IT資産管理システム
仕様書

国立研究開発法人
国立循環器病研究センター
令和7年6月

仕様書　目次

IT資産管理システム

【重要】仕様書で求める機能要件について

・全てが必須要件であり、開札後の実現不可の申入れには応じない。
・前提や制約がある場合はC列にコメントとして追記すること。ただし当センターが認めない場合は
　失格となるので留意すること。

項番	機能要件
A	目的・共通要件
A.1	基本要件
A.1.1	調達の背景と基本方針
A.1.1.1	国立研究開発法人 国立循環器病研究センター（以下、当センターと称する）は2019年7月の移転を機に更新した情報システム群の多くが2025年12月末を以て契約期間の満了を迎える予定である。本調達対象であるIT資産管理システムも前回のライセンス期限に合わせて構築したものであり、2026年3月末に期限を迎えるが、現行システムの課題や環境変化に対応したシステムとして新たに構築することとする。
A.1.1.2	管理対象範囲を見直し、VDI環境等も含めた当センターに接続する全ての端末を管理対象とする。ただし、別途調達予定の病院情報システムにて調達される端末は対象外とする。
A.1.1.3	当センターではインターネット接続が可能なネットワークと、主に診療に使用しているインターネット接続が不可なネットワークに論理分割している。
A.1.1.4	この仕様書に定めのない事項が生じた場合、また不明な点が生じた場合等はセンターと受注者で協議し決定することとする。しかし、この仕様書に明記のない場合においても、技術的並びにその性質上当然必要なものについては誠意をもって行うこと。
A.1.2	本調達の範囲
A.1.2.1	IT資産管理システムライセンス一式
A.1.2.2	2026年1月1日を稼働開始日として6年間のライセンス費用
A.1.3	ライセンス
A.1.3.1	当センターで利用するIT資産（サーバ、PC、スマートデバイス、仮想サーバ、仮想PC、その他ネットワーク接続する機器）を登録管理ができるライセンスを契約期間にわたって提供すること。
A.1.3.2	ユーザーライセンスの場合、2025年3月時点で2,500ユーザーである。 デバイスライセンスの場合、登録数ベースで4,000台、90日間の接続数ベースでは3,280台である。 上記の情報を元に適切なライセンス数量を導入すること。想定される登録数ベースの内訳は下記の通り。（詳細は別紙1を参照すること）
A.1.3.3	WindowsPC　：　2,800台（サーバ、仮想サーバ含む）
A.1.3.4	仮想PC(Windows環境のVDI等)：　250台
A.1.3.5	MAC PC　：　600台
A.1.3.6	Linux/Unix PC　：　350台（サーバ、仮想サーバ含む）
A.1.3.7	管理コンソールの操作ユーザー数は40名以上とすること。管理コンソール同時接続数6以上とすること。
A.1.3.8	管理コンソールはWindows 11 Proから操作できる環境とすること。インストールアプリケーションでも、WEBアプリケーションでも形式は問わない。WEBアプリケーションの場合は最新のChrome、Edgeに対応し、IE互換モードなどの利用は認めない。
A.1.3.9	端末のリモート操作にライセンスが必要な場合、リモート操作ユーザー数30以上、同時接続セッション数6以上とすること。
A.1.3.10	下記に含まれないライセンス(OS、DB、CAL、その他稼働に必要な有償ライセンス)は全て本調達に含めること。 ・当センターはMicrosoft 365 Enterprise E3を契約している。契約に含まれるCALは本調達に含まなくてよい。 ・Windows Server 2025のライセンスは別途調達予定である為、本調達に含まなくてよい。本システムは別途調達の仮想化基盤上に当センターが構築する。この際、Windows Server 2025を利用予定である。
A.1.3.11	データベースライセンスが必要な場合は、システムの安定性・拡張性・標準化への対応、仮想化基盤上でのライセンス費用を考慮した、最良の製品を採用すること。
A.1.3.12	ライセンスのカウント、制御についての情報を提示すること。例えばライセンス数を超えたときの動き、長期間未接続端末のライセンスのはく奪、再適用、どの程度の期間でライセンスがはく奪されるか、紳士協定の場合ライセンス数確認タイミングなど。
A.1.3.13	別紙1の同時接続や期間平均ライセンスでの提案の場合、移行開始時や年度末などは登録数のピークを迎えることが想定される。前項及び、登録数のピークを考慮に入れたうえで見積を行うこと。
A.2	共通要件
A.2.1	全体
A.2.1.1	本仕様書は、当センターに導入するIT資産管理システム一式について規定するものである。
A.2.1.2	本システムの利用期間は2026年1月から2031年12月末の6年とする。
A.2.1.3	納入場所は、国立研究開発法人 国立循環器病研究センター 大阪府吹田市岸部新町とすること。
A.2.1.4	今回の調達するライセンスは当センターの用意する仮想基盤上に当センターにて構築する予定である。必要なサーバ数、スペックは提示すること。
A.2.1.5	ライセンスはより低価格で、より良い医療ICTを調達するという目的に沿った提案を行うこと。

