羽曳野市立小中義務教育学校セキュリティ対策強化業務

仕様書

羽曳野市

令和５年４月

１．調達の概要

１－１　背景

平成２９年度に文部科学省が「教育情報セキュリティポリシーに関するガイドライン」を策定し、校務ネットワーク（個人情報を取り扱う領域）のセキュリティ強化の必要性が示された。

平成元年度よりインターネット接続セキュリティ強化を実現するべく、不正な通信を検知・遮断するためのセキュリティ対策に必要な機器を導入し、人的なログ監視/分析サービスの提供を受けることで、本市の教育ネットワークのセキュリティ強化を実施し、令和２年度には、GIGA スクール校内通信ネットワーク整備により、学習系ネットワークと校務系ネットワークのインターネット接続経路の変更を実施し、令和３年度には、総合型校務支援システムを導入し運用を実施している。

現状の校務系ネットワークにおいては、不正な通信を検知・遮断するためのセキュリティ対策により、適宜不正通信を遮断し大きな被害には至っていないものの、学校ではウイルス感染等の事案が度々発生しており、発生した際には原因の確認と対策に非常に負荷が発生している状況となっている。

そのような中、令和４年３月に文部科学省が改訂した「教育情報セキュリティポリシーに関するガイドライン」では、マルウェアに感染し攻撃を検知した場合には、その根本原因や感染した端末の特定と隔離、影響範囲の関係や時系列での不正なふるまいの状況を一元的に把握することができる EDR（Endpoint Detection and Response）の有効性が示されている。

１－２　目的

本業務は、現状のシグネチャー型のマルウェア対策ソフトでは検知できなかった、マルウェア特有の動作を手がかりに検知し早期対応を実現できる技術に変更するとともに、校務系ネットワーク内の端末等がマルウェアに感染し攻撃を検知した場合において、その根本原因や感染した端末の特定と隔離、影響範囲の関係や時系列での不正なふるまいの状況を一元的に把握できる EDR（Endpoint Detection and Response）を導入し、人的なログ監視/分析サービスとして SOC（Security Operation Center）提供を受けることで、本市の教育ネットワークの更なるセキュリティ強化を行うものである。

１－３　調達内容

クラウド環境整備等の構築作業及び本市職員が実施するエージェント展開支援作業、以下の１－６記載の利用期間中のクラウドサービスを提供すること。

（１）未知のマルウェアを AI・機械学習エンジンで検知し事前に防御する機能
（２）EDR（Endpoint Detection and Response）
（３）SOC（Security Operation Center）

１－４　調達範囲

（１）本調達は後述の教育ネットワークにおいて、セキュリティ対策の強化実現に必要なクラウドサービスの提供を行うこととし、クラウドサービスを利用する上で必要となる場合は、教育ネットワークとの接続に必要な機器及び回線サービス等も含めて準備をするものとする。提案内容に応じて既存機器及び回線サービス等を活用することも可能とする。
（２）SOC サービスの提供に係る設定費用や、提案内容に応じて監視サービスを行うための VPN 装置や回線サービスが必要な場合は含めて準備するものとする。
（３）機能実現のために既存ネットワークや既存機器の設定変更を行う場合は、既存ネットワークベ

ンダーによる変更作業を行い、当該変更作業内容についても調達の範囲に含めるものとする。そのための作業費用についても、提案に含めるものする。

（4）その他、教育ネットワークとの接続に必要な機器及び回線サービス等も含めて準備をする場合は、既存機器との接続に必要なLAN ケーブル等や、機器の設置・固定に必要な器具・金具等も全て調達に含めるものとする。

（5）本仕様書は、機能等を実現する上で有するべき要件を提示したものであり、要件を実現する上での規模・性能等の最低限のレベルを示すために例を示したものである。機能を実現するために仕様書に記載されていない事項が必要な場合はこれを含むこと。

１－５　納入場所

羽曳野市 指定場所

※ 提案に応じて、発注者と協議すること。

１－６　期間

構築期間：契約締結日～令和５年８月 31 日

利用期間：令和５年９月１日から令和 10 年８月 31 日

※ 社会的な状況等により、期間中に業務が完了しない場合は、別途発注者と協議すること。

２．構成

２－１　現状の教育ネットワークの構成

別紙のとおり

２－２　監視対象について

校務系ネットワーク配下のサーバ 10 台、端末 790 台　合計 800 台

※上記の台数は変更する場合があります。

３．各種要件

３－１　共通要件

（1）提案内容は、本市のセキュリティ運用負担を軽減するものであること。

（2）サービス提供元による保守支援等のサポート体制が整っていること。

（3）既存のネットワーク通信に遅延等の影響がでないこと。

（4）管理サーバはクラウド型の導入とする。

３－２　機能要件

以下の（1）～（3）に要求する必須機能要件は、（様式第３号）必須機能要件確認票の通りとする。

（1）未知のマルウェアを AI・機械学習エンジンで検知し事前に防御する機能

（2）EDR (Endpoint Detection and Response)

