

仕様書

I. 納入物件

1. 納入物件と内訳

(件名) サーバー・ネットワーク機器等の調達

(1)ドメインコントローラ	2 式
(2)仮想サーバ	1 式
(3)ファイルサーバ	2 式
(4)バックアップサーバ	2 式
(5)無停電電源装置	4 式
(6)コアスイッチ	4 台
(7)メインスイッチ	1 台
(8)VPN ルータ	2 式
(9)VPN ルータ	16 式
(10)無線アクセスポイントと統合管理ソフトウェア	1 式
(11)既存サーバのデータ消去とリース返却	1 式
(12)保守運用	1 式
(13)サーバラック設備	2 式

2. 納入物件に関する留意事項

提案する機器及びソフトウェアはすでに製品化されているものから構成すること。

ただし、納品する物件が決定した後に代替の新製品が発表された場合には、当機構と協議し、システム稼働に問題ないと判断した場合は、提案した物件に替えて新製品の納品に努めること。

3. 納入スケジュールについて

新サーバシステムの検収日を令和 5 年 3 月 31 日とする。

4. 契約方法

(1) 機器と役務に関する契約について

本仕様書を元に算出した見積額（P.14 の(12)の保守運用費は除く）から全額 5 年リースとし、リース契約を取り交わすこととする。尚、リース契約先の会社は問わない。また、落札者は当機構と本件に関する業務委託契約書を取り交わすこととする。

(2) 保守に関する契約について

①ハードウェア保守

保守受付時間は平日 9:00 から 17:30 の間とし、一元窓口での受付とする。

a. 24 時間 365 日オンサイト) 全サーバ、本部のメインスイッチ、全ルータ

b. 先出 SEND バック) コアスイッチ、無線アクセスポイント

c. 平日 9 時から 17 時のオンサイト) 無停電電源装置

②ソフトウェア保守

期間内におけるソフトウェアアップデート、技術的な質問受付

③運用保守

P.14 の(12)の内容

①、②は 5 年分の保守費用を見積書に含めること。

③の運用保守費は別途月額の見積書を作成し、その月額費用を入札書に記載すること。

(3) 必要な電源と通信回線について

機器設置先で必要な電源、通信回線は当機構が準備する。必要となる電源の種類と本数、通信回線の種類と本数を提示すること。

II. 調達物品に備えるべき技術的要件

1. 包括的業務要件

以下の機能を満たすハードウェア及びソフトウェアにより構成されており、問題なく動作できること。

- ①納入物件については、十分に高い信頼性を有し、且つ納入時点での最新のものであること。また、製品の品質管理が充分に行われていること。万が一製品に欠陥または初期不良が発見された場合には、迅速に対応すること。なお、市場に流通している製品を改造したものについては、これを認めない。
- ②保守及び管理の一元化を考慮し、出来る限り統一化を図ること。
※ 用途によって統一できないものについては性能及び用途、保守対応方法について詳細の提示をもとめる場合がある。
- ③ソフトウェア、ドライバは、納入時点において、最新バージョンのものをインストールすること（セキュリティパッチも含む）。ただし、情報センター室が別途、搭載バージョンの変更指示を行う場合がある。
- ④オペレーティングソフトウェア以外のプレインストールソフトウェアの中で、情報センター室が必要ないと判断したものについてはアンインストールを行うこと。
- ⑤少なくとも稼働中のクライアント PC300 台(Windows10 Pro)を想定した設計とすること。
- ⑥Windows Server 2019 Standard Core 32 を当機構から支給し、不足分は調達とする。
- ⑦Windows Server 2019 Standard CAL は全て当機構から支給する。
- ⑧既設の LAN 及びインターネットに接続し、安定して通信できること。
- ⑨24 時間稼働が問題なく可能な機器であること。
- ⑩システム構築に際し、既設環境調査と結果報告を行うとともに、新システムの構築設計を行い情報センター室の承認を得ること。承認を得た内容に対し、構築スケジュールを作成し情報センター室の承認を得ること。
- ⑪導入するハードウェア、ソフトウェアの安定稼働を当機構が判断するまで、現行システムの安定稼働に向けた措置を行うこと。サーバ機器については令和 4 年 12 月 15 日に現行ベンダーが提供する保守が切れるため、受注者が責任をもって旧機材の稼働を確保すること。
新しく導入する機材の検収予定を 3 月とし、それまでの稼働について第三者保守契約などの対策を講じ、当機構の承認を得ることとする。
- ⑫構築期間中は週 1 回を目安に定例進捗会議を実施し、議事録を作成し、議事内容の承認を得ること。
定例進捗会議の出席者はプロジェクトマネージャーのほかに、会議内容により必要に応じてシステムエンジニア、ネットワークエンジニア、カスタマーエンジニア等を参加させること。
- ⑬納入物件については、納入後 1 年間の瑕疵期間を設定する。

2. 性能・機能に関する要件

(1) ドメインコントローラ (本部 1 式/災害対策サイト 1 式)

