別紙１　医療情報システム要求仕様書

							要求仕様	必須
24							セキュリティシステム	
24	1						基本要件及び機能要件	
24	1	1					基本要件	
24	1	1	1				導入システムは令和7年5月1日の本稼働より運用できるものとすること。	○
24	1	1	2				クライアント運用管理ソフトウェアの仕様及び機能については、OS動作中に常に動作する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（フリーソフトウェア及びシェアウェアソフトでの実現は不可とする）。また、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。	○
24	1	1	3				ソフトウェアについては、別途に記載された契約期間中に有効な保守契約をメーカーとの間で結んでおき、電話、E-Mail、Faxによる問い合わせサポート、メーカーで提供するユーザー向け情報提供Webサイトの利用、最新版へのソフトウェアバージョンアップが行えるようにしておくこと。保守契約中の電話による問い合わせサポートはフリーダイヤルが望ましい。	○
24	1	1	4				同等品以上の製品で参加を希望するものは、令和※年※月※日（※）※時までに、本団体が指定する各要求機能に対する実現方法を図解入りのカタログで提出し、仕様機能が満たされていることについて本団体の承認を得ること。その際には、メーカー社印入りの機能証明書を提出すること。技術審査の結果、仕様を満たしていないと本部が判断した場合は、仕様を満たす他の製品で再提出を行い、本団体の承認を得た場合のみ入札に参加することができる。	○
24	1	2					機能要件	
24	1	2	1				資産管理	
24	1	2	1	1	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を、資産情報として自動的に収集できること。	○
24	1	2	1	1	2		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。	○
24	1	2	1	1	3		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。	○
24	1	2	1	1	4		クライアントコンピューターが通信している、本システムのマスターサーバーを一覧で確認できること。	○
24	1	2	1	1	5		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。	○
24	1	2	1	1	6		検索の際には、本システム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。	○

							要求仕様	必須
24	1	2	1	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を指定できること。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。	○
24	1	2	1	3			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。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。	○
24	1	2	1	4			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。	○
24	1	2	2				ソフトウェア配布	
24	1	2	2	1			指定したクライアントコンピューターおよび検索グループに対して、複数の任意のプログラムを配布し、自動的にプログラムの実行および解除を行う機能を有すること。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。また、配布時に利用する帯域を制限できること。	○
24	1	2	2	2			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。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	○
24	1	2	2	3			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。	○
24	1	2	2	4	1		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。	○
24	1	2	2	4	2		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。	○
24	1	2	2	4	3		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。	○
24	1	2	3				アラート設定	
24	1	2	3	1			事前定義されたルールに反した際に，通知する機能及び操作を禁止する機能を有すること。また，設定はグループごと，コンピューターごと，利用者ごとに行えること。	○
24	1	2	3	2			特定の種別のBluetoothデバイスに対する接続が行われた場合、もしくは、特定のサーバーおよびセグメントへの、事前定義されたルールに反する通信が行われた場合、アラートとして通知できること。後者については、通信元のIPアドレスを取得できること。	○

別紙１　医療情報システム要求仕様書

							要求仕様	必須
24	1	2	3	3			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、その操作ログはアラートログとして、ログ閲覧画面および検索画面にて、アラート項目の優先順位に応じて3段階以上に色分けして表示できること。端末一覧画面では、発生している一番優先順位の高いアラート項目の色で、クライアントコンピューターを色付けして表示できること。アラート優先順位を用いて、クライアントコンピューターやログを絞り込んで表示できること。アラートの優先順位は、アラート項目ごとに設定できること。	○
24	1	2	3	4			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送られるメール・ポップアップについて、指定するキーワードごとにメールやポップアップの通知を行うか指定できること。	○
24	1	2	3	5			ルールの定義の際には、操作ログのログ種別を基準に、特定の曜日や時間帯、および特定時間内の操作回数などの複数条件を組み合わせて定義することもできること。	○
24	1	2	3	6			アラート発生時における端末操作画面を、マウスカーソルの位置が強調された形式で表示し、不正操作及び誤操作発生時に早期の問題把握ができる機能を有すること。	○
24	1	2	3	7			指定した定刻時刻、または申請した残業終了時刻が近づいたり業務時間外になると、クライアントコンピューター上にメッセージを表示する機能を有すること。メッセージは、毎週決まった曜日もしくは特定の日を定時退社日として設定できること。メッセージには残業時間や理由を申告でき、申告時間を超えた場合はネットワークからの遮断ができること。また、オフライン状態であっても画面のロックが行えること。システム管理者が事前に設定した解除コードを入力することにより、ネットワーク遮断、および画面のロックが解除できること。申告された残業時間および実残業時間を集計し、当日の残業時間や、当月のおおよその累計残業時間を一覧で表示できること。	○
24	1	2	3	8			本システムによる、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、電子証明書による認証を行うこと。同じ電子証明書を持っていない端末からの、本システムへの通信を制限すること。不正な通信が行われた場合、管理者に対してメールで通知できること。	○
24	1	2	3	9			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。	○
24	1	2	3	10			本システムの通信を行うため、Windowsファイアウォールの通信許可設定について、部署ごとに許可するプロファイルの範囲を指定できること。クライアントコンピューターのネットワークカードごとのネットワークカテゴリ情報を、一覧で確認できること。	○

