長野広域連合情報セキュリティネットワーク再構築業務委託
調達仕様書

長野広域連合事務局　総務課

1　委託内容

１　件名

長野広域連合情報セキュリティネットワーク再構築業務委託（以下、「本業務」という。）

２　業務期間及び契約方法

(1) 構築業務：契約締結日から平成 30 年６月 30 日まで

※契約締結日とは、リース会社と長野広域連合（以下、「本連合」という。）との三者契約によるリース契約締結日をいう。

※契約期間は、平成 35 年６月 30 日までの長期継続契約とする。

(2) 保守及び運用支援業務

：平成 30 年７月１日から平成 31 年３月 31 日

※契約方法は、受託事業者と本連合による随意契約とする。

※平成 31 年度以降の契約については、予算が確保されることを条件に、本連合と受注事業者双方に異存がなければ、平成 35 年６月 30 日まで年度単位で契約更新するものとする。

３　履行場所

本連合の事務局、本連合が所管する７拠点の老人福祉施設（以下、「連合施設」という。）及び本連合より指定された場所

４　提案上限額（60 ヵ月分）

(1) 構築（リース契約）分：　**金　１７，１４２，０００円（消費税込）**

〔費用項目〕ハード・ソフトウェア購入費、導入及び構築作業等費、ネットワーク関連機器購入費（保守費用含む）

(2) 保守・運用支援業務分：　**金　１２，１９５，３６０円（消費税込）**

〔費用項目〕サーバ機器保守費用、運用支援業務費用、データセンターハウジングサービス費用

※上限額は上記業務期間満了までに要する額とする。

※上限額は予定価格を示すものではなく、企画内容の規模を示すためのものである。

※提案額上限を超える額で提案した事業者は失格とする。

５　委託内容

本調達仕様書に掲げる事項を行うものとする。

６　スケジュール

(1) 本業務の全体スケジュールは図１のとおり。

(2) 平成 30 年６月 30 日までに本業務の構築を行うため、 以下のアからエに示す内容を実施するものとする。

ア　本業務を実現するための詳細なスケジュールを本連合と協議の上、「業務計画書」を策定すること。

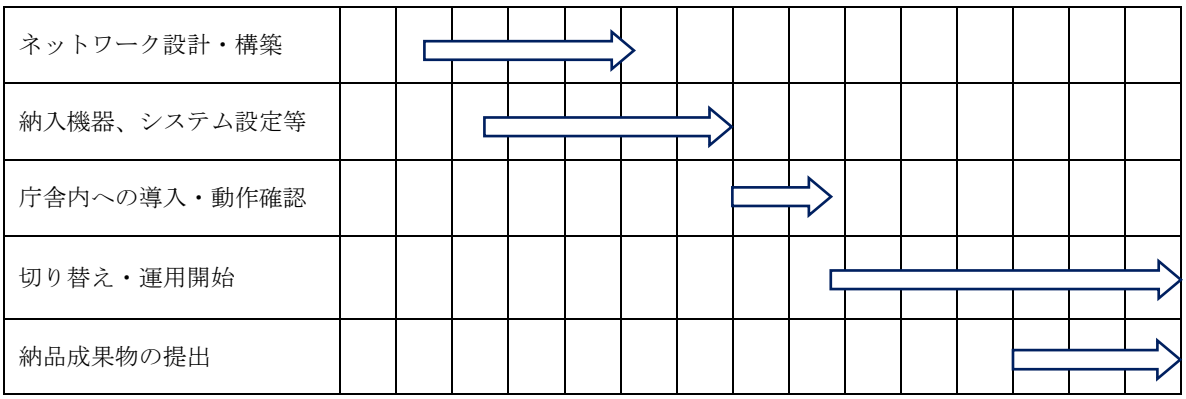
イ　本業務の実施（本連合による確認、受託事業者による修正に要する期間を含む）について、必要な期間を確保すること。

ウ　本連合が実施する検査において、問題点が確認された場合に平成 30 年６月 30 日までに修正等の対応が完了するよう、必要な期間を確保すること。

エ　本連合における本業務の運用開始日は、平成 30 年７月１日とする。

図１　スケジュール

	４月			５月			６月			７月			８月		
	上旬	中旬	下旬	上旬	中旬	下旬	上旬	中旬	下旬	上旬	中旬	下旬	上旬	中旬	下旬
納入物品調達・論理設計	⇒														



2　ネットワーク構築の基本要件

1　ネットワークシステム構築の基本方針

日本年金機構の情報漏えい事故を受けて、総務省は、各地方自治体に対して「自治体情報システム強靭性向上モデル」の実施を求め、各自治体はこれを受けて平成 29 年度中に強靭化対策を実施している状況である。特別地方公共団体である本連合の業務においては、連合施設の利用者情報やマイナンバー関係事務による個人情報の取扱業務があるにも関わらず、現状では十分なセキュリティ対策が施されていないことから、ネットワーク環境の再構築及びセキュリティ対策の実施が必要である。

