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強化用ネットワーク監視機器整備業務

2. 契約期間

契約締結日から令和 6 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。
先の大阪府下の医療機関におけるサイバー攻撃においてはサプライチェーンからの侵入による障害が発生しており、ネットワークセキュリティにおいては従来の境界型防御では不十分であることが示されたところである。

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ネットワーク内の不正な通信を検知・遮断する仕組みを構築し、更なるセキュリティ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、「7. 調達機器詳細仕様」を参照すること。

・不正通信検知・遮断システム・・・・・・1200 デバイスに対応できること
・当センターコアスイッチ(QX-S6648XP)から調達機器までの LAN 配線部材一式とその敷設
（SFP モジュール２つを含むこと）

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)令和 5 年 4 月 1 日から 1 年間の運用保守に要する費用は調達額に含むこと。
(ウ)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。
(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。現地調査の上で既設 LAN ケーブルが利用可能な場合は流用しても構わない。
(カ)本仕様に定めていない事項に関しては、落札者と当センターとの協議により決定する。
(キ)落札者は、仕様内容に疑義が生じた場合は、当センターと協議の上、その指示に従うこと。
(ク)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

仕様
筐体サイズは 19 インチラックの 2U 以内に収まるサイズであること。
1Gbe 管理者インターフェイスを１つ以上有すること。
1Gbe 分析ポート１つと 10Gbe 分析ポートを４つ以上有すること。
ピーク持続スループットは最大 5Gbps まで対応できる処理能力を有すること。
拡張モジュールを使うことにより 10Gbe のポートをさらに 6 つ増やせること。
最大ユニーク内部デバイス数は最大で 36,000 デバイスまで収容できること。
1 分あたりの最大接続数は 100,000 まで解析可能な処理能力を有すること。

6.1. 不正通信検知機能

仕様
IDS/IPS ゲートウェイ型サンドボックス、アンチウィルス等で一般的に用いられるパターンマッチングやふるまい検知では検出できない、未知のマルウェアへの感染や疑わしい挙動を検出できること。
通信元、通信先、データ送受信量、時間帯などのトラフィック特性を自動で学習・分析し、インシデントの検出基準として用いること。
インシデント発生時に事象の詳細を迅速に分析し、原因や影響範囲を確認できること。また、アップロード/ダウンロードなどの通信を再現できること。
自動的にネットワーク構成を検出し、３Ｄモデルなどの判りやすい形式で可視化し、該当端末の通信先などを俯瞰的かつ直感的に確認できること
リアルタイムでネットワークトラフィックを監視・分析し、インシデントの発生を即時にアラートとして複数の指定メールアドレスへ通知できること
SSH の連続した認証の失敗、DNS サーバへの大量のクエリ送信、Windows ログイン時に通常と異なるアカウントを使用した等、不正な活動の兆候を捉え、インシデントの発生を検知できること
セキュリティリスク等に基づく重要度に応じた閾値を設定することにより、通知するアラートのレベルをコントロールできること
リアルタイムで通信の監視・分析ができるだけでなく、特定端末の通信状況を最大 1 ヶ月前まで遡って確認できる機能を有すること
アラートの検出ロジックはベイズ推定など数学モデルに基づいたものであること
端末内のプロセスの動作を停止させることにより、マルウェアの起動を阻止する製品ではなく、LAN を監視し、不自然な振る舞いを行う端末を検知する製品であること
LAN 内部のマルウェアに感染した端末からの、ポートスキャンや脆弱性スキャンなどの偵察行動や、ファイルのアップロードなどの情報窃取行動など、悪意ある振る舞いを検知できること
前記 2 のマルウェアについては、シグネチャやブラックリストに掲載される前(いわゆるゼロデイ攻撃)であっても検知できること
検知エンジンは、ファイアウォールや IPS で一般的なシグネチャやブラックリストを使用するものではなく、AI による自己学習機能によるものであること
AI による自己学習は、LAN での通常の通信や動作を学習するものであることとし、LAN 内の情報を収集・監視し、通常の振る舞いと異常な振る舞いを判定するものであること
ネットワークに接続される機器を無理なく監視できること
異常を検知した場合に、検知された異常の分析を支援する管理画面が用意されていること

6.2. 通信遮断機能

仕様
TCP/IP 通信に対してリセットパケットを用いることでアラートの元となった特定の通信を遮断できること。
また、この通信遮断機能は動作対象となったデバイスに対してエージェントを事前にインストールすることなく機能すること。
通信遮断の方式は管理者による承認が必要なパッシブモードと、承認が不要な自動モードの双方を有していること。
通信遮断の範囲は管理者にてチューニングできることとし、特定の通信の遮断からデバイスの隔離など範囲を選べること。

7. 運用保守（令和 5 年 4 月 1 日～）

納入する機器及びソフトウェアを令和 5 年 4 月 1 日から運用開始するため、運用保守に関するサービスを以下の通り提供すること。

（ア）システム保守・障害対応

① ハードウェア故障時の交換機器の送付を行うこと
② 機器の故障・不良後の設定作業の支援を保守に含めること
③ 操作方法・機器の各種設定の問い合わせに応じること
④ 最新情報の提供とソフトウェアアップデートモジュールを検証し提供すること
⑤ 各種問い合わせの対応は平日 9:30～17:00（祝祭日、年末年始、指定休日を除く）で対応すること

(イ)不正検知・遮断時対応

① 通信遮断等が行われた際に、検知された通信の調査の問い合わせの対応に応じること。調査結果は日本語レポートで報告すること
② 問い合わせの対応は平日 9:30～17:00（祝祭日、年末年始、指定休日を除く）で対応すること

8. 納品物

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)各種マニュアル

以　上