クラウド型 IT 資産管理システム
一式
（Cloud-based IT asset management system）

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

目次

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。）において平成２８年から利用しているクラウド型 IT 資産管理システムの更新にあたり、IT 資産管理システムの調達及び設定等を目的とする。

2. 契約期間

本調達物品について、下記の契約期間とすること。
契約期間：令和４年１２月１日～令和１０年１１月３０日［６年間］

3. 調達物品名及び構成内訳

（調達物品名）
クラウド型 IT 資産管理システム　一式

（構成内訳）
（１）SaaS 環境
（２）IT 資産管理システム　一式
（３）機器への導入・調整・運用支援　一式

4. 技術的要件及びその他の要件の概要

① 本調達物品に係る性能、機能及び技術（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 ①以外の要求要件（以下、「その他の要件」という。）は、「Ⅲ．導入実施と納品の備えるべき要求要件」に示すとおりである。
③ 技術的要件およびその他の要件は全て必須の要求要件である。
④ 必須の技術的要件及びその他の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・仕様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。
⑤ 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、技術審査において、入札物品に係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

5. 性能、機能に関する要件

5.1. クラウド型 IT 資産管理システムの基本要件

(1) SaaS 環境

① 特定非営利活動法人日本データセンター協会のデータファシリティスタンダードに基づくティア 3 相当以上の日本国内にあるデータセンター上に構成されること。
② 用意する SaaS 環境の準拠法は日本の法律であること。また、管轄裁判所を日本国内の裁判所とすること。
③ 物理サーバ故障時においても、5 分以内を目安として、他の物理サーバに切り替わり再起動され利用可能であること。
④ 資産管理データベース及びシステムは、RAID6 相当以上の構成で冗長化されたディスクに格納すること。
⑤ システム構成コンポーネントは全て二重化し、高信頼性を確保すること。
⑥ DDoS 攻撃やウイルス・スパイウェアに対してセキュリティ対策が施されていること。
⑦ データセンター内への入退室管理について、24 時間の監視、ID カード等による不正入室の排除、監視カメラ、ネットワークの監視等を備えること。
⑧ 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情報セキュリティマネジマントシステム（ISMS）の国際規格「ISO/IEC27001」を取得し、かつ、米国公認会計士協会の基準に基づき提供される内部統制の仕組み「SOC2 保証報告書」を受領している、第三者機関の評価としても信頼に足るデータセンターを利用すること。
⑨ クラウド型（SaaS 型）IT 資産管理システム（以下「管理システム」という）は、定期保守等の計画停止を除き、99%以上の稼働率を SLA として保証すること。
⑩ 管理システムは、一般財団法人マルチメディア振興センターの運用する「ASP・SaaS 安全・信頼性に係る情報開示認定制度」の認定、もしくは、特定非営利活動法人 ASP・SaaS・クラウドコンソーシアムの主催する「ASP・SaaS・クラウドアワード」を受けていることとし、第三者機関の評価として信頼に足る SaaS システムであること。
⑪ 管理システム上のデータは、適切なバックアップを行い、万一の際に少なくとも前日の状態に戻せるようにすること。
⑫ SaaS 利用環境の準備や設定等については、契約初年度でのライセンス契約とする。

(2) 管理システム

① 提案する管理システムについては、入札時において製品化されていること。
② 年度ごとの管理対象 PC の入れ替え等を想定し、ライセンス契約は年度ごとの利用料金制にて行うものとする。管理対象 PC が入れ替わった際でも、当該年度の終了時点で契約台数を大幅に超えないことを条件に、この利用料金の中で対応可能であることとし、入れ替え後の新規管理対象 PC に対するライセンスを含むものであること。
③ 年度ごとのライセンス利用料金の中には、全てのシステム保守、システムのバージョンアップの無償権、サポートデスク（問い合わせ窓口）利用料金を含むもの

