令和５年度南区デマンド交通実証実験支援業務仕様書

１　業務の名称

令和５年度南区デマンド交通実証実験支援業務

２　業務期間

⑴　契約期間

契約締結日から令和６年３月 31 日（日）まで

⑵　予約受付期間

令和５年８月 25 日（金）から令和６年３月 31 日（日）まで（予定)。

⑶　デマンド交通運行期間

令和５年９月１日（金）から令和６年３月 31 日（日）まで（予定)。

３　実証実験の概要

⑴　役割分担

①　運行事業者

ア　事業者名

株式会社じょうてつ

イ　事業者所在地

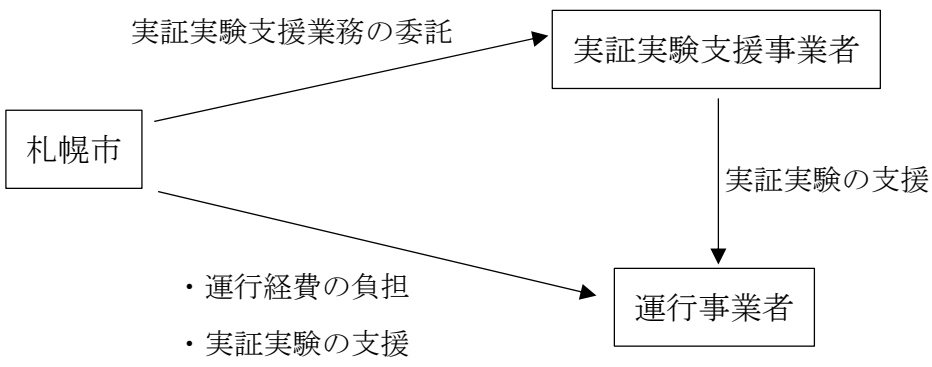
札幌市白石区東札幌１条１丁目１－８

ウ　運行事業者の業務

車両の管理、運行の管理及び運賃の管理とする。

②　本市、運行事業者及び本業務の受託者の関係

下図のとおり。



⑵　運行計画

①　運行日時

２-⑶の期間内における月曜日から金曜日とし、１日あたり７時間運行する。運行時間は９時から 16 時までを想定している。ただし、令和５年 12 月 29 日から令和６年１月３日まで及び国民の祝日に関する法律に規定する祝日は運休とする（運行予定日数 139 日）。

②　実施箇所

別紙地図のとおり。乗降場所については、40 箇所を予定している。

③　運賃

一般運賃	350 円	中学生以上
福祉割引運賃	180 円	身体障がい者手帳・療育手帳・施設長の発行する割引証明書の所持者と介護者
こども運賃	150 円	６歳～12 歳未満（小学生）
乳幼児運賃	無料	６歳未満（小学校入学前）

④　運行車両

運行事業者が所有するジャンボタクシー型車両１台（乗客定員６名を想定）

⑤　利用者

事前会員登録者

４　業務内容

⑴　会員登録及び乗車予約の受付・管理

①　会員登録受付体制

インターネット及び書面での会員登録に対応可能なシステム及び受付体制を構築し、令和６年３月 31 日までの間は随時受付すること。

②　予約受付体制

インターネット及び電話での利用予約に対応可能な予約システム及び電話受付体制を構築すること。

③　予約受付時間

電話での予約は運行日のみ受付することとし、３-⑵-①にて示した運行開始時

刻の１時間前から運行終了時刻までとする。インターネットでの予約は原則として毎日 24 時間受け付けるものとする。

なお、予約可能時間は利用予定日の１週間前から利用予定時間の 30 分前までを想定している。

④　運行事業者への伝達

利用予約情報については、予約受付完了後、速やかに車載端末を通じて運行事業者へ伝達すること。

なお、車載端末は予備端末１台を含めた合計２台を受託者が用意し運行事業者に無償貸与することとし、通信に係る費用も受託者の負担とする。

⑤　電話予約受付

ア　１日当たりの電話予約者数を 50 人程度と想定し、予約の受付時間は常に電話の受付ができる体制を維持すること。

イ　交通事情などにより、送迎時間に大幅な遅延が見込まれる旨の連絡を運転者から受けた場合、すみやかに予約者へ電話連絡をするなど適切な対応を行うこと。

ウ　予約人数が乗車定員に達するなどして、予約が受け付けられない場合は、その理由を丁寧に説明し、別便の利用などを案内すること。

⑵　プロジェクトマネジメント業務

①　実証実験の実施に係る進捗管理

契約後、実証実験実施までの準備から実施後の結果報告に至るまでの間、本市及び運行事業者と随時打合せを行い、事業進捗に係る相談・支援を行うこと。

②　地域公共交通会議開催及び地域合意形成に向けた支援

地域公共交通会議の開催のほか、実証実験について地域住民や地元交通事業者、関係各所（地方運輸局等）への説明・協議を実施するにあたり、資料の準備や説明事項の整理に関し、相談・支援を行うこと。