事務局及び連合施設ではそれぞれインターネット接続口を持っており、セキュリティレベルが統一されていない状況であることから、インターネット接続口を１カ所に集約した上で、既設のクライアント端末を一元管理化したネットワーク環境を整備し、セキュリティ対策を集中的に実施することで、本連合におけるセキュリティレベルの向上と平準化を実現するものとする。

情報セキュリティネットワークシステムを再構築することで、各種業務の適正化や安全な業務管理の実現を目指すものとする。

2　作業内容

(1) 本業務に係る必要な作業内容

ア　機器の調達・設置

本仕様書に記載の仕様を満たすネットワーク機器、サーバやライセンス等を調達し、必要な調整を行って本連合が指示した連合施設へ設置、納品すること。

イ　ネットワークの設定調整及び試験作業

既設機器及び調達したネットワーク機器を用いてネットワークを構築し、事務局及び連合施設において、通信試験を実施すること。

ウ　移行支援作業及び運用サポート

現行の連合施設内ネットワークとの並列稼働への対応を含め、移行時の具体的な作業を踏まえた支援作業を実施すること。また、平成 30 年度以降の平常運用に備えたサポートを実施すること。

エ　事務局及び連合施設内の LAN 工事・LAN 配線作業

本業務におけるネットワーク配線は、基本的には既設環境を流用することを前提としている。ただし、業務実現にあたり LAN 工事及び LAN 配線作業が必要となった場合には、本連合との事前協議の上、本契約内で実施すること。

オ　受託事業者の作業内容

本連合の示す方針に従い、全て受託事業者が実施すること。

・業務計画書の作成
・ネットワークの見直し・設計・管理（打ち合わせ、進捗管理）
・ネットワーク構成図の作成
・導入システムの構築・導入・試験
・ネットワーク機器の設定・導入・試験
・LAN 工事、配線作業

・既存ネットワーク機器の設定変更・試験
・プリンタの設定・試験
・既存端末の設定変更支援・試験
・納品ドキュメントの作成
・管理者向け職員研修の実施
・運用支援
・導入するすべてのハード及びソフトウェアの保守
・データセンター内のサーバ機器のアウトソーシング（死活監視及び Windows のイベントログ監視を含む）及び利用開始に伴う設定作業（ラック設備、構内専用線等）
・初期セットアップ、ユーザー登録（設定）、AD 連携設定作業

(2) 本業務に係る成果物等の納品

ア　成果物一覧

本業務においては、以下の「図２　成果物一覧」に示すとおり納品すること。提出期限は、業務計画書作成時に本連合と協議の上で決定するものとし、印刷物を正副１部、各成果物の電子データを収納した電子媒体（DVD-R）１部を納入すること。

イ　納入条件

「図２　成果物一覧」に示すとおり。また、本連合と協議の上で、必要と判断された納入成果物は、別途提出すること。

ウ　必要な消耗品は、受託事業者負担にて調達すること。

エ　納入場所は、本連合が指定する場所とすること。

図２　成果物一覧

No.	成果物	内容	納入日
1	業務計画書	本業務の遂行計画についてまとめた資料	平成 30 年 6 月 30 日
2	構成図	全体ネットワーク、納入機器についての構成資料（LAN 配線図・機器設置図含む）	同上
3	工程表	本業務の工程表（スケジュールを含む）	同上
4	設計書	納品システム、機器について設定内容をまとめた資料	同上
5	試験成績書	納入システム、機器についての試験実施内容、試験結果についてまとめた資料	同上
6	納入機器一覧	納入機器について機器スペック、シリアル番号等をまとめた資料	同上
7	施工写真	施行前後（施行前、施行中、施工後、設置機器、取外し機器）の写真資料…施行写真には表紙をつけて納品すること	同上
8	各種マニュアル	納入システム、機器についての運用マニュアル	同上
9	業務完了報告書	本仕様書に示されているすべての要件が実現されていることを確認した上で業務の完了を報告する資料	同上
10	保守業務完了報告書	別途契約する運用支援契約の委託期間内に生じた課題および対応状況を記載したもの、適宜必要な情報を付記すること	委託期間終了日

３　セキュリティネットワークの基本要件

(1) ファイヤーフォールの導入、端末設定等ネットワーク関連の構築作業

必要な通信と不必要な通信を区別し、不必要な通信がネットワーク内に入ってこないよう構成すること。内部から外部にアクセスする際も同様であり、許可されない端末が外部に接続してしまい、セキュリティ事故を引き起こさないための作業を実施すること。

(2) ウイルス定義ファイル（セキュリティ対策ソフト及びウイルス対策ソフト）を常に最新化すること。サーバ及び端末機器に対し、ウイルス定義体の最新版を配信すること。

(3) 事務局及び連合施設にあるインターネット接続口を一本化し、Web 通信のウイルス対策を実施すること。インターネット上のマルウェアやその他の有害なコンテンツに対し、フィルタリング

を行い、ゲートウェイで内部ネットワークへの侵入を防ぐこと。
(4) ユーザー管理（ID/PASS）の一元化により、利用者権限（IP アドレスの変更権限）を管理すること。
(5) USB 接続の機器を個別に制御し、使用制限することで、自宅での利用など、許可されていない USB を接続できないようにすること。本連合の個人情報を自宅の端末に移替ることを防ぎ、情報漏洩リスクを軽減させること。