別紙１　医療情報システム要求仕様書

							要求仕様	必須
24	1	2	3	11			総務省の地方公共団体における情報セキュリティガイドラインに準拠したフリーメール、ネットワークストレージサイトなどの情報漏えいにつながりうる代表的なWebサイトの利用禁止を行う機能を有すること。この代表的なWebサイトの情報については、メーカーより保守契約期間中は最新版のデータ提供を受けられること。	○
24	1	2	3	12			コンピューターに対し管理者権限(Admin権限)を持つユーザーでのログインを出来ないように抑止する機能を有すること。	○
24	1	2	3	13			管理者権限でのログインを抑止した事を指定されたメールやクライアントコンピューターにポップアップでデスクトップ上に通知する機能を有すること。	○
24	1	2	3	14			物理カメラや画面キャプチャによる撮影抑止のため、特定のアプリケーションの画面上およびデスクトップ全体にログオンユーザー名やIPアドレス、現在日時等の透かし文字（ウォーターマーク）を表示できること。	○
24	1	2	3	15			外部記憶媒体へのデータ書き込みや、印刷などを禁止したい特定のフォルダを監視対象として登録することで、制限をかける機能を有すること。監視対象になったフォルダは、以下のような特定の操作をおこなった際に、自動的にメール等で通知し、操作そのものを禁止する機能を有すること。設定できる項目については次の通りとする。	○
24	1	2	3	15	1		リモート操作受信	○
24	1	2	3	15	2		クリップボードへのコピー	○
24	1	2	3	15	3		印刷	○
24	1	2	3	15	4		画面キャプチャー	○
24	1	2	3	15	5		外部記憶媒体へのデータ書き込み	○
24	1	2	3	15	6		Print Screen	○
24	1	2	3	16			コンピューターウイルスに感染した場合に、クライアントコンピューターをネットワークから遮断しつつ資産情報やログを収集するため、特定イベントの検出時に、ネットワークからの遮断を除外する通信を設定できること。また、本ソフトウェアによる通信は維持できること。任意のウイルス対策ソフトウェア等に対応するため、検知対象のイベントは任意に設定できること。	○
24	1	2	3	17			UTM製品が出力したsyslogおよびSNMPトラップをもとに、マルウェア侵入などによる不審な通信を管理機にアラート通知し、ログとして記録できること。マルウェア侵入などによる不審な通信をUTM製品が検知すると、検知されたクライアントコンピューターは、ネットワークから自動的に遮断されること。管理機から遮断された任意のクライアントコンピューターを指定して、遮断の解除を行えること。	○
24	1	2	3	18			クライアントコンピューターが、予め指定したネットワークの外へ持ち出された場合、インターネットへの接続を制限できること。予め指定したネットワーク以外のネットワークを利用する際、使用指定したVPNサーバーとプロキシサーバーを経由するインターネット通信のみを許可できること。	○

							要求仕様	必須
24	1	2	3	19			標的型攻撃およびランサムウェア対策のため、指定した重要なフォルダに対して、指定したアプリケーション以外によるアクセスを禁止できること。なお、ローカルフォルダも重要なフォルダとして指定できること。アクセスを禁止する設定を行った後に作成された共有フォルダに対しても、自動的にアクセスの禁止設定が行われること。	○
24	1	2	3	20			アプリケーションの指定は、ファイル名を偽装したアプリケーションと正確に区別できるよう、ハッシュ値で指定できること。ローカルフォルダのマイドキュメント等は、実際のファイルパスが環境によって異なる場合も指定できること。	○
24	1	2	3	21			アクセスを制限されている共有フォルダに対して、特定のアプリケーションによるアクセスのみを許可する設定が行えること。	○
24	1	2	4				USBデバイス制御	
24	1	2	4	1			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デバイスのメーカー名、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。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。	○
24	1	2	4	2			SDカード、MOディスク、DVD-RAMなどのメディアを登録できる、管理台帳を作成できること。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。	○
24	1	2	4	3			USBデバイスの棚卸する機能を有すること。棚卸しの期限は任意で設定でき、期限を超過しても棚卸しが確認できていないUSBデバイスや利用者を表示できること。また、棚卸し期間を超過したUSBデバイスの利用を制限できること。	○
24	1	2	4	4			USBメモリ等の端末への着脱日時と記録されたファイル情報とを利用して、外部漏洩の危険性があるファイルを自動判定する機能を有すること。	○
24	1	2	4	5			USBデバイス内ファイルの日時情報を比較し、システム外で作成・編集された外部ファイルの持ち込みを自動判定し、そのUSBデバイスを使用禁止にする機能を有すること。	○
24	1	2	4	6			指定したクライアントコンピューターに対して、特定した一定時間のみ禁止を解除し、時間が過ぎると自動で禁止に戻す機能を有すること。	○
24	1	2	5				暗号化	
24	1	2	5	1			BitLockerによるドライブ暗号化が実施されていないクライアントコンピューターに対して、暗号化実施を促すメッセージを自動的に表示できること。また、クライアントコンピューターに表示されたメッセージ画面から、管理者が事前に設定した内容に沿ってBitLockerによるドライブ暗号化をユーザーが実行できること。	○

