参考資料 「ＬＡＮシステム一式の賃貸借契約書、仕様書」より抜粋

別紙３ セキュリティ対策等

１　クライアントパソコンのウィルス対策管理

⑴　仮想サーバ仕様

ウィルス対策サーバの仕様のとおり

⑵　ソフトウェア仕様

ア　世界規模で展開されたウィルス解析機関を有し、ウィルス定義ファイルを1日1回以上更新する事が可能な環境及び機能を有していること。

イ　リアルタイムスキャン機能、スケジュールスキャン機能を有すること。スケジュールスキャンの設定を「日」、「週」、「月」単位で設定することが可能であること。

ウ　ヒューリスティック技術を搭載し、新種・亜種等の未知のウィルスも検出する機能を有する　こと。

エ　メモリ上に存在するウィルスに対しても検出する事が可能な機能を有すること。

オ　定義ファイルで検知しないウィルスの場合、振る舞い挙動検知により、トロイの木馬、キーロガーや未知のマルウェアの検出機能を有すること。

カ　特定のアプリケーションの起動制御や外部デバイスの利用制限機能を有すること。

キ　ウィルス対策サーバから対象デバイスへ最新の定義ファイルを配信する機能を有すること。

ク　ダウンロードファイルに関するレピュテーション(評価)機能を有しており、評価によってダウンロードの可能/不可能を決定する事が出来ること。

ケ　シングルコンソール（統一管理ツール）で管理が可能なこと。

コ　ダウンロードをするファイルのマルウェアを検知し、世界規模で展開しているセキュリティ解析機関にて管理をしている脅威情報と同期を取り、感染を防止させる機能を有していること。

サ　ウィルス検出時、管理者宛てにメールで通知する機能を有すること。

シ　アンチウィルスの定義ファイルを更新する機能があり、インターネットを通じて入手する事が可能なこと。

ス　ウィルススキャンの状況、パソコン／サーバのウィルス定義ファイルの状態が、把握出来る機能を有すること。

２　スパム対策、ウィルス対策、ＵＲＬフィルタリング対策

⑴　ハードウェア仕様

ファイアウォールの仕様のとおり

⑵　機能仕様（ウィルス対策）

ア　メール、Webアクセストラフィックへのウィルスチェック機能を有すること。

イ　ウィルスチェックのためのデータベースを持ち、自動更新がされること。

⑶　機能仕様（スパムメール対策）

ア　IP アドレスチェック、E-mail アドレスチェックやリバースDNS ルックアップなど複数のアンチスパムフィルタを装備し、スパムの可能性があるメールをブロックする機能を有すること。

イ　スパム検索するデータベースを有し、自動更新がされること。

⑷　機能仕様（URL フィルタリング）

ア　Web アクセス時のURL フィルタリング機能を有すること。

イ　URL/IP レベルでリサーチされたWeb コンテンツカテゴリーによる分類がなされ、フィルタリングできること。

ウ　Web コンテンツカテゴリの自動更新機能を有すること。

３　既知／未知の脅威への対応 （２台）【アプライアンスサーバ】

⑴　ハードウェア仕様

ア　CPUはインテル®Xeon®X3450(2.66GHz)相当以上のものを1個以上搭載した機能相当以上であること。

イ　8GB以上のメモリを搭載していること。

ウ　ハードディスクは300GB以上を有すること。

⑵　ソフトウェア仕様

ア　一定以上の期間/人数で評価を行った検知対象ファイルの評価に基づいた、疑わしいファイル/アプリケーションを検知出来る機能・振る舞い検知の機能を有すること。

イ　標的型攻撃対策として、定義ファイルで検知されず侵入してきたマルウェアに対して、ネットワーク的な観点でマルウェアを見つけ出すことができる機能を有すること（ボット、スパイウェアなど）。

ウ　マルウェアとインターネット指令サイトとの通信を検知、ブロック可能であること。

エ　標的型攻撃の防御のために未知のマルウェアを含め、ウィルス/スパイウェアに感染しているパソコンをIPアドレスで特定し、その通信を監視、ボット通信の検知を行う機能を有していること。

オ　複数の通信ログを相関的に分析し検知が可能なエンジンを有していること。

カ　外部のマルウェアサイト及びインターネット指令サイトの情報を随時アップデートし通信を監視できること。

キ　悪意あるWebサイトの閲覧を検知し、ブロックする機能を有すること。

ク　外部Webサイトへのファイルのアップロードの監視が可能であること。

ケ　P2P通信の検知が可能であること。

コ　レポート機能を有し、各種インシデントを可視化出来る機能を有すること。

サ　Spanポートに接続し、ネットワークのパフォーマンスに影響なく設置、運用が可能なこと。

シ　ボットと疑われる通信が発生した際、問題解決に向けたサービスが提供されること。

４．クライアントパソコンのセキュリティ状況管理

⑴　基本要件

ア　サービスの開発元は国内企業とし、国内で開発されたシステムで日本語化対応であること。

イ　クラウドサービス（SaaS）による提供を行うこと。

ウ　管理者によるポリシー（設定情報）の配付、セキュリティ診断結果及び資産管理情報の収集が可能で、毎月の保守報告と合わせて、各共同利用団体に収集した情報の概要等について報告すること。

