（運用基準　様式３）
令和４年３月７日
総務局ＩＣＴ基盤管理課

# 「横浜市行政情報ネットワークにおけるEDR及びMDR導入業務委託契約」

## 契約結果

横浜市行政情報ネットワークにおけるEDR及びMDR導入業務委託について、公募型プロポーザル方式で、受託候補者を特定し、次のとおり契約しました。

1　件名
横浜市行政情報ネットワークにおけるEDR及びMDR導入業務委託

2　委託内容
(1) プロジェクト管理
(2) 要件定義
(3) 方式設計
(4) 環境設計
(5) 運用設計
(6) 導入計画
(7) 環境構築
(8) テスト
(9) 展開
(10) 初期稼働支援
(11) ドキュメント作成

3　契約の相手方
富士通Japan株式会社　神奈川支社

4　契約金額
62,686,800円

5　契約日
令和４年２月28日

6　評価結果

| 提案者 | 評価点数（2,460 点満点） | 順位 |
|---|---|---|
| 富士通 Japan 株式会社　神奈川支社 | 2,172 | 1 |
| 株式会社日立製作所　横浜支店 | 2,124 | 2 |

7　評価基準・評価委員会開催経過等

(1) 評価基準

別紙のとおり。

(2) 評価委員会開催経過等

| | | | |
|---|---|---|---|
| 委員会開催日時 | 第一回 | 令和 3 年 12 月 22 日（水）13：30～15：40 | |
| | 第二回 | 令和 4 年 1 月 6 日（木）10：00～10：15 | |
| 委員会開催場所 | 第一回 | 市庁舎 25 階共用会議室（25-S02） | |
| | 第二回 | 市庁舎 27 階共用会議室（27-N02） | |
| 評価委員の出席状況 | 第一回 | 評価委員 6 名中 6 名出席 | 充足率：6/6 |
| | 第二回 | 評価委員 6 名中 6 名出席 | 充足率：6/6 |
| 議事内容 | 第一回 | ・提案者ヒアリングの実施 | |
| | 第二回 | ・評価結果の集計及び集計結果の確認<br>・受託候補者の決定 | |
| 事務局 | 総務局ＩＣＴ基盤管理課 | | |

8　問合せ先

総務局ＩＣＴ基盤管理課
担当　森田、牧野、加山
電話　045-671-2015
Ｅメール　so-it-sec@city.yokohama.jp

# 提案書評価基準

1　評価事項

提案書に対する評価項目や評価の視点等は別紙「提案書評価項目一覧」を参照。

2　評価方法

(1)　評価

各評価項目について、次のいずれかの評価を行う。

ア　Ａ、Ｅの２段階評価

イ　Ａ、Ｃ、Ｅの３段階評価

ウ　Ａ、Ｂ、Ｃ、Ｄ、Ｅの５段階評価

(2)　評価点

評価を基に表１のように評価点を算出する。

**表１　評価点の算出**

| 配点 | 評価点 | | | | |
|---|---|---|---|---|---|
| | A | B | C | D | E |
| 20 | 20 | 16 | 12 | 8 | 4 |
| 10 | 10 | 8 | 6 | 4 | 2 |
| 10 | 10 | | 6 | | 2 |
| 5 | 5 | 4 | 3 | 2 | 1 |
| 5 | 5 | | 3 | | 1 |
| 5 | 5 | | | | 1 |

3　提案者の選定方法及び受託候補者の特定方法

(1)　評価項目について、委員長及び副委員長を含む全ての評価委員が与えた合計点が最も高い者を受託候補者として特定します。

(2)　総合計点を比較してもなお、受託候補者を特定できない場合には、次の順序で受託候補者を特定します。

ア　「EDR 機能要件の実現」の合計点が上位の者

イ　「MDR サービス要件の実現」の合計点が上位の者

ウ　「導入・運用」の合計点が上位の者

提案書評価項目一覧

| 評価項目 | 記述内容（要求要件） | 評価の着眼点 | 配点 | 評価基準 | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | A | B | C | D | E |
| 1　企業としての実績・信頼性等 | | | | | | | | |
| 1.1　企業実績 | | | | | | | | |
| 1.1.1　従業員数 | 従業員数及びプロジェクトメンバー以外に代替できる要員の有無を記載してください。 | 十分な従業員数があり、不慮の事故等の際のプロジェクト関係者の代替が可能であるか。 | 10 | 従業員数が300人より多く、プロジェクトメンバー以外の要員の代替が可能である。 | － | 従業員数が300人以下であるが、プロジェクトメンバー以外の要員の代替が可能である。 | － | プロジェクトメンバー以外の要員の代替ができない。 |
| 1.1.2　本業務と同種・類似業務の事業実績 | 国内の自治体・政府・民間企業等の単一組織において、１万台を超えるエンドポイントセキュリティ製品の導入・運用実績を記載してください。なお、監視対象となった端末・サーバー台数およびサポートをしたOSの種類等についても記載してください。 | エンドポイントセキュリティ製品の運用に関する十分な経験を有しているか（導入・運用の経験期間は十分か）。 | 10 | １万台を超えるエンドポイントセキュリティ製品の導入・運用実績が複数あり、サポートをしたOSの種類が３種以上ある。 | － | １万台を超えるエンドポイントセキュリティ製品の導入・運用実績が複数あり、サポートをしたOSの種類が２種以上ある。 | － | １万台を超えるエンドポイントセキュリティ製品の導入・運用実績があり、サポートをしたOSの種類が１種以上ある。 |
| 1.2　配置予定技術者の業務実績・経験等 | | | | | | | | |
| 1.2.1　プロジェクト管理者 | エンドポイントセキュリティ製品の導入及び運用保守のプロジェクトの実績・経験等を記載してください。 | エンドポイントセキュリティ製品の導入・運用保守プロジェクトの管理又はそれに準ずる経験があるか。 | 5 | 国内の自治体・政府におけるエンドポイントセキュリティ製品の導入・運用のプロジェクト経験が複数ある。 | 国内の自治体・政府におけるエンドポイントセキュリティ製品の導入・運用のプロジェクト経験がある。 | 国内の民間企業におけるエンドポイントセキュリティ製品の導入・運用のプロジェクト経験が複数ある。 | 国内の民間企業におけるエンドポイントセキュリティ製品の導入・運用のプロジェクト経験がある。 | 業務実績・能力に不十分な点がある。 |
| 1.2.2　チームリーダーA | エンドポイントセキュリティ製品の導入に関する実績・経験等を記載してください。 | ・エンドポイントセキュリティ製品の導入に関する経験を有しているか。<br>・チームリーダーとして十分な経験を有しているか。 | 5 | 国内の自治体・政府におけるエンドポイントセキュリティ製品の導入・運用のプロジェクト経験が複数ある。 | 国内の自治体・政府におけるエンドポイントセキュリティ製品の導入・運用のプロジェクト経験がある。 | 国内の民間企業におけるエンドポイントセキュリティ製品の導入・運用のプロジェクト経験が複数ある。 | 国内の民間企業におけるエンドポイントセキュリティ製品の導入・運用のプロジェクト経験がある。 | 業務実績・能力に不十分な点がある。 |
| 1.2.3　チームリーダーB | エンドポイントセキュリティ製品の運用保守に関する実績・経験等を記載してください。 | ・エンドポイントセキュリティ製品の運用保守に関する経験を有しているか。<br>・チームリーダーとして十分な経験を有しているか。 | 5 | 国内の自治体・政府におけるエンドポイントセキュリティ製品の導入・運用のプロジェクト経験が複数ある。 | 国内の自治体・政府におけるエンドポイントセキュリティ製品の導入・運用のプロジェクト経験がある。 | 国内の民間企業におけるエンドポイントセキュリティ製品の導入・運用のプロジェクト経験が複数ある。 | 国内の民間企業におけるエンドポイントセキュリティ製品の導入・運用のプロジェクト経験がある。 | 業務実績・能力に不十分な点がある。 |
| 2　プロジェクトマネジメント | | | | | | | | |
| 2.1　プロジェクト運用 | | | | | | | | |

