令和６年（2024 年）度

アクセス認証型ネットワークの構築、

導入及び運用保守業務

別紙１　要件定義書

札幌市教育委員会

内容

1　はじめに

要件定義書（以下「本書」という。）では、アクセス認証型ネットワークの機能要件、非機能要件について示す。

2　機能要件

(1) 要求機能

ア　アクセス認証型ネットワークの要求機能

導入する技術要素を以下とする。

・通信の暗号化技術
・SOC サービス（Security Operation Center サービス）
・IDaaS（Identity as a Service）
・MDM（Mobile Device Management）
・EPP（Endpoint Protect Platform）
・EDR（Endpoint Detection and Response）
・SIEM（Security Information and Event Management）
・DLP（Data Loss Prevention）
・IRM（Information Rights Management）
・SWG（Secure Web Gateway）
・Web フィルタリング
・CASB（Cloud Access Security Broker）
・FWaaS（Firewall as a Service）
・NDR（Network Detection and Response）
・SASE（Secure Access Service Edge）
・SDP（Software Defined Perimeter）

各技術要素に係る要求事項を調達仕様書別紙２「要求機能一覧」に示す。なお、別紙に記載されている機能を実現できること。

なお、要件に対して適合性が低いが、別のオプションや機能等による代替運用により要求内容を満たすことを可とする。

(2) 前提条件

以下に記す前提条件を満たすこと。

ア　前提事項

（ア）導入形態は、クラウド型による提供・利用を前提とすること。

（イ）情報資産の取扱いをクラウドサービス上のみで行うことを原則とする。

（ウ）エージェントのインストール及びバージョンアップ時にOSの再起動を要しないこと。

（エ）本書「２(1)」を実現するにあたりログを収集するサーバ、収集したデータの保管およびその処理について、国内の事業所またはデータセンター内であること。海外のサーバを利用する場合および海外でデータを保管・処理する場合は、合意管轄裁判所を国内とすること。

（オ）監視対象範囲は、調達仕様書別紙３「サービス適用範囲」を参照すること。

（カ）OSサポートは、以下に記載するOSに対応すること。

① Microsoft 社がサポート中の Windows クライアント

② Microsoft 社がサポート中の Windows Server

③ Windows10 Enterprise (64bit)

④ Windows11 Enterprise (64bit)

⑤ Red Hat 社がサポート中の Red Hat Enterprise Linux

（キ）OSバージョンアップに伴う対応は、各 OS ともに新バージョン（メジャーバージョン、マイナーバージョン、機能更新）がリリースされた際は、その正式リリースから２か月以内を目標に対応版をリリースすること。セキュリティパッチ（品質更新）がリリースされた際は、その当日からサポート対象とし、万が一不測の不具合が発生した場合は速やかに対応したサービス・製品をリリースすること。

（ク）ライセンスは、本書「３(2)ア」に記す校務用端末・教育用端末に対し、適用できること。なお、校務用端末・教育用端末以外にセキュリティ製品・サービス適用に必要なライセンスがある場合は、それらを考慮すること。

また、将来的なライセンスの増減にも対応でき、ライセンスの増減（最大１割）において契約変更・追加費用が発生しないことに留意すること。

（ケ）組織再編や人事異動等に伴い発生する監視対象となる端末の入れ替え作業などによる一時的なライセンス超過が発生する（概ね１ヶ月以内の期間において最大１割程度、新旧端末の登録が重複する）場合においても、ライセンス超過による機能停止等が発生せずにサービスを利用することができること。なお、その際の連絡・運用手順は、契約締結後に本市と別途協議のうえ決定することとする。

