端末管理ソフトウェア機能仕様書

○基本要件

1. 本要求仕様項目については、OS 動作中に常駐するソフトウェアの動作上、複数メーカーの製品を組み合わせることは、コンピューター自体が不安定になる可能性や、グルーピング情報及びリストの情報に不整合が発生する可能性があるため、メーカーが、一つの製品として提供しているものを選定すること。
2. 調達するソフトウェア製品の仕様及び機能については、安定稼働の観点から、本調達の仕様書公告時点において開発が完了しており、導入実績があるもの以外は一切認めないものとする。
3. 保守契約期間中はマイナー/メジャー/後継品を問わず、ミドルウェア含め常に最新版のプログラム提供を行うこと。またサポート体制として ISO/IEC20000 の認定を受けているメーカーの製品であること。
4. 端末にインストールするアプリケーションは、すべての機能が一つのインストーラーで提供されること。
5. 各クライアントコンピューターの利用状況を把握するため、クライアントコンピューターの操作画面を管理端末で一覧表示する機能を有すること。

○IT 資産管理

1. 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やソフトウェアに関するインストール状況等（Microsoft Office/ JUST Office 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、Windows11 以降 OS の OS サービスモデルの設定状態を含む）を、資産情報として自動的に収集でき、一覧で表示できること。
2. 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および数値の範囲を指定して検索が可能であること。
3. 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。
4. 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。
5. 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。

○ログ取得

1. 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、実行されたソフトウェアについての起動時刻・操作時間、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（テキスト・画像)、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を記録する機能を有すること。
2. Microsoft 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ログとして記録する機能を有すること。
3. 収集されたファイル操作ログから、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する機能を有すること。また、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。
4. バックアップされたログについても、リストアすることなくサーバー上に保存されている直近のログと同様に管理コンソール上で検索、閲覧が行えること。

5. 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。

○制限・制御・アラート管理

1. 各クライアントコンピューターに対して、指定したアプリケーション起動、Windows ストア アプリ起動、指定アプリケーションの名前変更、インストールの実行、Windows システム構成変更、レジストリ変更、Windows ストアの実行、Windows ストアアプリの自動更新などを禁止できること。
2. 起動禁止を除外できる時間設定が、特定のアプリケーションごとに可能である機能を有すること。

○デバイス管理

1. USB デバイスをシリアルナンバーごとに管理する機能を有すること。保有 USB デバイスはシステムで台帳管理し、一覧で表示できること。なお、台帳への登録は 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。
2. USB デバイスの一覧を元に、指定した USB デバイスに対して使用許可／不許可および書き込み禁止の、使用制限を設定できること。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。
3. USB メモリがクライアントコンピューターに装着された日時を利用して、所定期間以上使用実績のない USB メモリを、紛失の可能性があると自動判定し、最後の使用者または管理者に対して、USB メモリの所在確認（クライアントコンピューターへの装着）を促す通知を行う機能を有すること。

○リモート操作

1. 特定のクライアントコンピューターに対して、ネットワーク経由で、リモート操作が行える機能を有すること。なお、管理機操作の際のログオンパスワードは、変更できること。
2. 遠隔操作によってクライアントコンピューターのメンテナンスをする際に、遠隔操作を実行するクライアントコンピューターで行われた操作内容に応じて遠隔操作中の通信量を自動でコントロールする機能を有すること。
3. 特定及び複数のクライアントコンピューターに対して、ネットワーク経由でキー及びマウス操作をリモートで行える機能を有すること。操作時はクライアントコンピューターの操作をロックできること。操作する対象となる複数のクライアントコンピューター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。また，複数クライアントコンピューターの一斉操作と単体操作を切り替えて利用できること。

【参考品】「SKYSEA Client View」または同等以上の機能を有する製品

以上