計 2 式

以下の条件を全て満たす機器を導入し、利用可能な状態に設定を行うこと。

- ①形状はラックマウント型であること。
- ②CPU はインテル® Xeon® E-2314 2.8GHz, 8M キャッシュ, 4C/4T, ターボ (65W), 3200 MT/s 以上であること。搭載数量は 1CPU とする。
- ③メインメモリは 16GB 以上を搭載すること。ただしメモリミラーリング機能もしくはメモリスペアリング機能を用いる場合は 8GB 以上を確保すること。
- ④HDD 装置は 480GB SSD (SATA) を 4 基以上搭載し RAID5 で構成すること。その構成に必要な機器がある場合は構成に含むこと。また障害時に電源を切らなくても HDD の交換が可能なようホットプラグ対応の機器であること。
- ⑤DVD ドライブを搭載すること。
- ⑥操作のディスプレイ、キーボード、マウスは既存機器を利用すること。
既存機器) NEC 社製 17 型 LCD コンソールユニット、サーバスイッチユニット (4Server)
- ⑦LAN ポートを 2 基以上 (1000Base-T/100Base-TX 自動認識) 持つこと。コアスイッチに接続する際、チーミングに準ずる接続により冗長性を確保する設定を実施すること。
- ⑧本体の最大消費電力は 450W 以下であること。
- ⑨本体の高さは 1U 以内であること。
- ⑩iDRAC Enterprise を用いて仮想コンソールを用いたりリモートメンテナンスが可能なこと。
- ⑪サーバに搭載するソフトウェア (調達対象※一部支給品あり)
 - a. Windows Server 2019 Standard (Device CAL は当機構から支給する)
 - b. バックアップソフトウェア (Arcserve UDP 8.0 Advanced Edition)
 - c. 電源管理用ソフトウェア (ESMPRO/UPSManager Ver2.8)
 - d. ウイルス対策ソフトウェア (Apex One※当機構から支給する)上記ソフトウェア以外で、本見積要件書で求めるシステムの構築に必要なものがある場合は別途含めること。
- ⑫本部並びに災害対策サイトにドメインコントローラを配置し、同期を図ることで業務に支障がないよう冗長性及び負荷分散を行うこと。
- ⑬現行ドメインの環境を移行するとともに、必要・不要と思われるドメインオブジェクトを選定し、情報センター室に報告・承認のうえ整理・改修すること。フォルダリダイレクト、プリンタの割り当てなど、新旧環境で変更となる箇所があるため、グループポリシーに変更を加えること。
- ⑭現行ドメインの引き継ぎ期間終了後はドメイン/フォレストの機能レベルを Windows Server 2016 へ変更すること。
- ⑮Arcserve UDP を用いて、1 日 1 回以上バックアップサーバを RPS とするバックアップを取得し、HDD 障害からの復旧の際にベアメタル復旧にて容易にシステム設定の復元を可能とすること。バックアップの管理をバックアップ管理サーバにて実施できること。
※バックアップスケジュールは業務に影響がないよう夜間で構築すること。
- ⑯ESMPRO/UPSManager を用いて、停電時に安全にシャットダウンができること。
※他のサーバと連携し、問題が発生しないようにシャットダウンの順番を設計すること。

- ⑰Trend Micro 社の Apex One を用いてウイルス対策を行うこと。ウイルス対策管理をウイルス対策管理サーバにて実施できること。
- ⑱ネットワーク監視サーバから ICMP 監視が可能になるようファイアウォール設定を実施すること。
- ⑲メーカーによる保守を付帯させること。24 時間 365 日での当日対応とし、オンサイトによる切り分け作業も含めた対応を実施することとする。HDD 障害が発生した場合は、障害機器の引き取りには応じるが、データ漏洩などが発生しないように対策を講じられていることとする。

(2)仮想サーバ (本部 1 式)

