仕様書

１　業務名

広島市立病院機構機構内ＬＡＮ（事務系）管理用ソフトウェア導入業務

２　業務場所

広島市立病院機構本部事務局財務課情報システム係、その他本機構が指定する場所

３　契約期間

契約締結日から令和６年３月３１日まで

４　業務内容

機構内ＬＡＮ（事務系）のネットワークに接続された端末（２９０台）の運用管理・セキュリティ管理の強化を図るため､以下の機能要件を満たす管理用ソフトウェアを導入する。

⑴　情報セキュリティ対策機能要件

機構内ＬＡＮ（事務系）配下の端末に対し、資産情報収集、操作ログ収集、外部記憶媒体の使用制限、リモート操作を行う構成とすること。これらの機能は一つのコンソールから統合的に管理できること。また、セキュリティを考慮し、専用のアプリケーションからのみ設定、閲覧を可能とし、マスターとなる管理コンソールから許可がない限り利用できないものとする。

ア　資産情報収集

(ｱ)　各クライアントコンピューターに関する各種ハードウェア情報を、資産情報として自動的に収集できること。

(ｲ)　メモリ増設等資産情報が変化した際には変更された資産内容を変更した期間や変更内容を限定して抽出することができること。

(ｳ)　各クライアントコンピューター上のソフトウェアに関するインストール状況（Microsoft Office/ OpenOffice.org インストール状況、Windows 更新プログラム適用状況、ハードディスク上に存在する実行ファイル一覧、Windows10 以降 OS の OS サービスモデルの設定状態を含む）等についても、自動的に収集可能であること。

(ｴ)　収集したハードウェアおよびソフトウェア情報を、一覧で表示できること。

(ｵ)　資産情報の検索の際は、インベントリ情報やWindowsOS のバージョン、サービスパックなどから、同時に複数項目、複数キーワードおよび数値の範囲を指定して検索が可能であること。

(ｶ)　検索の際には、本ソフトウェアから削除されたクライアントコンピューターも、

検索対象として指定できること。

(ｷ) 規定の資産情報の項目以外に、任意の項目を管理者が入力できること。また、アンケート機能を用いて利用者が入力できること。

(ｸ) クライアントコンピューターで資産情報を収集する際に、ソフトウェアが自動的に収集することが出来ない項目については、アンケート形式でクライアントコンピューター利用者に情報を入力させることで、その回答を資産情報として登録することができること。また、これらは部署ごとに異なるアンケートを複数実施でき、配信したアンケートの複製や再配信、配信期間の指定、結果の CSV 出力、配信中アンケートへの対象クライアントコンピューターの追加が可能であること。

(ｹ) 自由入力で任意の設問を作成してアンケート配信できること。

(ｺ) コンピューターおよびネットワーク機器に対して、Ping 応答もしくは Windows が認識している機器情報（NetBIOS）を用いて以下の項目を収集できること。

・検出日時　・機器種別　・ネットワーク機器名　・IP アドレス
・MAC アドレス　・システム製造元　・ドメイン名

(ｻ) 本ソフトウェアを導入できないコンピューターの資産情報を、資産台帳へ直接アップロードするツールを提供すること。

(ｼ) ネットワーク機器情報を活用してネットワーク機器情報を自動収集し、クライアントコンピューター情報とあわせて台帳管理できること。

(ｽ) 各クライアントコンピューターから自動収集した、クライアントコンピューターやレジストリの情報を一覧表示すること。

(ｾ) 収集した資産情報を検索できること。検索条件には、インベントリ情報や OS のバージョン、空き容量、死活監視状態など複数項目を指定した AND,OR,NOT 検索が可能で、キーワードを指定する際は、空白を挟むことで複数のキーワードを指定できること。

(ｿ) 検索条件ごとに表示項目の順序・表示非表示を定義・保存でき、呼び出せること。

(ﾀ) CSV ファイル形式でインポートしたデータを資産情報として登録できること。また、収集した資産情報を CSV ファイル形式で出力できること。

(ﾁ) 当該ソフトウェアで収集したネットワーク機器の接続状況を定期的に監視する設定ができる機能を有すること。また、接続状況に異常（通信不可）が生じた場合には、自動的にメール等で通知する機能を有すること。

