業務仕様書

１　業務名

札幌市公衆無線LAN更改業務

２　業務概要

札幌市が整備・運用を行っている公衆無線LANサービス「Sapporo City Wi-Fi」（以下「本サービス」という。）の提供エリアにおいて、外国人観光客をはじめとする利用者がスマートフォン等の個人端末でインターネットに接続できる通信環境の維持・向上を図るため、本サービスに係る機器及びシステムの更改を行う。

３　業務期間

契約締結日から令和９年（2027年）３月31日まで

４　業務概要

⑴　全般

受託者は委託者が別紙１～17に定めるエリアにおいて、令和９年（2027年）２月１日から新たな本サービスの提供が可能となるように下記の整備を行うこととする。なお、令和９年（2027年）２月１日以降の運用及び保守に係る契約は別途契約を締結する。

- 本サービスの提供に必要なサーバおよびネットワークの設計、敷設、設定、動作試験
- 本サービスの提供に必要なハードウェアおよびソフトウェア等の準備、構築
- ハードウェアの稼働・通信に必要なLAN配線の敷設等整備作業
- 本サービスの提供に必要なインターネット回線の準備

また、下記の点も踏まえたうえで整備を行うこと。

- 整備に際して必要となる配線、配管は新設・既存設備の活用いずれも妨げないが、既存設備の利用は、当該設備の所有者（現サービス事業者）の承諾を要する。承諾が得られていない既存設備を前提とした工程・費用計画は認めない。
- 本業務において設置するアクセスポイント、ルータ、スイッチ、サーバ、附帯機材等の設備については、委託者は所有権を取得せず、契約に定める範囲で本サービスの提供を受ける。
- 受託者は、関係諸法令を遵守し、関係機関への許認可・届出等が必要な場合は、受託者の責任で行うこと。
- 本業務の実施にあたっては、原則として既存サービスの停止又は機能制限を伴わない方法で実施すること。技術的にやむを得ない場合は委託者および現行のサービス提供者と調整を行うこと。

- 本業務において、公衆無線LANサービスを提供するために受託者が調達し、構築した構成機器等の正常動作及び安定動作における責任は、受託者が負うこと。
- 本サービスの運用が開始された後、運用及び保守に係る契約が終了となり、更新がされなかった場合、提供設備は受託者が撤去・回収する。原状回復の要否・範囲・費用負担は委託者と協議し決定する。
- 地下鉄駅構内における作業は夜間となり、工事に際して作業認定者の資格を有しているか有している者の立ち合いが必要になる。

⑵ 設置場所

受託者は、委託者が定める別紙１～17に定めるエリアにおいて本サービスの提供を行うため必要な設備を自ら設計し、これらの配置や数量等を決定すること。

- 設置場所は、施設所有者の特段の定めがない限り、受託者が施設所有者と契約等を行うものとし、設置場所の確保に係る費用（設置料、光熱費等）は受託者の負担とすること。
- 令和９年（2027年）１月末までは既存設備による本サービスの提供を予定していることから、既存設備による本サービスの提供に支障が出ないように整備を行うこと。

⑶ 利用環境

下記の利用環境を確保すること。

- 利用者が本サービスを無料で利用することができること。
- 利用規約に同意し、必要な認証を行った利用者にインターネット接続を提供すること。
- インターネットが利用できる環境を保有していない利用者等は認証を行うことが困難であるため、認証手続きに係る最初の一定時間（最低10分を目安とする）はインターネット接続を可能とすること。
- 登録した利用者情報を一定期間保持し、一度利用者情報を登録した利用者は再度のアクセス時の認証ポータル画面が簡易となるようにすること。
- １回あたりの利用可能時間内であれば、利用者が拠点間を移動しても認証ポータル画面による再認証をスキップしてインターネット接続ができること。
- 認証ポータル画面は多言語に対応し、利用者端末の言語設定を自動判別し、その言語による画面表示機能を有すること。なお、日本語、英語、中国語（簡体字・繁体字）、韓国語、タイ語への対応は必須とする。
- 本サービスの接続制限時間及び回数は委託者が任意に指定できること。
- 災害時には利用者登録の有無に関わらず、利用者がインターネットに接続でき、災害時利用モードへの切替等は委託者側にて行うことができること。また、気象庁から受信する災害情報をもとに災害時利用モードへ自動で切り替える機能を有していること。具体的な内容は提案による。