計 1 式

以下の条件を全て満たす機器を導入し、利用可能な状態に設定を行うこと。

- ①形状はラックマウント型であること。
- ②CPU はインテル® Xeon® Gold 6326 2.9G, 16C/32T, 11.2GT/s, 24M キャッシュ, ターボ, HT (185W) DDR4-3200 以上であること。搭載数量は 2CPU であること。
- ③メインメモリは 192GB 以上を搭載すること。メモリミラーリング機能もしくはメモリスペアリング機能を用いる場合は 96GB 以上を確保すること。
- ④HDD 装置は 480GB SSD (SATA) を 6 基以上搭載し RAID5 で構成すること。その構成に必要な機器がある場合は構成に含むこと。また障害時に電源を切らなくても HDD の交換が可能なようホットプラグ対応の機器であること。
- ⑤OS セットアップに利用可能なサーバメーカー純正の外付け DVD-ROM を準備すること。
- ⑥操作用のディスプレイ、キーボード、マウスは既存機器を利用すること。
既存機器) NEC 社製 17 型 LCD コンソールユニット、サーバスイッチユニット (4Server)
- ⑦LAN ポートを 4 基以上 (10GbE) 持つこと。本部用コアスイッチに接続する際、2 基ずつチームングに準ずる接続により冗長性を確保する設定を実施すること。2 基をサービス提供用とし、2 基をバックアップ用とすること。
- ⑧本体の最大消費電力は 1,400W 以下であること。また電源部に障害が発生した場合に自動的に切り替わりサーバ停止が起こらないよう冗長性を確保した構成であること。
- ⑨本体の高さは 2U 以内であること。
- ⑩iDRAC Enterprise を用いて仮想コンソールを用いたリモートメンテナンスが可能なこと。
- ⑪サーバに搭載するソフトウェア (調達対象※一部支給品あり)
- a. Windows Server 2019 Standard (Device CAL は当機構から支給する)
※仮想サーバ 6 台分のコアライセンスも調達範囲とする
 - b. バックアップソフトウェア (Arcserve UDP 8.0 Advanced Edition)
 - c. 電源管理用ソフトウェア (ESMPRO/UPSManager Ver2.8)
 - d. クライアント管理ソフトウェア (SKYSEA Client View※当機構から支給する)
 - e. ウイルス対策ソフトウェア (Apex One※当機構から支給する)
 - f. Microsoft 社 WSUS
 - g. ネットワーク監視ソフトウェア (ZABBIX)
- 上記ソフトウェア以外で、本見積要件書で求めるシステムの構築に必要なものがある場合は別途含めること。

⑫前述(1)にて構築したドメインのメンバサーバとすること。

⑬Hyper-V 機能を用いて仮想サーバを構築すること。

仮想インスタンスは次のとおりとする。(HDD は可変設定)

	サーバ	割当コア	メモリ	HDD	備考
1	バックアップ管理	2	16GB	300GB	Arcserve UDP
2	クライアント管理サーバ	8	16GB	300GB	SKYSEA Client View
3	ウイルス対策管理サーバ	4	24GB	300GB	Apex One
4	Windows Update 管理サーバ	2	8GB	700GB	WSUS
5	ネットワーク監視サーバ	2	8GB	300GB	ZABBIX
6	ファイル管理サーバ	2	16GB	300GB	NIAS (移行)

⑮バックアップ管理サーバについては Windows Server 2019 で構築し、ドメインのメンバサーバとしたうえで、Arcserve UDP8.0 を導入することとする。このサーバでバックアップ対象となるドメインコントローラ、仮想サーバ、ファイルサーバのバックアップジョブを管理するとともに、RPS として配置するバックアップサーバを管理することとする。また、ウイルス対策ソフトを導入することとし、Windows Update は別途構築する Windows Update 管理サーバの管理下に入ることとする。

⑯クライアント管理機能については Windows Server 2019 で構築し、ドメインのメンバサーバとしたうえで、現行の SKY SEA Client View を移行することとする。サーバ、クライアントによっては、サーバ監査、不許可端末検知などのオプションが導入されているため、それらが移行前同様問題なく動作するように設定すること。各クライアントが問題なく管理できるか、リモート接続（リモートデスクトップ、もしくは SKYSEA のリモート操作）を活用して動作確認すること。また、ウイルス対策ソフトを導入することとし、Windows Update は別途構築する Windows Update 管理サーバの管理下に入ることとする。

⑰ウイルス対策管理サーバについては Windows Server 2019 で構築し、ドメインのメンバサーバとしたうえで、現行の Trend Micro 社 Apex One を移行することとする。ウイルス対策ソフトを導入したネットワーク内のサーバ、クライアントを管理できること。各クライアントが問題なく管理できるか、リモート接続（リモートデスクトップ、もしくは SKYSEA のリモート操作）を活用して動作確認すること。また、ウイルス対策ソフトを導入することとし、Windows Update は別途構築する Windows Update 管理サーバの管理下に入ることとする。

⑱Windows Update 管理サーバについては Windows Server 2019 で構築し、ドメインのメンバサーバとしたうえで、Windows Server Update Services を構築すること。現在設定しているグループポリシーと連携して Update が行われるように設定すること。また、ウイルス対策ソフトを導入することとし、構築した Windows Update 管理サーバの管理下に入ることとする。

⑲ネットワーク監視サーバについては Linux で構築したうえで、ZABBIX を導入することとする。各サーバを ICMP 監視し、一定以上応答がない場合には特定のグループアドレスへメール発報するよう設定すること。またルータやスイッチについては前述の監視に加えて、SNMP を用いてトラフィックをグラフ化させること。

⑳現行サーバにて稼働しているファイル管理サーバ (IMM-FM01) を移行し、正常稼働することを確認すること。

㉑Arcserve UDP を用いて、1 日 1 回以上バックアップサーバを RPS とするバックアップを取得し、HDD 障

害からの復旧の際にベアメタル復旧にて容易にシステム設定の復元を可能とすること。バックアップの管理をバックアップ管理サーバにて実施できること。

※バックアップスケジュールは業務に影響がないよう夜間で構築すること。

②ESMPRO/UPSManager を用いて、停電時に安全にシャットダウンができること。

※他のサーバと連携し、問題が発生しないようにシャットダウンの順番を設計すること。

③Trend Micro 社の Apex One を用いてウイルス対策を行うこと。ウイルス対策管理をウイルス対策管理サーバにて実施できること。

④ネットワーク監視サーバから ICMP 監視が可能になるようファイアウォール設定を実施すること。

⑤メーカーによる保守を付帯させること。24 時間 365 日での当日対応とし、オンサイトによる切り分け作業も含めた対応を実施することとする。HDD 障害が発生した場合は、障害機器の引き取りには応じるが、データ漏洩などが発生しないように対策を講じられていることとする。

