仕様書

1　業務名

「地下鉄南北線に関するワークショップ」実施業務

2　業務委託期間

契約締結日から令和７年３月 31 日（月）まで

3　業務目的及び概要

営業開始から 50 年以上が経過し、今後さっぽろ駅のホーム増設、車両更新などが予定されている本市南北線について、参加者に関心を持ってもらうこと、地下鉄のあり方についての意見を聴取することを目的として、市民を対象としたワークショップ全 2 回を開催する。

4　業務内容

(1)　ワークショップの企画・運営

以下のとおりに企画・運営を行うこと。なお、詳細については、別途、受託者と委託者との協議により決定するものとする。

○　テーマ設定

南北線について理解を深め、市民の足として求められるもの、備えるべき機能等について考えるものとする。

なお、参加者が、ワークショップ後も南北線に愛着をもてるような内容が望ましい。

○　参加対象者

参加対象者については、札幌市内に居住する札幌市民、各回 50 名程度を想定しており、第 1 回目は大人、第 2 回目は小学生（小学生と保護者 25 組程度）を対象に開催する。

開催当日の参加者については抽選による事を想定しているが、詳細は受託者と委託者との協議のうえ、決定するものとする。

○　広報・参加者募集

ワークショップについて SNS を活用するなど効果的な広報を実施し、必要な参加者を集めること。詳細は別途委託者と協議するものとする。

募集案内の作成や、参加申込者の管理等、募集に係る業務は、受託者の負担により行うものとする。ただし、交通局関係施設にてポスター掲出、配架物の設置を行う場合は、印刷したものを交通局の指定する場所に納品すれば、その後の作業は交通局にて行うことも可能であるため、必要に応じて委託者と協議すること。

印刷物を作成する場合そのデザインは、受託者が作成したデザイン案をもとに、委託者との協議のうえ決定する。

なお、当局関係施設への掲出等を実施する場合には、車内用ポスター（B3）は 900 枚程度、駅用ポスター（B1）は 250 枚程度、チラシ（A4）は 8,500 枚程度の掲出、配架が可能であるが、ポスターはコート紙（135 ㎏）で作成すること。

また、この場合の納品場所は、最大で 20 か所程度となる。

○　実施方法

参加者を少人数のグループに分け意見交換を行うものとする。なお、実施に当たっては下記のことに留意すること。

ア ワークショップで生まれた意見や話し合った内容は、当日会場いなかったものにもわかりやすいよう整理し概要版に活かすこと。

イ 運営にあたって必要なスタッフ（機材オペレーターやファシリテーター等）、備品・消耗品、当日使用する資料等については受託者の負担で準備・作成すること。

なお、資料作成に必要な素材（画像データ等）については、委託者が保持しているものの提供も可能であることから、必要に応じて委託者と協議すること。

○　開催日・時間・場所

開催時期は令和７年３月、時間は１回あたり２時間程度で、２回の実施を前提に、詳細は別途委託者と協議するものとする。

なお、委託者が確保する会場にて行うものとし、会場の使用にかかる費用は委託者が負担する。

⑵　成果物

○　実施報告書

ア 報告書（電子データ）

イ 報告書概要版 Ａ３サイズ１枚程度（電子データ）

ウ 上記報告書の編集可能な電子データ及び業務に用いたデータ等

5　環境への配慮

本業務においては、札幌市の環境マネジメントシステムに準じ、環境負荷低減に努めること。

⑴　電気、水道、油、ガス等の使用に当たっては、極力節約に努めること。

⑵　ごみ減量及びリサイクルに努めること。

⑶　両面コピーの徹底やミスコピーを減らし、紙の使用量を減らすように努めること。

⑷　自動車等を使用する場合は、できるだけ環境負荷の少ない車両を使用し、アイドリングストップの実施など環境に配慮した運転を心がけること。

⑸　業務に係る用品等は、札幌市グリーン購入ガイドラインに従い、極力ガイドライン指定品を使用すること。

6　その他特記事項

⑴　守秘義務

受託者は、本業務を通じて知りえた秘密を第三者に漏えいすること及び資料並びにデータの紛失、滅失、毀損、盗難等を防止するために必要な措置を講ずること。

また、本業務の結果データ等の使用・保存・処分等にあたっては、秘密の保持に十分配慮するとともに、委託者の指示に従うこと。受託者は、委託者より廃棄の指示を受けた時は、データの内容を破棄し、その処理経過は書面をもって、委託者へ報告すること。

