮尺にあわせ、表示するタイルサイズも動的に変更
- 評価対象とする経路選択のために、指定エリア来訪者が通行した道路に関するヒートマップを表示

［イメージ図］





２－（４）－⑦　２エリア間の行動理解

対象地と駅周辺の商業施設など、特定エリア間を移動している人が、どのような経路で移動しているのかを可視化する。

イ　可視化要素

(イ)保存リストより選択された２エリア間のエリア外行動履歴

(ロ)追加で指定された道路（複数）移動者の比率（経路Ａと Ｂで３：４とか）

ロ　可視化・絞り込みの切り口

- 日にち（複数選択）
- エリア選択（２エリア）
- エリア間の所要時間（15 分間、30 分間、60 分間）
- 評価対象とする経路の指定　※イ可視化要素(ロ)のみ
- 移動手段　※イ可視化要素(ロ)のみ

ハ　可視化形態

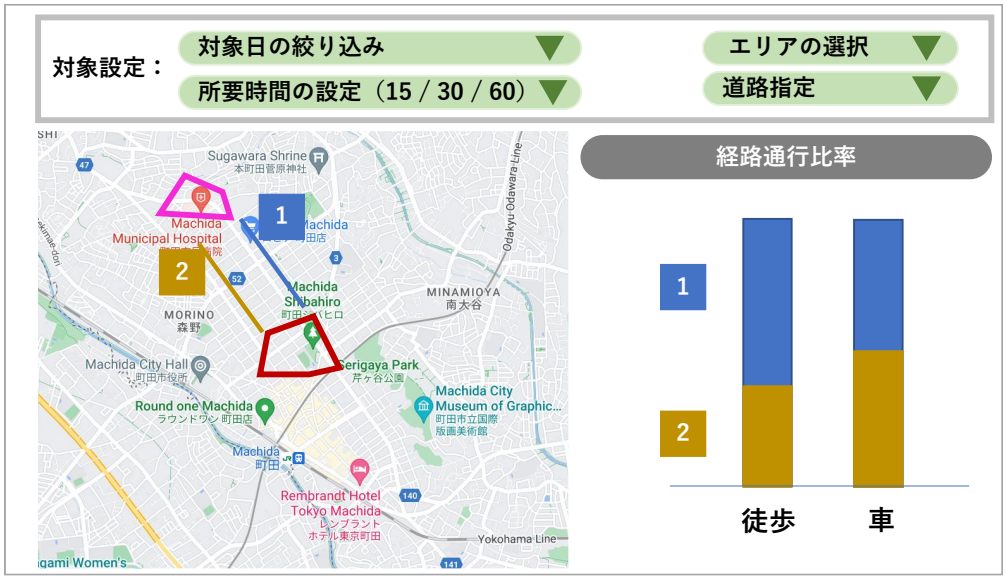
[表・グラフ表現]

- 経路通行比率

[地図表現]

- 来訪者のエリア外の行動履歴（地区外含む）
  - ➢ 単位面積あたりの人の量に関する分布図
  - ➢ 色の濃淡や色分けで人の量を表現
  - ➢ 地図の縮尺にあわせ、表示するタイルサイズも動的に変更
- 評価対象とする経路選択のために、指定エリア来訪者が通行した道路に関するヒートマップを表示

[イメージ図]



２－（５）　可視化に関わる制御

地図へのデータ表現における視認性の高さや操作性の良さ（直観的操作、表示までのスピード等）を重視し、システムを構築すること。

可視化・評価対象となる「エリア」は比較的固定的であると想定しているため、ビッグデータを扱いつつも、スピーディーな表示を実現するような仕組みを構築すること。

２－（６）　データダウンロード

画面に出力される分析結果等は、以下のフォーマットでのダウンロードが可能となること。

■地図

- 地図エリアの描画結果をそのまま画像としてダウンロードできること。
- 画像には、描画結果の理解に必要な凡例及び地図の印刷物利用に必要な著作権表記も含めること。

■グラフ・表

- 表示されているグラフ、表のフォーマット通りに csv 形式でのデータがダウンロードできること。

２－（７）　その他ツールユーザー向け機能

２－（１）～（６）に規定された機能以外にも、ツールユーザー向け機能として以下を実現すること。

２－（７）－①　エリア設定の保存・読み込み

- 「2－(3)」で記載した「エリア等定義」の結果を、保存し、同一地区内のデータ集計等を行う際には、他のツールユーザーにも利用できるようにすること。
- 「エリア等定義」を保存する際には、エリア情報のみならず任意のエリア名称を付与できるようにすること。
- 保存済みの「エリア等定義」を利用する場合は、エリア名称のリストから選択可能とし、選択時には、具体的なエリア等の指定範囲をツールユーザーが視覚的に確認できるようにすること。（地図上でのポリゴン、四角形、円の表記を想定）

２－（７）－②　ツールユーザー向けガイド

- 各可視化結果（地図、グラフ、表）をツールユーザーが解釈するために必要な数値の定義等に対する補足説明を、ツールユーザーが適宜参照できるようにすること。

２－（７）－③　分析条件の保存・読み込み

・　ツールユーザーが実行した分析条件（データ、エリア、フィルタ項目）の保存、再表示機能を設けること。

２－（８）　管理者向け機能

ツールの管理者向けに以下の機能を具備すること。

２－（８）－①　ツールユーザーの作成・編集・削除

ツールユーザー登録依頼などを受け、以下の登録・変更・削除を可能とする。

・　新規ツールユーザーの登録：ツールユーザーの ID、パスワードを発行するとともに、当該ツールユーザーが閲覧、編集可能な地区の設定を行う。
・　編集：パスワードのリセット（再発行）や閲覧、編集可能な地区の修正を行う。
・　削除：ツールユーザーの削除を行う。

【補足】ツールユーザーの権限体系

ツールユーザー種別は、以下の３種類

いずれも、個人に対する発行ではなく、プロジェクトメンバー、チーム内での共用を想定

■閲覧者：プロジェクト担当外のメンバーへの割り当てを想定

・　保存済みの「エリア等定義」にもとづく各種可視化結果の画面で閲覧及びデータダウンロードが可能。

■編集者：当該地区のプロジェクト推進担当メンバーへの割り当てを想定

・　閲覧者権限に加え、「エリア等定義」の追加・編集・削除が可能。

■管理者：ツールの管理運営チームへの割り当てを想定

・　編集者権限に加え、ツールユーザーの新規登録・変更・削除が可能、データの削除が可能。

２－（８）－②　データ登録

・　調達した地区の GNSS データを csv ファイル形式にてツールへアップロードする機能を具備すること。
・　なお、GNSS データ提供会社からの納入データを格納するディスクスペースを整備しておき、当該スペースに格納されたファイルを読み込むことを想定している。

２－（８）－③　データ削除

・　ツールに登録されている人流データの削除を行えること。

・　人流データの削除により、付帯する「エリア等定義」のデータもあわせて削除する

３　システムの非機能要件

３－（１）　サーバー環境

・　別紙２セキュリティ要件書を満たすものとすること。また、過去１年以内に情報セキュリティインシデントが発生している場合は、当該インシデント原因に対して適切に対策されていること。なお、ISMAP 又は ISMAP-LIU クラウドサービスリストに登録されているクラウドサービスを提供する場合は、 本項目の確認は不要

・　同時アクセス数は数人程度と想定されるが、今後の処理能力等の拡張が柔軟に行えること。

３－（２）　利用環境

・　UR にて別途調達する端末・通信環境での利用を想定。

・　端末・通信環境については UR と別途協議し決定すること。

・　ウェブブラウザ（Microsoft Edge_111.0.1551.44_64 ビット）での利用が可能であること。また、機構が使用するウェブブラウザのバージョンアップが行われた際には、適宜新環境での利用が可能になるように対応すること。

３－（３）　セキュリティ

仕様書及び別紙２セキュリティ要件書に準ずること。

３－（４）　サービス提供時間

原則として、平日 24 時間とする。

４．データ等に関する要件

４－（１）：人流データ

- データ種別：スマートフォンアプリから取得できる GNSS ログ
  なお、位置情報の取得について利用者承諾済かつ個人情報を含まないデータであること
- データ項目：
  - ユーザーID、緯度・経度、取得日時
  - ユーザーID、性別・年代、居住地の緯度・経度
    なお、居住地の緯度・経度は、個人を特定できないレベルであることを前提とする。
- エリア指定：
  - UR が指定する緯度・経度を中心とした半径１～５km に来訪したユーザーの同日行動ログ（円外のログを含む）
- 期間指定：
  - 原則月単位での指定とする
- その他数値：
  - GNSS ログをベースにカウントしたユーザー数を実数換算するための拡大係数を提示すること。
- （参考）調達候補企業：
  - 株式会社ブログウォッチャー（https://www.blogwatcher.co.jp/）
  - 株式会社 unerry（https://www.unerry.co.jp/）
  - 株式会社 Agoop（https://agoop.co.jp/）

