別紙２

ハードウェア・ソフトウェア機能要件一覧

（１）モバイル端末

筐体形式	モバイルノート型
ハードウェアメーカ	久留米市が認めるメーカー（ショップブランド不可）
台数	100台
インストールOS	Windows11 Pro 64bit
CPU	Corei5　13世代以降
メモリ	16GB
ストレージ容量	SSD　128GB以上
ディスプレイサイズ	12インチ以上14インチ以下
解像度	1920×1080ドット以上、1677万色
外部ディスプレイ出力	USB（type-C)×1、HDMI端子×1
無線LAN	Wi-Fi 6E（2.4GBPS）対応、IEEE802.11a/b/g/n/ac/ax準拠、MU-MIMO対応
WWAN	LTE（4G）対応
対応SIMサイズ	下記モバイル通信サービスにおけるSIMサイズに対応すること
USB	Type-A：USB3.2（Gen1）以上×2、Type-C：USB3.2（Gen2）以上× 2
その他インターフェイス	ヘッドホン端子× 1 があること
マウス	２ボタン以上の光学式ホイールマウス（サードパーティー製も可とする）
Webカメラ	有効画素数92万画素以上
音源機能	Windows11 Pro 64bit 版対応で、マルチメディアソフト等が支障なく使用できるもの
スピーカー	上記音源機能で使用可能な内蔵型
本体重量	1.3kg以下
バッテリ	６時間以上の駆動時間があること（バッテリーの種類、充電時間は問わない）。 バッテリーの膨張、充電されない（アダプタを抜くと電源が落ちる）等の不具合の場合は、無償で交換対応（オンサイト）すること。 （バッテリーの寿命、通常使用外での故障は除く）
アプリケーション	・Microsoft365　Apps for enterprise ・Web会議用アプリケーション（Zoom、Microsoft Teams、Cisco Webex Meeting） ※いずれのアプリケーションも当市保有のライセンスを使用するため、アプリケーションのインストール及び必要に応じて当該ライセンスの設定のみを行うこと。
設定・納品	全台数共にWindows初期設定、必要アプリケーションのインストール設定を行い納品すること。（ドメイン参加は不要） 設定方法については問わないが、万一の初期化、再設定に備え設定後のバックアップイメージを作成すること。 クローニングを行う場合はOS他ライセンスの扱いに留意し、必要なライセンスを準備すること。
機器の返却	契約期間終了後は受注者が機器を回収すること、回収に要する費用は受注者の負担とする。

（２）モバイル 通信サービス

対応通信サービス網	インターネット接続（ベストエフォート型）4G/5G対応
回線種	データSIM
対応SIMサイズ	USIMカード　標準SIM/Micro SIM/nano SIM
データSIM容量	10GB以上
サポート	インターネット回線障害時の調査 使用デバイス紛失時のUSIMカードの利用停止 当月使用データ量の確認
利用料金	月額・定額制

