教育行政用コンピュータウイルス対策システム
賃貸借契約に係る仕様書

1 調達概要

(1)調達物品及び数量

コンピュータウイルス対策システム　1式
システム管理サーバ機器　1式
セキュリティソフト　4,268 ライセンス(4年保守)

(2)賃貸借期間

令和8年2月1日～令和12年1月31日まで(48か月)
※ただし、契約日から令和8年1月31日までの期間については設置・設定作業期間とし、賃借料は発生しないものとする。

(3)納入場所

大分県庁舎新館サーバ室

2 機能・性能等に関する仕様

以下に示す機能及び性能等に関する仕様を満たしているものであること。

①コンピュータウイルス対策システム

No.	カテゴリ	内容
1	メーカー	選定する製品のメーカー、サイバーセキュリティビジネスにおいて少なくとも 20 年以上の実績があること
2	メーカー	日本国内にサポート拠点を持ち、日本語による Web サイト、チャット、または電話でサポートが受けられること。
3	メーカー	都道府県や主要な自治体に対し導入実績があること。
4	メーカー	LGWAN-ASP に定義ファイルの配信サーバーをメーカーが設置し、導入対象となるすべての製品において、無料で定義ファイル更新サービスを提供していること。(自治体情報セキュリティ向上プラットフォームを利用した更新は不可とする)
5	管理	管理サーバーはオンプレミス・クラウドの二通りから自由に選択でき、どちらの利用においても価格に変更はないこと。
6	管理	OS とアプリケーションに存在する脆弱性の情報を、管理サーバー上にアップロードし一覧化する機能を有し緊急度がレポート上に表示されること

7	管理	クライアントが社内ネットワークと社外ネットワークにいる状況でそれぞれ異なるポリシーを自動的に適用できる機能を有していること
8	管理	Windows クライアント OS と Windows サーバーOS のハードウェア情報を一覧でレポート出来ること。
9	管理	Windows クライアント OS と Windows サーバーOS 上にある、OS とアプリケーションの脆弱性を一覧でレポート出来ること。
10	管理	Windows クライアント OS と Windows サーバーOS 上にある実行ファイルを一覧でレポート出来ること。
11	管理	管理サーバが ActiveDirectory と連携可能であること
12	管理	クライアントコンピュータを管理サーバ上で設定したルールに基づき自動的にグループに割り当てる機能を有すること
13	管理	クライアントの IP サブネット毎に管理サーバへの接続トラフィックを制限することが出来ること
14	管理	クライアントのステータス、ウイルスの検知状況、発生イベント、定義データベースの更新状況、ライセンスの使用状況について管理者に定期的にメール送信する機能を有していること
15	管理	クライアント上で隔離、削除されたオブジェクトを管理サーバ側で把握、オブジェクト自体の取得が可能であること
16	管理	同一の管理サーバで、Windows/Linux/Mac/モバイル OS 向けのアプリケーションが管理できること
17	管理	アンチウイルス部分と通信部分（ネットワークエージェント）が独立してインストール出来ること。
18	管理	定義ファイルのロールバックが出来ること。
19	管理	定義データベースや修正プログラム、パッチ等の配信に関して、管理サーバーとクライアントの間にこれらの配布ポイントを自動または手動で設置できること。
20	管理	管理サーバーからサードパーティ製アプリケーションのリモートインストール、リモート削除ができること
21	管理	管理サーバーからクライアントに対し、リモートデスクトップ接続、Windows デスクトップ共有の双方でリモート接続ができること。
22	EPP	定義による検出のみでなく、ヒューリスティック技術を有し、振る舞い検知も有すること。
23	EPP	機械学習テクノロジーを有すること
24	EPP	ファイルアンチウイルス、WEB アンチウイルス、アンチフィッシングのそれぞれにヒューリスティック検知があり、それぞれ独立してヒューリスティックレベルを設定出来ること。