(ﾂ) BitLocker および他サードパーティ製品により、ハードディスクを暗号化した際に生成される回復キーを収集し、管理できること。収集した BitLocker の回復キー情報は CSV 形式でエクスポートできること。また、これらの暗号化状態をハードウェア一覧で確認でき、暗号化状態が変更された時はドライブログとして記

録できること。

(ﾃ) 収集したアプリケーション一覧の情報を CSV ファイル形式で出力できること。

(ﾄ) 指定したアプリケーションがインストールされていないクライアントコンピューターを一覧表示できること。また、指定したアプリケーションがインストールされていないクライアントコンピューターに対してメッセージを表示できること。

(ﾅ) ソフトウェアの配布日時と対象端末を設定し、配布したソフトウェアの配布状況および実行状況を確認することができること。

(ﾆ) 配布時に利用する帯域を制限できること。

(ﾇ) Administrator 権限がない端末であっても実行が出来るよう、配布方法とし管理機からのプッシュ、およびクライアントコンピューターからのプルを選択可能なこと。

(ﾈ) クライアントコンピューターがソフトウェアの配布を受ける際、すでに同一のセグメント内のクライアントコンピューターに配布されたソフトウェアがキャッシュとして残っていた場合、そのクライアントコンピューター（以下キャッシュ端末と呼ぶ）からソフトウェアを配布できること。

(ﾉ) キャッシュ端末からソフトウェアをダウンロードする際、通信帯域を制限できること。

(ﾊ) キャッシュ端末に同時に接続できる端末数を制限し、キャッシュ端末の負荷を抑えられること。

(ﾋ) ４GB 以上のサイズのソフトウェアをキャッシュ配布で配布できること。

(ﾌ) 指定したクライアントコンピューターに対して、Windows 更新プログラムを配布し、自動的に更新プログラムの実行を行う等のセキュリティパッチを適用する機能を有すること。

(ﾍ) クライアントコンピューター毎の更新プログラムの適用状況が管理コンソールで確認できること。

(ﾎ) クライアントコンピューターに対して、Windows 更新プログラムを配布し、自動的に更新プログラムの実行を行う等のセキュリティパッチを適用する際、WSUS（Microsoft Windows Server Update Services）と連携し、更新日や更新時間を設定して適用できること。電源 ON/OFF を制御できる環境下にある場合、適用時に、クライアントコンピューターの電源 ON/OFF が自動で行える設定ができること。さらに、設定により Windows Update からの更新プログラムダウンロード（デュアルスキャン機能）を制限できること。

(ﾏ) IP アドレスの管理台帳と、資産情報（不許可端末検知情報も含む）を照合し、競合や不正使用、使用期限切れの表示を行えること。また表示方法は、一覧表示およびマップ表示を行えること。

(ﾐ)　廃棄したクライアントコンピューターの情報も管理できること。また、廃棄済み端末として登録したクライアントコンピューターについては、ライセンスが不要であること。

イ　操作ログ収集機能

(ｱ)　機構内ＬＡＮ（事務系）配下の端末に対し、自動的に対象端末から操作ログを収集して管理できる機能を有すること。

(ｲ)　収集可能なログは、アクティブ状態のウインドウタイトルと稼働時間、ログオン、ログオフの日時、操作開始、操作終了、実行されたソフトウェアについての起動・終了時間、ファイル操作、共有フォルダへのアクセス・ファイル操作、Web へのアクセス・書き込み・アップロード、クリップボードにコピーされた内容、USB メモリなどの記憶媒体を利用した内容、記憶媒体のシリアル情報、接続した通信デバイス、および外部との通信状況等とする。

(ｳ)　端末機上のファイルおよびサーバー上の共有ファイルに対する操作について、操作したファイルのフルパスを記録し、一つのファイルに対して、どのような操作（コピー・ファイル名変更、新規作成、削除など）が行われたかを抽出して表示できること。Microsoft Office 製品については、名前を付けて保存（別ファイル名保存）ログを取得し、表示できること。

(ｴ)　クライアントコンピューター上で、CD-R/DVD-R へファイルの書き込みを行ったファイル名をログとして記録する機能を有すること。

(ｵ)　クライアントコンピューター上でクリップボードが利用された際に、クリップボードにコピーされたテキストや画像を記録する機能を有すること。

(ｶ)　クライアントコンピューター上でアプリケーションソフトウェアから印刷が実行された際に、その印刷されたドキュメント名、１回の印刷枚数、ファイルパスを記録する機能を有すること。

