令和５年（2023 年）度

EDR を利用した SOC サービスの設計、構築、導入及び運用保守業務

調達仕様書

札幌市

内容

1　調達案件の概要

(1) 調達件名

EDR を利用した SOC サービスの設計、構築、導入及び運用保守業務

(2) 調達の背景

本市は、総務省「地方公共団体における情報セキュリティポリシーに関するガイドライン（令和２ 年 12 月版）」にて示された「三層の対策」のβ′モデルへの移行を決定し、インターネット接続系での業務端末の運用を行うこととなったが、ガイドラインで示されている要件を満たすため、SOC サービスを調達する必要が出てきた。

(3) 調達目的及び調達の期待する効果

本業務は、総務省が実施した、地方自治体の庁内ネットワークにおけるいわゆる「三層の分離」の見直しを受け、本市では別途運用している Microsoft 365 を始めとする各種クラウドサービス等をさらに活用すべく、庁内ネットワークの「β´モデル」への移行を予定している。しかしながら、本市の庁内ネットワークの一つでありメインの業務ネットワークであるイントラネット（インターネット接続系とは分離状態）に属する業務用 FAT 端末（以下、「イントラネット端末」という。）及び業務システムサーバ等を新たに構築予定のインターネット接続系環境（以下、「NEWS(NEw Work Style)ネット」という）のネットワークへ一斉に移行することは困難であり、ある程度の期間をかけて段階的に移行を実施することを決定した。そうしたことから、NEWS ネットにイントラネット端末を移行できていない一部の職員がインターネット接続系で各種業務を行うためのツールとして、令和６年１月運用開始を目標に、イントラネット端末からリモート接続して利用する「クラウド型仮想デスクトップ」を新たに導入することとした。この「クラウド型仮想デスクトップ」上で実行される「デスクトップ及びアプリの仮想化サービス（Azure Virtual Desktop）」（以下、「AVD」という）及び「NEWS ネットへある程度の期間をかけて段階的に移行する業務用 FAT 端末」（以下、「NEWS ネット端末」という）へエンドポイント防御（以下「EDR」という。）を利用した SOC サービスを適用することで、扱う情報資産の機密性に応じた在宅ワーク、モバイルワークが可能となり、セキュリティリスクの減少やクラウド活用による Web 会議やビジネスチャット等に

よるコミュニケーションツールの充実を図れる環境を早期に構築することを目的とする。

(4) 本業務の概要

令和６年１月運用開始予定の「AVD」及び「NEWS ネット端末」を監視対象とするEDR を利用した SOC サービスの提供のための EDR 製品の導入を含む SOC サービスの設計、導入、導入後の運用設計及び運用等の作業を行う業務である。