項番	機能要件
A	目的・共通要件
A.2.1.6	仕様回答書で対応可能と回答した機能要件を満たすための費用は、全て本調達に含めること。
A.2.1.7	仕様書の必須項目は、完全に実現できなければならない要件であるが、部分的にできない内容やシステム上の機能が異なる場合は、その旨を記載してシステム上又は運用上での回避方法を明記すること。
A.2.1.8	その提案が合理的であると当センターが判断すれば、仕様を満たしていると判断することもある。ただし、提案内容が不十分であれば、失格となる場合があるので十分に注意すること。
A.2.1.9	提出された資料について、当センターが不明確であると判断した場合は、技術的要件を満たしていない資料とみなす場合があるので十分に注意すること。
A.2.1.10	デファクトスタンダードに準拠した環境対応を基本とし、システムのOS・通信プロトコル等は国際標準・業界標準を積極的に対応すること。
A.2.1.11	本調達システムを構成するソフトウェアは、稼動実績のあるプロダクトを採用すること。
A.2.1.12	前項に関し、提案者が当センターにとって有益であると判断した場合は、実績のない製品を利用してもよい。ただし、医療現場での利用を前提としたものであることを十分に説明できる資料を添付すること。
A.2.1.13	仕様書に記載されていない機能を最新標準パッケージ機能として搭載している場合は、その利用を前提として機能を提供すること。
A.2.1.14	円滑な構築業務遂行のため、当センター又は当センターと同規模以上(500床以上)の医療機関において、IT資産管理システム納入実績を有することを客観的に証明すること。
A.2.1.15	受注者は、本調達システムの明細書(ソフトウェア・ライセンス費用等の品名、数量、標準価格、提供価格が記載された明細書)を提示すること。
A.2.1.16	契約期間に先立って、構築のための試用や機能確認ができるような製品および情報の提供を行うこと。具体的には2025年10月ごろよりサーバーを構築し、連携、動作確認を行う予定である。無償での試用にユーザー数、デバイス数に限りがある場合はその範囲で試用を行う。別途有償ならば、先行して20ユーザーライセンスもしくは30デバイスライセンスを2025年10月1日からの費用に含めること。
A.2.1.17	契約期間中であっても利用状況に応じて構成や単価の見直しについて協議を行い、双方合意の上で変更契約ができること。
A.2.1.18	本調達のライセンスは、2025年12月末までに確実に納入すること。
A.2.1.19	受注者の責めに帰すべき理由により、当センターへのライセンスやアプリケーションデータの納入遅延が発生した場合は、契約書に規定する条項に沿った損害負担をすること。
A.2.1.20	受注者の自社製品だけで仕様を満たさない場合は、他社製品を使って仕様を満たしてもよい。ただし、受注者は、他社製品を用いて満たす要件も含めて、本仕様書の全要件の内容を把握し、各章にまたがる要件を整理の上、他社製品との機能範囲を明確にすること。
A.2.1.21	AD連携(CSV連携)、Windows Server Update Services (WSUS)連携、接続に必要なライセンス費用は本調達に含めること。ただし、接続先のシステムや機器に必要となる費用及び接続作業に必要となる費用は当センターにて対応とする。
A.2.1.22	疑義がある場合には、入札前に質問事項として当センターに提出し、その回答に従うこと。
A.2.1.23	本システムの構成が理解できるように、ハードウェア・ソフトウェア等の構成図を提出すること。
A.2.2	情報セキュリティ管理
A.2.2.1	ソフトウェアの選定に当たっては、サプライチェーン・リスクに配慮すること。 調達後、保守期間を通じて新たなサプライチェーン上の脅威が発見された場合には、受注者は当センターに対しかかる脅威についての情報提供を行うこと。 （参考文献） ◦ 「IT製品の調達におけるセキュリティ要件リスト」 ◦ 「ITセキュリティ評価及び認証制度(JISEC)」
A.2.2.2	受注者の資本関係・役員等の情報について情報提供を行うこと。
A.2.2.3	納入候補となるソフトウェアについては予め当センターに構成リストを提出すること。当センター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、提案の見直しを図ること。
A.2.2.4	データベース内に格納するデータは可能な限り暗号化に対応すること。
A.2.2.5	操作ログには操作対象データや操作内容を含むこと。
A.2.2.6	主体認証のパスワードは可能な限り英大文字（26種類）小文字（26種類）＋数字（10種類）＋記号（26種類）の計88種類の文字をランダムに使って、10桁以上の設定に対応すること。
A.2.2.7	アカウントロックの機能を可能な限り設定可能なこと。アカウントロック機能を有する場合、アカウントロックされた際は、可能な限り管理者へ通知ができ、システム管理者によるロック解除か、一定時間経過でのロック解除を可能な限り設定可能なこと。
A.2.2.8	一定回数以上のログイン試行を可能な限り管理者に通知する仕組みを有すること。

項番	機能要件
A	目的・共通要件
A.2.2.9	本調達で納品されるライセンスは、最新のプログラムやセキュリティパッチを適用の上でシステム動作試験を行う。Windows Server 2025、データベースの更新プログラムやセキュリティパッチへの対応状況について可能な限り情報提供を行うこと。なお、適用は当センターにて行う。
A.2.2.10	ソフトウェア及びサイバーセキュリティリスクの高い機器等の調達における透明性の確認を必要とするため、SBOM(Software Bill of Materials：ソフトウェア部品表)を可能な限り提出すること。または、構成するソフトウェアに関する脆弱性、サプライチェーンリスクについて確認したSBOMと同等の効果が発揮できる資料の提示でもよい。
A.2.3	高可用性
A.2.3.1	本調達システムは、24時間・365日稼動可能であること。ただし、システムのメンテナンス時は除く。
A.2.3.2	メンテナンス等の必要時を除き、再起動の必要がないこと。必要な場合は、その頻度を記載すること。
A.2.3.3	システムの不慮の停止時において、データベースが破壊される可能性はゼロではないので、毎日のデータベースバックアップが必要となるが、データベースバックアップ処理中もシステムの運用中断を伴わないようなシステムであること。バックアップデータは7世代程度を想定している。
A.2.3.4	システムのバックアップには別途調達する仮想化基盤の仕組みとしてスナップショットやイメージ取得といった仮想化基盤のソリューションを利用する予定である。スナップショットなどのバックアップによる実績があること。日次で増分、週次のフルバックアップ2世代保存する予定である。
A.2.4	障害対策
A.2.4.1	障害発生時においても、病院業務の遂行に支障を及ぼす影響を極小化し、復旧時の保守管理操作も容易なシステムを提供すること。
A.2.5	院内ネットワーク
A.2.5.1	当センターの用意するネットワークインフラにて運用できること。
A.2.5.2	その場合は、指定したIPアドレス体系を利用できること。
A.2.5.3	ライセンス認証やアップデート等の基盤維持に必要な目的以外で、データが当センターの用意するインフラ以外を経由しないこと。
A.3	共通機能
A.3.1	設定管理
A.3.1.1	各設定変更やメンテナンスは、当センター職員ができること。
A.3.1.2	各設定変更やメンテナンスは、権限を与えられた管理者のみが操作できること。
A.3.2	本調達システムの管理用ログイン・認証は、以下のとおりとすること。
A.3.2.1	パスワードの変更は、ログインユーザー自身にてできること。
A.3.2.2	管理者ユーザー、または管理端末毎に、使用機能を制限できること。
A.3.2.3	一定時間システムを使用しなかった場合は、可能な限り自動的にログオフする設定が可能なこと。制限時間については、可能な限りシステム管理者で設定できること。
A.3.3	運用管理機能
A.3.3.1	データのバックアップは、自動でできること。
A.3.3.2	IT資産管理システムは当センターのタイムサーバー又はOSの時刻に同期できること。OSとタイムサーバーの時刻同期設定は当センターで実施する。