(3) ファイルサーバ (本部 1 式/災害対策サイト 1 式)

計 2 式

以下の条件を全て満たす機器を導入し、利用可能な状態に設定を行うこと。

①形状はラックマウント型であること。

②CPU はインテル® Xeon® E-2324G 3.1GHz, 8M キャッシュ, 4C/4T, ターボ (65W), 3200 MT/s 以上であること。搭載数量は 1CPU 以上であること。

③メインメモリは 16GB 以上を搭載すること。ただしメモリミラーリング機能もしくはメモリスペアリング機能を用いる場合は 8GB 以上を確保すること。

④HDD 装置は 3.84TB SSD (SATA) を 3 基以上搭載し RAID5 で構成すること。その構成に必要な機器がある場合は構成に含むこと。また障害時に電源を切らなくても HDD の交換が可能なようホットプラグ対応の機器であること。

⑤OS セットアップに利用可能なサーバメーカー純正の外付け DVD-ROM を準備すること。

⑥操作のディスプレイ、キーボード、マウスは既存機器を利用すること。

既存機器) NEC 社製 17 型 LCD コンソールユニット、サーバスイッチユニット (4Server)

⑦LAN ポートを 2 基以上 (10GbE) 持つこと。コアスイッチに接続する際、チーミングに準ずる接続により冗長性を確保する設定を実施すること。

⑧本体の最大消費電力は 600W 以下であること。

⑨本体の高さは 1U 以内であること。

⑩iDRAC Enterprise を用いて仮想コンソールを用いたリモートメンテナンスが可能なこと。

⑪サーバに導入するソフトウェア (調達対象※一部支給品あり)

a. Windows Server 2019 Standard (Device CAL は当機構から支給する)

b. バックアップソフトウェア (Arcserve UDP 8.0 Premium Edition)

c. 電源管理用ソフトウェア (ESMPRO/UPSManager Ver2.8)

d. クライアント管理ソフトウェア (SKYSEA Client View※当機構から支給する)

e. ウイルス対策ソフトウェア (Apex One※当機構から支給する)

f. レプリケーションソフトウェア (b 項のソフトウェアを流用)

⑫前述(1)にて構築したドメインのメンバサーバとすること。

- ⑬支局サーバデータを本部ファイルサーバに統合するにあたり、フォルダ構造を設計し承認を得ること。
- ⑭本部、各支局のデータ移行を行うこと。(ACL情報の移行を含む)
- ⑮Arcserve UDP を用いて、本部と災害対策サイトで共有ファイルのレプリケーションを実施すること。
サイト間複製は別途準備している L2 網を利用すること。
- ⑯Arcserve UDP を用いて、1 日 1 回以上バックアップサーバを RPS とするバックアップを取得し、HDD 障害からの復旧の際にベアメタル復旧にて容易にシステム設定の復元を可能とすること。バックアップの管理をバックアップ管理サーバにて実施できること。
※バックアップスケジュールは業務に影響がないよう夜間で構築すること。
- ⑰ESMPRO/UPSManager を用いて、停電時に安全にシャットダウンができること。
※他のサーバと連携し、問題が発生しないようにシャットダウンの順番を設計すること。
- ⑱Trend Micro 社の Apex One を用いてウイルス対策を行うこと。ウイルス対策管理をウイルス対策管理サーバにて実施できること。
- ⑲ネットワーク監視サーバから ICMP 監視が可能になるようファイアウォール設定を実施すること。
- ⑳メーカーによる保守を付帯させること。24 時間 365 日での当日対応とし、オンサイトによる切り分け作業も含めた対応を実施することとする。HDD 障害が発生した場合は、障害機器の引き取りには応じるが、データ漏洩などが発生しないように対策を講じられていることとする。

(4)バックアップサーバ (本部 1 式/災害対策サイト 1 式)