４　ネットワーク構成の基本要件

(1) 現在の本連合事務局庁舎は、長野市役所からの借受けであり、かつ耐災害性が低い建物のため、ネットワークの中枢機能をデータセンターに設置する構成とすること。よってサーバ機器はデータセンター内に設置（ハウジング）すること。
(2) 24 時間 365 日安定稼働が可能な高い耐障害性及び柔軟な拡張性を持った構成とすること。
(3) 本連合の要求を充足するセキュリティ対策を備えた構成とすること。
(4) 事務局移転に伴う機器の移設 及びそれに伴う設定作業、または機構改革等に伴う端末台数の増減に柔軟に対応できる構成とすること。
(5) 端末数、業務システム数などが増加した場合にも、機器増強等による性能向上が可能で、さらに WAN 回線の帯域増強等、トラフィックの増加や変化が生じた場合にも、柔軟に対応できる拡張性を有すること。
(6) 法人モデルで提案すること。
(7) エッジスイッチから端末までの LAN ケーブルは、カテゴリー５ｅ以上を使用し、接続先もしくは用途ごとに色を変えたものを使用すること。
(8) LAN ケーブルにはタグを付けること。
(9) 本連合のネットワーク構成は、事務局（総務課、福祉課、環境推進課）内のネットワーク（以下「事務局系ネットワーク」という。）と事務局（福祉課のみ）及び施設内・施設間のネットワーク（以下、「施設系ネットワーク」という。）で構成されているため、以下に示す既存業務システムがすべて問題なく稼働できるよう、本業務を実施すること。
※業務システムの接続環境を確保するとともに、本業務の運用開始後も問題なく正常稼働するよう考慮したネットワーク設計及びシステム構築を行うこと。
＜事務局系ネットワーク及び施設系ネットワーク（共通）＞
・財務会計システム
・グループウェアシステム
＜事務局系ネットワーク＞
・事務局ファイル共有サーバ
・介護認定審査システム
＜施設系ネットワーク＞
・介護事業者支援システム
・施設ファイル共有サーバ
・ウイルス配信サーバ
＜インターネット系＞
・給与センターサービスシステム
・国保連合会介護伝送ソフト
・例規システム
・ホームページ（Web サーバ及びメールサーバ）
＜ネットワーク管理外＞
・栄養管理システム
(10) 既存の LAN 配線を使用することに問題ないが、本連合全体としてのネットワーク環境を安定稼働させるよう配慮すること。また、新規配線する LAN ケーブルは、カテゴリー５ｅ以上を使用すること。
(11) 敷設後、一年以内の環境不安定については、必要に応じて調査、設定変更を繰り返し行い、ネットワーク環境を安定させること。
(12) 最新の IT 技術動向を踏まえた最適なネットワーク構成であること。また 効率化できる構成があれば、提案に含めること。
(13) その他、導入の中で発見された既存環境の問題点については、本業務の目的を理解した上で、現地確認を主として解消に向けた誠意ある対応を行うこと。

５　調達範囲等

(1) 調達の対象機器等

ア　ネットワーク関連

・センタールータ（データセンター内設置とし、予備機１台を含む）
・サーバスイッチ（データセンター内設置とし、予備機１台を含む）
・ルータ（本連合事務局庁舎内及び連合施設内設置）
・エッジスイッチ（本連合事務局庁舎内及び連合施設内設置）
・ファイヤーウォール（データセンター内設置）
・その他 エッジ HUB 及び LAN ケーブル等構築する上で必要となるもの（本連合事務局庁舎内連合施設内設置）

イ　サーバ関連（データセンター内設置）

サーバ構成については、サーバ上で、複数の仮想的なサーバ（仮想サーバ）を構成し、運用することは可能とする。ただし、高スペックの物理サーバとし、構築だけでなく運用対策及び障害対策について提案するものとする。

・情報漏洩対策サーバ
・Proxy サーバ
・ウイルス配信サーバ
・WSUS（Windows パッチ配信）サーバ
・Active Directory
・バックアップサーバ

ウ　ソフトウェア

・導入するウイルス対策ソフトについては、TrendMicro ウイルスバスターのみとする。
・配信対象端末数は、事務局内にあるクライアント端末 49 台とする。ライセンス数は、更に必要に応じてサーバ台数分等を加味するものとする。
・情報漏えい対策ソフトによる管理・監視対象端末数は、 事務局及び連合施設内にある全ての既設クライアント端末 160 台とする。
・クライアント OS は、Windows７、８、8.1、10 に対応するものとする。
・フリーウェアではなく、 国内メーカーが保証するシェアウェアやパッケージソフト等の市販製品であるものとする。

(2) 調達範囲の概要

ア　ネットワーク調査

事務局及び連合施設内の配線構成を示す UTP 配線図等の資料が存在しないため、そのことを考慮した上でネットワーク調査をするものとする。

イ　ネットワーク設計

ネットワーク調査に基づき、設計を行うこと。(物理構成設計、論理構成設計、配線構成設計、IP アドレス設計、ルーティング設計、情報セキュリティ設計、運用設計等)