４－（２） 地図等のデータ

- 地図データ：視認性が良く、印刷も含めた外部利用が可能であること。
  - Google マップもしくは同等の視認性がある地図が望ましく、また航空写真による地図確認も行えることが望ましい。
- 道路データ：車道のみならず、歩道も含めた路線データ（線分データ）があること
- 鉄道路線データ：国土交通省が提供する「鉄道データ」の利用を想定
  （https://nlftp.mlit.go.jp/ksj/gml/datalist/KsjTmplt－N02－v2_3.html）

以上

別紙－２

令和８年度人流データ可視化システム運用保守業務

セキュリティ要件書

1. 情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、受注者は、当該事項について速やかに機構に報告すること。
2. 受注者は、以下の情報セキュリティ対策を実施すること。
   (ア) 受注者、再委託先又はその他の者によって、情報システムに機構が意図しない変更が加えられないための管理体制の確保
   (イ) 前号を確認する際の参照情報として用いるための、委託業務の実施場所、委託業務従事者の所属・専門性（情報セキュリティに係る資格（情報処理安全確保支援士等）・研修実績等）及び実績に関する情報提供
3. 情報システムに実装されたセキュリティ機能が適切に運用されるために、情報システムの運用環境に課せられるべき条件（物理的、ネットワーク環境的及び人的側面）を整備し、機構の承認を得ること。
4. 受注者は、受注者が実施する情報セキュリティ対策による情報システムの変更内容について、機構に速やかに報告すること。
5. 受注者は、クラウドサービスの安全管理について、以下の対策を実施すること。
   (ア) 適切な主体認証、アクセス制御の管理の実施
   (イ) 情報の滅失、破壊等に備えたバックアップの取得
6. 受注者は、クラウドサービスを安全に利用するため、以下の措置を講ずること。
   (ア) 以下のクラウドサービスの利用に係る安全管理の実施
      ① クラウドサービスを管理する機能に対して適切に主体認証、アクセス制御の管理を行うこと
      ② クラウドサービスの利用者に対して識別コードを付与する場合において、適切に主体認証、アクセス制御の管理を行うこと。
      ③ クラウドサービス利用者が情報の公開設定を変更することができる機能を有するクラウドサービスである場合は、公開設定が正しく運用できているかの定期的な確認を実施すること
      ④ バックアップの機能を有するクラウドサービスである場合は、適切なバックアップの取得をすること。
   (イ) クラウドサービスで情報セキュリティインシデントが発生した際の連絡体制の機構への事前提出
7. 受注者は、機器等の納入時又は情報システムの受入れ時の確認・検査において、以下の情報セキュリティ対策に係る要件が満たされていることを証明すること。
   (ア) 情報システムの構築時に使用し、運用時に不要となる識別コードが削除されていること。
   (イ) 機器等において推測可能な初期値として設定されている主体認証情報等が変更されていること。
   (ウ) 機器等において公開された脆弱性について対策を実施していること。

(エ) 機器等において不要なポートが開放されていない、不要なサービスが起動していない、利用を認めていないソフトウェアが動作していないこと。

8. 受注者は、情報システムの運用・保守において、情報システムに実装されたセキュリティ機能が適切に運用されていることを確認すること。
9. 受注者は、情報システムで不要となった識別コードや過剰なアクセス権限等の付与がないか適時見直すこと。
10. 受注者は、運用中の情報システムにおいて３か月毎に脆弱性対策の状況を確認すること。
11. 受注者は、運用中の情報システムの脆弱性の存在が明らかになった場合には、情報セキュリティを確保するための措置を講ずること。
12. 受注者は、不正な行為及び意図しない情報システムへのアクセス等の事象が発生した際に追跡できるように、運用・保守に係る作業についての記録を管理し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、見直しが必要な場合には機構に提案すること。
13. 受注者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を機構に提案すること。
14. 受注者は、情報システムの更改又は廃棄を行う場合は、当該情報システムに保存されている情報について、当該情報の格付及び取扱制限を考慮した上で、以下の措置を適切に講ずること。

    (ア) 情報システム更改時の情報の移行作業における情報セキュリティ対策

    (イ) 情報システム廃棄時の不要な情報の抹消（利用不能かつ復元が困難な状態にすること）
15. 受注者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを３か月毎に検討し、必要な措置を機構に提案すること。
16. 多様なソフトウェアを利用することにより脆弱性が存在する可能性が増大することを防止するため、以下を全て考慮した上で、仮想サーバ・クラウドサービス及びそれらの環境で利用を認めるソフトウェアのバージョンも含め定め、機構に承認をとること。また、利用を認めるソフトウェアについて、３か月毎に見直しを行うこと。

    (ア) ソフトウェアベンダ等のサポート状況

    (イ) ソフトウェアと外部との通信の有無及び通信する場合は、プロトコル（バージョンを含む）、使用するポート、暗号化の有無

    (ウ) インストール時に同時にインストールされる他のソフトウェア

    (エ) その他、ソフトウェアの利用に伴う情報セキュリティリスク
17. 受注者は、仮想サーバ・クラウドサービスに新たな機能が追加されていないか、アクセス権が適切に付与されているか等を３か月毎に確認し、不適切な状態にあると判断した場合には改善を図ること。なお、改善を図る場合は、作業日、作業を行った仮想サー

バ・クラウドサービス名、具体的な作業内容及び作業者、正常動作を確認した者などを含む変更事項等を記録し、管理すること。

18. 受注者は、仮想サーバ又はクラウドサービス上での情報セキュリティインシデントの発生を監視するため、以下の対策を講ずること。
    (ア) アクセスログ等を３か月毎に確認する。
    (イ) IDS/IPS、WAF（Web Application Firewall）等を設置する。
    (ウ) 不正プログラム対策ソフトウェアを利用する。
    (エ) ファイル完全性チェックツールを利用する。
    (オ) CPU、メモリ、ディスク I/O 等のシステム状態を確認する。
    (カ) ホスト型の IDS/IPS を利用する。
    (キ) ユーザ、グループ、システム管理者の追加、変更の有無を確認する。
    (ク) 管理者、ユーザのパスワード漏洩の有無、大量のログオン失敗や、通常とは異なる時間帯やアクセス元 IP アドレスからのログインがないか確認する。
19. 受注者は、脆弱性が存在する可能性が増大することを防止するため、以下のウェブサーバの管理や設定を行い、ウェブサーバが備える機能のうち、必要な機能のみを利用すること。
    (ア) CGI 機能を用いるスクリプト等は必要最低限のものに限定し、CGI 機能を必要としない場合は設定で CGI 機能を使用不可とする。
    (イ) ディレクトリインデックスの表示を禁止する。
    (ウ) ウェブコンテンツ作成ツールやコンテンツ・マネジメント・システム（CMS）等における不要な機能を制限する。
    (エ) ウェブサーバ上で動作するソフトウェアは、最新のものを利用するなど、既知の脆弱性が解消された状態を維持する。
20. 受注者は、ウェブサーバからの不用意な情報漏えいを防止するために、以下のウェブサーバの管理や設定を行うこと。
    (ア) 公開を想定していないファイルをウェブ公開用ディレクトリに置かない。
    (イ) 初期状態で用意されるサンプルのページ、プログラム等、不要なものは削除する。
    (ウ) ウェブサーバに保存する情報を特定し、サービスの提供に必要のない情報がウェブサーバに保存されないことを確認する。
21. 受注者は、ウェブコンテンツの編集作業を担当するアカウントの限定として、以下のウェブサーバの管理や設定を行うこと。
    (ア) ウェブサーバ上のウェブコンテンツへのアクセス権限は、ウェブコンテンツの作成や更新に必要な者以外に更新権を与えない。
    (イ) OS やアプリケーションのインストール時に標準で作成される識別コードやテスト用に作成した識別コード等、不要なものは削除する。
22. 受注者は、ウェブコンテンツの編集作業に用いる端末の限定、識別コード及び主体認証