（３）IT運用管理サービス

資産管理	資産情報収集	収集可能な資産項目	資産情報の自動収集	・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。 ・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 WordなどのMicrosoft Office製品、Windowsストアアプリ、ウイルス対策ソフトウェア、その他のアプリケーション、Windows更新プログラム適用状況、Windows10以降OSのOSサービスモデルの設定状態を含む）を、自動的に収集可できること。 ・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。
			任意項目（50個）	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。任意項目として設定できる項目数は50程度あること。
			資産情報の検索 / 検索条件保存	・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WindowsOSのバージョン、ビルド番号、サービスパック、空き容量などから、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。 ・キーワードを指定する際は、AND,OR,NOT検索が可能で、空白を挟むことで複数のキーワードを指定できること。 ・検索条件に任意の名称をつけ保存でき、呼び出せること。
			CSVファイル入力（インポート）	CSV形式のファイルでインポートしたデータをハードウェア資産情報として登録できること。
			CSVファイル出力（エクスポート）	収集したハードウェア資産情報をCSV形式のファイルで出力できること。
			BitLockerによるドライブ暗号化情報を収集 / 確認	BitLockerによるハードディスクの暗号化状態を収集し、ハードウェア一覧で確認できること。
		アプリケーション一覧	ウイルス対策ソフトウェアインストール状況	【Windows端末】 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を収集する機能を有すること。収集できる内容としては、以下の通りとする。 また、クライアントコンピューターごとにアプリケーション状況を把握できること。 収集対象：ウイルス対策ソフトウェアインストール状況・アプリケーションインストール状況・OSインストール状況・Officeインストール状況・Windowsストアアプリインストール状況・Windows更新プログラムインストール状況
			アプリケーションインストール状況	
			OSインストール状況	
			Officeインストール状況	
			Windowsストアアプリインストール状況	
			Windows更新プログラムインストール状況	
			CSVファイル出力（エクスポート）	収集したアプリケーション資産情報をCSV形式のファイルで出力できること。
			ソフトウェア配布	・指定したクライアントコンピューターに対して、任意のプログラムを配布し、自動的にプログラムのインストールおよびアンインストールを行う機能を有すること。 ・配布したソフトウェアの配布状況およびインストール状況を確認することができること。配布したソフトウェアのインストール / アンインストールが失敗した場合は、失敗したクライアントコンピューターを指定して再実行が行えること。
			配布したソフトウェアのインストール状況確認	