求める要件の詳細は、本書「３　本業務に求める要件」を参照すること。

なお、サービスの適用イメージは次のとおりである。

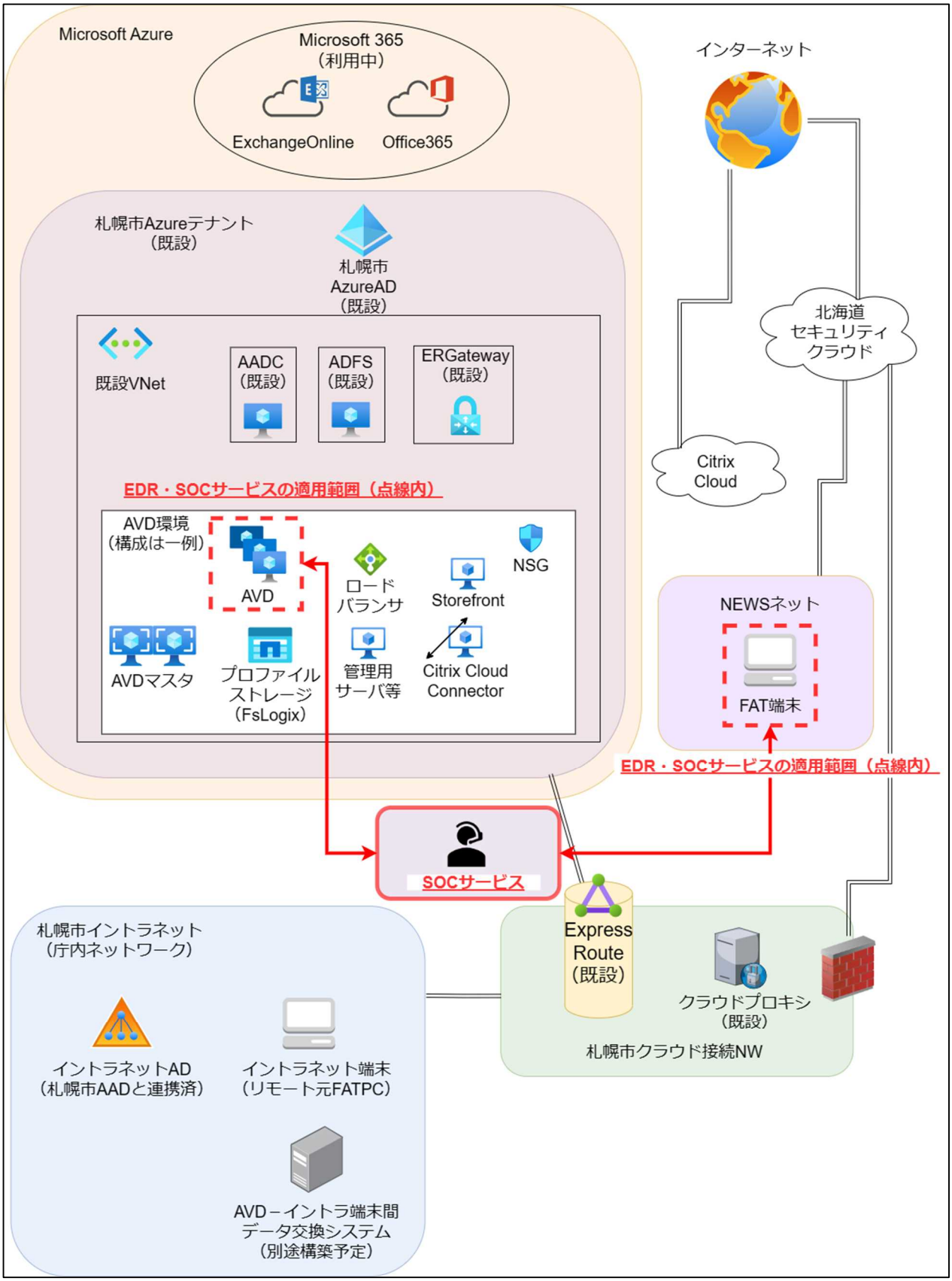

図 1-1 サービス適用イメージ

(5) 契約期間

契約締結日から令和６年 12 月 31 日まで

なお、EDR 製品のライセンス利用期間は次のとおりを想定している。

・令和５年 11 月 1 日から令和６年 12 月 31 日

(6) 作業スケジュール

作業スケジュール上のマイルストーンを以下に示す。

なお、マイルストーンを基準として本書「４(3)ア(ア)」に記載のプロジェクト計画書の作成作業の中で、スケジュール計画を立案すること。

ア　令和５年 11 月 17 日：導入完了

イ　令和５年 11 月 20 日：初期稼働支援開始

ウ　令和６年１月１日：運用・保守開始

2　本調達案件及び関連調達案件の実施時期

(1) 調達案件及び関連調達案件の調達単位

本業務及び本業務と関連する調達案件の実施時期を以下に示す。

表 2-1　調達案件一覧

No.	調達案件名	案件概要	実施時期	補足
1	EDR を利用した SOC サービスの設計、構築、導入及び運用保守業務	本書「１(4)」参照	入札告示：令和５年７月下旬 落札者決定：令和５年８月下旬	本業務
2	クラウド型仮想デスクトップ環境提供業務	イントラネットから NEWS ネットへの移行期のツールとして、仮想デスクトップ環境を提供する業務	入札告示：令和４年２月 17 日 落札者決定：令和５年４月 10 日	
3	NEWS ネット環境提供業務（予定）	「β´モデル」移行に際して、NEWS ネット環境を提供する業務	未定	
4	NEWS ネット環境に係る運用・保守業務（予定）	NEWS ネット環境の稼働監視、障害検知と対処、ユーザの管理等を行う業務	未定	

(2) 調達案件間の入札制限

「表 2-1　調達案件一覧」に示す調達案件間の入札・提案制限は特にない。

3　本業務に求める要件

本業務の実施に当たっては、別紙１「要件定義書」の各要件を満たすこと。

4　作業の実施内容

(1) 作業内容

ア　全体管理

(ア) プロジェクト管理

①　『プロジェクト計画書』を作成し、本市担当者の承認を受けること。『プロジェクト計画書』には、「表 6-1　提出書類一覧」に記載された項目を含めること。

②　『プロジェクト計画書』の作成は契約締結後速やかに実施すること。計画内容に変更が生じた場合は、修正案を遅滞なく本市担当者に提示し、承認を得たうえで変更すること。また、「運用・保守」にて変更が生じた場合も同様の方法で修正を行うこと。

③　本市が別途委託する「クラウド型仮想デスクトップ環境提供業務」の受託者及び「NEWS ネット」構築事業者に対し、本業務の課題状況を共有すること（関連する他業務の受託者とのコミュニケーション計画は、「プロジェクト計画書」の中で定義すること。）。個別に検討が必要な課題等が発生した際にも、「プロジェクト計画書」で定めるコミュニケーション計画に従い、その必要に応じて適宜情報共有すること。

イ　設計・導入

以下に記す内容は「AVD」及び「NEWS ネット端末」を作業範囲とすること。なお、各作業におけるドキュメントは、作成途中及び完成前の適切なタイミングで本市担当者のレビューを受け、作業を進めるにあたっての承認を受けること。

(ア) 方式設計

①　「別紙１　要件定義書」の機能要件を満たすための実現方式を設計し、『方式設計書』及び『各種構成図』を作成すること。他業務に影響がある部分は、本市や関係する受託者と十分協議すること。

(イ) 環境設計

①　方式設計に基づき、EDR 管理コンソールで設定する各種設定値の設計を行い、『環境設計書』を作成すること。他業務に影響がある部分は、本市や関係する受託者と十分協議すること。

② EDR 及び SOC サービスの利用を開始するための各種申請書の作成支援を行うこと。

（ウ）運用実施計画の立案

① 運用業務を実施するために必要な『運用計画書』を作成すること。他業務に影響がある部分は、本市や関係する受託者と十分協議すること。

（エ）運用設計

① EDR、SOC サービス に関する運用項目の洗い出しを行うこと。

② 『運用計画書』に基づき、運用項目ごとの作業フロー、本市と受託者との役割分担、参照する手順書等を記載した『運用設計書』を作成すること。

③ 運用設計に基づき、『運用手順書』を作成すること。他業務に影響がある部分は、本市や関係する受託者と十分協議すること。

④ 『運用手順書』には、以下の要素を記載すること。

- 「AVD」及び「NEWS ネット端末」に対する EDR クライアントのキッティングの手順
- 運用上必要な環境上の設定等の手順
- 将来的に EDR 製品が変更になった場合のアンインストールの手順

（オ）導入計画の立案

① 導入について、スケジュールや手順を整理し、『導入計画書』としてまとめること。

② 導入方法は、本市が別途委託する「クラウド型仮想デスクトップ環境提供業務」の受託者と協力のうえ、利用者の操作負担を最小化するよう配慮すること。

③ 展開スケジュールは、本市のネットワーク負荷や業務に支障が無いよう、異なる日程の複数ステップで行う計画とし、詳細は本市担当者と協議の上、決定するものとする。

（カ）環境構築

① 『環境設計書』に基づき、EDR 管理コンソール等のセットアップ作業を行うこと。

(キ) テスト

① 本市が用意・指定する「テスト用仮想デスクトップ端末」及び「テスト用NEWS ネット端末」に EDR クライアントを展開すること。

② 「テスト用仮想デスクトップ端末」及び「テスト用 NEWS ネット端末」を用いて、単体テスト、システムテストを行うこと。なお、単体テスト、システムテストについて、テスト体制、テスト環境、作業内容、作業スケジュール、合否判定基準等を記載した『テスト計画書』を作成し、本市担当者の承認を受けること。

③ EDR の単体動作確認を行うためのテスト項目を洗い出し、『単体テスト仕様書』を作成すること。

④ EDR の方式設計に関する動作確認を行うためのテスト項目を洗い出し、『システムテスト仕様書』を作成すること。

⑤ テスト結果については次フェーズのテスト開始前に本市担当者に提出し、完了の承認を得ること。

(ク) 導入

① 本番環境への EDR 導入に関するスケジュールや作業手順等を記載した『導入計画書』を「クラウド型仮想デスクトップ環境提供業務」及び、今後本市が調達を予定する「NEWS ネット環境提供業務」の受託者へ連携のうえ、EDR 導入作業の支援を行うこと。なお、適宜情報共有を密に行い、滞りなく導入できるよう作業を実施すること。

