項番	分類	要件	必須要件	必要要件
1	資産管理機能	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。	◎	
2	資産管理機能	各クライアントコンピューターのOS情報（OSバージョン、ビルド番号、適用済み更新プログラム）やソフトウェアインストール状況（アプリケーション名、バージョン）等を自動的に収集可能であること。	◎	
3	資産管理機能	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。	◎	
4	資産管理機能	クライアントコンピューターが通信している、本ソフトウェアのマスターサーバーを一覧で確認できること。	◎	
5	資産管理機能	資産情報の検索の際は、インベントリ情報やWindowsOSのバージョンなど複数条件を指定した検索が可能であること。	◎	

項番	分類	要件	必須要件	必要要件
6	資産管理機能	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		◎
7	資産管理機能	コンピューターおよびネットワーク機器から管理機までのネットワーク経路情報の確認が行えること。		◎
8	資産管理機能	端末のIPアドレス・セグメント、現在接続している無線LANのアクセスポイント（SSID、BSSID）、無線LANの信号強度等の取得ができること。		◎
9	資産管理機能	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。	◎	
10	資産管理機能	セグメントまたはアクセスポイント毎のグループからキャッシュ端末を選定し、ソフトウェア等の分散配布ができること。	◎	
11	資産管理機能	キャッシュ端末からソフトウェアを配布する際、通信帯域を制限できること。	◎	

項番	分類	要件	必須要件	必要要件
12	資産管理機能	ソフトウェア配布時など、キャッシュ端末の負荷を抑えることができること。	◎	
13	証跡管理機能	クライアントコンピュータで行われた操作で、以下の項目を取得し記録する機能を有すること。 ・操作時刻 ・ログオン、ログオフ ・操作したソフトウェア（プロセスID、ハッシュ値、ファイルパス） ・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、ファイルのフルパス） ・Webアクセス、アップロード ・クリップボード操作 ・USBメモリなどの外部記憶媒体（デバイスインスタンスID） ・Bluetooth機器（デバイスインスタンスID）	◎	
14	証跡管理機能	検索結果に対して、任意のログを選び、マーキングできること。		◎
15	証跡管理機能	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。		◎
16	証跡管理機能	リモート操作した場合のログ証跡を考慮して、接続元の管理者が行った操作と接続先の利用者が行った操作を区別することができるログを記録できること。	◎	

項番	分類	要件	必須要件	必要要件
17	証跡管理機能	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、メール送信など）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。	◎	
18	証跡管理機能	クライアントコンピューターの操作ログの検索を行う場合に、検索対象として複数のデータサーバーが存在している場合でも、データサーバーを一度にまとめて選択できる機能を有すること。また、操作ログをリアルタイムに収集し分析可能なこと。	◎	
19	証跡管理機能	複数のバックアップログに対しても、現在のログと同様に検索が行えること。	◎	
20	証跡管理機能	バックアップログの検索時に、部署・検索グループおよびクライアントコンピューターごとに絞り込めること。また、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の選択も可能であること。	◎	
21	証跡管理機能	クライアントコンピューターから収集したログデータをバックアップし、またバックアップデータを管理コンソール上で閲覧またはデータの保全ができること。	◎	
22	証跡管理機能	収集したログを一定期間ごとに自動でバックアップする機能を有すること。		◎
23	証跡管理機能	圧縮してバックアップした複数のログデータに対して、同時に検索できること。	◎	

項番	分類	要件	必須要件	必要要件
24	証跡管理機能	データサーバーのハードウェアの障害等に備えてバックアップ後から障害発生までのログを保全するため、冗長化等の対応によりログの保全ができること。	◎	
25	証跡管理機能	端末側で保存されているログデータが改変されないように、保護されていること。	◎	
26	アラート管理機能	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、その操作ログを管理者が把握できること。	◎	
27	アラート管理機能	本ソフトウェアによる、サーバーとクライアントコンピューター間および、クライアントコンピューター間の通信は、証明書または暗号キーなどにより認証が行われること。	◎	
28	アラート管理機能	同じ証明書または暗号キーを持っていない端末からの、本ソフトウェアへの通信を制限すること。	◎	
29	アラート管理機能	不正な通信が行われた場合、管理者が把握できること。	◎	
30	デバイス管理機能	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。	◎	

項番	分類	要件	必須要件	必要要件
31	デバイス管理機能	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。	◎	
32	デバイス管理機能	USBメモリ等外部記憶媒体は、許可したデバイスのみ接続可能なこと。また、使用許可は、ユーザ、クライアントコンピュータ、デバイスインスタンスID毎に設定が可能なこと。	◎	
33	デバイス管理機能	USBデバイス毎にユーザーまたは端末単位で許可指定が可能なこと。	◎	
34	リモート操作機能	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、リモート操作は許可したユーザ、端末からのみ行えるよう管理できること。	◎	
35	リモート操作機能	リモート操作は、複数のクライアントコンピュータに対して同時に行えること。	◎	
36	リモート操作機能	リモート操作されているクライアントコンピューターのデスクトップに、操作中であることを通知するポップアップを表示する設定ができること。	◎	
37	リモート操作機能	フリーウェアVNCの使用を禁止している環境であっても、リモート操作が行えること。	◎	