| 評価項目 | | 記述内容（要求要件） | 評価の着眼点 | 配点 | 評価基準 | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | A | B | C | D | E |
| 2.1.1 | 実施体制 | 運用体制図と各部門に携わる人数（概数で構いません）について、現在の想定値を記載してください。 | ・実施体制が明確にされているか。<br>・業務遂行に必要な責任体制（意思決定者の明確化、位置付け）となっているか。<br>・導入に係る本市管理者職員並びに横浜市行政情報ネットワーク運用保守事業者との連携が考慮されているか。<br>・導入だけでなく、運用時の体制が考慮されているか。<br>・構築中におけるトラブル等に速やかに対応できるよう、業務拠点が遠方でないか。 | 5 | 体制が明確で、十分整っている。 | － | 体制が明確で、整っている。 | － | 体制が明確に示されていない。または、不十分である。 |
| 2.1.2 | 実施計画 | 履行期間における全体スケジュールを記載してください。何を、いつ、どのくらいの期間行うのか具体的な提案をしてください。 | ・実施計画が明確にされているか。<br>・本市が移行を計画しているβ´モデルにおける本業務の位置付けについて理解した計画となっているか。<br>・職員（企業局を含む）にとって分かりやすく、スムーズな移行計画となっているか。 | 5 | 計画が明確で、十分整っている。 | － | 計画が明確で、整っている。 | － | 計画が明確に示されていない。または、不十分である。 |
| 3 EDR機能要件の実現 | | | | | | | | | |
| 3.1 要件一覧への適合 | | | | | | | | | |
| 3.1.1 | 必須項目の実現 | 別添の「EDR機能要件」の必須項目の機能を実現できるかどうか、別紙「EDR機能要件対応表」に記載してください。 | 「EDR機能要件対応表」の必須項目の機能を実現できるか。<br>【別紙に基づき評価】<br>機能実現が出来ない又は実現手法に課題があり、実用には問題がある場合は不合格。 | － | ヒアリング対象外 | | | | |
| 3.1.2 | 任意項目の実現 | 別添の「EDR機能要件」の任意項目の機能を実現できるかどうか、別紙「EDR機能要件対応表」に記載してください。 | 「EDR機能要件対応表」の任意項目の機能を実現できるか。<br>【別紙に基づき評価】 | 56 | ヒアリング対象外 | | | | |
| 3.2 提供機能 | | | | | | | | | |
| 3.2.1 | システム概要 | システムの構成や機能概要について、記載してください。また、システムの特長について記載してください。 | 概要であり、評価は以下の詳細で行うこととする。 | － | 評価対象外 | | | | |

| 評価項目 | 記述内容（要求要件） | 評価の着眼点 | 配点 | 評価基準 | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | A | B | C | D | E |
| 3.2.2　製品導入実績 | EDR製品としての日本国内における導入実績（組織数、総ユーザー数）について記載してください。<br>また、単一組織内で最大値となる導入実績台数を記載してください。 | ・EDRを導入している組織数や総ユーザー数は十分な実績であるか。<br>・単一組織内で、本市EDR導入予定台数（約50,000台）と同等、もしくはそれ以上の導入実績台数を有するか。 | 10 | 十分な実績がある。 | － | ＡとＥの中間に該当する場合 | － | 実績が不十分である。 |
| 3.2.3　脅威への対応力 | EDR製品として脅威への高い対応能力を有していることを記載してください。 | ・リアルタイム検知能力の優位性が客観的に示されているか。<br>・様々な脅威に対して、柔軟に対応可能なことが示されているか。<br>・日本固有の脅威に対応可能なことが示されているか。 | 20 | 脅威への対応力が非常に高い。 | 脅威への対応力が高い。 | 脅威への対応力が相応にある。 | 脅威への対応力が低い。 | 脅威への対応力が非常に低い。 |
| 3.2.4　端末・業務影響への配慮 | PCMark 8 Work test またはその他の業務利用を前提とした定量的測定手法によりパフォーマンス測定を同一端末のエージェント導入前後でそれぞれ行い、エージェント導入による性能低下がどの程度かを示してください。<br>システム全体のメモリ使用量がエージェント導入前後でどの程度変化するかを示してください。<br>エージェントが行う通信量（インストール時、平常時それぞれ）がどの程度かを示してください。<br>その他、エージェントが端末の安定動作維持のために工夫していること等があれば記載してください。 | ・端末での通信量や負荷について、検証結果に基づいた具体的な値を示されており、それが軽微であると考えられるか。<br>・OS・SKYSEA Client View・QND、他、アプリケーションとの競合によるブルースクリーン等の不具合を防ぐ工夫がされているか。 | 20 | 端末への負荷や通信量が非常に少なく、ユーザーに与える影響度が非常に低い。 | 端末への負荷や通信量が少なく、ユーザーに与える影響度が低い。 | 端末への負荷や通信量が相応であり、ユーザーに与える影響度も相応である。 | 端末への負荷や通信量が多く、ユーザーに与える影響度が高い。 | 端末への負荷や通信量が非常に多く、ユーザーに与える影響度が非常に高い。 |
| 3.2.5　OS 新バージョンへの対応実績 | 2019年以降にリリースされた Windows のメジャーバージョンアップ（Windows 11、Windows Server 2022）や Windows 10 の機能更新リリース時、Red Hat Enterprise Linux のメジャーバージョンアップ（RHEL 8）やマイナーバージョンアップ時に、その OS の一般向け提供開始日から起算してそれに対応した新しいエージェントの提供までに要した日数の実績を記載してください。既存のエージェントからバージョンアップすること自体が不要だった場合は、その旨を記載してください。 | ・エージェントのバージョンアップが不要だった場合は最も高評価とする。<br>・エージェントのバージョンアップが必要だった場合は、対応した新バージョンの提供開始までのタイムラグが短いものを高評価とする。 | 10 | エージェントのバージョンアップ自体がほとんど不要だった。 | エージェントの新バージョン提供まで概ね１か月以内 | エージェントの新バージョン提供まで概ね３か月以内 | エージェントの新バージョン提供まで概ね６か月以内 | エージェントの新バージョン提供まで概ね６か月を超える。 |