とする。

(3) 機器への導入・調整・運用支援に関する要件

① 機構が所有する管理対象 PC 全 30,000 台について、インベントリ情報収集及び IT 資産管理台帳を実現するために必要な管理システムを導入する。
② 管理システムは、SaaS 型で導入することとし、管理用のサーバ機器、サーバシステムの導入は、サービスとして利用することとする。また、必要となるデータベースソフトのミドルウェア類を含め、これらに要する費用は、応札業者の負担とし、調達金額に含めるものとする。
③ 各高専や拠点等には、データ中継用サーバ、管理対象 PC 台数に応じた分散サーバ等の一切の設備負担をすることなく、導入が可能であること。
④ 管理対象 PC からの PC 情報の収集及び各種管理台帳及びレポートの利用に際しては、HTTPS 通信で経路暗号化を行うこと。
⑤ HTTPS 通信においては、信頼に足る実績豊富なベンダーの SSL サーバ証明書を必須とし、デジタル署名を付与すること。ただし、アクセス先 URL に機構の指定ドメインを利用可能な場合、SSL サーバ証明書は機構にて用意するものとし、それを受領して設定を行うこと。
⑥ パスワードを設定する必要が有る場合、高専統一パスワードポリシーに準拠するように設定すること。

5.2. 管理対象 PC

① 機構が設置する国立高等専門学校（全 51 校　55 キャンパス）及び機構拠点内に存在する管理対象 PC を対象とする。
② 管理対象 PC として以下の全ての OS に対応していること。

Windows	・Windows11 （Pro、Enterprise、Education、Home） ・Windows10 （Pro、Enterprise、Education、Home） ・Windows8.1 （無印、Pro、Enterprise） ・Windows Server 2012、2012 R2、2016、2019、2022 ※32bit 版と 64bit 版に対応すること
Macintosh	・macOS Monterey 12 ・macOS Big Sur 11 ・macOS Catalina 10.15 ・macOS Mojave 10.14 ・macOS High Sierra 10.13

③ Windows、macOS の新たな OS への対応については、システム保守の一環として契約費用の範囲で提供すること。
④ 各 OS の日本語版と英語版に対応すること。
⑤ 仮想 OS 上で運用されている場合や、異なる OS を多重起動している場合も、各 OS 環境での PC 情報を収集する機能を有すること。
⑥ 管理対象 PC は、ドメイン未参加等多様な形態で利用されているため、本システム以外に、エージェント（「5.3(2) インベントリ情報収集」を参照）を除く特殊なソフトウェアのインストールや、ポート開放を含むネットワークの設定等、事前

に特段の変更をせずに利用可能であること。
⑦ 有線 LAN、無線 LAN 等のネットワーク接続形態並びに NAT 又は NAPT によって接続されている場合においても、PC 情報を収集する機能を有すること。
⑧ 収集した PC 情報を管理システムの管理サーバ（以下「管理サーバ」という）に送信する際には、HTTPS 通信による経路暗号化をすること。また、プロキシ環境を有する場合等についても PC 情報の収集が可能であること。
⑨ 管理対象 PC への管理システムのインストールは、利用者自身で実施できること。

5.3. 管理システムの機能要件

(1) 全般及び基本機能

① 管理システムが作成する各種管理台帳及びレポートは、機構を最上位とし、各高専・学科・研究室・センターといった管理階層ごとに作成すること。これを「管理単位」と称する。また、「事務系」「教育系」や「教員用」「学生用」といった仮想の階層を設けられること。この階層管理により、機構本部管理者及び高専管理者（以下「各管理者」という）に対して管理範囲に応じた権限設定ができること。なお、管理階層の情報は機構から指示された階層を設定すること。
② 管理階層は、最大で 10 階層以上作成可能なこと。また、各階層 1 管理単位の直下に作成可能な管理単位は 20 以上であること。
③ 各管理者が専用の管理機を用意することなく、業務で通常使用している PC を管理用端末として使用できること。また、各種台帳及びレポートは、Web ブラウザ又は管理用ソフトウェアからの閲覧・管理が可能であること。アドオンのインストールを含め、何らかの追加対応を行うことなく利用可能であること。なお、管理用ソフトウェアからの閲覧が可能な場合も可とするが、その場合、管理対象 PC と同様の OS に対応していること。
④ 各種管理台帳及びレポートは、日本語表示と、英語表示を切り替えて利用可能であること。
⑤ 管理対象 PC への本システム展開稼動後も、リソースの消費は最小限に抑えること。利用者が特段の意識をすることなく、通常通り業務が可能であること。

