

箕面市行政情報ネットワークにおける  
EDR ソフトウェア等導入業務委託  
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、初期設定・導入支援等を行う。

## 2. 名称

箕面市行政情報ネットワークにおける EDR ソフトウェア等導入業務委託

## 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導入のための初期設定・導入支援等 (1,165 ライセンス)
契約期間	契約締結日から令和4年8月31日（水）まで

## 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、ウイ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。
- 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

- エージェントインストール作業は、本市OAサポートが行うものとし、受注者は資産管理ツールを用いた配布テストを実施し、全庁配布ができるように手順をレクチャーすること。なお事前配信前にクラウド環境は構築していることとする。
- 共存するウイルス対策の検索対象から、導入するEDR関連のディレクトリを除外すること。また、検索除外対象とすべきディレクトリ情報を提供すること。
- 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. 導入業務等

4.機能等の要件を満たす EDR ソフトウェアの導入を行うために必要な初期設定・導入支援等を行うこと。

## 6. 実施要件

- ・本仕様書の条件を満たすこと。
- ・本業務について、必要に応じて本市 OA サポートと連携すること。
- ・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。