| 評価項目 | 記述内容（要求要件） | 評価の着眼点 | 配点 | 評価基準 | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | A | B | C | D | E |
| 3.2.6　ユーザインターフェース | 管理画面および管理レポートを参照する職員（管理部署職員）並びに横浜市行政情報ネットワーク運用保守事業者が状況を把握しやすいよう工夫されている点を記載してください。また、マルウェアを検知した際に利用者に表示されるメッセージ等がわかりやすいよう、工夫されている点を記載してください。 | ・攻撃フェーズごとの感染状況（規模、経過時間）が可視化され、迅速な初動が可能になっているか。<br>・最小限のオペレーションで対象端末、対象ユーザ、感染の拡大状況を把握することができるか。<br>・攻撃内容の説明部分まで日本語対応されることで、インシデント発生時の迅速な対応がとれるようにされているか。<br>・利用者に表示されるメッセージ等が日本語対応でわかりやすく、認知しやすいか。 | 20 | 管理画面の表示内容や利用者に表示されるメッセージが非常にわかりやすく、認知しやすい。 | 管理画面の表示内容や利用者に表示されるメッセージがわかりやすく、認知しやすい。 | 管理画面の表示内容や利用者に表示されるメッセージが相応である。 | 管理画面の表示内容や利用者に表示されるメッセージが分かりづらく、認知しずらい。 | 管理画面の表示内容や利用者に表示されるメッセージが非常に分かりづらく、認知しずらい。 |
| 4　MDRサービス要件の実現 | | | | | | | | |
| 4.1　要件一覧への適合 | | | | | | | | |
| 4.1.1　必須項目の実現 | 別添の「MDRサービス要件」の必須項目の機能を実現できるかどうか、別紙「MDRサービス要件対応表」に記載してください。 | 「MDRサービス要件対応表」の必須項目の機能を実現できるか。<br>【別紙に基づき評価】<br>機能実現が出来ない又は実現手法に課題があり、実用には問題がある場合は不合格。 | － | ヒアリング対象外 | | | | |
| 4.1.2　任意項目の実現 | 別添の「MDRサービス要件」の任意項目の機能を実現できるかどうか、別紙「MDRサービス要件対応表」に記載してください。 | 「MDRサービス要件対応表」の任意項目の機能を実現できるか。<br>【別紙に基づき評価】 | 24 | ヒアリング対象外 | | | | |
| 4.2　監視センター | | | | | | | | |
| 4.2.1　監視センター体制 | 監視センターの体制を記載してください。監視センターの運用には職員（管理部署職員）並びに横浜市行政情報ネットワーク運用保守事業者に対する、迅速かつ高度なインシデント対応を実現するために、どのような工夫がされているか記載してください。 | ・情報セキュリティ専門人材が十分に体制に組み込まれているか。<br>・監視センターから本市への連絡体制について、効率的かつ臨機応変に対応できる仕組みとなっているか。<br>・情報セキュリティ専門人材はプロダクトメーカによるトレーニングを受けているか。<br>・アラートレベル判定等において、属人性を排除する工夫があるか。 | 20 | 監視センターの体制が十分に整っている。 | AとCの中間に該当する場合 | 監視センターの体制がある程度整っている。 | CとEの中間に該当する場合 | 監視センターの体制が整っていない。 |

| 評価項目 | | | 記述内容（要求要件） | 評価の着眼点 | 配点 | 評価基準 | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | A | B | C | D | E |
| | | 4.2.2　インシデント発生時の対処 | インシデントレベルに応じた監視センターの対応について、工夫されている点があれば記載してください。また、本市環境に即したインシデント対処案があれば提案してください。 | ・情報セキュリティ専門人材は予め決められた対処を行うだけでなく、推奨対策案の提示が可能であるか。<br>・報告レポートは一般的な対策の提示だけでなく、本市の環境に即した対策案の提示も記載されているか。<br>・インシデント発生状況についてレポート報告会などで、情報セキュリティ専門人材が本市職員へ説明を行うことが可能であるか。<br>・EDR 起点ではなく、外部組織からの通報等により判明したインシデントについても、調査支援を受けられるか。<br>・不審なファイルが発見され、詳細調査が必要となった場合、そのファイルの解析にも対応可能 | 20 | 対策案について、優れた提案である。また、調査支援や詳細調査が必要になった場合でも、運用内で全て無償対応可能となる。 | 対策案について、優れた提案である。また、調査支援や詳細調査が必要になった場合でも、一部無償対応可能となる。 | 対策案について、優れた提案である。 | 対策案について、相応の提案である。 | 対策案について、提案が不十分である。 |
| 5　セキュリティ | | | | | | | | | | |
| | 5.1　具体的なセキュリティ対策 | | | | | | | | | |
| | | 5.1.1　個人情報保護対策 | 個人情報保護マネジメント、情報セキュリティマネジメントの内容、特に個人情報保護対策（個人情報取扱方法、監査方法など）について記載してください。 | 個人情報保護マネジメント、情報セキュリティマネジメントの内容、特に個人情報保護対策（個人情報取扱方法、監査方法など）が具体的であるか。 | 10 | 具体的かつ適正で充実した内容である。 | ＡとＣの中間に該当する場合 | 具体的かつ適正な内容である。 | ＣとＥの中間に該当する場合 | 具体的な内容となっていない。または、適正な内容となっていない。 |
| | | 5.1.2　セキュリティ対策 | データセンターやクラウドサービス等のファシリティは、物理的、技術的、人的にどのようなセキュリティ対策を施すかを具体的に記載してください。また、セキュリティに対する社員教育、守秘義務の社内基準やセキュリティ監査の仕組みがあれば記載してください。 | ・データセンターは日本国内に存在するか。<br>・データセンターは国際規格に準拠した運用がなされているか。<br>・取得している国際規格が明記されているか。<br>・物理的、技術的、人的なセキュリティ対策が実施されており、セキュリティ対策が明確かつ適正であるか。<br>・管理するログ情報について、十分なセキュリティ対策や適切な保管期間が設けられているか。 | 10 | 対策が十分である。 | ＡとＣの中間に該当する場合 | 対策が相応である。 | ＣとＥの中間に該当する場合 | 対策が不十分である。 |
| | | 5.1.3　メーカーの信頼性 | 当該メーカーのエンドポイントセキュリティ製品（今回提案する製品に限りません）において、2019年以降に製品自身の脆弱性のパッチ提供遅れに起因するセキュリティ被害を顧客環境に発生させたことがある場合は記載してください。発生させたことがある場合はどのような再発防止策を取ったのか記載してください。 | ・当該製品に起因する顧客へのセキュリティ被害が発生していないか。<br>・もし発生した場合は、十分な再発防止体制が取られているか。 | 10 | 当該製品に対するセキュリティ被害が発生していない。 | ＡとＣの中間に該当する場合 | 当該製品に対するセキュリティ被害が発生したが、十分な再発防止体制が取られている。 | ＣとＥの中間に該当する場合 | 当該製品に対するセキュリティ被害が発生しており、再発防止体制も取られていない。 |

