別紙４　システム機能要件表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| No | ページ  番号 | 項目名 | 機能要件 | 標準対応 | オプション対応 | 摘要 |
| 1 | 11 | システム要件－(1)クラウド基盤  ア）認証基盤 | 複数のサービス（Webサービスやアプリケーション）に登録されているIDとパスワードの一元管理、ならびに各システムへの認証をクラウドサービスにて行う（IDaaS：Identity as a Service）としての機能を備えること。 |  |  |  |
| 2 | 人事異動等の発生時に、本市によるアカウントの随時追加、削除、編集等が可能であること。 |  |  |  |
| 3 | 現行のMicrosoftアカウント情報（児童生徒含む〇〇アカウント程度）を引き継ぐとともに、本市が業務利用する各システムおよびサービスとのシングルサインオン連携またはユーザー情報連携が可能であること。 |  |  |  |
| 4 | 生体情報（顔）および知識情報（PINまたはパスワード）の２つを組み合わせた多要素認証が可能であること。また、非常の際には、多要素認証を利用せずに、業務端末へログインできる設定が可能であること。 |  |  |  |
| 5 | イ）アクセス制御 | 事前に定義した不正アクセスパターンとのマッチングにより、クラウド等への不正なアクセスを検知（IDS：Intrusion Detection System）または遮断（IPS：Intrusion Prevention System）できること。 |  |  |  |
| 6 | 個人契約のテナントやシャドーIT等、セキュリティ上懸念があるサービス等へのアクセスを制御できること。 |  |  |  |
| 7 | ウ）フィルタリング | 認証基盤（IDaaS）と連携するとともに、悪質なWebコンテンツやアプリケーション等へのフィルタリングが可能であること。 |  |  |  |
| 8 | フィルタリング設定のテンプレートが用意されているとともに、グループごとのルール設定やホワイトリスト運用が可能であること。 |  |  |  |
| 9 | エ）アンチウィルス | パターンマッチングの他、機械学習やふるまい解析等の技術により、既知または未知にかかわらず、不審な挙動をするマルウェア等の検知や遮断が可能であること。（ふるまい検知） |  |  |  |
| No | ページ  番号 | 項目名 | 機能要件 | 標準対応 | オプション対応 | 摘要 |
| 10 | 11 | エ）アンチウィルス | パターンファイルの存在しない未知のマルウェアに対応するため、外部のシステムと断続的に通信を行うなどの不審な挙動をするプログラムの検知や感染拡大の防止（EDR：Endpoint Detection and Response）が可能であること。 |  |  |  |
| 11 | 認証基盤（IDaaS）と連携するとともに、脅威が検出された時は、即座にメール等で管理担当者へ当該校務PC端末やユーザー情報等を通報できること。 |  |  |  |
| 12 | 随時、最新のセキュリティ状態に更新できること。 |  |  |  |
| 13 | 脅威の侵入経路等について、トラッキングが可能であること。 |  |  |  |
| 14 | 12 | オ）デバイス管理 | 校務PC端末に対して、アプリケーションの一斉配付やWindows Update等の一斉管理ができること。その際、配付の時間帯等を本市が任意に指定できるとともに、ネットワーク等の負荷分散を図る機能を備えること。 |  |  |  |
| 15 | 校務PC端末を紛失した際、遠隔操作にて当該端末内の特定フォルダのデータ消去等ができること。 |  |  |  |
| 16 | ユーザーからの操作方法等の問合せ時に、管理担当者が当該ユーザーの校務PC端末にリモートでアクセスし、両者が当該端末画面を確認しながら管理担当者による操作ができること。 |  |  |  |
| 17 | 13 | カ）共有ストレージとデータファイルの暗号化  b)新システム（クラウドストレージ） | 校務系ネットワーク（校務PC端末）および学習系ネットワーク（学習用１人１台タブレット端末）のユーザーがインターネット経由でアクセスするクラウドストレージは、全体領域として138TB程度（基本100TB＋380ユーザー×100GB）のディスク容量を備えること。 |  |  |  |