項番	分類	要件	必須要件	必要要件
38	リモート操作機能	リモート操作を円滑に行うための、技術的考慮がされていること。	◎	
39	リモート操作機能	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設定が可能なこと。	◎	
40	リモート操作機能	操作画面を隠しながらの遠隔操作中は、操作側の画面に隠しながら操作中である旨を通知すること。	◎	
41	セキュリティ管理機能	Windows更新プログラムの情報を一覧で取得でき、取得した一覧から必要な更新プログラムを、指定した端末または全台に配布・適用することができること。		◎
42	セキュリティ管理機能	クライアントコンピューターを管理する管理機コンピューターがインターネットに接続できない場合、インターネット接続が可能なクライアントコンピューターにて、ダウンロードした更新プログラムを管理機から指定した端末に配布・適用ができること。	◎	
43	セキュリティ管理機能	管理下の端末に対して、未適用のWindows更新プログラムを一覧で取得が可能であること。	◎	
44	セキュリティ管理機能	未適用のクライアントコンピューターの絞込により、更新プログラムの再配布・再適用ができること。	◎	

項番	分類	要件	必須要件	必要要件
45	不許可端末遮断	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（IPアドレス、MACアドレス、ゲートウェイMACアドレス、ゲートウェイIPアドレス）を収集できること。		◎
46	不許可端末遮断	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。また、接続されたことを管理機のデスクトップにポップアップ表示および、メールで通知できること。		◎
47	不許可端末遮断	あらかじめ登録されていないIPアドレスが付与されたネットワーク機器が接続された場合、該当のネットワーク機器を自動でネットワークから遮断できること。		◎
48	セキュリティ対策強化機能	起動元アプリケーションのファイルパス、ハッシュ値、およびプロセスIDを記録する機能を有すること。	◎	
49	セキュリティ対策強化機能	ZIP形式に圧縮されたファイル内に格納されている各ファイルのファイル名を収集できること。	◎	
50	セキュリティ対策強化機能	コンピューターウイルスに感染した場合等に、ネットワークから隔離することができること。また、本ソフトウェアによる通信は維持できること。	◎	
51	セキュリティ対策強化機能	クライアントコンピューターにインストールされているMicrosoft Office製品の更新（アップデート）や、展開（インストール）を設定する機能を有すること。	◎	

項番	分類	要件	必須要件	必要要件
52	セキュリティ対策強化機能	USBメモリ等の外部記憶媒体へファイルを書き込む際に、ファイル拡張子に依存せず自動的に暗号化を行うことが可能なこと。	◎	
53	セキュリティ対策強化機能	暗号化されたファイルを管理者が庁内と定めた領域に戻したときに、自動的に復号化されること。また、復号化に際し、パスワードの入力が不要なこと。		◎
54	セキュリティ対策強化機能	AES暗号256bit以上の暗号強度が利用できること。	◎	
55	勤怠管理・稼働管理機能	ユーザー別・端末別に稼働状況を指定した期間において一覧化することができること。また、表示した一覧をエクスポートすることができること。	◎	
56	勤怠管理・稼働管理機能	PC操作時間の割合をユーザ毎・部局毎に集計・分析することができること。	◎	
57	勤怠管理・稼働管理機能	出退勤時刻とPC使用時間を確認し一覧としてエクスポートすることができること。	◎	
58	その他機能	それぞれの機能がどのような機能であるのか、管理コンソールやマニュアルで表示・説明できること。	◎	

項番	分類	要件	必須要件	必要要件
59	その他機能	管理機は複数台の端末から同時に起動することが前提の設計となっていること。	◎	
60	その他機能	管理機能について、機能に応じてアクセスできるアカウントを限定することができること。	◎	
61	運用保守・サポートサービス	電話、E-Mail、Fax・現地対応などによるメーカーサポートが利用できること。	◎	
62	運用保守・サポートサービス	テクニカルサポート（インストールや設定）、オペレーションサポート（操作方法）、トラブルサポート（障害）のいずれについても利用可能であること。	◎	
63	運用保守・サポートサービス	サポート受付日の翌営業日までに回答が行えること。	◎	
64	運用保守・サポートサービス	国際標準規格 ISO/IEC15408 EAL3又は同等の第三者認証を取得したソフトウェアであること。	◎	
65	運用保守・サポートサービス	保守契約期間中は最新版のソフトウェアが利用できること	◎	

項番	分類	要件	必須要件	必要要件
66	運用保守・サポートサービス	サポート情報や技術情報等のメーカーから提供される情報については、すべて日本語であること。	◎	
67	運用保守・サポートサービス	各製品の初期構築はメーカーが現地で実施すること。また構築のための会議等に出席が出来ること。	◎	
68	運用保守・サポートサービス	各製品の利活用促進のため、利用者向けの操作講習会をメーカーが現地で実施すること。	◎	
69	運用保守・サポートサービス	ソフトウェアの開発・保守サポートはすべて日本国内で行われていること。	◎	
70	運用保守・サポートサービス	サポート情報や技術情報等のメーカーから提供される情報については、すべて日本語であること。	◎	