国立研究開発法人建築研究所
情報資産管理システム導入及び運用保守支援業務
調達仕様書

令和６年３月

国立研究開発法人建築研究所

本調達仕様書は、国立研究開発法人建築研究所情報資産管理システム導入及び運用保守支援業務に関して、受注者が実施すべき業務について定めるものである。

目次

1 件名 1
2 数量 1
3 納入場所 1
4 借入及び運用保守期間 1
5 業務の範囲 1
6 仕様書概要説明 1
6.1 システムの基本的要件 1
6.2 本業務の全般的要件 2
6.2.1 共通要件 2
6.2.2 業務の実施日及び業務の実施時間 2
6.2.3 業務計画書の作成 3
6.2.4 本業務の引継ぎ 3
6.3 調達物品名及び構成内訳 4
6.4 技術的要件の概要 4
6.5 その他 4
7 システムの要求要件 5
7.1 情報セキュリティ上のサプライチェーン・リスク対応 5
7.2 設計、運用上の責任 6
7.3 ActiveDirectory および二要素認証システム 6
7.3.1 ActiveDirectory サーバ 6
7.3.2 二要素認証サーバ 7
7.3.3 二要素認証ソフトウェア 9
7.4 IT 資産管理システム 9
7.4.1 IT 資産管理サーバ 9
7.4.2 IT 資産管理ソフトウェア 11
7.5 ID 連携システム 12
7.6 ファイルサーバ 14
7.6.1 ファイルサーバ 14
7.6.2 バックアップ世代管理用サーバ 15
7.6.3 ファイルサーバ管理ソフトウェア 16
7.7 バックアップシステム 18
7.7.1 バックアップサーバ 18
7.8 サーバ集約スイッチングハブ 18

7.9　ネットワーク監視サーバ 20
7.10　無停電電源装置 21
7.11　19インチラック 21
8　性能、機能以外の要件 21
8.1　搬入、据付、配線、調整、分電盤・電源配線等の付帯電気工事及び撤去について 21
8.2　システムの導入について 21
8.3　現行システム資産の移行に関する要件 23
8.3.1　移行における基本要件 23
8.3.2　移行計画及び関連ドキュメントの作成 23
8.4　保守サービス 24
8.4.1　保守サービスについて 24
8.4.2　障害受付窓口対応 24
8.4.3　ハードウェア保守サービス 24
8.4.4　ソフトウェア保守サービス 24
8.5　業務の管理 25
8.6　サービスレベルアグリーメント（SLA）の締結について 26
8.6.1　SLAの締結 26
8.6.2　SLAの改訂 27
8.6.3　SLAに係る免責事項 27
8.6.4　SLAに係る是正処置 27
8.7　システム運用管理サポート、エンドユーザサポートについて 27
8.7.1　システム運用管理サポート 27
8.7.2　エンドユーザサポート 29
8.7.3　稼動状況報告 29
8.8　説明書・マニュアル等の要件 30
8.9　検査 30
8.10　契約不適合責任 30
8.11　特記事項 30
8.11.1　知的財産権 30
8.11.2　委託・再委託 31
8.11.3　閲覧資料及び実施場所の確認 32
8.11.4　機密保持 32
8.11.5　検収時における注意事項 33
8.11.6　賃貸借期間終了後の導入品について 33
8.12　その他 33
8.13　疑義 34

1　件名

国立研究開発法人建築研究所情報資産管理システム導入及び運用保守支援業務

2　数量

一式

3　納入場所

茨城県つくば市立原１番地３

国立研究開発法人建築研究所

4　借入及び運用保守期間

令和６年１２月１日から令和１１年３月３１日まで（５２ヶ月）

ただし、令和 10 年 4 月 1 日から令和 11 年 3 月 31 日までの間については、当該期間にかかる中長期計画に対する国土交通大臣の認可を条件とする。

5　業務の範囲

本業務の範囲は、ActiveDirectory、二要素認証システム、IT 資産管理システム、ID 連携システム、ファイルサーバ及びバックアップサーバからなる情報資産管理システムの賃貸借及び導入、これらを安定的かつ適切に稼働させるためのシステム運用管理、エンドユーザサポートとする。

6　仕様書概要説明

6.1　システムの基本的要件

導入を計画している情報資産管理システムにおいて、必要とされる基本的要件は以下のとおりである。

(1) 信頼性の高いシステムであること。
(2) 高度なシステムの可用性が提供できること。
(3) 高度なセキュリティのネットワークを提供できること。
(4) 利用者、資源等の管理及びシステム運用が、高度かつ柔軟に行える機能を有すること。
(5) システムの構築及び既設の共用計算機システムとの連携を円滑に行えること。
(6) コンパクトで省電力に優れていること。
(7) システムのトータルバランスに配慮がされていること。
(8) サービス・システムは汎用的で複数ベンダーの製品に入替可能であること。
(9) 他システムとの連携が容易な製品が選定されていること。

6.2　本業務の全般的要件

6.2.1 共通要件

(1) 本業務の実施に際しては、諸法規及び条例等を遵守すること。

(2) 本調達仕様書に明記されていない事項についても、業務遂行上必要と認められるものについては、発注者と協議し、受注者の責任において充足すること。

(3) 本業務の実施に際しては、各種ネットワークサーバ、ネットワーク機器、運用管理サーバからなる既設の共用計算機システム（以下「既設システム」という。）及び本システムが提供する各種機能に影響を与えないことを前提とし、確実に実施すること。ただし、受注者が検討した結果、どうしても当該機能への影響を回避できないと判断した場合は、監督職員に影響について報告し対応を協議すること。

(4) 本業務の実施に際しては、利用者に対する業務停止時間の低減を考慮した作業手順とすること。

(5) 受注者は、本業務の遂行に必要な施設、設備等として、次に掲げる施設、設備等を適切な管理の下、無償で使用することができる。

① 業務に必要な電気、PC 端末等

② ②その他、当所と協議し、承認された業務に必要な施設、設備等

③ ③本業務に必要なライセンス及び ID などの一時貸与

(6) 上記(5)において無償使用する施設、設備等について、本業務の実施及び実施に付随する業務以外の目的で利用してはならない。

(7) 受注者はあらかじめ、監督職員と協議した上で、発注者の業務に支障を来たさない範囲内において、施設内に本業務の実施に必要な設備等を持ち込むことができる。

(8) 受注者が本業務の実施に伴い必要となる作業で、発注者の施設内の作業場所を使用する場合は、事前に監督職員に申請し、承諾を得なければならない。

(9) 受注者は、作業場所を整理・整頓し、安全に留意して事故の防止に努めるとともに、関係法令等を遵守して、安全の徹底を図り、作業すること。

(10) 受注者は、設備等を設置した場合は、設備等の使用を終了又は中止した後、直ちに、必要な原状回復を行うこと。

(11) 受注者は、既存の建築物及び工作物等に、汚損、損傷等を与えないよう十分注意し、損傷（機器の故障等を含む。）が生じるおそれがある場合は、養生を行うこと。万一損傷が生じた場合は、受注者の責任と負担において速やかに復旧すること。

(12) 本業務の遂行上必要な消耗品は、発注者の負担において準備するので、受注者は損傷及び紛失等無いよう取り扱うこと。

6.2.2 業務の実施日及び業務の実施時間

本業務の実施日及び実施時間は、当所の業務日の通常業務時間（8 時 30 分から 17

時 15 分まで）とする。なお、事前に予想しえない突発的なシステム障害、情報セキュリティに係る事故等の緊急に作業が必要と判断される場合においては、前記の通常業務時間以外においても業務を行うこと。ただし、災害対応については、別途協議する。

6.2.3 業務管理責任者の通知及び業務計画書の作成

(1) 受注者は契約後、本業務の管理を行う業務管理責任者を定め、その氏名その他必要な事項を書面をもって発注者に通知すること。業務管理責任者を変更したときも同様とする。

(2) 受注者は契約締結後速やかに業務計画書を作成し、監督職員へ提出すること。

(3) 業務計画書の記載内容は主に以下を想定しているが、詳細は監督職員と事前に協議し決定すること。

① 業務概要
② 業務工程
③ 業務実施体制（業務実施計画と要員との対応関係、体制、監督職員との関係、連絡先（緊急連絡先を含む。）を含む。）
④ 業務実施計画（業務の実施内容、実施フロー、実施手順を含む。）
⑤ 業務管理計画（安全管理計画、品質管理計画、課題管理計画、リスク管理計画、情報セキュリティ管理計画を含む。）
⑥ サービスレベルアグリーメント（SLA）に関する項目
⑦ 業務報告計画（方法及び様式を含む。）
⑧ 情報取扱者名簿及び情報管理体制図
⑨ その他

