

## 令和4年度デマンド交通実証実験業務仕様書

### 1 業務の名称

令和4年度デマンド交通実証実験業務

### 2 業務期間

#### (1) 契約期間

契約締結日から令和5年3月31日（金）まで

#### (2) 予約受付期間

令和4年11月14日（月）から令和5年3月31日（金）まで（予定）。

#### (3) デマンド交通運行期間

令和4年11月21日（月）から令和5年3月31日（金）まで（予定）。

### 3 業務の内容

#### (1) デマンド交通の運行

##### ① 運行日時

2-(3)の期間内における月曜日から金曜日とし、1日あたり6時間運行する。運行時間は9時から15時までを想定している。ただし、令和4年12月29日から令和5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87日）。

##### ② 実施箇所

別紙地図のとおり

##### ③ 運賃

|        |      |               |
|--------|------|---------------|
| 一般運賃   | 350円 | 中学生以上         |
| 高齢者運賃  | 150円 | 70歳以上         |
| 障がい者運賃 | 150円 | 障がい者手帳保有者     |
| 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）  |

※運賃については、今後の地域協議等で変更する可能性がある。

##### ④ 乗降ポイント

②で指定するエリア内において、40箇所程度（今後の地域協議等に変更する可能性がある。）を設置する。

⑤ 運行事業者

ア 一般社団法人札幌ハイヤー協会から事前に推薦のあった下記の事業者による道路運送法第 21 条に定める一般乗用旅客自動車運送事業の乗合許可運行とする。

- ・事業者名 東邦交通株式会社
- ・事業者所在地 札幌市西区発寒 14 条 11 丁目 1-15

イ 受託者は、運行事業者と協力体制を構築し、安全運行に努めること。また、運行経費から運賃収入を差し引いた運行経費負担金について、運行事業者へ支払うこと。

ウ 運行事業者の業務は車両の管理、運行の管理及び運賃の管理とする。

⑥ 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 8 名を想定）

⑦ 利用者

事前会員登録者

(2) 乗車予約の受付・管理

① 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。

② 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-(1)-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。

③ 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。

### (3) 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、および実施後の結果報告に至るまでの間、本市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 地域合意形成に向けた支援

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、委託業務範囲に係る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 運行事業者による運行体制構築に向けた支援

運行業務を担う運行事業者への業務委託において、業務委託の内容の準備等に関し、相談・支援を行うこと。

#### ④ 利用促進に向けた支援

利用者登録支援に向けたチラシの作成やプレスリリース、住民説明会（3回程度を想定）の実施にあたり、委託業務範囲に係る企画の立案や、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。

チラシは両面カラー印刷とし、1部あたりA4用紙1枚以上とする。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実施し、結果を分析すること。

### (4) 予約システムの構築

#### ① システム設計・打合せ

ア 本市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 本市の就業時間内（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およ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、本市に随時報告すること。

⑤ データ分析業務

実証実験により取得したデータや地域住民のアンケートを分析・検証し、新たな交通サービスとしての実現可能性の検討を行う。

⑥ 乗降ポイント設置業務

予約システムに設定した乗降ポイントの目印を作成、設置すること。設置にあたっては、積雪地であっても識別可能な設置場所、方法とすること。

#### 4 予約システム概要

- (1) 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。
- (2) 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。
- (3) 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。
- (4) 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。
- (5) 個人情報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

(1) 予約・配車・運行管理にかかわる基本機能

- ① 電話またはインターネットにより利用者から乗車予約を受け付け、即時に予約された時間に出発場所または到着場所に車両をリアルタイム配車するシステムと

すること。

- ② 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。
- ③ 予約締切時間を任意に指定することができること。
- ④ 運行範囲の設定が可能であること。
- ⑤ 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。
- ⑥ 予定乗降場所数を登録、運用できるシステムとすること。

(2) 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、乗降ポイントの案内ができること。
- ② 乗車人数、乗車希望時間、乗降ポイントを任意に指定することができること。

(3) ドライバーアプリ

- ① 利用者の属性により、ドライバーが車載端末で乗車する利用者の乗車賃を確認する機能があり、かつシステムで乗車賃を管理できるシステムとすること。
- ② 運転者へテキストによるメッセージが伝達できること。
- ③ 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。

(4) 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。また、過去の運行記録について確認できること。
- ⑥ 利用実績（日別・時間帯別、乗降ポイント別等）を随時確認できること。

(5) 電話予約受付

- ① 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。
- ② 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。
- ③ 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。

## 6 個人情報の保護について

- (1) 「個人情報の保護に関する法律」、「札幌市個人情報保護条例」を遵守して業務を行うこと。
- (2) 別紙「個人情報取扱注意事項」を遵守して業務を行うこと。