項番	機能要件
B	役務・保守他
B.1	役務等
B.1.1	本調達はソフトウェア製品のライセンス購入であり、導入時の役務は求めない。
B.2	納品
B.2.1	納品物
B.2.1.1	必要なライセンスと合わせて以下を納品すること。
B.2.1.2	◦ 調達ソフトウェア、ライセンス類一覧
B.2.1.3	◦ 標準マニュアル
B.2.1.4	◦ 情報セキュリティに関する文書
B.2.2	用語定義(納品物)
B.2.2.1	◦ 調達ソフトウェア、ライセンス類一覧：本調達システムの構築に必要なライセンス及びソフトウェアを記載したもの。　※ただし、当センターが用意するライセンス及びソフトウェアは対象外とする。
B.2.2.2	◦ 標準マニュアル：「B.2.3」記載のもの。なお、当センター向けにカスタマイズは不要である。
B.2.2.3	◦ 情報セキュリティに関する文書：「A.2.2　情報セキュリテイ管理」で求める文書類。
B.2.3	マニュアル
B.2.3.1	以下のマニュアルを電子媒体の形式で提供すること。提供方法はDVD等の媒体、メール、サポートサイトからのダウンロードいずれでも良いものとする。
B.2.3.2	◦ インストールマニュアル
B.2.3.3	◦ 設定マニュアル(各種設定パラメータ)
B.2.3.4	◦ 操作マニュアル
B.2.3.5	◦ バージョンアップマニュアル
B.2.3.6	◦ バックアップ/リカバリマニュアル
B.2.3.7	◦ その他製品マニュアル
B.2.4	その他
B.2.4.1	本調達で納入する全てのソフトウェアに関するマニュアルを提供すること。
B.2.4.2	マニュアルは、日本語版で提供すること。
B.2.4.3	物理媒体、メール等でのデータ納品時には必ずマルウェアに対するセキュリティチェックを行い、クリーニングした上でその証左と共に納品すること。
B.3	保守
B.3.1	全般
B.3.1.1	2031年12月末までの稼動後6年間の全ての保守費用を本調達に含めること。なお、本調達範囲内での稼動後6年間の追加費用の発生は認めない。
B.3.1.2	本調達ライセンスに含まれる標準サポートを行うこと。
B.3.1.3	標準サポートでは技術的な問合せに対応できること。
B.3.1.4	ライセンス付属以外の標準サポート以外の費用は原則として含めないが、アプリケーションのアップグレード権に別途費用が必要な場合はライセンス期間中のアップグレード権費用を含める事。なお、アップグレード作業は当センターにて行う為、アップグレード作業費を含める必要は無い。
B.3.2	ソフトウェア保守
B.3.2.1	ソフトウェアの瑕疵に対応し、更新プログラムや対応方法等を提供すること。