(2) インベントリ情報収集

① 管理対象 PC のインベントリ情報を収集するプログラム（以下「エージェント」という）の展開においては、利用者が管理サーバへ Web ブラウザからアクセスしログインすることで実行できる仕組みであること。
② エージェントは、初回実行時に、管理対象 PC にインストールされ機構管理者が設定するスケジュールで定期的にインベントリ情報収集が自動実行される常駐タイプと、PC にプログラムファイル等を残さない非常駐タイプを用意し、管理対象 PC や各高専、利用組織の特性や要件に応じて選択可能であることと。
③ 常駐タイプのインベントリ情報収集については、定期的な自動実行の他に、管理対象 PC からの利用者による随時起動が可能であること。
④ Web ブラウザは、Microsoft Edge、FireFox、Safari、Google Chrome に対応し、各 OS 環境からのマルチブラウザアクセスに対応すること。
⑤ 定期自動実行によるエージェント起動は、スケジュールされた時刻に集中起動しないよう、実行タイミングをランダムに分散させる負荷分散が図られていること。また、バックグラウンドで行うものとする。
⑥ 定期自動実行によるエージェント起動時にネットワークに接続されていない場合

や、電源が入っていない場合に対し、ネットワーク接続された後、又は電源を入れた後に自動的にエージェント起動を実施する機能を有すること。

⑦ 定期自動実行によるエージェント起動時に管理サーバが保守等により停止していた場合でも、管理対象 PC にエラー通知やメッセージを出さないこと。

⑧ 収集するインベントリ情報は以下の項目を収集すること。

ハードウェア情報 ※「コンピュータ名」や「IP アドレス」は重複が十分予想されるため、PC の識別のキー項目として用いてはならない。これらが重複するような場合でも、固体識別が問題なく可能であること。	・PC 名 ・OS ・OS タイプ ・OS バージョン ・PC メーカ名 ・PC モデル名 ・PC タイプ(デスクトップ、ノート等) ・ハードウェアシリアル番号 ・スペック情報（CPU クロック数、メモリ容量、ハードディスク容量） ・MAC アドレス ・
属性情報 ※これら項目については、導入時に機構が指定する内容で収集可能なよう設定をすること。また利用者の負荷軽減のため、項目に応じて、文字入力以外にプルダウン選択等が可能であること。	・管理単位（高専名・所属の・学科・研究室や部局組織等） ・情報システム名 ・利用用途 ・責任者名 ・使用者名（氏名） ・設置場所（備考） ・資産の種別 ・物品管理番号 ・購入日 ・ネットワーク接続形態 ・ドメイン名（ActiveDirectory 上） ・ワークグループ名 ・プライベート IP アドレス
ソフトウェア情報	・ソフトウェア名称 ・メーカ名 ・エディション ・バージョン ・プロダクト ID
ウイルス対策状況 対象：シマンテック社、トレンドマイクロ社、マカフィー社、ソフォス社、CA 社、ESET 社のコーポレート版ウイルス対策ソフトウェア ※上記以外についてはウイルス対策ソフトウェア名のみを収集することとする	・ウイルス対策ソフトウェア名 ・定義ファイルのバージョンと更新日付 ・リアルタイム保護の状態

⑨ 管理対象 PC の「高専名、専攻科・研究室名」等、機構が指定する管理項目について、入力が可能であり、この内容が各種台帳に反映されること。また負荷軽減のため、入力以外にプルダウン選択等も可能であること。これらはマスターとして導入時にセットアップを行うこと。

⑩ ネットワークに接続されないオフライン PC のインベントリ収集にも対応すること。容易に同レベルの情報を収集し、台帳にて管理可能であること。収集したオ

フライン PC のインベントリ情報は、利用者自身がネットワーク接続 PC から管理サーバにアクセスし、容易な手順でインポート登録が可能であること。

⑪ 教員の PC が高専外に持ち出されて利用されることを想定し、高専及び機構のネットワーク以外の接続環境（自宅や長期の海外出張を含む）においても同様にインベントリ収集可能であること。

