我孫子市庁内ＩＣＴインフラ及びセキュリティ環境提供業務委託情報提供依頼書（ＲＦＩ）

平成３１年４月１日

我孫子市総務部情報政策課

— 目　次 —

1 目的

本市では、２０１２年１月から開始した電算システム包括委託が２０２１年１２月末をもって契約が終了します。この契約に含まれていた庁内ネットワーク・パソコン・仮想基盤等のＩＣＴインフラ及び各種セキュリティ機器等の更新を２０２２年１月に予定しています。

ＩＣＴインフラ及びセキュリティ環境を一括で更新することにより、管理の一元化や運用の効率化を図るため、新しい技術及びコスト、実現方法などの調査・検討を進めています。

本情報提供依頼は、これらの調査・検討を進めるにあたり、次期ＩＣＴインフラ及びセキュリティに求める機能、当該機能を実現させるための方法、全体構成、機器構成、運用想定、コスト等について、事業者などから広く意見を収集し、今後実施を予定している調達仕様書作成の際に参考情報として活用させていただくため、積極的な情報提供を求めるものです。

2 現状と課題

2.1 現状の概要

2.1.1 現状の契約形態

本市は、基幹システムを中心とした複数の電算システムと運用を包括的に１０年間の契約で委託しており、ＩＣＴインフラ及びセキュリティの多くもこの委託契約に含まれています。

この契約は、サービス提供型の委託契約であり、インフラ資産は本市の資産ではなく、機能及びパフォーマンスの提供を受ける契約を締結しています。

次期契約についてもサービス提供型の契約を想定しています。

2.1.2 庁内ネットワーク

①各拠点との接続方法

本市の庁内ネットワークは、本庁舎の他、３６ヵ所の拠点がビジネスイーサワイドにて接続しています。回線速度は使用状況に応じて１Ｍ～１００Ｍの設定です。

接続するためのネットワーク機器は、本庁舎はＬ３スイッチ、生涯学習センターはＬ２スイッチ、その他の拠点はルータを設置しています。

本庁舎と近接の東別館・西別館・分館は、光ケーブルでの接続です。

②本庁舎及び別館等の機器

フロア又は部署毎にＬ２スイッチを設置しており、市民課・国保年金課・課税課・収税課の各Ｌ２スイッチは冗長化しています。

スイッチはサーバ室も含め、Ｌ３スイッチ２台（冗長化）、Ｌ２スイッチ２０台の設置です。

③論理分離とアクセス制御

情報セキュリティ強靭化へ対応するために、個人番号利用事務・ＬＧＷＡＮ・インターネットの３系統に論理分離しています。

それぞれのセグメントのアクセス制御は、スイッチのＡＣＬにて実施しています。

2.1.3 仮想基盤及び物理サーバ等

①仮想基盤

現在使用している仮想基盤は、主にセキュリティを担うもの（インターネット閲覧用ＲＤＳを含む)、シンクライアント用、各種業務システム用の３種類があり、全て VMware 製ですがそれぞれが独立したハイパーバイザーとなっています。

このうち各種業務システム用の仮想基盤は、２０２０年３月に機器更改を行い、VMware と Oracle 用の２種類のハイパーバイザーに分割する予定です。

２０２５年３月にこの仮想基盤は本事業に集約する予定です。

②物理サーバ

現在、物理サーバにて運用している業務システムは次のとおりです。

・外部メール、ＤＮＳ（１台）
・メール無害化システム（１台）
・ＬＧＷＡＮ用ゲート（１台）
・ファイルサーバ（２台）

③ファイルサーバ

本番環境と複製環境の２台構成です。共有スペースの実効容量は、9.32TB あり、2.45TB 使用済です。

各部署には基本的に 10GB のクォータで制限しており、各課の運用状況に応じて必要な容量を増加しています。

④ファイヤーウォール

インターネット接続用のファイヤーウォールは２台で冗長化しています。

直接インターネットを接続されておらず、セキュリティクラウドへ接続しています。

2.1.4 端末及びプリンタ

現在使用している端末及びプリンタの内訳は次のとおりです。

①パソコン（1,480 台）

	個人番号利用系	LGWAN 系	ｲﾝﾀｰﾈｯﾄ系	予備	計
ＦＡＴ端末	185 台	568 台	140 台	－	893 台
ｼﾝｸﾗｲｱﾝﾄ	158 台	416 台	－	－	574 台
予備機	－	－	－	13 台	13 台
計	343 台	984 台	140 台	13 台	1,480 台

ＬＧＷＡＮ系からインターネットに接続するためのＲＤＳが 1,000 ライセンスあります。

②プリンタ（計 206 台）

・レーザープリンタ…206 台

・プリンタサーバ…18 台

※プリンタのＵＳＢ又はパラレルポートをＬＡＮに変換する機器

2.1.5 システム及びソフトウェア

現在のインフラ及びセキュリティ関連で使用しているシステム等は次のとおりです。(セキュリティに関連する事項のため詳細は非公開)