（コ）監視対象の端末等で収集されたログやアラート対象となるログは最低限１年間保持すること。なお、ログの保存期間により、追加費用が発生しないことに留意すること。

（サ）国内の自治体・政府・民間企業等の組織において、単一組織で 15,000 台を超える導入実績を有する製品であること。

3　非機能要件

(1) 方式

ア　構成に関する全体方針

(ア) アーキテクチャ

クラウドサービスを主体とした方式とすること。

(イ) クラウドサービスの活用方針

① クラウドサービスプロバイダが提供するサービス・機能を最大限活用した構成とすること。

② 要件を満たすため、本市内に機器の設置が必要な場合、付帯機器として導入を行うこと。

③ マルチテナント環境において、特定のクラウド利用者に対して発生したセキュリティ侵害が、他のクラウド利用者に影響を与えないように対策を講じること。

(2) 規模

ア　機器数

校務用端末：約 13,000 台

教育用端末（小中学校、HP 作成用 PC）：298 台

教育用端末（高等学校・特別支援学校、PC 教室等）1,700 台

イ　利用者区分（校務用端末）

1.　札幌市教育委員会（教職員・事務職員他）：29 台

2.　学校等（教職員、事務職員等）：13,000 台

小学校　197 校

中学校　97 校

義務教育学校　2 校

中等教育学校　1 校

高等学校　7 校

特別支援学校　5 校

幼稚園　5 園

計 314 拠点

教育センター（ちえりあ）　1 台

3.　教育ネットワークセンター（札幌総合情報センター）　75 台

ウ　利用者数（職員数等）

教職員・事務職員数　約 11,000 人

児童生徒・園児数　約 140,000 人

小学校　86,707 人

中学校　43,503 人

義務教育学校　100 人

中等教育学校　930 人

高等学校　6,118 人

特別支援学校　341 人

幼稚園　289 人

(3) 性能

調達仕様書別紙２「要求機能一覧」に記す性能に係る内容を参照すること。

(4) 信頼性

ア　可用性要件

導入するサービス・製品の SLO は 99.5%以上であること。

イ　完全性要件

導入するサービス・製品に求める完全性は以下のとおりとする。

① データの滅失や改変を防止する対策

② ログ等の証跡対策

③ データが毀損しないよう、保護する対策

④ 毀損したデータ及び毀損していないデータを特定するための対策

(5) 拡張性

本市が将来的に構築・利用予定である端末・サーバ等に導入したサービス・製品のエージェント等をインストールできること。

(6) 上位互換性

本業務期間中において、導入したサービス・製品の最新バージョンアップ情報が公開された場合は、以下を行うこと。

- バージョンアップ時の影響範囲の整理
- 支障なく利用できることの確認
- OS・併存する他ソフトウェアとの互換性の確認
- 上記を行った上で本市と協議し、本書「(15)エ(ウ)」に示す内容を速やかに行うこと。

(7) 継続性

インシデント発生時の影響の最小化において必須である、検知、通知、調査・対応、復旧のサービスの継続性は以下を原則とすること。

ア　監視に係るサービス提供時間

24 時間 365 日とすること。

イ　インシデント検知に係る報告時間

重要なインシデントが発生していると判断した場合、内容の決定から 60 分以内を原則とし、本市運用管理者へ報告すること。

ウ　インシデント通報に関する問合せ

24 時間 365 日対応可能すること。

エ　インシデント通報に関する報告

影響範囲調査・対応開始を起点とし、翌営業日以内に報告すること。

(8) 情報セキュリティ対策

ア　実施場所

（ア）本業務の実施場所は、原則、受託者のオフィスとすること。なお、機器設置や既設機器への作業実施に際し、本市での作業が発生する場合は、事前に本市担当者の承認を得ること。

（イ）受託者は、本業務の実施場所に、以下に示すような情報漏洩等のセキュリティリスクへの対策を実施すること。

①　許可されていない者の不正な立ち入り（悪意ある者のなりすましによる立ち入りを含む）。

②　端末及び情報の不正な持ち出し。

（ウ）受託者は、本業務の実施場所に対する情報漏洩等のセキュリティリスクへの対策の履行状況に係る調査について、本市担当者から依頼を受けた場合、協力すること。

（エ）受託者は、本書「３(8)ア」で定めた受託者のオフィスと異なる場所からリモートで本業務を実施する場合は、リモート接続する方法及び本書「３(8)イ」に示す情報漏洩等のセキュリティリスクへの対策について、本市担当者の承認を得ること。