(4) 受注者は、業務計画書の内容を変更する場合は、理由を明確にしたうえで、その都度監督職員に変更業務計画書を提出すること。

(5) 監督職員が指示した事項については、さらに詳細な業務計画に係る資料を提出すること。

6.2.4 本業務の引継ぎ

受注者は、本業務期間満了の際、業者変更が生じた場合は、次回業務の受注者に対し、次回業務の落札決定から業務期間の開始までの間に必要な業務引継ぎを行わなければならない。

また、当所は、当該業務引継ぎが円滑に実施されるよう、受注者及び次回業務の受注者に対して必要な措置を講ずるとともに、引継ぎが完了したことを確認する。

なお、当該業務引継ぎの際に発生した経費は受注者の負担とする。次回業務の受注者に発生した経費は、次回業務の受注者の負担とする。

6.3　調達物品名及び構成内訳

情報資産管理システムは原則として下記ハードウェア及びソフトウェアで構成する。

(1) ActiveDirectory および二要素認証システム　1式
　① ActiveDirectory サーバ
　② 二要素認証サーバ
　③ 二要素認証ソフトウェア
(2) IT 資産管理システム　1式
　① IT 資産管理サーバ
　② IT 資産管理ソフトウェア
(3) ID 連携システム　1式
(4) ファイルサーバ　1式
　① ファイルサーバ
　② バックアップ世代管理用サーバ
　③ ファイルサーバ管理ソフトウェア
(5) バックアップサーバ　1式
(6) サーバ集約スイッチ　1式
(7) ネットワーク監視サーバ　1式
(8) 無停電電源装置　1式
(9) １９インチラック　1式

6.4　技術的要件の概要

(1) 本調達物品に係る性能、機能及び技術等の要求要件は、「7. システムの要求要件」「8. 性能・機能以外の要件」に示す。
(2) 本仕様書に示す各要件は最低限の要求要件であり、全ての要求要件を満たす必要がある。

6.5　その他

(1) 使用する機器及びソフトウェアは、入札時点で全て製品化されていること。入札時点で製品化されていない機器、又はソフトウェアにより応札する場合には、要件を満たすこと及び納入期限までに製品化され納入できることを証明できる書類を添付すること。
(2) 導入に関して、導入時スケジュールは監督職員と協議し、その指示に従い導入機器の搬入・設置を行うこと。なお、調達物品のうち、ActiveDirectory サーバ及び ID 連携システムは令和６年 10 月 1 日から稼動開始すること。システムの本運用開始は令和６年 12 月 1 日とする。

(3) 搬入、据付、配線、調整、既設設備との接続、分電盤・電源設備等の付帯電気工事、ハードウェア・ソフトウェア保守、印刷マニュアル等に要する全ての費用は、本調達に含まれる。

(4) 借入物品の故障時、撤去時及び本業務期間満了時には、受注者の費用において借入物品の内蔵記憶装置のデータ内容を復元不可能となるよう完全に消去した上で、借入物品を回収すること。消去作業は当所で指定する方式により当所内で実施するものとし、消去完了後はデータ消去方法、消去回数、対象機器を記載した「データ消去完了報告書」を提出すること。

7　システムの要求要件

7.1　情報セキュリティ上のサプライチェーン・リスク対応

(1) 選定予定の機器について、本業務の競争参加資格技術審査申請書提出時に、予め当所に機器等リストを提出すること。なお、当所がサプライチェーン・リスクに係る懸念が払拭されないと判断した場合には、代替品選定やリスク低減対策等、当所と迅速かつ密接に連携し提案の見直しを図ること。

(2) 当該機器等は製造工程において意図しない変更が加えられないよう適切な措置がとられており、当該措置を継続的に実施していること。また、当該措置の実施状況を証明する資料を提出すること。

(3) 当該機器等は製造工程の履歴に関する記録を含む製造工程の管理体制が適切に整備されていること。また、当該管理体制を証明する資料を提出すること。

(4) 当該機器等に対して不正な変更が加えられないように製造者等が定めたセキュリティ確保のための基準等が整備されており、その基準等が当該機器等に適用されていること。また、それらを証明する資料を提出すること。

(5) 当該機器等の設計から部品検査、製造、完成品検査に至る工程について、不正な変更が行われないことを保証する管理が一貫した品質保証体制の下でなされていること。機器に不正が見つかったときに、追跡調査や立入検査等、当所と迅速かつ密接に連携して原因を調査し、排除できる体制を整備している生産工程による製品であること。

(6) 情報システムを構成する要素(ソフトウェア及びハードウェア)に対して不正な変更があった場合に識別できる構成管理体制が確立していること。また、当該構成管理体制が書類等で確認できること。

(7) 受注者が情報システムを構成する要素(ソフトウェア及びハードウェア)として採用した機器等について、不正な変更が加えられていないことを検査する体制が受注者において確立していること。また、当該検査体制が書類等で確認できること。

(8) 納入する機器等の開発工程、製造工程等において、下記①から⑤の情報セキュリティに係るサプライチェーン・リスクを低減する対策が行われていること。

① 開発工程において信頼できる品質保証体制が確立されていること。
② 脆弱性検査等のテストの実施が確認できること。
③ 製造工程における不正行為の有無について、定期的な監査が行われていること。
④ 製造者が不正な変更を加えないよう、サプライチェーン全体が適切に管理されていること。
⑤ 不正な変更が発見された場合に、当所と受注者が連携して原因を調査・排除できる体制を整備していること。

7.2 設計、運用上の責任

(1) 検収後の運用上の不具合等に関しては、導入したシステムに関して関連性がある場合、既設システムとの連携、関係性など切り分けを実施し、不具合解消を行うこと。切り分けに関しては、接続元の末端から接続先までを対象に、関わるシステムを把握して切り分けを行い、解決策を提示し、対応すること。
(2) 運用に関しては、今後のシステム導入に合わせ柔軟に対応できるように設計をしなければならない。(今後の予定などについてヒアリングを行い設計コンセプトに含めること)
(3) 契約後、受注者は、落札費用内で、システム設計について当所と合意をとって、期日までに導入し、運用を行えるようにすること。
(4) セキュリティポリシー及び統一基準群を把握して、各種のセキュリティ要素を組み込み設計を行うこと。

7.3 ActiveDirectory および二要素認証システム

7.3.1 ActiveDirectory サーバ

(1) 導入要件
① オンプレミス環境に 2 台以上導入すること。
② ウイルス対策ソフトを令和 6 年 10 月 1 日より、1 年間利用できるよう導入すること。
③ CPU 処理能力がインテル® Xeon® プロセッサー E-2334 相当以上であること。
④ メモリ容量が 16GB 以上であること。
⑤ OS が Windows Server Standard 2022 以上であること。
⑥ ディスク数が HDD600GB×2 以上であること。
⑦ RAID1/5/6 を使用して構築すること。
⑧ 1000BASE-T ネットワークポートは４つ以上有すること。
⑨ 標準的な 19 インチラックに収容できること。
⑩ DVD-ROM ドライブを内蔵もしくは外付けで用意すること。
⑪ 筐体前面に、施錠可能なカバーを装着可能で、サービス状態や温度、マシン名

を文字で表示可能なLCDパネルを有すること。

⑫ 障害検知機能を有し、ネットワーク経由での遠隔監視が可能であること。

⑬ IPMI2.0に対応したリモート管理用コントローラを搭載し、OSの状態に依存せずにネットワーク経由でのサーバの管理/制御（電源管理、仮想コンソール/仮想メディア）が可能であること。また、専用のネットワークポートを有しており、HTML5により管理可能なこと。

⑭ PCI スロットに搭載される各拡張カード毎に最適な冷却ができるよう、サーバ内部のファンが温度センサーの情報やファンの電力消費、エアフローを考慮し自動的に回転数を制御する機能を有すること。

⑮ システムセキュリティの観点から、BIOSやフォームウェアについて意図しないもしくは悪意のある変更から保護する為、これらのバージョンアップや設定変更を禁止する機能を持つこと。またBIOSイメージおよびOSイメージに破損または悪意ある改ざんがあった場合、サーバの内蔵機能による正常なイメージへの自動復旧が可能であること。

⑯ 保守管理用にシリアル番号を記録できるように引出し式のラベルパネルがあること。

(2) 機能要件

① Active Directoryを導入し､ユーザアカウント及び端末の一元管理を行うこと。

② 2台のActiveDirectoryサーバを所内における各ネットワークセグメントに適切に配置し、サーバ間でユーザ情報等のレプリケーションを行うこと。また、所内におけるネットワークセグメント間のセキュリティを踏まえた構成とすること。