| 評価項目 | 記述内容（要求要件） | 評価の着眼点 | 配点 | 評価基準 | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | A | B | C | D | E |
| 5.1.4　監視センターの信頼性 | 当該MDRサービスにおいて、2019年以降に監視センター自身のセキュリティインシデントに起因するセキュリティ被害を顧客環境に発生させたことがある場合は記載してください。発生させたことがある場合はどのような再発防止策を取ったのか記載してください。 | ・当該サービスに起因する顧客へのセキュリティ被害が発生していないか。<br>・もし発生した場合は、十分な再発防止体制が取られているか。 | 10 | 当該サービスに対するセキュリティ被害が発生していない。 | ＡとＣの中間に該当する場合 | 当該サービスに対するセキュリティ被害が発生したが、十分な再発防止体制が取られている。 | ＣとＥの中間に該当する場合 | 当該サービスに対するセキュリティ被害が発生しており、再発防止体制も取られていない。 |
| 6　導入・運用 | | | | | | | | |
| 6.1　作業・計画 | | | | | | | | |
| 6.1.1　導入作業 | 円滑にサービスを開始し、運用できるよう、導入作業をどのように行うのか、導入内容と職員対応が必要な内容、移行作業を行う職員への支援内容を具体的に提案してください。また、現行エンドポイント製品との並行稼働も考慮し、職員の負担の少ない移行方法を提案してください。 | ・本市のネットワーク状況を考慮した効率的な導入計画が示されているか。<br>・エージェントの展開は、利用者によるオペレーションを最小限とする工夫がなされているか。<br>・本市の既存システムを活用した効率的な移行計画となっているか。<br>・本市職員（企業局を含む）並びに行政情報ネットワーク運用保守事業者の負荷軽減を考慮した移行計画となっているか。 | 20 | 具体的な導入計画があり、職員や運用保守事業者における業務負担の低減がかなり期待できる。 | ＡとＣの中間に該当する場合 | 具体的な導入計画があり、職員や運用保守事業者における業務負担の低減が期待できる。 | ＣとＥの中間に該当する場合 | 職員や運用保守事業者の低減が期待できない。 |
| 6.1.2　運用計画 | 令和４年10月から令和５年３月の運用初期および、令和５年４月以降における運用計画を具体的に提案してください。 | ・運用初期に必要となる過検知・誤検知の調整やチューニングを速やかに行える体制となっているか。<br>・次期神奈川情報セキュリティクラウドへの切り替えを考慮した計画となっているか。<br>・職員からの問い合わせに対して、柔軟に対応できる体制になっているか。<br>・職員並びに行政情報ネットワーク運用保守事業者の負荷軽減を考慮した計画になっているか。 | 20 | 具体的な運用計画があり、十分に迅速・柔軟に行える体制となっている。 | ＡとＣの中間に該当する場合 | 具体的な運用計画があり、迅速・柔軟に行える体制となっている。 | ＣとＥの中間に該当する場合 | 迅速・柔軟に行える体制となっていない。 |
| 7　将来性・拡張性 | | | | | | | | |
| 7.1　将来性・コスト | | | | | | | | |

| 評価項目 | | | 記述内容（要求要件） | 評価の着眼点 | 配点 | 評価基準 | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | A | B | C | D | E |
| | | 7.1.1　拡張性とコスト | (1)動作環境拡大への対応<br>新しいOSのリリースや同居するセキュリティ製品について、どのように対応するか記載してください。 | 新しいOSや同居するセキュリティ製品のリリースによって、利用者の動作環境が拡大された際の対応ができるか。 | 5 | 動作環境拡大の対応は運用内で実施し、迅速な対応が期待できる。 | 動作環境拡大の対応は運用内で実施される。 | 主な動作環境拡大の対応は運用内で実施するが、一部運用外となる部分がある。 | 全ての動作環境拡大対応に費用負担が必須となる。 | 動作環境拡大には対応しない。 |
| | | | (2)本市の要件に応じて、EDR以外の製品のログも監視、分析対象とすることが可能かどうか等についても記載してください。 | ・ファイアウォール・プロキシサーバー・メールサーバー等のログを分析対象とすることが可能か。<br>・実績のない製品のログも分析対象とすることが可能か。<br>・1つのMDRサービスの中で、全てのログを統一的に監視可能か。 | 5 | 拡張性が非常に高い。 | ＡとＣの中間に該当する場合 | 拡張性が相応にある。 | ＣとＥの中間に該当する場合 | 拡張性が見込めない。 |
| | | | (3)提案に対する経費の妥当性<br>導入から運用（令和３年度～令和９年度９月）までの総経費について記載してください。 | 総経費が提案に対して適正か。 | 20 | 経費に対し非常に高度な技術提案を行っている。 | 経費に対して高度な技術提案を行っている。 | 経費に対して相応な技術提案を行っている。 | 技術提案内容に対して経費が高い。 | 技術提案内容に対して経費が高すぎる。 |
| 8　企業としての取り組み | | | | | | | | | | |
| | 8.1　取り組み状況 | | | | | | | | | |
| | | 8.1.1　ワーク・ライフ・バランスに関する取組 | ワーク・ライフ・バランスに関する取組について、取得している認定を記載してください。（要領ー１） | 次のいずれかを取得しているか。<br>①次世代育成支援対策推進法に基づく認定（くるみんマーク、プラチナくるみんマーク）<br>②女性の職業生活における活躍の推進に関する法律に基づく認定（えるぼし）<br>③若者雇用促進法に基づく認定(ユースエール)<br>④よこはまグッドバランス賞 | 5 | ２件以上取得している。 | － | １件取得している。 | － | 取得していない。 |

| 評価項目 | 記述内容（要求要件） | 評価の着眼点 | 配点 | 評価基準 | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | A | B | C | D | E |
| 8.1.2　障害者雇用に関する取組 | 障害者雇用に関する取組として、従業員数、障害者雇用数、障害者雇用率を記載してください。（要領ー２） | 障害者雇用促進法に基づく法定雇用率2.3%の達成をしているか。 | 5 | 達成している（従業員43.5人以上）、又は障害者を１人以上雇用している。（従業員43.5人未満） | － | － | － | 達成していない（従業員43.5人以上）、又は障害者を１人以上雇用していない。（従業員43.5人未満） |
| 8.1.3　健康経営に関する取組 | 健康経営に関する取組について、取得している認定を記載してください。（要領ー３） | 健康経営銘柄、健康経営優良法人（大規模法人・中小規模法人）の取得、又は、横浜健康経営認証のAAAクラス若しくはAAクラスの認証を取得しているか。 | 5 | 健康経営銘柄、健康経営優良法人（大規模法人・中小規模法人）の取得、又は、横浜健康経営認証クラスAAA）を取得している。 | － | 横浜健康経営認証クラスAAを取得している。 | － | 取得していない。 |
| 9　提案内容 | | | | | | | | |
| 9.1　総合評価 | | | | | | | | |
| 9.1.1　本業務への意欲・取組意欲 | － | ・提案書全体の評価やヒアリングを通じた総合的な印象として、本業務の遂行を任せられるだけの十分な意欲・取組姿勢が見られるか。<br>・自社の都合だけに固執せず、本市にとってより効果的な提案をする姿勢が見られるか。 | 10 | 十分な意欲・取組姿勢を見られる。 | ＡとＣの中間に該当する場合 | 一定の意欲・取組姿勢を見られる。 | ＣとＥの中間に該当する場合 | 意欲・取組姿勢が見られない。 |
| 9.1.2　提案内容全体のわかりやすさ | － | ・提案書全体の評価やヒアリングを通じた総合的な印象として、本市の視点に立ったわかりやすい説明がなされているか。<br>・技術的な専門知識を前提とした説明、本市にとっての利点が不明瞭な説明が少なく、本市にとって理解しやすい説明になっているか。<br>・質問に対する回答は、適切かつ明瞭なものか。 | 10 | 非常に理解しやすい。 | ＡとＣの中間に該当する場合 | 概ね理解できる。 | ＣとＥの中間に該当する場合 | 理解しにくい。 |