## 7 情報資産の取り扱いについて

- (1) 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。
- (2) 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。
- (3) 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。
- (4) 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。
- (5) 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。
- (6) 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。
- (7) 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。
- (8) 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。
- (9) 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。
- (10) 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。
- (11) 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。
- (12) 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。
- (13) 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。

(14) 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。

(15) 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。

(16) 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。

(17) 本業務を第三者に再委託する場合の条件

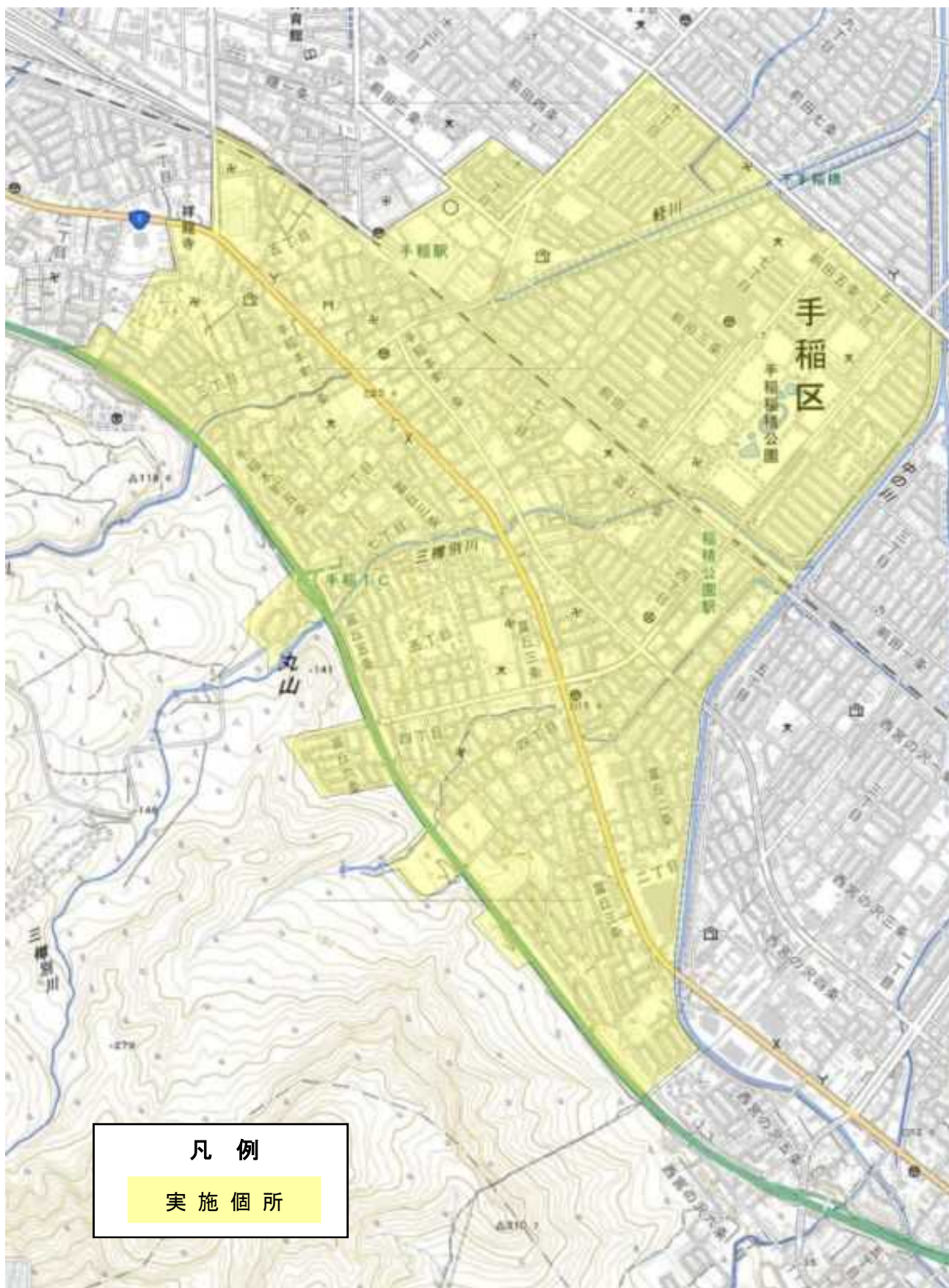
- ① 本業務を合理的な理由及び必要性により再委託する場合には、セキュリティ対策が確認できる資料を提出し、本市の承認を受けること。
- ② 再委託先に対しては、本業務委託契約書の内容を周知徹底し、情報資産の破壊、盗難、改ざん、消去等を未然に防止するための措置を取ること。
- ③ 受託者は、再委託先が行った本業務に関する行為について一切の責任を負うこと。

(18) 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。





## 個人情報取扱注意事項

(個人情報を取り扱う際の基本的事項)