項番	機能要件
C	IT資産管理システム
C.1	基本方針
C.1.1	仕様書の必須項目は、完全に実現できなければならない要件であるが、部分的にできない内容やシステム上の機能が異なる場合は、その旨を記載してシステム上又は運用上での回避方法を明記すること。
C.1.2	その提案が合理的であると当センターが判断すれば、仕様を満たしていると判断することもある。ただし、提案内容が不十分であれば、失格となる場合があるので十分に注意すること。
C.1.3	基本機能についてすべての機能をWindows、MacOS、Linuxにて満たせることが望ましいが、特記なき限り、Windows端末について満たせればよいものとする。特記は大項目に記載がある場合、小項目すべてに適用される。大項目、小項目両方に記載がある場合、小項目が優先される。大項目、小項目両方に記載がない場合、Windows端末について満たせれば良いものとする。
C.2	基本要件
C.2.1	ネットワークに接続されているサーバ、PC、スマートデバイス、仮想サーバ、仮想PCについて、資産情報の収集が可能なこと。対象のOSは、下記とする。 ・Windows：Server 2016以上、11 pro以上 ・MacOS：13以上(Ventura、Sonoma、Sequoia以降) ・Linux：Ubuntu,Red Hat Enterprise Linux(サポート期間中のOSに限る)
C.2.2	下記リモート環境にエージェントインストール及び、管理できること。 ・リモート(VDI等)ホスト(接続先)環境対応(Windows) ・シンクライアント環境対応(Windows) ・リモート(VDI等)クライアント(接続元)環境対応(Windows、MacOS)
C.2.3	その他ネットワークに接続する機器（プリンター、PCの周辺機器、医療機器、監視カメラPC、入退室管理機器など）の稼働状況を一括管理できること。(例：SNMPでMIB情報収集、PINGによる死活監視等)
C.2.4	接続機器の情報セキュリティの強化に資すること。
C.2.5	接続機器の資産棚卸が管理者の負担なくできること。
C.2.6	エージェントをインストールする事で、接続機器をIT資産管理システムへ自動登録ができること。エージェントをインストールできない機器（プリンター、周辺機器、医療機器など）は任意で登録、又はCSVインポート等により一括登録ができること。
C.2.7	収集したデータはCSV形式で出力することができ、出力したデータは自由に加工できること。
C.2.8	MDM（Mobile Device Manegement）は別途とするが、スマートデバイス情報の登録などの簡易的な機能を有すること。
C.2.9	利用者の属性情報や利用機器情報、スマートデバイス情報からグルーピングができること。
C.2.10	資産情報は一覧表示及び、特定の端末の資産情報を個別確認できること。
C.2.11	仕様書に記載のない資産管理項目もパッケージに実装している項目は含むこと。
C.3	ハードウエアIT資産管理 ※Windows、MacOS、Linux
C.3.1	接続機器のハードウェアIT資産情報が速やかに収集できること。
C.3.2	IT資産情報収集は原則として自動でできること。
C.3.3	IT資産情報収集が自動でできないものは任意にできること。(自動登録できない端末)
C.3.4	IT資産情報のネットワーク接続状況は1時間毎等、定期的に監視でき、一覧表示できること。
C.3.5	任意の登録は、手入力による個別登録とCSVデータによる一括登録の2つができること。
C.3.6	変更があったIT資産情報は速やか(少なくとも約1時間毎)に反映され、一覧などで確認ができること。(Windows、MacOS)
C.3.7	IT資産情報から必要な情報を指定して一覧表示できること。
C.3.8	IT資産情報を検索し、絞込できること。検索条件は複数項目を指定したAND,OR,NOT検索が可能。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。検索キーとして、機器名称、コンピュータ名称、IPアドレス、MACアドレス（有線/無線）等が使用できること。
C.3.9	ネットワーク機器情報もIT資産情報として収集できること。(ネットワーク機器)
C.3.10	IT資産情報・ネットワーク機器の接続状況は定期的に監視できること。
C.3.11	ネットワーク機器の接続状況の状況を分かりやすく表示できること。
C.3.12	ネットワーク機器の接続状況の異常を管理者へ通知できること。
C.3.13	収集したハードウェアのIT資産情報はCSV形式でデータ出力できること。
C.3.14	データ出力は、全データの一括抽出とデータ範囲や期間を指定した部分抽出ができること。
C.3.15	IT資産情報をグループ管理可能であること。
C.3.16	IT資産情報のグループはツリー構造で管理できること。

項番	機能要件
C	IT資産管理システム
C.3.17	IT資産管理システムにデバイスが登録される際、自動でグループに振り分けが可能なこと。具体的にはインストールするエージェントにより振り分けられるグループが変わることを想定している。但しエージェントをインストールできないネットワーク機器については任意の登録操作の際にグループ分けが可能なこと。IPアドレスによる振り分けを用いる場合、エージェントインストール（IT資産管理サーバ接続）時点と、その後の利用の際ではIPアドレス体系が変わることに注意すること。
C.3.18	IT資産情報の所属するグループを変更可能であること。
C.3.19	グループの振り分けはCSVデータによる一括登録・変更ができること。