ウ　ネットワーク機器及びソフトの調達

ネットワーク設計に基づき、ネットワーク機器及びソフトの調達を行うものとする。

エ　ネットワーク構築

ネットワーク構築については、データセンター側と事務局側を先に行い、その後連合施設側について行うものとする。

事務局及び連合施設側については、本業務に係るネットワーク動作環境に必要な既存ルータ等の設定変更作業も含むものとする。

(3) 調達対象外機器等

ア　既設機器

・ファイルサーバ
・グループウェアシステム

イ　既設の無線アクセスポイント及び無線 LAN 環境

６　データセンター要件

(1) 事務局及び連合施設内には、サーバ室は構築せず、データセンターにサーバ機器類を設置すること。

(2) データセンター内に設置するサーバ機器をネットワークに接続すること。

(3) データセンターは、被災可能性の低い立地であることとし、高度なセキュリティ設備を有していること。
(4) 迅速な障害復旧実現へ向けて、ハードウェア保守要員、ソフトウェア保守要員、ネットワーク保守作業員との密な連携を行うこと。
(5) データセンターは、以下の要件を満たすこと。
ア　立地
・長野県内に所在すること。
・データセンターの周囲半径 100 メートル以内に消防法による指定数以上の危険物製造設備、火薬製造設備、及び高圧ガス設備がないこと並びに隣接建物から延焼防止の為に充分な距離が保たれていること。
イ　建物
・震度７の地震に耐えられ、建物の倒壊、崩壊の恐れがないものとし、更に建物内の設備、機器等にも損傷を与えない構造であること。
ウ　電源設備
・停電時に自家発電機が起動するまでに、瞬断することなくサーバ機器に 10 分以上十分な電力供給が可能な容量を持つ無停電電源装置（UPS）が設置されていること。
・商用電力の供給が停止した場合、コンピュータシステムに影響を及ぼさない状態を確保できるよう十分な容量を持つ非常用自家発電設備が設置されていること。なお、自家発電設備は、商用電力の供給が止まった場合でも停止から５分以内（この間は UPS から電力供給）に電力が供給できることとし、更に無給油で 72 時間以上の連続運転が可能であること。（72 時間以上の燃料を備蓄していること。）また、優先的に燃料供給が受けられる契約を燃料供給会社と結んでいること。
エ　空調設備
・サーバルームの機器等に対して十分な空調能力があること。なお、空調設備は 24 時間 365 日連続して稼動可能であること。
オ　防火設備
・サーバルームは、設置機器に影響を与えないよう、水を使用しない不活性ガス（窒素ガス等）の消火設備を設置していること。
カ　セキュリティ対策
・データセンターへの入退管理は、セキュリティ管理システムにより、24 時間 365 日実施されていること。
・サーバルームへの入退室者を識別・記録できるセキュリティ設備（ＩＣカード等）により、許可された者のみ入退室が可能なこと。さらにサーバ室への入室はバイオメトリクス認証システムを採用していること。
・サーバルームおよび館内を監視するための監視カメラを設置していること。
・施設内の電源設備、空気調和設備、セキュリティ設備等は、常時故障監視がされているとともに巡回監視が実施されていること。またサーバ室は、死角がないように複数の監視カメラにて目視監視可能であり、記録データは１ヶ月以上保管できること。
キ　実績
・地方公共団体への導入実績があること。
(6) データセンターは以下の資格を有していること。
ア　環境：ＩＳＯ１４００１規格
イ　セキュリティ：ＩＳＯ２７００１規格（ＩＳＭＳ）
ウ　個人情報保護：プライバシーマーク（日本情報処理開発協会:総務省および経済産業省）
（ただし、プライバシーマークより厳格な自社の規定がある場合はこの限りではない。）

７　導入機器（ハードウェア）要件

・既存の機器及びサーバと整合性をとり構築すること。
・既存の機器及びサーバからデータ移行が必要な場合にも極力停止が発生しないように心掛けること。
・既存設備の設定変更が必要な場合には、受託事業者自身が行うか、受託事業者が費用負担の上、既存設備の保守事業者へ作業を依頼すること。
・導入後、５年の保守が可能なものであること。
・本業務の構築対象となるクライアント端末は、すべて既存端末となるため、導入するソフトウェ

アのインストールや設定変更、設置などは、各拠点において受託事業者が行うこと。
・既設システムの動作確認の実施も行い、正常稼働に必要な設定作業等は受託事業者が実施すること。
・連合施設に設置するネットワーク機器については、本連合が用意する 19 インチラック（W600×D500×H400）内に設置するものとする。設置場所については、本連合と事前に協議した上で決定するものとする。
・サーバについては、国内メーカー製品を選定すること。また、速やかな障害復旧のため、長野県内に選定メーカーのサポート等の拠点を要すること。
・サーバの構築については、「５　調達範囲等（1）イ　サーバ関連」のとおり。