(ｷ)　Web へのアクセスログについては、https での通信も含め、Microsoft Edge、Firefox および Google Chrome を使って Web の閲覧やダウンロード、アップロード、および書き込みが行われた内容について、ウインドウタイトル、URL、書き込み内容、アップロードしたファイル名および、Microsoft Office 365 / Office Online 上でファイルをローカルに作成した時の、ファイル名やファイルパスを記録できること。

(ｸ)　クライアントコンピューター上から FTP サーバにファイルをアップロードした際に、ログとしてアップロードしたファイル名を記録する機能を有すること。

(ｹ)　クライアントコンピューター上で、USB メモリなどの記憶媒体を利用した内容をログとして記録する機能を有すること。

(ｺ)　シリアルが取得可能な記憶媒体の利用や記憶媒体へのファイル操作については、記憶媒体のシリアル情報も含むこと。

(ｻ)　Bluetooth 接続、無線 LAN アクセスポイントへの接続、TCP/IP 通信等による接続が行われた際に、通信デバイスの情報を記録できること。

(ｼ)　端末機を管理する管理機コンピューターの操作に対しても同様にログ収集が行えること。また、ログ検索・閲覧やリモート操作などの情報セキュリティ対策機能に対する操作のログも取得でき、管理者間で相互に検索および閲覧が行えること。

(ｽ)　エージェントのインストールおよび再起動と同時にログの取得が開始されること。

(ｾ)　リモート操作時には接続元及び接続先のコンピューター名及び IP アドレスが取得可能であること。

(ｿ)　リモート操作した場合のログ証跡を考慮して、管理者の操作ログとクライアントコンピューターの操作ログは、同時検索し、時系列に一覧表示できること。
また、リモート操作時に操作開始/操作終了のログを取得できること。

(ﾀ)　下記の機能は、管理コンソール内ですべて可能でなければならない。

- ログの閲覧範囲は、管理機が登録されているグループ内に限定されること。
- ログを閲覧する際、アプリケーションのインストール状況および資産情報から絞り込んだ端末や、過去にログ検索から絞り込んだ端末に対して、検索を行うことが可能なこと。絞り込み条件は複合的に利用可能なこと。
- ログを閲覧する際、任意の複数カテゴリを選択したうえで、選択したすべてのカテゴリのログを時系列に一覧に並べて閲覧が可能なこと。
- 全カテゴリのログを時系列に並べ替えて一つの画面で表示できること。抽出されたログの一覧から一つの行を選択し、該当端末の前後のログを全カテゴリ分時系列に並べ替えて出力が可能なこと。
- 収集したログに基づいて、事前定義されたルールに反した際に、そのクライアントコンピューターを一覧として表示し、指定したクライアントコンピューターに対して発生したルール違反の操作の前後 5 分間のログを抽出できること。

(ﾁ)　収集したクライアントコンピューターのログを管理画面にて複数条件で検索できること。

(ﾂ)　検索条件はそれぞれ名前をつけて複数の条件を保存できること。

(ﾃ)　検索結果に表示されたクライアントコンピューターをグループ化し、検索グループとして登録できること。

(ﾄ)　収集したログデータは一定期間ごとに圧縮した状態で自動的にバックアップでき、バックアップデータも展開やリストアの作業をすることなく管理コンソールから複数のログ種別を横断的に閲覧できること。

(ﾅ)　端末側で保存するログデータは改変されないように難読化されていること。

(ﾆ)　収集されたログに関しては、CSV 形式で出力する機能を有すること。

(ヌ)　エージェントソフトをアンインストールしたクライアントコンピューターのログを閲覧することができること。

(ネ)　特定の行為及び内容から、事前定義されたルールに従い、自動で通知する機能を有すること。

(ノ)　あらかじめ登録されていないクライアントコンピューターが接続された場合、該当のクライアントコンピューター情報を取得し、一覧表示できること。

ウ　外部記憶媒体の使用制限機能

(ア)　デバイス種別やデバイス種別に対応するメディアごとに、一括で使用制限設定（使用不可/読み取り専用/使用不可能）ができること。

(イ)　使用制限設定は、端末機を管理するグループ単位、端末単位および、Active Directory のユーザー単位にも設定ができること。

(ウ)　設定ができるデバイス種別、メディアは、デバイス種別（USB メモリ、USB ハードディスクドライブ、フロッピーディスクドライブ、CD/DVD ドライブ、Blu-ray ドライブ、イメージスキャナー、デジタルカメラ、モバイル端末、Windows ポータブル デバイス)、メディア（DVD-RAM、SD カード、MO ディスク、コンパクトフラッシュなど）とする。