③　住民説明会に向けた支援

運行事業者が主催する住民説明会（運行区域周辺にて３回程度開催を想定）に同席するほか、実施に向けた企画の立案や、資料の準備、説明事項の整理等に関し、相談・支援を行うこと。

④　パンフレットの作成

パンフレットは乗降場所の地図を含めたものを作成し、１部あたり A4 用紙１枚以上の両面カラー印刷とする。作成にあたっては、3,000 部の印刷も行うこと。な

お、詳細な部数については、契約の際に別途本市と協議の上、決定する。

⑤　利用者アンケートの実施・分析

利用者を 500 人と想定し、利用者全員に対するアンケート項目の検討・選定を行った上でアンケート調査を１回実施し、結果を分析すること。

⑥　データ分析業務

実証実験により取得したデータや利用者アンケートの結果を分析・検証し、本市及び運行事業者へ提供すること。また、運行改善に向けた検討を行うこと。

⑦　乗降場所目印設置業務

乗降場所を示す目印を作成、設置すること。設置方法は既存バス停やゴミステーション、公共施設等への貼付けを想定しており、内訳は下表のとおり。設置に当たっては、積雪地であっても識別可能な設置場所、方法とすること。

既存バス停への設置	20 箇所程度
ゴミステーションへの設置	10 箇所程度
公共施設、民間施設等への設置	10 箇所程度

※設置場所及びその内訳は、今後の地域協議等で変更する可能性がある。

⑧　利用者向け広報誌の作成

利用促進や利便性向上に向けた取り組みとして、運行に係る情報や地域のイベント情報等を掲載した広報誌を作成し、利用者全員へ送付すること。なお、広報誌の作成・送付は期間中２回を想定している。

⑶　予約システムの構築

①　システム設計・打合せ

ア　本市及び運行事業者と綿密な打ち合わせを行い、使用者に配慮した設計とすること。

イ　本市情報セキュリティポリシーに則った設計とすること。

ウ　個人情報を保護できるシステムとすること。

エ　業務の進行管理を遺漏のないよう行うこと。

②　構築業務

デマンド交通に係る本書に示す要求水準に沿ったシステムを構築し、各調整、マスタ設定等を行うこと。

③　利用方法の説明・指導業務

ア　本市担当者への説明・指導業務

イ　運行事業者への説明・指導業務

ウ　住民説明会における説明・指導に係る相談・支援業務

④　保守・運用業務

ア　平日８時 45 分から 17 時 15 分までは、本市及び運行事業者からの電話及び電子メール等による問い合わせの受付を行うこと。ただし、緊急時においてはこの限りではない。

イ　システムの障害が発生した場合は、速やかに復旧の措置を講じること。また、障害の原因や対応状況について、復旧までの間、本市及び運行事業者に随時報告すること。

4　予約システム概要

⑴　利用者からの予約に対し、効率的な運行ルートを即時に作成するデマンド型乗合予約システムであり、クラウド型システムにて構築されていること。

⑵　オペレーターによる電話予約とインターネット予約の運用を前提とすること。

⑶　システムに蓄積されたデータにより、利用者層・時間帯の把握、乗合率などのデータが確認でき、更なる利用促進に向けた運行方法の改善検討等に活用できるシステムとすること。