項番	機能要件
C	IT資産管理システム
C.3.20	IT資産情報のグループ毎にポリシーを設定できること。(Windows、MacOS)
C.3.21	ポリシーではデバイス制限の運用ルールが設定できること。(Windows、MacOS)
C.3.22	同一のIT資産情報が2重登録されない仕組みを有すること。なお当センターの運用上、異なるPCであってもPC名の重複は発生する。2重登録が避けられない場合があれば提示すること。
C.3.23	新規に管理対象となるPCに対して、管理対象になったことを自動判断できること。
C.3.24	以下のIT資産管理情報が収集できること。 ※Windows、MacOS、Linux
C.3.24.1	OS名称
C.3.24.2	OSのバージョン情報 ※WindowsについてはWindows10以降のOSサービスモデルの設定状態を含むこと
C.3.24.3	機器名称（PC、プリンター、サーバ、医療機器など）
C.3.24.4	コンピュータ名称
C.3.24.5	IPアドレス
C.3.24.6	MACアドレス（有線/無線）
C.4	ソフトウエアIT資産管理　※Windows、MacOS、Linux
C.4.1	接続機器のソフトウエアIT資産情報が速やかに収集できること。
C.4.2	情報収集は原則として自動でできること。
C.4.3	変更があったソフトウェアIT資産情報は速やか(少なくとも1時間毎)に反映され、一覧などで確認ができること。(Windows、MacOS)
C.4.4	IT資産情報から必要な情報を指定して一覧表示できること。
C.4.5	収集したソフトウェアのIT資産情報はCSV形式でデータ出力できること。
C.4.6	データ出力は、全データの一括抽出とデータ範囲や期間を指定した部分抽出ができること。
C.4.7	Microsoft Office 365のバージョン情報が管理できること。(Windows)
C.4.8	以下のIT資産管理情報が収集できること。 ※Windows、MacOS、Linux
C.4.8.1	インストールされているウイルス対策ソフトのアプリケーション名称
C.4.8.2	インストールされているウイルス対策ソフトアプリケーションのバージョン情報(Windows、MacOS)
C.4.8.3	インストールされているアプリケーション名称
C.4.8.4	インストールアプリケーションのバージョン情報
C.4.8.5	実行ファイルインストール状況（Windows）
C.4.9	アプリケーション稼働管理 ※Windows
C.4.9.1	アプリケーションの稼働情報が速やかに収集できること。
C.4.9.2	未使用アプリケーションの情報が速やかに収集できること。
C.4.9.3	アプリケーションの追加と削除の情報を収集し、保有ライセンス数とインストール数を照合できること。
C.4.9.4	不正アプリケーションは、exe名で禁止することができること。
C.4.9.5	アプリケーションの操作時間
C.5	デバイス管理　※Windows、MacOS
C.5.1	管理対象の機器のデバイス、接続されたデバイスを管理できること。デバイスは下記とする。 ・外付けのCD/DVDドライブ ・記憶領域をもつUSB接続機器 主にUSBメモリやUSBハードディスク等 スマートフォンやタブレットなどのスマートデバイスを含む USBハブ、SDカードリーダ等を経由した接続を含む
C.5.2	PC毎、及びグループ毎にデバイスの使用認可制限できること。 ※デバイスについてのグループはデバイスのグループ、又はPCのグループ等、一定のグルーピングされた状態を指すものとする。 ※デバイスについての使用認可制限は利用禁止、読み込みのみ許可、及び読み書き許可を指すものとする。使用認可とした場合、読み込みのみ許可、又は読み書き許可を指すものとする。
C.5.3	PC毎、及びグループ毎に内臓CD/DVDドライブの使用認可制限できること。
C.5.4	PC毎、及びグループ毎にデバイスの制限をしない事ができること。
C.5.5	PCがサーバと通信できない状態の場合、最後にサーバと通信した時点で、オフラインとなるPCで使用可能なデバイスは継続して使用可能であること
C.5.6	デバイスのシリアル情報が取得できない場合、PC毎、又はグループ毎に対してベンダーIDとプロダクトIDが一致していれば使用可能、もしくはシリアル番号とは別に個体識別が可能といった回避設定での使用認可制限が可能なこと。
C.5.7	使用認可したデバイスのみを使用可能にできること。
C.5.8	デバイスはグループ別のデバイス表示が可能なこと。
C.5.9	PC毎に使用認可したデバイスに対して別PCに対しても使用認可できること。
C.5.10	グループ毎に使用認可したデバイスに対して別グループに対しても使用認可できること。
C.5.11	PC毎、デバイス毎の使用認可制限を併用できること。

項番	機能要件
C	IT資産管理システム
C.5.12	デバイス個別に利用可能なPCを1対1で指定が可能なこと。
C.5.13	デバイス個別に利用可能なPCを複数指定可能なこと。
C.5.14	使用認可していないデバイスが接続された際にデバイスのシリアルナンバー、ベンダID、ベンダ名、プロダクトID、プロダクト名を自動で収集し、管理台帳へ登録可能なこと。
C.5.15	記憶領域を持たないマウス、キーボードなどのデバイスについてはPC毎、グループ毎、デバイス毎に許可設定を行わずとも使用できること。
C.5.16	棚卸機能によりデバイスの所有状況を確認できること。
C.5.17	所有状況は各デバイスの利用者もしくは管理責任者が確認し、デバイスをPCに接続することでその状況を一括管理でき、管理台帳に反映できること。
C.5.18	デバイス紛失時の確認の為、最後にサーバと通信した際にデバイス内に保存されていたファイル情報一覧を確認できること。ファイル数は10,000以上確認できること。
C.5.19	デバイスの所属するグループは変更できること。
C.5.20	USB2.0、3.0等の規格に関わらず制御ができること。
C.5.21	許可しているデバイスを接続している場合、リモート環境にデバイスがリダイレクト可能である(禁止しているデバイスならリダイレクトされない)こと。
C.5.22	デバイスを一覧管理できること。
C.5.23	一覧管理情報はCSVファイルインポートによる登録、削除、変更が可能なこと。
C.5.24	一覧管理情報は管理コンソール操作により手動登録、手動削除、一覧エクスポートができること。
C.5.25	一覧管理情報は検索から絞込表示が可能なこと。
C.5.26	以下のデバイス数の管理が可能なこと。使用認可ポリシー数が足りない場合は明記し、当センターと協議の上、適切なポリシー設定に協力すること。 総管理デバイス数：2,500 個人利用の機器に紐づけて制御したいデバイス数：1,400　対象個人数：500　※必ずしも個人利用機器と1対1ではない。 部署管理として制御したいデバイス数：600　部署数：85
C.5.27	一覧では下記が管理できること。 ※Windows、MacOS
C.5.27.1	デバイス名
C.5.27.2	ベンダーID
C.5.27.3	プロダクトID
C.5.27.4	シリアルNo
C.5.27.5	デバイス名
C.5.27.6	デバイスの所属するグループ情報
C.5.27.7	最終使用端末名
C.5.27.8	最終使用日時
C.5.27.9	最終使用ログオンユーザ名
C.5.27.10	所有者名
C.5.27.11	備考
C.6	省電力管理 ※Windows
C.6.1	管理対象のPCの省電力設定ができること。
C.6.2	管理対象のPCの省電力設定が一括変更できること。
C.6.3	指定時刻にPC電源の強制OFFができること。
C.7	メッセージ ※Windows
C.7.1	管理者から利用者に対してメッセージ送信できること。
C.7.2	メッセージ送信は、指定した任意のグループにできること。
C.7.3	メッセージ送信は、事前の送信予約ができること。
C.8	プログラム配布 ※Windows
C.8.1	プログラムを一括配布してPCにインストールができること。
C.8.2	特定のPCに対してプログラムの配布ができること。
C.8.3	プログラム配布に失敗したPCに対してのリトライ配信が一定期間できること。
C.8.4	プログラム配布が完了していないPCを検索できること。
C.8.5	配付したプログラムのインベントリ管理ができること。
C.8.6	利用者のPC操作で以下のことができること。
C.8.6.1	利用者のPC操作により、管理者より配布されたプログラムのダウンロードができること。
C.8.6.2	利用者はPC上のアイコンなどで、管理者よりプログラムが配布されていることが簡単に分かること。
C.8.6.3	管理者は配布するPCが選択できること。
C.8.7	WSUS（Windows Server Update Services）連携 ※Windows
C.8.7.1	指定したWindows更新プログラムを指定したPCへ適用可能なこと。
C.8.7.2	Windows更新プログラム適用は手動またはスケジュールで適用可能なこと。

