【資料1－2 】

群馬県社会福祉協議会

ネットワーク構築・運用保守業務仕様書

令和4年12月

社会福祉法人　群馬県社会福祉協議会

目次

1　業務内容

(1)業務名　群馬県社会福祉協議会クラウトによるネットワーク構築・運用保守業務

(2)履行期限

運用開始は令和5年4月1日とする。

(3)履行場所

群馬県社会福祉協議会

2 現行ネットワークの課題

(1)ファイルサーバーの耐用年数、データ容量、OS(Windows サーバー2012)の問題

・現行のファイルサーバーが耐用年数の5年を償却してしまっている状態(現在8年目)で故障等のリスクが高くなっている。

・事務所内のデータ容量がサーバー本体の容量を超えているため、別途課によってはNASにわけて保存している状態で、今後も増え続けるデータに合わせた容量が必要となる。

・令和5年10月で現 Windows サーバー2012 のサポート終了となるため、それまでに新たなネットワークの構築、現サーバーからの移行を完了しなければならないこと。

(2)ファイルサーバーでは定期的な入替による費用が必要

現行のファイルサーバーによるネットワーク管理では、5年で新たにサーバーの入れ替え、再構築、移行に多額の費用が必要となること。

(3)ウィルスやスパイウェア等対策、近年の動向に合わせたセキュリティ管理体制

ウィルスやスパイウェア等対策、近年の動向に合わせたセキュリティ管理体制を構築する必要があること(ウィルス等に感染しないための対策)。

(4)災害やウィルス感染等によるデータ破損といった障害等によるデータ損失に伴う影響

災害やウィルス感染等によるデータ破損といった障害等によるデータ損失に伴う影響を最小限にするため、データの保全と運用保守、業務復旧に関する適切なバックアップ機能を有する必要があること。

バックアップの現状は、毎日 0 時更新、毎週日曜日 0 時更新で 2 回バックアップをとっているが、ウィルス等に感染したことが数日後に判明した場合、前日と1週間前だけでは不安である。

(5)在宅ワークの推進

在宅ワークの推進等、柔軟なネット環境に対応できるもの

3 システム要件

各要件から機器のサイジングを行い経費的に過剰にならず最適なハードウェア機器、ソフトウェア構成を提案すること

(1)現行のファイルサーバーからクラウド方式によるネットワーク管理で、県社協に最も合った提案をすること。

・現サーバーの廃棄等について安全かつ確実な方法でデータを消去し、処理すること。処分後は証明書を交付すること

・現行のサーバー等機器類で使用できると思われるものは提案のうえ有効活用を行い、できないものについての廃棄は業者にて行うこと。

・機器の納入にあたっては、安全性のため鍵の掛かるサーバーラックの中で管理をすること。サーバーラックの費用は業者の導入経費に含める。

なお、現サーバーラック（内計、縦 80 ㎝×横 50 ㎝×高さ 88 ㎝）2台については、そのまま使用できるが、使用しない場合は廃棄の費用を含める。

（2）現在のデータ量は4TB であるため、実利用領域を最低6TB 以上確保し、データ量の増加やアクセス集中の際にも安定した性能を確保すること。

（3）クライアント　　120台として計算すること。

デスクトップ PC　県社協　67台（人）

内部団体9団体で13台（人）

ノート PC　　40台　※ノート PC はテレワーク、研修等で使用するため普段はネットワークには接続しない。

（4）ウィルス対策

ウィルス対策ソフトの初期導入、クライアントへのインストール及び運用保守経費を入れること

※現行はオンプレ版ウィルスバスターTrend Micro ApexOne を導入し、クライアントへのインストールも完了している。

ウィルスバスターは必須では無いが、同等以上のウィルス対策ソフトは必須で、その場合は、運用保守経費とともに、導入にともなうクライアントへのインストール等を行い・その初期経費を入れること。

