業務仕様書

1. 件名

市立東大阪医療センターセキュリティ対策環境整備業務

2. 納入期限

令和5年3月31日まで

3. 調達背景および目的

昨今、医療機関へのサイバー攻撃が増加してきており、セキュリティ対策は喫緊の課題である。
当センターにおいてもセキュリティアドバイザーを用いて調査した結果、以下の指摘を受けた。

・不正な通信を検知する仕組みがない
・USBメモリ等の外部デバイスの制限がない
・PCの操作記録を取る仕組みがない
・ネットワークに接続されている機器の管理が不十分
・従来型のウィルス対策ソフトのみで保護されており、最新のサイバー攻撃への対応ができていない

現在は従来型のウィルス対策ソフト等を用いてセキュリティ対策を施しているが、最新のサイバー攻撃等への対応のため必要な機器並びにシステムを構築し、更なるセキュリティ対策の向上を目的とする。

4. 調達範囲

本業務で調達するシステムの内訳を以下に示す。詳細は、「6. 調達機器詳細仕様」を参照すること。

・TrendMicro Deep Discovery Inspector 1300 with XDR HW 5年保証版 ・・ 2台
・TrendMicro ApexOne Saas with XDR ・・・・・・・・・・ クライアント1200台分
・MOTEX LANSCOPE エンドポイントマネージャー オンプレミス版 ・ Pack1000 1000台分

いずれも構築費用と初年度ソフトウェア費用を含む

5. 基本要件

(ア)令和5年3月31日までに本仕様に定める設計・設定・設置作業を実施の上、当センターに納品し、本システムを稼働させること。
(イ)設計・設定が明記無き場合、当センターと協議の上、仕様を確定させ構築作業を行うこと。
(ウ)令和5年4月1日以降の運用保守については、落札者と協議のうえ別途契約とする。
(エ)調達機器は必要な要件を満たし、全ての機能が正常に動作することを確認したうえで納品すること。
(オ)調達機器と既存機器との接続に必要となるLAN敷設作業は本調達に含めること。なお必要なLANケーブル（Cat5e）については当センターで用意可能である。

(カ)本仕様に定めていない事項並びに仕様内容に疑義が生じた場合は、当センターと協議の上、決定する。
(キ)本契約を通じて知り得た情報については、第三者に情報を漏らしてはならない。

6. 調達機器詳細仕様

6.1.TrendMicro Deep Discovery Inspector

仕様
不正な URL へのアクセス検知ができること
疑わしい拡張子の付いた実行ファイルの転送（各種通信プロトコル）が検知できること
疑わしいファイル（実行ファイル・Office ドキュメント・PDF など）を仮想環境で実行し危険性を判別できること
解析処理可能な総スループットが 1Gbps 以上であること
通信監視用のポートとして 10/100/1000 BASE-T イーサネットポートを 5 以上有すること
GUI、レポート、ドキュメント、ヘルプが日本語化されていること
仮想アナライザの環境として、Windows10×4 領域（Office2016 インストール）を用意すること
ハードウェア保守 5 年分、初年度ソフトウェア保守費用を含むこと
当センターの指定するラックへの設置作業、LAN 配線作業、設置に要する部材の費用を含むこと。なお、既設のコアスイッチへの接続については、別途当センターが用意する。 必要な LAN ケーブルは当センターが用意する。
ネットワーク接続後、適切なモニタリング状態になるようチューニングを行うこと
複数の監視対象をカバーするため、機能要件を満たす製品を 2 台導入すること
概ね 5 分程度の電源停止に耐えうる UPS 装置を含むこと

6.2.TrendMicro ApexOne Saas with XDR

仕様
TSSL Trend Micro Apex One SaaS with XDR 1200 台分のライセンス費用（既存 250 台の更新＋950 台の新規）
TSSL Trend Micro Apex One SaaS Cloud Sandbox Option 1200 台分のライセンス費用（既存 250 台の更新＋950 台の新規）
EDR 環境としての管理サーバ環境を受託者で設定すること。
ネットワークセンサーのログデータと相関分析が可能なコンソールが提供され、左記のコンソールにおいて保護対象のクライアントへのコマンド実行等のリモート調査機能が提供されること
HIS 系ネットワークから SaaS 環境への通信のために必要な通信先のアドレス・プロトコル・ポート番号などの接続情報を明示すること
EDR インストール後の管理対象 PC でのセキュリティ監視サービスを提供すること（令和 5 年 4 月以降）
対象クライアントへのインストール作業について、インストール手順書を用意すること