25	EPP	悪意のあるファイル操作を監視、記録し、その攻撃をブロックした際、記録された情報を元に自動的に修復（ロールバック）できること。
26	EPP	ランサムウェアなどに感染しブロックされる前に暗号化されたファイルをロールバックする機能を持つこと。
27	EPP	共有フォルダに対して、外部からの悪意のあるファイル操作を監視・ブロックできること。（監視動作：削除、内容変更、サイズ変更、移動）
28	EPP	脆弱性攻撃に対しブロック機能を有すること。
29	EPP	WEB アンチウイルスがブラウザーに依存しないこと。
30	EPP	意図したスケジュールでクライアントのスキャンを実施できること。
31	EPP	ファイルのチェックサム・更新タイムスタンプ及び NTFS 識別子により差分スキャンができること
32	EPP	アプリケーションの起動制限を設定できること
33	EPP	アプリケーションがシステムにダメージを与える可能性のある行為を防御し、オペレーティングシステムリソースにアクセスすることを制御する機能を持つこと。
34	EPP	接続するデバイスの制御ができ、接続するデバイスの種類において、リムーバブルドライブと MTP 接続を制御できること
35	EPP	リムーバブルドライブ接続時に自動でスキャン出来る機能を有し、オン・オフが設定可能であり、リムーバブルドライブスキャンのドライブサイズ上限値が設定出来ること。
36	EPP	Web コンテンツフィルタリング機能を有し、Web 経由でダウンロードまたは、表示させるコンテンツをファイル形式、拡張子で制限することが出来ること
37	EPP	メールに添付された添付ファイルの名前または拡張子を変更する機能を有していること
38	EPP	F/W、IPS 機能を有していること
39	EPP	あらかじめ定義されたルールに対し、使用方法を学習し定常状態を記録。定常状態から逸脱した場合に対象行動をブロックする機能を持つこと。
40	EPP	Antimalware Scan Interface（AMSI）と連携し難読化されたスクリプトの検知が可能なこと。
41	EPP	Windows OS の端末においてクラウドサービス（アプリケーションおよび Web）の使用を監視し、不要と判断されるクラウドサービスへのアクセスをブロックできること
42	脆弱性管理	OS とアプリケーションに存在する脆弱性の修正とアップデートを、管理サーバーからの指示により実行できること。

43	脆弱性管理	脆弱性の緊急度ごとに配信有無を決められること。
44	脆弱性管理	Microsoft 社の Windows10 及び 11 における FU の管理と配信が可能であること。
45	脆弱性管理	80 社 150 種類以上のサードパーティ製アプリケーションのパッチ配信が可能なこと。
46	EDR	エンドポイントで検出されたサイバー攻撃の脅威に関し、インシデントカードの作成（脅威の可視化）が行えること。
47	EDR	インシデントカードには、検出された脅威に関する少なくとも以下の情報が含まれていること。 - 脅威の発展連鎖グラフ（キルチェーン） - 脅威が検出されたデバイスに関する情報（名前、IP アドレス、MAC アドレス、ユーザーリスト、オペレーティン グシステム）。 - 検知に関する一般的な情報。 - 検知に関連するレジストリの変更有無および該当箇所 - デバイス上のファイル存在の履歴。 - アプリケーションが実行した動作内容 - プロセスの発生箇所 - ネットワーク接続先の情報 -- オブジェクトのダウンロードの有無 - 作成されたオブジェクトの有無
48	EDR	脅威の検出時に管理サーバーとの通信を維持しながら他のネットワークへの接続を論理的に遮断する機能を持つこと。
49	EDR	サイバー攻撃の痕跡となる IoC（Indicator of Compromise）を元に、ネットワークに存在する端末に対し管理サーバーから IoC スキャンおよび論理的ネットワーク隔離が行えること。
50	EDR	ネットワークから隔離された端末に対し、IoC スキャン、オンデマンドスキャンの実行、プログラム/プロセス/コマンドの実行が管理サーバーから実行できること。
51	EDR	ネットワークから隔離された端末は、管理サーバーからリモートでオンラインに戻せること。
52	EDR	オブジェクトのハッシュ情報をもとに実行ファイルの起動をブロックすることができること。
53	EDR	Windows / MacOS / Linux で EDR 機能が利用できること

② 管理サーバ（例示品：DELL PowerEdge R650）

・スペック CPU：12 コア、メモリ：32GB、ストレージ：600GB 以上

③ セキュリティソフト(例示品:Kaspersky Next EDR Optimum 2500-4999 User 4 年 ベース)

・EPP 及び EDR の機能を有すること。

・オンサイト保守を付帯すること

・大分県教育庁の教育行政用ネットワークにて稼働すること

・以下の OS で保護機能が利用できること。

Windows10、Windows11、WindowsSever2012、WindowsSever 2016、WindowsSever 2019、WindowsSever 2022、WindowsSever2025