(1) 情報漏洩対策サーバ
基本機能として以下の各機能を提供すること。
ア　デバイス管理
・USB デバイスをシリアルナンバーごとに管理する機能を有すること。
・保有 USB デバイスはシステムで台帳管理し、一覧で表示できること。
・USB デバイスをクライアント端末もしくは管理者のクライアント端末に挿入した際、利用した USB デバイスのメーカー名、シリアルナンバー、ベンダーID を自動で収集し、管理台帳を作成できること。
・収集した情報にもとに指定した USB デバイスを使用許可/不許可を設定できること。使用許可／不許可の設定は、ネットワーク全体および指定した部署のみ利用可など柔軟な設定が行えること。
イ　ログ管理
・クライアント端末に対して行われた操作、ログオン、ログオフの日時、実行されたソフトウェアについての起動・終了時間、ファイル操作、USB メモリなどの記憶媒体を利用した内容等を記録する機能を有すること。
ウ　ログ閲覧
・ログの閲覧が可能なこと。
※　受託事業者は、アからウの基本機能以外にも、最新の情報漏えい対策機能について提案できるものとする。

(2) Proxy サーバ
・日本国内でオンサイト保守が提供されているメーカー製で、19 インチラックに搭載可能。
・Xeon プロセッサー E5-2630v4（2.20GHz 10 コア）以上の CPU を１基搭載していること。
・メモリを８GB 以上搭載していること。
・300GB 以上のディスク領域を確保すること。
・1,000BASE-T 対応のネットワークインターフェースを 1 基以上搭載していること。
・Red Hat Enter price Linux をインストールしたサーバを構築すること。
・Proxy 機能を有すること。
・自サーバのウイルス定義ファイルの自動更新すること。
・サイトの評価を確認して危険な Web サイトに対する保護機能を提供すること。信頼済みのサイトから Web コンテンツ制御を除外できること。
・なお、ネットワーク機器による制御も可とするが、高スペックの機器とし、構築だけでなく、運用対策及び障害対策について提案するものとする。

(3) ウイルス配信サーバ
・ウイルス配信サーバは、事務局系ネットワーク上に構築すること。
・定義ファイルの随時更新が可能な仕組みを構築すること。
・施設系ネットワークのウイルス配信サーバによる定義ファイルは、本業務の対象外とする。
・ウイルス対策ソフトは、Trend Micro とする。
（なお、現在、事務局系ネットワークにて使用しているウイルス対策ソフトは、ESET End Point）
・ディスクについては、導入後５年以上利用可能となるディスク容量で構成とすること。
・その他、必要となる周辺機器を導入すること。
・その他、必要となるソフトやそのライセンスを導入すること。

(4) WSUS サーバ
・Windows Server 2016 standard をインストールした WSUS サーバを構築すること。なお、ウイルス配信サーバとの兼用も可とする。
・WSUS サーバは、事務局系ネットワーク上に構築すること。
・施設系ネットワークの Windows Update の定義ファイル等は本業務の対象外とする。
・Office 製品・Windows OS に対しての重要パッチ及びセキュリティパッチの更新作業を一元管理できるようにすること。
・クライアントは、Microsoft Update の取得元として WSUS サーバを利用するように構成すること。
・更新のスケジュールを指定し、自動的にインストール・再起動が行われるように設定が可能なこと。
・クライアント・サーバ用のアップデートファイルはすべて事前にダウンロードされる設定が可能なこと。

(5) Active Directory サーバ
・ディスクについては RAID 構成で導入すること。
・必要に応じてサーバに対応する UPS を調達し設定すること。
・ディスクの増設に対応できること。
・ディスク容量は構築環境に見合ったものを提案すること。
・その他必要となる周辺機器及びソフトやライセンスを導入すること。
・Active Directory 配下で管理対象となる事務局系ネットワークのクライアント端末（49 台）の設定作業は、受託事業者にて行うこと。本連合に設置された端末 OS の情報を参考とし、インストールされたアプリケーションが正常動作するよう配慮の上、具体的な方法を提案すること。

(6) バックアップサーバ
・導入するサーバのデータバックアップ先として構築すること。
・導入するサーバに障害が発生した際に速やかにデータ復旧できる構築環境を提案すること。
・必要に応じてサーバに対応する UPS を調達し設定すること。

８　導入機器（その他）要件

(1) センタールータ
・インターネット系センタールータとして機能すること。
・データセンター内に設置すること。
・フレッツＶＰＮワイドグループに参加し、センタールータとして再構築すること。また各拠点に新規設置するインターネット専用ルータとＶＰＮ接続すること。
・L3 スイッチ機能を有すること。
・10/100/1000BASE-T を 1 台あたり 10 ポート以上実装していること。
・MAC アドレスを 1,000 個以上登録可能であること。
・IEEE802.1Q に準拠した VLAN を設定可能であること。
・VLAN の種類として、ポートベース VLAN、IEEE802.1Q タグベース VLAN。プロトコル VLAN の各 VLAN に対応可能なこと。
・VPN 機能を有し、最大 100 か所との接続が可能なこと。
・コマンドライン及び GUI 機能を有すること。
・予備機を用意すること。