(2) 個人情報の取扱い

受託者は、この契約による業務を処理するに当たって個人情報を取り扱う際には、別紙「個人情報取扱安全管理基準」に基づき、適切な措置を講じること。

なお、開札後、契約締結までに、必要書類を添付のうえ様式１「個人情報取扱安全管理基準適合申出書」を提出すること。

(3) 身分証明書の携行等

受託者の作業従事者は、本市の施設内及び本業務に関して立ち入りが必要となる本市以外の施設内では、常に身分証明書を携行すること。また、本市施設内においては、本市業務担当者が許可しない限り、作業上必要でない場所へ無断で立ち入らないこと。

(4) 疑義の解消等

業務の実施にあたって必要な事項のうち、本書で明記の無い点または疑義が生じた場合、並びにこれに係る変更を行う場合には、必ず委託者と協議し承認を得ること。

業務の実施にあたって必要な事項について、本書で明記の無い点または疑義や状況の変化があった場合は、別途、受託者と委託者との協議により内容を変更することができるものとする。

(5) 成果物に係る留意事項

本業務成果物については、意味不明、不完全または曖昧な表現の記述をしないように留意し、専門的または特殊な用語については用語解説または注釈を付記すること。

また、成果物の納入後、委託者において実施する成果物検査の結果、本仕様書記載の内容と著しく異なる又は不足する場合は、受託者の責任において関連する項目を精査し、当該個所の修正又は追加を行うこと。

なお、委託者は、本業務の報告書等の成果物の一部または全部をホームページに掲載することができるものとする。受託者は、この点を念頭に置いて成果物を作成すること。

(6) 著作権等

受託者は、本業務の遂行により生じた著作権（著作権法第 27 条及び 28 条に定められた権利を含む。）を、成果物の納入、検査合格後、ただちに委託者に無償で譲渡するものとする。

また、受託者は、委託業務の遂行に当たり、第三者の知的財産権（著作権、意匠権、商標権等）、プライバシー又は肖像権・パブリシティ権その他の権利を侵害しないこと。

7 委託者担当部局

〒004-8555 札幌市厚別区大谷地東２丁目４－１ 交通局本局庁舎４階
札幌市交通局高速電車部業務課、車両課（担当：長澤、清見）
電話：011-896-2742　FAX：011-896-2793　E-mail：st.gyomu@city.sapporo.jp

【別紙】

個人情報取扱安全管理基準

1　個人情報の取扱いに関する基本方針、規程及び取扱手順の策定

個人情報の適正な取扱いの確保について基本方針を策定していること。

また、以下の内容を記載した個人情報の保護に関する規程及び個人情報の取扱手順等が定められていること。

(1) 組織的安全管理措置

(2) 人的安全管理措置

(3) 物理的安全管理措置

(4) 技術的安全管理措置

※　上記(1)～(4)の具体的内容については、個人情報保護委員会ホームページ（https://www.ppc.go.jp）に掲載されている「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）」の「４－３－１」の「安全管理措置（法第６６条）」を御確認ください。

2　個人情報の取扱いに関する総括保護管理者及び保護管理者の設置

個人情報の取扱いに関する総括保護管理者及び保護管理者が定められており、基本方針、規程及び個人情報の取扱手順等に明記されていること。

3　従業者の指定、教育及び監督

(1) 個人情報の秘密保持に関する事項が就業規則等に明記されていること。

(2) 個人情報を取り扱う従業者を指定すること。

(3) 個人情報の取扱い、情報システムの運用・管理・セキュリティ対策及びサイバーセキュリティの研修計画を策定し、従業者に対し毎年１回以上研修等を実施していること。また、個人情報を取り扱う従業者は、必ず１回以上研修等を受講している者としていること。

(4) 総括保護管理者及び保護管理者は、従業者に対して必要かつ適切な監督を行うこと。

4　管理区域の設定及び安全管理措置の実施

(1) 個人情報を取り扱う管理区域を明確にし、当該区域に壁又は間仕切り等を設置すること。

【管理区域の例】

- サーバ等の重要な情報システムを管理する区域
- 個人情報を保管する区域
- その他個人情報を取り扱う事務を実施する区域

(2) (1)で設定した管理区域について入室する権限を有する従業者を定めること。

また、入室に当たっては、用件の確認、入退室の記録、部外者についての識別化及び部外者が入室する場合は、管理者の立会い等の措置を講ずること。さらに、入退室の記録を保管していること。

(3) (1)で設定した管理区域について入室に係る認証機能を設定し、パスワード等の管理に関する定めの整備及びパスワード等の読取防止等を行うために必要な措置を講ずること。
(4) 外部からの不正な侵入に備え、施錠装置、警報措置及び監視装置の設置等の措置を講ずること。
(5) 管理区域では、許可された電子媒体又は機器等以外のものについて使用の制限等の必要な措置を講ずること。