⑷　本市情報セキュリティポリシーに則った設計とすること。

⑸　個人情報を保護できるシステムとすること。

5　システムに関わる要件

⑴　予約・配車・運行管理にかかわる基本機能

①　電話での予約を受け付ける際は、オペレーターによる管理者 WEB への手動登録ができること。

②　予約締切時間を任意に指定することができること。

③　運行範囲の設定が可能であること。

④　複数台の予約端末から、同時に予約等ができるシステムとすること。

⑤　予定乗降場所数を登録、運用できるシステムとすること。

⑵　ユーザーアプリ

①　予約の確定及び予約状況の確認、そのキャンセル、乗降場所の案内ができること。

②　乗車人数、乗車希望時間、乗降場所を任意に指定することができること。

⑶　ドライバーアプリ

① 利用者の属性により、運転者が車載端末で乗車する利用者の運賃を確認する機能があり、かつシステムで運賃を管理できるシステムとすること。

② 運転者側で運賃の変更操作ができること。

③ 運転者へテキストによるメッセージが伝達できること。

④ 運行事業者が予約の状況と車両の位置が確認できるシステムとすること。

⑷ 運行管理機能

① 管理者 WEB にて運行車両の予約状況を把握できること

② 管理者 WEB にて利用者情報を登録、修正、削除できること。また、情報をリスト表示できること。

③ 管理者 WEB にて利用者の予約状況を把握できること。また、予約情報を登録、修正、削除できること。

④ 管理者 WEB にて運行により取得する乗降データを出力できること。

⑤ 異常発生時に管理者 WEB にて新規の予約受付停止ができること。

⑥ 利用実績（日別・時間帯別、乗降場所別等）を随時確認できること。

⑦ 過去の運行記録について確認できること。

6 個人情報の保護について

⑴ 「個人情報の保護に関する法律」及び別紙「個人情報の取扱いに関する特記事項」を遵守して業務を行うこと。

⑵ 毎月、個人情報取扱状況報告書を作成し、本市に報告すること。

7 情報資産の取り扱いについて

⑴ 別紙「札幌市情報セキュリティポリシー」を遵守して業務を行うこと。

⑵ 情報セキュリティ対策

① 受託者は、下記のような情報セキュリティに対する脅威から情報資産を保護するための対策を講ずるものとする。

ア 故意の不正アクセス又は不正操作による機器又は情報資産の破壊、盗難、改ざん、消去等

イ リモート接続及びその端末の使用による情報資産の破壊、盗難、改ざん、消去等

ウ 誤操作等によって起きる情報資産の破壊、漏洩、消去等及び搬送中の事故等による情報資産の盗難、漏洩等

エ 地震、落雷、火災、水害、停電等の災害又は事故による情報資産の破壊、消

失、業務の停止等

② 情報資産を取り扱う際は、多要素認証を備えること。

③ 暗号化の機能を備えること。

⑶ 体制の整備

① 本業務の作業実施体制・連絡体制を提示すること。

② セキュリティ対策の責任者にはセキュリティ対策を十分に管理できる者を配置すること。

③ 情報を取り扱うことができる職員を指定すること。

⑷ 情報資産の目的外使用の禁止

受託者及び情報資産の取扱者は情報資産を業務上の利用目的以外で使用してはならない。

⑸ 情報資産の複写及び複製について

受託者が、業務の履行にあたり本市の情報資産を複写及び複製する必要がある場合は、本市の許可を得なければならない。

⑹ 秘密保持

① 本業務の遂行に当たり知りえたすべての情報は、履行機関及び履行後において第三者に漏らしてはならない。データの取扱についても同様とする。

② 秘密保持及びデータの取扱について、従業員その他関係者への徹底を行うこと。

⑺ 運用・保守・点検における情報セキュリティ対策の実施

運用に当たってはデータの消失を防ぐため、定期的にバックアップを行うこと。

⑻ 脆弱性対策の実施

① システムで使用するソフトウェア等の最新の脆弱性情報を把握しシステムへの影響を調査・評価すること。

② セキュリティパッチの提供がある場合はシステムへの影響を考慮し、影響がない場合は適用すること。

⑼ セキュリティの検証と妥当性確認

本業務に基づくシステム構築が影響する範囲について、脆弱性検査を実施し、その結果を書面にて報告すること。

⑽ 事故発生時の報告

① 情報セキュリティインシデントが発生した場合には、すみやかに本市に報告しなければならない。

② 短時間で被害が拡大する情報セキュリティインシデントについては緊急時対策を受託者が行うこと。

⑾　情報資産の保管及び移動

①　本市の情報資産を個人所有の記憶媒体に記録・保管してはならない。

②　原則として本市の情報資産を執務室外に持ち出してはならない。やむを得ず持ち出す場合は業務責任者の許可を得ることとする。また、インターネットメールによる情報資産の送信についても同様とする。

③　業務責任者の許可を得て本市の情報資産を執務室外に持ち出す場合には、搬送中の記憶媒体の盗難、破損及び情報流出等の被害を防止するために、必要な措置を講じなければならない。

⑿　製品のサポート期間への対応

システムで使用するソフトウェアについては、システム更改の時期を考慮し、メーカーによるサポート対象の製品、バージョンを用いること。

⒀　情報資産の管理に関する定期的な履行確認について

受託者は、定期的に情報資産のセキュリティ保全の報告を実施することとし、本市が行う情報資産の管理に関する履行確認に対して適切に応じ、確認事項についての説明を行うこと。