| 評価項目 | 記述内容（要求要件） | 評価の着眼点 | 配点 | 評価基準 | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | A | B | C | D | E |
| 9.1.3　本業務の理解 | - | 提案書全体の評価やヒアリングを通じた総合的な印象として、本業務の目的、目標、業務範囲等を正しく理解しているか。 | 10 | 十分に理解している。 | ＡとＣの中間に該当する場合 | 概ね理解している。 | ＣとＥの中間に該当する場合 | 理解に不十分な点がある。 |
| 9.1.4　業務実績・能力 | - | 提案書全体の評価やヒアリングを通じた総合的な印象として、本業務に必要な専門性を有し、本業務を適切に遂行できることが期待できるか。 | 10 | 十分に期待できる。 | ＡとＣの中間に該当する場合 | 一定の期待が持てる。 | ＣとＥの中間に該当する場合 | 業務遂行に疑わしい点がある。 |
| 合計 | | | 410 | | | | | |

# 別紙 EDR機能要件対応表（評価基準）

「対応」欄については以下の基準で記入してください。
いずれも本契約期間中（令和4年9月末）までに対応予定であれば良いものとします。予定のものは備考欄にその旨を記載してください。

「必須」欄が○の項目
○ ： 対応可能
× ： 対応不可（対応不可が1項目でもある場合不合格）

「必須」欄が○でない項目
○ ： 対応可能
△ ： 部分的に対応可能または代替手段により対応可能等（「備考」欄に記入してください）
× ： 対応不可

## 1 基本機能

| # | 要件 | 対応可否欄の記載 | | |
|---|---|---|---|---|
| | | ○ | △ | × |
| (1) | 既知のマルウェア対策機能（EPP）・未知のマルウェア対策機能（NGAV）・端末の動作ログを収集・分析しリアルタイムにマルウェアの攻撃を検知・制御する機能（EDR）の全ての機能を提供すること。Windows における EPP については Windows Defender を併用することで実現しても良いが、それが検知したマルウェアを EDR 製品とともに統一的に管理できること。 | - | - | - |
| (2) | クライアント及びサーバー合計5万3千台で利用可能なライセンスを用意すること。 | - | - | - |
| (3) | 監視対象のクライアント・端末の入れ替えがあった場合に備え、一時的にライセンスを超過してもサービスの提供に問題がないこと。 | - | - | - |
| (4) | 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。 | 6 | 3 | 0 |
| (5) | 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。 | - | - | - |
| (6) | エージェントの配布方法として、SKYSEA Client View による展開実績を有すること。 | 2 | 1 | 0 |
| (7) | エージェントのインストール時に OS の再起動を要しないこと。 | 2 | 1 | 0 |
| (8) | エージェントのバージョンアップ時に OS の再起動を要しないこと。 | 2 | 1 | 0 |
| (9) | 初期展開時の動作確認・チューニングのため、ブロックせずにログ収集・分析・検知のみを行えること。 | - | - | - |
| (10) | エージェントは以下の OS をサポートすること。<br>・Microsoft 社がサポート中の Windows クライアント<br>・Microsoft 社がサポート中の Windows Server<br>・Red Hat 社がサポート中の Red Hat Enterprise Linux<br>・Apple 社がサポート中の macOS | - | - | - |
| (11) | 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。 | 4 | 2 | 0 |
| (12) | 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3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。 | - | - | - |
| (13) | ユーザーによるエージェントのアンインストールやサービス停止を抑制または検知・通知可能なこと。 | - | - | - |
| (14) | 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。 | - | - | - |
| (15) | 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。 | - | - | - |
| (16) | 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。 | - | - | - |
| (17) | 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。 | - | - | - |
| (18) | ネットワーク帯域圧迫のリスク低減のために、端末にて収集されたログは負荷分散を目的として、一定の間隔でマネージャーにアップロードされること。また、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。シグネチャ等のダウンロードについても同様にタイミングが分散されること。 | - | - | - |
| (19) | リンククローン等のマスターイメージ+差分方式の DaaS にて利用可能なこと。 | - | - | - |
| (20) | 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1万台を超える導入実績を有する製品であること。 | - | - | - |
| (21) | 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5万台を超える導入実績を有する製品であること。 | 2 | 1 | 0 |

## 2 マルウェア対策機能、ログ収集・分析・対処（EDR）機能

| # | 要件 | 対応可否欄の記載 | | |
|---|---|---|---|---|
| | | ○ | △ | × |
| (1) | マルウェア、好ましくないプログラム（PUP）、正規プロセス（PowerShell や WMI 等）を不正利用したファイルレスマルウェア、ランサムウェアなどの攻撃を自動的にブロック可能なこと。 | - | - | - |
| (2) | 不審な振る舞いやプロセスフローを基に、未知の攻撃に対してもブロック可能なこと。 | - | - | - |
| (3) | 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）が可能なこと。 | - | - | - |
| (4) | エンドユーザーが指定したファイルやフォルダーに対して即時スキャンとその結果表示が GUI で可能なこと。 | 2 | 1 | 0 |
| (5) | ブロックポリシーについて、管理者が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。 | - | - | - |
| (6) | 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。 | - | - | - |