(エ)　登録されたメディアに対して個体識別情報を自動発行し、指定したメディアの使用不可/読み取り専用/使用不可能を設定できること。

(オ)　外部記憶媒体をコンピューターに接続した際にデバイス名、シリアルナンバー、ベンダーID を自動で収集・台帳登録が行えること。

(カ)　台帳に登録した外部記憶媒体に対して、シリアルナンバーごとに使用制限（使用不可/読み取り専用/使用不可能）の設定ができ、設定対象を Active Directory のユーザー単位、クライアントコンピューター単位、およびユーザーとクライアントコンピューターの組み合わせ単位で指定ができること。

(キ)　外部記憶媒体の管理台帳に登録されている USB メモリについて、各 USB メモリの利用者もしくは管理責任者が USB メモリをクライアントコンピューターに挿入することで管理台帳に登録されているデバイス名、シリアルナンバー、ベンダーID と照合が行われてその所在確認を一括管理でき、管理台帳に反映できること。

(ク)　外部記憶媒体の紛失時に端末への着脱日時と記録されたファイル名、作成日時、更新日時、ファイルサイズの情報とを利用して、外部漏洩の危険性があるファイルを抽出できること。

(ケ)　管理機で作成したワンタイムパスワードをクライアントコンピューター上のツールに入力することで、一時的に USB デバイスのシリアルナンバー単位でデバイスの使用制限を解除する機能を有すること。

(コ)　使用制限を解除する期間・端末・デバイスをそれぞれ指定することができること。

エ　リモート操作機能

(ｱ)　機構内ＬＡＮ（事務系）配下の各端末機にリモート接続できる機能を有し、画質を落とすなどでデータ転送量を削減できること。

(ｲ)　複数の端末機に対して、一斉にリモート操作ができ、操作をする対象となる端末機のウインドウ画面をセンタリング、左上もしくは代表画面にそろえる機能を有すること。

(ｳ)　Windows 端末の 2 画面以上のディスプレイを同時に使用しているコンピューターに対してリモート操作を行う場合、操作するディスプレイを切り替えて対応できる機能を有すること。

(ｴ)　パスワード入力など、セキュリティの観点からクライアントコンピューターに表示したくない遠隔操作を行う場合は、クライアントコンピューターに対して操作画面を隠しながら遠隔操作を行えること。

(ｵ)　フリーソフトとして提供されているアプリケーションからのアクセスは不可能であること。

(ｶ)　リモート操作時に、操作機側とクライアントコンピューター間でテキストデータやビットマップ形式の画像データをコピー&ペーストし、共有できる機能を有すること。

(ｷ)　リモート操作を受けるクライアントコンピューターの画面を、管理者画面で拡大・縮小、全画面表示を行うことができること。リモート操作を受ける側の PC の画像解像度が、リモート操作を行う側（管理機）の PC より低い場合でも、管理者画面で拡大・縮小、全画面表示を行えること。

(ｸ)　遠隔操作を開始する際、クライアントコンピューター側がその開始を確認できる機能を有すること。

(ｹ)　遠隔操作を開始する際、予め指定したアプリケーションをクライアントコンピューターが起動中である場合、クライアントコンピューター側で、リモート操作の許可/拒否/アプリケーション画面を保護して許可、の 3 つを選択できること。

(ｺ)　アプリケーション画面を保護して許可を選択した際は、あらかじめ指定したアプリケーションの画面のみが隠れた状態で遠隔操作ができること。

(ｻ)　端末に対してリモート操作を行うことが可能なこと。これらの操作は、管理コンソール内ですべて可能でなければならない。

- リモート操作の範囲は、管理機が登録されているグループ内に限定されること。
- リモート操作を行う際、アプリケーションのインストール状況および資産情報から絞り込んだクライアントコンピューターに対して、リモート操作を行うことが可能なこと。絞り込み条件は複合的に利用可能なこと。