イ　端末

（ア）本業務に使用する端末は、受託者が用意すること。なお、本業務の専用とする必要はない。

（イ）本業務に使用する端末は、以下に示すような情報漏洩等のセキュリティリスクへの対策が実施されていること。

①　許可されていない者による不正な操作

②　不正な情報の持ち出しや操作などの内部不正

③　端末の盗難や不正な持ち出し

④　画面に表示された情報の盗み見

⑤　既知及び未知の不正プログラムへの感染

ウ　ネットワーク回線

（ア）ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施すること。

エ　テストデータ

（ア）個人情報及び機密性の高い生データを、テストデータに使用しないこと。

(9) 稼働環境

ア　本業務の基本構成

調達仕様書「１．４　本業務の概要」を参照すること。

イ　施設・設備要件

（ア）　サーバ設置国・合意管轄裁判所

①　ログを収集するサーバ、収集したデータの保管およびその処理について、国内の事業所またはデータセンター内であること。海外のサーバを利用する場合および海外でデータを保管・処理する場合は、合意管轄裁判所を国内とすること。本市の指示によらない限り、一切の情報資産について日本国外への持ち出しを行わないこと。

②　契約の解釈が日本法に基づくものであること。

③　情報資産の所有権が本調達のサービス提供事業者に移管されるものではないこと。

④　法令や規制に従って、本調達のサービス上の記録を保護すること。

⑤　情報資産が残留して漏えいすることがないよう、必要な措置を講じること。

⑥　自らの知的財産権について本調達のユーザに利用を許諾する範囲及び制約を通知すること。

(10) テスト

ア　基本方針

受託者は、以下の基本方針に従い、各テストを実施すること。

（ア）テスト手法及び品質検証の手法は、受託者が他のシステム構築案件において、豊富な成功実績を有する手法を利用すること。

（イ）必要に応じてテストツール、テスト管理ツールを活用し、効率良くテストを実施すること。

（ウ）テスト実施時は、必要に応じてテスト結果を検証するための証跡を採取すること。

（エ）欠陥を検知した場合は、その原因を明らかにすること。

（オ）本市からの要請がある場合には、関連するテスト項目等について、再度テストを行うこと。

（カ）単体テスト、システムテストの実施及び体制・環境・内容・スケジュールをテスト計画書に記載すること。

（キ）テスト項目の洗い出した上で単体テスト仕様書、システムテスト仕様書を作成すること。

（ク）テスト結果について本市から承認の得ること。

（ケ）運用環境への移行に先立ち、脆弱性テストを行い、その結果を確認すること。

イ　テストの種類

本業務で想定するテストの種類を以下に示す。ただし、「ア．基本方針」に示すとおり、テスト手法は受託者が採用する手法に基づくものとし、各テスト工程の考え方や実施内容等について、全体テスト計画時に定義し、本市の承認を得ること。

（ア）単体テスト

セキュリティ製品単体の機能確認（※）テストを実施すること。

※アクセス権限の設定確認、認証確認、レポート出力、各種パラメータ設定値（ログ保管期間、等）等の動作確認

（イ）システムテスト

機能要件を満たすための実現方式を定義した「方式設計」に基づくテストを実施すること。

(11) 移行

ア　共通

(ア) 本番環境へ導入するサービス・製品に係る導入に関する計画を立案すること。立案した内容を『導入計画書』として以下の項目を含めて作成し、本市担当者から承認を得ること。

① 導入実施体制

② 導入環境

③ 導入作業内容

④ 導入スケジュール

⑤ 導入合否判定指針

(イ) サービス・製品の導入にあたり、エージェント等を配布する場合は、方法を検討し、『運用手順書』に含めること。

(ウ) 導入する製品・サービスの設計によって、移行出来ない機能や設定については本市担当者と協議し合意を得ること。

(エ) 情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮すること。

(オ)インストール及びアンインストール（環境の切り戻し）が正常に実施できることは、導入リハーサルにおいて確認すること。

イ　導入リハーサル

(ア) 導入作業を実施する前に、事前に導入手順や導入に要する時間などの測定を目的とした導入リハーサルを実施すること。

(イ) 導入リハーサルの結果は導入リハーサル実施報告書を作成し、本市に報告すること。

(ウ) 導入リハーサルの実施後、導入リハーサルによって得られた知見を活かして、導入計画書の改定を行い、本市の承認を得ること。

(エ) 導入リハーサルの実施結果を踏まえ、必要に応じて修正済みの導入計画書により、改めて導入リハーサルを実施すること。

(12) 引継ぎ

所管するシステムにおいて、システム変更等の作業を行った場合は、アップデート等の作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理すること。