計 2 式

以下の条件を全て満たす機器を導入し、利用可能な状態に設定を行うこと。

- ①形状はラックマウント型であること。
- ②CPU はインテル® Xeon® E-2324G 3.1GHz, 8M キャッシュ, 4C/4T, ターボ (65W), 3200 MT/s 以上であること。搭載数量は 1CPU 以上であること。
- ③メインメモリは 16GB 以上を搭載すること。ただしメモリミラーリング機能もしくはメモリスペアリング機能を用いる場合は 8GB 以上を確保すること。
- ④HDD 装置は 8TB HDD (SATA) を 4 基以上搭載し RAID5 で構成すること。その構成に必要な機器がある場合は構成に含むこと。また障害時に電源を切らなくても HDD の交換が可能なようホットプラグ対応の機器であること。
- ⑤DVD ドライブを搭載すること。
- ⑥操作用のディスプレイ、キーボード、マウスは既存機器を利用すること。
既存機器) NEC 社製 17 型 LCD コンソールユニット、サーバスイッチユニット (4Server)
- ⑦LAN ポートを 2 基以上 (1000Base-T/100Base-TX 自動認識) 持つこと。
コアシッチに接続する際、チーミングに準ずる接続により冗長性を確保する設定を実施すること。
- ⑧本体の最大消費電力は 450W 以下であること。
- ⑨本体の高さは 1U 以内であること。
- ⑩iDRAC Enterprise を用いて仮想コンソールを用いたリモートメンテナンスが可能なこと。
- ⑪サーバに導入するソフトウェア (調達対象※一部支給品あり)
 - a. Windows Server 2019 Standard (Device CAL は当機構から支給する)
 - b. バックアップソフトウェア (Arcserve UDP 8.0 RPS)

c. 電源管理用ソフトウェア (ESMPRO/UPSManager Ver2.8)

d. ウイルス対策ソフトウェア (Apex One※当機構から支給する)

⑫前述(1)にて構築したドメインのメンバサーバとすること。

⑬復旧ポイントサーバ (RPS) として構築し、バックアップクライアントのデータを保存できるように構築すること。

⑭本部と災害対策サイトに設置している RPS でデータ連携を行い、片方が使用不能となってもデータをリカバリできる状態とすること。サイト間で複製を行う場合は別途準備している L2 網を利用すること。

⑮ESMPRO/UPSManager を用いて、停電時に安全にシャットダウンができること。

※他のサーバと連携し、問題が発生しないようにシャットダウンの順番を設計すること。

⑯Trend Micro 社の Apex One を用いてウイルス対策を行うこと。ウイルス対策管理をウイルス対策管理サーバにて実施できること。

⑰ネットワーク監視サーバから ICMP 監視が可能になるようファイアウォール設定を実施すること。

⑱メーカーによる保守を付帯させること。24 時間 365 日での当日対応とし、オンサイトによる切り分け作業も含めた対応を実施することとする。HDD 障害が発生した場合は、障害機器の引き取りには応じるが、データ漏洩などが発生しないように対策を講じられていることとする。

(5)無停電電源装置 (本部 3 式/災害対策サイト 1 式)

計 4 式

以下の条件を全て満たす機器を導入し、利用可能な状態に設定を行うこと。

①形状はラック型 2U 以内であること。

②APC 社 Smart-UPS 1,500VA 以上であること。

③UPS にはインタフェース拡張ボードを装着することし、各サーバとはシリアルケーブルで接続すること。

④各サーバに導入するソフトウェアと連携し、安全にシャットダウンさせる機能を有すること。

⑤平日 9 時から 17 時対応のオンサイト保守を付帯させること。

(6) コアスイッチ (本部 2 台+災害対策サイト 2 台)

計 4 台

以下の条件を全て満たす機器を導入し、利用可能な状態に設定を行うこと。

- ①1/2.5/5/10GBASE-T に対応していること。
- ②上記①を満たすインタフェースのポート数は 24 ポート以上を有すること。
- ③ラックマウントが可能であり、搭載する際に必要となるラック取り付の金具を提供すること。
- ④サイズ (高さ) は「1U 以下」とし、ラック搭載スペースを占有しない機器を選定すること。
- ⑤操作用の管理ポートを有しており、設定が可能であること。
- ⑥マネージメントポート (運用ネットワークに影響を与えることなく、ファームウェアや設定ファイルを転送したり、SNMP で情報を取得する目的で使用する管理用 Ethernet ポート) を標準搭載すること
- ⑦スイッチング容量は 640Gbps 以上を有すること。
- ⑧転送レートは 239.5Mpps 以上を有すること。
- ⑨ポートベース、プロトコルベース、IP サブネットベース等の VLAN 機能を有しており、ネットワークの分割が可能であること。
- ⑩IRF スタックによる冗長を構成し提供すること。また、スタック接続ケーブルが完全に切断されてしまう障害が発生した場合に、複数の同一設定装置がネットワーク上に出現することになり、アドレス重複障害や通信障害が発生するが、これを防ぐ機能を有すること。
- ⑪スタック接続ケーブルに関してメタルケーブル、光ケーブルのどちらでも接続可能であること。
- ⑫複数のポートを 1 つの論理グループポートとして利用できる機能を有しており、コアスイッチとサーバ間の冗長を実現できること。
- ⑬STATIC/RIP (RIP v1/v2/ng)/OSPF (OSPF v2/v3)/BGP (BGP4/4+) の動的ルーティング機能を有すること。
- ⑭電源と FAN を冗長構成とすること。
- ⑮一元的に管理可能なクラウド型統合管理サービス (無償) が提供されていること。
- ⑯購入日から出荷停止後 5 年までの間、ハードウェアを無償交換 (保障) 可能な機器であること。