② EDR の導入作業期間は、令和５年 10 月～11 月の２か月間を想定すること。

(ケ) 教育

① 端末利用者や本市運用管理者それぞれが行うべき手順をまとめた『運用手順書』を作成すること。

② 本市運用管理者向けに EDR を利用するうえで必要となる『操作手順書』及び教育を実施すること。

ウ　初期稼働支援

（ア）初期稼働支援

①　EDR 導入後の稼働支援を行うこと。

②　過検知・誤検知の整理、また、必要に応じてチューニングを行うこと。

③　稼働支援期間中の本市担当者からの問い合わせに対し回答を行うこと。

④　必要に応じてオンサイトでの調査、切り分け、ログ採取等を行うこと。

⑤　EDR 管理コンソールの設定値チューニングを行うこと。

エ　運用・保守

（ア）サポート

①　EDR メーカーと密に連携し、サービス開始後の諸問題に迅速に対応すること。

（イ）問合せ・障害対応

①　サービス開始後の本市担当者からの問い合わせ、調査依頼を受け付け、対応・回答を行うこと。

（ウ）バージョンアップ対応

①　新しいバージョン及びセキュリティパッチ（品質更新）がリリースされた際は、適用の影響を確認したうえで、可能な限り速やかにバージョンアップすること。

②　バージョンアップ方法については、本市担当者と協議して決定すること。

③　バージョンアップ対応・展開作業は、以下のとおり対応すること。

・　「AVD」：「クラウド型仮想デスクトップ環境提供業務」の受託者が実施するものとし、本業務ではバージョンアップに必要な情報を『運用手順書』に記載し、「クラウド型仮想デスクトップ環境提供業務」の受託者へ連携のうえ、作業の支援を行うこと。

・「NEWS ネット端末」：「NEWS ネット環境に係る運用・保守業務」の受託者が実施するものとし、本業務ではバージョンアップに必要な情報を『運用手順書』に記載し、「NEWS ネット環境に係る運用・保守業務」の受託者へ連携のうえ、作業の支援を行うこと。

④　事前に展開スケジュールやアップデート手順等を本市担当者に提示すること。なお、OS のライフサイクルサポートが終了した際には、新 OS への入替に対応すること。

（エ）運用報告

本報告については、令和５年度は月次の定例会にて、運用実績を報告すること。定例会の資料は電子ファイルの形式で提出すること。また、定例会には、本市からの機能改善などの要望をくみ取る仕組みを設けること。令和６年度以降は本市と協議のうえ、決定すること。

（オ）引継ぎ

令和６年 11 月から 12 月の期間は、運用・保守作業と並行して、令和７年１月以降に別途調達・契約する運用・保守業務の受託者に対し、必要な「設計・導入」及び「運用・保守」の内容、成果物等の引継ぎを行うこと。なお、引継ぎに際して、以下を留意すること。また、引継ぎにかかる費用は受託者が負担すること。

①　円滑かつ効率的な運用・保守の実施

運用・保守業務の受託者に対して、成果物に関する以下を主とした事項に留意し実施すること。

・　課題・リスクに係る引継事項
・　業務特性及び EDR 製品・SOC サービスの特性に伴う個別の引継事項
・　ライセンス関連情報

上記以外の留意事項は、本市と協議のうえ、決定及び実施すること。

② 公正性及び競争性の担保

運用・保守業務にて、改変（仕様の変更、追加を伴う機能改修、各種設定値の変更・追加等）が発生した際に、いわゆるベンダーロックインに陥ることなく、本市及び運用・保守業務の受託者が自由に改変を行えることを担保すること。また、以下を主とした事項に留意すること。

- EDR 製品・SOC サービスの特性に伴い、技術的な専門用語を使うときは、本市及び運用・保守業務の受託者がその用語に理解があるかを確認し、理解がなければ事前に用語集等を整備すること。
- EDR 製品・SOC サービスの特性に伴い、特殊な仕様を設計した場合、その設計理由を明記すること。
- 上記に記す内容を「表 6-1 提出書類一覧」の各項に記載された内容へ含めること。