							要求仕様	必須
24	1	2	5	2			任意のフォルダを自動暗号化フォルダとして設定し、自動暗号化フォルダにファイルやフォルダをコピー・保存することで自動的に暗号化できること。また、指定したWebサイトにファイルをアップロードする際、自動暗号化フォルダに格納されている暗号化されたファイルのみをアップロードするよう設定ができること。	○
24	1	2	5	2	1		暗号化形式は、復号ツールを使用して復号する形式、もしくは復号ツールが不要なパスワード付きzipファイルを作成する形式から選択できること。	○
24	1	2	5	2	2		暗号化ファイルは、本ソフトウェアをインストールした組織内のPCでのみ復号が可能に設定できること。	○
24	1	2	5	2	3		暗号化の際、パスワード入力の失敗回数の上限および復号可能な期間を設定できること。	○
24	1	2	5	3			任意のファイルサーバー上のフォルダを自動暗号化フォルダとして設定し、自動暗号化フォルダにファイルやフォルダをコピー・保存することで自動的に暗号化できること。また、暗号化ファイルは、復号パスワードを必要とせず、本ソフトウェアをインストールした組織内のPCでのみ復号が可能なこと。	○
24	1	2	5	3	1		自動暗号化フォルダで、自動暗号化されないファイルの拡張子を指定して設定できること。	○
24	1	2	5	3	2		自動暗号化されたファイルに対して、復号を許可するアプリケーションを指定して設定できること。	○
24	1	2	5	4			USBデバイス/USBハードディスク/光学メディアに対して、専用ツールへファイルをドラッグ＆ドロップすることで、ファイルを暗号化できること。	○
24	1	2	5	4	1		暗号化する際に、復号時のパスワードに必要な文字数・文字種、復号の有効期間や失敗できる回数を設定できること。また、設定した有効期間および失敗回数を超えた場合、ファイルは自動削除されること。	○
24	1	2	5	4	2		暗号化する際に、暗号ファイルを書き込んだデバイスが端末に接続されている場合のみ復号を可能にする設定ができること。	○
24	1	2	5	4	3		本ソフトウェアが入っていない環境でも、Webからダウンロードした復号ツールを用いて復号できること。	○
24	1	2	5	4	4		ファイル暗号化におけるログとファイル操作ログを、同じ画面上で閲覧、検索することができること。	○
24	1	2	5	4	5		読み取り専用に設定したUSBデバイスに対して、暗号化したファイルの書き込みをクライアントコンピューター単位で許可できること。	○
24	1	2	5	4	6		ファイル操作ログの追跡を行った際に、ファイル暗号化および復号操作についても追跡できること。	○
24	1	2	5	5			USBデバイスおよび外付けHDD/SSDを暗号化デバイスとして設定し、書き込んだファイルを暗号化・復号できること。暗号化・復号は、暗号化デバイスとして設定されたデバイスを、本ソフトウェアをインストールした組織内のPCへ接続した際に自動的に行われること。また、暗号化したデバイスのデータは、本ソフトウェアをインストールした組織内のPCにおいてのみ復号できること。	○
24	1	2	5	5	1		復号できない場合に、回復キーによる同一組織内PCでの復号ができること。	○