③ 本調達に含まれる ID 連携システムを導入し、アカウントの統合管理を行うこと。

④ 所内で導入しているMicrosoft 365のテナントとアカウント情報を同期できる構成とすること。

⑤ クライアント環境（端末等）の設定変更は本調達の範囲外とする。但し、滞りなくActiveDirectoryを利用できるよう、利用者向けの設定変更手順書を提供し、発注者の指定する端末に対し、実施すること。
同手順について、既設システムにて作成されている新規端末セットアップ手順書を発注者より提供するので、前後関係を考慮の上追記すること。

⑥ システムバックアップを取得できる構成とし、障害等で OS 起動不可となった際にバックアップからシステムデータを復旧できること。

7.3.2 二要素認証サーバ

(1) 導入要件

① オンプレミス環境に 2 台以上導入すること。
② ウイルス対策ソフトを令和 6 年 10 月１日より、１年間利用できるよう導入すること。
③ CPU 処理能力がインテル® Xeon® プロセッサー E-2334 相当以上であること。
④ メモリ容量が 16GB 以上であること。
⑤ OS が Windows Server Standard 2022 以上であること。
⑥ ディスク数が HDD600GB×2 以上であること。
⑦ RAID1/5/6 を使用して構築すること。
⑧ 1000BASE-T ネットワークポートは４つ以上有すること。
⑨ 標準的な 19 インチラックに収容できること。
⑩ DVD-ROM ドライブを内蔵もしくは外付けで用意すること。
⑪ 筐体前面に、施錠可能なカバーを装着可能で、サービス状態や温度、マシン名を文字で表示可能な LCD パネルを有すること。
⑫ 障害検知機能を有し、ネットワーク経由での遠隔監視が可能であること。
⑬ IPMI2.0 に対応したリモート管理用コントローラを搭載し、OS の状態に依存せずにネットワーク経由でのサーバの管理/制御（電源管理、仮想コンソール/仮想メディア）が可能であること。また、専用のネットワークポートを有しており、HTML5 により管理可能なこと。
⑭ PCI スロットに搭載される各拡張カード毎に最適な冷却ができるよう、サーバ内部のファンが温度センサーの情報やファンの電力消費、エアフローを考慮し自動的に回転数を制御する機能を有すること。
⑮ システムセキュリティの観点から、BIOS やフォームウェアについて意図しないもしくは悪意のある変更から保護する為、これらのバージョンアップや設定変更を禁止する機能を持つこと。また BIOS イメージおよび OS イメージに破損または悪意ある改ざんがあった場合、サーバの内蔵機能による正常なイメージへの自動復旧が可能であること。
⑯ 保守管理用にシリアル番号を記録できるように引出し式のラベルパネルがあること。

(2) 機能要件
① 二要素認証ソフトウェアを導入し、所内の端末を対象とした二要素認証を行うこと。認証方式は顔認証とする。
② 冗長構成とし、単一サーバ停止時においても二要素認証を実施できること。
③ クライアント環境（端末等）の設定変更は本調達の範囲外とする。但し、滞りなく二要素認証システムを利用できるよう、利用者向けの設定変更手順書を提供すること。
同手順について、既設システムにて作成されている新規端末セットアップ手順

書を発注者より提供するので、前後関係を考慮の上追記すること。

④ システムバックアップを取得できる構成とし、障害等で OS 起動不可となった際にバックアップからシステムデータを復旧できること。

7.3.3 二要素認証ソフトウェア

二要素認証ソフトウェアとして、以下の仕様を満たすソフトウェアを 120 式納入すること。

(1) 既存の Active Directory ドメインサーバを変更しないこと。(ソフトウェア等をインストールしたり、認証情報を保存したりしないこと。)

(2) 異なるドメイン環境においても、ドメイン間で認証情報を共有することなく、認証/設定管理サーバで一元管理ができること。

(3) 認証/設定管理サーバは、ユーザの属性や Windows 認証のための情報、アプリケーション権限、暗号鍵、アプリケーション認証用パスワード、クライアント設定情報などを管理、格納できること。

(4) 認証/設定管理サーバは、クライアント端末にインストールするクライアントモジュールの設定情報を管理し、ネットワーク経由で自動的にクライアントモジュールの更新インストール作業を行う機能を有すること。

(5) 認証/設定管理サーバは、冗長化及び負荷分散構成が可能であること。

(6) 顔認証のエンジン部分の機能を同一メーカーだけでなく、複数社選択できること。

(7) QR コードを使用した認証機能と併用できること。

(8) 顔認証成功/失敗時の画像を保存する機能を有すること。また、保存する画像は暗号化されていること。

(9) 顔認証エンジンのロバスト性向上に加えて、マスク着用有無の判定結果を用いる独自の照合アルゴリズムにより、社内評価においてマスク着用時の 1:1 認証の認証率（他人受入率 10 万分の 1 の時の本人受入率）で 99.9%以上を実現していること。

(10) マスク着用時に照度変化や顔の向き、角度変動があった場合でも本人認証エラーを低減する仕組みを用いていること。

(11) ユーザ情報を CSV ファイルで、認証/設定管理サーバにインポートするツールを有すること。

(12) 親和性の関係から、現在稼働している EDR のシステムに、この主体認証ソフトで適用した固有のアカウント情報を EDR のログで取得できること。

7.4 IT 資産管理システム

7.4.1 IT 資産管理サーバ

(1) 導入要件

① オンプレミス環境に 1 台以上導入すること。

② ウイルス対策ソフトを令和 6 年 10 月 1 日より、1 年間利用できるよう導入すること。
③ CPU 処理能力がインテル® Xeon® プロセッサー E-2378 相当以上であること。
④ メモリ容量が 32GB 以上であること。
⑤ OS が Windows Server Standard 2022 以上であること。
⑥ ディスク数が HDD1.2TB×3 以上であること。
あわせて、OS 領域用に M.2 SSD カード 480GB×2 以上を搭載すること。
⑦ RAID1/5/6 を使用して構築すること。
⑧ 1000BASE-T ネットワークポートは４つ以上有すること。
⑨ 標準的な 19 インチラックに収容できること。
⑩ DVD-ROM ドライブを内蔵もしくは外付けで用意すること。
⑪ 筐体前面に、施錠可能なカバーを装着可能で、サービス状態や温度、マシン名を文字で表示可能な LCD パネルを有すること。
⑫ 障害検知機能を有し、ネットワーク経由での遠隔監視が可能であること。
⑬ IPMI2.0 に対応したリモート管理用コントローラを搭載し、OS の状態に依存せずにネットワーク経由でのサーバの管理/制御（電源管理、仮想コンソール/仮想メディア）が可能であること。また、専用のネットワークポートを有しており、HTML5 により管理可能なこと。
⑭ PCI スロットに搭載される各拡張カード毎に最適な冷却ができるよう、サーバ内部のファンが温度センサーの情報やファンの電力消費、エアフローを考慮し自動的に回転数を制御する機能を有すること。
⑮ システムセキュリティの観点から、BIOS やフォームウェアについて意図しないもしくは悪意のある変更から保護する為、これらのバージョンアップや設定変更を禁止する機能を持つこと。また BIOS イメージおよび OS イメージに破損または悪意ある改ざんがあった場合、サーバの内蔵機能による正常なイメージへの自動復旧が可能であること。
⑯ 保守管理用にシリアル番号を記録できるように引出し式のラベルパネルがあること。

(2) 機能要件
① 所内の Windows クライアント、Mac クライアントを対象にクライアントソフトウェアを導入し、資産情報の自動収集が可能であること。
② 所内の管理者を対象とした操作説明を 1 回以上行うこと。
③ クライアント環境（端末等）の設定変更は本調達の範囲外とする。但し、滞りなく IT 資産管理システムを利用できるよう、利用者向けの設定変更手順書を提供すること。同手順について、既設システムにて作成されている新規端末セットアップ手順書を発注者より提供するので、前後関係を考慮の上追記するこ

と。

④ システムバックアップを取得できる構成とし、障害等で OS 起動不可となった際にバックアップからシステムデータを復旧できること。

7.4.2 IT 資産管理ソフトウェア

IT 資産管理ソフトウェアとして、以下の仕様を満たすソフトウェアを 500 式納入すること。また、メーカーの保守サポートサービスを利用できるよう契約期間内は保守契約を行うこと。

(1) 管理対象クライアントは WindowsOS、MacOS 上で稼働可能なこと。

(2) IT 資産管理ソフトウェアを導入し、以下の機能が使用可能であること。また、操作性統一の観点から以下の機能を同一製造元の同一製品で提供することができること。

① WindowsOS

A) 資産管理機能/ライセンス管理機能

B) アプリケーション配布機能

C) ログ収集機能

D) デバイス制御機能

E) 個人情報/機密情報の監査機能

F) 不正 PC 検知遮断機能

G) 指定端末へのリモートコントロール機能

② MacOS

A) 資産管理機能/ライセンス管理機能

B) ログ収集機能

C) デバイス制御機能

③ 将来的な主管業務の拡張または見直しに合わせて、今回導入予定の主たる機能以外にも、同一製造元の同一製品における下記オプションを含む機能の中から選択し追加導入ができること。