(13) 教育

ア　本市運用管理者向け

本市運用管理者向けに、以下の項目を含む『運用手順書』を作成し、教育を実施すること。教育の実施方法はオンサイトまたはオンラインでの対面方式とし、アーカイブを残すこととする。当該『運用手順書』は日本語で作成すること。

（ア）管理機能を操作するための手順

（イ）運用機能を操作するための手順

（ウ）その他、利用するうえで必要となる管理者手順

（エ）本業務の受託者と本市運用管理者による運用業務の責任分界点、作業分担を区別して記載すること。

イ　端末利用者向け

端末利用者向けに、以下の操作手順書を作成すること。当該『操作手順書』は具体的かつ平易な日本語で作成すること。

（ア）利用するうえで必要となる利用者手順を全て網羅した「操作手順書（詳細版）」

（イ）端末利用者の実務に係る部分を抽出した簡易的な「操作手順書（簡易版）」

(14) 運用

ア　期間

令和８年１月から３月：初期稼働支援

令和８年４月１日から令和 13 年３月 31 日：運用・保守

イ　利用時間

SOC サービスの提供時間は 24 時間 365 日とする。

ウ　運用業務対象

（ア）SOC サービスは EDR、SASE を対象とする。

（イ）運用支援業務を行う時間は原則として開庁日８:45～17:15 とすること。

（ウ）受託者は、運用業務時間を変更する場合は、本市担当者と協議の上、決定すること。

（エ）受託者は、重大なインシデント等の緊急対応が必要な場合は、運用業務時間に限らず保守業務として対応すること。

（オ）クラウド事業者に対して、サービスの一時停止等クラウド利用者に影響があり得る運用手順の有無、有る場合にはクラウド利用者への影響範囲（時間、サービス内容）、連絡方法等について情報提供を求め、クラウド利用者が業務運営に支障がないことを確認し、本市と合意する手順とすること。また、利用するクラウドサービスの提供サービスや利用規約等に変更があった場合、クラウド事業者の設定不備等によるインシデント発生時にも同様の確認をすること。

エ　運用業務内容

（ア）運用実施計画

①　受託者は、初期稼働支援開始までに、初期稼働支援及び運用業務を実施するために必要な『運用計画書』を作成し、本市の承認を得ること。

②　『運用計画書』には、具体的な運用方法や利用するツール、監視対象や閾値、サービスレベル目標（Service Level Objective：以下「SLO」という。）・項目及び指標値の設定、本業務の受託者と本市運用管理者による運用業務の責任分界点、作業分担を記載したうえで本市と協議し、承認を得る

こと。本市と受託者は、合意されたSLOの内容をもって運用業務を実施できるよう計画書を整備すること。

③　『運用計画書』には、初期稼働支援及び運用業務を実施する上で必要となる事項、SOCサービスにおいては、インシデントレベルの段階・内容の定義、インシデントレベル毎の対処方法を記すこと。その際、インシデントの検知方法と報告手順、運用体制と本市への報告手順・方法についても示すこと。

④　『運用計画書』に記載された体制をやむを得ない理由により変更する場合には、事前に本市担当者の承認を得ること。

⑤　『運用計画書』に記載された事項を変更する場合には、本市担当者の承認を得た上で改訂を行うこと。なお、変更にあたっては改訂履歴を残すこと。

⑥　自然災害、大規模又は広範囲に及ぶ疾病等に備えた業務継続を目的として、「運用計画書」にセキュリティ製品のサーバが長期間機能しなくなった場合の各機能の稼働可否を整理し対応を記載すること。

（イ）問い合わせ・調査依頼対応

①　受託者は、問い合わせ窓口対応業務として、本市担当者からの問い合わせに対応すること。なお、問い合わせ業務は、電話・電子メール等の利用手段を本市担当者と協議し決めること。