情報の適切な管理として、以下のウェブサーバの管理や設定を行うこと。

(ア) ウェブコンテンツの更新に用いる管理機能については、多要素認証又はこれと同等の認証を実施するとともに、接続元 IP アドレスの制限その他適切なアクセス制御を実施すること。

(イ) ウェブコンテンツの更新の際は、ウェブサーバに接続する接続元の IP アドレスを必要最小限に制限する。

(ウ) ウェブコンテンツの更新に利用する識別コードや主体認証情報は、情報セキュリティを確保した管理を行う。

23. 受注者は、インターネットを介した通信時の盗聴による第三者への情報の漏えい及び改ざんの防止並びに正当なウェブサーバであることを利用者が確認できるようにするための措置として、以下のウェブサーバの実装を行い、全ての情報に対する暗号化及び電子証明書による認証の対策を講ずること。

(ア) TLS 機能を適切に用いる。

(イ) TLS 機能のために必要となるサーバ証明書には、利用者が事前のルート証明書のインストールを必要とすることなく、その正当性を検証できる認証局（証明書発行機関）により発行された電子証明書を用いる。

(ウ) 暗号技術検討会及び関連委員会（CRYPTREC）により作成された「TLS 暗号設定ガイドライン」に従って、TLS サーバを適切に設定する。

24. 受注者は、データベースに対する内部不正を防止するため、以下の管理者アカウントの適正な権限管理を行うこと。

(ア) 必要に応じて情報システムの管理者とデータベースの管理者を別にする。

(イ) データベースに格納されているデータにアクセスする必要のない管理者に対して、データへのアクセス権を付与しない。

(ウ) データベースの管理に関する権限の不適切な付与を検知できるよう、措置を講ずる。

25. 受注者は、データベースに格納されているデータにアクセスした利用者を特定できるよう、措置を講ずること。

26. 受注者は、データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、以下の措置を講ずること。

(ア) 一定数以上のデータの取得に関するログを記録し、警告を発する。

(イ) データを取得した時刻が不自然であるなど、通常の業務によるデータベースの操作から逸脱した操作に関するログを記録し、警告を発する。

27. 受注者は、データベース及びデータベースへアクセスする機器等の脆弱性を悪用した、データの不正な操作を防止するため、データベースにアクセスする機器上で動作するプログラムに対して、SQL インジェクションの脆弱性を排除すること。

28. 受注者は、適切に暗号化を行うこと。また、データベースに格納されているデータに対

して暗号化を実施する場合には、バックアップデータやトランザクションデータ等についても暗号化を実施すること。

29. 受注者は、主体の識別及び主体認証を行う機能（知識：パスワード等、利用者本人のみが知り得る情報）を設けること。

30. 受注者は、主体認証情報としてパスワードを使用し、主体認証情報を付与された主体自らがパスワードを設定することを可能とする場合には、辞書攻撃等によるパスワード解析への耐性を考慮し、強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を使用することを利用者に守らせる機能を設けること。

31. 受注者は、主体認証を行う情報システムにおいて、主体認証情報の漏えい等による不正行為を防止するための措置及び不正な主体認証の試行に対抗するための措置として、以下の対策を講ずること。

(ア) 主体認証情報の漏えい等による不正なアクセスを防止するため、以下を全て含む措置を講ずること。

① 原則として、機器等において初期値として設定されている識別コードを使用しない。

② 不要な識別コードを無効にする。

(イ) 主体認証情報が第三者に対して明らかにならないよう、以下を全て含む方法を用いて適切に管理すること。

① 主体認証情報を送信又は保存する場合には、その内容を暗号化する。

② 主体認証情報に対するアクセス制限を設ける。

③ 主体認証情報に対するアクセスに関するログを保存し、アクセスした主体を確認する。

(ウ) 主体認証情報を他の主体に不正に利用され、又は利用されるおそれを認識した場合の対策として、以下の機能を設けること。

① 当該主体認証情報及び対応する識別コードの利用を停止する機能

② 主体認証情報の再設定を利用者に要求する機能

32. 受注者は、情報システムにアクセスする全ての主体に対して、識別コード及び主体認証情報を適切に付与（発行、更新及び変更を含む。）し、管理するため、以下の措置を講ずること。

(ア) 情報システムを利用する許可を得た主体に対してのみ、識別コード及び主体認証情報を付与すること。

(イ) 識別コードの付与に当たっては、以下の措置を講ずること。

① 単一の情報システムにおいて、ある主体に付与した識別コード（共用識別コードを除く。）を別の主体に対して付与することの禁止

② 主体への識別コードの付与に関する記録を消去する場合の機構からの事前の許可

(ウ) 主体以外の者が識別コード又は主体認証情報を設定する場合、主体以外の者が設定する主体認証情報は強固なパスワードに必要な十分な桁数を備えた第三者に容易に推測できないパスフレーズ等を設定し、主体へ安全な方法で主体認証情報を配布するよう、措置を講ずること。

(エ) 識別コード及び知識による主体認証情報を付与された主体に対し、主体以外の者が設定した主体認証情報（必要に応じて、初期設定の識別コードも）を速やかに変更するよう、促すこと。なお、主体認証情報の変更を確認できる機能がある場合は、変更日時を確認し変更がなされない（使用していない）識別コードについては無効にするなどの措置を講ずること。

(オ) 知識による主体認証方式を用いる場合には、他の情報システムで利用している主体認証情報を設定しないよう主体に注意を促すこと。

(カ) 情報システムを利用する主体ごとに識別コードを個別に付与すること。ただし、機構の判断の下、やむを得ず共用識別コードを付与する必要がある場合には、利用者を特定できる仕組みを設けた上で、機構が定めた共用識別コードの取扱いに関する実施手順に従って利用者に付与すること。

33. 受注者は、主体が情報システムを利用する必要がなくなった場合は、当該主体の識別コード及び主体認証情報の不正な利用を防止するために、以下を例とする措置を講ずること。

(ア) 当該主体の識別コードを無効にする。

(イ) 当該主体に交付した主体認証情報格納装置を返還させる。

(ウ) 無効化した識別コードを他の主体に新たに発行することを禁止する。

34. 受注者は、主体の属性やアクセス対象の属性等に基づき、以下を例とするアクセス制御を実施すること。

(ア) 利用時間や利用時間帯によるアクセス制御

(イ) 同一主体による複数アクセスの制限

(ウ) IP アドレスによる端末の制限

(エ) ネットワークセグメントの分割によるアクセス制御

(オ) ファイルに記録された情報へのアクセスを制御するサーバにおいて主体認証を受けたユーザのみが、暗号化されたファイルに記録された情報に対し、与えられた権限の範囲でアクセス可能となる制御

35. 受注者は、情報システム及び情報へのアクセスを許可する主体が確実に制限されるように、アクセス制御機能を適切に運用すること。また、主体の属性、アクセス対象の属性に基づくアクセス制御の要件を３か月毎の確認により見直すこと。

36. 受注者は、主体から対象に対するアクセスの権限を必要最小限の範囲で適切に設定するよう、措置を講ずること。また、初期値として利用可能な管理者権限を有する識別コード（Administrator、root、admin 等）には、管理者権限を付与しない又は無効化す

ること。

37. 受注者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置として、以下の対策を講ずること。

(ア) 以下を例とする措置を講ずること。

① 業務上必要な場合に限定する

② 必要最小限の権限のみ付与する

③ 管理者権限を行使する場合は、当該権限の利用者を限定し、多要素認証及び必要に応じた IP アドレス制限等のアクセス制御を実施する

(イ) 管理者権限を有する識別コードの利用は権限を必要とする業務に限定し、一般の業務として使用させないこと。

38. 受注者は、主体から対象に対する不要なアクセス権限が付与されていないか３か月毎に確認すること。

39. 受注者は、情報システムにおいて、情報システムが正しく利用されていることの検証及び不正侵入、不正操作等がなされていないことの検証を行うために以下を例とする必要なログを取得すること。なお、情報システムに含まれる構成要素のうち、時刻設定が可能なものについては、情報システムにおいて基準となる時刻に、当該構成要素の時刻を同期させ、ログに時刻情報も記録されるよう、設定すること。

