マルウェア対策システム　一式

Anti-Malware Systems
1 set

仕　様　書

令和４年６月

独立行政法人　国立高等専門学校機構

内容

Ⅰ. 仕様概要説明

1. 調達の背景及び目的

独立行政法人国立高等専門学校機構（以下「機構」という）において、情報セキュリティ対策の一つとして、端末およびサーバ等のマルウェア対策システムを調達するものである。

2. 契約期間・納期

契約期間：令和４年１２月１日～令和９年１１月３０日［６０ヵ月間］

納　　期：令和４年１１月３０日

3. 調達物品名及び構成内訳

3.1 概要

機構の各高等専門学校および機構本部（以下「各高専等」という）の端末およびサーバ等に使用可能なマルウェア対策ソフトウェアとその管理サーバから構成されるマルウェア対策システムを調達するものである。

マルウェア対策ソフトウェアは、各高専等で稼働する端末やサーバ等だけでなく、各高専等がクラウド上で稼働させる端末やサーバ等も保護する。なお、クライアント OS の動作するホストを「端末」、サーバ OS の動作するホストを「サーバ」という。

また、管理サーバはマルウェア対策ソフトウェアの動作状況等を把握し、検知状況の管理や定義ファイルの配布・管理を行う。

3.2 本システム基盤調達の範囲

マルウェア対策システムについて以下を提供すること。

① 管理サーバ
② 管理マニュアル
③ マルウェア対策ソフトウェア
④ ユーザ用インストールマニュアル
⑤ 上記項目提供のための設計、構築、設定
⑥ 完成図書
⑦ 設計、構築、設定、調整、保守を含む
（詳細については、「Ⅱ．調達物品に備えるべき技術的要件」に示す）

4. 技術的要件の概要

① 本調達物品に係る性能、機能及び技術等（以下、「性能等」という。）の要求要件（以下、「技術的要件」という。）は、「Ⅱ　調達物品に備えるべき技術的要件」に

示すとおりである。

② 技術的要件はすべて必須の要求要件である。

③ 必須の要求要件は機構が必要とする最低要件を示しており、入札物品の性能等がこれらを満たしていないとの判定がなされた場合には不合格となり、落札決定の対象から除外する。

④ 入札物品の性能等が技術的要件を満たしているか否かの判定は、技術審査委員会において、入札物品にかかる技術仕様書その他の入札説明書で求める提案資料の内容を審査して行う。

Ⅱ. 調達物品に備えるべき技術的要件

1. 性能、機能に関する要件

1.1 管理サーバ　一式

各高専等で使用されるマルウェア対策ソフトウェアの動作状況等を把握し、検知状況の管理や定義ファイルの配布・管理を行う。

管理サーバを実装するハードウェア基盤は基本的に機構で用意したものを使用するものとするが、それ以外のクラウドサービス等の使用を希望する場合は、本調達に含め、応札すること。

1） 管理サーバ構成

① 各高専等で独立した管理が出来るようアクセス権の設定が出来ること。独立した管理は、グループや管理サーバ単位と言った製品の管理体系に沿って実装し、他の管理下にある情報は閲覧出来ないものとすること。

② 国立高等専門学校機構本部（以下「本部」という）では、各高専等の製品動作状態・脅威の検知状況などのレポートが作成可能で、イベントログの参照が出来ること。また、ログは１年以上保持できること。

③ レポートは定時レポートの作成が出来て、指定したメールアドレスに PDF など参照しやすいフォーマットで送信が出来ること。

④ 管理サーバの構築に必要な OS、ミドルウェア等は受注者側にて用意し、費用は本調達に含めること。また、契約期間中にバージョンアップ等が必要となった場合は受注者の負担で行うこと。

2） 管理サーバ機能要件

① 管理配下となる端末の情報(コンピューター名、MAC アドレス、IP アドレス、OS、製品名、製品バージョン、マルウェア定義データベースバージョン)やサーバの情報(製品バージョン、マルウェア定義データベースバージョン)を表示できること。