| | | | | |
|---|---|---|---|---|
| (7) | マルウェアを検出した際やプロセスがブロックされた際に利用者にポップアップが表示可能なこと。 | － | － | － |
| (8) | マルウェアを検出した際に利用者側に表示されるポップアップは、利用者が気づき応答操作を行うまで表示され続けること。 | 2 | 1 | 0 |
| (9) | メール経由の攻撃、HTTPS を含むウェブ経由の攻撃、USB からの感染など、あらゆる経路からのエンドポイントへの攻撃に対応すること。 | － | － | － |
| (10) | ランサムウェアにおいては、リアルタイムでの対応を必要とするため、管理者がオペレーション関与することなく、Windows 端末にある該当プロセスを停止するなどの処置を行えること。 | － | － | － |
| (11) | 正常な動作を攻撃と過検知した場合には、ファイルハッシュ値や特定のふるまいを基にした検知の無効化が可能であること。 | － | － | － |
| (12) | 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。 | － | － | － |
| (13) | 防御ルール（ブロックポリシー）を追加する際、防御対象となりうるイベントを過去30日以上のログから検索し、業務影響を判別できること。 | 2 | 1 | 0 |
| (14) | EDR 機能にて収集されたログ情報から、マルウェアなどのインシデントを検知可能なこと。 | － | － | － |
| (15) | 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。<br>・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）<br>・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）<br>・実行されたファイル名およびハッシュ値<br>・実行されたコマンドラインの内容<br>・通信先のドメイン、IPアドレス<br>・レジストリの変更履歴<br>・呼び出されたDLLライブラリ<br>・特権名<br>・権限昇格の有無 | － | － | － |
| (16) | 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こと。 | － | － | － |
| (17) | 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。 | － | － | － |
| (18) | 攻撃を検知した場合には、その根本原因、感染した端末の全台の特定、影響範囲の関係、時系列での不正なふるまいの状況を管理コンソールで把握できること。 | － | － | － |
| (19) | 攻撃手法の分析や特定などに活用するために、検知されたアラートログに対して、攻撃種別を示す独自のタグ情報および攻撃手法を分類したフレームワークであるMITRE ATT&CK のTID が付与できること。 | － | － | － |
| (20) | サイバー攻撃の予防と対策を強化を目的として、STIX/TAXII または YARA ルールに対応していること。 | 2 | 1 | 0 |
| (21) | 収集されたログの検索機能を有すること。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。 | － | － | － |
| (22) | 脅威であるかに関わらず、Windows 端末上に存在するスクリプト及び実行ファイルのハッシュ値やファイル名等のメタデータを収集できること。 | － | － | － |
| (23) | 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。 | 2 | 1 | 0 |
| (24) | エンドポイントがオフライン状態であっても、管理コンソールで直近のログに対して調査が可能であること。 | － | － | － |
| (25) | エンドポイントがオフライン状態であっても、エージェントはログを収集し、後でオンラインになったときにマネージャーに送信すること。 | － | － | － |
| (26) | 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。 | － | － | － |
| (27) | 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、利用者に表示されるメッセージに任意の内容を記載できること。 | 2 | 1 | 0 |
| (28) | 独自のふるまい検知のルールを作成可能なこと。 | 2 | 1 | 0 |
| (29) | 利用者側に表示されるポップアップやエージェントの管理画面などの言語は日本語であること。 | － | － | － |

### 3 端末管理・調査および衛生管理機能

| # | 要件 | 対応可否欄の記載 | | |
|---|---|---|---|---|
| | | ○ | △ | × |
| (1) | インシデント検知後の対策として、Windowsに対して管理コンソールから被疑端末を隔離（ネットワークから遮断）することが可能であること。この際、管理コンソールとの接続のみ維持できること。 | － | － | － |
| (2) | 管理コンソールより、端末の隔離解除が可能であること。 | － | － | － |
| (3) | 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。 | － | － | － |
| (4) | 端末が管理コンソールと未接続の場合には、一定期間内に接続復帰した際の対応を予め設定可能であること。 | － | － | － |
| (5) | 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。<br>・被疑ファイルの隔離または削除<br>・ファイルのうち調査に必要な箇所の取得<br>・ファイルの配置、実行<br>・プロセスの終了<br>・メモリダンプの取得<br>・レジストリの修復または削除<br>・OS 標準コマンド等を用いて任意のコマンドを実行 | － | － | － |

| | | | | |
|---|---|---|---|---|
| (6) | 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。<br>・被疑ファイルの隔離または削除<br>・ファイルのうち調査に必要な箇所の取得<br>・ファイルの配置、実行<br>・プロセスの終了<br>・メモリダンプの取得<br>・OS 標準コマンド等を用いて任意のコマンドを実行 | 2 | 1 | 0 |
| (7) | 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（端末内のユーザー、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、全端末に対して任意のタイミング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。 | － | － | － |
| (8) | 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。<br>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。 | － | － | － |
| (9) | 第三者機関（全世界の脅威を監視し、それを元にインテリジェンスを日々作成し、提供するベンダ）の脅威インテリジェンスを無償で取り込むことができること。 | － | － | － |

## 4 管理機能

| # | 要件 | 対応可否欄の記載 | | |
|---|---|---|---|---|
| | | ○ | △ | × |
| (1) | 1～3項に記載の各機能を利用するための管理コンソールは部局ごとに単一（シングルコンソール）であること。 | － | － | － |
| (2) | 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。 | － | － | － |
| (3) | 管理コンソールの表示言語は日本語であること。 | － | － | － |
| (4) | 管理画面よりレポートファイル（PDF等）が日本語で出力できること。 | 4 | 2 | 0 |
| (5) | アラート検知時に、メール発報が可能なこと。また、発報条件をカスタマイズできること。 | － | － | － |
| (6) | アラート検知時に発報されるメールは日本語のプレーンテキスト形式であること。 | 2 | 1 | 0 |
| (7) | 端末にて収集された不審事項のログは30日以上保持すること。また、アラート対象となるログは1年以上保持すること。ただし、3か月以上経過したものについては、MDR 側で抽出・提供可能な状態であれば、EDR の管理コンソールで直接確認できなくても良いものとする。収集されたログは、保存期間経過後に自動で削除されること。 | － | － | － |
| (8) | 外部連携を目的として、SIEM 製品またはログサーバーへ検知ログを送付することができること。また、別製品との連携ができるよう API が一般公開されていること。 | 2 | 1 | 0 |
| (9) | 端末と管理サーバー間の通信は暗号化されていること。 | － | － | － |
| (10) | 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。 | － | － | － |
| (11) | エージェントの動作ログ取得、再起動、アップデート、ログアップロードの停止が、管理画面より遠隔にて実施できること。 | － | － | － |
| (12) | Windows に対して、エージェントのバージョンアップが管理コンソール上から実施可能であること。 | － | － | － |
| (13) | Windows に対して、エージェントのアンインストールまたは機能停止が管理コンソール上から実施可能であること。 | － | － | － |
| (14) | Linux および macOS に対して、エージェントのバージョンアップが、管理コンソール上から実施可能であること。 | 2 | 1 | 0 |
| (15) | エージェントのバージョンアップにおいて、管理画面にて対象端末を任意に選択でき、対応できること。 | － | － | － |
| (16) | 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。 | 2 | 1 | 0 |
| (17) | 既存のネットワーク装置に影響がないよう、ローカルスキャンのためのシグネチャ配信サーバーを市に用意し、エンドポイントが配信サーバーからシグネチャのアップデートができること。または、サーバーからダウンロードするシグネチャ等のファイルについては経路のプロキシサーバーでキャッシュ可能なよう配慮されていること。 | － | － | － |
| (18) | 複数の部局に分かれて管理が可能なよう、管理コンソールにてマルチテナント機能を有すること。（部局単位で登録クライアントを分け、部局管理者アカウントではそれぞれの部局の範囲内のクライアントに関する情報だけを確認することができ、部局毎に異なる EDR の管理および制御ポリシーを作成し、かつ作成されたポリシー毎に MDR にて運用フローの策定やインシデント対応、月次の運用レポートを提供することができること。インシデントを発見した際に送信される通報メールは当該部局管理者のみに送られること。） | － | － | － |
| (19) | 設定の即時反映のために、管理コンソール上で変更されたポリシーが速やかに適用されること。<br>(ネットワークにボトルネックがない場合において、概ね2分以内なら○、概ね5分以内なら△、それを超える場合は×としてください) | 4 | 2 | 0 |