エ　クライアントライセンスをクライアントパソコンの台数分準備すること。

オ　クライアントパソコンの動作環境を確認し、動作環境が不十分な場合は、共同利用団体に対して必要な助言を行うこと。ただし、メモリーの増設等クライアントパソコンの動作環境に係る経費は、本契約に含まれない。

⑵　管理者機能

ア　日々の全体把握を管理者及び各共同利用団体が即座にできるよう、Web 上のワンビュー（１画面）で、セキュリティアラート情報、セキュリティポリシー遵守状況、棚卸し実施状況、機器稼働状況、ソフトウェアライセンス管理状況、電力使用容量、印刷状況が確認できる機能を有すること。

イ　セキュリティ違反のクライアントは、ドリルダウン方式にてクライアント一覧と個別のクライアント状況が表示される機能を有すること。

ウ　管理者パソコンから各共同利用団体の拠点施設単位もしくは全クライアントに対し、一斉にポリシーの適用ができる機能を有すること。

⑶　セキュリティ関連機能

ア　ウィルス対策ソフトウェアのパターンファイルのチェックを行い、古い場合はクライアントにメッセージを表示し、最新化へ誘導する機能を有すること。

イ　ウィルス対策ソフトウェアの最終スキャン日時をチェックし、管理者が指定した一定期間以上スキャンを実行していない場合は、警告を出す機能を有すること。

ウ　Windows のパッチ適用のチェックを行い、古い場合はクライアントにメッセージを表示し、最新化へ誘導する機能を有すること。

エ　Adobe Flash Player、Adobe Reader、Java Runtime Plugin のバージョンのチェックを行い、古い場合はクライアントにメッセージを表示し、最新化へ誘導する機能を有すること。

オ　クライアントパソコンのログオンパスワード、スクリーンセーバーパスワード、ハードディスクパスワード、BIOS パスワードをチェックする機能を有し、スクリーンセーバ起動時間のチェックについても可能なこと。

カ　管理者が指定した利用禁止アプリケーションがクライアントにインストールされていないかどうかをチェックし、インストールしている場合は警告を出す機能を有すること。なお、利用禁止アプリケーションについては、受注者から履行期間までに利用禁止として指定するアプリケーション案を共同利用団体に提示すること。

キ　端末においてセキュリティ診断結果を表示することができ、違反項目を解決するためのガイダンスが表示されること。

⑷　利用制限

ア　管理者が許可していないUSB メモリ等のUSB 媒体の使用を禁止する機能を有すること。違反者には警告メッセージを表示し、管理者側にも通知できること。

⑸　資産管理

ア　ハードウェア資産情報を自動的に収集する機能を有すること。自動収集の項目は以下のとおりとする。

・　CPU 関連（種別、クロック）

・　メモリ関連（物理、仮想）

・　パソコン関連（種別、型名、メーカー、製造番号）

・　ネットワーク関連（アダプタ名、IP アドレス、MAC アドレス、サブネットマスク、デフォルトゲートウェイ）

・　ハードディスク関連（全体容量、空き容量）

イ　ソフトウェア資産情報を自動的に収集する機能を有すること。自動収集の項目は以下のとおりとする。

・　OS 名

・　サービスパック名

・　ウィルス対策ソフトウェア名

・　インストールソフトウェア名

ウ　資産管理情報を手動で追加できる機能を有すること。追加項目は、機器管理番号、登録日、　　導入責任者、購入形式、購入日、購入先、購入金額、リースまたはレンタル情報（開始日、終了日、取引先、経費、管理番号、契約番号）、管理部署、担当職員、使用部署、使用者、設置場所及び備考とする。

エ　ソフトウェア情報と管理者が入力したソフトウェア(保有ライセンス）情報を比較し、ソフト　ウェアライセンス数の利用状況を確認し、ライセンス違反をチェックする機能を有すること。

オ　任意のクライアントに対して、棚卸し指示を依頼することができ、棚卸し指示を受けたクライアントにおいて登録した棚卸し情報を管理者が確認できること。クライアントで登録が可能な情報には、「管理部門名」「担当職員」「棚卸し実施者名」「設置場所」「利用状況」が含まれること。