⑵　システム構築要件

ア　発注者が準備する仮想サーバ（CPU：8 コア、メモリ：8GB、ストレージ 500GB、OS：

Windows Server 2022（64 ビット））に受注者はシステムを構築すること。

イ　構築範囲は仮想サーバ OS の初期設定及び資産管理ソフトを動作させるために必要な設定を行うこと。

ウ　資産管理ソフトの構築に伴う事前打ち合わせ及び構築作業は資産管理ソフトのメーカーが行うこと。

エ　資産管理ソフトのメーカーが管理者向けの教育を行うこと。

オ　日本語の操作マニュアルを提供すること。

カ　発注者が準備するテスト用クライアント機（10 台）に対して動作確認を行うこと。

⑶　システム運用保守要件

本件で導入したシステムの運用保守に係る契約は、別途（令和７年４月１日開始）予定しているが、それまでの間においても以下の項目に対応すること。

ア　受注者は、発注者からの電話やメール等によるシステムに関する問い合わせを、平日午前９時から午後１７時（土日祝日以外の営業日）までの間、受付し、回答すること。

イ　保守範囲に仮想サーバの OS についても保守の対象とすること。

ウ　保守範囲の障害対応は一時切り分けまでとし、障害への対策は本契約に含めない。

エ　保守範囲にシステムの設定変更・パッチあて・バージョンアップは含めない。

５　テスト

⑴　受注者によるテスト

受注者は本書に示した要件が実現されているかテストを実施し、テスト結果を本機構に報告すること。

⑵　利用者によるテスト

ア　受注者は、本機構の職員がテストを行うために必要な準備を行うこと。

イ　受注者は、利用者によるテストで発見された課題・問題点を管理表で管理し、全ての課題・問題点の対応を完了した上で、本機構の承認を得ること。

６　プロジェクト管理

⑴　実施計画

ア　受注者は、業務履行開始に当たり、契約締結後５日以内に速やかに本機構委託契約約款第６条に規定する実施計画書を作成し、本機構の承認を得ること。

イ　実施計画書では、現場責任者の氏名及び連絡先、作業実施体制（従業員の氏名及び連絡先、役割分担）を明らかにすること。

ウ　実施計画書を変更する必要があるときは、本機構の承認を得た上で計画を変更し、変更後の実施計画書を提出すること。

⑵　進捗報告

ア　受注者は、定期的に作業の進捗状況を説明する報告書を作成した上で、本機構と協議を行い、進捗状況、課題等について本機構に説明すること。

イ　本機構との打ち合わせ・協議を行う際には、あらかじめ協議事項を連絡すること。終了後には議事録を作成した上で１週間以内に本機構に提出し、内容に疑義がある場合は速やかに補正すること。

ウ　課題については、議事録とは別に一覧にまとめること。

⑶　実施報告

受注者は、全ての業務完了後、本機構委託契約約款第 12 条に規定する実施報告書を令和６年３月３１日までに提出し、本機構の承認を得ること。

7　納品成果物

⑴　成果物

区分	成果物	内容
設計	基本設計書	本システムの設計内容の概要等を記載した文書
	詳細設計書	本システムの各種設定内容を記載した文書
テスト	テスト結果報告書	受注者によるテストの結果を記載したもの
運用	管理者用マニュアル	本システムの管理者が実施する作業の内容と手順を記載した操作マニュアル
	利用者用マニュアル	本システムの利用者向けの操作マニュアル

⑵　納品形態

各成果物は、本機構が別途指定する紙及び可搬記録媒体に記録した電子データにて提出すること。ただし、紙での提供が難しいものについては、本機構と受託者が協議の上、納品形態を決定する。

8　その他

⑴　本業務の実施に当たっては、病院業務に支障を来たさないよう配慮すること。

⑵　本仕様書に疑義が生じたとき、又は、定めのない事項については、本機構と受注者で協議して定めるものとする。

⑶　受注者は、業務の実施に当たり、本機構が定める「広島市立病院機構情報セキュリティポリシー」を遵守すること。