(ア) 情報システムで導入するソフトウェアにおいて、アクセスログを取得すること

(イ) ファイルアクセスを伴う場合、データベース及びファイルに対する操作に関するログを取得すること。

(ウ) 情報システムの利用記録、例外事象の発生に関するログを取得すること。

40. 受注者は、ログを取得する対象、ログの保存期間、要保護情報の観点でのログ情報の取扱方法等とともに以下のログとして取得する情報項目を管理すること。

(ア) 事象の主体（人物又は機器等）を示す識別コード

(イ) 識別コードの発行等の管理記録

(ウ) 情報システムの操作記録

(エ) 事象の種類

(オ) 事象の対象

(カ) 正確な日付及び時刻

(キ) 試みられたアクセスに関わる情報

(ク) 通信パケットの内容

(ケ) 操作する者、監視する者、保守する者等への通知の内容

41. 受注者は、取得したログに対する、不正な消去、改ざん及びアクセスを防止するため、適切なアクセス制御を含む、ログ情報の保全方法を定めること。

42. 受注者は、情報システムにおいて、取得したログを３か月毎に点検又は分析する機能を

設け、悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施すること。また、取得したログを効率的かつ確実に点検及び分析し、その結果を機構に報告するために、以下の対策を実施すること。

43. 受注者は、暗号化又は電子署名について、以下の措置を講ずること。

(ア) 情報システムのコンポーネント（部品）として、暗号モジュールを交換することが可能な構成とすること。

(イ) 複数のアルゴリズム、鍵長及びそれらに基づいた安全なプロトコルを選択することが可能な構成とすること。

(ウ) 選択したアルゴリズム及び鍵長が導入するソフトウェアに実装されており、かつ、暗号化された情報の復号又は電子署名の付与に用いる鍵及びそれに対応する主体認証情報等が安全に保護されることを確実にするため、「暗号モジュール試験及び認証制度」に基づく認証を取得している製品を選択すること。

(エ) 暗号化された情報の復号又は電子署名の付与に用いる鍵については、耐タンパ性を有する暗号モジュールへ格納すること。

44. 受注者は、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」に基づき、情報システムで使用する暗号及び電子署名のアルゴリズム及び鍵長並びにそれらを利用した安全なプロトコルを採用すること。また、暗号化された情報の復号又は電子署名の付与に用いる鍵について、管理手順を定めること。

45. 受注者は、電子署名を行うに当たり、電子署名の目的に合致し、かつ適用可能な公的な公開鍵基盤が存在する場合はそれを使用するなど、目的に応じた適切な公開鍵基盤を使用すること。

46. 受注者は、暗号及び電子署名を適切な状況で利用するため、以下の措置を講ずること

(ア) 電子署名の付与を行う情報システムにおいて、電子署名の正当性を検証するための情報又は手段を、以下のどちらかの方法により、署名検証者へ安全な方法で提供すること。

① 信頼できる機関による電子証明書の提供

② 機構の窓口での電子証明書の提供

(イ) 暗号化を行う情報システム又は電子署名の付与若しくは検証を行う情報システムにおいて、暗号化又は電子署名のために選択されたアルゴリズム又は鍵長の危殆化及びプロトコルの脆弱性に関する情報を３か月毎に入手し、必要に応じて、機構と共有を図ること。

47. 受注者は、情報システムの運用におけるセキュリティ監視について、以下の内容を含む監視手順を定め、適切に監視運用すること。

(ア) 監視するイベントの種類や重要度

(イ) 監視体制

(ウ) 監視状況の報告手順や重要度に応じた報告手段
(エ) 情報セキュリティインシデントの可能性を認知した場合の報告手順
(オ) 監視運用における情報の取扱い

48. 受注者は、ソフトウェアの脆弱性に関して、以下の情報を適宜入手すること。
(ア) 脆弱性の原因
(イ) 影響範囲
(ウ) 対策方法
(エ) 脆弱性を悪用する不正プログラムの流通状況

49. 受注者は、利用するソフトウェア（マネージドサービス・個別機能含む）は、サポート期間を考慮して選定し、サポートが受けられないソフトウェアは利用しないこと。

50. 受注者は、構成要素ごとにソフトウェアのバージョン等を把握し、当該ソフトウェアの脆弱性の有無を確認すること。

51. 受注者は、情報システムを構成する機器へのセキュリティパッチの適時の適用を前提とした運用設計を行うこと。

52. 受注者は、公開された脆弱性の情報がない段階において、クラウドサービス及びクラウドサービス上に構築するソフトウェア上でとり得る対策がある場合は、当該対策を実施すること。

53. 受注者は、クラウドサービス上で利用するソフトウェアにおける脆弱性対策の状況を３か月毎及び適時に確認すること。

54. 受注者は、脆弱性対策の状況の確認により、脆弱性対策が講じられていない状態が確認された場合及びクラウドサービス上で利用するソフトウェアに関連する脆弱性情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関する脆弱性対策計画を策定し、措置を講ずること。なお、ソフトウェアに関する脆弱性対策計画を策定する場合には、以下の事項を含めること。
(ア) 対策の必要性
(イ) 対策方法。この際、自動でソフトウェアを更新する機能を有する IT 資産管理ソフトウェアを導入するなどにより、効率的に脆弱性対策を実施する手法をあらかじめ決定すること。
(ウ) 対策方法が存在しないゼロデイと呼ばれる状態の場合又は対策が完了するまでの期間に対する一時的な回避方法
(エ) 対策方法又は回避方法が情報システムに与える影響
(オ) 対策の実施予定時期
(カ) 対策試験の必要性
(キ) 対策試験の方法
(ク) 対策試験の実施予定時期

55. 受注者は、脆弱性対策を実施する場合には、以下の事項を記録し、これらの事項のほかに必要事項があれば適宜記録すること。
(ア) 実施日
(イ) 実施内容
(ウ) 実施者
56. セキュリティパッチ、バージョンアップソフトウェア等の脆弱性を解決するために利用されるファイルは、信頼できる方法で入手し、完全性を検証すること。
57. 受注者は、不正プログラム対策ソフトウェア等の導入に当たり、以下の措置を講ずること。
(ア) 既知及び未知の不正プログラムの検知並びにその実行の防止の機能を有するソフトウェアを導入すること。
(イ) 不正プログラム対策ソフトウェア等が常に最新の状態となるように構成すること。
(ウ) 不正プログラム対策ソフトウェア等に定義ファイルを用いる場合、その定義ファイルが常に最新の状態となるように構成すること。
(エ) 不正プログラム対策ソフトウェア等の設定変更権限については、システム管理者が一括管理し、システム利用者に当該権限を付与しないこと。
(オ) 不正プログラム対策ソフトウェア等を１か月毎に全てのファイルを対象としたスキャンを実施するように構成すること。
58. 受注者は、想定される全ての不正プログラムの感染経路を特定し、不正プログラム対策ソフトウェア等の導入による感染の防止、端末の接続制限及び機能の無効化等による感染拡大の防止等の必要な対策を行うこと。
59. 受注者は、EDR ソフトウェア等を利用し、サーバ装置の活動を監視し、感染したおそれのある装置を早期にネットワークから切り離す機能を導入すること。
60. 受注者は、不正プログラム対策の実施を徹底するため、以下の不正プログラム対策に関する状況を適宜把握し、機構に報告するとともに、必要な対処を行うこと。
(ア) 不正プログラム対策ソフトウェア等の導入状況
(イ) 不正プログラム対策ソフトウェア等の定義ファイルの更新状況
61. 受注者は、情報システムにおいて、標的型攻撃による組織内部への侵入を低減する対策（入口対策）として以下を例とする対策を行うこと。
(ア) サーバ装置について、組織内部への侵入を低減するため、以下の対策を行うこと。
① 不要なサービス機能やアプリケーションを削除又は停止する。
② 不審なプログラムが実行されないよう設定する。
③ パーソナルファイアウォール等を用いて、サーバ装置に入力される通信及び出力される通信を必要最小限に制限する。
④ サービスは原則「標準ユーザ」の権限で実行する。
(イ) USB メモリ等の外部電磁的記録媒体を利用した組織内部への侵入を低減するため、

以下の対策を行うこと。

① 出所不明の外部電磁的記録媒体を組織内ネットワーク上の端末に接続させない。接続する外部電磁的記録媒体を事前に特定する。

② 外部電磁的記録媒体をサーバ装置に接続する際、不正プログラム対策ソフトウェアを用いて検査する。

③ サーバ装置について、自動再生（オートラン）機能や自動実行機能を無効化する。

④ サーバ装置について、使用を想定しないUSBポートを無効化する。

⑤ 組織内ネットワーク上の端末に対する外部電磁的記録媒体の接続を制御及び管理するための製品やサービスを導入する。

62. 受注者は、情報システムにおいて、内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる及び外部との不正通信を検知して対処する対策（内部対策及び出口対策）として以下の対策を行うこと。