①Ｗｅｂセキュリティ対策・プロキシ（上位）

Ｗｅｂ経由で感染する不正なプログラムをブロックし、また危険なＷｅｂサイトへのアクセスもブロックしています。

②Ｗｅｂフィルタリング・プロキシ（下位）

Ｗｅｂフィルタリング、アクセスログ、ＰＯＳＴログ、ＳＳＬ通信の可視化などの機能を使用しています。

③メールウイルス対策

スパムメール、標的型メールなどをブロックしています。

④メール無害化

受診するメールの添付ファイルの削除及び HTML メールのテキスト化の機能を使用しています。

送信メールのセキュリティ対策の機能は使用していません。

⑤ウイルス対策（クライアント）

リアルタイム検索及び予約検索により、各端末及びサーバのウイルス対策を実施しています。

⑥WSUS

Windows Update の管理を行っています。

⑦二要素認証・暗号化・持出制御

ＩＣカードによる認証基盤を導入し、二要素認証、ファイル暗号化、ＵＳＢデバイスによる持出制御を実施しています。

⑧その他未導入のシステム

現在、資産管理、ファイル無害化、常時暗号化については未導入です。

2.1.6 管理及び運用方法

①ネットワーク

Ｌ３、Ｌ２スイッチについては、基幹システムの包括委託契約に含まれており受託者が保守を行っています。ルータについては、別途契約ですが同じ受託者が保守を行っています。

設定変更は職員で行うことができず、必要に応じてその都度別途契約を行い有償で設定変更を依頼しています。

②仮想基盤

業務システム用の仮想基盤については、職員が管理及び運用を行っています。新たな仮想マシンの作成は、テンプレートからのデプロイ又はリソ

ースの割り当て等の設定から行っています。

職員が基本的な設定の仮想サーバを作成後に各業務システムのベンダーがシステムの構築を行っています。

データベースのバックアップの設定は、各業務システムベンダーが行っています。各仮想マシンのバックアップは、職員が手動で行っています。仮想基盤全体のバックアップは実施していません。

セキュリティ用及びシンクライアント用については、職員は監視以外の運用を殆ど行っていません。

③端末及びプリンタ

基幹システムの包括委託契約に含まれているため、受託者が保守を行っています。ＡＤによる端末管理も同受託者により実施しています。

各端末へのソフトウェアのインストールや設定変更、移動などの運用は情報政策課の職員が行っています。

職員の過失による端末の破損、プリンタの有償交換部品、トナーカートリッジについては、市が費用を負担しています。

障害時の一次切り分けは情報政策課の職員が行っており、この結果に基づいて保守を依頼する場合と、一次切り分けでは判明できなかった障害について調査を含めて保守を依頼する場合があります。

④セキュリティ関連

基幹システムの包括委託契約により提供されていますが、監視を含めて運用は情報政策課の職員が行っています。プログラムプロダクト、メーカーへの問い合わせ等の保守は受託者が行っています。

2.1.7 構築ベンダーによる仮想基盤の保守業務

構築ベンダーは２社あり、セキュリティ用とシンクライアント用の仮想基盤は、基幹システムの契約に保守が含まれています。業務システム用仮想基盤は、別途保守契約を締結しています。保守業務の内容は次のとおりです。

①ハードウェアの障害対応

②VMware 製品の障害対応

③定期的なログの取得と確認

④バックアップ用ソフトウェアの障害対応（業務システムの仮想基盤のみ）

⑤操作方法等の運用サポート（業務システムの仮想基盤のみ）

2.2 次期システムにおける課題

2.2.1 ＨＣＩの導入による高集約化

現在３つに分かれている仮想基盤の全てを効率的に集約するため次期システムでは、ＨＣＩによる更なる高集約化と管理面の向上を目指す必要があります。

１０年間の運用において、ハードウェアの増強の必要性も出てくる可能性があることから、拡張性の高い構成にする必要があります。

2.2.2 ネットワークの論理分離

社会保障・税番号制度の導入により、現在の庁内ネットワークは、個人番号利用事務系・ＬＧＷＡＮ系・インターネット系の３系統に分離されています。それぞれの系統間のアクセス制御は、Ｌ３、Ｌ２スイッチに膨大なＡＣＬを設定して行っていますが、軽微な修正も保守業者への作業依頼となることから運用上の課題となっています。

また、Ｌ３、Ｌ２スイッチに記述しているＡＣＬの数も限界値に迫っているため、次期システムでは抜本的な対策が必要となります。

2.2.3 多数のセグメント管理

３系統のネットワーク分離により、用途ごと及び施設、フロアごとに多数のセグメントが必要になります。現在は総数で概ね１３０種類のセグメントですが、再設計及び集約化による約１００種類まで減少できる想定です。

サーバ室のネットワーク機器及び出先機関のルータは、軽微な設定変更などを職員が実施できるよう機種を選定する必要があります。

2.2.4 業務システム用仮想基盤の集約

２０２５年３月には業務システム用の仮想基盤を集約する必要があり、この時期に合わせて仮想基盤のハードウェアの増強を行う必要があります。

全体的なサイジングについては、各種システム、ソフトウェア、シンクライアントの構成により大きく変わるため、現時点では概要を示すことはできません。各種システム・ソフトウェアの集約化、シンクライアント端末のパフォーマンス等を考慮してリソースの積算をしてください。