⒁　情報セキュリティ監査の実施

本市の要請等に基づき、サービス提供者のセキュリティ対策、運用体制等に関し、監査を行うことができる。

⒂　情報セキュリティ対策の履行が不十分であると思われる場合の対処

受託者の責に起因する情報セキュリティインシデントが発生するなどの万一の事故があった場合に直ちに報告する義務や、損害に対する賠償等の責任を負うこと。

⒃　責任

受託者及び本市の責任については、別途契約書にて定める。

⒄　本業務を第三者に再委託する場合の条件

①　本業務を合理的な理由及び必要性により再委託する場合には、セキュリティ対策が確認できる資料を提出し、本市の承認を受けること。

②　再委託先に対しては、本業務委託契約書の内容を周知徹底し、情報資産の破壊、盗難、改ざん、消去等を未然に防止するための措置を取ること。

③　受託者は、再委託先が行った本業務に関する行為について一切の責任を負うこと。

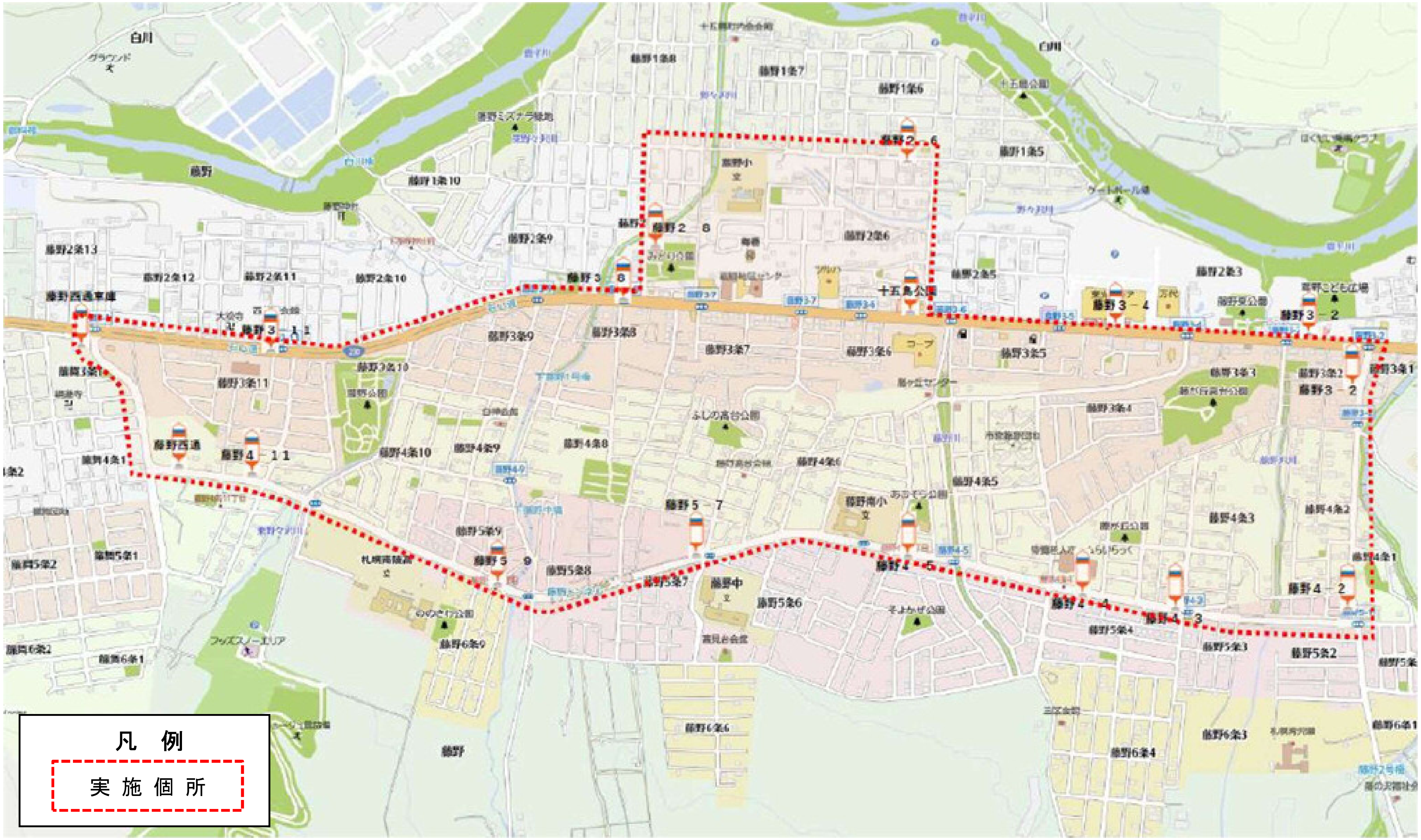
⒅　受託者は、業務の完了日または契約解除の日をもって、情報資産を本市に返還するとともに、その複製複写物を一切保持してはならない。ただし、本市が必要と認める場合は、その返還日を延期することができる。

⑲　サーバの設置国は日本国内とする。

８　協議

本仕様書に記載されていない事項または業務の遂行において疑義が生じた場合は、双方の協議により定めることとする。

別紙地図



藤野2－6
藤野2－8
藤野3－8
十五島公園
藤野3－4
藤野3－2
藤野西通車庫
藤野3－11
藤野西通
藤野4－11
藤野5－7
藤野5－9
藤野4－5
藤野4－4
藤野4－3
藤野4－2
凡　例
実施個所