上記以外の留意事項は、本市と協議のうえ、決定及び実施すること。

5　作業の実施体制・方法

(1) 作業実施体制

ア　本業務全体の実施体制

本業務における本市の実施体制を以下に示す。

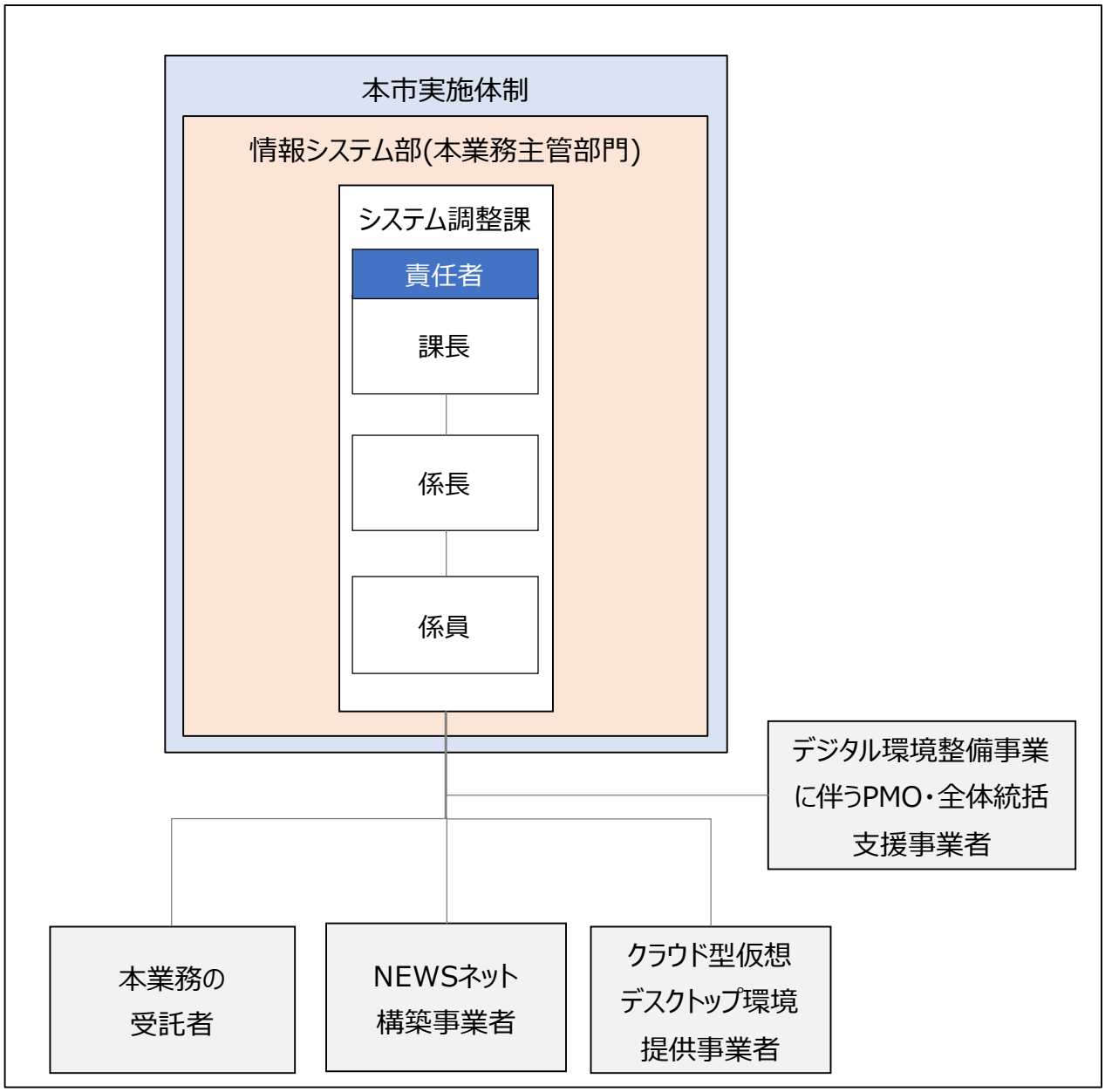

図 5-1　本業務の推進体制

本市情報システム部（以下、「本市主管部門」という。）が本業務を推進し、本市の関係部門や関連事業者との連携を行う想定であるが、本業務の受託者においても、本業務の円滑な推進のため、主体的に関係部門、関係事業者との連携を図ること。ただし、他業務の受託業者と連絡調整、情報共有を行う場合は、必ず本市主管部門を介すこと。

（ア）図 5-1 に記載された他の事業者と、本市主管部門を通じて緊密な連携をとり、常に相互に最新の情報を共有すること。なお、「デジタル環境整備事業に伴う PMO・全体統括支援事業者」は、本市主管部門を補助する役割である。そのため本業務の受託者に対して、本市主管部門を補佐し、または代理して進捗状況の確認や、問題が発生した場合の支援を行うことがあるので留意すること。

（イ）本市主管部門と連携した上で、関連事業者や関係部門からの求めに応じて、資料の提示やヒアリング対応、質問に対する回答や指摘事項に対して協力すること。

（ウ）本書に記載のない細部事項、プロジェクト計画書に記載のない事項、業務上の問題点等については、本市主管部門と協議し、その指示に従うこと。

イ　受託者の実施体制

本業務の受託者は本業務を効率良く実施できるよう、以下に示すプロジェクト体制を整備すること。

（ア）本業務の実務の責任者として、業務責任者（プロジェクトの実施主体として進捗・課題管理等を行い、本市への報告窓口となる役割を担うプロジェクトマネージャ）を配置すること。

（イ）本業務に携わる本市や関連事業者等、全ての者を含む体制図をプロジェクト計画書に明示すること。

（ウ）担当者の交代、担当者の増員及び減員がある場合は、体制図を更新するとともに、速やかに本市に報告すること。

(2) 作業要員に求める資格等の要件

ア　業務統括責任者

経済産業大臣が認定するプロジェクトマネージャ、または 米国 PMI (Project Management Institute) が認定する PMP (Project Management Professional) の有資格者、または同等以上の資格または経験を有する者とすること。

イ　業務責任者

本業務と同等規模や類似案件におけるプロジェクト責任者としての実績を有していること。なお、当該実績を有しない場合においては、PMP の有資格者、または同等以上の資格を有する者を業務責任者として配置することを可とする。

(3) 作業場所

本業務の作業場所及び作業に当たり必要となる設備、備品及び消耗品等については、受託者の責任において用意すること。なお、セキュリティ保全状況の確認のため、本市の担当者が現地確認を実施することがあるので留意すること。

(4) 作業の管理に関する要領

受託者は、本市が承認した『プロジェクト計画書』の作業体制、スケジュール等に従い、記載された提出書類を作成すること。その際、『プロジェクト計画書』に従い、コミュニケーション管理、体制管理、作業管理、品質管理、リスク管理、課題管理、システム構成管理、変更管理、情報セキュリティ対策を行うこと。

6　提出書類

(1) 提出書類の範囲、納入記述等

本業務における提出書類を「表 6-1　提出書類一覧」に示す。また、本市との協議により必要と判断された提出書類が生じた際には、別途提出すること。

表 6-1　提出書類一覧

No.	提出書類	内容	提出時期	提出方法
1	業務着手届 業務責任者指定通知書 情報資産取扱者知書 (従事者名簿) セキュリティ保全に関わる文書	業務開始時に提出する契約書類文書。 業務責任者指定通知書、情報資産取扱者知書(従事者名簿)には、業務統括責任者、業務責任者に定めた者の氏名を記すこと。	契約締結後、業務着手までの間	各１部を１冊に綴り、袋とじしたうえ、表紙・裏表紙に１か所ずつ割印する。
2	公的な資格や認証等の取得に関する書類	本書「７(1)から７(4)」に該当していることを証する書類。	契約締結後、業務着手までの間	別途定める。
3	プロジェクト計画書	本業務に係る作業内容、作業体制、スケジュール（WBSを含む）、成果物、適切に遂行するためのコミュニケーション管理、進捗管理、品質管理、リスク管理、課題管理、変更管理、セキュリティ管理等を定めた文書。	契約締結日から2週間以内	別途定める。
4	プロジェクト計画書に基づく管理資料、進捗報告書	プロジェクト計画書に基づく進捗報告書、品質報告書、課題管理台帳、リスク管理台帳等の各種管理資料及び報告資料。	随時（原則毎週）	別途定める。

No.	提出書類	内容	提出時期	提出方法
5	各種会議資料	受託者が主催する会議体における配布資料一式。	随時 ※原則として会議の前日までに電子ファイルをメールで納品	電子データ
6	方式設計書	機能要件・非機能要件を満たすための方式設計を記す。	令和5年11月17日	別途定める。
7	各種構成図	以下に示す構成図を記す。 ・　ネットワーク構成図 ・　ソフトウェア構成図 ・　ハードウェア構成図	令和5年11月17日	別途定める。
8	環境設計書	方式設計に基づき、EDR管理コンソールで設定する各種パラメータを記す。	令和5年11月17日	別途定める。
9	運用計画書	初期稼働支援、運用・保守期間における作業計画を示す。	令和5年11月17日	別途定める。
10	運用設計書 運用手順書	非機能要件を満たすための運用設計を記す。詳細は「別紙１ 要件定義書」を参照すること。	「運用・保守」開始前	別途定める。
11	導入計画書	本番環境へのEDR導入に関するスケジュールや作業手順を記す。以下の項目を含めること。 ・　導入実施体制 ・　導入環境 ・　導入作業内容 ・　導入スケジュール ・　導入合否判定指針	「環境構築」開始前	別途定める。
12	操作手順書	本市管理者向け及び端末利用者向けのEDRの管理・運用機能を操作するための手順、EDRを利用するうえで必要となる手順を記す。	「運用・保守」開始前	別途定める。