(2) サーバスイッチ
・10/100/1000BASE-T のポートを 1 台あたり 10 ポート以上実装していること。
・SFP+スロットを 1 台あたり 2 ポート以上実装していること。
・装置単体でスイッチングファブリックは 20Gbps 以上であること。
・装置単体で MAC アドレスを 8,000 個以上登録可能であること。
・VLAN の種類としてポートベース VLAN、IEEE802.1Q タグベース VLAN。プロトコル VLAN の各 VLAN に対応可能なこと。

・Link Aggregation 機能（LACP 及び Manual Configuration）を有すること。
・予備機を用意すること。

(3) エッジスイッチ
・各フロア、各連合施設の拠点に対しエッジスイッチを設定すること。
・必要台数については事務局及び施設のレイアウト図を見て受託事業者側で提案すること。
・ループを検出する機能に対応し、ループを検出した場合には、ポートをリンクダウンさせることが可能なこと。
・装置単体でスイッチングファブリックは 20Gbps 以上であること。
・装置単体で MAC アドレスを 8,000 個以上登録可能であること。
・AP とクライアント端末間への通信に負荷がかからないよう配慮された機器と構築環境を提案すること。

９　その他要件

ソフトウェア及びハードウェアの導入に伴い必要となるもの。(CAL、ソフトウェア保守パック５年分等。)

3　運用支援の基本要件

１　対応時間

本業務により構築したネットワークシステム（以下、「本システム」という。）における運用支援の対応時間は、原則として平日の８時 30 分から 17 時 30 分までとする。

ただし、人事異動に伴う設定作業等が必要な場合やサービスに影響がある等の緊急時は当該時間帯以外においても連絡及び対応を行うものとする。

２　運用環境

運用環境は、関係法令及び条例等に基づき、セキュリティを確保することを前提に受託事業者の事業所からリモートオペレーションによる運用も可能とする。

ただし、緊急時に迅速な対応を行うため、１時間以内の駆け付け目標が可能な場所に保守拠点及びデータセンターが存在するものとする。

また、本システムと運用環境との接続は、専用線、広域イーサネット、または IP-VPN 等の閉鎖網とし、インターネット経由（インターネット VPN を含む）による接続は不可とする。

なお、リモートオペレーションに必要となる機器及び回線費用は、本業務の調達費用に含めるものとする。

３　運用窓口

本システムの運用支援作業を円滑に行うため、本システムに係る運用窓口を設置し、本連合からの問い合わせに対応できるよう、本システムの運用要員を確保するものとする。

４　定常対応

定常対応として、以下の作業を行うこととする。また、本システムを維持・運用する上でその他の作業が必要となる場合は、その作業も定常対応に含めるものとする。

ア　セキュリティパッチの適用支援・助言
イ　ウィルス対策ソフトの管理・更新（５年間）
ウ　バックアップの取得及びリストア
・バックアップについては、フルバックアップし、保管すること。(仮想化の場合は、構築時の仮想イメージをフルバックアップし、保管すること。)
・日次にてファイルバックアップデータを取得すること。
・バックアップデータ取得作業は自動化し、本連合職員の作業を必要としないこと。
・リストア手順については、十分な検証を行い、取得したバックアップデータを用いて正しく復旧できることを事前に確認すること。
・本稼働前に必ずフルバックアップ及びフルリストアの試験を実施すること。

エ　計画停電に係る対応
・主にデータセンター内での対応とするが、ネットワーク機器の起動に関しては必要に応じて対応を行うこと。
オ　質問に対する対応
カ　運用にあたっての情報提供・助言
キ　トラブルへの対応及び対応後の状況報告
ク　サーバ等機器の管理
ケ　ソフトウェア、ファームウェアのバージョンアップ作業

５　障害・異常時の対応

障害発生時及びシステムの異常検知時において、以下の作業を行うものとする。

(1) 本連合にて障害・異常を検知した場合は、既存システムと本業務の調達に係るものとの簡易的な一次切り分けを行い、本システムに異常が認められた場合は速やかに運用フローに則り、障害の原因の切り分け、調査、復旧作業、確認作業において支援または対応を行うこと。

(2) 監視により本システムの異常が検知された場合は、速やかに運用フローに則り、当該機器の障害対応を行うこと。

(3) ウイルス検知等の際は、必要に応じて本システム内の被疑箇所をネットワークから分離 及びクリーンアップ作業の支援を行うこと。また、取得しているログから関係個所を CSV 形式で抜き出すなど、解決のための一次支援を行うこと。

(4) 本システムにおける業務停止時の目標復旧水準は、以下のとおりとする。
ただし、端末の復旧に係る作業は、業務システムの初期セットアップが必要になることが想定されるため、原則として業務システム側での対応とし、本業務に含まない。