2.2.5 限られたスペースでの機器更新

現状の仮想基盤及びサーバは、３６Ｕラック２台、４４Ｕラック１台に搭載されており、３６Ｕラックは２４Ｕ、２８Ｕのスペースを、４４Ｕラックは２２Ｕのスペースをそれぞれ占めています。３６Ｕラックの空スペースはそれぞれ１２Ｕ、８Ｕありますが、まとまったスペースではありません。

別の３６Ｕラックで今後空スペースが出る想定ですが、３６Ｕラックでは１６Ｕ程度の空きスペースとなる予定です。４４Ｕラックでは２２Ｕのまとまった空きスペースが確保できる予定です。

新たなサーバラックを設置することは不可能ではありませんが、サーバ室のレイアウト、エアフロー、電源工事などについて検討及び積算が必要になります。

限られたスペースでの機器更新作業が必要となります。

2.2.6 各種システム・ソフトウェアの集約

各種システム・アプリケーションについては、現状に捕らわれず効率的な管理のために統合パッケージを活用するなど集約化を検討してください。ただし、それぞれのソフトウェア等の優れた部分を活かすために有用であれば、統合にこだわる必要はありません。

機能及び管理面からバランスの良いシステム構築が課題となります。

2.2.7 運用コストの低減

ネットワーク機器やＡＤは、運用上軽微な設定変更を職員が行えず、有償にて作業依頼を行うケースが多くあります。

軽微な変更作業や日々の運用を職員が行うことで、費用の削減や契約手続の省略により安価でかつスピーディに運用することができます。

作業の役割分担、責任分界点、最新方法の管理などを検討する必要があります

3 事業概要

3.1 事業計画の範囲

3.1.1 業務内容及び範囲

本ＲＦＩにおける業務内容及び範囲は次のとおりです。

①庁内ネットワーク機器の調達（本庁及び出先機関）

②庁内ネットワークの構成の見直し及び設計

③仮想基盤の機器調達

④仮想基盤の構築・テスト

⑤業務システム用の仮想基盤の集約・移行（２０２５年３月実施）

⑥外部用メールサーバ及びＤＮＳサーバ構築

⑦セキュリティ環境の構築

ファイヤーウォール、プロキシ、Ｗｅｂフィルタリング、メールフィルタリング、Ｗｅｂセキュリティ、クライアントウイルス対策、インターネット無害化、メール無害化、二要素認証、常時暗号化、ファイル持出制御の機能を想定しています。

⑧ＦＡＴ端末・プリンタ調達及び設置

現状と同等の想定台数は、ＦＡＴ端末９２０台、プリンタ２１０台です。

⑨シンクライアントの構築（６００台）

現状と同等の数は、６００台の想定ですが、シンクライアント及びＦＡＴ端末の数は、構成により大きく変動するとものと考えます。全職員に仮想デスクトップを割り当てる方式も検討が必要です。

⑩端末管理（ＡＤ構築、WSUS、資産管理）

⑪ファイルサーバ

⑫ＬＧＷＡＮ接続機器（ファイヤーウォール、ゲート用サーバ）

⑬情報管理部門の職員向け操作研修

⑭運用保守

仮想基盤、ハードウェア保守、プログラムプロダクト保守、運用サポートを想定しています。

⑮旧機器の撤去・保管（処分は含まない）

3.1.2 契約形態及び期間

①契約形態

サービス提供型の委託契約を想定しています。

本事業に求めるサービスは、機器の提供、ソフトウェア製品の提供、ライセンスの提供、品質（パフォーマンス)、保守サービスであり、要件を満たせばどのように構築するかはベンダーのノウハウによります。

１０年間の安定稼働のために適切な時期にハードウェアのリプレースが必要となりますが、時期・手法について指定はなく、市と協議のうえ決定します。

②契約期間及びサービス提供期間

契約期間　　２０２０年８月頃　～２０３１年１２月３１日

サービス提供期間　２０２２年１月１日～２０３１年１２月３１日

3.1.3 運用想定

①一般職員の利用方法

一般職員が利用するものは、オフィスソフト、グループウェア等の内部システム、無害化されたインターネット上のＷｅｂページの閲覧、ファイルサーバ、基幹システム、各部署で導入した個別業務システムなどです。

二要素認証による端末へのログインを行い、データの持ち出しは制限され、管理職又は情報管理部門の許可のもと持ち出しが許可されます。

ファイルやデータは、常時又は適宜暗号化され、外部へ持ち出したりメールに添付して送信するときは、手動で復号する必要があります。

②情報管理部門の職員による運用

情報管理部門の職員は、システム管理者としての運用を行います。具体的には、リモートによる端末の管理、ＡＤの運用（簡易的)、WSUS の運用、資産管理、軽微なネットワークの設定変更、仮想基盤の監視（簡易的)、仮想マシンの作成及び削除、ウイルス対策等各種セキュリティシステムの管理、障害の一次切り分け（簡易的）などです。