⑫ CSV を含むテキスト形式に、ハードウェア情報、ソフトウェア情報を記入したものを入力情報としてインポート登録できる機能を備えること。

⑬ エージェントのアンインストールに際しては、専用のアンインストーラを用意すること。またエージェントを構成するプログラム類はアンインストール後にシステム領域に残存させないこと。

(3) ハードウェア管理台帳

① 収集したインベントリ情報から、管理単位ごとに、「ハードウェア管理台帳」を自動的に作成すること。

② 管理単位ごとに管理 ID を設定し、自 ID の範囲内での管理、及び上位 ID は下位管理単位の管理を可能とするよう、権限設定が可能であること。また機構管理者は全高専分の情報を閲覧管理できること。

③ 「ハードウェア管理台帳」には以下の項目を一覧表示させ、台帳画面には以下の各項目を検索条件として用意し、指定しての絞込み検索が容易に可能であること。

ハードウェア管理台帳	・ 管理単位名 ・ PC の設置場所情報 ・ PC の使用者（又は管理者）名 ・ 利用の用途等の属性情報 ・ コンピュータ名 ・ OS ・ メーカ名 ・ モデル名 ・ IP アドレス ・ MAC アドレス ・ 各種スペック情報 ・ インベントリ情報を取得した日付
検索条件	・ 管理単位 ・ 設置場所 ・ 使用者名 ・ コンピュータ名 ・ OS ・ メーカ名 ・ モデル名 ・ 属性情報

④ 「ハードウェア台帳」に関する各項目について、全件、また検索絞込み条件に沿って、容易に CSV 形式で出力し、2 次利用が可能であること。

⑤ 必要に応じて、「リース管理台帳」、「PC 購入台帳」を作成できること。この際、「ハードウェア管理台帳」の情報を活用することで、作成や管理の負担を軽減する措置が講じられていること。

⑥ 廃棄やリース返却等によりハードウェア管理台帳から削除した PC について、削

除履歴を確認することが可能なこと。

(4) ソフトウェア台帳とソフトウェア資産管理

① 収集したインベントリ情報から、全てのソフトウェアの一覧及びインストール数の集計表である「ソフトウェア台帳」、及び管理対象 PC 別のインストールソフトウェア一覧表となる「PC 別ソフトウェア台帳」を自動的に作成すること。
② これらソフトウェアの台帳類は、管理単位ごとに作成すること。
③ 管理単位ごとに管理 ID を設定し、自 ID の範囲内での管理、及び上位 ID は下位管理単位の管理を可能とするよう権限設定が可能であること。また機構管理者は全部を閲覧管理できること。
④ 台帳画面には各項目を検索条件として用意し、「管理単位」、「ソフトウェア名」、「メーカ名」を指定しての絞込み検索が容易に可能であること。
⑤ 各ソフトウェアは OS プラットフォームを識別し、ソフトウェア台帳類において「Windows 版」、「Mac 版」の判別、絞込み検索が可能であること。
⑥ 管理単位ごとにソフトウェアのインストール数やライセンス数が集計され、照合確認が可能であること。
⑦ ソフトウェアに対し、「管理対象」、「管理対象外」、「未決定」という状態を管理区分として管理できること。同一のソフトウェアでも、管理単位ごとに異なる指定が可能であること。また、Microsoft 社や Adobe 社の主要製品については、ソフトウェア名称内の詳細バージョン等を識別し、ライセンス管理すべき製品名に名寄せして台帳化すること。
⑧ ソフトウェアの主要メーカ名について、管理対象 PC から収集した生データのまま台帳にするのではなく、「Adobe 社」、「Microsoft 社」といった形で、1 回の操作で検索可能となるよう、適正なデータ補正を行うこと。
⑨ Adobe 社の CS シリーズ(Windows 版)や、Microsoft 社の Office シリーズ(Windows 版）等について、製品本体と同梱ソフトウェアの識別が可能であり、ライセンスの二重カウント等を防止できること。
⑩ インストール数に対して所有のライセンス数の照合を行う「管理対象ソフトウェア」について、「ソフトウェア台帳」上で個別に指定が可能であること。
⑪ 機構が独自に設定するソフトウェアのグルーピング情報をマスターとして保持可能であること。機構管理者側での登録・修正・削除が可能であること。ソフトウェア台帳においては、このマスターに「登録済」、「未登録」等の条件を指定して把握することが可能であること。
⑫ ライセンス契約情報を登録し、インストール情報と関連付けての内訳の詳細な管理が可能であること。ライセンスによって許諾される、セカンドライセンスやアップグレード・ダウングレードインストールの管理が可能であること。管理単位を横断しての関連付けも可能であること。また、ソフトウェアのグルーピングマスター情報に基づき、ダウングレードの自動判定が行えること。
⑬ アップグレードやダウングレードの利用に対しては、アップグレードの元となったライセンス情報、アップグレード先のライセンス情報が関連付けて管理され、また利用可能なライセンス数について適正に管理が可能であること。
⑭ ライセンス契約情報には、調達したソフトウェアライセンスについての、以下の情報を登録できること。この時、「ソフトウェア名」については、収集したインストール名称を指定できるようにして利用者の入力負荷を軽減すること。インストールが行われておらず名称情報が無い場合でも、仮登録を行い、後から再指定が可能であること。またライセンス契約情報は、画面からの入力による登録以外に、CSV 形式のファイルを入力としたインポートによる一括取り込み機能も備えるこ