(7) メインスイッチ (本部 1 台)

計 1 台

以下の条件を全て満たす機器を導入し、利用可能な状態に設定を行うこと。

- ①10/100/1000BASE-T に対応していること。
- ②上記①を満たすインタフェースのポート数は 48 ポート以上を有すること。
- ③ラックマウントが可能であり、搭載する際に必要となるラック取り付の金具を提供すること。
- ④サイズ (高さ) は「1U 以下」とし、ラック搭載スペースを占有しない機器を選定すること。
- ⑤操作用の管理ポートを有しており、設定が可能であること。
- ⑥スイッチング容量は 104Gbps 以上を有すること。
- ⑦転送レートは 77.3Mpps 以上を有すること。
- ⑧ポートベース、プロトコルベース等の VLAN 機能を有しており、ネットワークの分割が可能であること。
- ⑨IRF スタックによる冗長構成の機能を有すること。また、スタック接続ケーブルが完全に切断されてしまう障害が発生した場合に、複数の同一設定装置がネットワーク上に出現することになり、アドレス重複障害や通信障害が発生するが、これを防ぐ機能を有すること。
- ⑩STATIC ルーティング機能を有すること

⑪一元的に管理可能なクラウド型統合管理サービス（無償）が提供されていること。

⑫24時間365日の当日オンサイト保守を付帯させること。

(8)VPN ルータ（本部1式、災害対策サイト1式）

計2式

以下の条件を全て満たす機器を導入し、利用可能な状態に設定を行うこと。

①10/100/1000/2.5G/5G/10GBASE-Tに対応していること。

②インタフェースのポート数は、4ポート以上有すること。

③サイズ（高さ）は「1U以下」とし、ラック搭載スペースを占有しない機器を選定すること。

④ラックマウントが可能であり、搭載する際に必要となるラック取り付けの金具、もしくは棚を提供すること。

⑤IPv4 PPPoE、IPv6PPoEの機能を有すること。

⑥IPSecの機能を有すること。

⑦動的ルーティングのRIP、OSPF、BGPの機能を有すること。

⑧IPSec性能は4Gbps以上であること。

⑨NEC Net Meisterで管理が可能なこと。

⑩各支局とVPN接続できるように設定すること。

⑪外部から機構のPCがVPN接続でアクセスできるように設定すること。PC台数は300台を想定している。

⑫24時間365日の当日オンサイト保守を付帯させること。

(9)VPN ルータ（トレーニングセンター3式、支局13式）

計16式

以下の条件を全て満たす機器を導入し、利用可能な状態に設定を行うこと。

①10/100/1000GBASE-Tに対応していること。

②インタフェースのポート数は、8ポート以上有すること。

③サイズ（高さ）は「1U以下」とし、ラック搭載スペースを占有しない機器を選定すること。

④据え置き用のスタンドを準備すること。

⑤IPv4 PPPoE、IPv6PPoEの機能を有すること。

⑥IPSecの機能を有すること。

⑦動的ルーティングのRIP、OSPF、BGPの機能を有すること。

⑧IPSec性能は1.3Gbps以上であること。

⑨NEC Net Meisterで管理が可能なこと。

⑩本部、災害対策サイトにVPN接続できるように設定すること。

⑪24時間365日の当日オンサイト保守を付帯させること。

(10) 無線アクセスポイントと統合管理ソフトウェア

計 1 式

以下の条件を全て満たす機器を導入し、利用可能な状態に設定を行うこと。

- ①10BASE-T/100BASE-TX/1000BASE-T/2.5GBASE-Tに対応していること。
- ②上記①を満たすインタフェースのポート数は2ポート以上を有すること。
- ③無線アクセスポイントの台数は以下とすること

拠点	台数
本部/東京支局	4台
災害対策サイト（北陸支局）	1台
その他の支局、トレーニングセンター（計16か所）	各1台

- ④無線アクセスポイントはスマートなデザインであり、壁への取付け金具を含むこと。PoEインジェクターも添付すること。
- ⑤本部以外について、本機器はルータ近辺への設置を予定している（机上や棚上等への据え置き）。ただし、電波の到達に支障がある場合において、ルータと離して設置する場合、壁等への取付けが必要となった場合の工事については、別途費用で対応すること。
- ⑥無線の規格については、Wi-Fi6に対応していること。アンテナは内蔵とし6本有すること。
- ⑦無線の周波数に対しては、5GHz帯、2.4GHz帯を同時利用が可能であること。
- ⑧WPA3、WPA2の両方をサポートしていること。
- ⑨暗号化方式はAESとTKIPに対応していること。
- ⑩MACアドレスフィルタリングの機能を有すること。
- ⑪5GHz帯に優先接続を促す「無線バンドステアリング機能」、クライアントの無線通信時間を一定にする「無線通信公平化機能」など、無線LANで発生する問題への対策機能を実装し、通信の安定化を実現可能なこと。
- ⑫設計上、1台の無線アクセスポイントで2.4GHz帯と5GHz帯それぞれに各512台（合計1024台）の端末接続が可能なこと。
- ⑬統合管理ソフトウェアについては、クラウドでの管理システムを提供すること。
- ⑭統合管理ソフトウェアについては、端末間の通信は統合管理ソフトウェアを経由しないものであること。又、障害等により統合管理ソフトウェアが利用できない状態であっても無線アクセスポイントは継続利用が可能であること。
- ⑮無線アクセスポイント本体は5年間の先出センドバック保証が付帯されていること。