また、パターンファイル更新する仕組みを構築し、定期的に更新すること

バージョンアップへの更新作業（クライアントへのインストールを含む）についても運用保守経費に含めること

（5）SKYSEA Client View 環境を設定、運用保守経費を含めること。

120 クライアント　※クライアント数は、変更の可能性有り

（6）UTM（総合脅威管理）の導入、設定、クライアントへのインストール　※

※現行は、Fortigate60F　UTM プロテクション版更新1年を導入している。UTM を導入する場合は、新たに導入するための経費、及び運用保守経費を入れること。また、120 クライアントへ設定する。

現在、Fortigate はメール及びノート PC30 台に FotiClient を設定し、本会サーバーと VPN 接続により在宅勤務を可能にしている。新ネットワークにおいても同等以上の機能が可能とすること。

（7）ドメイン管理、メールサーバー使用料

新たなにメールサーバーを移行する場合は、メール設定、セキュリティ対策を含めること

(8)ソフトウェア全般、OS 等に関して、導入後の利用期間中はサポート切れとならないよう最新版や標準的な製品を優先して採用すること。

(9)ソフトウェアのライセンス体系も踏まえて、経済的な提案をすること。

(10)ネットワーク等に不具合が判明した場合、不具合の情報を即時に提供するとともに、対応すること。

(11)ネットワーク運用保守について

ネットワークに入れない、インターネットができない、印刷ができない等、ネットワークに障害が発生した場合の対応について迅速かつ万全の対策を講じること。

(12)データのウィルス感染やシステム侵入が発覚した場合の対応を明記すること。

(13)バックアップ

災害やウィルス感染等によるデータ破損といった障害等によるデータ損失に伴う影響を最小限にするため、データの保全と運用保守、業務復旧に関する適切なバックアップ機能を有すること。

・障害等によるデータ損失に伴う影響を最小限にするため、適切なバックアップ機能を有すること

・バックアップを行う際に、バックアップ装置に対する各種操作、メディア管理、バックアップの世代管理等が行えるバックアップ管理機能を備えること。

・毎日のデータバックアップに加え、システムバックアップについても定期的に行うこと。

・バックアップはスケジューリングされ、自動的に行われること。

・バックアップに必要な媒体の費用は、本契約に含めること。

(14)ハードウェア・ソフトウェア(OS を含む)は、契約期間において開発元等の脆弱性改修などのサポート提供が受けられること。

(15)今後新たに発生するネットワーク管理、ファイル管理のための業務機能の追加や変更等の要望に対応可能なシステム構成とすること。

(16)セキュリティ要件

・個人情報保護・データ保護

本会業務で保有するデータは機密情報が含まれているため、セキュリティにおいて万全の対策を講じること

・システム

利用者及び管理権限を割り当てることができ、システム上でもその権限に応じた処理の制限が行えること。ログインした操作者ごとの権限に応じた画面標示項目を設定できる機能を有すること。ログイン業務処理等の操作について、監査証跡として適切に管理し紹介が行えること。

・脆弱性等への対応

コンピューターやソフトウェア等に関する脆弱性や危険性が判明した際には、本契約で導入する機器やソフトウェア等について調査し、該当の有無や初期対応等についてすみやかに報告し、その対策をとること。

(17)機器の入替または撤去

入替または撤去する際は、設定情報等を削除すること。データの消去方法は物理的な破壊、または米国家安全保障局(NSA)推奨方式以上のセキュリティレベルでデータを削除すること。なお、その際にはデータ消去書類を発行すること。その際にかかる入替・撤去費用、運搬費用、その他撤去等にかかる費用も業者にて負担すること。

・現行ネットワーク及びサーバー仕様を参照　　(別紙1)参照

※現行のネットワーク概要図については、資格審査後、合格者にメールにて送るものとする。

(18)事故が発生した場合の対応

・情報が流出した場合の対応、責任体制について万全の対策を講じること。

・情報が流出した場合の原因究明、再発防止策について万全の対策を講じること。

・損害を受けた場合の対応、保障等について十分な対策を講じること。