取扱厳重注意

札幌市情報セキュリティポリシー

平成１６年６月３０日市長決裁

令和５年３月 17 日改正情報セキュリティ委員会承認

〈　目　　次　〉

序　札幌市情報セキュリティポリシーの構成

札幌市情報セキュリティポリシー（以下「ポリシー」という。）は、札幌市が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものである。

ポリシーは、札幌市が所掌する情報資産に携わる職員、委託事業者等にも浸透、普及、定着されるものであり、安定的な規範であることが要請される。また一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、ポリシーは一定の普遍性を備えた部分としての「情報セキュリティ基本方針」と情報資産を取巻く状況の変化に依存する部分「情報セキュリティ対策基準」の２層に分けて構成する。（下表参照）

札幌市情報セキュリティポリシーの構成

文　書　名		内　容
札幌市 情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すためのすべてのネットワーク及び情報システムに共通の情報セキュリティ対策の基準

第１章　情報セキュリティ基本方針

１　目的

本市は、ＩＣＴを活用した持続可能なまちづくりを推進しているところである。

本市の情報システムが取り扱う情報には、市民の個人情報のみならず行政運営上重要な情報など、外部への漏えい等が発生した場合には極めて重大な結果を招く情報が多数含まれていることから、取り扱う情報を様々な脅威から防御することは、市民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠なものである。

本市は、市民が安心・信頼して行政サービスを利用することができるようにするとともに、継続的かつ安定的な行政事務の執行を確保するために、情報資産の機密性、完全性及び可用性(注)を維持するための対策（情報セキュリティ対策）を整備するものである。

（注）：国際標準化機構（ＩＳＯ）が定めるもの(IS07498-2：1989)

機密性（confidentiality）：情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。

完全性（integrity）　：情報及び処理の方法の正確さ及び完全である状態を安全防御すること。

可用性（availability）　：許可された利用者が必要な時に情報にアクセスできることを確実にすること。

２　定義

⑴　情報セキュリティ

情報資産の機密の保持、正確性及び完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

⑵　ネットワーク

電子計算機等を相互に接続するための通信回線及びその構成機器（ハードウェア及びソフトウェア）をいう。

⑶　情報システム

電子計算機、ネットワーク、電磁的記憶媒体等により、情報処理を行う仕組みをいう。

⑷　情報資産

情報システムで取り扱うすべての電磁的データをいう。

⑸　住民基本台帳ネットワークシステム

電気通信回線を通じた送信又は磁気ディスクの送付の方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準（平成 14 年総務省告示第 334 号）第１の１に規定する住民基本台帳ネットワークシステムをいう。

⑹　マイナンバー利用事務系

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システムをいう。

⑺　校務系情報

児童生徒の成績、出欠席、健康診断結果及び指導要録、教員の個人情報等、学校が所有する情報

資産のうち、学校・学級の管理運営、学習指導、生徒指導及び生活指導等に活用することを想定しており、かつ、児童生徒がアクセスすることが想定されていないものをいう。

⑻　教育系情報

児童生徒のワークシート及び作品等、学校が所有する情報資産のうち、それら情報を学校における教育活動において活用することを想定しており、かつ当該情報に教員及び児童生徒がアクセスすることが想定されている情報をいう。

⑼　学校情報システム

校務系情報又は教育系情報を取り扱う札幌市情報通信ネットワークに接続していない情報システムをいう。

3　対象範囲

ポリシーは、本市のすべての執行機関（市長、教育委員会、選挙管理委員会、人事委員会、監査委員、農業委員会、固定資産評価審査委員会、公営企業管理者及び消防長）及び議会事務局を対象とする。ただし、学校情報システム及び当該システムで取り扱う情報資産については、対象から除く。

4　ポリシーの位置付け

ポリシーは、本市の情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ管理の最上位の位置付けとする。

5　職員の責務

本市の情報資産に接するすべての職員（特別職、会計年度任用職員、非常勤職員及び臨時職員を含む。以下同じ。）は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たってポリシーを遵守する義務を負うものとする。