## 5 運用保守

| # | 要件 | 対応可否欄の記載 | | |
|---|---|---|---|---|
| | | ○ | △ | × |
| (1) | 構築期間（～2022/9/30）及び本サービス予定期間（2022/10/1～2027/9/30）において、製品に関する問い合わせや不具合修正、バージョンアップ等の保守サポートを受けられること。 | － | － | － |
| (2) | 保守サポートは少なくとも平日日中帯（9:00～17:00）において受け付け、日本語で対応されること。ただしシステム障害等の緊急対応が必要となる事案が発生した場合については24時間365日受け付けること。 | － | － | － |
| (3) | 保守サポート期間中は、最新の製品（エージェント）バージョンが利用可能なこと。 | － | － | － |
| (4) | 日本語の製品ドキュメントが提供されること。 | － | － | － |
| (5) | 本市環境の設計・構築に携わった、またはその引継ぎを受けたエンジニアによる、本市での導入・稼働状況を踏まえた運用支援サービスを提供すること。 | － | － | － |

| | | | | |
|---|---|---|---|---|
| (6) | 運用支援サービスでは、EDR 製品メーカーのエンジニアと連携し EDR 製品の運用保守に関わる全般の問い合わせに対応を行うこと。 | － | － | － |
| (7) | 運用支援エンジニアは運用期間中は本市の構成や製品バージョンを常に把握すること。<br>運用期間中に構成変更があった場合は最新構成を把握した上で、EDR 製品で実現可能な最適なセキュリティ対策を提言すること。 | － | － | － |
| (8) | 運用支援エンジニアは EDR 製品の不具合に起因したインシデント発生時など有事の際に迅速かつ確実に対応可能なよう、受託者とともに MDR サービス、EDR 製品メーカーのエンジニアと連携して対応できる体制を構築すること。 | － | － | － |
| (9) | 運用支援エンジニアは EDR ポリシーの最適化や変更手順の支援、MDR からのレポートや脆弱性情報、直近のセキュリティ攻撃動向を踏まえたシステム最適化検討を行うこと。 | － | － | － |
| (10) | 運用支援エンジニアは EDR 製品を利用期間を通じて適切に運用維持がなされるために、エージェントバージョンアップ時の影響範囲の整理や、OS や併存する資産管理製品との互換性確認、手順の検討支援、導入前検証の支援等を行うこと。 | － | － | － |
| (11) | EDR 製品メーカーのエンジニアと連携した運用支援エンジニアによる運用保守定例会議を月次で開催すること。 | － | － | － |
| (12) | 定例会議では、本市の端末・サーバー環境のセキュリティ維持・向上及び EDR 自体の安定稼働とセキュリティ維持を目的として、少なくとも次のような内容を含むこと。<br>・EDR 製品メーカーより提供される既知事例やセキュリティ情報を日本語で提供すること。ただし本市のセキュリティを脅かす重大な問題や脆弱性が発見された場合は、定例会議を待たずに臨時での情報提供と対策を検討すること。<br>・不具合修正パッチ、セキュリティパッチ、バージョンアップの適用是非を検討・提案すること。また、本市ネットワーク構成を踏まえた適用計画を立案すること。<br>・バージョンアップに伴い提供される新機能の活用検討を行うこと。<br>・最適なセキュリティレベルを維持するための EDR 制御ポリシーの策定およびシステム最適化検討を行うこと。 | － | － | － |
| (13) | 障害発生時に取得すべき情報や切り分け手法を提供し、障害発生時に迅速に対応できるようにすること。 | － | － | － |
| (14) | 本市運用者に対する教育を実施すること。 | － | － | － |
| (15) | EDR 製品に起因する不具合が発生した場合、市に対して誠意をもって対応すること。 | － | － | － |

## 6 クラウドサービス （※クラウド型で提案する場合に限る）

| # | 要件 | 対応可否欄の記載 | | |
|---|---|---|---|---|
| | | ○ | △ | × |
| (1) | 日本国内のデータセンター（日本リージョン）に存在すること。 | － | － | － |
| (2) | 日本法に準拠し、裁判管轄は日本であること。 | － | － | － |
| (3) | ISO/IEC 27001, 27017, 27018 又は SOC2 の外部監査による認証を取得していること。 | － | － | － |
| (4) | クラウドサービスの可用性に関する SLA は99.5%以上であること。 | － | － | － |
| (5) | ペネトレーションテストを定期的に実施していること。 | － | － | － |
| (6) | ペネトレーションテストの診断レポートを提出可能であること。 | 2 | 1 | 0 |
| (7) | 管理コンソールへのログインは二要素認証が可能なこと。 | － | － | － |
| (8) | 管理コンソールへの接続手段として、インターネット VPN や閉域網が受け入れ可能であるか、インターネットからの直接接続に関しては接続元 IP アドレスを限定できること。 | 4 | 2 | 0 |

| | |
|---|---|
| 合計 | 56 |

# 別紙 MDRサービス要件対応表（評価基準）

「対応」欄については以下の基準で記入してください。
いずれも本契約期間中（令和4年9月末）までに対応予定であれば良いものとします。予定のものは備考欄にその旨を記載してください。