(ア) 情報窃取や破壊等の攻撃対象となる蓋然性が高いと想定される認証サーバやファイルサーバ等の重要なサーバについて、以下の対策を行うこと。

① 認証サーバについては、利用者端末から管理者権限を狙う攻撃（辞書攻撃、ブルートフォース攻撃等）を受けることを想定した対策を講ずる。

(イ) 以下の内部対策及び出口対策を行う。

① プロキシサーバ等により、C&Cサーバ等への不正な通信を監視し、遮断する。

別紙－３

令和８年度人流データ可視化システム運用保守業務

調達データ要件書

1　要件

（1）　次の各号を満たす人流データであること。

①　人流データは以下のエリア・範囲・分析データ対象期間・データ保持期間・月間アクティブユーザー数とする。

ア）エリア；別途指示

（現時点では案件ごとにタイプ A:東京 23 区都心エリア等、タイプ B:首都圏住宅地エリア&中京圏・関西圏・福岡圏中心～一部周辺エリア/タイプ C:首都圏郊外部・政令市中核市中心エリア等/タイプ D:人口 10 万人規模地方都市等/タイプ E:その他を想定）

イ）分析範囲　　；別途指示（現時点では半径１～10km 程度を想定）

ウ）分析データ対象期間　；別途指示（現時点では１～６か月間程度を想定）

エ）データ保持期間(※1）；別途指示（現時点では６～24 か月間程度を想定）

オ）アクティブユーザー数；別途協議（現時点では案件ごとにタイプ A：50 万 MAU/タイプ B:25 万 MAU/タイプ C:12 万 MAU/タイプ D:5 万 MAU/タイプ E:1 万 MAU から選択することを想定）

（※1）データ保持期間とは、Google Cloud BigQuery に登録された人流データを発注者が分析利用できる期間をいう。保持期間満了後、受注者は当該人流データを本システム及び関連する保存領域から削除するものとする。なお、当該人流データを利用して保持期間満了前に作成された統計資料、分析結果、報告書その他の成果物については、保持期間満了後も発注者は継続して利用できるものとする。

②　スマートフォンアプリから取得した GPS データであること。

③　位置情報の取得時に利用者承諾済かつ個人情報を含まないデータであること。

④　スマートフォンアプリのユーザーを一意に識別する ID が付与されていること。（ID にランダマイズ処理を施すなど、意図的に ID を変えていないこと）

⑤　人流データは別添仕様を満たすデータであること。

⑥　下記すべての項目が記載されたデータが、全体のデータ数の７割以上あること。

１.年代（10 代、20 代、30 代、40 代、50 代、60 代、70 代以上）

２.性別（男性、女性）

３.居住地

４.勤務地

５.交通手段

⑦　使用する人流データの月間アクティブユーザー数が 1000 万 MAU 以上であること。

（2）　データ取得方法およびデータに付与する属性（年代、性別、居住地、勤務地、拡大推計係数）の判定方法について、説明用資料を提出すること。

2　納品方法

（１）　１（１）①に定める人流データの要件については、独立行政法人都市再生機構（以下「発注者」という。）がその都度、内容及び履行期限等を記載した発注者所定の注文書（以下「注文書」という。）に定め、受注者に対して発行する。受注者はこの注文書に基づき、要件を満たす人流データを調達すること。

（２）　調達した人流データについて、発注者が管理する Google Cloud BigQuery に登録すること。登録方法は、発注者と都度協議のうえ決定すること。なお、受注者は登録後にデータの欠損又は形式不整合等がないことを確認し、本システムにおいて分析可能な状態で納品すること。なお、受注者は登録後にデータの欠損又は形式不整合等がないことを確認し、本システムにおいて分析可能な状態で納品すること。

（３）　納品時に、データ対象地点、データ期間を記入した納品書を添付すること。

（４）　データ登録に要する費用は、受注者が負担すること。

（５）　納品後、データの不良又は位置又は期間の相違があった場合は、速やかに正しいデータを納品すること。

（６）　人流データの調達業務は、要件を満たすデータがシステムへ登録され、本システム上で検索及び分析可能な状態となり、発注者の検査に合格した時点で完了とする。

３　特記事項

（１）　受注者は、天災その他の不可抗力により、注文書に指定された履行期限（以下「履行期限」という。）内に、当該注文書に基づく業務を完了することができないときは、あらかじめ、発注者に届け出て、履行期限を延長することができる。ただし、その延長日数は、発注者と受注者とが協議して定めるものとする。

（２）　本要件書に記載なき事項、又は契約履行上疑義を生じた事項については、当機構担当者と協議の上決定する。

以　上

別添

人流データ調達仕様

1．位置情報ログ

No	物理名	論理名	抽出条件	特記事項
1	gps_log	位置情報ログ	・指定した緯度経度を中心とした半径による範囲抽出 ・上記範囲に来訪したユーザーの同日の行動ログを、上記抽出範囲を半径 50km 拡大して抽出したもの ・抽出期間は原則月単位での指定	

No	物理項目名	論理項目名	型	モード	桁数	説明	フォーマット
1	id	ユーザーID	STRING	REQUIRED	—	個人が特定されないようユーザーIDをハッシュ化したもの	
2	jst_date_time	ログ記録日時	DATETIME	REQUIRED	—	JST での日時. 秒単位.	yyyy-mm-dd hh:mm:ss
3	latitude	緯度	FLOAT64	REQUIRED	—	世界測地系	
4	longitude	経度	FLOAT64	REQUIRED	—	世界測地系	
5	horizontal_accuracy	水平精度	FLOAT64	REQUIRED	—	緯度経度の水平精度（単位：m）. null はゼロ埋めすること	

2．年代

No	物理名	論理名	抽出条件	特記事項
2	user_profile_age	年代	位置情報ログで抽出したユーザーの年代	

No	物理項目名	論理項目名	型	モード	桁数	説明	フォーマット
1	id	ユーザーID	STRING	REQUIRED	—	個人が特定されないようユーザーIDをハッシュ化したもの	
2	age	年代	INT64	REQUIRED	2		10、20、30、40、50、60、70

3．性別

No	物理名	論理名	抽出条件	特記事項
3	user_profile_gender	性別	位置情報ログで抽出したユーザーの性別	

No	物理項目名	論理項目名	型	モード	桁数	説明	フォーマット
1	id	ユーザーID	STRING	REQUIRED	—	個人が特定されないようユーザーIDをハッシュ化したもの	
2	gender	性別	STRING	REQUIRED	1		F、M

4．居住地

No	物理名	論理名	抽出条件	特記事項
4	user_profile_home	居住地	位置情報ログで抽出したユーザーの居住地	

No	物理項目名	論理項目名	型	モード	桁数	説明	フォーマット
1	id	ユーザーID	STRING	REQUIRED	—	個人が特定されないようユーザーIDをハッシュ化したもの	
2	latitude	緯度	FLOAT64	REQUIRED	—	世界測地系. 個人が特定されないよう小数点以下4桁に丸めたもの	
3	longitude	経度	FLOAT64	REQUIRED	—	世界測地系. 個人が特定されないよう小数点以下4桁に丸めたもの	
4	region_id	全国地方公共団体コード	STRING	REQUIRED	—	都道府県コード - 市区町村コード - 町丁目コード	01-101-00202
5	prefecture	都道府県	STRING	REQUIRED	—		北海道
6	city	市区町村	STRING	REQUIRED	—		札幌市中央区
7	oaza	町丁目	STRING	NULLABLE	—		南一条西８丁目

5．勤務地

No	物理名	論理名	抽出条件	特記事項
5	user_profile_office	勤務地	位置情報ログで抽出したユーザーの勤務地	

No	物理項目名	論理項目名	型	モード	桁数	説明	フォーマット
1	id	ユーザーID	STRING	REQUIRED	—	個人が特定されないようユーザーIDをハッシュ化したもの	
2	latitude	緯度	FLOAT64	REQUIRED	—	世界測地系. 個人が特定されないよう小数点以下4桁に丸めたもの	
3	longitude	経度	FLOAT64	REQUIRED	—	世界測地系. 個人が特定されないよう小数点以下4桁に丸めたもの	
4	region_id	全国地方公共団体コード	STRING	REQUIRED	—	都道府県コード - 市区町村コード - 町丁目コード	01-101-00202
5	prefecture	都道府県	STRING	REQUIRED	—		北海道
6	city	市区町村	STRING	REQUIRED	—		札幌市中央区
7	oaza	町丁目	STRING	NULLABLE	—		南一条西８丁目