⑷　機能

以下の規格・仕様とすること。

認証方式	以下２つの認証方式が利用できること １　メールアドレスによる認証 利用開始時にメールアドレスを登録し、登録したメールアドレスに返信されるURLを押下することで利用ができること ２　SNSアカウントによる認証 FacebookやX等、SNSアカウントの認証情報を入力することで利用ができること
対応OS	スマートフォン、タブレット端末、ノートPCで動作することを前提とし、下記をはじめとするメーカーサポートが継続されている標準的なブラウザで閲覧・操作ができること。 ・OS Android、iOS、Windows、macOS、iPadOS ・ブラウザ Microsoft Edge、Google Chrome、Safari
利用者登録情報の保持期間	365日間保持
１回あたりの接続時間	30分間（※委託者との協議で変更が可能であること）
サービス提供時間	24時間365日
アクセスログの記録	MACアドレス、IPアドレス、利用者登録情報（メールアドレス等）、利用日時等を取得し、保存期間は６カ月以上とする。
ネットワーク	光回線、ISPは受託者が用意すること。光回線引き込みが困難な場合はLTE（キャリア回線）もしくはケーブルテレビ回線とすること。
AP接続回線帯域	ベストエフォート１Gbps以上（※ただし有線敷設が不可能な箇所はこれに限らない）
SSID	委託者と協議のうえ決定する。Open Roamingによる認証があることを鑑み、複数のSSIDが設定可能であることとする。なお、携帯キャリアのSSIDは送波しないこと。

⑸　セキュリティ

下記の内容を順守すること。

- サーバ及びネットワーク施設は、セキュリティ責任者等により、24時間体制でビデオ監視される等のセキュリティが強化されていること。
- 電源、サーバ等は冗長性を持たせること。
- 本サービスに接続する利用者の端末同士の通信を遮断すること。
- アクセスポイントを含めた機器にはメンテナンス用の端末からのみアクセス可能とし、利用者の端末からの不正アクセスを遮断すること。

- システムの安全性と信頼性を維持するため、受託者が用意する機器及びソフトウェアに関して、セキュリティパッチ等の更新が更改された場合は、必要に応じて、速やかに適用すること。
- WPA2以上に対応すること。
- アクセスポイント側から公衆無線LANサービス接続環境のネットワークをVPN網等によりグループ化し、グループ外の回線からの接続を拒否すること。
- サーバ、アクセスポイント等に保有する利用者情報等の情報漏えい対策を講じること。
- インターネットからの攻撃をブロックできるファイアウォール等を設けること。
- 不正アクセス防止、改ざん防止等のセキュリティ対策を講じること。
- 外部からの不正な攻撃に備えて、IDS及びDDoS攻撃等の対策が施されていること。
- クラウドサービスを利用する場合は、別途提供する「クラウド向け技術対策基準」及び「業務委託及び外部サービス(クラウドサービス)の利用に関する規定」に準拠することを原則とする。

⑹ 有害サイトのフィルタリング

公序良俗に反するコンテンツ、青少年に有害なサイト、セキュリティ上危険なサイトに対するフィルタリングを行うこと。具体的な内容は委託者との協議による。

⑺ アクセスポイント

以下の規格・仕様と同等またはそれ以上のものとすること。

なお、無線LAN規格については、利便性・コスト面を考慮のうえ、特定の場所において、IEEE 802.11beの対応が望ましい場合は提案すること。

ア　屋内型（光回線対応）

無線LAN規格	IEEE 802.11ax/ac/n
使用周波数帯	2.4GHz、5GHz、6GHz
同時接続数（帯域当たり）	512
動作保証温度	0℃～+50℃