「必須」欄が○の項目
○ ： 対応可能
× ： 対応不可（対応不可が1項目でもある場合不合格）

「必須」欄が○でない項目
○ ： 対応可能
△ ： 部分的に対応可能または代替手段により対応可能等（「備考」欄に記入してください）
× ： 対応不可

## 1 インシデント調査・対応

| # | 要件 | 対応可否欄の記載 | | |
|---|---|---|---|---|
| | | ○ | △ | × |
| (1) | 「別紙 EDR機能要件」のセキュリティ対策ソフトウェア（EDR）を利用して、発生したインシデントに対して早期に、検知、通知、対策、解析、回復を行うことを目的としたセキュリティ運用管理サービス（MDR）を提供すること。 | － | － | － |
| (2) | セキュリティ運用管理サービスの提供時間は24時間365日とすること。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、対策、解析、回復のサービスを提供すること。 | － | － | － |
| (3) | 監視対象は EDR のほか Active Directory サーバーのイベントログを含み、常時監視・相関分析対象とし、インシデントレベルに応じた通知を行うこと。<br>なお、Active Directory サーバーの状況は以下の通り。<br>・監視対象のサーバー数は、合計10程度を予定している。<br>・監視対象のサーバー群が出力するイベントログの総量は 15GB/日 程度である。 | － | － | － |
| (4) | 監視対象について常時監視を行い、相関分析できること。<br>発生したアラートについて、アナリストにより分析し、重要度をふるい分け、重要なもののみを通知すること。<br>重要度のふるい分けの考え方をあらかじめ共有すること。 | － | － | － |
| (5) | 発生したインシデントについて、EDRの判定だけでなく、運用管理サービスが有する判定基準（脅威インテリジェンス）も適用し、アラートレベルの判定を行うこと。 | － | － | － |
| (6) | 判定されたアラートレベルに応じて、脅威（検体）や被疑端末の隔離措置が可能なこと。また、隔離措置の実施を運用管理者が判断できるよう、WebUI、メール、チャット、電話等による隔離承認が可能なこと。 | － | － | － |
| (7) | 端末隔離時には指定のメッセージをデスクトップに通知が可能なこと。メッセージには任意の文字列を設定可能なこと。 | 2 | 1 | 0 |
| (8) | インシデント対応完了後に隔離解除を実施すること。隔離解除の際も、指定のメッセージをデスクトップに通知が可能なこと。メッセージには任意の文字列を設定可能なこと。 | 2 | 1 | 0 |
| (9) | 判定されたアラートレベルに応じて、運用管理サービスから管理者に対してメール通知が可能なこと。緊急性の高いインシデントが発生した場合には、メールでの通知だけでなく、指定された番号に対して、電話で通知が可能なこと。<br>電話通知先は少なくとも5件以上登録できること。<br>通知に際しては平日業務時間内、平日業務時間外、土日祝祭日で通知先を切り替えられること。<br>なお、本運用フロー（ルール）は、本市の要望に応じて部局毎に定義が可能なこと。 | － | － | － |
| (10) | 発生したインシデントのアラートレベルが変化した際、都度通報を行うこと。 | 2 | 1 | 0 |
| (11) | インシデント通報に関する問合せも24時間365日対応可能すること。 | － | － | － |
| (12) | 運用管理サービスとして、初期通知に加えて追加の通知が必要と判断した場合、原則としてアラートレベル判定後翌営業日までに詳細の分析結果（インシデントの発生に至るまでのプロセスや影響範囲など）を通知すること。 | － | － | － |
| (13) | EDRの防御機能で対策が行われなかったインシデントが発生した場合、運用管理サービスにて必要な対策を実施すること。対策として、プロセスの停止、ファイルの削除、レジストリの修正など侵害の痕跡を除去すること。 | － | － | － |
| (14) | インシデントの再発を抑制するために、検出された検体のファイルハッシュ値などを用いたブラックリストの登録、攻撃に用いられたC&Cサーバーの URL情報や適用すべきパッチ、ソフトウェア情報の提供など、再発防止策を講ずること。 | － | － | － |
| (15) | 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、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。 | 2 | 1 | 0 |
| (16) | EDRのポリシーにより実行停止されたアプリケーションのうち明らかに過検知・誤検知とアナリストが判断できたものについては、運用管理者の依頼を受けることなく自発的にホワイトリストに登録する対応が可能なこと。 | 2 | 1 | 0 |
| (17) | インシデント対応の進捗状況を随時確認できる仕組みを提供すること。 | － | － | － |
| (18) | 本市の要望に応じて、EDRのホワイトリスト／ブラックリスト管理ができること。 | － | － | － |
| (19) | 必要に応じて、関連するセキュリティ装置（Active Directory サーバーやファイアウォール、プロキシなど）とのログの突合調査にも対応可能なこと。 | － | － | － |
| (20) | 現在神奈川セキュリティクラウドで監視・分析を行っている、ファイアウォール・IPS・プロキシ・メールゲートウェイ・DNS 等についても、別途協議により監視・分析対象とする拡張が可能なこと。 | 4 | 2 | 0 |
| (21) | 問い合わせ対応言語は時間帯によらず日本語であること。 | － | － | － |

## 2 運用管理

| # | 要件 | 対応可否欄の記載 | | |
|---|---|---|---|---|
| | | ○ | △ | × |

| | | | | |
|---|---|---|---|---|
| (1) | 提供する運用フローや運用管理者情報などを決定するために、サービス開始前にヒアリングシートなどをもとに、サービス提供設計を実施すること。また、運用フローの設計内容は、サービス開始後でも変更可能なこと。 | － | － | － |
| (2) | 月内に発生したアラートの検知および対応結果のサマリ、緊急度の高いセキュリティ関連情報を含む月次レポートを提供すること。 | － | － | － |
| (3) | レポートには、導入端末の監視機能を用いた脅威情報や端末のパッチ適用状況や RDP 等の危険性の高いサービスの設定状況、ブラウザのアドオンなど脆弱性につながる恐れがある情報等の健全性情報を含むこと。 | 2 | 1 | 0 |
| (4) | レポートは本市の要望に合わせて、部局毎に提示可能なこと。レポートは、他部局の利用状況や導入端末情報がレポートに表記されないようにすること。ただし、検出された検体のブラックリスト登録は全部局に適用すること。 | － | － | － |
| (5) | 月次レポートの情報共有及び MDR 運用の最適化を目的とした打ち合わせに対応可能なこと。開催頻度は令和4年度中は月次、令和5年度以降は四半期に1回程度を想定する。 | － | － | － |
| (6) | 端末の属性（PC、サーバー、設置拠点、所属部署など）に応じた運用フローを部局毎に設計できること。 | － | － | － |
| (7) | サービス提供を実施するデータセンターおよび本サービスに関連するデータが保存されるデータセンターは日本国内に存在すること。 | － | － | － |
| (8) | サービス提供終了時は、サービスにて定められた内容に従い、適切にデータが削除されること。 | － | － | － |
| (9) | 本市専用のポータルサイト（ページ）を用意すること。ポータルサイトでは、各種レポート（月次レポートや、一次/二次レポート）のダウンロードが可能なこと。 | 2 | 1 | 0 |
| (10) | 令和4年度末に更新予定の次期神奈川情報セキュリティクラウド（KSC）へインシデント情報を通報するなど、別途協議により次期 KSC と連携する対応が可能であること。 | 4 | 2 | 0 |

3 その他

| # | 要件 | 対応可否欄の記載 | | |
|---|---|---|---|---|
| | | ○ | △ | × |
| (1) | 日本国内でデータを処理し、保管していること。また、分析基盤も国内であること。 | － | － | － |
| (2) | 日本法に準拠し、裁判管轄は日本であること。 | － | － | － |
| (3) | 監視センターは、ISO/IEC27001 の外部監査による認証を取得していること。 | － | － | － |
| (4) | 監視センターは、(独)情報処理推進機構が公開する「情報セキュリティサービス基準適合サービスリスト」の「セキュリティ監視・運用サービス」に含まれているものであること。 | － | － | － |
| (5) | 「別紙 EDR機能要件」のEDRとして提案する製品に対するMDRサービスとして、単一組織で1万台を超える導入・運用実績を有すること。 | 2 | 1 | 0 |

| | |
|---|---|
| 合計 | 24 |