6．拡大推計係数

No	物理名	論理名	抽出条件	特記事項
6	magnification_factor	実人数推計拡大係数	位置情報ログの抽出範囲において、ユーザー数を実人数換算するための拡大係数	

No	物理項目名	論理項目名	型	モード	桁数	説明	フォーマット
1	mag_factor_area	地区全体での実人数推計拡大係数	FLOAT64	REQUIRED	—	位置情報ログの抽出範囲において、ユーザー数を実人数換算するための拡大係数（n.nnn...倍）	
2	mag_factor_road	地区内道路通行者の実人数推計拡大係数	FLOAT64	REQUIRED	—	位置情報ログの抽出範囲内の道路において、道路通過ユーザー数を実人数換算するための拡大係数（n.nnn...倍）	

以上

別紙－４

令和８年度人流データ可視化システム運用保守業務

受注者等が生成 AI を利用する場合における取扱いについて

本別紙は、仕様書の一部を構成するものであり、本業務において受注者等が生成 AI を利用する場合の条件及び手続を定めるものである。受注者等は、本業務において生成 AI を利用する場合には、本契約及び仕様書に従い、生成 AI 及び生成物を適正に取り扱わなければならない。

1　目的及び適用

(1) 本別紙は、生成 AI の適切な活用により本業務の効率化及び品質向上を図るとともに、情報漏えい、不正確な出力、第三者の権利侵害その他のリスクを適切に管理することを目的とする。

(2) 本別紙は、受注者（請負者、受託者その他名称を問わず本業務を実施する者をいう。）又は当該受注者から本業務の全部若しくは一部について再委託若しくは下請負を受けた者（これらの者からさらに再委託又は下請負を受けた者を含み、これらを総称して「再委託先等」という。）（以下、「受注者等」という。）が、本業務の遂行手段として自ら契約し、又は管理する生成 AI を利用する場合に適用する。

(3) 本業務において受注者等のいずれも生成 AI を利用しない場合、本別紙別添「生成 AI の取扱いに関する確認書兼誓約書」（以下、「確認書兼誓約書」という。）の発注者への提出は要しない。

2　用語の定義

(1) 「生成 AI」とは、人工知能に関する技術を用いて、利用者による情報の入力又はアップロード（以下、「入力等」という。）に応じ、文章、画像その他の情報を生成する機能を有するシステム、プログラム又はクラウドサービスをいう。

(2) 「生成物」とは、受注者等が生成 AI を利用して得た文章、画像その他の情報をいう。

(3) 「個人情報等」とは、個人情報の保護に関する法律（平成 15 年法律第 57 号）に規定する個人情報及び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）に規定する個人番号を含む情報をいう。

(4) 「氏名等」とは、発注者の職員及び受注者等の氏名、役職、所属及び業務用連絡先のうち、本業務の遂行に必要なものをいう。

(5) 「同意取得個人情報」とは、発注者又は受注者等が、本人に対し、本業務において生成 AI に入力等すること、その利用目的及び入力等する個人情報の項目をあらかじめ明示し、本人の同意を得た個人情報をいう。ただし、要配慮個人情報及び個人番号を含む情報を除く。

3　生成 AI を利用するための条件及び手続

(1) 受注者等は、本業務の遂行のために生成 AI を利用することができる。ただし、「４　入力等条件」の全てを満たし、「５　利用する生成 AI の安全要件」（以

下、「安全要件」という。）の全てに適合する場合に限る。なお、再委託先等に生成 AI を利用させない場合は、安全要件 No. 9 は適用しない。

(2) 受注者は、生成 AI の利用開始前に、あらかじめ確認書兼誓約書を発注者に提出しなければならないものとし、受注者等は、発注者から当該生成 AI の利用を開始して差し支えない旨の連絡を受けた後、利用を開始するものとする。なお、受注者による確認書兼誓約書の提出及び発注者による当該連絡又は(4)に基づく発注者の確認若しくは措置は、発注者が生成 AI の安全性又は適合性を保証するものではなく、受注者等の本契約及び本別紙に基づく義務及び責任を免除又は軽減するものではない。

(3) 受注者等が複数の生成 AI サービス又は契約プランを利用する場合、受注者は、それぞれについて安全要件への適合を確認し、生成 AI サービス又は契約プランごとに確認書兼誓約書を作成し、発注者に提出しなければならない。

(4) 発注者は、確認書兼誓約書の記載内容を確認し、記載内容に不備がある場合又は受注者等による生成 AI の利用が本契約及び本別紙に適合しないと認める場合、受注者等に対し、確認書兼誓約書の修正、当該利用の停止その他必要な措置を求めることができる。

4　入力等条件

(1) 受注者等は、次に掲げる情報を生成 AI に入力等してはならない。

区分	生成 AI に入力等してはならない情報
ア	個人情報等（氏名等及び同意取得個人情報を除く。）
イ	第三者の秘密情報（受注者等が第三者に対して秘密保持義務を負う情報をいう。）
ウ	受注者等が利用する権限を有しない著作物その他第三者の権利の対象となる情報
エ	発注者が生成 AI への入力等を禁止した情報

(2) 氏名等は、議事録の作成その他本業務の遂行に必要な範囲で入力等することができる。

(3) 同意取得個人情報は、本人に明示した利用目的の達成に必要な範囲に限り、生成 AI に入力等することができる。この場合、受注者等は、入力等を行う前に、発注者又は受注者等が、本人に対し、本業務において生成 AI に入力等すること、その利用目的及び入力等する個人情報の項目をあらかじめ明示し、本人の同意を得ていることを確認しなければならない。

(4) 発注者は、本業務の内容、情報の性質その他の事情を踏まえ、生成 AI への入力等を禁止する情報を指定することができ、受注者等は、当該指定に従わなければならない。

(5) 受注者等は、入力等を行う情報を本業務の遂行に必要な範囲に限定するものとし、入力等可否に疑義がある場合は、当該情報を入力等する前に、あらかじめ発注者に確認するものとする。

5　利用する生成 AI の安全要件

受注者は、自らの責任において、利用規約、サービス仕様、利用環境、設定その他必要な事項を確認し、利用する生成 AI 及びその利用に係る管理体制が次の安全要件に適合することを確認しなければならない。ただし、再委託先等に生成 AI を利用させない場合は、No. 9 は適用しない。

No.	安全要件
1	入力等情報及び生成物が、生成 AI モデルの学習、再学習、追加学習、性能向上及びサービス改善に使用されないこと。
2	入力等情報及び生成物が、本業務の遂行に必要な範囲を超えてサービス提供者又は第三者に使用又は提供されないこと。
3	入力等情報及び生成物が、物理的又は論理的に他の利用者から分離して管理され、閲覧、取得又は使用されない環境であること。
4	入力等情報及び生成物が、通信時及び保存時の暗号化その他の技術的措置により、第三者による不正なアクセス、漏えい、改ざん又は滅失から適切に保護されること。
5	受注者等が組織として管理するアカウント（事業者向けの契約に基づくものに限り、個人の利用を前提とするプラン又は利用規約の内容を個別に確認することができないサービスに係るものを除く。）を使用し、利用者及びアクセス権限を本業務に必要な者及び範囲に限定するとともに、適切な認証管理が行われていること。受注者等は、生成 AI の利用者の一覧を作成し、本業務の期間中これを最新の状態に保持すること。
6	生成 AI サービス上における入力等情報及び生成物の保存の有無、保存場所及び保存期間が明確であり、保存されない設定又は本業務の遂行に必要な最小限の期間に限り保存され、当該期間の経過後若しくは本業務終了後に削除される設定若しくは運用となっていること。ただし、次に掲げる情報については削除を要しない。この場合、受注者等は、本業務における生成 AI の利用終了後、当該情報を本業務以外の目的で利用し、又は生成 AI による新たな処理に用いないこと。 （ア）受注者等又はサービス提供者が、法令遵守、セキュリティ確保その他これらに準ずる目的で保持する情報であって、受注者等が削除することができない情報 （イ）生成 AI サービスの機能若しくは仕様又は情報の管理単位により、本業務に係る情報を合理的に区分して削除することが困難な情報
7	サービス上の利用履歴等の記録により、サービス所定の保存期間内に利用状況を確認できること。