6.3.MOTEX LANSCOPE エンドポイントマネージャー オンプレミス版

仕様
LANSCOPE オンプレミス版 マネージャーライセンス 4 コア版　1 セット
LANSCOPE オンプレミス版　パック 1000(資産管理・ファイル配布・操作ログ管理・デバイス管理機能を含む) 1000 セット
LANSCOPE オンプレミス版 PC 遮断ライセンス　10 式
1000 ライセンスの管理および 5 年間のログ保存に必要十分な性能を持つ管理サーバを構築し、当センター指定のラックへ設置、LAN 配線を行うこと 必要な LAN ケーブルは当センターが用意する。
概ね 5 分程度の電源停止に耐えうる UPS 装置を含むこと
USB-HDD 等のバックアップ用ディスクを含み定期的にバックアップを行うこと
対象クライアント PC へのインストール作業は ActiveDirectory のログオンスクリプトでの展開を想定し、対象クライアントへのインストール状況を確認すること。
不正 PC を遮断するために、当センターが指定するセグメントに対して、遮断エージェントの設定を行うこと。

7. 納入する機器のハード保守

(ア)調達機器は構築完了後の本稼働(令和 5 年 4 月 1 日)から 5 年間の運用保守が可能な機器を選定し、調達機器に関するハードウェア保守費用については、本契約金額に含めること。

(イ)5 年間内にメーカ保守が終了するなど運用保守ができなくなった場合は、落札者の責任においてサポート可能な機器へ無償で入れ替えること。

8. 運用保守（令和 5 年 4 月 1 日～令和 6 年 3 月 31 日　1 年間）

納入する機器及びソフトウェアが令和 5 年 4 月 1 日から本稼動するため、運用保守に関するサービス費用を積算すること。なお、運用保守は別途契約となるため、今回の調達には含まないが、参考見積として提示すること。

(ア)TrendMicro Deep Discovery Inspector

① 24 時間 365 日のアラートモニタリングを実施し、リスク度を判定した上でリスクの高い検知が行われた場合に、電話またはメールにて当センター担当者へ一次連絡を行うこと。

② 高リスクに対しての影響度合いを考慮し、初動対応の指示を当センター担当者へ行うこと。

③ リスク度の高い検知が行われ、侵害が起こった場合等の現地対応は別途契約するものとする。

④ 落札者は、納入したシステムに関する問い合わせ、セキュリティ情報の提供、障害発生時における解決支援を行うこと。

(イ) TrendMicro ApexOne Saas with XDR

① インストール済みクライアント PC の監視サービスを提供すること。

② 対応時間は最低限平日 9 時～17 時の範囲とし、セキュリティリスクの高い挙動が確認された場合は、当センター担当者へ通報すること。

③ 状況に応じ、対象のクライアント PC を遮断し、調査を行うこと。

④ 落札者は、納入したシステムに関する問い合わせ、セキュリティ情報の提供、障害発生時にお

ける解決支援を行うこととする。

(ウ) MOTEX LANSCOPE

① 納入したソフトウェアに対する不具合修正に対するマイナーバージョン等がリリースされた場合は、その影響度を判断したうえで当院と協議の上、適用作業を行うこと。目安は年 1 回程度の頻度を想定している。

② メジャーバージョンアップおよびその際のクライアント展開は別途契約するものとする。

(エ)その他

① 運用保守は原則落札者と別途契約するが、運用保守業者は別途選定することがある。

9. 完成図書

以下に示すものを作成し、業務完了後、電子媒体で 1 部を提出すること。

(ア)作業計画書

(イ)基本、詳細設計書

(ウ)業務完了報告書

(エ)施工写真

(オ)各種運用マニュアル

以　上