		ソフトウェア配布・インストール	キャッシュ配布	・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る場合、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。 ・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。
			実行ファイル/Windows更新プログラム配布	・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を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。 ・配布したWindows更新プログラムが適用されていないクライアントコンピューターを検出し、一覧化できること。
			ダッシュボード上での資産情報閲覧	・収集されたクライアントコンピューターのOSバージョンやウイルス対策ソフトウェアのインストール状況などの資産情報を集計し、管理コンソール内のダッシュボード上にて円グラフで視覚的に表示する機能を有すること。 集計対象：資産情報未アップロード端末の割合、未起動 / 再起動端末の割合、本ソフトウェア最新バージョンのインストール状況、Microsoft Defenderの有効状況、ウイルス対策ソフトウェアのインストール状況、Windows OSバージョンごとのインストール状況、Windows 大型アップデートの適用状況、Microsoft Edge / Google Chrome /の最新または指定のバージョンのインストール状況 ・ダッシュボードに表示 / 非表示する資産情報を設定できること。 ・ダッシュボードに表示する資産情報の集計条件を設定できること。 ・集計結果をクリックすると、端末情報を一覧表示できること。
ログ管理	ログ収集	収集可能なログ	ログ収集全体	クライアントコンピューターに対して行われた操作、ログオン・ログオフの日時、ファイル操作、Webへのアクセスおよび書き込み・アップロード・ダウンロード、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等をログとして記録する機能を有すること。
			-起動・終了ログ	・クライアントコンピューターのログオン・ログオフ・電源ON・電源OFF・操作開始・操作終了の日時をログとして記録できること。 ・一定時間キーボードやマウスの操作が行われなかった場合、その状態をログとし記録できること。
			-アプリケーションログ	クライアントコンピューター上で実行されたソフトウェアについて、起動時刻、終了時刻などをログとして記録できること。
			-ファイル操作ログ	クライアントコンピューターが行ったファイル操作(作成、コピー、ファイル名変更、移動、上書き、削除)をログとして記録できること。
			-プリントログ	クライアントコンピューター上で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、ファイルパスなどをログとして記録できること。
			-Webアクセスログ	・Webサイトの閲覧が行われた内容について、ウインドウタイトル、URLをログとして記録できること。尚、以下のブラウザに対応していること。 Google Chrome、Safari、Microsoft Edge（EdgeHTML版）、Microsoft Edge（Chromium版）、Firefox、Internet Explorer ・WebダウンロードおよびWebサイトへの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、書き込み内容などをログとして記録できること。尚、以下のブラウザに対応していること。 Google Chrome、Microsoft Edge（Chromium版）
			-Webファイルアップロードログ	クライアントコンピューター上でMicrosoft Edge（Chromium版）、Google Chormeを使って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。
			-ドライブ追加・削除ログ	クライアントコンピューター上で、USBメモリやCD/DVD-ROMなどの記憶媒体を利用した内容をログとして記録できること。 シリアルが取得可能な記憶媒体については、記憶媒体のシリアル情報も含むこと。
			-Dropboxログ	クライアントコンピューターからDropboxへのアップロードおよびダウンロード操作に対して、ログを収集できること。 また、アップロード元およびダウンロード先ファイルのフルパスを記録できること。
			-Googleドライブログ	クライアントコンピューターからGoogleドライブへのアップロードおよびダウンロード操作に対して、ログを収集できること。 また、アップロード元およびダウンロード先ファイルのフルパスを記録できること。
	ダッシュボード上でのアラート情報閲覧			・収集されたアラート情報を集計し、管理コンソール内のダッシュボードにおいてアラートの発生件数を視覚的に表示する機能を有すること。 ・アラートの発生件数をクリックすると、端末情報を一覧表示できること。
セキュリティ管理	注意表示通知	通知方法	端末機の画面にメッセージを表示（ポップアップ通知）	・事前定義されたルールに反した操作が行われた際、その操作を行った利用者のクライアントコンピューターのデスクトップ上にリアルタイムで、ポップアップ形式による通知ができること。 ・ルールに反した操作をしたクライアントコンピューターの利用者に注意を促すため、メッセージの内容はルール違反の操作ごとに設定できること。
			キーワードごとにアラート通知のON/OFFを設定	特定のキーワードを含むWebサイト閲覧やアプリケーション実行などの操作を行うと自動で表示されるポップアップについて、指定するキーワードごとにポップアップの通知を行うか指定できること。
	端末アラート設定項目	資産アラート	端末未起動期間設定	クライアントコンピューターが指定の日数以上起動していない場合やログの収集ができない場合に検知できること。
			アプリケーション実行（デスクトップアプリ）	指定したアプリケーションの実行を検知および禁止できること。
		その他アラート	Webアップロード	・クライアントコンピューター上での、Webサイトの閲覧やWebサイトからのファイルダウンロード/アップロード操作を検知および禁止できること。 ・Webサイトの閲覧やWebサイトからのファイルアップロードを禁止する際は、キーワードやURLで禁止サイトを設定できること。 ・特定のURLからのダウンロードを禁止から除外するよう、設定できること。
			Webダウンロード	
			Web閲覧	
	紛失端末制御		紛失端末制御	・クライアントコンピューターを紛失した際などに、インターネットを経由して遠隔から、クライアントコンピューターの画面をロックし操作の制御を行うことや、あらかじめ登録したクライアントコンピューター上の指定フォルダの削除を行う機能を有すること。また、GPSやWi-Fi、IPアドレス、携帯電話基地局からの取得情報を用いて、クライアントコンピューターの位置情報をインターネット経由で確認できること。 ・インターネットを経由して、クライアントコンピューターの制御状態（画面ロック）を解除できること。さらに、オフラインであっても、管理者が発行した解除コードを、制御中のクライアントコンピューター上で入力することで、制御状態を解除できること。
	セキュリティ強化		ワンタイムパスワードを利用した二要素認証	ログイン時に、契約ID・ユーザー名・パスワードでの認証に加え、ワンタイムパスワードなどによる多要素認証に対応していること。
デバイス管理	デバイス管理	登録・管理・棚卸	USBデバイスの台帳登録	・USBデバイスをクライアントコンピューターもしくは管理者のクライアントコンピューターに挿入した際、利用したUSBデバイスのシリアルナンバー、ベンダーIDを自動で収集し、管理台帳を作成できること。 ・利用者や所属部署、管理番号などを任意で入力できること。 ・収集した情報にもとに、指定したUSBデバイスを使用許可 / 不許可を設定できること。 ・使用許可 / 不許可の設定は、ネットワーク全体および指定した部署のみ利用可など柔軟な設定が行えること。
			USBデバイス台帳管理	
		使用制限	デバイス使用制限	USBデバイス台帳に登録されたデバイス情報を基に、そのUSBデバイスの使用許可/不許可などを設定できること。
			-部署別使用制限	・許可したUSBデバイスのみを使用可能としそれ以外の使用を禁止できるような運用が可能であること。 ・個々のUSBデバイスに使用可能/読み取り専用/使用不可能を設定できること。
			-デバイス種別制御	デバイス種別ごとに、一括で使用可能/読み取り専用/使用不可能の設定ができること。 設定ができるデバイスの種類は以下の通りとする。 デバイス種別：USBメモリ、USBハードディスク、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
		デバイスアラート設定	記憶媒体使用	USBデバイスやCD/DVD/Blu-rayドライブなどの記憶媒体を、クライアントコンピューターに接続したり書き込みを行った場合に検知および禁止ができること。
			記憶媒体書き込み	
レポート	PC活用状況分析レポート		レポート閲覧（PC操作率、PC操作時間）	・業務時間に対してクライアントコンピューターの操作時間の割合を集計した操作率、およびクライアントコンピューターの操作時間の集計結果を、管理コンソール内のダッシュボード上にて円グラフ、棒グラフ、折れ線グラフで視覚的に表示して一覧化できること。 ・クライアントコンピューターの操作率が予め設定したしきい値以下になると、グラフの表示色が正常・注意・警告の3段階で切り替わること。
			レポート出力（PC操作率、PC操作時間）	・業務時間に対してクライアントコンピューターの操作時間の割合を集計した操作率、およびクライアントコンピューターの操作時間の集計結果のレポートをCSV形式のファイル（ZIP圧縮）としてダウンロードできること。 ・本機能を有効にする前の期間についても、エクスポートした操作ログのレポートをインポートすることで、さかのぼってレポートを出力できること。
その他	セキュリティ			サービスを提供する施設等は、日本国内に所在地を置き、必要なセキュリティ及び災害対策等の措置がとられていること。また、本件サーバに保存したデータが日本国の法律で保護されること。
	教育支援			管理者向けの基本操作教育を実施すること。