No.	提出書類	内容	提出時期	提出方法
13	テスト計画書	実施予定のテストに関する計画を記す。以下の項目を含めること。 ・　テスト実施体制 ・　テスト環境 ・　作業内容 ・　作業スケジュール ・　合否判定指針	「環境構築」開始前	別途定める。
14	テスト仕様書・成績書	単体テスト、総合テストの具体的な内容、方法とその結果を記す。テスト結果については次フェーズのテスト開始前に本市担当者に提出し、完了の承認を得ること。	テスト仕様書：各テスト実施前 テスト成績書：次フェーズのテスト開始前	別途定める。
15	セキュリティ保全状況報告書	受託業務の履行にあたり、情報セキュリティ対策の履行状況の報告書。	毎月末	別途定める。
16	その他、本市が必要とする資料等	契約後、本市担当者と協議の上、決定する。		別途定める。
17	業務完了届 成果品目録	業務完了時に提出する契約書類文書。	業務完了と同時	別途定める。

(2) 納品方法

ア　提出書類は、全て日本語で作成すること。

イ　情報処理に関する用語の表記については、日本産業規格（JIS）の規定を参考にすること。

ウ　提出書類は紙媒体及び電磁的記録媒体により作成し、本市から特別に示す場合を除き、電磁的記録媒体は１部を納品すること。

エ　紙媒体による納品について、用紙のサイズは、原則として日本産業規格A列４番とするが、必要に応じて日本産業規格A列３番を使用すること。

オ　電磁的記録媒体による納品について、Microsoft Office又はPDFのファイル形式で作成し、CD-R等の電磁的記録媒体に格納して納品すること。

カ　納品後、本市において改変が可能となるよう、図表等の元データも併せて納品すること。

キ　提出書類の作成に当たって、特別なツールを使用する場合は、本市担当者の承認を得ること。

ク　提出書類が外部に不正に使用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、提出書類の情報セキュリティの確保に留意すること。

ケ　電磁的記録媒体により納品する場合は、不正プログラム対策ソフトウェアによる確認を行うなどして、提出書類に不正プログラムが混入することのないよう、適切に対処すること。なお、対策ソフトウェアに関する情報（対策ソフトウェア名称、定義パターンバージョン、確認年月日）を記載したラベルを貼り付けること。

(3) 納品場所

原則として、提出書類は次の場所において引渡しを行うこと。ただし、納品場所を別途指示する場合はこの限りではない。

札幌市白石区菊水１条３丁目１番５号 菊水分庁舎

札幌市デジタル戦略推進局情報システム部システム調整課

7　公的な資格や認証等の取得に関する事項

応札する事業者または提供する EDR 製品及び SOC サービスのいずれかで以下を満たしていること。

(1) 以下のいずれかの認証を受けている、取得していること。

ア　品質管理体制について、ISO9001:2008 又は ISO9001:2015

イ　組織としての能力成熟度について CMMI レベル 3 以上

ウ　プライバシーマーク付与認定

エ　ISO/IEC 27001 認証（国際標準規格）

オ　JIS Q 27001 認証（日本工業標準規格）

(2) 情報セキュリティサービス基準適合サービスリストに適合していること。

(3) 日本政府が求めるセキュリティ要件を満たした「政府情報システムのためのセキュリティ評価制度（ISMAP：Information system Security Management and Assessment Program）」又は 、「政府情報システムにおけるクラウドサービスの利用にかかる基本方針 4 補足 4.1 ISMAP 以外のクラウドセキュリティ認証等」に示される以下を取得していること。

ア　認証制度

（ア）ISO/IEC 27017（クラウドサービスセキュリティ管理策）による認証取得

（イ）JASA クラウドセキュリティ推進協議会ゴールドマーク

（ウ）FedRAMP（米国政府機関におけるクラウドセキュリティ認証制度

イ　監査フレームワーク

（ア）AICPA SOC2（日本公認会計士協会　IT7 号）

（イ）AICPA SOC3（SysTrust/WebTrsuts）（日本公認会計士協会　IT2 号）

(4) 以下の第三者評価機関から２つ以上の評価・実績を有していること。

ア　MITRE ATT&CK ：Attack Evaluations - Enterprise Evaluations の過去 4 回（2018-2022）のいずれかに参加していること。

イ　AV-TEST ：Approved の評価を受けていること。

ウ　AV-Comparatives ：Approved の評価を受けていること。

エ　SE Labs ：AAA　の評価を受けていること。

(5) その他、入札説明書の入札参加資格に記載の条件を満たすこと。

8　留意事項

(1) 本仕様書の内容に関して疑義が生じた場合必ず本市と協議し、承認を得ること。なお、協議の内容については書面に記録し提出するものとする。

(2) 業務履行上やむを得ずサービスの停止を必要とする場合は事前に本市と協議し、日時及び期間を決定すること。

(3) 過失によりサービスに影響を与えた場合はすみやかに本市へ報告し、本市指示のもと受託者の責任において復旧作業を行うこと。

(4) 本業務の遂行にあたり、受託者は業務上知り得た事項を本業務の目的以外に使用又は第三者に開示若しくは外部漏洩してはならないものとし、そのために必要な措置を講ずること。

(5) 本業務の一部を再委託する場合には、その必要性や再委託先に対する管理体制等を説明したうえで本市の承認を受けること。また、受託者は、再委託先の行為について一切の責任を負うものとする。

(6) 受託者は、受託者の責任によって生じたソフトウェアの欠陥及びこれに起因するシステム障害、データ破壊並びに各種仕様書などのドキュメントの表記誤りについては、その事実を知った日から1年間は無償で修正等対応すること。

(7) 本業務の一部を合理的な理由及び必要性により再委託する場合には、委託者の承認を受けること。また、受託者は、再委託先の行為について一切の責任を負うものとする。

(8) この仕様書に定めのない事項については、双方で協議するものとする。

９　環境への配慮

(1) 本業務においては、環境関連法令等を遵守するとともに、本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。