項番	機能要件
C	IT資産管理システム
C.9	操作ログ管理 ※Windows、MacOS
C.9.1	PCでのファイルやアプリケーションの操作ログが速やかに収集できること。
C.9.2	操作ログデータは最新6カ月分を同一サーバに収集保存できること。古いログは定期的にCSV形式などの可読可能な状態で、別サーバに退避すること。保存場所や実行時間等の環境設定は当センターと協議の上、決定すること。
C.9.3	操作ログデータの検索は、ストレスを与えない速度であること。問題があった場合、当センターと協議を行うこと。
C.9.4	端末のレコードを削除した場合であっても、削除済みのレコードから当該端末を検索し、対象ログを参照できること。
C.9.5	サーバと接続できない環境等の操作ログは端末のローカルに保存されること。
C.9.6	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。
C.9.7	端末側の当日ログデータは、管理コンソールから端末を指定して取得操作が可能なこと。又は一定程度リアルタイムな反映があるならば、定期的にサーバへ送信する形等でもよい。定期的にサーバへ送信する形の場合はネットワーク・端末負荷が少ないこと、ログデータ取得間隔を提示すること。
C.9.8	退避したバックアップログに対して、現在のログと同様に管理コンソール上で検索が行えること。バックアップログの検索操作は特定端末やサーバ上の管理コンソールに限定されても良い。
C.9.9	操作ログデータに大量のシステムログ等が出力されるなどにより、操作ログデータが肥大化しないよう、対策設定が可能なこと。導入時には推奨される設定を提示すること。
C.9.10	操作ログは管理コンソールで閲覧している内容をCSVエクスポート可能なこと。
C.9.11	1日の操作ログが複数ページにわたって表示されている場合、全ページの操作ログを一括エクスポートできること。
C.9.12	以下の条件で操作ログが検索できること。 ※Windows、MacOS
C.9.12.1	コンピュータ名
C.9.12.2	ユーザ名
C.9.12.3	ログオン
C.9.12.4	ログオフ
C.9.12.5	電源ON
C.9.12.6	電源OFF
C.9.12.7	クリップボードログ(テキスト文字、画像イメージ) (Windows) ※画像イメージは容量を圧迫しない仕組みを有する事
C.9.12.8	コンピュータの操作開始、終了（キーボードマウス等を操作開始した時刻と操作が検知できなくなった時刻）。操作開始からの操作時間を記録できる形でもよい。
C.9.12.9	操作内容等
C.9.12.10	画面閲覧時のウインドータイトル
C.9.12.11	画面閲覧におけるファイル操作
C.9.12.12	操作ログデータの検索は同一画面でできることと。
C.9.12.13	アプリケーションの実行ファイル名
C.9.13	以下の内容でアプリケーションの操作ログを取得できること。 ※Windows、MacOS
C.9.13.1	インターネットブラウザ(Microsoft Edge,Google Chrome, Safari)により参照したURLが取得可能なこと。
C.9.13.2	インターネットブラウザ(Microsoft Edge,Google Chrome, Safari)により、ファイルのアップロードを行った場合はそのファイル名等が取得可能なこと。
C.9.13.3	インターネットブラウザ(Microsoft Edge,Google Chrome, Safari)により、ファイルのダウンロードを行った場合はそのファイル名等が取得可能なこと。
C.9.13.4	インターネットブラウザ(Microsoft Edge,Google Chrome, Safari)により、ログイン操作した際のログインIDが取得可能なこと。
C.9.13.5	インターネットブラウザ(Microsoft Edge,Google Chrome, Safari)により、WEBサイトへの書き込みを行った場合、書き込んだ内容が取得可能なこと。
C.9.14	以下の内容でネットワーク接続や通信に関するログを取得できること。 ※Windows
C.9.14.1	・Wi-Fi
C.9.14.2	・有線
C.9.14.3	ブラウザ、アプリケーションの通信ログにはIPアドレス以外に、TCP通信ポートも含めて記録可能なこと。なお、保存する内容をフィルタするなどにより、容量軽減可能なこと。
C.9.15	以下の内容でファイル操作ログを取得できること。 ※Windows、MacOS
C.9.15.1	操作対象ファイル名
C.9.15.2	コピー元とコピー先
C.9.15.3	移動元と移動先
C.9.15.4	名前変更前と名前変更後
C.9.15.5	作成と削除
C.9.15.6	デバイスへ書き込んだファイル名を取得できること。この際、書き込み先のデバイス名、デバイスシリアルNoなどデバイスを特定できる内容を合わせて記録できること。