情報管理部門の職員が運用しやすい環境の構築が必要になります。

なお、職員が変更した設定情報については、ベンダーと情報共有し常に最新の状態に保つ必要があります。

3.2 導入スケジュール想定

本ＲＦＩの実施後、事業費用を積算し予算要求行いプロポーザルにて受託業者を決定する予定です。

①２０１９年　４月　　本ＲＦＩの発行

②２０１９年１１月　　事業費の概算積算及び予算要求（債務負担行為）

③２０２０年　４月　　プロポーザルによる受託者の選定

④２０２０年　７月　　事業費の精査及び契約額の決定

⑤２０２０年　８月　　委託契約・要件定義・設計・構築開始

⑥２０２２年　１月　　サービス提供開始・運用開始

3.3 業務にかる要件

3.3.1 ネットワーク

①共通

庁内ＬＡＮは、個人番号利用事務系・ＬＧＷＡＮ系・インター-ネット系の大きく３系統のネットワークに論理分離しています。

ＩＰアドレスの第一オクテットは、全て共通で１種類のみですが、消防関係は専用アドレス体系になっていますので合計２種類です。

論理分離した３系統のネットワークは、第２オクテットで分類し、スイッチのＡＣＬでアクセス制御をしています。

建物やフロア毎に第３オクテットで分類しています。

一部の端末やプリンタでは、ネットワーク分離前のアドレスを持っているものがありますが、次期システムの導入時に解消する必要があります。

スイッチ、ルータ、ファイヤーウォール等の機器は、職員が監視及び軽微な設定変更を行えるよう WebGUI やログのバックアップ等の機能を考慮してください。

②本庁舎・議会棟

本庁舎は地下１階～２階までの３フロアにＬＡＮを敷設しています。

議会棟は、１階と２階にＬＡＮを敷設していますが、スイッチは２階のみに設置しています。議会棟のＬＡＮの幹線は、本庁舎２階のＬ２スイッチから引いています。

本庁舎２階のＬ２スイッチは１台のみですが、１階は各部署に設置し冗長化しています。

地階は、情報政策課に管理用のＬ３スイッチ（冗長化）及びＬ２スイッチを設置しています。

本庁舎及び議会棟では、Ｌ３スイッチ２台、Ｌ２スイッチ１２台の計１４台設置しています。

必要なスイッチの種類と数量を積算し、上記「①共通」に記載の３系統の分離を考慮したネットワーク体系の構築が必要です。

③東別館

東別館は本庁舎と光ケーブルによって接続しています。Ｌ２スイッチを１台設置しており、１階及び２階は共通のセグメントです。

Ｌ２スイッチ及び３系統のネットワーク分離が必要です。

④西別館

西別館は本庁舎と光ケーブルによって接続しています。１～４階の各フロアにＬ２スイッチを１台ずつ設置しており、１～２階が同一セグメント、３～４階が同一セグメントになっています。

Ｌ２スイッチ及び３系統のネットワーク分離が必要です。

⑤分館

分館は本庁舎と光ケーブルによって接続しています。Ｌ２スイッチを１台設置しており、１階及び２階は共通のセグメントです。

Ｌ２スイッチ及び３系統のネットワーク分離が必要です。

⑥生涯学習センター（アビスタ）

生涯学習センター（アビスタ）は、公民館と図書館の複合施設です。ビジネスイーサワイドによって庁内ＬＡＮと接続しています。

Ｌ２スイッチを１台設置しており、公民館と図書館でセグメントを分けています。

Ｌ２スイッチ及び３系統のネットワーク分離が必要です。

⑦消防本部・消防署・指令センター

消防関係の部署は、本庁とは異なる独自のアドレス体系になっていますが、他の拠点と同様に庁内ＬＡＮに接続できます。

消防本部、つくし野分署、東消防署、湖北分署、指令センターの５ヵ所の拠点があり、拠点毎にセグメントが分かれています。

Ｌ２スイッチは設置しておらずルータのみの設置です。

ルータ及び３系統のネットワーク分離が必要です。

⑧出先機関・拠点

その他の出先機関等は、保育園、子育て支援施設、行政サービスセンター、教育委員会、クリーンセンター、保健センター、体育館、博物館・文化関連施設、障害者支援施設、図書館分館、地区公民館など２８ヵ所にルータを設置しています。Ｌ２スイッチは設置していません。

ビジネスイーサワードによって庁内ＬＡＮと接続していますが、回線速度は、業務の規模により１Mbps・１０Mbps・１００Mbpsがそれぞれ設定されています。

拠点毎に固有のセグメントを設定しており、フロア毎に分割している場所はありません。

全ての拠点にルータが必要ですが、ネットワーク分離の数が３系統必要なく２系統のみで足りる拠点もありますが、将来的に３系統必要になる可能性があるため、設計思想には入れておく必要があります。

⑧運用

コアスイッチ、各フロアスイッチ、ＵＴＭなどによるアクセス制御については、軽微な設定変更であれば職員が実施する想定です。

各種スイッチ、ルータ、ファイヤーウォールの機器は、ＡＣＬの確認及び軽微な変更等を行うため、ＧＵＩ機能を備えた製品を選定する必要があります。

3.3.2 仮想基盤

①システム用

現行では主にセキュリティを担っているシステムの仮想マシンを構築するためのクラスタが必要です。サイジングに関しては、これらのシステムの構成が大きく影響するので、提供するシステムと合わせて検討が必要です。