(2) 電気、水道、油、ガス等の使用にあたっては、極力節約に努めること。

(3) ごみ減量及びリサイクルに努めること。

(4) 両面コピーの徹底やミスコピーを減らすことで、紙の使用量を減らすよう努めること。

(5) 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。

(6) 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。

１０　附属文書

(1) 別紙１　要件定義書

(2) 別紙２　EDR 要求機能一覧

(3) 別紙３　SOC サービス要求機能一覧

以 上

令和５年（2023 年）度

EDR を利用した SOC サービスの設計、構築、導入及び運用保守業務

別紙１　要件定義書

札幌市

内容

1　はじめに

要件定義書（以下「本書」という。）では、EDR 及び SOC サービスの機能要件、非機能要件について示す。

2　機能要件

(1) 要求機能

ア　EDR 及び SOC サービスへの要求機能

要求機能を以下に示す。

（ア）別紙２ EDR 要求機能一覧

（イ）別紙３ SOC サービス要求機能一覧

なお、上記に記載されている機能を実現できること。

(2) 前提条件

前提条件については、以下に記す前提条件を満たすこと。

ア　EDR

（ア）導入形態は、脅威への迅速な対応のために、クラウド型の EDR サービスの利用を前提とすること。

（イ）EDR の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。

（ウ）監視対象範囲は、本市が利用予定である「クラウド型仮想デスクトップ」上で実行される「デスクトップおよびアプリの仮想化サービス（Azure Virtual Desktop）」（以下、「AVD」という。）及び「NEWS ネットへある程度の期間をかけて段階的に移行する業務用 FAT 端末」（以下、「NEWS ネット端末」という。）とする。また、監視対象に EDR のエージェントをインストールし、サーバとエージェントを連携させること。

（エ）通信暗号化は、端末と管理サーバ間の通信は暗号化されていること。

（オ）導入実績は、調達仕様書「７(2)」を満たすこと。

（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 マルチセッション版の Windows10 Enterprise（64bit）

④ マルチセッション版の 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製品をリリースすること。

（ク）ライセンスは、本市が利用予定である「AVD」（マルチセッション接続に対応し、１台に対して６ユーザの接続を予定しているが、検討結果により変更となる可能性もあり）及び「NEWS ネット端末」に対し、最大で 16,500 台に適用できること。利用端末を「AVD」から「NEWS ネット端末」に変更した利用者は「AVD」を利用しなくなるため、最終的に「AVD」の利用は、3,000 名程度となる想定である。また、将来的なライセンスの増減にも対応できること。

（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（概ね一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。

イ SOC サービス

（ア）監視対象の端末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。

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。

(2) 規模

ア　機器数及び設置場所

本市が利用予定である「AVD」及び「NEWS ネット端末」に EDR のエージェントをインストールし、サーバとエージェントを連携させること。

イ　利用者区分及び利用者数

本市職員のほぼ全数にあたる、最大で 16,500 名

(3) 性能

有人監視による SOC サービスにて「早期対応が必要」或いは「攻撃が成功した可能性が高い」に該当した緊急度の高い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できること。

(4) 信頼性

ア　可用性要件

クラウドサービスの可用性に関する SLO は 99.5%以上であること。

イ　完全性要件

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

「NEWS ネット」上に存在する認証基盤(Active Directory)、本市が将来的に構築・利用予定である集中ファイルサーバ、庁内データ交換フォルダ等のサーバ群に EDR のエージェントをインストールし、サーバとエージェントを連携できること。

(6) 上位互換性

本業務期間中において、EDR 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
- 「AVD」及び「NEWS ネット端末」を支障なく利用できることの確認
- 「AVD」及び「NEWS ネット端末」の 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

SOC サービスの提供時間は 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

(9) 稼働環境

ア　本業務の基本構成

調達仕様書「1 (4)」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　EDR の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。

(イ) 技術的条件

調達仕様書「7 (1)」に記載した条件を満たすこと。

(10) テスト

調達仕様書「4 (1)イ(キ)」に記載したテストを実施すること。テストには以下の項目を含めること。

・　単体テスト

・　システムテスト

(11) 移行

ア　共通

(ア) 本番環境への EDR 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。

- 導入実施体制
- 導入環境
- 導入作業内容
- 導入スケジュール
- 導入合否判定指針

(イ) EDR の導入にあたり、EDR を配布する方法を検討し、『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。

(12) 引継ぎ

調達仕様書「４(1)エ(オ)」に記載した条件を満たすこと。

(13) 教育

ア　本市管理者向け

本市管理者向けに、以下の項目を含む『操作手順書』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する。当該操作手順書は日本語で作成すること。

(ア) EDR の管理機能を操作するための手順

(イ) EDR の運用機能を操作するための手順

(ウ) その他、EDR を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、以下の項目を含む「各種マニュアル」を作成すること。当該『操作手順書』は日本語で作成すること。

（ア）EDR 利用するうえで必要となる端末利用者手順

(14) 運用

ア　期間

令和５年 11 月から 12 月：初期稼働支援

令和６年１月１日から令和６年 12 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）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。

（イ）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。

（ウ）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。

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、本市担当者の承認を得ること。

②　『運用計画書』には、本業務の受託者と本市管理者による運用業務の責任分界点、作業分担を記載すること。

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、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。

（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EDR製品・SOCサービスの提供者（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。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。

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、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、SOC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SOCサービス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５年度は月次を想定し、令和６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

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６年１月１日から令和６年 12 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

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、SOC サービスから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。

（イ）チューニング

①　EDR のポリシーにより実行停止されたアプリケーションを本市運用管理者が確認できること。また、実行停止されたアプリケーションについて、本市運用管理者の依頼によりホワイトリストに登録可能なこと。