② マルウェア検出ログ表示機能を有すること。
③ ポリシーの設定及び管理は、操作しやすい GUI 画面を有すること。
④ 定義ファイルによってスキャンする機能を有する場合、マルウェア定義ファイルのロールバックが出来ること。
⑤ WindowsOS のホストに対するリモートインストール機能を有すること。
⑥ マルウェア検知時のアラートメールを送信出来ること。各高専等の管理者は、管理対象端末での検知のみを受信することが可能なこと。
⑦ アクセスログ、認証ログ、システムログ、システムへのログイン履歴及び操作ログについて 1 年以上保持すること。また、機構担当者から依頼があった場合に、これを提供すること。

3) 定義配信設計

定義ファイルによってスキャンを行う場合、以下の仕様を満たすこと。

① 通常時は、定義配信は管理サーバから行い、各端末が直接インターネット接続を行わないこと。なお、管理サーバの他に別途、定義配信用サーバを利用することで同様の機能を提供できる場合も可とする。その場合、定義配信機能を管理サーバに含むこと。
② 障害時には、設定変更により、各端末が直接インターネットから定義取得することも可能であること。
③ 外出時に、各端末が直接インターネットから定義取得するように自動切り替えが出来ること。
④ 定義配信の取得先を手動で指定できること。
⑤ 各高専等に定義配信サーバを置くことが必須の場合は、購入・構築・運用に必要な費用を全て含むこと。

1.2 マルウェア対策ソフトウェア

① 各高専等で稼働する端末やサーバ等だけでなく、各高専等がクラウド上で稼働させる端末やサーバ等も保護する。保護の対象に、Windows・Mac・Linux・Android を OS とする端末やサーバ等を含むものとする。なお、Linux については、以下のディストリビューションを対象に含んでいれば、仕様を満たすものとする。

- Red Hat Enterprise Linux 7
- Red Hat Enterprise Linux 8
- SUSE Linux Enterprise 12
- SUSE Linux Enterprise 15
- CentOS 7

② インストール対象台数は、機構の管理する端末及びサーバ 56,000 台とする。

1) セキュリティ機能要件

マルウェア対策ソフトウェアは、以下の機能を有すること。

① リアルタイムスキャン
② オンデマンドスキャン
③ 感染ファイルの自動駆除。ただし、Android については、検知の通知のみでも可とする。
④ 定期的なスキャン
⑤ ヒューリスティック検知機能
⑥ 端末における振舞検知機能
⑦ 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もしくは、リムーバブルドライブからＰＣへのファイルのコピー時や、リムーバブルドライブからのファイル実行時にスキャンを行う機能。本機能については、オン・オフが設定可能であること。ただし、Android については、本機能が非対応でも可とする。

2) その他の要件

マルウェア対策ソフトウェアは、1)に加えて、以下の機能を有すること。

① インターネット接続を行わなくてもソフトウェアの更新が可能であること。
② オフライン状態でも、1)に示すスキャンが行える機能。
③ ソフトウェアをインストールした端末を、各高専等の敷地外に設置した場合に、インターネットを通じて定義ファイルの更新を行う機能。

2. 性能、機能以外に関する要件

2.1 受注条件

一般財団法人日本情報経済社会推進協会からプライバシーマーク制度によるプライバシーマーク使用許諾、又は、一般財団法人日本情報経済社会推進協会又は海外の認定機関により認定された審査登録機関による ISMS（ISO/IEC27001）の認証を受けていること。

2.2 設置条件等

① 作業日程は、当機構担当者と協議の上決定すること。
② 設計、構築、設定に要する全ての費用は本調達に含むこと。
③ 設置や導入構築等の際は作業日程と体制を前もって掲示し、受注者及び当機構の作業を明確にし、当機構担当者の承諾を得ること。また、作業の実施時間帯は、原則「平日（国民の祝日に関する法律第３条に規定する休日を除く月曜日～金曜日）の９時～１７時」とするが、状況によっては土日祝・夜間となることも想定されることから、具体的な作業日時については、当機構担当者と協議の上決定すること。