イ　屋内型（LTE回線対応）

無線LAN規格	IEEE 802.11ax/ac/n
使用周波数帯	2.4GHz、5GHz、6GHz
同時接続数（帯域当たり）	512
動作保証温度	0℃～+40℃

ウ　屋外型

無線LAN規格	IEEE 802.11ax/ac/n
使用周波数帯	2.4GHz、5GHz
同時接続数（帯域当たり）	256以上
動作保証温度	-40℃～+55℃以上

⑻　OpenRoaming

利用者の利便性を向上するため、OpenRoamingに対応すること。

また、OpenRoamingに接続するため、アカウントの利用確認を行ったうえで接続に必要な認証プロファイルを利用者の端末にインストールする機能を提供すること。

なお、OpenRoamingは本サービスとは異なる認証基盤を用いた連携サービスであり、別途定める利用規約および認証事業者の規約に基づくものとする。

（注）本仕様書は、本サービスに係る各種仕様を定めたものであり、
OpenRoamingに関連する仕様を規定するものではない。

⑼　保守・運用

本サービスに関わる保守運用契約は別途締結することとするが、受託者は以下の内容を考慮し本業務を実施すること。

ア　遠隔監視

本サービスの安定運用を確保するため、安定的な運用に必要となる24時間365日体制で遠隔による死活監視ができるように対応すること。また、定期保守及び障害対応を行った場合はその都度速やかに委託者へ報告すること。

イ　業務報告

日別、拠点別、言語別等で利用実績を集計し、委託者へ提供すること。具体的な内容は提案による。

ウ　故障修理

故障が発生した場合を想定し、速やかに現地拠点設備等の切り分け、機器交換等の故障対応ができるよう考慮し整備すること。障害発生時は、委託者及びアクセスポイント等を設置している施設と協議のうえ速やかに復旧作業を行うこと。

利用者が安心してサービスを利用できる環境を維持するため、オンサイトでの故障修理又は機器の交換対応を行える体制を構築すること。

故障発生時の迅速な復旧を確保するため、通信用回線（固定回線）に関する修理対応については、通常営業時間外（夜間）における現地出張修理も可能とすること。対応時間帯、費用負担、事前連絡方法等の詳細は、委託者と協議のうえ決定すること。

エ　問い合わせ対応

以下のとおり、利用者及び委託者からの問い合わせ窓口を設けること。

	項目	内容
利用者問い合わせ	対応時間	365日　9:00～18:00
	対応言語	日本語、英語、中国語（簡体・繁体）、韓国語
	対応方法	電話、メール
委託者問い合わせ 故障申告	対応時間	365日　24時間
	対応言語	日本語
	対応方法	電話

オ　周知および利用促進

本サービスが利用できるエリアの可視化や接続方法の案内を行うこと。具体的な内容は提案による。なお、認証後のリダイレクト先は別途協議の上決定する。

5　実施体制の確保

本市の求める情報セキュリティを確保するため、下記⑴～⑮の対策を行うための体制を整備し、これを報告すること。

⑴　情報セキュリティ対策等の実施における責任者及び技術担当窓口の者を定めること。また、作業者及び作業場所についても定め、担当の変更があった場合は速やかに委託者へ報告すること。

⑵　受託者において、情報セキュリティに対する意識の向上を図るために、従業員に対し教育を行うこと。

⑶　情報システムの開発を行う場合には、委託者の意図しない変更が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。また当該品質保証体制が書類等で確認できること。

⑷　情報システムに本市の意図しない変更が行われるなどの不正が見付かったときに委託者と受託者が連携して原因を調査・排除できる体制を整備していること。また、当該体制が書類等で確認できること。

⑸　必要が認められる場合に限り委託者の求めに応じ、受託事業者の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・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）・実績及び国籍に関する情報を提供すること。