（3）SOC (Security Operation Center)

３－３　導入作業

（1）クラウド環境整備に必要となる要件を本市職員よりヒアリングし、クラウド環境を整備すること。

（2）エージェント展開作業は本市職員により実施するため、手順書を提供し、手順をレクチャーすること。なお、Active Directory サーバの機能もしくは、SKYSEA Client View の機能を用いてエージェント展開を実施することを想定している。上記機能で展開できない場合は、展開に必要な作業・支援に必要な費用も含めること。

（3）エージェント展開が正常に実施できているかを確認するために、クラウドサービスの管理画面にて確認するとともに、確認手順を本市職員にレクチャーすること。

（4）円滑な運用が開始できるよう、本市職員と協議の上、テスト仕様書を作成し、市の指定するテスト用端末にエージェントを展開し、動作確認テストを実施するものとする。エージェントを導入した端末の各種業務確認、既存ウイルス対策ソフトのアンインストール、及びエージェント展開は本市職員が実施することから、必要な支援を実施すること。また、テスト結果及びテスト時に不具合などが発生した場合は詳細を記録し、解決策を検討・実施し報告をすること。なお、構築期間から展開作業中に必要となるクラウドサービス利用料についても。本調達に含めること。また、機器端末の入替を予定しているが、既存のウイルス対策ソフトが令和５年８月 31 日でライセンスが終了するため、機器端末の調達（納品）が遅れた場合は、既存のウイルス対策ソフトを継続更新しないよう調整すること。

（5）初期稼働支援

初期化同支援作業として、以下の作業を実施すること。

（ア）過検知・誤検知の整理、また必要に応じてチューニングを行うこと。

（イ）稼働支援期間中の本市職員からの問い合わせに対し回答を行うこと。

（ウ）必要に応じてオンサイトでの調査、切り分け、ログ採取等を行うこと。

（エ）システム管理者向けトレーニング資料の提供及びトレーニングを行うこと。

（6）導入業務問い合せ・障害対応

本市職員からの問い合わせ、調査依頼を受け付け、対応・回答を行うこと。 本市開庁日月曜日～金曜日（法定休日、年末年始は除く。）

※法定休日とは「国民の祝日に関する法律（昭和23年法律第178号）」に定める休日をいい、年末年始とは12月29日、12月30日、12月31日、1月1日、1月2日、1月3日をいう。

（ア）問い合わせ対応は、開庁日の 9:00～17:00 とする。夜間・休日に受信した電子メールへの回答は、原則翌開庁日に対応すること。

（イ）システム全体の運用に係る重大故障が発生した際は、受付対応時間に関わらず可能な限り迅速に対応を行うこと。

３－４　既存機器・既存ネットワーク部分の変更について

既存ネットワーク部分における変更を行う場合（既存機器への機能追加等も含む）の要件は以下のとおりとする。

（1）作業及び費用に関しては、本市担当者を通して、既存ネットワークベンダーと調整を行うこと。

（2）作業については基本的に既存ネットワークベンダーにより行うものとする。ただし受注者によって行う必要がある場合は、既存ネットワークベンダーと調整の上、発注者の許可を得て実施すること。

（3）作業に係る費用については、本調達に係る費用として見なすものとする。既存ネットワークベンダーと調整を行い、作業内容は提案内容として含めること。提案者の見積総額と既存ベンダーの作業費用総額の合計が、予定価格を上回る場合は失格とする。（提案時の見積書は各社別個で作成すること。）

（4）既存ネットワークベンダーが行う作業内容については、提案者と既存ネットワークベンダーが綿密に調整を行い、責任の所在を明確にすること。

（5）必要となる既存ネットワークベンダー作業分の契約については、受注者との契約とは別に、本市と既存ネットワークベンダーが直接契約を行うものとする。

（6）既存ネットワーク部分の保守は引き続き既存ネットワークベンダーが行うものとする。ただし、保守範囲が広くなり、保守費用が増額となる場合は、本調達の保守費用として計上すること。

4．保守・支援・運用・セキュリティ体制について

4－1　要求水準

（1）管理サーバのメンテナンス（バージョンアップ作業等）はライセンス期間中、回数無制限および無償で提供すること。

（2）既知の脅威に分類される誤検知が発生した場合は、誤検知したファイルを製品サポート窓口に送付することにより、エンジンのアップデートの検討が行われる体制を有すること。

（3）メーカは日本に法人格を登記し、社員による製品サポートを実施すること。

（4）監視サービスを行うための VPN 装置等の通信機器等を導入する場合は、当該機器障害が発生した場合は、速やかに復旧の措置をとること。なお、保守対応時間、受付方法、オンサイト対応については以下の体制以上が望ましい。