No.	安全要件
8	入力等情報及び生成物を本業務の遂行に必要な範囲でのみ取り扱い、本業務以外の目的で使用し、又は発注者の承諾なく第三者に提供しないために必要な管理が行われていること。
9	再委託先等に生成 AI を利用させる場合に、当該利用が本契約に反しないことを確認するとともに、当該再委託先等に本項の安全要件を遵守させるために必要な管理が行われていること。
10	事故、本項の安全要件への不適合又はこれらのおそれを把握した場合に、直ちに生成 AI の利用を停止し、速やかに発注者に報告するための体制が整備されていること。
11	利用規約、契約プラン、利用環境、設定等の変更を把握し、変更後の利用開始前に No. 1 から No. 10 の安全要件への適合を再確認するための管理が行われていること。

6　生成物の確認及び利用

(1) 受注者等は、生成物を本業務に係る判断、処理、成果物の作成、発注者への提出物の作成その他本業務の遂行に利用する場合、自らの責任において、その内容及び利用の適否を確認し、必要な修正を行わなければならない。

(2) 受注者等は、生成物のみに基づいて本業務に係る判断その他の業務遂行を行ってはならない。

(3) 受注者等は、生成物に虚偽若しくは誤り、第三者の著作権その他の権利を侵害する内容、偏見及び差別を含む内容又は本業務に不適切な内容が含まれていないことを確認しなければならない。

(4) 受注者等は、(1)から(3)までの確認の結果、生成物に修正を加えずに、成果物、発注者への提出物その他発注者に提示する資料等に使用する場合、生成 AI を利用して作成した旨を当該成果物等に明記しなければならない。

(5) (4)の明記は、受注者等の本業務に関する義務及び責任を免除又は軽減するものではない。

7　適合状態の維持、変更時の対応及び利用終了

(1) 受注者は、生成 AI の利用期間中、安全要件への適合状態を維持するとともに、再委託先等に維持させなければならない。ただし、再委託先等に生成 AI を利用させない場合は、安全要件 No. 9 は適用しない。

(2) 利用規約、契約プラン、利用環境、設定その他安全要件への適合に影響する事項に変更があった場合、受注者は、変更後の生成 AI 利用開始前に、安全要件への適合状態を再確認しなければならない。

(3) 受注者等は、(2)の再確認により、安全要件への適合を確認できない場合、当該生成 AI を利用してはならない。

(4) 受注者は、(2)の再確認の結果、確認書兼誓約書の「１　基本情報及び利用する生成 AI」の記載内容に変更が生じる場合、変更後の利用開始前に、変更後の確認書兼誓約書を発注者に再提出しなければならない。受注者等は、発注者から変更後の内容で当該生成 AI の利用を開始して差し支えない旨の連絡を受けた後に、利用を開始する。

(5) 生成 AI の利用を終了した場合、受注者等は、安全要件 No. 6 記載の運用に従い、生成 AI サービス上の入力等情報及び生成物を削除し、又は削除されることを確保しなければならない。なお、同 No. 6 に定める受注者等が削除を要しない情報については、削除対象に含まないが、受注者等は、本業務における生成 AI の利用終了後、当該情報を本業務以外の目的で利用し、又は生成 AI による新たな処理に用いてはならない。

(6) 受注者は、発注者から求めがあった場合、再委託先等による利用を含む生成 AI の利用状況、安全要件への適合状況及びこれらの確認方法を説明し、必要な資料を提示しなければならない。

8　事故、不適合等への対応

(1) 受注者は、事故、安全要件への不適合又はこれらのおそれを把握した場合、直ちに生成 AI の利用を停止し又は再委託先等に利用を停止させ、発生した事象、影響範囲及び講じた措置を速やかに発注者に報告しなければならない。

(2) 受注者は、発注者の求めに応じ、必要な調査、是正、影響拡大の防止、再発防止その他の対応を行わなければならない。

(3) 受注者は、発注者から求めがあった場合、安全要件への適合を確認した方法、事故等への対応状況を説明し、必要な資料を提示しなければならない。

9　再委託

(1) 受注者は、再委託先等に生成 AI を利用させる場合、当該利用が本契約及び本別紙に反しないことを確認した上で、当該再委託先等に本別紙及び確認書兼誓約書に定める受注者の義務と同等の義務を課し、これを遵守させなければならない。

(2) 再委託先等による生成 AI の利用及び生成物の取扱いについて、受注者は、自ら行った場合と同様に、本契約及び本別紙に基づく責任を負う。

(3) 受注者は、再委託先等が利用する生成 AI についても、その利用開始前に、当該再委託先等を明記した確認書兼誓約書を提出しなければならない。

10　成果物としての生成 AI システムとの関係

(1) 発注者が利用することを目的として、本業務の成果物として生成 AI システムを構築又は導入する場合であっても、受注者等が本業務の遂行手段として別の生成 AI を利用するときは、その利用に本別紙を適用する。

(2) 成果物として構築又は導入される生成 AI システムそのものの仕様、利用条件、検証及び導入後の運用管理については、仕様書その他発注者が定める条件による。

11　本別紙への違反等

受注者等が本別紙又は確認書兼誓約書に違反した場合、発注者は、生成 AI の利用停止、是正、再発防止策の提出その他必要な措置を求めることができる。この場合において、発注者は、本項に定める措置に加え、本契約に基づく解除、損害賠償請求その他の権利を行使することができる。

以　上

別紙５

作業の実施にあたっての遵守事項

1. 要保護情報を取り扱う作業実施前の対策

(1) 受注者は、要保護情報を取り扱う作業の実施までに、以下の内容を全て含む情報セキュリティ対策を整備すること。

一　受注者における情報の適正な取扱いのための情報セキュリティ対策の実施内容及び管理体制

二　以下の内容を含む、受注者において発生した情報セキュリティインシデントへの対処方法

イ　準備から事後処理に至る全般的なインシデント対処プロセス

ロ　当事者及び関係者の役割を含む体制

ハ　インシデント対処体制、責任者、作業担当者から当該体制への報告フロー等の概要

三　情報セキュリティ対策の履行状況の確認方法

四　情報セキュリティ対策の履行が不十分な場合の対処方法

五　機構との情報の受渡し方法や作業終了時の情報の廃棄方法等を含む情報の取扱手順

2. 要保護情報を取り扱う作業実施期間中の対策

(1) 受注者は、作業の実施期間を通じて、以下を全て含む対策を遵守すること。

一　受注者に提供する情報の受注者における目的外利用の禁止

二　機構と合意した情報の取扱手順による情報の取扱い

三　作業において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、作業の一時中断などの必要な措置を含む対処及び報告手順に従った遅滞のない機構への報告

(2) 受注者は、情報セキュリティ監査について、以下を全て含む内容を実施すること。

一　作業の遂行にあたり、機構から指示があった場合には、機構の情報セキュリティ監査を受入れること

二　情報セキュリティ監査の結果、機構が改善を求めた場合には、機構と協議の上、必要な改善策を立案して速やかに実施すること

三　機構が外部からの監査を受けるにあたり、機構から指示があった場合には、監査の対応に関して協力すること

(3) 受注者は、作業の実施期間を通じて、作業における情報の適正な取扱いを担保するため、以下の内容を全て含む情報セキュリティ対策を実施すること。

一　作業の実施期間中に情報セキュリティインシデントの検出有無等について定期的な報告を行うこと

二　作業に関して機構が提供する要保護情報を取り扱う受注者内の情報システムにアクセスする主体を特定するため、情報へアクセスする主体の識別とアクセスの制御に関する以下の対策を実施すること

イ　管理者権限を持つアカウントは必要最低限の権限と利用に制限した上で、ログを取得すること

ロ　システムにアクセスした主体が一意で特定されていること

ハ　情報システムに管理者権限でアクセスする場合、多要素主体認証を採用すること

ニ　リモートアクセスを実施する際は、通信経路の暗号化やその通信の監視等の対策を行うこと

ホ　無線 LAN を利用する際は、通信路の暗号化や無線 LAN へのアクセス主体の認証等の対策を行うこと

ヘ　「パスワード長を 10 文字以上とするとともに、アルファベットの大文字、小文字、数字及び記号を組み合わせる」と同等以上のパスワードポリシーを設けること

三　作業に関して機構が提供する要保護情報を取り扱う受注者内の情報システムへの不正アクセスを検知・抑止するためのログを取得・監視し、要保護情報にアクセスする全てのシステム利用者についてシステム操作履歴を取得するため、ログの取得・監視に関する以下の対策を実施すること