３ 作業概要

（１）事前打合せ

上記２②、③の機器の搬入に先立って、教育ＤＸ推進課及び教育委員会ヘルプデスクと機器の設定方法、導入スケジュール等の事前打合せを行うこと。

（２）機器の搬入

上記２②の機器を大分県庁新館９Ｆのサーバ室に納入を行うこと。

（３）設置・設定

・サーバ機器については、大分県庁新館９Ｆサーバ室の教育庁ラック内の指定位置に設置すること。 ※システムラック：河村電器産業㈱製 ROF41-1019W

・サーバ設置に必要なケーブル類及び配線作業に関わる経費は、本調達費用に含めること。

・サーバ機器設定については、教育ＤＸ推進課および教育委員会ヘルプデスクの指示に従い作業を行うこと。

・設置・設定の時間については、平日日中作業（8:30～17:15）を基本とするが、これ以外の時間帯で作業が必要な場合は、別途協議の上で決定すること。

・環境構築後は正常に動作することを確認し大分県へ報告すること。

（４）ＯＳ・ソフトのインストール及び環境構築

・構築する際は、既存のサーバへ影響を与えないよう十分に配慮し、構築すること。なお、導入については既存システムの停止がないように構築すること。

・OSをインストールすること。

※インストールから4年間、アップデートプログラムやセキュリティパッチの提供等が可能であること。

・納入時に最新のOSアップデートプラグラムを適用していること。

・既存のウィルス対策ソフトにて設定しているポリシー等を引き継ぐこと。

・必要に応じて既存の EPP 製品をクライアント端末から削除すること。

（５）その他

・メーカーが販売している純正品かつ新品を納入すること。

・開梱後に梱包材一式を回収すること。

・機器の設置後に大分県教育委員会から障害発生の連絡を受けた場合は、原因を調査し、機器の修理等対策を行い報告すること。障害対応に係る費用は本調達に含めること。

4 保守

(1)保守対象

本調達に係る「システム管理サーバ機器」、「セキュリティソフト」

(2)保守内容

①障害箇所の特定及び原因除去のための適切な対処(システム及びソフトウェアのリカバリを含む)

②障害回復後の正常動作確認(OS、ソフトウェアを含む)

③障害対応状況・結果報告

④各部調整

⑤ユーザ取扱いに起因する障害の場合、予防のためのユーザ指導／助言

⑥バージョンアップ、修正モジュール、パッチの適応、OS等のチューニング等の実施

(3)保守要件

①障害が発生した場合は、オンサイトにより対応を行うこと。

②オンサイト保守の受付を行う時間は、平日(土曜日、日曜日及び国民の祝日に関する法律(昭和23年法律第178号)に規定する休日及び12月29日から翌年1月3日までの日を除く)の9:00～17:00とする。ただし、障害の内容に応じ県が必要と判断した場合は、上記以外でも対応を行うこと。

③保守作業は、原則、大分県の職員(教育委員会ヘルプデスクを含む)が保守担当業者に対して保守作業の連絡を行った日に、概ね4時間以内に機器等設置場所を訪問し対応を行う。

④オンサイト保守の対応に伴い発生する交通費、輸送費等は全て本契約に含むものとする。

⑤契約時に障害対応体制証明書(別紙)及び保守作業の責任分担、業務フローを作成し提出すること。

(4)保守作業完了報告

保守作業を完了したときは、保守作業完了報告書を提出すること。(様式の指定なし)

5 データ消去

回収したシステムログ等は、大分県の指示に従い保管後、NIST SP800-88rev.1 のフラッシュメモリベースのストレージデバイスの除去にあたる方法により内蔵記憶装置のデータ読み出しが出来ないように処理を行うこと。

データ消去または破壊作業完了後、データ消去作業完了報告書(任意様式)を大分県に提出すること。作業完了および報告書提出の期限は契約の終了後または解除後、90 日以内とする。

6 その他

（1）運用支援

①システム管理者向け運用支援講習を実施すること。

②保守の責任分界点

調達物件の稼働・保守については、物品の製造者の如何に関わらず、納入業者が最終責任を負うこととし、これを製造業者との間の契約等によって担保していること。

③不具合・バージョンアップ対応

納品物の OS、ファームウェアを含むソフトウェアの不具合が判明した場合は、大分県に遅滞なく情報提供を行うこと。大分県と協議の上、バージョンアップ対応を行うこととなった場合は、速やかに必要なファイル（修正プログラム、ファームウェア等）及び作業手順書を提供すること。

（2）提出物

①管理者マニュアル（機器操作マニュアル）

②デザインシート、詳細設定シート

③打ち合わせ等資料（議事録、作業報告書、動作確認結果報告等。様式の指定なし）

④保守体制連絡図

※上記資料は CD(DVD)-ROM による電子データで納品すること。

（3）納入に係る経費や保守業務経費など本仕様書で記載する業務に係る経費は全て計上し、賃貸借料に含めること。