A) ファイル制御暗号化機能

B) PC 更新管理機能

C) Web フィルタリング機能

D) モバイルデバイスマネジメント機能（閉域網での利用も含む）

④ 管理者向け管理用コンソールはライセンスフリーであること。

⑤ 操作性統一の観点から各機能を同一製造元の同一製品で提供することができること。

⑥ クライアントモジュールのアンインストールはパスワード等で保護しユーザでは行えないこと。

⑦ クライアントモジュール自身のプロセスを落とした場合でも自動復旧を行える

こと。また、クライアント端末自身ではサービス停止はできないこと。

⑧ ネットワーク負荷対策として帯域調整が可能であること。

⑨ クライアント端末とサーバ間の通信ポートを、任意に設定できること。なお、すべての通信を個別に変更できない場合は、連番等の対応が可能であること。

⑩ 管理画面にてクライアントモジュールを簡易に更新、削除できること。

⑪ データベースに破損が発生した場合に備え、復旧用のバックアップを取得する機能を有すること。

⑫ 端末に接続したUSBデバイスなどの外部記憶媒体へローカル上（デスクトップなど）からファイルコピーまたは移動した際に、ファイルそのものを管理サーバ上に複製保存（シャドウイング）することができること。

⑬ ファイルやセキュリティパッチの配布実行を行う際に、スクリプトを使用せずに GUI 操作（マウス操作）のみで設定ができること。

⑭ Windows 上で行った操作を記録し、実行ファイルに保存して再現し、マウスやキーボードの操作に条件判断を設定することで、処理を自動化が可能であること。

⑮ クライアント端末に保存されているファイルを対象に、個人情報を含む可能性のあるファイルを検出できること。また、クライアント端末に保存されているファイルに対して、検索を行うことができること。

⑯ リモート接続先のクライアント端末がマルチモニターの場合に、表示するモニターの切り替えができること。また、ビデオレートを変更することにより、リモート接続中のCPU使用率や通信量を抑制することができること。

7.5 ID連携システム

ID 連携ソフトウェアとして、以下の仕様を満たすソフトウェアを 300 ユーザ分納入すること。また、最大３システムと連携できるようライセンスを考慮すること。

(1) プロビジョニング機能

以下のシステムのユーザオブジェクトをAPI経由で新規追加、変更、削除できること。

① 本調達内のAcitive Directory

② 本調達内の二要素認証ソフトウェア

③ 既設のMFA認証サービス（ソリトンシステムズ社 Soliton OneGate）

(2) マスタ管理機能

3 種類のマスタデータを保持し，ユーザとアカウントの紐づけだけでなく、さらにそのアカウントで利用可能な情報資産をユーザと紐づけて管理ができること。

これらのマスタデータはブラウザ管理画面上での対話操作もしくはCSVファイルによって新規登録・変更・削除ができること。

① 職員情報マスタ

A) 名前関連情報（漢字・ローマ字・かな等）

B) 所属組織（部署・役職・職務・雇用形態等）情報

・ 所属開始と所属終了の情報も日単位（yyyy/mm/dd 形式）で併せて管理でき、下記３項及び４項記載のルールと連動できること

・ 兼務情報も兼務所属数に制限なく管理できること

C) 追加登録情報

・ 任意複数の登録項目を追加できること

② 組織情報マスタ

A) 部署・役職・職務・雇用形態等

・ 部署マスタは、階層構造で登録できること

・ 下記③及び④記載のルールは、上位部署で設定したルールが下位部署に継承できること

③ 情報資産情報マスタ

A) 管理対象システムのアカウントを介してユーザに適用させたい権限情報
例：ActiveDirectory 関連権限（部署グループや共有フォルダアクセスグループ等） 等

(3) 組織ルール機能

職員の所属する組織（部署・役職・雇用形態等）ごとに，アカウント作成、職員情報マスタ項目への値の入力と情報資産適用のルールをブラウザ管理画面上で容易に設定でき、それらのルールに基づき前記①に記載した各システムへのアカウントの新規登録・変更・削除や属性値の設定、及び上記①-C)で登録された権限の適用・削除が実行できること。これらの実行は，手動実行，スケジュールによる自動実行の２通りの方法が可能であること。

(4) 未来所属の管理機能

前項(3)で記載した組織情報とルールは、期間の管理ができ、かつ現在の職員のマスタ情報に未来の所属組織を事前登録できること。例えば１か月後に組織改編がある場合、その改編後の部署情報とルールを、事前に登録でき、現在の職員をその未来部署に配属した状態で職員マスタに登録できること。そのままの状態で１か月後に自動的に組織改編後の組織とルールが適用され、システムに連携され、適切なアカウント状態と情報資産が適用される運用が可能なこと。

(5) 情報資産利用ログ管理機能

ブラウザ管理画面上で以下ログを参照及びテキスト形式で出力できること。

① 情報資産利用ログ（利用者単位）

職員情報マスタに登録された職員一覧リストから、個々の職員に適用されている情報資産（所属する AD グループ情報や IC カード情報）の一覧情報を出力

する機能

② 情報資産利用ログ（情報資産利用単位）

情報資産マスタに登録された情報資産一覧リストから、個々の情報資産が適用されている（AD グループに所属している）職員の情報や IC カードに紐づけられた職員の情報を出力する機能

(6) ワークフロー機能

部門ごとに担当者をおいて、アカウントの払い出しができること。

また、申請権限を付与されたユーザが申請を行い承認権限を付与されたユーザが承認を行うことでアカウントの新規登録・更新・削除や各システムの権限の付与や剥奪を行うことができること。

(7) ジョブ実行管理機能

CSV ファイルの取込みや、連携先システムへのアカウントプロビジョニング処理については、パッケージ内のジョブ管理機能でスケジュール実行できること。

7.6 ファイルサーバ

7.6.1 ファイルサーバ

(1) 導入要件

① オンプレミス環境に 1 台以上導入すること。

② ウイルス対策ソフトを令和 6 年 10 月 1 日より、1 年間利用できるよう導入すること。

③ CPU 処理能力がインテル® Xeon® Silver 4310 相当以上であること。

④ メモリ容量が 32GB 以上であること。

⑤ OS が Windows Server Standard 2022 以上であること。

⑥ ディスク数が SSD1.6TB×2 以上および HDD2.4TB×3 以上であること。
あわせて、OS 領域用に M.2 SSD カード 240GB×2 以上を搭載すること。

⑦ RAID1/5/6 を使用して構築すること。

⑧ 10GBASE-T ネットワークポートは１つ以上有すること。

⑨ 1000BASE-T ネットワークポートは４つ以上有すること。

⑩ 標準的な 19 インチラックに収容できること。

⑪ DVD-ROM ドライブを内蔵もしくは外付けで用意すること。

⑫ 筐体前面に、施錠可能なカバーを装着可能で、サービス状態や温度、マシン名を文字で表示可能な LCD パネルを有すること。

⑬ 障害検知機能を有し、ネットワーク経由での遠隔監視が可能であること。

⑭ IPMI2.0 に対応したリモート管理用コントローラを搭載し、OS の状態に依存せずにネットワーク経由でのサーバの管理/制御（電源管理、仮想コンソール/仮想メディア）が可能であること。また、専用のネットワークポートを有してお

り、HTML5 により管理可能なこと。

⑮ PCI スロットに搭載される各拡張カード毎に最適な冷却ができるよう、サーバ内部のファンが温度センサーの情報やファンの電力消費、エアフローを考慮し自動的に回転数を制御する機能を有すること。

⑯ システムセキュリティの観点から、BIOS やフォームウェアについて意図しないもしくは悪意のある変更から保護する為、これらのバージョンアップや設定変更を禁止する機能を持つこと。また BIOS イメージおよび OS イメージに破損または悪意ある改ざんがあった場合、サーバの内蔵機能による正常なイメージへの自動復旧が可能であること。