・保守受付時間 24 時間 365 日
・受付方法 電話もしくはメール
・オンサイト対応 平日 9～17 時

（5）監視サービスを行うための VPN 装置等の通信機器等を導入する場合は、機器や部品等の交換が発生する場合は、受注者の負担により行うこと。

（6）監視サービスを行うための VPN 装置等の通信機器等を導入する場合は、通信機器のファームアップや更新の際に、適用の可否や方法等を検証し、現地作業またはリモートにて提要を行うこと。また適用後の機能等について支援を行うこと。

（7）導入する機器及びソフトウェアは、契約期間中メーカーサポートを必ず受けられる状態にすること。

（8）監視サービスを行うベンダーのセキュリティについては、以下の認証を２つ以上取得したセキュリティ体制であり、本市のログや機密情報などが適切に管理されていること。

・SOC2 TypeⅡ
・Fed RAMP
・ISO/IEC 27017
・ISMAP

（9）ログ・分析データ等は、データセンターに保管すること。データセンターについては以下のファシリティ基準を満たしているサービスレベルであること。

（ア）国内であれば JDCC ファシリティスタンダードのティア３相当以上であること。

（イ）国外であれば Uptime Institute の Tier3 相当以上であること。

（ウ）ISO-9001 及び ISO22301 を取得したデータセンターであること。

(10) 監視を行うセンターにおいて、CISSP 及び情報処理安全確保支援士の上級セキュリティ資格者が複数名在籍すること。

４－２　サービス指標

次の表に示す以上のサービス指標を達成できること。

表　サービス指標

項目	指標
SOCサービス（インシデント対応）	
検知、通知、対策（隔離）	24時間365日
分析	24時間 コンソールのUIは日本語とし、影響範囲の封じ込めを主眼に一次対処方法を決定し、実行すること。
検知時の本市への対応	検知時の本市への対応は30分以内に実施すること。 24時間365日の対応を行い、緊急のインシデントは電話での対応、それ以外はメールにて対応を行うこと。契約期間内の対応件数は無制限とする。
停止/隔離オペレーション	24時間365日を基本とし、対象機材の隔離を行う。
完了率	100％（上記サービスレベルでの対応完了）
SOCサービス（問い合わせ窓口）	
本市からの電話受付	月曜日から金曜日9:00～17:00 （法定休日、年末年始を除く）
本市からのメール受付	24時間365日
問題回答率	100％
ＥＤＲの可用性	
サービス対応期間	24時間365日
サービス可用性	稼動率99.9％以上※システムメンテナンスを含まず

５．納入成果物

５－１　成果物

成果物について本市に電子・紙で納品すること。

（1）クラウド環境設定シート

（2）各種手順書・マニュアル

（3）その他（議事録・Ｑ＆Ａ表等）

（4）上記ドキュメントを保存した CD 又は DVD

6． 費用

6－1　イニシャル費用

イニシャル費用の内訳

（1）機器購入費用、回線敷設費用（提案により必要な場合）

（2）クラウドサービス初期費用、監視サービス初期費用

（3）導入支援作業費用

（4）クラウドサービス及び監視サービス利用料（初年度）

（5）既存ベンダーによる機器・ネットワークの変更作業費用

（6）その他

6－2　ランニング費用

ランニング費用の内訳

（1）機器保守費用、回線利用料（提案により必要な場合）

（2）クラウドサービス及び監視サービス利用料

（3）既存ベンダーによる機器・ネットワーク部分の保守費用(増額分)

（4）その他

7． スケジュール

7－1　想定スケジュール

構築完了を令和５年８月 31 日とした場合に、想定しているスケジュールは以下のとおりとする。なお具体的なスケジュールについては、発注者と受注者が協議して決めるものとする。

（1）令和５年４月　　公募

（2）令和５年５・６月　　業者選定・契約

（3）令和５年７月　　機器導入回線敷設／クラウド環境初期構築

（4）令和５年８月　　エージェント展開テスト／展開、初期稼働支援

（5）令和５年９月～　　本稼働

※端末の納品が間に合わなかった場合は、別途協議とする。

8． その他条件

8－1　その他

（1）仕様書に明記されてない事項については、発注者と協議の上決定すること。

（2）IP アドレスの体系は既存の構成を維持すること。ただし、クラウドサービスを用いる場合等、接続方法及び通信回線の変更等に伴う IP アドレスの変更が発生する場合については、発注者と協議の上、実施すること。

（3）稼動後、導入した機器・サービス及び設定変更等が原因となり、大幅なネットワークの通信遅延や障害等が発生した場合、調査・復旧を行うこと。

（4）契約期間満了後に設置機器等の引き上げが発生する場合には、受注者の負担により行うこと。

（5）履行にあたっては本市の情報セキュリティポリシー等を遵守すること。
（6）履行にあたっては発注者と受注者で十分に協議した上で実施すること。また、その協議した内容を記録し、書面により発注者に提出し、承認を得ること。
（7）受託者は、本委託業務に関して直接・間接に知り得た一切の内容を受託作業期間のみならず、その終了後も第三者に漏らさないこと。
（8）本仕様書に記載のない事項であっても、本業務の目的に照らして必要であることが明白なものについては、受託者の責任において実施すること。

以上