①以下の各サーバに対しデータ消去を実施すること。作業は当機構内で実施することとし、消去レベルは米国国防総省準拠方式とする。データ消去ログと消去作業証明書を提出すること。

- a. 本部設置のラックマウント型サーバ4台、タワー型サーバ4台
- b. 北陸支局設置のラックマウント型サーバ2台、タワー型サーバ5台
- c. 各支局（北陸支局と東京支局を除く）、トレーニングセンターに設置しているタワー型サーバ各1台（総数16台）

※ただし、データ消去を実施しない機器が発生する場合は別途指示する。

②以下の各ネットワーク機器に対し設定データの消去を実施すること。作業は当機構内で実施することとする。

- a. 本部設置機器
ルータ1台、ファイアウォール1台、メインスイッチ1台、コアスイッチ2台
アクセスポイント4台（PoEインジェクタを含む）、アクセスポイント管理装置1台
- b. 北陸支局設置機器
ルータ1台、ファイアウォール1台、メインスイッチ1台、コアスイッチ2台
アクセスポイント1台（PoEインジェクタを含む）、アクセスポイント管理装置1台
- c. 各支局（北陸支局と東京支局を除く）、トレーニングセンター設置機器
ルータ1台、アクセスポイント1台（PoEインジェクタを含む）

③以下の機器について廃棄を行うこと。

- a. ①、②の各機器
- b. 本部設置のラックマウント型UPS 3台
- c. 北陸支局設置のラックマウント型UPS 2台
- d. 各支局、トレーニングセンター設置の据置型UPS各1台 総数17台（北陸支局含む）

なお廃棄に際し産廃許可免許を有しない場合は、当該作業を委託してもよいが、費用清算についてはその行為を代行すること。また本案件の見積もりにその費用を含めること。

廃棄証明としてマニフェストの交付を行うこととする。

(12) 保守運用

1 式

以下の内容を満たす保守契約の月額見積もりを入札書の内訳に記載すること。また、リース物件の再リースを行った場合、本保守契約についても同額で継続できること。

- ①障害、問い合わせ窓口を平日 9:00～17:30 の間で準備すること。夏季、年末年始等で窓口を閉める場合は事前に連絡すること。
- ②対応速度を向上させるためにリモートメンテナンスの手段を準備すること。ただし、リモートメンテナンス設備、ならびに実行環境は情報セキュリティの観点から、ISMS 認証取得サイトであること。
- ③システム障害、ハードウェア障害発生時に遅くとも翌営業日に対応可能な体制を設けること。
リモート対応不可による対応遅延はこれを認めない。
- ④年 1 回の災害対策サイト稼働訓練（休日 1 日想定）を実施すること。
- ⑤月 8 時間までのリモート対応工数を確保すること。訪問工数、ならびに 8 時間を超える工数が発生した場合は超過費用で対応すること。

(13) サーバラック設備

2 式

- ①前述の機器をすべて既設ラック内に搭載すること。
- ②すべてのサーバが一つのディスプレイ、マウス、キーボードで操作ができるよう既設のディスプレイ、キーボード切替器で利用可能とすること。
- ③動作に必要なケーブル類や機器を耐震固定する器具、棚、結束バンドなどを準備すること。
- ④保守管理上、接続されるケーブルがどのサーバに接続されているか判断できるようタグをつけること。

3. 性能・機能以外の要件

1) 設置条件等

1-1) 設置場所

公益財団法人 国際人材育成機構

本部/東京支局)

東京都中央区日本橋堀留町 2 丁目 4-3 日本橋堀留町 2 丁目ビル 7 階

支局、トレーニングセンター)