（４）リモートアクセスサービス

運用方法	情報政策課等で貸し出しを行うモバイル端末（以下「インターネット側端末」という。）から庁内LGWAN ネットワークにある各職員へ配布された自席の端末（以下「LGWAN側端末」という。）へリモート接続する。

数量	同時にリモート接続する対象人数は100名とする。
サービス提供形式	LGWAN-ASPで提供されるサービスであること。
対応OS	Windowsに対応したデスクトップアプリで利用できること。
操作方式	画面転送によりインターネット側端末からLGWAN側端末をリモート操作する方式であること。
最大フレームレート	設定により最大30フレーム/秒の画像転送が可能であること。
暗号化	暗号化（SSL/TLS、AES256）により通信を保護していること。
多要素認証	多要素認証に対応していること
管理画面	管理画面が LGWAN・インターネット側双方からアクセスできること。また、管理画面へのログイン機能（ID・パスワード）があること。
ログ管理	サービスにおいて利用者の接続状況が記録され、管理者がリモートアクセスした端末のアクセス記録を容易に確認できる画面やリスト等があること。
端末制限	ユーザーIDごとに、接続が可能なLGWAN側端末を制限できること。
その他機能等	LGWAN側とインターネット側の直接の通信を遮断でき、インターネット側端末に画面転送で接続したデータが保存されない仕組みとすること。
	画像転送により接続したデータ等をインターネット側端末にコピーできないようにすること。
	画面撮影抑止機能 (電子透かし) の機能を有すること。
	リモートでの接続中、LGWAN側端末の画面非表示及びキーボード・マウスロックの機能を有すること。
	サービスの運用支援及びサポートを含み、本市担当者からのサービスに関する問い合わせ(電話等による)に対応すること。（原則、平日9時～17時）
	USB等の差し込み不要で利用できること。
	インターネット側端末又はLGWAN側端末において、ユーザー登録時又は利用時にMACアドレス又はIPアドレス等の識別子を入力することなく利用できること。
	サービスを提供する施設等は、日本国内に所在地を置き、必要なセキュリティ及び災害対策等の措置がとられていること。また、本件サーバに保存したデータが日本国の法律で保護されること。