ア　目標復旧地点
・前日の時点に復旧できること。

イ　目標復旧時間
・可能な範囲で速やかに復旧させること。復旧が困難な場合は代替案にて対応できること。

ウ　目標復旧レベル
・すべてのシステム機能が実行可能な状態に復旧させること。

(5) 発生したネットワーク障害の状況から、 今後における本連合及び受託事業者が把握できる仕組みを構築又は提案すること。

６　設定変更対応

本システムで必要となる設定変更対応について、大規模となる変更を除き、運用支援の中で以下の作業を行うものとする。

(1) セキュリティゲートウェイ 及びファイヤーウォールにおけるファイヤーウォールポリシーの変更。

(2) セキュリティゲートウェイにおける URL フィルタリングの変更。

(3) ウイルス対策ソフトのスキャン時間、その他のオプションの変更。

(4) その他、システム運用上必要な設定変更。

７　情報管理

本システムに係る情報管理として以下の内容を適切に管理するものとする。

(1) インシデント管理（セキュリティインシデントを含む）

(2) 問題・課題管理

(3) リソース管理

(4) 変更管理

８　他システムへの移行作業

他システムとの接続及び他システムへの切り替え・移行に際して必要となる場合は、システム構築事業者が安全で確実な作業を行えるよう、当事業者に対し可能な限り協力するものとする。

ただし、業務システム側の変更に起因する設定変更や修正作業が生じた場合は別途両者で協議により対応を決定するものとする。

９　報告会の実施

必要に応じて報告会を実施し、各種作業実績及び情報管理の状況を報告書にまとめて報告するものとする。

ただし、緊急での対応が必要な場合は、適宜、報告会を実施するものとする。

なお、システムリソースの枯渇や新たなセキュリティ脅威への対応等、情報管理を行う中で発見した問題及び課題については、運用支援の中で改善提案を行うものとする。

4　保守の基本要件

１　保守対象

(1) 保守対象は、原則として本業務の調達により導入するすべての借入物品とする。ただし、保守サービス自体が存在しない製品については対象外とする。

(2) 利用者の故意 または重大な過失により発生したハードウェア障害については、保守対象外とする。

ただし、保守対象外と判断したものについては、その理由及び原因について、本連合へ報告し承認を得るものとする。

２　保守内容

(1) 借入れ物品について契約期間満了（５年間）まで保守の対象とすること。

(2) 障害発生時に迅速な対応を可能とするため、 借入れ物品の保守に係る一元的な連絡窓口を設置すること。また連絡窓口は、月曜日から金曜日（休日・祝日を除く）の午前８時 30 分から 17 時 30 分の受付が可能なこと。

(3) 借入れ物品の障害発生時には、ログ等を解析し、原因究明を行うこと。

(4) ハードウェアに係る保守は、月曜日から金曜日（休日・祝日を除く）の午前８時 30 分から 17 時 30 分のオンサイト保守もしくは、予備機を調達物品に加えた上でのセンドバック保守とする。

(5) オンサイト保守は、障害の検知、連絡から２時間以内を目標に現場に到着し復旧作業に取り組むこと。

なお、アプライアンス製品などで、事業者の事務所にて環境設定後に現場作業を行った方が復旧作業の短縮が見込まれる場合などは別途協議する。

(6) ハードウェア交換時における代替機器のソフトウェアバージョンは、稼働している機器と同一のバージョンとすること。

(7) 借入れ物品のハードウェア故障修理に伴い、再インストールが必要な場合は、受託者が実施すること。

(8) ハードディスク等の秘密情報を含む部品の処分については、 第三者に漏えいすることのないよう、データ消去等の処理をすること。

(9) ソフトウェアに係る保守は、月曜日から金曜日（休日・祝日を除く）の午前８時 30 分から 17 時 30 分までとする。

(10) 借入れ物品に不具合が発見され、バージョンアップ情報、修正パッチ、セキュリティパッチ、及び対策部品等が提供された場合は、速やかに本連合へ報告を行い、対応について協議した上で対策を実施すること。

(11) 受託事業者は、本連合から借入れ物品の操作や設定に関する問い合わせに対して速やかに技術支援を行うこと。

(12) メーカーによるサポート打ち切り又は脆弱性対応、障害への恒久対策等のため、バージョンアップが必要な場合、速やかに報告を行うとともに、システムへの影響調査を行い、調査結果を本連合に報告すること。また本連合と協議した上で必要に応じて対応策を実施すること。

(13) バージョンアップ等により機器操作マニュアルに変更が発生した場合には、機器操作マニュアルを改訂し、本連合に提出すること。

※　なお、「３　運用支援の基本要件」及び「４　保守の基本要件」については、受託事業者の実施体制に応じて、運用支援業務または保守業務のいずれかにおいて実現するものとする。

5　その他

1　作業体制

本業務の調達において、業務目的を理解し、業務遂行に適した全体統括責任者を配置するものとする。また、責任者は情報を一元管理し、本調達にかかる本連合との窓口となるものとする。

2　作業場所

本調達に係る作業は、賃貸人の事業所又はそれに付随する場所で行うものとする。

ただし、本連合と行う会議、搬入、設置、トレーニング等については、本連合が指定する場所で行うものとする。

3　本連合庁舎内での作業時間

原則として平日８時 30 分から 17 時 30 までとする。ただし、本連合における業務への影響を最小限とするための理由による作業時間の変更は、本連合の承認を得るものとする。