②　受託者は、導入したサービス・製品の提供者（サービスプロバイダ・開発元・製造元等を指す）へ問合せを行い、問合せ状況について本市担当者へ報告すること。

③　受注者は、問い合わせ内容と対応した結果について、その内容を記録の上、月次報告書にて対応状況を報告すること。

④　受注者は、本市担当者からデータの提供を要求された場合は、速やかに対応すること。

（ウ）ログ管理

①　監視対象の端末等で収集されたログやアラート対象となるログは1年間保持可能であること。

②　受託者は、保存対象ログの取り出しについて、本市担当者から依頼・指示を受けた場合は、速やかに対応すること。

（エ）変更管理

① 受託者が設定変更及び設計変更等を行った場合、各種設計書及び「3.(13)教育」で定義したマニュアルを随時更新し、本市担当者の承認を得ること。

② 本市が設定変更及び設計変更等を行った場合も、各種設計書及び「3.(13)教育」で定義したマニュアルを随時更新し、本市担当者の承認を得ること。

（オ）運用業務報告

① 共通

- 受託者は、本市担当者に対して「月次報告」を満たす報告を行うこと。
- 本業務の報告におけるコミュニケーションは、『運用計画書』で合意した手段を用いること。
- 受託者は、SOC サービスにおいては、インシデント発生時の影響の最小化において必須である、検知、通知、調査、対応、復旧のサービスを提供し、影響範囲調査・対応開始を起点とし、翌営業日以内を原則とし、本市管理者へ報告すること。
- 「月次報告」で用いる報告書については、原則電子媒体とする。
- 判定されたインシデントレベルに応じて、導入した製品・サービスから本市運用管理者へメール、電話による通知すること。
- 月次レポートの情報共有及び運用の最適化を目的とした打ち合わせに対応すること。

② 月次報告

- 受託者は、月次報告会議を開催すること。開催頻度は令和７年度は月次を想定し、令和８年度以降は本市と協議のうえ、決定すること。
- 月次報告会議では、「月次報告書」を作成した上で、業務の進捗状況を報告すること。
- 「月次報告書」の報告事項には以下を含めること。なお、報告事項は本市担当者と協議の上、適宜見直しを行うこと。
  - ・月内に発生したアラートの統計情報
  - ・月内に発生したアラートの対応結果のサマリー
  - ・緊急度の高いインシデント関連情報

③ ドキュメント管理

・　受託者は、本業務に関連するドキュメントを最新に保ち、改版履歴はドキュメントに記録するとともに、月次報告で報告すること。

（カ）その他

サービスを終了若しくはサービス利用契約終了後は、保有データを本市へ提供したのち、速やかにシステムから消去すること。消去においては、復元不可能な状態にすること。また、各種データについて、複製複写物は保持しないこと。

また、その他本業務にて必要と思われる運用事項については「設計」工程にて、本市担当者と協議すること。

(15) 保守

ア　保守期間

令和８年４月１日から令和 13 年３月 31 日

イ　対応時間と受付方法

対応は日本語で行うこととし、依頼の受付は、24 時間 365 日にて対応すること。

ウ　保守対象

本業務で監視対象としている端末等やそれらに付随するソフトウェアおよび機器類全般とする。

エ　保守業務

（ア）インシデント対応、隔離、隔離解除（SOC サービス）

①　重要なインシデントが発生していると判断した場合、内容の決定から 60 分以内を原則とし、本市運用管理者へ報告すること。

②　判定されたインシデントレベルに応じて、本市運用管理者へメール、電話による通知が可能なこと。

③　判定されたインシデントレベルに応じて、脅威（検体）や被疑端末等の隔離措置が可能なこと。また、隔離実行の判断は本市ではせず、基本的には隔離。誤検知の場合は隔離解除とすること。

④　インシデント対応完了後に隔離解除を実施し、隔離解除した旨を運用管理者が判断できるよう、メール、電話による隔離承認が可能なこと。

（ウ）バージョンアップ対応

① 受託者は、全ての利用者に影響があるバージョンアップについて、本市担当者から指示を受けた場合、影響範囲が最小限となるようにスケジュールを調整した上で、実施すること。なお、影響範囲によっては本市担当者と協議の上、業務時間外での対応を行うこと。

② 受託者は、バージョンアップを実施する際、事前に作業申請を本市担当者に提出し、承認を得ること。なお、作業申請は原則として、作業日の５開所日前までに承認を得ること。

③ 受託者は、開発・保守用のソフトウェア等を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認すること。

オ　その他

電磁的記録媒体を内蔵する機器を本業務で導入後に修理、廃棄、リース返却等が発生する場合について、本市情報資産の取扱いを事前に本市と協議し合意のうえ、適切に対応すること。

その他、本業務にて必要と思われる保守事項については「設計」工程にて、本市担当者と協議すること。

以 上