5　セキュリティ強化のための管理策

情報資産の盗難、紛失、持出し、複写・複製、目的外の使用及び第三者への提供を防止するため以下の対策を実施していること。

(1) 個人情報の取扱いに使用する電子計算機等は、他のコンピュータと接続しない単独による設置又は当該業務に必要な機器のみと接続していること。また、インターネット及び当該業務を実施する施設外に接続するイントラネット等の他のネットワークに接続していないこと。ただし、本市の許可を得た場合はこの限りでない。
(2) 個人情報の取扱いにおいてサーバを使用している場合は、当該業務を実施する施設内に設置していること。また、サーバへのアクセス権限を有する従業者を定めること。さらに、部外者のアクセスは必要最小限とし、管理者の立会い等の措置を講ずること。ただし、本市の許可を得た場合はこの限りでない。
(3) 個人情報の取扱いにおいて使用する電子計算機等は、アクセス権等を設定し、使用できる従業者を限定すること。また、アクセスログやログイン実績等から従業者の利用状況を記録し、保管していること。
(4) 記録機能を有する機器の電子計算機等への接続制限について必要な措置を講ずること。
(5) 本市が貸与する文書、電子媒体及び業務にて作成した電子データを取り扱う従業者を定めること。
(6) 業務にて作成した電子データを保存するときは、暗号化又はパスワードにより秘匿すること。また、保存した電子データにアクセスできる従業者を限定するとともにアクセスログ等から従業者の利用状況を記録し、契約期間終了後、１年以上保管していること。
(7) 本市が貸与する文書及び電子媒体は、施錠できる耐火金庫及び耐火キャビネット等にて保管すること。また、書類の持ち出し記録等を作成していること。
(8) 個人情報の取扱いにおいて使用する電子計算機は、従業者が正当なアクセス権を有する者であることをユーザ ID、パスワード、磁気・IC カード又は生体情報等のいずれかにより識別し、認証していること。
(9) 個人情報の取扱いにおいて使用する電子計算機は、セキュリティ対策ソフトウェア等（ウィルス対策ソフトウェア等）を導入していること。
(10)業務にて作成した電子データを削除した場合は、削除した記録を作成していること。また、削除したことについて証明書等により確認できる措置を講ずること。
(11)個人情報の取扱いにおいて使用する電子計算機等を廃棄する場合は、専用のデータ削除ソフトウェアの利用又は物理的な破壊等により、復元不可能な手段を採用すること。
(12)本市の許可なく第三者に委託しないこと。

6　事件・事故における報告連絡体制

(1) 従業者が取扱規程等に違反している事実又は兆候を把握した場合の管理者への報告連絡体制を整備していること。

(2) 情報の漏えい、滅失又は毀損等事案の発生又は兆候を把握した場合の従業者から管理者等への報告連絡体制を整備していること。

(3) 情報の漏えい、滅失又は毀損等事案が発生した際の本市及び関連団体への報告連絡体制を整備していること。併せて、事実関係の調査、原因の究明及び再発防止策の検討並びに決定等に係る体制及び手順等を整備していること。

7　情報資産の搬送及び持ち運ぶ際の保護体制

本市が貸与する文書、電子媒体及び左記書類等に基づき作成される電子データを持ち運ぶ場合は、施錠した搬送容器を使用すること。また、暗号化、パスワードによる保護、追跡可能な移送手段等により、破損、紛失、盗難等のないよう十分に配慮していること。

8　関係法令の遵守

個人情報の保護に係る関係法令を遵守するために、必要な体制を備えていること。

9　定期監査の実施

個人情報の管理の状況について、定期に、及び必要に応じ、随時に点検、内部監査及び外部監査を実施すること。

１０　個人情報取扱状況報告書の提出

本市の求めに応じ、又は当該業務契約に基づき、各月の期間ごとの役務完了の書面提出時において、本市が指定する様式にて個人情報取扱状況報告書を提出すること。

【様式１】

個人情報取扱安全管理基準適合申出書

年　　月　　日

（申請者）

貴市の個人情報取扱安全管理基準について下記のとおり適合していることを申し出ます。

記

●個人情報取扱安全管理基準及び確認事項

※　本申出書において各種資料のご提出をお願いしております。資料が提出できない場合は、実地の監査、調査等の際などに当該書類の内容を確認いたします。

１　個人情報の取扱いに関する基本方針、規程及び取扱手順の策定

貴社の策定した個人情報の取扱いに関する基本方針、規程及び取扱手順等をご記入ください。併せて、当該規程をご提出ください。

２　個人情報の取扱いに関する総括保護管理者及び保護管理者の設置

個人情報の取扱いに関する総括保護管理者及び保護管理者を記載した書類をご提出ください。上記１により提出した基本方針等に記載がある場合は提出不要です。なお、付箋等で該当箇所をご教示願います。

