セキュリティシステム要件

カテゴリ	No.	要件
クライアント	1	対象クライアントOS：Windows 10
	2	クライアント数：1,162台　※令和3年度に小1～2年生を含む1,447台となる予定。
サーバ	3	サーバ数：1台（1,162台のクライアントを管理するのに必要な台数）　※令和3年度の整備台数も含めて1台で管理可能。
暗号化・復号化	4	校内領域/校外領域の定義は管理者により設定可能なこと。 ※校内領域の定義は、パソコンのローカルドライブ、ファイルサーバやNAS、学習系システムサーバ等のホスト名・IPアドレス・共有フォルダパス、及びURL（校内ポータル・システムや校外クラウドサービス等）にて設定可能なこと。
	5	ファイル暗号化による運用トラブル（ファイル破損、動作の遅延、既存システムへの影響等）を避けるため、校内領域（パソコンやファイルサーバ等）には平文で保存されること。
	6	校内のパソコンから校外領域へのファイル持ち出しは、管理者により許可されたプログラムのみ持ち出し可能とすること。
	7	校内領域（パソコンやファイルサーバ等）に存在する全てのファイルが、校外領域であるUSBメモリ等の外部記憶媒体、webメールに添付、webページへのアップロード、管理外サーバ等に持ち出される際は、ファイル形式に依存せず必ず自動的に暗号化または禁止（設定により切り替え可能なこと）されること。また、メールソフトに添付される際は、必ず自動的に暗号化されること。 ※暗号化に際し、パスワードの入力が不要なこと。
	8	暗号化されたファイルを校内領域に戻した際は、自動的に復号されること。 ※復号化に際し、パスワードの入力が不要なこと。
	9	職員・生徒が校内領域のファイルを正当に校外領域へ持ち出す場合は、持出専用フォルダを経由して持ち出しができること。持ち出すファイルは平文を禁止しパスワード暗号化をかけたZIP形式に強制することも可能なこと。
	10	校外領域へのファイル持ち出しにおいては、特定の管理者の承認を得たファイルのみ持ち出し可能な設定ができること。（以下、「承認機能」という。）承認を得たファイルにおいても、パスワード暗号化をかけたZIP形式に強制することも可能なこと。
	11	承認に関する申請があった場合は管理者に自動で通知が飛ばせること。また、承認・否認した場合は、申請者に自動で通知が飛ばせること。
	12	承認機能は、本システムの提供機能で実装できること。
	13	AES暗号256bit以上の暗号強度が利用できること。
操作性	14	暗号化及び復号化は、職員・生徒の意識やITスキルに依存しないよう、職員・生徒が新たに暗号化ソフトの使い方を覚えることなく、ファイル作成・コピー・保存・アップロードなど通常操作の延長で、意識することなく自動暗号化及び自動復号化されること。
履歴	15	校外領域へのファイル持ち出しに関し、ユーザ名、コンピュータ名、日時、対象ファイル名、操作内容、持ち出し経路の特定が可能な記録内容であること。
	16	webページ（SNS等）ごとのキー入力、ファイルごとのキー入力履歴を記録できること。また、キー入力履歴を取得するアプリケーションを指定できること。
	17	インシデント発生時に、いつ、だれが、何を、どのような手段で、どのような形式で外部に持ち出したかを迅速に追跡できる履歴を取得できること。また、被害状況の把握、原因の追跡を行い、再発防止を講じるための証跡管理が行えること。
	18	記録した履歴について一元管理が可能であること。
運用管理	19	運用管理負荷低減のため、上記要件を単一のソフトウェアで実現すること。
	20	配布ソフトやログオンスクリプト等の機能を用いて、サイレントインストールやアップデートができる機能を有すること。
	21	Active Directoryと連携して権限設定が行えること。
その他	22	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。