イ　ログの取得対象は定期的に見直しを実施し、必要に応じて対象の変更を実施すること

ロ　ログの取得プロセスにおいて、取得失敗時はエラーが出力され、取得失敗を検知できるようになっていること

ハ　取得したログ情報やその分析内容に応じて、不正アクセスや異常操作への対応が取れるようプロセス設計を行うこと

ニ　ログの分析機能やレポート作成機能を有していること

ホ　取得したログ情報及びログ取得機能について改変・削除から保護し、ログ取得機能の管理者権限付与を最低限の対象に限定すること

四　作業に関して機構が提供する要保護情報を格納する機器等（記録媒体、紙媒体を含む）の使用や保管に係る対策を実施するため、情報を取り扱う機器等の物理的保護に関する以下を例とする対策を実施すること

イ　情報又は機器等へのアクセスを許可されている要員だけに認めること

ロ　機器等を廃棄又は再利用する際は、事前にデータを抹消又は破壊すること。なお、クラウドサービスを利用する場合は、当該サービスにおいてデータの削除又は利用停止時の情報保護措置が講じられていることを確認すること。

ハ　外部電磁的記録媒体を使用する場合は、運送時における安全な取扱い、無許可利用の防止その他必要な対策を行うこと。なお、クラウドストレージその他のオンラインサービスを利用する場合は、アクセス制御及び通信の暗号化等の対策を実施すること。

ニ　作業の実施場所又は情報を取り扱う環境について、不正アクセス又は不適切な利用を防止するための管理措置を講じること。なお、クラウドサービスを利用する場合は、アクセス権管理、多要素認証その他同等以上の管理措置を実施すること。

ホ　機構の要保護情報をテレワーク時に取り扱う場合、テレワーク実施時の情報セキュリティ対策に関するルールを設け、機器等に技術的な情報セキュリティ対策を実施すること

五　作業に従事する受注者の従業員等及び機構が提供する要保護情報を取り扱う受注者内の情報システムにアクセスを許可する受注者の従業員等に、遵守すべき情報セキュリティ対策に関する事項を確実に認識させるため、情報を取り扱う要員への周知と統制に関する以下の対策を実施すること

イ　情報セキュリティに係る教育・訓練等を確実に受講させること

ロ　従業員等の異動・退職等の際にアクセス権の削除や秘密保持の徹底等を求めること

六　作業に関して機構が提供する要保護情報を取り扱う受注者内の情報システムに用いる機器等の適切な構成管理を実施するとともに、当該情報システムの運用に伴うリスクを継続的に評価するため、セキュ

リティ脅威に対処するための資産管理・リスク評価に関する以下の対策を実施すること

イ　情報システムの構成管理に必要な設定変更の作業履歴を残すこと

ロ　インターネット等の外部ネットワークから管理者画面にアクセスするときに多要素主体認証を実施すること

ハ　定期的及び重大な脆弱性の公表時に脆弱性スキャンを実施し、適時な脆弱性対策を行うこと

七　作業に関して機構が提供する要保護情報を取り扱う受注者内の情報システムが接続するネットワークの外部境界及び主要な内部境界において、通信又は送受信データを監視し、制御し、保護するため、受注者内の情報システムの完全性の保護に関する以下の対策を実施すること

イ　情報システムの改ざんや欠陥を適時に検出し是正すること

ロ　マルウェア等の混入に対する保護措置を講じること

ハ　脆弱性に係る注意喚起の情報を収集し、対処を行うこと

ニ　CRYPTREC 暗号リストに記載されたアルゴリズム及び鍵長による暗号化及び電子署名機能を実装し、暗号鍵を適切に管理すること

ホ　業務に必要な通信だけを許可し、許可していない不正な通信の発生を防止すること

ヘ　不正利用防止のための職務分掌を徹底すること

八　受注者が実施する情報セキュリティ対策の検証・評価・見直しのための以下の対策を実施すること

イ　受注者内の情報システムの欠陥の是正及び脆弱性対策について、対策計画を策定し実施すること

ロ　受注者内の情報システムの欠陥の是正及び脆弱性対策等の情報セキュリティ対策が有効に機能していることの継続的な監視と確認を行うこと

ハ　受注者が実施する情報セキュリティ対策の文書化と定期的な見直しを行うこと

3. 作業終了時の対策

(1) 受注者は、契約に基づき、作業の終了に際して以下を全て含む対策を実施すること。

一　作業の実施期間を通じてセキュリティ対策が適切に実施されたことの報告

二　提供を受けた情報を含め、作業において取り扱った情報の返却、廃棄又は抹消

4. 情報セキュリティポリシーの遵守

(1) 受注者は、政府機関統一基準等関連ガイドラインを理解した上で、次の機構の定めるセキュリティ関連規程を遵守し、システムの構成や特性に応じ情報の機密性・完全性・可用性を各々適切に確保し取組を行うものとすること。また、契約締結時に規程等が改正されている場合は、改正後の規程等を遵守すること。

【機構の定めるセキュリティ関連規程】

一　独立行政法人都市再生機構情報化等管理規程（平成 20 年規程第 21 号）

二　独立行政法人都市再生機構情報化等管理に関する達（平成 20 年達第 21 号）

三　独立行政法人都市再生機構情報セキュリティ管理に関する規程（令和 5 年規程第 27 号）

四　独立行政法人都市再生機構情報セキュリティ管理に関する達（令和 5 年達第 24 号）

【政府機関統一基準等関連ガイドライン】

一　政府情報システムの整備及び管理に関する標準ガイドライン（平成 26 年 12 月 3 日各府省情報化統括責任者(CIO)連絡会議決定）

二　政府機関等のサイバーセキュリティ対策のための統一基準群（令和 5 年度版）（令和 5 年 7 月 4 日、サイバーセキュリティ戦略本部・内閣サイバーセキュリティセンター）

イ　政府機関等のサイバーセキュリティ対策のための統一規範

ロ　政府機関等のサイバーセキュリティ対策のための統一基準（令和 5 年度版）

ハ　政府機関等の対策基準策定のためのガイドライン（令和 5 年度版）

三　「高度サイバー攻撃対処のためのリスク評価等のガイドライン」（内閣サイバーセキュリティセンター）

イ　『高度標的型攻撃』対策に向けたシステム設計ガイド（独立行政法人情報処理推進機構）

ロ　『新しいタイプの攻撃』の対策に向けた設計・運用ガイド（独立行政法人情報処理推進機構）

ハ　『標的型メール攻撃』対策に向けたシステム設計ガイド（独立行政法人情報処理推進機構）

四　「クラウドセキュリティガイドライン活用ガイドブック（2013 年度版）」（経済産業省）

五　「クラウドサービスの安全・信頼性に係る情報開示指針（総務省）」

イ　「クラウドサービス提供における情報セキュリティ対策ガイドライン（第 3 版）（令和 3 年 9 月改定）」

ロ　「ASP・SaaS 事業者連携ガイド（平成 24 年 7 月策定）」

ハ　「データセンターの安全・信頼性に係る情報開示指針（平成 29 年 3 月改定）」

ニ　「IaaS・PaaS の安全・信頼性に係る情報開示指針（第 2 版）（平成 29 年 3 月改定）」

ホ　「ASP・SaaS の安全・信頼性に係る情報開示指針（ASP・SaaS 編）第 3 版（令和 4 年 10 月改定）」

六　「安全なウェブサイトの作り方　改訂第 7 版（令和 3 年 3 月）」（独立行政法人情報処理推進機構）

イ　付属：「セキュリティ実装 チェックリスト」

ロ　別冊：「安全な SQL の呼び出し方（平成 22 年 3 月 18 日公開）」

ハ　別冊：「ウェブ健康診断仕様（平成 24 年 12 月 26 日公開）」

七　「ISO／IEC 15408(CC) IT セキュリティ評価及び認証制度(JISEC）」（独立行政法人情報処理推進機構）

八　「サイバーセキュリティ経済基盤構築事業クラウドセキュリティ監査制度の見直し（平成 27 年 2 月）」（経済産業省）

九　「政府情報システムのためのセキュリティ評価制度（ISMAP）」（令和 2 年 1 月 30 日サイバーセキュリティ戦略本部決定）

5. 再委託に関する対策

(1) 受注者は、その役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、「1. 要保護情報を取り扱う作業実施前の対策」及び「2. 要保護情報を取り扱う作業実施期間中の対策」の措置を再委託先に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を機構に提供し、機構の承認を受けること。