と。

- ソフトウェア名
- 購入日付
- 購入組織（専攻・学科・組織等）
- 購入理由
- 期間ライセンスの場合の開始日と終了日
- ライセンス種別
- 数量
- ライセンス契約形態
- ライセンス証書番号
- インストールキー

⑮ ソフトウェアのグルーピングマスター情報に基づき、以下の項目を機構全体、各高専の管理単位別に集計できること。

- 所有するライセンス数
- 関連付けられ消費された数
- うちライセンス所有組織と消費組織が異なる数
- ダウングレードインストールで消費された数
- セカンドライセンス等にて消費された数
- これらの合計としての消費数合計
- 所有するライセンス数との差異

⑯ 教員が個人で購入したソフトウェアを管理対象 PC にインストールして利用している場合においても、ライセンス契約情報とインストール実態情報とを紐付け管理することで適切に判別して管理が可能であること。

⑰ 棚卸ししたライセンス証書の現物について、管理台帳データとの連動性を確保するため、管理台帳上に証書原本の有無や資料番号・インデックス（紐付け番号）の情報を登録でき、対応付けて管理できること。

⑱ ソフトウェア台帳類に関する各項目について、全件、また検索絞込み条件に沿って、容易に CSV 形式で出力し、2 次利用が可能であること。この時、ハードウェア及びその属性情報も関連付けて加工利用しやすい形に出力できること。

(5) ソフトウェア辞書と各種ソフトウェア資産管理支援機能

① ソフトウェアについて、有償製品、シェアウェア、フリーソフトウェア、ドライバ、アドウェア・マルウェアといった分類の情報を、ソフトウェア辞書として提供すること。ソフトウェア資産管理台帳にて、管理対象ソフトウェアの選定や、ソフトウェアのグルーピングマスターの設定の際に利用できること。

② 分類情報は参考情報とし利用するものとし、機構が独自に判断して分類情報の確定ができるものであること。

③ ソフトウェアの分類情報については、機構が調査して判明した情報を、機構側で独自に追加設定が可能であること。

④ 収集した全ソフトウェア情報について、ソフトウェアの分類情報、管理対象の区分、ソフトウェアのグルーピングマスターへの登録内容を一覧管理する機能を有すること。

⑤ ソフトウェア分類情報を含むソフトウェア辞書の利用に際して、合致しなかった情報の外部機関への提出と言った機構の IT 資産情報を外部に出す義務を負わないこと。

⑥ 各種資産台帳への全ての更新業務（例：ライセンス契約情報の登録、インストール情報との関連付け）について、各管理者 ID 別に、更新日時と更新前内容、更新

後内容を、履歴として記録し、把握管理が可能であること。
⑦ 基準日等を指定しての不要となった履歴を削除する機能を有すること。
⑧ 管理対象 PC の属性情報の各項目について、管理画面から、個別、あるいは複数の管理対象 PC を指定しての一括で、内容を編集更新可能であること。