北海道支局 北海道札幌市北区北十条西 4-1-19 楠本第 10 ビル 7 階

東北支局 宮城県仙台市宮城野区榴岡 5-8-11 ナガイビル 6 階

埼玉支局 埼玉県さいたま市浦和区仲町 1-14-8 大樹生命浦和ビル 5 階

高崎支局 群馬県高崎市宮元町 227 高崎ステージビル 6 階

長野支局 長野県松本市島内 3505 インペリアルプラザ松島 2 階

静岡支局 静岡県浜松市中区連尺町 314-31 アーバンスクエア浜松ビル 7 階

東海支局 愛知県名古屋市中区丸の内 1-8-24 綿常第 5 ビル 9 階

北陸支局 富山県富山市北新町 2-2-7 今井ビル 4 階

関西支局 大阪府大阪市中央区内本町 1-3-5 いちご内本町ビル 10 階

広島支局 広島県広島市南区的場町 1-3-6 広島の場ビル 3 階

松山支局 愛媛県松山市三番町 4-4-6 松山センタービル 2 号館 3 階

福岡支局 福岡県福岡市博多区奈良屋町 3-1 ヒロカネビル 3 階

熊本支局 熊本県熊本市中央区細工町 4-12-12 S R ビル 4 階

沖縄支局 沖縄県那覇市天久 2-30-27 元氣堂天久ビル 2 階

春日部トレーニングセンター1号館 埼玉県春日部市中央 2-20-1

春日部トレーニングセンター2号館 埼玉県春日部市中央 2-21-10

春日部トレーニングセンター3号館 埼玉県春日部市大畑 7-3

1-2) 構築期間

契約締結日～令和 5 年 3 月 31 日

1-3) 設備要件

- ①原則として、既存電源設備（単相 100V）で機器が正常に稼動すること。
- ②原則として、機器用の電源コンセントは既設の規格のものを使用すること。ただし、コンセントの形状が異なる場合には、受注者が変換アダプタ等を用意すること。

1-4) 搬入、据付、配線、調整

- ①納入場所・納入日時・設置場所の詳細については情報センター室の指示に従うこと。作業の際のシステムの停止等の業務への影響は最小限度であること。
- ②導入機器の設置場所への搬入、据付、配線、調整、ネットワーク接続、機器設定、ソフトウェア設定、動作に必要な全ての作業を行い、各機器の動作確認及び既設 LAN を含むネットワーク全体の動作確認を行うこと。IP アドレス等 LAN の接続に必要な情報等詳細は別途指示する。
- ③機器の接続に必要なケーブル類を用意し、ネットワーク接続を行うこと。配線は美観を損なわないように注意すること。
- ④機器の納入時に、情報センター室が必要と認めた場合は搬入導線の養生を行うこと。

- ⑤梱包資材のうち情報センター室が不要と判断したものは、納入後、責任を持って処分すること。
- ⑥既設サーバは、データの移行後、HDD内のデータの消去を行うこと。作業は当機構内で実施することとし、消去レベルは米国国防総省準拠方式とする。
- ⑦廃棄する既設サーバ機器等について廃棄証明書を発行すること。
- ⑧これまで使用していた機器について、継続して活用されるもの及び廃棄する機器については情報センター室が指示する場所へ移動すること。
- ⑨作業全体において、不測の事態が発生した場合を考慮したスケジュール案と体制図を提出すること。

2) 保守契約等

- ①システム利用期間中（5年間を想定）において本部及び各支局、トレーニングセンターの障害発生時に迅速に対応できる体制を確保していること。障害発生時には、情報センター室及び財団職員からの通報後速やかに保守員が到着し、復旧作業を行うこと。障害復旧後、情報センター室に対しその障害の原因等に関する報告を行うこと。
- ②前記①項が確保されていることを証明するために、連絡体制を含む保守体制表を事前に提出すること。また、電話、FAX、電子メールによる質問・問い合わせ等を受け付けるための対応窓口を提出すること。
- ③保守対象のハードウェアは本調達で導入される全機器とする。
- ④ハードウェア保守に関する契約は平日 9:00 から 17:30 の時間帯における受付、並びにオンサイト対応を実施することとする。ただし、本部に設置する仮想サーバとファイルサーバについては 24 時間 365 日のオンサイト対応とする。コアスイッチと無線アクセスポイントについては先出し SEND バック対応とする。ハードウェア保守の契約期間は 5 年間とすること。
ただし、重大な障害発生の際は、時間外でも対応を依頼することがあるため、その際は可能な限り対応を行うこと。
- ⑤障害解決に 2 日以上を要する場合、受注者は同機種か同機能を有する機器等を情報センター室の事前の承諾を得て代替設置すること。
- ⑥障害復旧後は、システム全体及び当該機器以外のネットワーク機器についても稼動状態の正常性を確認すること。
- ⑦当機構が行うプログラム開発、性能・機能向上に伴う作業、及び既存機器の利用に関して、必要な技術情報を提供すること。
- ⑧導入機器の円滑な運用と有効な利用を図るため、操作説明を十分に行うこと。
- ⑨各種機器に必要な消耗品について、品名、型番、メーカー名、対応機種、価格等に関するリスト又はカタログを提供すること。

3) 納品物

- ①調達機器（ソフトウェア設定済）及び添付品
- ②機器及びソフトウェアのマニュアル
- ③ハードウェア、ソフトウェア設定書（詳細なもの）
- ④運用管理手順書（詳細なもの）

4) リース機器について

- ①本調達におけるリース物品の再リースを可能とすること。
- ②本調達におけるリース物品のリース期間満了後は、本調達機器の返還及び室内の現状復帰を行うこと。その際、HDD 内のデータの消去を行うこと。作業は当機構内で実施することとし、消去レベルは米国国防総省準拠方式とする。

5) その他

費用には、ハードウェア及びソフトウェア（当機構支給以外）の他、設置・動作確認作業費、動作検証にかかる費用、現場調査費用、保守費、既存ベンダー支援費等のすべての費用を明示すること。