②シンクライアント用

シンクライアントの台数は、現状と同等の場合６００台の想定です。Office などのアプリケーションや業務システムなどをインストールできる容量と快適に利用できる処理速度を実現するためのリソースが必要です。

ファイルサーバには格納しない利用者の個人的なデータ等を仮想マシン固有の領域に保存する必要がありますが、１台あたり数ＧＢあれば問題ありません。

現状の構成にかかわらず、全職員に専用の仮想デスクトップの構成を積極的に検討してください。

③２０２５年３月増設用

各種業務システムを運用している仮想基盤の機器更改を２０２０年３月に予定しています。この仮想基盤では５０台程度の仮想マシンを運用する想定をしており、本機器の５年リース満了後の２０２５年３月にＩＣＴインフラ基盤に集約する予定です。

サイジングについては、２０１９年６月に決定します。

④Oracle 用ハイパーバイザ

２０２０年３月に機器更改の仮想基盤は、Oracle 用のハイパーバイザを別途構築します。Oracle を使用するサーバの最終的な台数は不明ですが、６～１０台を想定しています。

サイジングについては、上記「③２０２５年３月増設用」と合わせて２０１９年６月に決定します。

⑤全体構成

上記①～④について複数のクラスタ及びハイパーバイザが必要となる想定です。ＨＣＩでの構築により機器構成やラックへの搭載の煩雑さを減少し長期間の安定稼働ができるよう、十分な能力、拡張性、可用性を実現する必要があります。

3.3.3 外部メールサーバ及びＤＮＳサーバ（ＤＭＺ）

現在は、外部メールとＤＮＳは１台の物理サーバで兼用しています。このサーバでセキュリティチェックなどは行っていません。

インターネットへ接続していくため、県のセキュリティクラウドへとリレー、フォワードする必要があります。

3.3.4 セキュリティ

次のセキュリティ環境を実現する必要がありますが、同様の機能、安全性を確保できる構成であるならば、どのような組み合わせでも可とします。また、複数の機能を統合したパッケージでの構成でも問題ありません。

①ファイヤーウォール

インターネットへ接続するために必要な機器です。現在は FORTINET 社製の機器にて冗長化しています。

インターネットは、県セキュリティクラウドを経由して接続しているため、県セキュリティクラウドが提供するファイヤーウォールに接続します。

②プロキシ、Ｗｅｂフィルタリング

インターネットアクセスにおけるＷｅｂフィルタリングの機能です。

カテゴリによるブロック、ホワイトリストによる許可、ＳＳＬのデコード、アクセスログ管理などの機能が必要です。

現在使用しているＷｅｂフィルタリングシステムは、Ｗｅｂウイルス対策の機能はありません。下位プロキシとして使用しています。

④メールフィルタリング

外部から送信される、スパム、標的型、フィッシング等のメールをブロックします。

現在使用しているシステムでは、添付ファイルの削除やサニタイズなど無害化の機能はありません。

⑤Ｗｅｂセキュリティ

ウイルス対策及びスパイウェア対策として、不正プログラムの防止、不正な通信のブロックを行います。上位プロキシとして使用しています。

⑥クライアントウイルス対策

庁内ＬＡＮに接続する全てのパソコン及び一部の業務システムサーバにウイルス対策ソフトをインストールします。

管理サーバから監視を行い、各種クライアントの設定の管理も行います。

パターンファイルやアップデートの入手は、J-Lis が提供する情報セキュリティ向上プラットフォーム（LGWAN-ASP）から行います。

⑦インターネット無害化

直接インターネットと通信しない方式でブラウザを無害化するのであればどのような方式でもかまいません。

現在は、ＲＤＳを使用し InternetExplorer の画面転送を行い、ファイルのアップロードを制限しています。

ＲＤＳは現在デバイスＣＡＬで 1,000 ライセンス保有し、仮想基盤でホスト６台、セッションブローカー２台（ＶＭ）、セッションホスト２０台（ＶＭ）によるＲＤＳ専用のクラスタで運用しています。

なお、この他、ＦＡＴ端末約１３０台をインターネット専用パソコンとして使用しています。

⑧メール無害化

現在、インターネットからのメールに対して、HTML のテキスト化及び添付ファイルの削除を行っています。

添付ファイルのサニタイズやウイルスチェックは実現しておらず次期システムにおける課題となります。

⑨サニタイズによるファイル無害化

インターネットからのファイルのダウンロードやメールの添付ファイルの無害化について、現在サニタイズは実現していません。次期システムでは、サニタイズによるファイルの無害化を実現したいと考えています。

⑩二要素認証

現在はＩＣカードを用いた二要素認証を導入しています。次期システムでは、指紋・静脈・顔などのバイオメトリクス認証やワンタイムパスワード等を利用した認証など幅広く検討する必要があります。

機能として重要なことは、運用面において各職員によるキー情報の管理が煩雑でないこと、ログイン時のトラブルが少ないこと、なりすましが困難であること、情報管理部門による監視・管理が煩雑でないことなどが課題となります。