(6) セキュリティ関連

① Microsoft 社セキュリティパッチについて、セキュリティパッチを指定しての適用の有無、未適用のパッチ情報を識別可能であること。
② Adobe 社製品セキュリティパッチ、Java 関連、各種ブラウザについての、適用されたセキュリティパッチ情報、未適用のセキュリティパッチ情報を、管理対象 PC 別に把握管理できること。
③ ウイルス対策ソフトウェアについては、シマンテック社、トレンドマイクロ社、マカフィー社、ソフォス社、CA 社、ESET 社のコーポレート版の「定義ファイル（パターンファイル）情報」、「稼動状態」の情報を一覧管理できる台帳を作成すること。
④ 管理対象 PC に複数のウイルス対策ソフトウェアが導入されている場合、上記③の情報を判定し、当該 PC が安全な状態にあるか否かを識別できる一覧レポート機能を有すること。
⑤ これらメーカ以外のウイルス対策ソフトウェアを含めて、ウイルス対策ソフトウェアが未インストールのものを識別可能であること。
⑥ 主要なファイル共有ソフトウェア（Winny、Share、BitTorrent、LimeWire、WinMX 等）について、管理対象 PC 上の存在を把握可能であること。

(7) 利用状況の確認機能

① 管理対象 PC の利用状況の確認のため、PC ごとに、日付ごとの最初のログオン、最後のログオフ情報を収集し、閲覧可能とすること。
② 当日から過去 45 日間以上のログが保持され、閲覧可能な状態であること。
③ 管理者が階層ごとの閲覧権限に基づいた範囲で閲覧でき、当該 PC からは当該 PC の履歴を閲覧可能であること。
④ CSV 形式で出力し、2 次利用が可能であること。

Ⅲ. 導入実施と納品に備えるべき要求要件

6. 導入支援作業

6.1. 管理システムの利用準備

① 全管理対象 PC に対して管理システムを利用可能な状態とする準備を行うこと。
② 管理単位の設定及び利用者 ID の発行に際しては、機構と十分な協議を行い、高精度で負担の少ない管理業務を継続的に行っていくための設定方法等について、他の大学や教育機関の事例等を提供し、円滑に進めること。

6.2. 管理対象 PC へのインストール

① 全管理対象 PC への管理システムのインストールについて、管理サーバにログインしてダウンロード実行することで、利用者自身が実施できるように準備すること。
② 管理対象 PC へのインストール時に発生した不具合事象に対しては、メール及び電話にて対応が可能なヘルプデスクを設置すること。ヘルプデスクへの連絡担当者に制限がある場合は機構と協議の上決定すること。
③ 管理対象 PC へのインストールの進捗状況は、リアルタイムで各管理者が把握できること。

7. 提案事業者に求める事項

(1) 過去の導入実績

日本国内の複数の大学や政府機関等における各 5,000 台以上の導入実績を有し、その実績を踏まえ、機構でソフトウェア資産管理を効果的に運用できるよう、適切な助言・支援を行うこと。

(2) 情報セキュリティを確保するための体制の整備

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。また、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適切に履行されていることを、定期的に書面にて機構に提出すること。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。

(3) 事業者の情報セキュリティ水準

① 受注者は、一般社団法人情報マネジメントシステム認定センター、公益財団法人日本適合性認定協会、もしくはその他認定機関により認定された審査登録機関による ISO/IEC27001 又は JIS Q 27001 の認証を受けていること。
② 受注者は、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（JISQ15001）使用許諾の認証を受けていること。

(4) 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、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。