2.3 導入構築

1) システム共通事項

① 導入構築にあたり、作業日程と体制に基づき、当機構との調整を密にしながら、各種管理（進捗、課題、品質、セキュリティ、障害）を実施すること。

② 管理サーバによる端末およびサーバの管理は各高専等で行うが、その作業に必要なマニュアルを作成し提出すること。

③ マルウェア対策ソフトウェアのインストールマニュアルを作成し提出すること。内容については事前に機構担当者の承諾を得ること。なお、本ソフトウェアの各端末へのインストールについては、前述のマニュアルを使用し、各高専等で行う。

④ 試験設計に基づき検証を行い、動作、品質、セキュリティ等を確認し、当機構担当者の承諾を得ること。

⑤ 導入構築に関して、本仕様書に明示されていない詳細設定については、機構担当者と協議の上決定すること。

2) 設計

① 当機構担当者及び他システム等納入業者・保守業者と連携し綿密な調整を行い、支障なく稼働できるよう各種設計を行うこと。

② 当機構及びシステム等納入業者・保守業者から収集したヒアリングシートを精査し、詳細設計、運用設計、試験設計等を行い、当機構担当者の承諾を得ること。

2.4 保守・運用サポート

① 保守・運用サポートの対象は、本調達物品全てとすること。

② 契約期間中における本調達物品のソフトウェア保守として、管理サーバの OS について、サブスクリプション及びテクニカルサポートサービスを提供すること。

③ 本調達物品に障害が発生した場合、原因の切り分けを行い、本調達物品に起因する障害については復旧作業を行うこと。なお、復旧作業の対応時間については、保守条件や運用サポート条件に従い行うものとする。また、場合によってはハードウェア保守業者との連携を図ること。

④ その他設定変更等の依頼があった場合は対応すること。なお、システム全体にかかる大幅な設定変更については、当機構担当者と協議の上決定すること。

⑤ 当機構担当者からの技術的相談にも応じること。

⑥ 障害発生時の調査及び対応や設定変更作業などは、本調達物品に対してリモートアクセスし行うこと。なお、リモートアクセス方法については、当機構担当者と協議の上決定するが、リモートアクセスに必要な通信回線費用（工事費、回線費、ISP 接続費など）等が発生する場合は、受注者の負担とすること。

⑦ リモートアクセスからの対応が難しい場合は、当機構担当者と日程調整の上、オンサイトで行うこと。なお、オンサイトでの対応時間については、平日（国民の祝日に関する法律第３条に規定する休日及び１２月２９日～１月３日の年末年始を除く月曜日～金曜日）の「９時～１７時」とする。

⑧ 本調達物品について、システムの不具合やセキュリティホール等が発見された際は、3 営業日以内に当機構担当者に情報を提供し、当機構担当者と協議の上、対策を実施すること。
⑨ 当機構担当者からの問い合わせについて、総合受付窓口（メール）を設け一本化し回数無制限で対応すること。なお、受付時間は２４時間３６５日とすること。
⑩ 当機構担当者との定例会議を、導入段階では１か月ごとに１回以上、運用段階では半年ごとに１回以上行うこと。会議開催時はその議事録を作成し、当機構担当者の承認を得ること。なお、定例会議の出席者は、営業担当者及び技術担当者とする。

2.5 提出物及び提出期限

① 障害発生時の保守手順マニュアルを日本語で提供すること。
② 運用手順マニュアルを日本語で提供すること。
③ 独自マニュアルを作成した際、製本された紙媒体及び改変できる電子データで提供すること。
④ 独自マニュアルは必要に応じて改訂し、変更した際はその都度提供すること。
⑤ 受注者が独自作成したマニュアルの著作権及び所有権は、当機構に帰属すること。
⑥ 下記の完成図書（冊子３部）と下記全ての電子データ（CD または DVD 格納）を契約開始日まで納品すること。また、内容については当機構担当者と協議の上で決定すること。

A） 機器の仕様書
B） プロジェクト計画書及び完了報告書
C） 設計書（詳細設計、運用設計等、本調達業務に係るもの等）
D） 設定書（パラメータシート等）
E） テスト報告書（テスト計画書、テスト結果報告書等）
F） 説明書、マニュアル（改訂版も含む）
G） 議事録（定例会、個別打合せ等）