３　従業者の指定、教育及び監督

(1) 当該業務に従事する従業者を「従業者名簿」にてご提出ください。

(2) 従業者の秘密保持に関する事項が明記されている書類をご提出ください。

(3) 従業者を対象とした研修実施報告書等をご提出ください。

４　管理区域の設定及び安全管理措置の実施

設定した管理区域の詳細についてご記入ください。□欄は管理区域に当該装置を設置している場合、■とチェックしてください。また、個人情報を黒塗りにした各管理区域の入退室記録を提出してください。

・管理区域の名称

入退室の認証方法

入退室記録の保存期間

□　施錠装置　□　警報装置　□　監視装置　□　その他（　　）

持込可能な電子媒体及び機器

・管理区域の名称

入退室の認証方法

入退室記録の保存期間

□　施錠装置　□　警報装置　□　監視装置　□　その他（　　）

持込可能な電子媒体及び機器

・管理区域の名称

入退室の認証方法

入退室記録の保存期間

□　施錠装置　□　警報装置　□　監視装置　□　その他（　　）

持込可能な電子媒体及び機器

・管理区域の名称

入退室の認証方法

入退室記録の保存期間

□　施錠装置　□　警報装置　□　監視装置　□　その他（　　）

持込可能な電子媒体及び機器

5　セキュリティ強化のための管理策

セキュリティ強化の詳細についてご記入ください。貴社のセキュリティが各項目の内容に合致している場合は、□欄を■とチェックしてください。

(1) 個人情報の取扱いに使用する電子計算機のセキュリティについて

□　他のネットワークと接続していない。

□　従業者にアクセス権限を設定している。

従業者の利用記録の保存期間（　　）

□　記録機能を有する機器の接続制御を実施している。

接続制御の方法（　　）

□　従業者の認証方法（　　）

□　セキュリティ対策ソフトウェア等を導入している。

※個人情報を黒塗りにした従業者の利用記録を提出してください。

(2) 文書、電子媒体の取扱いについて

□　取り扱うことができる従業者を定めている。

□　文書、電子媒体の持ち出しを記録している。

当該記録の保存期間（　　）

□　文書、電子媒体等について施錠できる耐火金庫等に保管している。

※個人情報を黒塗りにした文書、電子媒体の持ち出し記録を提出してください。

(3) 業務にて作成した電子データの取扱いについて

□　取り扱うことができる従業者を定めている。

□　電子データを保存する時は、暗号化又はパスワードを設定している。

□　電子データの利用状況について記録している。

□　作成した電子データの削除記録を作成している。

※個人情報を黒塗りにした電子データの利用状況の記録及び削除記録を提出してください。

6　事件・事故における報告連絡体制

個人情報取扱安全管理基準の「6　事件・事故における報告連絡体制」(1)から(3)までの内容を満たしていることが分かる書類を提出してください。上記１にて提出した基本方針等に記載がある場合は提出不要です。なお、付箋等で該当箇所をご教示願います。

7　情報資産の搬送及び持ち運ぶ際の保護体制

情報資産を搬送及び持ち運ぶ際の保護体制についてご記入ください。貴社の保護体制が各項目の内容に合致している場合は、□欄を■とチェックしてください。なお、その他の対策を実施している場合は、対策をご記入ください。

□　情報資産を持ち運ぶ場合は、施錠した搬送容器を使用している。

□　上記以外の盗難及び紛失対策を実施している。

対策を以下にご記入ください。

８　関係法令の遵守

個人情報の保護に係る関係法令を遵守するための体制及び取組等をご記入ください。

……

……

９　定期監査の実施

貴社の内部監査及び外部監査の実施状況についてご記入ください。各監査の実施状況が各項目の内容に合致している場合は、□欄を■とチェックしてください。また、各監査の実施状況が分かる書類をご提出ください。なお、外部監査は情報セキュリティマネジメントシステム等の認証を受ける際の審査を外部監査として取り扱っても問題ございません。その場合は、各種申請の認証通知を監査の実施状況の書類といたします。

□　内部監査を実施している。

□　外部監査を実施している。

１０　情報セキュリティマネジメントシステム（以下「ＩＳＭＳ」という。）、プライバシーマーク等の認証等、貴社が取得しているセキュリティ関連の認証についてご記入ください。

また、認証を受けたことが分かる書類をご提出願います。

取得しているセキュリティ関連の認証（ＩＳＭＳ・プライバシーマーク等）

名称……

認証年月日……　最終更新年月日……

名称……

認証年月日……　最終更新年月日……

名称……

認証年月日……　最終更新年月日……