県立学校コンピュータウイルス対策ライセンス
一式購入に係る要求仕様書

大分県教育庁教育デジタル改革室

県立学校コンピュータウイルス対策ライセンス一式購入に係る要求仕様書

１　目 的

県立学校の教育行政用パソコンにウイルス対策ソフトを導入することで高いセキュリティを確保し、ウイルス感染等を防止するもの。

２　利用期間及び納入場所

（１）利用期間：令和７年２月１日～令和８年１月 31 日（但し、納入期限は令和７年１月 31 日）

（２）納入場所：大分県教育庁教育デジタル改革室が指示する場所

※本調達は、教育行政用パソコンの更新に伴うものであるため、利用期間前であってもマスタ作成時には、要望に応じてライセンス情報の提供等協力すること。

※納入期限前に納品された場合は、納入日から納入期限までの間は試験利用期間として、この間のライセンス料は発生しないものとする。

３　調達物品及び機能・性能等に関する仕様

（１）調達物品　①ウイルス対策ソフトライセンス（4,082）

②ライセンス等管理用サーバ（仮想マシン）

※本調達に、仮想マシンの構築費及び利用期間の利用料を含む。

（２）機能・性能等に関する仕様

「８．調達物品等」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。

４　保守

（１）保守対象

本調達に係る「ウイルス対策ソフト」、「ライセンス等管理用サーバ」

（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　機密保護

契約書添付の「機密保持及び個人情報保護に関する特記事項」に従うこと。また、本契約の履行中に知り得た情報（業務に関わる事項及び付随する事項）に関して機密保持を行うこと。

７　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、本県に遅滞なく情報提供を行うこと。本県と協議の上、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）疑義のある場合

本仕様書に疑義がある場合は、必要に応じて速やかに本県と協議を行うこと。質問がある場合は、本県の回答または指示に従うこと。なお、契約後の本仕様書の解釈は本県によるものとする。

８　調達物品等

（１）機器等一覧

	機器	数量	備考（保守要件）
①	ウイルス対策ソフト	4,082	オンサイト保守あり
②	仮想マシン	－	・構築場所　豊の国IaaS ・スペック　CPU：８コア、メモリ：32ＧＢ、ストレージ：400ＧＢ　以上

（２）機器（システム）仕様

本調達で使用するコンピュータウイルス対策システムは以下の機能を有することとする。

（ア）Windows8.x、Windows10、Windows11　上でウイルス対策プログラムが動作すること
（イ）Windows Server 2008 R2 SP1、2012、2016、2019、2022　上でウイルス対策プログラム

が動作すること
（ウ）リアルタイムにファイルの入出力を監視し、ウイルス検出や処理ができること
（エ） スパイウェアがインストールされた PC から、スパイウェアを除去する機能を有すること また、それらの関連ファイルを自動的に更新する機能を有すること
（オ）スパイウェア検出の際、検出ログの取得ができること。但し、処理はしないこと
（カ）削除したスパイウェアの復元が可能なこと。また、復元の際、復元されるドライブやフォルダ、レジストリの場所が確認出来ること
（キ）ルートキットの検出・処理が可能なこと
（ク） ウイルス感染してしまったクライアント PC に対して、改ざんされたレジストリや設定ファイルの復旧、及び起動しているウイルスのプロセスを停止する機能を有すること また、それらの関連ファイルを自動的に更新する機能を有すること
（ケ）検出された不正プログラム名のみの情報で、プロセス停止・レジストリキー削除、ファイル削除を行える機能を有すること
（コ）圧縮ファイル内で自動実行される可能性のある、不正プログラムコードと疑われるコードを検出可能であること
（サ）クラウド上にある最新のセキュリティ情報を参照して、ウイルスの検索ができること
（シ）システム動作の監視と制限を行い、不正にシステムが変更されるのを検知できること
（ス）クライアントから発生する全ての HTTP 通信（PUT/GET 両方）を検知し、下記処理が可能であること ・全ての HTTP 通信先のドメインを評価出き、その評価結果は 3 段階以上であること ・評価結果により HTTP 通信をブロック出来ること ・評価から除外されるホワイトリストを設定可能であること ・社内、社外クライアントで評価基準を変更可能であること ・評価結果は各クライアントで一定時間メモリ上でキャッシュされること ・フィッシング等を含めた Web からのセキュリティリスクのブロックが可能であること ・全ての通信ポートにおける HTTP 通信を監視する事が可能であること
（セ）対応する圧縮形式 40 種類以上、エンコード形式 7 種類以上対応する機能を有すること
（ソ） ファイルタイプを正しく識別し、感染の危険があるとされるファイルだけを検索する機能を有すること
（タ）ウイルス検出時ウイルスの種類別に設定された推奨される各種検索処理を利用できること
（チ）管理サーバに対してブラウザで接続する際、HTTPS での接続が可能なこと
（ツ）通常のウィルス発見通知のほか、一定時間内に大量のウィルスが発生した場合において通知するアウトブレークアラート機能を有すること
（テ）ファイル共有の禁止、ポートブロック、特定ファイルのアクセス禁止を管理コンソールからクライアントに設定できる機能を有すること
（ト）クライアントの管理サーバ間の移動が Web 管理コンソールからサポートされること
（ナ） USB メモリなどの外部ストレージデバイス、ネットワークリソースに対するアクセス制御ができること
（ニ）不正な暗号化や変更から文書を保護するなどのランサムウェア対策機能を有していること
（ヌ）パターンファイル(シグネチャベース)に加えて、機械学習(AI 技術)型の検索機能により、マルウェア実行前(ファイル検出) および実行後(挙動監視)の検出が可能なこと
（ネ）インターネットに接続できないオフライン環境において、AI 技術(機械学習)を用いたファイル検索を行うことができること