2.6 操作教育

当機構担当者に対して、本調達物品の管理・運用に関する説明・教育を実施すること。なお、説明・教育の内容については、当機構担当者と協議の上決定すること。

2.7 機密保持

① 受注により知り得た全ての情報について守秘義務を負うものとし、これを第三者に漏らし、又は他の目的に使用しないこと。
② 受注により知り得た情報については、契約期間はもとより、契約終了後においても第三者に漏らさないこと。
③ 正当な理由があってやむを得ず第三者に開示する場合、書面によって事前に承諾

を得ること。また、情報の厳重な管理を実施すること。

④ 当機構が提供した資料は、 原則として全て複製禁止とすること。但し、業務上やむを得ず複製する場合であって、事前に書面にて当機構の許可を得た場合はこの限りではない。なお、この場合にあっても使用終了後はその複製を当機構に返納又は焼却・消去する等適切な措置をとり、機密を保持すること。

2.8 検査及び検収

高専機構担当職員の立ち会いのもと行われる、現場での動作確認及び納品成果物の納入をもって検収とする。

2.9 損害賠償

受注者が本契約に違反して、高専機構が損害を被った場合には、高専機構は受注者に対して損害賠償を請求し、かつ、高専機構が適当と考える必要な措置をとることを請求する権利を有するものとする。

2.10 サプライチェーンリスクマネジメントについて

① 受注者は、サプライチェーンリスクの要因となる脆弱性を発生させない又は増大させないための管理体制を構築すること。また、応札時に管理体制図を機構に提示すること。

② 受注者は、機構がサプライチェーンリスクに係る情報セキュリティインシデントを認知した場合又はその疑いが生じた場合に、必要に応じて業務内容、作業プロセス又は成果物を立ち入り検査等で機構が確認することを了承すること。

③ 本業務において使用する機器等については予め機構に機器等リストを提出し、機構がサプライチェーンリスクに係る懸念が払拭されないと判断した場合には、代替品選定やリスク低減対策等、機構と迅速かつ密接に連携し提案の見直しを図ること。

2.11 情報セキュリティを確保するための体制整備について

① 受注者は、情報セキュリティの確保を目的とした体制を整備し応札時に機構に提示すること。報告する体制には、情報セキュリティの確保に関する責任者を含めること。なお、体制が変更になった場合は速やかに機構へ報告を行うこと。
また、情報セキュリティ侵害発生時には、機構の情報セキュリティ監査を受け入れること。

② 受注者は、本業務における情報セキュリティ対策が継続して適切に履行されているかどうか、項 2.4⑩に示す定例会にて機構に報告すること（報告内容は議事録に記録すること）。また、情報セキュリティ対策が不十分だったことが判明した場合、受注者の責において、適切な対策を講ずること。

③ 受注者は、業務完了後、本件に係る情報を返却または抹消し、そのことを機構に

書面で報告すること。

2.12 その他

① 導入する物品については、入札時において製品化されていること。
② 導入する物品については、最新版を納品すること。なお、その最新版の導入にあたっては、当機構と協議の上決定すること。
③ 本調達の履行について疑義が生じたとき、又は、本調達に伴い高専機構と交わす契約書に定めない事項については、当機構及び受注者の双方で協議の上決定すること。
④ 本調達における保守・運用サポート条件以外の対応については、別途適正な価格による有償契約によって対応が可能なこと。
⑤ 追加業務等が発生する場合は、高専機構本部財務課契約係を通して発注するので、受注者はそれ以外の者からの発注や依頼を受け付けないこと。
⑥ 受注者の故意又は過失により損害が発生した場合は、受注者の責により原状復帰すること。
⑦ 本調達物品を導入するに当たっては、国立高専機構の情報セキュリティポリシーに基づき、情報セキュリティに係る事項等の説明を受け遵守すること。
⑧ 本調達を導入事例としてパンフレット発行等の各種メディアへの掲載やプレス発表を行う場合は、必ず当機構と調整の上とり行うこと。
⑨ 受注者は、本業務を自ら履行するものとし、本業務の全部を第三者に委託し、又は請け負わせてはならない。業務の一部を委託する場合は、機構の承認を得ること。

以上