項番	機能要件
C	IT資産管理システム
C.9.16	印刷ログ管理　※Windows
C.9.16.1	プリンターの印刷状況が記録管理できること。
C.9.16.2	各プリンターで印刷枚数を集計できること。
C.9.16.3	以下の内容で印刷ログを取得できること。　※Windows
C.9.16.3.1	印字出力した日時（年月日時分秒）
C.9.16.3.2	ログオンユーザ名
C.9.16.3.3	ホスト名またはIPアドレス
C.9.16.3.4	ファイル名
C.9.16.3.5	ページ数
C.9.16.3.6	出力したファイル名（拡張子含む）
C.9.16.3.7	印字出力したプリンタ名とIPアドレス
C.10	リモートコントロール ※Windows
C.10.1	PCのデスクトップ画面を共有し、画面の表示及びマウスの操作とキーボードにて文字の入力操作ができること。
C.10.2	管理者側とPC側の両方で操作を行うことを想定しているため、それぞれが操作できること。
C.10.3	管理者側からPC側への接続の際、PC側の承認操作が行われた上で、画面共有及び操作が可能となること。
C.10.4	管理者側の操作中に、PC側に管理者の操作を見せない設定ができること。
C.10.5	PCのログインID、パスワードを必要とせずにリモート操作できること。
C.10.6	PCのデスクトップ画面設定に合わせて、画面の拡大・縮小・解像度等を変更してリモート操作できること。
C.10.7	リモートコントロールを行うときにはネットワーク負荷が少ないこと。
C.10.8	リモートコントロールが行われた場合、リモートコントロール開始、終了がわかる形でログが記録されること。
C.10.9	管理者によるリモートコントロールは管理コンソールから対象PCを選択して、リモートコントロールが開始できること。
C.10.10	リモート操作において、開始から終了までのログをシステムログとして取得することができ、管理機からのリモート操作の内容がログから確認できること。
C.10.11	管理コンソールを操作するユーザー毎にリモートコントロールできるIT資産管理グループを設定出来ること。ただし、ログ確認や資産情報確認等は可能とする。
C.11	セキュリティ管理　※Windows
C.11.1	アラート設定と通知
C.11.1.1	アラート設定
C.11.1.1.1	簡易的な設定で利用者の操作を制限できること。
C.11.1.1.2	利用者の操作制限を行う時には、アラート表示ができること。
C.11.1.1.3	操作制限の適応範囲は、部署や端末PCごとに設定できること。
C.11.1.2	アプリケーション管理
C.11.1.2.1	利用を許可していないアプリケーションのインストールを検知できること。
C.11.1.2.2	利用禁止に指定したアプリケーションの利用を禁止できること。
C.11.1.2.3	利用禁止アプリケーションの起動の違反操作を行ったことを、リアルタイムに検知できること。
C.11.1.3	印刷管理
C.11.1.3.1	特定のプリンターからのみ印刷を許可する設定ができること。
C.11.1.3.2	部署や利用者毎に印刷を制限できること。
C.11.1.4	アラート表示
C.11.1.4.1	利用者が操作制限のある操作を行った時には、アラート表示できること。
C.11.1.4.2	利用者ごとのアラート設定ができること。
C.11.1.5	通信デバイス
C.11.1.5.1	指定した通信デバイスの使用を制限できること。
C.11.1.5.2	指定したネットワークやアクセスポイントへの接続だけを許可できること。
C.11.1.6	ファイル操作
C.11.1.6.1	未認可のデバイス接続時等にアラート検知できること
C.11.1.6.2	PrintScreenキーによる画面コピー時にアラート検知できること
C.11.2	以下のデバイスは利用制限ができること。 ※Windows
C.11.2.1	ネットワークカード
C.11.2.2	モデム
C.11.2.3	Bluetooth
C.11.2.4	赤外線
C.12	レポート ※Windows、MacOSに関するレポートにて必須
C.12.1	収集される資産データや操作ログから目的に応じたレポートが作成できること。
C.12.2	レポートは自動的に分析データが作成できること。

項番	機能要件
C	IT資産管理システム
C.12.3	以下のレポートが作成できること。
C.12.3.1	デバイスの利用状況
C.12.3.2	PCの利用状況
C.12.3.3	アプリケーションの利用状況
C.12.3.4	プリント出力の状況(Windows)
C.12.3.5	各種ログ解析(リスク診断等)
C.13	その他
C.13.1	管理者機能
C.13.1.1	管理者機能を有すること。
C.13.1.2	各管理者の操作履歴がログとして記録できること。
C.13.2	システム連携
C.13.2.1	利用者管理システムとの連携
C.13.2.1.1	利用者管理システムに登録された機器情報（PC名称、MACアドレスなど）のCSVファイルでの一括登録ができること。一括登録は定期的に自動実行することで連携を可能とすること。
C.13.2.1.2	CSVファイルの取り込みは手動でも実施できること。
C.13.2.1.3	プリンタなどの独自OSやスマートデバイスについてもCSVファイルで取り込み登録操作が可能なこと。
C.13.3	その他
C.13.3.1	サーバ接続に偏りが出ないようにサーバの負荷分散ができること。
C.13.3.2	ネットワークに対する負荷が少なく、ストレスなく実運用できること。
C.13.3.3	管理コンソールとサーバ間、エージェントとサーバ間の通信が暗号化されていること。
C.13.3.4	エージェントは異なるバージョンの存在を許す運用ができること。
C.13.3.5	サーバソフトは簡易・短時間にアップデートできるような仕組みになっていること。なお、データベースのサポート切れに伴い、データベースを変更が必要な場合等の特異な状況を除き、サーバソフトアップデートの都度、サーバソフトをアンインストールし再インストールするといった再セットアップが必要な手順は認めない。
C.13.3.6	バックアップ失敗や資産情報が更新できない等、サーバソフトのシステム異常発生時にメール等にて通知することができること。
C.13.3.7	エージェントをインストールする方式の場合、遠隔で各PCのエージェントを一括・個別アップデートできること。この際、アップデートはサイレントに行われ、原則PC側はアップデートに対する操作が不要であること。
C.13.3.8	エージェントをインストールする方式の場合、エージェントは簡易かつ短時間でインストール可能なこと。
C.13.3.9	エージェントは資産管理サーバ接続時に、エージェントのアップデートがあれば、エージェントを自動でアップデートする設定ができること。グループ毎に自動アップデートする、しないの設定が可能なこと。 アップデート操作を手動で行った時点でサーバと未接続であった端末が、次回サーバと接続された際にアップデートが適用される形や毎日定時にサーバと接続している端末が自動でアップデートされる形でも良いものとする。(Windows、MacOS)
C.13.3.10	IT資産管理システムがデバイスライセンス等で、登録数に上限がある場合、一定期間(1ヶ月または、3ヶ月程度の期間を想定)サーバとの接続がないデバイスを一括でライセンス対象外とすることが可能なこと。(Windows、MacOS、Linux)
C.13.3.11	IT資産管理システムにおいて、ライセンス数や登録数に上限がある場合、一定期間未接続でライセンス、登録対象外とする。対象外となったデバイスが再度サーバと通信可能となった場合、ライセンスが有効となること。(Windows、MacOS、Linux)
C.13.3.12	IT資産管理システムのサーバ環境のOSはセキュリティ更新プログラムなどの更新プログラムを適用可能なこと。なお、更新プログラム適用に際して、サポートへ事前確認が必要であることや適用にサービス停止等の手順が必要なことは問題ないが、サーバソフトをアンインストールし再インストールするといった再セットアップが必要な手順は認めない。