⑰ 保守管理用にシリアル番号を記録できるように引出し式のラベルパネルがあること。

(2) 機能要件

① ファイルサーバ管理ソフトウェアをインストールし、アクセスログの取得やファイルバックアップを実施できる構成とすること。

② ファイルバックアップデータはバックアップ世代管理用サーバに格納すること。

③ ファイルサーバを所内で滞りなく利用できるよう、発注者からの情報に基づき共有フォルダを作成し、適切なアクセス権、フォルダクォータの設定を行うこと。

④ ファイルサーバへのデータ移行は発注者にて実施するものとする。

⑤ システムバックアップを取得できる構成とし、障害等で OS 起動不可となった際にバックアップからシステムデータを復旧できること。

7.6.2 バックアップ世代管理用サーバ

(1) 導入要件

① オンプレミス環境に 1 台以上導入すること。

② ウイルス対策ソフトを令和 6 年 10 月 1 日より、1 年間利用できるよう導入すること。

③ CPU 処理能力がインテル® Xeon® E-2324G 相当以上であること。

④ メモリ容量が 16GB 以上であること。

⑤ OS が Windows Server Standard 2022 以上であること。

⑥ ディスク数が HDD8TB×2 以上であること。
あわせて、OS 領域用に M.2 SSD カード 240GB×2 以上を搭載すること。

⑦ RAID1/5/6 を使用して構築すること。

⑧ 10GBASE-T ネットワークポートは１つ以上有すること。

⑨ 1000BASE-T ネットワークポートは４つ以上有すること。

⑩ 標準的な 19 インチラックに収容できること。

⑪ DVD-ROM ドライブを内蔵もしくは外付けで用意すること。

⑫ 筐体前面に、施錠可能なカバーを装着可能で、サービス状態や温度、マシン名を文字で表示可能な LCD パネルを有すること。

⑬ 障害検知機能を有し、ネットワーク経由での遠隔監視が可能であること。

⑭ IPMI2.0 に対応したリモート管理用コントローラを搭載し、OS の状態に依存せずにネットワーク経由でのサーバの管理/制御（電源管理、仮想コンソール/仮想メディア）が可能であること。また、専用のネットワークポートを有しており、HTML5 により管理可能なこと。

⑮ PCI スロットに搭載される各拡張カード毎に最適な冷却ができるよう、サーバ内部のファンが温度センサーの情報やファンの電力消費、エアフローを考慮し自動的に回転数を制御する機能を有すること。

⑯ システムセキュリティの観点から、BIOS やフォームウェアについて意図しないもしくは悪意のある変更から保護する為、これらのバージョンアップや設定変更を禁止する機能を持つこと。また BIOS イメージおよび OS イメージに破損または悪意ある改ざんがあった場合、サーバの内蔵機能による正常なイメージへの自動復旧が可能であること。

⑰ 保守管理用にシリアル番号を記録できるように引出し式のラベルパネルがあること。

(2) 機能要件

① ファイルサーバのファイルバックアップデータを格納すること。

② システムバックアップを取得できる構成とし、障害等で OS 起動不可となった際にバックアップからシステムデータを復旧できること。

7.6.3 ファイルサーバ管理ソフトウェア

ファイルサーバ管理ソフトウェアとして、以下の仕様を満たすソフトウェアを 1 式納入すること。

(1) 動作環境

① オンプレ Windows Server OS 搭載のサーバで利用可能なこと

② クラウドの Windows Server OS 搭載の IaaS 上で利用可能なこと

③ 製品は、動作 OS メーカが推奨するアンチウィルス対策と共存可能なこと

④ ActiveDirectory サーバによる ACL 管理に対応していること

⑤ Windows エクスプローラーでアクセス可能なこと

⑥ Windows サーバシャットダウン時は、自動的にストレージシステムが終了すること

⑦ 管理端末からネットワーク越しにファイルサーバ設定が管理、変更できること

(2) ストレージ運用機能

① 仮想ストレージ技術を提供すること

② 必要に応じて自由にストレージを追加し、共有ディスクの総容量を増やせること
③ 必要に応じて自由にディスクを取り外し、共有ディスク交換が可能なこと
④ データの配置を最適化する階層化技術（ティアリング機能）を有していること
⑤ NAS や外付けディスクを用いて、共有ディスクの総容量を増やせること
⑥ ライセンス制限による搭載するディスクサイズ課金等がないこと
⑦ ライセンス制限による利用者数の課金等がないこと
⑧ クラウド・オブジェクト・ストレージが利用可能なこと
⑨ Windows アクセス権と連動し、アクセス権に応じてフォルダなどの存在を見えなくすることができること（ABE 機能）
⑩ 共有フォルダ毎に容量制限をつけるフォルダクォータが利用できること

(3) バックアップ・レプリケーション機能
① データの冗長化は、CDP 型による冗長化が可能なこと
② 任意の期間のデータをバックアップ可能なこと
③ データはデータ転送可能な任意の場所に配置されたストレージにバックアップ可能なこと
④ 任意の期間のデータをネットワーク越しに、別サーバへレプリケーション可能なこと
⑤ ファイルの世代管理が可能なこと
⑥ 期間を指定して古い世代ファイルを冗長化先から自動削除できること
⑦ データの保全を確認するために、冗長化処理に異常がある場合の確認ができること
⑧ 任意の保存期間全ての世代ファイルを保存、復元可能なこと
⑨ ファイルサービスを継続しながら、ファイル単位またはディレクトリ単位でデータ復元可能なこと
⑩ データ復元の進行状態が分かること
⑪ レプリケーションしたデータにより、別サーバでデータの継続運用が可能なこと

(4) ファイルサーバ監視機能及びランサムウェア攻撃対策機能
① アクセスログを取得保存および検索が可能なこと
② 必要な期間だけログが保存できること
③ 取得したログ情報をアーカイブ保存できること
④ ファイルへのアクセス監視機能があること
⑤ アクセス監視対象のデータが消去・編集された場合は通知が行われること
⑥ 共有フォルダへのランサムウェア攻撃を検知および自動ブロックする仕組みがあること

⑦ ランサムウェア攻撃を検知、ブロックし、冗長化先からデータ復元を可能であること

⑧ 冗長化のデータ転送は証明書で認証されたサーバ間を TLS 通信で行えること。

⑨ ランサムウェア攻撃検知の感度はユーザで調節できること

⑩ ランサムウェア攻撃検知後に、Windows イベントログへイベントを自動設定し他社製品と連携できること

(5) サポート

① 製品のサポートは、日本語での対応可能なこと

② 製品のサポートは、Web、メール、電話等で行えること

(6) その他

① 製品の操作マニュアル、リリースノート、その他の関連文書は日本語で提供されていること。

② 製品の操作は、管理画面で提供されており表記は日本語であること。

7.7 バックアップシステム

7.7.1 バックアップサーバ

(1) 導入要件

① 所内に導入されている既設システムのバックアップシステムを流用すること。その際、バックアップに必要なソフトウェアライセンスおよびバックアップリソース（データ容量）の確保は本調達内で実施すること。

(2) 機能要件

① 既設システムのバックアップシステムを使用してイメージバックアップを取得すること。バックアップの取得頻度、世代数は監督職員と協議の上で決定すること。なお、バックアップ設定（ライセンスの導入、バックアップジョブの追加等）は受注者にて行うこととし、既設システム運用業者と十分な調整の上で実施すること。

② システムバックアップを取得できる構成とし、障害等で OS 起動不可となった際にバックアップからシステムデータを復旧できること。

7.8 サーバ集約スイッチングハブ

(1) 導入要件

① オンプレミス環境に２台以上導入すること。

② 所内のクライアント端末から通信できるよう、既設システムのファイアウォールサーバと 10Gbps で接続すること。接続に際して既設システムの機器に対する設定変更、追加モジュール、ライセンス等が必要な場合、本調達に含めること。

③　既存環境と接続に必要な物品も調達範囲とする。

④　故障時の代替製品として予備機（SFP/SFP+スロットに実装する場合は、本製品も含む）を導入すること。

(2) ハードウェア構成要件

①　装置単体で10/100/1000BASE-T ×40ポート、100/1000/2.5G/5GBASE-T×8ポート以上のインターフェースを有すること。

②　装置単体でSFP/SFP+スロットを2 つ以上有すること。

③　IEEE 802.3ae 10GBASE-ER/LR/SR、IEEE 802.3an 10GBASE-T に準拠したSFP+(SmallForm-factor Pluggable+)を搭載可能なこと。

(3) パフォーマンス要件

①　装置単体でスイッチングファブリックは506Gbps 以上であること。

②　装置単体でMAC アドレス登録数は16,384 以上であること。

(4) 機能要件

①　装置単体でIEEE 802.1Q に準拠した4,094 以上のVLAN を設定可能なこと。

②　IEEE 802.1AX-2008 に準拠したLink Aggregation（static and dynamic）機能を有すること。

③　IEEE 802.1D-2004 およびIEEE 802.1Q-2005 準拠のスパニングツリー機能を有すること。

④　ポートミラーリング、リモートミラーリング機能を有すること。

⑤　RFC3619に準拠したレイヤー2 のリング型冗長化機能を有すること。

⑥　スタティックルーティング、RIPv1/v2、RIPng、OSPFv2、OSPFv3、PIM-SSMv4、PIM-SMv4、PIM-DMv4、PIM-SMv6、PIM-SSMv6、BGP 機能をライセンス追加により利用できること。

