自治体情報システム強靭性向上モデル更改業務　仕様書

１　業務概要

（１）業務名　自治体情報システム強靭性向上モデル更改業務

（２）履行期間

①構築業務：契約締結日から令和９年１月３１日まで

②本稼働日：令和９年２月１日（予定）

③運用・保守業務：本稼働日を含む月から６０か月

※詳細なスケジュールは、受注候補者と別途協議の上、決定

（３）業務場所　埼玉県羽生市

２　業務の目的

本市では、総務省の示す「自治体情報システム強靭性向上モデル」に基づき、いわゆる「三層の対策」を実施するための環境整備を行っている。

本業務は、業務効率化やセキュリティの強化のため、端末統合システムによる自治体情報システム強靭性向上モデルの更改に係る必要な業務を行うものである。

３　機能要件

（１）別表「システム機能要件」にある機能要件を満たすこと。

（２）物理サーバを手配する場合は、停電発生時に備えてＵＰＳを調達すること。

（３）管理サーバのバックアップを取得するためのバックアップＮＡＳを導入すること。

４　プロジェクト管理

（１）計画書の策定

本システムの構築における具体的な体制、スケジュール、プロジェクト管理方針、プロジェクト管理方法等を含んだ計画書を作成し、市の承認を得た上で業務を行うこと。

（２）プロジェクト管理会議

受注者は、プロジェクト管理に関する定例報告会を開催すること。開催頻度は、月１回程度を目安とし、詳細は発注者と協議し決定する。発注者が臨時的な会議が必要と判断した場合は、受注者と協議し開催する。受注者は、会議終了後７日以内に議事録を発注者に提出し、検収を受けること。

５　構築業務に係る要件

（１）システム設計

受注者は、現行のシステム環境について主体的に調査を行った上で、導入システムにおける要件定義、基本設計、詳細設計、移行設計を行うこと。提案するシステムの仕様

や更新対象がシステムとの連携に当たり、必要に応じて最適な設計内容への見直しを行うこと。

（２）運用試験

本稼働までに運用試験を行い、運用試験において発生した障害は、必要に応じて発注者に報告を行い、復旧作業及び原因の解明、対策を行うこと。また、性能面での問題が発生した場合は調整を施すこと。試験結果については、報告書を作成し、発注者に提出すること。

（３）システム導入

システムの導入は、各業務への影響を最小限に留めるよう、発注者と協議しスケジュールの調整を行うこと。

（４）既存システム等の設定変更及び連携

既設システム・機器に係る設定変更や連携が必要な場合は、保守運用業者に対して必要な情報を提供すること。また、既設システムの計画外の停止等が発生しないように留意すること。作業が発生する場合は、受注者が本市及び保守運用業者と調整すること。

６　納品物

以下のとおり納品すること。また、発注者が新たに必要としたものについては、適宜掲示すること。

・納品物目録
・プロジェクト計画書
・ネットワーク構成図
・基本設計書
・詳細設計書
・操作説明書
・ID/パスワード一覧
・管理者向けマニュアル
・利用者向けマニュアル
・その他必要と思われるもの

７　研修・教育に関する要件

一般職員及び運用管理職員に対して、導入システムの操作研修を実施すること。

・一般職員数４００人程度（複数回に分けて行う想定）
・運用管理職員３人程度

８　運用保守の要件

以下のとおり保守対応を行うこと。

（１）業務時間帯

原則、羽生市の開庁日（羽生市職員の勤務時間、休日及び休暇に関する条例第３条に定める日を除く日をいう。）とする。ただし、システム又は機器において発注者が緊急な対応が必要と判断した障害及びセキュリティインシデントが発生した場合における対応業務等、発注者が特に必要と認めた場合は、この限りではない。また、故障等で停止した際に運用影響が発生する機器は、２４時間３６５日のオンサイト保守を行うこと。

（２）保守体制

障害発生時に迅速に復旧が可能となる保守体制を確保していること。概ね２時間以内に現地へ到着できること。

（３）業務実施場所

羽生市役所及び各公共施設

（４）業務対象範囲

本業務で導入したハードウェア、ソフトウェア

（５）業務内容

・機器の稼働状況の監視
・バックアップ取得及びリストア対応
・構成図、手順書等の更新
・障害発生対応
・セキュリティインシデント対応
・ヘルプデスク対応

（別表）システム機能要件

※代替案による対応も可

項目	No.	機能要件
クライアント	1	対象クライアントOS：Windows 10、Windows 11
	2	クライアント数：450台
サーバ	3	サーバ数：１台（450台のクライアントを管理するのに必要な台数）
ネットワーク切り替え	4	１台の端末上のソフトウェアスイッチにより、インターネット系通信、LGWAN系通信と基幹系通信の切り替えが可能なこと。また、接続可能な通信の制御を有線LAN、Wi-Fiのアクセスポイント（SSID）、プロキシ、VPN接続の全てで行えること。
	5	業務の種類によってアクセス可能なローカル領域が区別できること。
	6	LGWAN系通信中のアクセス可能なローカル領域とインターネット系通信中のアクセス可能なローカル領域が区別できること。また、インターネット系通信中のローカル領域のデータは管理者が指定したタイミングで自動削除されること。
	7	インターネット系通信中は管理者が指定した特定のアプリケーションのみ起動可能なこと。
	8	LGWAN系とインターネット系の分離環境間でテキストのクリップボードが使用できること。
	9	インターネット系通信中に不正プログラムによりOSやアプリケーションのプログラム及びメモリが破壊・改ざんされないような対策が可能なこと。
	10	Web会議時は管理者が指定した特定のアプリケーションのみ起動可能なこと。 また、クライアントのカメラ、マイク、スピーカーを接続してWeb会議が行えること。
情報漏洩対策機能	11	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、パソコン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。
	12	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、パソコンのローカルドライブ以外の庁内領域には平文で保存されること。パソコンのローカルドライブについては、ドライブ暗号化を行うが、Windows上では平文ファイルとして利用できること。
	13	庁内のパソコン(以下「庁内PC」という。）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とすること。
	14	庁内領域（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、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、管理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、又は持ち出しを禁止されること。また、暗号化に際し、パスワードの入力が不要なこと。
	15	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。
	16	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（以下「パスワードZIP」という。）に強制することも可能なこと。また、持ち出し先（外部記憶媒体、メール、Web、管理外サーバ）により、持ち出し可能なファイル形式を変更することも可能なこと。（例：メールは平文とパスワードZIPの選択制、メール以外の持ち出し先はパスワードZIPのみ）
	17	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。
	18	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。
	19	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。
	20	AES暗号256bit以上の暗号強度が利用できること。
ローカルドライブ保存制限及び削除	21	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。）のみに制限をかけることができること。
	22	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削除できること。 ※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。
	23	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。
操作性	24	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	25	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。
	26	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。
	27	記録した履歴について一元管理が可能であること。
その他	28	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。
	29	Active Directoryと連携して権限設定が行えること。
	30	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。
	31	管理サーバが障害等でダウンした差でも、ソフトウェアスイッチが可能であること
	32	LGWAN系と基幹系の間で、上長承認の上、ファイルを受け渡す機能があること。
	33	ファイルの受け渡しについて、ログを記録する機能があること。