端末・ユーザー数・ライセンス数量計算表

・各表中の端末数は2023年7月～2025年1月の期間の最大値。
・HIS-VDIは廃止前提で、設置端末数はThinClientとして、Windows-HIS-PCに含めている
・事務PCは、Windows-T2-PCに含まれる（2025年1月にWindows-T2-thinclientから置き換わり）
・一般VDI分は、Windows-T2-thinclient として動作してきたが、次期200-230台の物理PCで検討中のため、調達時予定数として250を計上
・HIS調達PCはHISにて調達される資産管理ソフトにて管理するため、対象外

A. 登録機器数ベースの端末数（利用登録された端末数を日ごとに計算し、期間中の最大値を取得）

機器種別	機器種別-詳細	期間中 最大端末数	調達時 予定端末数	資産管理対象予定数			
				対象	ライセンス 対象数	対象	管理 対象数
サーバ ・仮想化基盤上＋物理	Windows-NCVC	102	105	o	105	o	105
	Linux/UNIX-NCVC	118	130	o	130	o	130
	Windows-HIS	212	220	-	0	-	0
	Linux/UNIX-HIS	23	25	-	0	-	0
クライアント（物理） ・NW機器除く	Windows-HIS-PC	1,930	2,000	-	0	-	0
	Windows-HIS-医療機器等付帯	441	445	o	445	o	445
	Windows-T2-PC	2,155	2,250	o	2250	o	2250
	Windows-T2-thinclient	350	250	o	250	o	250
	MacOS	577	600	o	600	o	600
	Linux/UNIX	194	220	o	220	o	220
	iOS	737	700	-	0	-	0
	Android	190	200	-	0	-	0
	iOS_FMC	180	200	-	0	-	0
	Android_FMC	1,100	1,100	-	0	-	0
	独自OS	2,987	3,000	-	0	-	0
クライアント（VDI）	T3-HIS	#計算外 2,100	0	-	0	-	0
	T2-事務・T2-一般	#計算外 700	0	-	0	-	0
	計	11296	11445		4000		4000

B. 過去90日に接続した端末のユニーク数（日ごとに過去90日の接続端末ユニーク数を計算し、期間中最大値を取得）

機器種別	機器種別-詳細	期間中 最大端末数	調達時 予定端末数	資産管理対象予定数			
				対象	ライセンス 対象数	対象	管理 対象数
サーバ ・仮想化基盤上＋物理	Windows	102	105	o	105	o	105
	Linux/UNIX	118	130	o	130	o	130
	Windows-HIS	212	220	-	0	-	0
	Linux/UNIX-HIS	23	25	-	0	-	0
クライアント（物理） ・NW機器除く	Windows-HIS-PC	1,689	1,700	-	0	-	0
	Windows-HIS-医療機器等付帯	316	345	o	345	o	345
	Windows-T2-PC	1,776	1,850	o	1850	o	1850
	Windows-T2-thinclient	295	250	o	250	o	250
	MacOS	488	450	o	450	o	450
	Linux/UNIX	138	150	o	150	o	150
	iOS	541	550	-	0	-	0
	Android	98	100	-	0	-	0
	iOS_FMC	180	200	-	0	-	0
	Android_FMC	1,100	1,100	-	0	-	0
	独自OS	1,876	2,000	-	0	-	0
クライアント（VDI）	T3-HIS	# 未計算	0	-	0	-	0
	T2-事務・T2-一般	# 未計算	0	-	0	-	0
	計	8952	9175		3280		3280

C.2025年3月21日時点のアカウント数

ユーザー種別	種別詳細	実数	調達時 予定数	ユーザー予定数	
				対象	ライセンス 対象数
職員	有効アカウント数	2,237		o	0
	2025年度継続アカウント数	1,771	1,800	o	1800
	2025年度増員見込み	100	150	o	150
一時在籍者	有効アカウント数	139		-	0
	過去３ヶ月週1回以上来訪人数	27	50	o	50
外部関係者(委託、システムベンダ等)	有効アカウント数	297		-	0
	委託（当センター常駐者）	263	300	o	300
	システムベンダ（エージェントインストール対象外）	34	0	-	0
共有アカウント（目的別アカウント）	有効アカウント数	3251		-	0
	特定個人に紐づくアカウント	0	0	-	0
					2300