⑹　委託者から受託者へ提供する情報資産及び受託者によるアクセスを認める情報資産がある場合について、アクセス範囲とアクセス方法を明確化し、機密性・完全性・可変性の確保と目的外利用、必要以上の複製及び配布を禁止すること。また、業務中及び業務を終了した後も、情報の漏えいを防止するために、業務上知りえた秘密を漏らしてはならない旨を定めること。

⑺　情報システムに以下のセキュリティ項目を確保すること。

ア　情報システム等の利用に関する主体認証機能、アクセス制御機能及び権限管理機能

イ　情報システムに関する証跡管理機能

ウ　情報の機密性を確報するための暗号化機能

エ　情報システムへの不正アクセスを防止するためのネットワーク構成

オ　情報システムを構成する機器及びソフトウェアの設定による情報セキュリティ対策の強化

カ　情報システムの稼働状態、セキュリティ侵害等を監視するための機能

キ　情報システムの可用性を確保するための機器、通信回線等の冗長化

⑻　情報システムの運用・保守・点検の実施に際して、利用者管理（主体認証情報の付与、削除）、情報セキュリティ監視、情報のバックアップの取得、監査証跡に関する運用捜査等の情報セキュリティ対策を実施する。

⑼　脆弱性対策として、対象とするソフトウェア、機器等について、下記の手順を実施する。

ア　ソフトウェア開発事業者又は機器等の製造事業者等により公表される脆弱性情報を把握する。

イ　ソフトウェア開発事業者又は機器等の製造事業者等により公表された脆弱性情報の当該情報システム等への影響を調査・評価する。

ウ　当該税癪性に対するセキュリティパッチの提供の有無及びソフトウェア開発事業者又は機器等の製造事業者等が提示する対処方法を調査、把握する。

エ　当該脆弱性への対応方法を定める。なお、セキュリティパッチの提供がある場合は、セキュリティパッチの適用による情報システムへの影響を考慮した上で、影響のない場合は最新のセキュリティパッチを適用する。

オ　当該脆弱性への対応を実施する。

⑽　脆弱性検査を含む情報セキュリティの観点での試験を実施すること。なお、その際は、脆弱性検査ツールや点検基準を用いた第三者による検査の実施を検討し、必要な措置を講ずる。

⑾　情報セキュリティインシデントが発生した場合の報告の体制及び連絡方法を定めること。情報セキュリティインシデントが発生した場合には速やかに委託者へ報告すること。なお、不正アクセス、サービス不能攻撃、不正プログラムの感染等、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、緊急時対策を行うこと。また、情報セキュリティインシデントが発生した場合、住民に対し適正な説明責任を果たすため、当該情報セキュリティインシデントの公表を必要に応じて行うこと。

⑿　情報セキュリティ対策の履行状況について業務の履行状況の報告と併せて月次報告を行うこと。また、必要に応じて委託者による監査を実施する。

⒀　⑿の結果、または情報セキュリティ事故の発生等を契機として受託者による情報セキュリティ対策の履行が不十分である可能性を認識した場合、協議の上で、委託事業の一時中断や損害賠償など、必要な措置を行うことがあること

⑭　本サービスの終了時または受託者による本サービスへの参画が終了した際に不要になった情報資産は委託者へ返還または廃棄すること。

⑮　業務の一部を再委託する場合には、再委託先にも⑴～⑮の内容を順守させること。また、受託者は再委託先の情報セキュリティ対策の実施状況も併せて委託者へ報告すること。

6　納品物

⑴　業務完了報告書・機器仕様書

⑵　提供設備一覧（型番・設置場所）

⑶　運用手順書（障害連絡、窓口、災害時利用モード）

7　その他

⑴　独自手案事項

本業務を実施するにあたり、仕様書に具体的に示す事柄以外に、本業務の趣旨に合致し、かつ大きな効果を見込むことができる独自の取組・手法を示すこと。

⑵　保守・運用

本業務の範囲外であり、別途契約を締結する令和９年２月以降の保守・運用に要する費用について今後の見通しを示すこと。