別紙１　医療情報システム要求仕様書

							要求仕様	必須
24	1	2	5	5	2		暗号化設定されているデバイスの暗号化機能が、デバイスのフォーマットなどで無効となった場合、暗号化が無効になっている旨を利用者に通知する機能を有すること。	○
24	1	2	6				操作ログ	
24	1	2	6	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・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を記録する機能を有すること。	○
24	1	2	6	2			クライアントコンピューターからサーバ上の共有ファイルや、他のコンピューターからクライアントコンピューター上に作成された共有フォルダへのアクセスおよびファイル操作をログとして記録する機能を有すること。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)を行ったアプリケーションのプロセスID、ハッシュ値およびファイルパスも記録できること。	○
24	1	2	6	3			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でき、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。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。なお、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、指定した期間は端末機側でもログを保持し、データサーバーへの再回収が行えること。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	○
24	1	2	6	4			後述するリモート操作を行った履歴及び管理者側が行った操作としてログが残せ、ログ検索・閲覧などの操作に対するログも取得できること。	○
24	1	2	6	5			Microsoft Internet Explorer、Firefox、Google Chrome、Safari、Microsoft Edge（EdgeHTML）、Microsoft Edge（Chromium）を使ってWebの閲覧やダウンロード、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、書き込み内容などをログとして記録できること。また、閲覧先のURLだけでなく、広告として表示されるURLも記録でき、httpsによる通信も記録可能であること。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ログとして記録する機能を有すること。なお、最前面に表示されているWebブラウザ上で、ユーザーがマウスやキーボードを操作していた時間を集計し記録できること。	○
24	1	2	6	6			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。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。	○

							要求仕様	必須
24	1	2	6	7			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の操作に対して、クライアントコンピューターと同様にログ収集が行えること。また、ログ検索・閲覧などの操作に対するログも取得できること。	○
24	1	2	6	8			指定した範囲のIPアドレス以外に対するTCP通信をログとして記録する機能を有すること。なお、httpプロトコル以外の通信を行った場合、およびブラウザ以外のアプリケーションが外部と通信を行ったログも記録すること。指定したIPアドレス範囲内であっても、特定のIPアドレスについては記録対象から除外する設定が行えること。また、指定したデータ送受信量の閾値、ファイルおよびフォルダについても、記録対象から除外する設定が行えること。	○
24	1	2	6	9			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。また、コマンドプロンプト（cmd.exe）、Windows PowerShell（powershell.exe）で実行したコマンドおよび引数を記録する機能を有すること。	○
24	1	2	6	10			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。	○
24	1	2	6	11	1		電子カルテシステムログイン中に行われたクライアントコンピュータの操作ログには、電子カルテのログインユーザーIDならびに利用者名が、IPアドレス、コンピュータ名などと共に記録されること。	○
24	1	2	6	11	2		電子カルテシステムにログインしている場合、USBデバイスの個体識別情報と電子カルテシステムのログインユーザーIDを連携させることで、使用許可／不許可および書き込み禁止の使用制限設定を行えること。	○
24	1	2	7				リモート操作	
24	1	2	7	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。管理機は、クライアントコンピューター1台もしくは複数台の画面を静止画で同時に確認することができ、その静止画は順次更新できること。管理機から複数のクライアントコンピューターを同時に画面に表示させ、切り替えてリモート操作できること。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。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。リモート操作を円滑に行うため、ミラードライバー設定が可能であること。	○
24	1	2	7	2			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。操作を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。	○

							要求仕様	必須
24	1	2	7	3			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。Windows8以降でも可能であること。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。	○
24	1	2	7	4			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。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。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。	○
24	1	2	7	5			クライアントコンピューターが故障した際には、代替機を同一の端末としてログや資産情報を収集し、収集した情報は同一の端末として閲覧・検索できること。	○
24	1	2	7	6			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。Windows8以降でも可能であること。	○
24	1	2	7	7			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。	○
24	1	2	8				管理コンソール	
24	1	2	8	1			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表示する機能を有すること。アラートが発生したクライアントコンピューターは画面を拡大表示できること。ただし、設定された期間を経過すると自動で解除する機能を有すること。	○
24	1	2	8	2			よく使用する機能を登録でき、クリックすると登録したボタンが表示されること。	○
24	1	2	8	3			端末の操作画面を管理端末で表示する際に、アラート未発生端末の操作画面は非表示とする、プライバシー保護に配慮した機能を有すること。	○
24	1	2	8	4			アラート発生時における端末操作画面を、マウスカーソルの位置が強調された形式で表示し、不正操作及び誤操作発生時に早期の問題把握ができる機能を有すること。	○
24	1	2	8	5			セキュリティの観点から、管理コンソールはWebベースではなく、モジュール常駐型とする。	○
24	1	2	8	6			円滑な情報周知する為、管理機から任意の部署およびクライアントコンピューターに対してメッセージを作成し、クライアントコンピューターの画面上にポップアップ表示できること。メッセージは、タイトル、フォントサイズ、文字色、太字、斜体、下線、背景色、リンクの設定が行えること。リンクの設定はメッセージ内の任意の箇所に、複数設定可能であること。メッセージの既読確認が行えること。メッセージ送信前にプレビューで確認が行えること。表示位置設定、自動リサイズの挙動もプレビューで行えること。	○