⑪常時暗号化

現在は二要素認証用のアプリケーションの機能を利用し、端末内の指定した場所の暗号化を行っています。

端末全体の暗号化及びファイルサーバの暗号化が課題となっているためこの機能の実現を検討してください。

なお、リンク先のファイルや設定ファイルなどが暗号化され読み込めないなどの問題が生じないよう考慮が必要です。

⑫ファイル持出制御

現在は二要素認証用のアプリケーションの機能を利用し、ＩＣカードの権限による外部媒体へのデータの持ち出し制御を行っています。

個人番号利用事務系の端末は、情報管理部門の承認のもとファイルの持ち出しを行う運用が必要になるため、この承認手順が煩雑になりすぎないよう検討が必要です。

ＬＧＷＡＮ系の端末は､一般職員は自由にファイルの持ち出しができず、所属長の承認のもと持ち出しを行う運用となります。

これらの承認の行為は、必ずしもオンラインで実施する必要はなく、記録簿などによる対応も可能ですが、確実な履歴管理の観点からオンライン化が望ましいと考えます。

3.3.5 バックアップ要件

各種サーバは、その用途により最新の Config だけあれば良いもの、日次バックアップが必要なものなど様々です。障害の復旧を考慮し適切なバックアップを行う必要があります。

各機器の構成により効率的なバックアップの方法が異なります。

バックアップの頻度やかかる時間、容量などについても十分に考慮してください。

3.3.6 端末導入及び管理

①全体共通

端末の数量については、上記「3.1.1 業務内容及び範囲」に示す内容が前提となりますが、個人番号利用事務系とＬＧＷＡＮ系の端末の併設が不要な場合は数量が減らせます。

また、職員１人に１つの仮想デスクトップで構築する場合は、端末の殆どがシンクライアントとなり、ＦＡＴ端末でしかできない作業のための共用端末をわずかに設置するようになります。パソコンを使用する職員の総数は 1,300 名程度の想定です。

全体の構成次第では、ほぼ全てをシンクライアント化し、リモートでのデータ移動を制限することで端末の併設をなくし、職員が庁内のどこでも個人専用のデスクトップを使用できる環境にすることも可能と考えます。

実現方法は多種多様なため、現時点で要件は限定しません。効率的で画期的な提案が可能であれば、仕様として採用を積極的に検討します。

全台シンクライアント化する場合の要件は明示できませんが、参考として現状と同等の構成とした場合の要件を下記に記載します。

②ＦＡＴ端末

必要なＦＡＴ端末の台数は９２０台の想定です。個人番号利用事務系とＬＧＷＡＮ系と併設する場合は、デスクトップ切替器が必要になるためコンパクトタイプのデスクトップパソコンが必要になります。

併設する必要がない場合は切替器が不要になるのでノートパソコンで問題ありません。

③プリンタ

モノクロのレーザープリンタは、２１０台必要となる想定です。全て共通のリサイクルトナーを使用して運用することが望ましいです。

サーバ室に高速プリンタ（Ａ４ヨコ片面　５５頁/分以上の速度）１台の設置が必要です。

個人番号利用事務系とＬＧＷＡＮ系のどちらかのネットワークに接続しますが、両方のネットワークから印刷する必要がある場合は、２台設置せずにプリントサーバ(ＵＳＢ又はパラレル)による対応が必要です。

④シンクライアント

現行と同等の構成の場合、シンクライアントは６００台の想定ですが、構成により想定台数が大きく変わるものと思われます。

台数に捕らわれずに、職員１名につき１デスクトップの構成を積極的に検討してください。

⑤デスクトップ切替器

現在175個の切替器を利用しており、２台のデスクトップパソコンにおいて、モニター、キーボード、マウス、ＩＣカードリーダーを共用しています。

個人番号利用事務系とＬＧＷＡＮ系の端末が共用できない場合は、それぞれのハードウェアを併設し切替器による運用が必要になります。

⑥インターネット接続環境

現在は、ＬＧＷＡＮ系の端末からＲＤＳによる接続が1,000ライセンス、インターネット専用のノートパソコンが約１３０台あります。

各職員が専用のデスクトップを持ちＲＤＳ接続が可能な場合、インターネット専用のＦＡＴ端末は、７０台程度に削減できます。

インターネットからのファイルのダウンロードはＲＤＳで可能ですが、アップロードは、インターネット専用端末のみ可能とし、業務の端末から直接インターネットへのデータの送信等を制限する必要があります。

⑦Ative Directory

全ての端末がドメインに参加する必要があります。ＡＤは、個人番号利用事務系とＬＧＷＡＮ系にそれぞれ必要となり、共用する場合は特定通信に限定する必要があります。

運用は原則情報政策課の職員が行いますが、ベンダーによる障害対応や運用サポートが必要になります。

⑦資産管理

現在、端末及びソフトウェア等の管理ソフトは導入していません。

端末管理、監視、制御、資産管理の必要性は高く、セキュリティ機能などと合わせて検討する必要があります。

運用は職員により行う想定です。

⑧WSUS

WindowsUpdateはWSUSにて実施しています。ファイルの取得は、J-Lisが提供する情報セキュリティ向上プラットフォーム（LGWAN-ASP）から行います。