また、情報資産を取り扱う委託事業者等に対しても、契約を通じて、又は別途取り決めを行うことにより、ポリシーを遵守させるための措置を講じなければならない。

6　情報セキュリティ管理体制

本市の情報資産について、情報セキュリティ対策を推進し、管理するための組織・体制を確立し、その役割、責任等を定める。

情報セキュリティインシデント対応及び外部との情報共有を役割とした統一的な体制「ＣＳＩＲＴ（シーサート）」を構築する。

7　情報資産の分類

情報資産をその内容に応じて分類し、その重要性に応じた情報セキュリティ対策を行うものとする。

8　情報セキュリティに対する脅威

情報セキュリティに対する脅威とは、情報セキュリティを脅かす好ましからぬ事態及び事故をいう。特に認識すべき脅威は、次のとおりである。

⑴　意図的（計画的）な人為的脅威

故意の不正アクセス、サービス不能攻撃又は不正操作による機器又は情報資産の破壊、盗難、改ざん、消去、無断持ち出し、ソフトウェアのライセンス違反、ＡＰＴ攻撃等。

⑵　偶発的な人為的脅威

誤操作等によって起きる情報資産の破壊、漏えい、消去等及び搬送中の事故等による情報資産の盗難、漏えい、紛失等。

また、開発・設計・設定・メンテナンスの不備によるシステム障害や、委託先管理・マネジメントの欠如による情報資産の盗難、漏えい、紛失等。

⑶　環境的脅威

地震、落雷、火災、水害、停電、パンデミック（業務執行体制の維持が困難となるような大規模な感染症の流行）等の災害又は事故による情報資産の破壊、消失、サービス又は業務の停止等。

9　情報セキュリティ対策

情報セキュリティに対する脅威から本市の情報資産を保護するために次の対策を講ずる。

⑴　人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、十分な教育及び啓発により、すべての職員、委託事業者等にポリシーの内容を周知徹底するなど、守るべき行動基準及び判断基準を定める。

⑵　物理的セキュリティ対策

不正侵入又は盗難から情報資産を保護するために、管理区域の設置等情報資産への物理的なアクセスを制御するための対策を講ずる。

⑶　技術面及び運用面におけるセキュリティ対策

情報資産を外部又は内部からの不正アクセス等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策及び委託等による情報システム開発・運用保守の基準、ポリシー遵守状況の確認等の運用面の対策を講ずる。

⑷　情報システム全体の強靭性の向上

ア　本市における住民基本台帳ネットワークシステム及びマイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐための措置を講ずる。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外部接続先については、この限りではなく、インターネット等からマイナンバー利用事務系との双方向でのデータの移送を可能とする。

イ　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クラウドサービス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する。ただし、国が提供するガバメントクラウドを利用する場合で、特段の理由がある場合（修正プログラムの適用、ソフトウェアのアクティベーションの実施及び管理コンソール接続）については、例外的にインターネット接続を可能とする。

ウ　行政情報系ネットワーク（基幹系情報システムを除く）の情報システムを、専用回線を用いてクラウドサービス上へ配置することを情報システム部長が認める場合は、その領域を行政情報系ネットワークとして扱う。

⑸　危機管理対策

緊急事態が発生した際に迅速な対応を可能とするための危機管理対策を講ずる。

10　情報セキュリティ実施手順の策定

対策基準を遵守して情報セキュリティ対策を実施するために、情報資産に対する脅威及び情報資産の重要性に対応する対策基準の基本的な要件に基づき、各部局の長等が所管する情報資産の情報セキュリティ実施手順（以下「実施手順」という。）を策定する。

11　情報セキュリティ監査及び自己点検の実施

ポリシーが遵守されていることを検証するため、定期的に情報セキュリティ監査及び自己点検を実施する。また、情報セキュリティに関する状況が変化した場合には必要に応じて情報セキュリティ監査及び自己点検を実施する。

12　評価及び見直しの実施

情報セキュリティ監査及び自己点検の結果等により、ポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するため、ポリシーの見直しを実施する。

13　情報セキュリティに関する違反への対応

ポリシー及び実施手順に違反した職員については、その重大性、発生した事案の状況等に応じて懲戒処分の対象となることがある。

14　公開方針

ポリシー及び実施手順は、公表することにより本市の行政運営に重大な支障を及ぼすおそれのある事項を含んでいることから、基本方針を公開とし、対策基準及び実施手順は非公開とする。また、情報セキュリティ監査の概要については、公開とする。

別紙

個人情報の取扱いに関する特記事項

（個人情報の保護に関する法令等の遵守）

第１条　受託者は、「個人情報の保護に関する法律」（平成１５年法律第５７号。以下「個人情報保護法」という。）、個人情報保護委員会が定める「個人情報の保護に関する法律についての事務対応ガイド（行政機関等向け）」（以下「事務対応ガイド」という。）、「札幌市情報セキュリティポリシー」等に基づき、この個人情報の取扱いに関する特記事項（以下「特記事項」という。）を遵守しなければならない。

（管理体制の整備）

第２条　受託者は、個人情報（個人情報保護法第２条第１項に規定する個人情報をいう。以下同じ。）の安全管理について、内部における管理体制を構築し、その体制を維持しなければならない。

（管理責任者及び従業者）

第３条　受託者は、個人情報の取扱いに係る保護管理者及び従業者を定め、書面（当該書面に記載すべき事項を記録した電磁的記録を含む。以下同じ。）により委託者に報告しなければならない。