⑦　同一ポート上でIEEE 802.1X 認証/Web 認証/MAC アドレスベース認証が可能であること。

⑧　DHCP サーバ機能を有すること。

⑨　DHCP リレー機能を有すること。

(5) 冗長機能要件

①　スタックケーブルで機器間(最大8 台)を接続することにより、仮想的に1 台の装置として扱うことができる､スタック機能(以下､スタック)を有すること。

②　スタック接続されている装置間では、コンフィグ、FDB、ARP テーブル、IP ルーティングテーブル等の各種情報を同期することが可能なこと。

③　スタック接続した際は装置間の帯域を80Gbps（双方向）以上有すること。

(6) ネットワーク仮想化機能要件

①　製品間で管理専用ネットワークを自動構成し、ネットワークの管理・保守作業を効率化する機能を有しており、メンバーノードとして動作可能であること。

② メンバーノードの機器交換時に、バックアップデータからファームウェア、コンフィグ、スクリプトなどを自動復元する機能を有すること。なお、交換用の機器は購入時の状態でよく、事前設定の必要がないものとする。

③ 異なる機種間での機器交換時に、バックアップデータからコンフィグを自動復元する機能を有すること。なお、交換用の機器は購入時の状態でよく、事前設定の必要がないものとする。

(7) 運用・管理機能要件

① Telnet（クライアント/サーバ）機能およびSecure Shell（クライアント/サーバ）機能を有すること。

② 時刻同期を行うためにNTP（クライアント/サーバ）機能を有すること。また他のNTPサーバに同期していない場合であっても、装置単体で権威のあるNTP サーバとして動作することが可能なこと。

③ SNMP エージェント機能を有し、SNMPv1/v2c/v3 による管理が可能なこと。

④ Syslog サーバへログを転送できること。

⑤ 外部メディア（USB メモリ）へログを転送できること

⑥ 決められた時刻や特定のイベントが発生したときに、任意のスクリプトを自動実行するトリガー機能を有すること。

⑦ インターネットに接続された環境において、ライセンスをオンラインで更新可能なこと。

⑧ USB メモリにファームウェアやコンフィグファイルを直接アップロード/ダウンロード可能なこと。

⑨ 短時間でリンクダウン/アップを繰り返すポートフラッピング現象を検出し、当該ポートの自動シャットダウンが可能なこと。

⑩ 光ファイバーケーブルの受信光レベルを常時監視し、任意のしきい値を下回った場合に当該ポートのシャットダウンおよびSNMP トラップ通知が可能であること。

7.9 ネットワーク監視サーバ

(1) 導入要件

① 所内に導入されている既設システムのネットワーク監視装置に対し、必要な監視設定を追加すること。

(2) 機能要件

① 本調達にて導入するサーバ機器を監視し、障害を検知した際に管理者にアラートメールを送付すること。

② 監視を行う為の設定変更は本調達に含めること。

7.10 無停電電源装置

(1) 導入要件

① オンプレミス環境に各機器の消費電力、コンセント数等を考慮の上、必要な電源容量、台数の UPS を導入すること。

② オンプレミス環境のサーバ装置全てを、UPS に接続すること。

(2) 機器要件

① 各 UPS は、定格出力で停電補償時間が 5 分以上であること。

② オンプレミス環境に設置するサーバ装置は UPS と連携し、停電時に自動シャットダウン、電源切断が可能であること。

7.11 19 インチラック

(1) 導入要件

① オンプレミス環境に２台導入すること。

② オンプレミス環境の機器を 19 インチラックに収納して納品すること。

③ ラック内に搭載するサーバ用ＫＶＭを適切な台数導入すること。

(2) 製品要件

① 42 ユニット以上の 19 インチラックを導入すること。

② 内部機器の稼働状況を確認可能な扉（鍵付）がついていること。

③ 調達機器のラック搭載に必要な機器（UTP ケーブル等）は納入業者が用意すること。

④ 19 インチラックは、アンカー固定、免振装置等の耐震対策を施して設置すること。

8 性能、機能以外の要件

8.1 搬入、据付、配線、調整、分電盤・電源配線等の付帯電気工事及び撤去について

(1) 導入システムの設置場所への搬入、据付、配線、調整、既設ネットワークへの接続・調整、及び付帯電気工事において必要とする関連機器及び関連用品も、本調達に含むこと。

(2) 既設ネットワークとの接続において障害が発生した場合は原因の切りわけを行い、本調達に起因する障害については対処すること。

(3) 導入時の作業日程と体制を提示し監督職員と協議を行い、その指示に従うこと。なお、導入に当たっては、必ず監督職員の立ち会いのもと作業を実施すること。

(4) 本調達システムの構成に必要となるアプリケーション開発費用は全て含めること。また、開発に必要となる機器も受注者が用意すること。

8.2 システムの導入について

受注者は、監督職員と協議を行い、納入期日までに下記の導入作業を実施すること。実施に当たっては、監督職員が必ず立ち会うこと。

受注者は本調達機器等の搬入・設置，本システムの設計・構築・インストール及び環境設定・動作検証・教育・操作説明等を令和 6 年 11 月 30 日までに完了させるものとする。なお、ActiveDirectory サーバ及び ID 連携システムについては令和 6 年 9 月 30 日までに完了させることとする。

(1) 「7.システムの要求要件」で記載した全ての機器に関して、システム全体の運用、各ハードウェア・ソフトウェアの運用方法等については、原則として受注者が検討し、監督職員と協議の上決定すること。
(2) 運用方法に基づいた各ハードウェア・ソフトウェアの設定等については、全て受注者が検討し、監督職員と協議の上決定すること。
(3) ネットワークセグメント間の通信を考慮し設計すること。
(4) オンプレミス環境に機器を導入する際は必要に応じてスイッチ等への設定変更を実施すること。また、同装置は運用機関において撤去する予定である為、撤去後においても撤去前と同等のセキュリティを考慮した設計とすること。
(5) 運用の検討及び設定に際しては、ネットワークセキュリティ、及びサーバセキュリティを十分考慮すること。
(6) 各ハードウェア・ソフトウェアの設定については、(1)、(2)に基づき、全て受注者が設定作業を実施すること。
(7) 動作試験については、システム全体の運用、各ハードウェア・ソフトウェアの動作試験仕様を全て受注者が検討し、監督職員と協議の上実施すること。
(8) 動作試験の結果については、受注者が報告し、監督職員の承認を得ること。
(9) 導入作業完了後、導入に関する下記のドキュメントを提出し、監督職員の承認を得ること。
    ① 要件定義書
    ② 基本設計書
    ③ 詳細設計書
    ④ 運用設計書
    ⑤ 各ハードウェア、ソフトウェア設定報告書
    ⑥ 動作試験仕様書
    ⑦ 動作試験成績書
(10) システムの起動、停止方法、ユーザ登録・削除方法等、日常の管理運用方法を示した運用手順書を作成し、システム導入時に提供すること。
(11) 既設ネットワークとの接続に際しては、既設システム受注者と連携し実施すること。
(12) 既設ネットワークとの接続において障害が発生した場合は、原因の切り分けを行い、本調達に起因する障害については対処すること。

(13) 本システムの導入及び既設システムの連携について、既設システム受注者と連携し実施すること。

(14) 上記のシステム導入作業実施に際しては、ハードウェア、ソフトウェア、及びシステム運用管理に係わる技術と経験が必要と考えられる。そのため、システム導入体制の信頼性を確保するため、競争参加資格技術審査申請書において、以下の資格等を有することを証明する資料を添付することとし、当所において十分な技術と経験を有するかどうか判断する。

① ISO9001 の登録認証

② プライバシーマークの付与又は ISMS27001 の登録認証

(15) 本システムの導入工程等の調整等に際しては、受注者の負担と責任において既設システム受注者との調整、連携協力等を行い、当所に随時報告すること。

(16) システムの本運用開始までに行う作業について、進捗状況を確認するため、週に１回程度定例会議を開催し、監督職員へ報告を行うこと。なお、作業が遅延する場合には監督職員へ速やかに報告を行うこと。

8.3 導入要件

8.3.1 導入作業における基本要件

(1) システム利用者・関係者へのヒアリングや、システムの要件定義などを踏まえ、導入要件の定義を行うこと。要件定義に先立ち制約となる情報（繁忙期の回避・法改正などの制約、サポート期限、品質など）についても調査・整理すること。

(2) 導入については、リスクや業務への影響を最小限に減らすよう計画すること。

(3) 詳細な導入スケジュールを作成し、作業タスク、担当者、順序など明確化すること。

(4) 導入にあたり、現行システムへ修正・追加作業が必要になる場合は、監督職員へその旨を連絡し、監督職員の指示を仰ぐこと。既設システム受注者とのやり取りが発生する場合でも監督職員がやり取り内容を適宜把握出来ること。