WSUSの運用は職員が行いますが、WSUSサーバの構築及び端末の登録、グルーピングなどの作業は、ベンダーが実施する想定です。

大容量のWindowsUpdateによる帯域の圧迫及びクライアントの適用時間の長時間化への対応策も考慮する必要があります。

⑨ハードウェア保守

故障等の障害対応のオンサイト保守が必要です。障害の一時切り分けは情報政策課職員で行う想定です。ノートパソコンのバッテリーやプリンタの定期交換部品等の有償交換については費用の積算の不要です。

3.3.7 ファイルサーバ

①ＬＧＷＡＮ系

現在利用しているファイルサーバの実効容量は約 9.3TB あり、約 2.7TB を使用しています。2 台で冗長化しておりリアルタイムで同期してします。

スナップショットを有効にしており各職員が過去のファイルを復元することができます。

部署毎にクオータを設定しており、基本 10GB を割り当て部署により必要に応じた容量を追加で割り当てます。

②個人番号利用事務系

現在利用している個人番号利用事務系のファイルサーバは、QNAP 製のＮＡＳを使用しています。実効容量は 1.82TB で使用容量は 160GB です。

部署毎にユーザーを作成し、20GB のクオータを設定しています。

スナップショットは有効にしていません。

ＮＡＳにＵＳＢの外付けハードディスクを接続し日次バックアップを取っています。

実効容量は十分ですが、可用性に問題があります。またスナップショットが無効のためデータの復元にも課題があり、次期システムではこれらの課題をクリアする必要があります。

3.3.8 ＬＧＷＡＮ接続機器

現行のＬＧＷＡＮ接続機器は、ゲート用サーバ１台及びファイヤーウォール１台の構成です。現行機種は２０１９年１月～２０２３年１２月末までリースにより運用するため、２０２４年１月から組み入れる必要があります。

２０２４年１月には、第５次ＬＧＷＡＮへの対応が必要となる想定です。回線の冗長化に合わせ、ファイヤーウォールの冗長化が必要になります。

ルータの費用については、現状の回線契約に含まれているため、次期システムでも積算に含める必要はありません。

3.3.9 データ移行

①ＦＡＴ端末

ＦＡＴ端末は各職員がデータの移行を行いますので、積算に含める必要はありません。

②シンクライアント

シンクライアントの個人用データの保管スペースは、ネットワークドライブで接続しています。

データ移行を行うか、一定期間旧環境に接続できるようにして職員が移行できる環境への対応が必要になります。

③ファイルサーバ

ファイルサーバ内のデータは全て移行が必要になります。

ＬＧＷＡＮ系及び個人番号利用事務系の両方のファイルサーバのデータを移行する必要があります。

④仮想基盤

上記「3.3.2 仮想基盤　①システム用」に記載のものは、再設計、再調達になるためサーバの移行は不要です。

「3.3.2 仮想基盤　③２０２５年３月増設用」に記載の仮想基盤については、全てのサーバの移行が必要です。

「3.3.2 仮想基盤　④Oracle 用ハイパーバイザ」については、現時点では、全てのサーバの移行が必要な想定で積算してください。ただし、仮想基盤での Oracle の運用はコストの増大を招く可能性があるため､本事業には含めずに物理サーバで運用する可能性があります。

3.3.10 旧機器の撤去及び保管

現行契約の機器は既存ベンダーに返却となるため、一定期間専用の保管場所の確保が必要です｡このスペースを市役所内に確保することは困難なため、旧機器の撤去及び保管にかかる費用を積算してください。

保管する期間は、機器の入替作業にかかる日程によるため、十分な期間を想定してください。

機器の処分費は、現行契約のベンダーの負担となるため積算は不要です。

3.4 保守業務の要件

本事業の契約は、サービス提供型の委託契約となる想定です。機器の納入及び構築の他、保守業務が契約範囲に含まれます。

①ハードウェア保守

納入した機器が故障した際にオンサイトによる修理対応をしてください。

職員の過失による故障は保守の対象外になります。

②ソフトウェア保守

プログラムプロダクト保守を行ってください。

必要性に応じたバージョンアップ等の作業を含みます。

③定期メンテナンス保守（年数回、エラーログ、イベント等の調査）

仮想基盤については、定期的にチェックし必要に応じ予防保守やチューニングを実施する必要があります。

④運用サポート（随時）

情報政策課の職員が運用を行うため、導入したソフトウェアの操作方法や効率的な運用等について問い合わせを行う場合があります。

これらの運用サポートの費用を積算してください。

⑤各種設定情報の管理と共有

ネットワークの設定、端末のグループポリシー、仮想基盤上の仮想マシンの追加等について、職員による運用を行うことから、事前事後に設定情報などを相互に共有する必要があります。