(5) ログの保持

本システムに関するログ（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）を取得すること。取得したログは取得後少なくとも１年間保持し、機構担当者から提供の依頼があった場合に応じること。

8. 性能、機能以外に関する要件

8.1. 保守要件

① 本調達に、契約期間中におけるソフトウェア保守（サポート）費用を含めること。

② 本稼動開始以降の保守・運用支援のため、専門知識を有する要員を確保し、遠隔保守又は現地対応の体制を保持すること。

③ トラブル対応は迅速かつ的確なものであり、導入ベンダーが直接対応できること。

④ メール、電話の対応に加え、重大なトラブル時はオンサイトでの対応が可能であること。

⑤ 保守対応時間は以下のとおりとする。

「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（ただし年末年始 12/29～1/3 を除く）」対応（問い合わせ窓口含む）で応答時間が翌営業日以内

⑥ 保守に係る問い合わせ先を機構へ明示すること。また、その保守開始時にメーカ等へのユーザ登録等の作業が必要な場合は、受注者側で登録作業を行うこと。

⑦ 保守に係る問い合わせ内容、問い合わせ者、対応結果（対応途中の時はその見通し）等については取りまとめて翌月７日までに月次報告書として機構に提出すること。提出方法や様式の詳細については機構から指示を受けること。

⑧ 必要に応じクラウド提供ベンダーと密な連絡を取り業務に当たること。

⑨ 本システムのバージョンアップを保守契約期間内に限り無償で受けられること。

⑩ 本システム内にセキュリティ上の脆弱性等があった場合は、すみやかに機構にその旨連絡し、日程調整の上、対策を講じること。なおシステムの停止が伴わない場合は応札者の判断で対策を最優先とすることができる。

⑪ ソフトウェアの障害対応パッチのうち、安定に動作するために必要なもの及びセキュリティ保持に必要なものは、速やかに導入すること。その他、緊急度の低いパッチの導入については、必要に応じて随時導入すること。

⑫ ソフトウェア辞書情報の最新の情報を保守契約期間内で提供されること。

8.2. 操作教育・研修

① 各管理者向けマニュアルを作成し、各管理者に対し操作研修を行うこと。日程については機構と協議の上行うこと。

② 利用者向けマニュアル及び利用者向けインストール簡易マニュアルを作成し、各利用担当者に対し操作説明会を行うこと。日程については機構と協議の上行うこと。

③ 作成したマニュアルは、編集可能な形式で機構へ提供し、著作権（著作権法第２７条及び第２８条の権利を含む）を譲渡し、また、著作者人格権を行使しないこと。

（ただし、提供マニュアルの内、外部公開しているマニュアル（公式マニュアル）はその限りではない）

8.3. 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してはならない。
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機構の承諾を得ること。また、情報の厳重な管理を実施すること。
④ 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。

8.4. 検査及び検収

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以下の納品成果物の納入をもって検収とする。

① 完成図書
② システムの操作マニュアル（各管理者向け、利用者向け）
③ 利用者向けインストール簡易マニュアル
④ システムの設定内容の記述書（ID 情報一覧を含む）
⑤ システム試験報告書
⑥ 以上全ての文書の電子データ（CD-ROM 格納）

8.5. 損害賠償

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

8.6. その他

① 納入する物品は、中古品であってはならない。
② 納入するアプリケーションソフト、システムについて、バーションアップ、製造中止が発生した場合､技術的要件及び価格が同等である場合は最新版を導入すること。
③ 本調達の履行について疑義が生じたとき、又は本調達に伴い機構と交わす契約書に定めない事項については、機構及び受注者の双方で協議の上決定すること。
④ 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。
⑤ 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。
⑥ 本調達物品を導入するに当たっては、機構から「国立高専機構サイバー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。
⑦ 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、必ず機構と調整の上とり行うこと。

⑧ 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、又は請け負わせてはならない。ただし、本業務の一部を第三者に委託する場合であり、かつ、機構に書面によって外部委託の詳細を提出し許可された場合は、この限りではない。なお第三者委託を許可された場合であっても、受注者は契約による責任を免れることはできない。

以　上