（ウ）バージョンアップ対応

① 受託者は、全ての端末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。

オ　その他

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

EDR要求機能一覧

No.	Lv1	Lv2	要件
1	前提条件	導入形態	脅威への迅速な対応のために、クラウド型のEDRサービスの利用を前提とすること。
2		エージェントの実装	本項に記載の要件は、複数の製品の組み合わせではなく単一のエージェントにて実装していること。
3		サーバ設置国・合意管轄裁判所	EDRの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。
4		監視対象範囲	本市が利用予定である「クラウド型仮想デスクトップ」上で実行される「デスクトップおよびアプリの仮想化サービス（Azure Virtual Desktop）」にEDRのエージェントをインストールし、サーバとエージェントを連携させること。
5			以下に対して、利用可能な機能に差異がなく、横断的に一元管理できること。 ・「クラウド型仮想デスクトップ」上で実行される「デスクトップおよびアプリの仮想化サービス（Azure Virtual Desktop）」 ・NEWSネットへある程度の期間をかけて段階的に移行する業務用FAT端末
6			本市が将来的に構築・利用予定である認証基盤(Active Directory)にEDRのエージェントをインストールし、サーバとエージェントを連携できる機能を有していること。
7			本市が将来的に構築・利用予定である集中ファイルサーバ、庁内データ交換フォルダ等のサーバ群にEDRのエージェントをインストールし、サーバとエージェントを連携できる機能を有していること。
8		通信暗号化	端末と管理サーバ間の通信は暗号化されていること。
9		導入実績	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。
10		利用者の意図しない行動への対策	端末上での証跡機能（セキュリティログ機能）の停止やログの改ざんを抑制または検知・通知可能なこと。
11			エージェントインストールフォルダーの中身の改ざんを抑制または検知・通知可能なこと。
12			エージェントに関連するレジストリ値の変更を抑制または検知・通知可能なこと。
13		OSサポート	以下に記載するOSに対応すること。 ・Microsoft 社がサポート中の Windows クライアント ・Microsoft 社がサポート中の Windows Server ・マルチセッション版のWindows10 Enterprise（64bit） ・マルチセッション版のWindows11 Enterprise（64bit） ・Red Hat 社がサポート中の Red Hat Enterprise Linux
14			エージェントがサポートする Red Hat Enterprise Linux は延長ライフサイクルサポート期間のものも含むこと。
15		OSバージョンアップに伴う対応	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製品をリリースすること。
16		一時的なライセンス超過への対応	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り、概ね一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。
17	管理機能	ロールベースのアクセス制限	管理コンソールにアクセスする複数のユーザーを作ることができ、システム機能のアクセス権、メール通知の有無を個別に設定できること。
18		セキュリティ対策	管理コンソールへのログインに二要素認証に対応していること。
19			管理コンソールへのログインにSAMLまたは、OpenID Connect認証に対応していること。
20			管理サーバへの通信は暗号化可能であること。
21		配布・適用	エージェントはサイレントインストールに対応し、効率的な展開が可能なこと。
22		リアルタイム性	端末上で起こった動作はリアルタイムに近い形(数分以内)で管理コンソールから全台検索が可能なこと。
23		帯域圧迫の回避	端末にて収集されたログは、リアルタイムにクラウド上にアップロードする機能を有していること。有していない場合は、都度アップロードされることなくリアルタイムに近い形（数分以内）で管理コンソールから全台検索が可能な状態であること。なお、負荷分散を目的として、一定の間隔でクラウド上にアップロードされることや、アップロードのタイミングが極力重ならないよう、端末間でアップロードタイミングが自動で調整されることなどの、端末から取得したログ等の情報の送受信において端末・ネットワークに特定の負荷がかからないようにコントロールできる機能を有していること。
24			既存のネットワーク装置に影響がないよう、端末と管理サーバーは通信が確立した後、セッションを永続的に維持しないこと。（必要な場合にのみ、セッションを確立すること）または、端末1台あたりの管理サーバーとの確立セッション数が1、またはそれ以下であること。なお、1日1台あたりの通信量30MBを基準とし帯域を圧迫させないこと。
25		EDR製品自体のログ取得	エージェント・ソフトウェアの動作ログが、管理画面より遠隔にて取得できること。
26		操作性、閲覧性	管理コンソール上に、調査をする際に役立つ検索ガイドが実装されていること。
27		セグメント管理	複数の部・局でわけて管理ができ、かつ、それらを一元管理するセグメント管理できる機能を有していること。
28	基本機能	未知の不正プログラム対策（エンドポイント対策）	EPP/NGAVがマルウェア、ランサムウェア、悪意のある有害な可能性のあるプログラム、正規プロセスを不正利用したファイルレスマルウェアなどの攻撃を検知した場合は、自動的にブロック可能なこと。
29		インシデント発生に係る処理	運用設計において定義したしきい値を上回るリスクレベルのインシデントが発生した場合に、自動処理、または、手動処理により、該当のサービスやプロセスを停止、または、端末を隔離することを可能とすること。また、判定したリスクレベルをアラートメールにおいて明示すること。
30		セキュリティ対策	EPP/NGAVのブロックポリシーについて、ファイルパスや動作条件を指定して、任意のプロセスの実行や停止を制御可能なこと。
31			サンドボックスを検知回避する技術を持った攻撃にも対応すること。
32		ログの収集対象	アラート対象であるかどうかに関わらず、以下をはじめとするWindowsの全プロセスのログをフィルタすることなく収集できること。その他OSについては、インシデント検知・追跡において必要となるプロセスのログをフィルタすることなく収集できること。 ・実行されたプロセスの概要（プロセス名、プロセスID、起動日時、実行ユーザー等） ・実行されたプロセスの一連のフロー（親プロセス、子プロセス） ・実行されたファイル名およびハッシュ値 ・実行されたコマンドラインの内容 ・通信先のドメイン、IPアドレス ・レジストリの変更履歴 ・呼び出されたDLLライブラリ ・特権名 ・権限昇格の有無 ・端末への遠隔操作歴
33		根本原因解決に係る仕組み	ルートキットなどによるプロセス偽装が行われた場合でも、正常なログを取得し、インシデントを確実に検知できるよう、カーネルモードによる取得が必要となる情報の収集ができること。
34			脅威であるかに関わらず、Windows 端末上で実行されたスクリプト及び実行ファイルのうち後からの調査に必要となる可能性のある箇所を自動収集できること。
35			EDRにより動作不可となったアプリケーションを、ホワイトリスト・ブラックリストに追加することで、速やかに動作可能にできる機能を有すること。
36		ログファイルの集約	端末で収集されたログを管理サーバに集約、あるいは、リアルタイムに近い形（数分以内）で管理コンソールから全台検索が可能な機能を有すること。
37		ログファイルの保管期間	監視対象の端末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。
38		ログファイルの保管対応	SIEM製品またはログサーバへ検知ログを送付することが可能であること。
39		一覧性、操作性	収集されたログに紐づくプロセス解析のために、プロセスの相関関係が一目で把握可能なプロセスツリーが表示できること。プロセスツリーから、影響範囲の調査・特定、各プロセスで発生したログの確認、分析結果の表示、隔離など対策の実行まで、一元的に操作できること。
40			収集されたログの検索機能を有すること。指定した条件（例：ファイル名、ドメイン、IPアドレス等）でログの検索を行うことで、監理しているエージェントの中から条件に関連した影響端末を特定できること。検索機能は管理コンソール上で提供され、正規表現などを用いて柔軟な検索が可能であること。