常に最新の情報を相互で管理することで、障害の切り分けや現状復旧に活かすほか、設定変更による事前のリスク検証にも役立てます。

⑥メーカーへの技術的問い合わせ等

導入した機器やアプリケーションについて、仕様、不具合等に関する問い合わせが必要になる場合があります。

⑦その他障害対応

障害発生時は、まず職員が一次切り分けを行います。障害箇所の特定に至った場合、その内容に応じた障害対応を実施していただきます。

一次切り分けができない場合や原因箇所の特定が困難な場合は、必要な調査を実施する必要があります。

3.5 担当者説明・教育の実施

運用に関する各種手順書を作成し、情報政策課職員への研修を実施してください。情報政策課職員のうち研修が必要人数は７名です。

端末操作に関して利用する一般の職員に説明が必要な場合は、全体説明会の実施を想定してください。なお、会場準備に関する費用の積算は不要です。

4 依頼内容

4.1 全体スケジュール

契約後から契約終了までを期間とし、要件定義、設計、機器調達、構築、運用開始、リプレースなどを記載した資料を作成してください。

4.2 構成概要

上記「3.1.1 業務内容及び範囲」に記載の業務の実施に必要な全ての機器に関して、それぞれ必要な構成資料として次のものを作成してください。

端末環境に関しては、どこまでシンクライアント化を進めるか、インターネット接続環境をどのように実現するかの自由度が高いため、運用及びコストの両面からバランスのよい構成を検討してください。

○ネットワーク構成図

○物理構成図

○ライセンス一覧

○参考機器構成表

4.3 概算見積

契約方法がサービス提供型の委託契約を想定しているため、イニシャルコスト及びランニングコストの区分はなく、全てのコストを含めた平準化した金額にしてください。ただし、契約開始後に遅れて導入する機器や業務については、そのサービスの提供時期から金額に反映させてください。

概算見積には次の内容を記載してください。なお、１０年間のサービス提供期間のため、殆どの機器及びライセンスの再調達が必要となる想定です。

①業務毎のサービス提供費用

上記「3.1.1 業務内容及び範囲」を参考に業務毎に区分してください。

「別紙１参考見積様式」を参考に作成してください。

②契約範囲に含めない業務

プリンタの消耗品や職員の瑕疵による機器破損の修理については契約範囲外となる想定です。

市側の都合による機器等の設定変更依頼のうち保守の範囲で実施できない作業は別途契約となる想定です。保守の範囲内でできる作業及び別途契約となる作業について基準となる考え方を示してください。

③エンジニアの作業単価

上記「②契約範囲に含めない業務」に記載の別途契約にて作業を依頼する際にかかる技術者の単価を示してください。

4.4 運用想定

①情報政策課職員による運用想定

日々の管理系の業務は情報政策課の職員が運用を行う想定です。

情報監視室職員が実施する必要のある作業を示してください。

②受託者の体制とサポート内容

運用開始後における受託者のサポート体制と運用サポートの内容を示してください。

③責任分界点

構築時から運用開始後まで契約全体の中で、市が責任を持ち実施すべき事項などを示してください。

5 情報等の取扱い

本ＲＦＩにおいて、提供を受けた情報及び資料は次のとおり取り扱うものとします。

①本ＲＦＩは、我孫子市庁内ＩＣＴインフラ及びセキュリティ環境提供業務に関する実現性を確認するために必要な技術、予算規模、運用方法等について、広く情報を得るための手段としたものであり、契約を前提としたものではありませんので御了承ください。

②資料の提供にあたっては、既存の提案資料、パンフレット等をご活用いただいて構いません。

③情報の提供を受けた事業者等に対し、後日、担当課から提出された資料等の内容等について照会又は追加の資料提供を依頼する場合があります。

④資料についてご説明を行っていただける場合は、事前にご連絡をお願いいたします。

⑤本ＲＦＩに関して、担当課へのヒアリングをご希望される場合は、事前にご連絡をお願いいたします。

⑥ご提供いただいた情報については、本市で使用するものであり、提供者に断りなく第三者への配布、結果の公表等は行いません。ただし、提供を受けた提案、資料等については、今後実施を予定するプロポーザル等の仕様に反映する場合があります。

⑦本情報提供依頼に係る資料の作成、提出等に要する費用は提供者のご負担でお願いいたします。

⑧ご提供していただいた情報・資料につきましては、返却致しません。

6 資料の提出方法等

6.1 資料の形式

資料については、Ａ４サイズまたはＡ３サイズの書類により２部提供するほか、同内容を記録した電子媒体（ＣＤ－Ｒ又はＤＶＤ－Ｒなど）を併せて、「8 資料の提出先」に記載する提出先に提出社名又は機関等の名称、担当者氏名、担当者連絡先を明記し提出してください。

なお、電子媒体によるファイル形式は「Microsoft Word」、「Microsoft Excel」、「Microsoft Power Point」（カタログ等を添付する場合は、ＰＤＦ形式による提出も可）で修正可能なファイル形式で作成してください。

6.2 提出期限

平成３１年７月１日（月）１７時必着

持参または郵送により提出してください。

7 本ＲＦＩに関する質問及び回答

7.1 質問方法

①様式１号の質問書に記載し、「8 資料の提出先」あてにメールにてお問い合わせください。

②件名：「庁内ＩＣＴインフラ及びセキュリティのＲＦＩに関する質問」

③郵送及びＦＡＸは不可とします。

7.2 質問受付期間

平成３１年４月１０日（水）～平成３１年６月７日（金）１７時

平成３１年６月１７日（月）までに個別に回答します。

8 資料の提出先

我孫子市総務部情報政策課　　担当 沖

〒２７０－１１９２ 千葉県我孫子市我孫子１８５８番地

電話：０４－７１８５－１１１１（内線２９３）

E-Mail：kasoukiban@city.abiko.chiba.jp