２　受託者は、個人情報の取扱いに係る保護管理者及び従業者を変更する場合の手続を定めなければならない。

３　受託者は、保護管理者を変更する場合は、事前に書面により委託者に申請し、その承認を得なければならない。

４　受託者は、従業者を変更する場合は、事前に書面により委託者に報告しなければならない。

５　保護管理者は、特記事項に定める事項を適切に実施するよう従業者を監督しなければならない。

６　従業者は、保護管理者の指示に従い、特記事項に定める事項を遵守しなければならない。

（取扱区域の特定）

第４条　受託者は、個人情報を取り扱う場所（以下「取扱区域」という。）を定め、業務の着手前に書面により委託者に報告しなければならない。

２　受託者は、取扱区域を変更する場合は、事前に書面により委託者に申請し、その承認を得なければならない。

３　受託者は、委託者が指定した場所へ持ち出す場合を除き、個人情報を定められた場所から持ち出してはならない。

（教育の実施）

第５条　受託者は、個人情報の保護、情報セキュリティに対する意識の向上、特記事項における従業者が遵守すべき事項その他本委託等業務の適切な履行に必要な教育及び研修を、従業者全員に対して実施しなければならない。

２　受託者は、前項の教育及び研修を実施するに当たり、実施計画を策定し、実施体制を確立しなければならない。

（守秘義務）

第６条　受託者は、本委託業務の履行により直接又は間接に知り得た個人情報を第三者に漏らしてはならない。

２　受託者は、その使用する者がこの契約による業務を処理するに当たって知り得た個人情報を他に漏らさないようにしなければならない。

３　前２項の規定は、この契約が終了し、又は解除された後においても、また同様とする。

４　受託者は、本委託等業務に関わる保護管理者及び従業者に対して、秘密保持に関する誓約書を提出させなければならない。

（再委託）

第７条　受託者は、やむを得ない理由がある場合を除き、本委託等業務の一部を第三者へ委託（以下「再委託」という。）してはならない。

２　受託者が再委託する場合には、あらかじめ委託者に申請し、委託者から書面により承諾を得なければならない。

3　受託者は、本委託等業務のうち、個人情報を取り扱う業務の再委託を申請する場合には、委託者に対して次の事項を明確に記載した書面を提出しなければならない。

(1) 再委託先の名称

(2) 再委託する理由

(3) 再委託して処理する内容

(4) 再委託先において取り扱う情報

(5) 再委託先における安全性及び信頼性を確保する対策

(6) 再委託先に対する管理及び監督の方法

4　受託者は、前項の申請に係る書面を委託者に対して提出する場合には、再委託者が委託者指定様式（本契約締結前に受託者が必要事項を記載して委託者に提出した様式をいう。）に必要事項を記載した書類を添付するものとする。

5　委託者が第２項の規定による申請に承諾した場合には、受託者は、再委託先に対して本契約に基づく一切の義務を遵守させるとともに、委託者に対して再委託先の全ての行為及びその結果について責任を負うものとする。

6　委託者が第２項から第４項までの規定により、受託者に対して個人情報を取り扱う業務の再委託を承諾した場合には、受託者は、再委託先との契約において、再委託先に対する管理及び監督の手続及び方法について具体的に規定しなければならない。

7　前項に規定する場合において、受託者は、再委託先の履行状況を管理・監督するとともに、委託者の求めに応じて、その管理・監督の状況を適宜報告しなければならない。

（複写、複製の禁止）

第８条　受託者は、本委託等業務を処理するに当たって、委託者から提供された個人情報が記録された資料等を、委託者の許諾を得ることなく複写し、又は複製してはならない。

（派遣労働者等の利用時の措置）

第９条　受託者は、本委託等業務を派遣労働者、契約社員その他の正社員以外の労働者に行わせる場合は、正社員以外の労働者に本契約に基づく一切の義務を遵守させなければならない。

２　受託者は、委託者に対して、正社員以外の労働者の全ての行為及びその結果について責任を負うものとする。

（個人情報の管理）

第１０条　受託者は、本委託等業務において利用する個人情報を保持している間は、事務対応ガイドに定める各種の安全管理措置を遵守するとともに、次の各号の定めるところにより、当該個人情報の管理を行わなければならない。

(1) 個人情報を取り扱う事務、個人情報の範囲及び同事務に従事する従業者を明確化し、取扱規程等を策定すること。

(2) 組織体制の整備、取扱規程等に基づく運用、取扱状況を確認する手段の整備、情報漏えい等事案に対応する体制の整備、取扱状況の把握及び安全管理措置の見直しを行うこと。

(3) 従業者の監督・教育を行うこと。

(4) 個人情報を取り扱う区域の管理、機器及び電子媒体等の盗難等の防止、電子媒体等の取扱いにおける漏えい等の防止、個人情報の削除並びに機器及び電子媒体等の廃棄を行うこと。