EDR要求機能一覧

No.	Lv1	Lv2	要件
41	EPP/NGAV	基本機能	マルウェア、不審なプログラム（PUP）、Powershellなどを用いたファイルレスマルウェア、ランサムウェアなどの攻撃に対して自動的に検知や不正なプロセスを停止することが可能なこと。
42			端末の振る舞いをリアルタイムで監視し、不審な挙動があった場合は即時で検知すること。
43			シグネチャまたはレピュテーションベースのファイルスキャン（パターンファイルマッチング）による防御機能を有していること。
44			Microsoft Office を始めとしたマクロ付きドキュメントファイルの攻撃そのものを検知できること。
45			ファイルだけではなくランサムウェアが示す挙動に基づいて検知できること。
46			製品インストール時に、インストール前より端末上に存在するマルウェアを洗い出せること。
47		未知の攻撃への対応	不審な振る舞いやフローを基に、未知の攻撃に対しても検知や不正なプロセスを停止することが可能なこと。
48			検知や不正なプロセスの停止に関わるポリシーについて、防御ルールとして管理者が任意のファイルパスに対して任意の動作条件を指定することにより、任意のプロセスの実行や停止を制御可能なこと。
49		運用の円滑化	初期展開時の動作確認・チューニングのため、ログ収集・分析・検知のみを行えること。
50			事前に設定した防御ポリシーにより、任意のプロセスの実行および停止が自動的におこなえること。
51			防御ルールを追加する際、防御対象となりうるイベントを過去のログから検索できること。
52			ブロックしたイベントを管理コンソール上で確認できること。
53			ブロック時に端末上でポップアップを表示すること。
54		監視対象がオフライン時の対策	インターネットに接続されていない場合もWindows端末に対してはパターンマッチングのウイルス対策等の最低限のセキュリティ対策が実行可能であること。
55			一度検知した危険なバイナリについては、端末がネットワークに接続していない状態であってもその実行を防止する機能を有すること。
56	ITハイジーン	基本機能	端末の脆弱性の排除や健全性状態の把握のために、端末に対して端末の基本情報（端末内のユーザ、OS・パッチのバージョンなど）や脆弱性に該当する可能性のあるリスク（SMBv1やRDPの有効化、USB利用の痕跡など）を検索、調査できること。また、必要に応じて、全端末に対してリアルタイムもしくはスケジューリングして情報収集することも可能であること。
57			エンドポイントの監視状況の可視化を提供する機能があること。
58			端末の健全性や脆弱性、マルウェアの横展開の有無などの調査を随時実施するため、下記の内容が実施できること。 ・SHA256に対応したハッシュ値やファイル名を基にした検索が可能であること ・ホスト名を基に検索が可能であること。 ・通信先のドメインやIP アドレスを基に検索が可能であること。
59		オフライン時の対策	端末がオフライン時など、端末が管理サーバに接続している/いないに関わらず、管理コンソール上で調査が可能であること。
60		迅速なインシデント対応	被疑端末のうち Windows のものに対して管理コンソールから以下の操作が実行可能なこと。 ・被疑ファイルの隔離または削除 ・ファイルのうち調査に必要な箇所の取得 ・ファイルの配置、実行 ・プロセスの終了 ・メモリダンプの取得 ・レジストリの修復または削除 ・OS 標準コマンド等を用いて任意のコマンドを実行
61			被疑端末のうち macOS、Linux のものに対して管理コンソールから以下の操作が実行可能なこと。 ・被疑ファイルの隔離または削除 ・ファイルのうち調査に必要な箇所の取得 ・ファイルの配置、実行 ・プロセスの終了 ・メモリダンプの取得 ・OS 標準コマンド等を用いて任意のコマンドを実行
62		一覧性、操作性	エージェントが収集した情報を任意のキーワードで検索できること。また、検索条件に合致する端末、プロセスおよびファイルなどが特定できること。さらに、検索した結果をCSVにて出力できること。また日本語データの出力にも対応していること。
63	通知	端末上での対応	検知や不正なプロセスを停止した際に端末上でポップアップが表示可能なこと。
64		通知内容	不審な挙動を示す端末のホスト名やIPアドレスなどの情報を管理者に通知できること。
65			不審な挙動を検知した場合にメール通知可能であること。
66	インシデント対応	隔離対応	インシデント検知後の対策として、管理コンソールから被疑端末を隔離（NWから遮断）できること。また、接続は管理コンソール間のみ維持できること。
67			当該アラートに該当する端末全てに対して一括で隔離の対応ができること。
68			管理コンソールより、端末の隔離解除が可能であること。
69		隔離時のユーザへの通知	エンドポイントがネットワークから隔離された際や、再接続された際に、利用者にポップアップが表示可能なこと。
70		操作性、閲覧性	管理コンソールにインシデントの発生状況を一覧で表示すること。
71			同じ内容のアラートをグルーピング可能なこと。
72	クラウドサービス適用時の留意事項	信頼性	ペネトレーションテストを定期的に実施していること。

SOCサービス要求機能一覧

No.	Lv1	Lv2	Lv3	要件
1	前提条件	ログ保管期間	ー	監視対象の端末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。
2		導入実績		『別紙２ EDR要求機能一覧』のEDRとして提案する製品に対するSOCサービスとして、単一組織で15,000台を超える導入・運用実績を有すること。
3	監視	サービス提供時間	ー	SOCサービスの提供時間は、24時間365日有人監視とすること。
4	検知	インシデントレベル	段階	最低限4つ以上の段階を設ける機能を有すること。
5			内容	最低限必要な4つの内容を設けることができる機能を有すること。 Lv4：早期対応が必要 Lv3：攻撃が成功した可能性が高い Lv2：攻撃につながる可能性が低い Lv1：攻撃とはいえないが留意すべき事項
6			報告	有人監視にて「早期対応が必要」或いは「攻撃が成功した可能性が高い」に該当した緊急度の高い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。
7		通知手段	ー	判定されたインシデントレベルに応じて、SOCサービスから本市運用管理者へメール、電話による通知できること。
8	調査・対応	調査	内容	インシデント通報に関する問合せも24時間365日対応とすること。提供時間内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・対応のサービスを提供すること。なお、復旧は以下の運用・保守業務を受託した事業者に対して、インシデントレベルや内容に応じて、作業を支援をすること。 ・「クラウド型仮想デスクトップ」上で実行される「デスクトップおよびアプリの仮想化サービス（Azure Virtual Desktop）」 ・NEWSネットへある程度の期間をかけて段階的に移行する業務用FAT端末
9			報告	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、本市運用管理者へ報告すること。
10		対応、隔離、隔離解除	ー	判定されたインシデントレベルに応じて、脅威（検体）や被疑端末の隔離措置ができること。また、隔離実行の判断は本市ではせず、インシデントレベルに応じて隔離を行い、誤検知だった場合は隔離解除できること。
11	復旧	通知内容		隔離された端末の情報をメール・電話を主とした方法で本市運用管理者へ通知すること。なお、インシデント対応完了後に隔離解除を実施し、隔離解除した旨を本市運用管理者が判断でき、隔離解除の承認ができること。
12		レポーティング	周期、内容	月内に発生したアラートの統計情報および対応結果のサマリ、「早期対応が必要」或いは「攻撃が成功した可能性が高い」に該当した緊急度の高いインシデント関連情報をサマリーした月次レポートを提供すること。
13		報告会	ー	月次レポートの情報共有及びSOCサービス運用の最適化を目的とした打ち合わせに対応できること。開催頻度は令和5年度中は月次を想定し、令和６年度以降は本市と協議のうえ、決定すること。
14	チューニング	アラート	ー	EDRのポリシーにより実行停止されたアプリケーションを本市運用管理者が確認できること。また、実行停止されたアプリケーションについて、本市運用管理者の依頼によりホワイトリストに登録できること。
15	外部監査	情報提供	ー	本市で実施する外部監査に際し、必要な情報を提供できること。具体的な情報の内容や提供方法については本市と協議のうえ、決定すること。