8.3.2 導入計画及び関連ドキュメントの作成

(1) 導入計画

受注者は、令和 6 年 9 月 30 日までに、システム毎、及び全体の導入作業に関する資料「導入計画書」・「導入手順実施手順書」・「切り戻し手順書」・「動作確認チェックリスト」の作成を行うこと。また、監督職員から導入計画について了承を得ること。

(2) 本番切換え

本番切換えは監督職員が以下の基準を全て満たしたと判断した上で、本番切換えの実施を可能とする。

(3) 本番切換え判断基準

① 不具合が発生した場合、全体もしくは不具合範囲のロールバック作業手順が確

立されていること。

② 各システムの動作テストに合格しており、かつ要件及び品質が満たされていること。

③ エンドユーザへの影響が最小限に抑えられていること。

8.4 保守サービス

8.4.1保守サービスについて

(1) システム導入後､運用及び業務の遂行を円滑に行うための支援体制を提供すること。

(2) 90 分以内に当所に駆け付けられる場所に受注者または協力業者の拠点があること。

(3) 本調達機器の障害受付窓口、ハードウェア保守、ソフトウェア保守を行うこと。本調達外機器は障害受付窓口を用意すること。なお、本調達外機器の保守サービスは当所が用意する。

8.4.2障害受付窓口対応

システム保守を効率的に行うため、技術者が一括してハードウェア、ソフトウェアの障害受付を行う以下の窓口を用意すること。

受付窓口対応時間：８：３０～１７：１５まで（平日）

なお、土曜日、日曜日、国民の祝日及び年末年始（１２月２９日から１月３日）は除くものとする。

8.4.3ハードウェア保守サービス

(1) ハードウェアに精通したカスタマエンジニアによって、常にハードウェアを良好な状態に保つこと。

(2) 定期保守に関する作業計画は、原則として 2 週間前までに提出すること。また、障害対応／定期保守の作業報告は原則として 2 週間以内に文書で提出すること。

(3) 本調達システムの障害は、所内ネットワークの停止に直接的に係わり、研究業務に多大な影響を及ぼす。そのため、障害連絡後 4 時間以内に障害復旧作業に着手できる地点に、保守要員が常駐するサービス拠点が整備されていること。

(4) 本調達機器のオンプレミス装置で発生した各種の異常を検知し、監督職員及び専任技術者へ E-Mail による自動通報を行うこと。

8.4.4ソフトウェア保守サービス

(1) 専門技術者による問題解決支援サービスを提供すること。

(2) 各ソフトウェアメーカーから契約期間中、下記について適宜入手可能であること。

① 製品に関する技術情報・運用ノウハウ

② 修正パッチの情報提供

③　問合せ対応

8.5　業務の管理

受注者は、業務計画書に基づき本業務の実施状況を把握し、円滑な推進を図ること。

(1) 安全管理

①　受注者は、業務等を履行するにあたり常に安全管理に心掛け、事故等に十分注意すること。

②　受注者は、履行期間に事故が発生した場合には、直ちに監督職員に通報するとともに、別に定める事故報告書を監督職員が指示する期日までに、監督職員に提出すること。

③　受注者は、契約後速やかに、本業務に従事する専任技術者に対し本業務における安全に関する教育等を実施すること。

(2) 品質管理

①　品質管理計画の立案、検証及び品質改善策の検討、実施を管理する体制を構築すること。また、各種取り組みがしかるべき手続きに則って実施されていることを定期的に確認すること。

②　受注者の関連会社及び協力会社等、本件の受注者でない主体が参画する体制を敷くことを監督職員が承諾する場合は、関連会社等の作業範囲及び責任範囲を明確にし、関連会社等の作業及び成果物に対して十分な管理・検査を実施すると共に、関連会社等に係る一切の事項について、受注者が全責任を負うこと。特に「労働者派遣事業の適正な運営の確保及び科研労働者の就業条件の整備等に関する法律（昭和 60 年 7 月 5 日法律第 88 号)」等の法規に抵触しないよう、適切な管理・対応を行うこと。

(3) 課題管理

①　業務遂行上様々な局面で発生する各種課題について、課題の認識、対応策の検討、解決及び報告のプロセスを明確にし、一元的な課題管理を行う体制を構築すること。

②　監督職員と状況を共有するため、起票、検討、対応及び承諾といった一連のワークフローを意識した管理プロセスを確立すること。

③　積極的に課題の早期発見に努め、速やかにその解決に取り組むこと。

④　対応状況を定期的に監視し、解決を促す仕組みを確立すること。

⑤　本システムの運用に影響を与えるような重大な課題が発生した場合には、速やかに監督職員に報告し、対応策について協議すること。

(4) リスク管理

①　技術的観点、財務的観点、進捗的観点、及び人員的観点当又は、本システムと類似する案件で発生した問題等から、業務の遂行に影響を与えるリスクを識別

し、その発生要因、発生確率、及び影響度等を整理すること。又、発生確率及び影響度に基づき、リスクの優先度を決定し、それに応じた対策を行うこと。

② 上記①で整理したリスク及び内容について、定期的に監視・評価し、その結果を反映すること。

③ リスクを顕在化させないための対応策（対応手順、体制等）を策定すること。

④ 長期にわたり正常に稼働できない事態・状況及び保有するデータの喪失等により、業務に多大な支障が生じるような重大障害を発生させないこと。発生した場合は別途協議とする。

(5) 情報セキュリティ管理

① 国立研究開発法人建築研究所情報セキュリティポリシー、統一基準群等の内容を把握、理解し、遵守すること。

② セキュリティ対策の実施状況については、定期的に内部監査し、監督職員に報告すること。

③ セキュリティ対策の内容については、各業務工程の状況に応じて、適宜改善策を検討し、監督職員の承諾を得ること。

④ セキュリティに関する事故及び障害等が発生した場合には、速やかに監督職員に報告し、対応策について協議すること。

⑤ 個人情報、施設等に関する情報その他の契約履行に際し知り得た情報の漏えいを発生させないこと。

⑥ 記憶媒体の交換、廃棄などは、破壊、不可逆的にデータ化できないような削除方法で消去を行い、消去した証明書を提出すること。

8.6 サービスレベルアグリーメント（SLA）の締結について

8.6.1 SLA の締結

本業務の効率化と品質向上並びに円滑化を図るため、以下に示す指標に対して SLA を締結するものとする。

(1) 情報資産管理システム全体の稼働率

本システムの稼働率は、99.0%以上とし、以下の計算により算出する。

稼働率（%）＝「年間実稼働時間」／「計画停止等を除いた年間予定稼働時間」×100

(2) 質問等の回答率（月平均回答率）

利用者からの質問等（受注者の知見で回答できないものは除く。）に対する２４時間以内の回答率は９０％（月平均）以上とすること。回答率は以下の計算式による。なお、２４時間以内の回答とは、通常業務時間内に受けた利用者からの質問等に対し、２４時間以内（問い合わせから２４時間後が業務日でない場合にあっては、翌業務日の当該２４時間後に相当する時刻まで）に回答することをいう。

回答率（%）　＝（一月あたりの２４時間以内の回答数）
／（一月あたりの質問等の数）×１００

(3) 作業遅延の件数

監督職員が示す所定の期日までに作業が完了しない件数は、0 件とすること。対象となる作業を以下に示す。なお、監督職員が示す所定の期日は、以下の作業を行うにあたり、受注者と協議して設定するものとする。

① ソフトウェアぜい弱性情報の適用作業

8.6.2 SLA の改訂

SLA については、必要に応じて見直しを実施し改訂するものとする。改訂の契機は以下の通りとする。

(1) 発注者及び受注者双方の合意事項に明確な変更が生じた時

(2) 発注者及び受注者双方が必要と認めた時

8.6.3 SLA に係る免責事項

予見できない不測の事態（社会通念上、受注者に責任がないと認められる事態）が発生した場合は、SLA の範囲外とする。

8.6.4 SLA に係る是正処置

(1) 受注者は、業務管理責任者を中心として 1 ヵ月ごとに SLA の達成状況の確認を行うこと。

(2) 確認結果は、月 1 回程度開催する定例会議において報告し、発注者の承諾を得ること。

(3) 受注者の責による未達成事項がある場合、受注者は以下に示すような処置により達成度合いの向上に努めること。

① 未達成の事項に対する改善策（仕組み又は手続きの見直し等）を提示し、発注者の承諾を得た上で対策を講じること。また、そのために必要となる作業等は受注者で行うこと。