第1 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、個人の権利利益を侵害することのないように努めなければならない。

(秘密の保持)

第2 受託者は、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。

(再委託等の禁止)

第3 受託者は、この契約による業務を第三者に委託し、又は請け負わせてはならない。ただし、あらかじめ、委託者が書面(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。)により承諾した場合は、この限りではない。

(複写、複製の禁止)

第4 受託者は、この契約による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、委託者の承諾を得ることなく複写し、又は複製をしてはならない。

(目的外使用の禁止)

第5 受託者は、この契約による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を目的外に使用し、又は第三者に提供してはならない。

(資料等の返還)

第6 受託者は、この契約による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、業務完了後速やかに委託者に返還するものとする。ただし、委託者が別に指示したときは、その方法によるものとする。

(事故の場合の措置)

第7 受託者は、個人情報取扱注意事項に違反する事態が生じ、又は生ずるおそれのあることを知ったときは、速やかに委託者に報告し、委託者の指示に従うものとする。

(契約解除及び損害賠償)

第8 委託者は、受託者が個人情報取扱注意事項に違反していると認めたときは、契約の解除及び損害賠償の請求をすることができる。

(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。

取扱嚴重注意

# 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4年3月18日改正情報セキュリティ委員会承認

この札幌市情報セキュリティポリシーは、本市における情報セキュリティ対策について、外部に公表できない内容を含んでいることから、取扱には十分注意をしてください。

- ① 対策基準は、本市職員以外に公開してはいけません。
- ② 受託事業者においても公開してはいけません。
- ③ 本書を机の上に放置することは止めましょう。

# 目 次

|                                |   |
|--------------------------------|---|
| 序 札幌市情報セキュリティポリシーの構成.....      | 1 |
| 第1章 情報セキュリティ基本方針 .....         | 2 |
| 1 目的 .....                     | 2 |
| 2 定義 .....                     | 2 |
| (1) 情報セキュリティ .....             | 2 |
| (2) ネットワーク .....               | 2 |
| (3) 情報システム .....               | 2 |
| (4) 情報資産 .....                 | 2 |
| (5) 住民基本台帳ネットワークシステム.....      | 2 |
| (6) マイナンバー利用事務系.....           | 3 |
| (7) 校務系情報.....                 | 3 |
| (8) 教育系情報.....                 | 3 |
| (9) 学校情報システム.....              | 3 |
| 3 対象範囲 .....                   | 3 |
| 4 ポリシーの位置付け.....               | 3 |
| 5 職員の責務 .....                  | 3 |
| 6 情報セキュリティ管理体制.....            | 3 |
| 7 情報資産の分類.....                 | 3 |
| 8 情報セキュリティに対する脅威 .....         | 4 |
| (1) 意図的（計画的）な人為的脅威.....        | 4 |
| (2) 偶発的な人為的脅威 .....            | 4 |
| (3) 環境的脅威.....                 | 4 |
| 9 情報セキュリティ対策 .....             | 4 |
| (1) 人的セキュリティ対策 .....           | 4 |
| (2) 物理的セキュリティ対策.....           | 4 |
| (3) 技術面及び運用面におけるセキュリティ対策 ..... | 4 |
| (4) 情報システム全体の強靱性の向上 .....      | 4 |
| (5) 危機管理対策 .....               | 4 |
| 10 情報セキュリティ実施手順の策定.....        | 5 |
| 11 情報セキュリティ監査及び自己点検の実施 .....   | 5 |
| 12 評価及び見直しの実施 .....            | 5 |
| 13 情報セキュリティに関する違反への対応.....     | 5 |
| 14 公開方針 .....                  | 5 |

## 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。しかしながら一方では、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<br>情報セキュリティ<br>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、市民生活を豊かにするまちづくりのために情報化を推進しているところである。しかし、情報活用的一方で、各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。

したがって、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である。ひいては、このことが本市に対する市民からの信頼の維持向上に寄与するものである。

また、近年いわゆるIT革命の進展により、電子商取引の発展や電子自治体の構築が現実のものとなっている。本市が電子自治体を構築するためには、すべてのネットワーク及び情報システムが高度な安全性を有することが不可欠な前提条件である。

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、本市における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<sup>(注)</sup>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（ISO7498-2：1989）

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

#### (1) 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。

#### (2) 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。

#### (3) 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。

#### (4) 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。

#### (5) 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。

(6) 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。

(7) 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。

(8) 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。

(9) 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。

### (1) 意図的（計画的）な人為的脅威

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、無断持ち出し、ソフトウェアのライセンス違反、APT攻撃等。

### (2) 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。

### (3) 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。

### (1) 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。

### (2) 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。

### (3) 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。

### (4) 情報システム全体の強靱性の向上

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。

### (5) 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。