箕面市行政情報ネットワークにおける
EDR ソフトウェア等保守業務委託
仕様書

令和４年６月

箕面市総務部システム管理室

１．目的

本件は、総務省ガイドラインにおいて求められている未知の不正プログラム対策（以下「EDR」という。）、及びそれを活用した情報セキュリティ専門人材によるインシデントの早期検知・対処サービス（以下「MDR」という。）として導入するものであり、EDR ソフトウェアにかかる保守業務等を行う。

２．名称

箕面市行政情報ネットワークにおける EDR ソフトウェア等保守業務委託

３．契約内容および契約期間

内容	EDR ソフトウェアライセンス（1,165 ライセンス） MDR によるインシデントの検知、解析、隔離等のサービス
稼働開始予定日	令和４年９月１日（木）
契約期間	令和４年９月１日（木）から令和７年８月３１日（日）まで （長期継続契約）

４．機能等の要件

EDR ソフトウェア等を導入するうえで、次の(1)～(3)を満たすことする。

（１）EDR サービスの機能要件

① 検知機能

端末上のログを取得、解析し、ウィルスなどの不審な挙動を自動で検知する機能。

- 端末上のログを取得、解析し、ウイルスなどの不審な挙動を IOC(Indicator of Compromise)によるリアルタイム検知が可能であること。
- 定義等が随時更新されること。
- 自動検知された不審な挙動を、管理者あてに速やかに通知すること。

② 隔離機能

アラートを検知した端末をネットワークから隔離する機能

- 隔離は管理サーバーと DNS サーバー以外、全ての通信を遮断すること。
- インターネットへの接続をリモートで停止できること。
- ポリシーを事前に定義することにより、検知と同時に自動で端末隔離ができること。

③ 調査機能

収集した端末のログ情報をもとに、マルウェアの侵入経路や内部活動、その影響範囲を調査する機能。

- 侵入経路、システム改変の有無、ファイル操作の有無、他の端末における感染等の有無を調査できること。

④ その他

- AI 型マルウェア検知機能で検知したファイルはセキュリティオペレーションセンター（以下「SOC」という。）で取得し、検体解析を実施することで、悪質なファイルとして特定されたファイルのみ通知を行うこと。
- 管理者用サイトから、EDR がインストールされている端末の管理、アラートの件数・内容の閲覧が可能であること。
- EDR のインストール数が契約総数を超えない限り、ソフトウェアのアンインストール、インストールを自由に行えること。
- 監視対象のクライアント・端末の入れ替え等があった場合に備え、一時的に契約ライセンス数を超過してもサービスの提供に問題がないこと。
- OS からより多くの情報を収集し、不審な挙動を検知するためにカーネルモードで動作させること。
- メーカーが主導して、遠隔でエージェントアップデートを実施できること。また、アップデートに際して時期やタイミングは調整可能なものとすること。
- 利用者向けに日本語で表記された管理画面があること。
- 日本語によるインシデント通知メール、件名、本文等のカスタマイズが可能であること。

（2）作業要件

- エージェントをインストールした端末が正常に管理サイトに登録されているか、SOC で確認すること。また、どの端末にインストールしたかは随時本市 OA サポートが連絡すること。
- インシデント発生時の、エージェントにおける対応フローを提示すること。

（3）端末の機能要件

OS：windows 10 Pro
メモリ：8GB
CPU：Intel

５．保守業務等

4.機能等の要件を満たすEDRソフトウェア等のサービスを受けるために必要な各種保守業務等を行うこと。また、必要に応じて、EDRソフトウェアのインストール用メディア２部、インストール手順書１通を、稼働開始日の１ヶ月前までに箕面市総務部システム管理室（箕面市西小路３丁目１番８号）へ納入すること。

６．実施要件

・本仕様書の条件を満たすこと。
・本件に係るサービスは、端末更新等の継続しがたい理由がある場合を除き、契約期間終了以降も継続して利用することを前提とする。
・EDRソフトウェアのインストール作業は、本市OAサポートが行う。
・本件に係る業務の範囲は検知後の隔離までとし、マルウェアの削除、端末の初期化及びリストア等の復旧作業は、本市OAサポートが行う。
・EDRソフトウェアの導入、及びMDRの運用に係る端末の監視、隔離、復旧等について、本市OAサポートと連携すること。
・インシデントには件数の上限無く対応できること。
・物品の仕様を遵守し、履行する上で必要となるすべての諸経費は受注者の負担とする。
・前記の各項に関し、または前記以外に必要な事項が生じた場合は、箕面市総務部システム管理室と協議すること。また、契約後における仕様書の疑義は発注者の解釈によるものとする。