別紙1　新暗号化システムライセンス機能要件

〇ファイル暗号化/持出制限システム

カテゴリ	No.	要件
ライセンス	1	クライアント数：6,974台（対象クライアントOS：Windows 10、11）
	2	6,974台のクライアントを管理するのに必要なサーバーライセンス（対象サーバOS：Windows server2019、Windows server2022）
サーバー	3	クライアントの管理サーバーは仮想基盤上に構築可能なソフトウェアであること。
暗号化・復号化／持出制限	4	庁内領域/庁外領域の定義は管理者により設定可能なこと。 ※庁内領域の定義は、庁内PCのローカルドライブ、ファイルサーバやNAS、業務サーバ等のホスト名・IPアドレス・共有フォルダパス、及び庁内イントラネットのURL（ポータルサイトや業務システム等）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、庁内領域には平文で保存されること。
	6	庁内PCから庁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なこと。
	7	庁内領域に存在する全てのファイルが、庁外領域であるUSBメモリ等の外部記憶媒体、メールに添付、Webページへのアップロード、許可外サーバ等に持ち出される際は、ファイル拡張子に依存せず必ず自動的に暗号化または禁止されること。また、暗号化とする場合、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庁内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。
	9	職員が庁内領域のファイルを正当に庁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	庁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	承認機能については、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。
ドライブ暗号化	14	庁内PCのHDD・SSDに対し、ドライブ全体の暗号化が可能なこと。
	15	庁内PCごとの暗号鍵管理が不要なこと。
	16	庁内PC破棄の際に情報を復元困難な状態にする措置として暗号化消去が可能なこと。また、暗号化消去の実施完了情報を出力可能なこと。
ローカルドライブ保存制限及び削除	17	庁内PCのローカルドライブにファイルを保存できる領域を、特定の領域(以下、「特定領域」という。）のみに制限可能なこと。
	18	特定領域に保存されたデータを、管理者が指定したタイミングで自動で削除されること。 ※削除タイミングはWindows起動・終了、ログオン・ログオフ、時間・曜日などから選択して設定可能なこと。
	19	管理者が特定の庁内PCに対して、遠隔で特定領域に保存されたファイルの削除命令を発行可能なこと。
アプリケーション起動制限	20	アプリケーションの起動を制限可能なこと。 ※起動の許可・制限は、アプリケーション名、ファイルパス、ハッシュ値の組合せにより設定可能なこと。
IP送信の制御	21	IPプロトコルを使用したデータ送信（書き込み）を制限可能なこと。 ※送信（書き込み）の許可・制限は、アプリケーション名、IP アドレス、ポート番号の組合せにより設定可能なこと。
PCモード定義	22	管理者が庁内PCに適用するセキュリティポリシーをモードとして複数定義でき、利用者が業務に応じて庁内PC上でモードの切り替えが可能なこと。
	23	№17～№19のローカルドライブ保存制限及び削除をモードごとに設定可能なこと。
	24	№20のアプリケーションの起動制限をモードごとに設定可能なこと。
	25	№21のIP送信の制限をモードごとに設定可能なこと。
	26	使用できる有線LAN、Wi-Fi のアクセスポイント(SSID)、プロキシ、あるいはVPN をモードごとに設定可能なこと。
	27	指定したパスのファイルに対するアクセスの制御（見せないまたはリードオンリー）をモードごとに設定可能なこと。
	28	モード間のクリップボードのデータの制御（破棄またはテキストのみ可）をモードごとに設定可能なこと。
	29	モード切り替え時に、スクリプト(.bat ファイル、.vbsファイル等) やプログラム(.exe) などのプロセスを実行可能なこと。
操作性	30	暗号化及び復号化は、職員の意識やITスキルに依存しないよう、職員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	31	庁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。
	32	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。
	33	承認機能において、誰が、いつ、どのファイルを、どのような理由で持ち出し申請・承認したのかを把握できる証跡を残せること。
	34	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	35	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。
	36	SCCM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。
	37	Active Directoryと連携して権限設定が行えること。
その他	38	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。
	39	それぞれのライセンスに別途保守ライセンスが必要な場合は、その保守ライセンス。

表１　上記仕様を満たす参考製品

分類	仕様	数量
ライセンス	セキュリティプラットフォーム サーバ ベーシック　evolution ／SV	3ライセンス
	セキュリティプラットフォーム トレーサオプション	3ライセンス
	セキュリティプラットフォーム サーバ エンクリプションオプション	3ライセンス
	セキュリティプラットフォーム サーバ イントラネットオプション	3ライセンス
	セキュリティプラットフォーム サーバ ストレージエンクリプションオプション	3ライセンス
	セキュリティプラットフォーム サーバ セパレートオプション	3ライセンス
	セキュリティプラットフォーム クライアント ベーシック　evolution ／SV	6,974ライセンス
	セキュリティプラットフォーム クライアント エンクリプションオプション	6,974ライセンス
	セキュリティプラットフォーム クライアント イントラネットオプション	6,974ライセンス
	セキュリティプラットフォーム クライアント ストレージエンクリプションオプション	6,974ライセンス
	セキュリティプラットフォーム クライアント セパレートオプション	6,974ライセンス
製品保守サービス	SePテクニカルサポートサービス（上記構成・数量）	4年間

〇履歴抽出エンジンシステム

カテゴリ	No.	要件
ライセンス	1	数量：1ライセンス
	2	Windows Server2022、2019　または　Windows 10、11で動作するシステム、ソフトウェアであること。
履歴高速抽出エンジン	3	ファイル暗号化/持出制限システムで記録された膨大の履歴を高速検索可能なフルテキストサーチ型のエンジンであること。
	4	保管されている ZIP形式の履歴に対し、検索前に解凍処理が不要で直接検索可能なこと。
	5	操作履歴の検索において、データベースへのインポートやインデックス作成など、検索前に加工処理が必要ないこと。
	6	検索条件は、AND、OR等で複数の指定が可能であること。
	7	検索結果のレコード数がカウントされること。
	8	複数の検索処理について、バッチ化が可能であること。

表２　上記仕様を満たす参考製品

分類	仕様	数量
ライセンス	スーパーサーチエンジン	1ライセンス
製品保守サービス	スーパーサーチエンジン保守サービス（上記数量）	4年間