また、本連合庁舎内での作業日程、作業内容はすべて事前協議とする。

4　既設の保守事業者との調整

サーバ等の移設に伴い、既存の設定情報を反映させる必要がある場合は、既設の保守事業者と調整を行うものとする。

5　撤去作業

契約期間満了後、借入物品は速やかに撤去するものとする。

なお、物品撤去に係る実施方法及びスケジュール等については、別途本連合と協議の上で決定するものとする。

撤去作業に係るすべての費用については、本契約に含めるものとする。

6　データ消去作業

契約期間満了後、賃貸人の負担により、物理的破壊またはデータ消去によりデータが漏えいしないように情報セキュリティ対策を講じるものとする。

データ消去の場合は米国国防総省規定に準拠した方式による２回上書き相当以上の方法で処理するものとする。

なお、スイッチ等については、初期化、ダミーデータの登録、初期化を連続して行う等、設定情報を２回以上上書きするものとする。

機器故障による記憶装置の交換の際も、この定めに準拠するものとする。

データ消去終了後に証明書を提出するものとする。

8　ドキュメント類の著作権

成果物に関する著作権上の取り扱いは次のとおりである。

(1) 受託事業者は著作権法（昭和 45 年法律第 48 号）第 21 条（複製権）、第 26 条の２（譲渡権）、第 26 条の３（貸与権）、第 27 条（翻訳件・翻案件等）及び第 28 条（二次的著作物の利用に関する原著作者の権利）に規定する権利を、本連合に無償で譲渡するものとする。

(2) 本連合は、著作権法第 20 条（同一性保持権）第２項に該当しない場合においても、その使用のために。本仕様書等で指定する物件を改変し、また任意の著作者名で任意に公表することかできるものとする。

(3) 受託事業者は、本連合に対して書面による事前の同意を得なければ、著作権法第 18 条（公表権）及び第 19 条（氏名表示権）を行使することができない。

(4) 受託事業者は、成果物の利用が、第三者の著作権、特許権その他の知的財産権、営業秘密、肖像権、パブリシティ権、プライバシー権、その他の権利又は利益（以下「知的財産権等」という。）を侵害していないことを保証する。

(5) 本連合又は本連合から成果物の利用を許諾された者が、 成果物の利用に関連して第三者の知的財産権等を侵害した旨の申立てを受けた場合、又は第三者の知的財産権等を侵害するおそれがあると本連合が判断した場合、事業者は、自己の費用と責任においてこれを解決するものとする。

(6) (5)の場合において、受託事業者は、本連合の指示に従い、受託事業者の費用負担において、知的財産権等の侵害のない他の成果物と交換し、成果物を変更し、又は当該第三者から成果物の継続使用・利用のために権利の取得を行わなければならない。この定めは、本連合の受託事業者に対する損害賠償の請求を妨げない。

(7) (6)の場合において、当該第三者からの申立てによって本連合又は本連合から成果物の利用を許諾された者が支払うべきとされた損害賠償額、その他当該第三者からの請求、訴訟等によって本連合に生じた一切の損害、及び申立ての対応に要した弁護士等の第三者に支払った費用その他の解決に要した費用は、受託事業者が負担するものとする。

９　検収

本業務の調達に係る納入成果物等について、納入日までに本連合に内容の説明を実施し、検収を受けるものとする。

なお、検収の結果、納入物に不備・不具合等があると判明した場合には、速やかに必要な修正、改修等を行い、変更点について本連合への説明を行った上で、指定する日時までに再度納入するものとする。

10　再委託

(1) 再委託の制限

借入れ物品及び付帯作業の調達において、原則として第三者への委託（以下、「再委託」という。）はできないものとする。

ただし、本契約を適正に履行するために、一部の範囲において再委託が必要な場合には、あらなじめ再委託を行う旨を書面により申し出て、本連合の承認を得ること。

(2) 承認の手続き

作業の一部について再委託の承認を求める場合は、次の事項を記載した文書を提出するものとする。

・再委託先の名称、代表者、所在地、連絡先
・再委託を行う内容
・再委託の理由
・再委託先の管理方法

11　機密保持及び資料の取り扱い

機密保持及び資料の取り扱いについて、以下に掲げる内容を遵守するものとする。

(1) 本業務に関して本連合が提示した情報（公知の情報等を除く）及び作業遂行過程で生じた納入成果物等に関する一切の情報を本業務の目的以外に使用又は第三者に開示もしくは漏えいしてはならないものとし、このために必要な措置を講ずること。なお、当該情報等を本業務の目的以外に使用または第三者に開示する必要がある場合は、事前に本連合と協議し、承認を得ること。

(2) 本業務を実施するにあたり、本連合から入手した資料等については、管理台帳等により適切に管理し、かつ、以下の事項を遵守すること。

ア　複製は行わないこと。ただし、本連合の許可を得た場合に限り複製を可能とする。なお、複製物についても原本と同様の取り扱いとする。

イ　本業務に必要がなくなり次第、速やかに本連合に返却すること。

ウ　情報が記録された資料について、本連合への返却を行う場合、本連合事務局総務課担当職員以外の者に返却してはならない。

エ　情報が記録された資料の破棄については、本連合の了承を得ること。

12　瑕疵担保責任

本業務の調達において納入するすべての成果物について瑕疵担保責任を負うものとし、納入成果物等瑕疵担保責任期間は、検収後１年間とする。