| 18 | クラウドストレージのフォルダ構成およびアクセス権限等は、認証基盤（IDaaS等）と連携して、ユーザーの職位やグループごとに柔軟に設定できること。 |  |  |  |
| 19 | バージョンの履歴機能および削除ファイルの復元機能を有すること。復元可能な期間は、削除操作から30日を保障すること。 |  |  |  |
| No | ページ  番号 | 項目名 | 機能要件 | 標準対応 | オプション対応 | 摘要 |
| 20 | 13 | b)新システム（クラウドストレージ） | ユーザーがアクセス可能なフォルダについては、Windows標準のエクスプローラからショートカット等により直接接続できるよう、個人で設定するためのマニュアルを作成するとともに、MDM等でのクラウドストレージへのショートカットの一斉配付が設定できること。 |  |  |  |
| 21 | 高島市教育情報セキュリティポリシー（令和２年３月）および高島市教育情報セキュリティ運用規程（令和２年３月）に定める情報資産等の分類に基づいて、アクセス権限がないユーザー（第三者含む）がデータファイルを扱えないよう制御できること。 |  |  |  |
| 22 | 機微情報を含む重要なデータファイルについては、その操作ログもしくは全てのファイルの操作ログを取得し、外部記憶媒体への持ち出しが制限可能であるとともに、クラウドストレージからのダウンロードを検知できること。 |  |  |  |
| 23 | クラウドストレージに保存するデータファイルは、ユーザーが特に意識することなく自動暗号化されること。 |  |  |  |
| 24 | 15 | システム要件－(2)個別システム  ③資産管理システム  ア）セキュリティパッチの管理 | 新システムの運用開始以降、セキュリティパッチを保守業務としてダウンロードおよび配信する。その際に、ネットワークへの影響を抑えることができること。 |  |  |  |
| 25 | セキュリティパッチおよび更新プログラムを配布する際、同一サブネット内の管理対象の校務PC端末に既にそれらのファイルがキャッシュとして残っていた場合は、そのキャッシュを使ってファイルを取得（ダウンロード）できること。 |  |  |  |
| 26 | セキュリティパッチ適用済み／未適用の結果を、Webレポート画面にて確認できること。 |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| No | ページ  番号 | 項目名 | 機能要件 | 標準対応 | オプション対応 | 摘要 |
| 27 | 15 | イ)USBデバイス制御 | USBメモリや外付けハードディスクなどの外部記憶媒体について、使用許可／不許可等の設定ができること。 |  |  |  |
| 28 | ウ)情報資産管理 | 校務PC端末上のハードウェア情報および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。 |  |  |  |
| 29 | 校務PC端末ごとにアプリケーション状況を把握できること。 |  |  |  |
| 30 | 情報の収集は、決められた時刻に全台一斉に実行されるのではなく、自動で分散実行して、ネットワークや校務PC端末の負荷を低減できること。 |  |  |  |
| 31 | 手動による任意タイミングでも実行できること。 |  |  |  |
| 32 | 16 | ハードウェア台帳で、重複した校務PC端末（端末シリアル番号またはMACアドレスが重複した端末）を抽出して表示できること。 |  |  |  |
| 33 | エ)操作ログ | ログオン、ログオフ、外部記憶媒体の利用などの校務PC端末の操作ログを収集できること。 |  |  |  |
| 34 | 17 | システム要件－(3)ネットワーク機器等②納入機器イ)校内LAN用スイッチa)基幹スイッチ | ・電源内蔵メタル筐体で、16ポート1000BASE-T対応のレイヤー２スイッチであること。  ・ループ防止機能を有し、静音ファンレス設計で、動作時環境温度50℃に対応すること。  【新機器：基準品】 エレコム　EHB-UG2B16-S |  |  |  |
| 35 | 18 | b)スイッチ（島HUB） | ・電源内蔵メタル筐体で、8ポート1000BASE-T対応のレイヤー２スイッチであること。  ・ループ防止機能を有し、静音ファンレス設計で、動作時環境温度50℃に対応すること。  【新機器：基準品】 エレコム　EHB-UG2C08-S |  |  |  |