(5) アクセス制御、アクセス者の識別と認証、外部からの不正アクセス等の防止及び情報漏えい等の防止を行うこと。

（提供された個人情報の目的外利用及び第三者への提供の禁止）

第１１条　受託者は、本委託等業務において利用する個人情報について、本委託等業務以外の目的で利用し、又は第三者へ提供してはならない。

（受渡し）

第１２条　受託者は、委託者と受託者との間の個人情報の受渡しを行う場合には、委託者が指定した手段、日時及び場所で行うものとする。この場合において、委託者は、受託者に対して個人情報の預り証の提出を求め、又は委託者が指定する方法による受渡し確認を行うものとする。

（個人情報の返還、消去又は廃棄）

第１３条　受託者は、本委託等業務の終了時に、本委託等業務において利用する個人情報について、委託者の指定した方法により、返還、消去又は廃棄しなければならない。

２　受託者は、本委託等業務において利用する個人情報を消去又は廃棄する場合は、事前に消去又は廃棄すべき個人情報の項目、媒体名、数量、消去又は廃棄の方法及び処理予定日を書面により委託者に申請し、その承諾を得なければならない。

３　受託者は、個人情報の消去又は廃棄に際し委託者から立会いを求められた場合は、これに応じなければならない。

４　受託者は、前３項の規定により個人情報を廃棄する場合には、当該個人情報が記録された電磁的記録媒体の物理的な破壊その他当該個人情報を判読不可能とするのに必要な措置を講じなければならない。

５　受託者は、個人情報を消去し、又は廃棄した場合には、委託者に対してその日時、担当者名及び消去又は廃棄の内容を記録した書面で報告しなければならない。

（定期報告及び緊急時報告）

第１４条　受託者は、委託者から、個人情報の取扱いの状況について報告を求められた場合は、直ちに報告しなければならない。

２　受託者は、個人情報の取扱状況に関する定期報告及び緊急時報告の手順を定めなければならない。

（監査及び調査）

第１５条　委託者は、本委託等業務に係る個人情報の取扱いについて、本契約の規定に基づき必要な措置が講じられているかどうか検証及び確認するため、受託者及び再委託者に対して、実地の監査又は調査を行うことができる。

２　委託者は、前項の目的を達するため、受託者に対して必要な情報を求め、又は本委託等業務の処理に関して必要な指示をすることができる。

（事故時の対応）

第１６条　受託者は、本委託等業務に関し個人情報の漏えい等の事故（個人情報保護法違反又はそのおそれのある事案を含む。）が発生した場合は、その事故の発生に係る帰責の有無にかかわらず、直ちに委託者に対して、当該事故に関わる個人情報の内容、

件数、事故の発生場所、発生状況等を書面により報告し、委託者の指示に従わなければならない。

２　受託者は、個人情報の漏えい等の事故が発生した場合に備え、委託者その他の関係者との連絡、証拠保全、被害拡大の防止、復旧、再発防止の措置を迅速かつ適切に実施するために、緊急時対応計画を定めなければならない。

３　委託者は、本委託等業務に関し個人情報の漏えい等の事故が発生した場合は、必要に応じて当該事故に関する情報を公表することができる。

（契約解除）

第１７条　委託者は、受託者が特記事項に定める業務を履行しない場合は、特記事項に関連する委託等業務の全部又は一部を解除することができる。

２　受託者は、前項の規定による契約の解除により損害を受けた場合においても、委託者に対して、その損害の賠償を請求することはできないものとする。

（損害賠償）

第１８条　受託者の責めに帰すべき事由により、特記事項に定める義務を履行しないことによって委託者に対する損害を発生させた場合は、受託者は、委託者に対して、その損害を賠償しなければならない。

（注）委託事務の実態に即して、適宜必要な事項を追加し、又は不要な事項を省略することとする。

個人情報取扱状況報告書

年　　月　　日

札幌市長　　様

住　所
会社名
代表者名

個人情報取扱安全管理基準及び個人情報の取扱いに関する特記事項に基づき実施している安全管理対策の実施状況について下記のとおり報告いたします。

記

委託業務名	
受託期間	
対象期間	
安全管理対策の実施状況	

1　当該業務において、標記の基準及び特記事項に従い、安全管理対策を適切に実施しています。また、個人情報取扱安全管理基準適合申出書の提出時点からの変更有無等について、以下のとおり報告いたします。

(1) 従業者の指定、教育及び監督（変更なし・変更あり）

(2) 管理区域の設定及び安全管理措置の実施（変更なし・変更あり）

(3) セキュリティ強化のための管理策（変更なし・変更あり）

(4) 事件・事故における報告連絡体制（変更なし・変更あり）
○（発生した場合）事件・事故の状況：

(5) 情報資産の搬送及び持ち運ぶ際の保護体制（変更なし・変更あり）
○（実績ある場合）概要：

(6) 関係法令の遵守（変更なし・変更あり）

(7) 定期監査の実施（変更なし・変更あり）

(8) その他個人情報取扱安全管理基準適合申出書からの変更（なし・あり）

2　その他特記事項等