② 改善策の実施効果を実施月より 3 ヵ月間、定例会議で報告し、発注者の承諾を得ること。

(4) SLA 未達成の事項が継続的に発生する場合、又は受注者により改善策が充分で無い場合、発注者が受注者に内部監査の実施を求めることが出来る。内部監査は、本業務に直接関わらない品質管理部門等の第三者が、SLA 報告内容についての監査を実施し、監査結果報告書を提出すること。

8.7　システム運用管理サポート、エンドユーザサポートについて

8.7.1 システム運用管理サポート

既設システムの常駐の専任技術者と連携して以下のシステム運用サポートを実施すること。

(1) 以下の支援を行うこと。

① システム障害、ウイルス対策時等の緊急時には、その影響範囲、重要度等を監督職員と協議し、必要に応じて通常業務時間以外及び休日にも対応を実施すること。

② 災害発生時における体制表（近隣で常駐又は巡回している専任技術者等による当所への緊急支援体制があれば、それも含む。）を提出すること。また、災害発生時には速やかに監督職員に連絡し、必要な支援・対応を実施すること。

③ システム運用管理に関して、システムを常に良好な状態に保つよう、以下に示す発注者支援を実施すること。また、当該システムに関して障害を検知した場合には、遅滞なく監督職員に連絡し、迅速かつ適切に復旧作業を行うこと。

A) システムの立ち上げ、停止作業等のオペレーション作業、及びスケジューリング

B) システムのトラブル対応

C) システムに関する機器、ライセンス等の管理

D) システムに関する予防保守、消耗品管理

E) 発注者の質問対応、資料提供

F) 発注者と協力し既存ネットワーク機器で障害が発生した際の原因切り分け

G) サーバ関連作業

(2) 以下を例とするアプリケーションレベルの運用は発注者が行うものとする。ただし、運用に必要な手順は受注者が提供すること。

① ActiveDirectory および二要素認証システム

A) グループポリシーの管理・割当

B) 二要素認証が利用できないユーザを対象とした、代替パスワードの発行

② IT 資産管理システム

A) クライアントがインストールできない IT 資産（プリンタ等）における手動での資産登録

B) 資産情報レポートの作成・提供

C) 脆弱性を持つソフトウェアがインストールされた端末一覧の出力

③ ID 管理システム

A) ユーザアカウントの登録・削除

B) セキュリティグループの作成・変更・削除

④ ファイルサーバ

A) 共有フォルダのメンテナンス（作成/削除/アクセス権変更/クォータ値変

更）

B) アクセスログ調査

C) ファイルリストア

(3) ハードウェア、OS レベルに係る以下の業務を受注者が行うこと。

① 日時点検業務として以下の作業を行うこと。

A) サーバ、ネットワーク機器等の目視確認（LED ランプ・アラーム）

B) ネットワーク機器の正常性確認

C) サーバの動作確認

D) システムの状況確認

E) プロセスの確認

F) サーバへのログイン状況の確認

G) バックアップの確認

H) システム管理者宛のメール確認

② システムの稼働に関しては、ディスク使用量、ＣＰＵ稼働率等のキャパシティ情報を定期的に収集して、運用履歴、及び診断レポートを作成すること。なお、運用履歴の報告については、毎月以下の項目について作成すること。

A) ＣＰＵ稼働率、ディスク使用量

③ 所内ネットワークの稼働に関しては、ネットワーク管理機能を用いて、ネットワークトラフィック、障害管理等のキャパシティ情報を定期的に収集して、運用履歴、及び診断レポートを作成すること。なお、運用履歴の報告については、毎月以下の項目について作成すること。

A) 各セグメントに関するネットワークトラフィック量

B) 各ネットワークスイッチの稼働状況

④ システムに導入されている OS およびソフトウェアの脆弱性を確認し、必要に応じてバージョンアップ、修正パッチの適用等の見直しを行うこと。

⑤ 発注者からの指示に基づき、導入製品のパラメータ変更作業を行うこと。作業は原則１回/月とする。

8.7.2 エンドユーザサポート

所内ネットワークに接続されているパソコン等を利用するエンドユーザに関するユーザ支援は発注者が行うこととするが、受注者は発注者に対し、受注者の知見の範囲内で支援を行うこと。

8.7.3 稼動状況報告

本業務においては、業務の実施状況の報告や今後の実施方針の協議等を行うことを目的に、月１回程度定例会議を開催する。月単位で下記内容を整理し、報告書として

提出すること。

(1) システム運用管理サポート

① 障害対応

② 各サーバの稼動状況

③ ネットワークの稼働状況

④ 資産管理システム登録状況

⑤ サーバ関連作業の対応履歴

8.8 説明書・マニュアル等の要件

(1) 説明書・マニュアルは日本語版を提供すること。(但し、日本語版の提供が難しいものにあっては、可能な限り日本語の解説や説明を用意するものとする)

(2) マニュアルはハードウェア、ソフトウェアともに各1部(オンラインマニュアルも可とする)を提供すること。

8.9 検査

本仕様書に基づき当所検査職員が行う。

8.10 契約不適合責任

(1) 当所は、受注者に対し、引き渡された成果物が種類又は品質に関して契約の内容に適合しないものである場合（その不適合が当所の指示によって生じた場合を除き、受注者の当該指示が不適当であることを知りながら、又は過失により知らずに告げなかった場合を含む。）において、その不適合を当所が知った時から起算して1年以内にその旨の通知を行ったときは、その成果物に対する修補等による履行の追完を請求することができる。ただし、受注者は、当所に不相当な負担を課するものでないときは、当所が請求した方法と異なる方法による履行の追完をすることができる。

(2) (1)の場合において、当所が相当の期間を定めて履行の追完の催告をし、その期間内に履行の追完がないときは、当所は、その不適合の程度に応じて代金の減額を請求することができる。

(3) (1)又は(2)の場合において、当所は、損害賠償を請求することができる。

8.11 特記事項

8.11.1 知的財産権

(1) 受注者は本調達にあたり作成される成果物に関し、「著作権法（昭和45年5月6日法律第48号)」第27条及び第28条を含む著作権の全てを発注者に無償で譲渡するものとする。

(2) 受注者は、成果物に関する著作者人格権（著作権法第18条から第20条までに規定

された権利をいう。）を行使しないものとする。ただし、発注者が承諾した場合は、この限りでない。

(3) (1)及び(2)に係わらず、成果物に受注者が既に著作権を保有しているもの（以下「受注者著作物」という。）が組み込まれている場合は、当該受注者著作物についてのみ、受注者に帰属する。

(4) 提出される成果物に第三者が権利を有する著作物が含まれる場合には、受注者が当該著作物の使用に必要な費用の負担及び使用許諾契約等に係る一切の手続きを行うものとする。

(5) 本調達に関し、第三者との知的財産権に係る権利侵害の紛争等を生じた場合には、当該紛争等の原因が専ら発注者の責めに帰すべき事由による場合を除き、受注者は自らの費用及び責任により、当該紛争等の解決に係る一切の処理をすること。この場合、発注者は係る紛争等の事実を知ったときは、受注者に通知し、必要な範囲での訴訟上の防衛を受注者に委ねる等の協力措置を講じるものとする。

8.11.2　委託・再委託

(1) 受注者は、本業務の実施にあたり、その全部または主たる部分を一括して再委託してはならない。また、委託等に関する統一基準群、セキュリティポリシーを遵守し、同様のサプライチェーン管理を行うこと。

(2) (1)の「主たる部分」とは、業務における総合的企画、業務遂行管理、手法の決定及び技術的判断等をいうものとする。

(3) 受注者は、本業務の実施にあたり、その一部（「主たる部分」を除く。）について再委託を行う場合には、原則として、あらかじめ競争参加資格技術審査申請書において、再委託先に委託する業務の範囲、再委託を行うことの合理性及び必要性、再委託先の履行能力並びに報告徴収、個人情報の管理その他運営管理の方法（以下「再委託先等」という。）について記載しなければならない。

(4) 受注者は、契約締結後やむを得ない事情により再委託を行う場合には、再委託先等を明らかにした上で、当所の承認を受けなければならない。

(5) 受注者は、(3)又は(4)により再委託を行う場合には、受注者が当所に対して負う義務を適切に履行するため、再委託先等の受注者に対し、「8.11.4 機密保持」に規定する事項、その他の事項について、必要な措置を講じさせるとともに、再委託先等から必要な報告を聴取することとする。

(6) (3)から(5)までに基づき、受注者が再委託先等の受注者に業務を実施させる場合、全て受注者の責任において行うものとし、再委託先等の受注者の責に帰すべき事由については、受注者の責に帰すべき事由と見なして、受注者が責任を負うものとする。

8.11.3　閲覧資料及び実施場所の確認

応札希望者は、本業務の内容を把握するために、別添２に示す情報システム及び現行の業務に関する資料の閲覧、及び業務実施場所である 0A 室を確認することができる。閲覧又は確認を希望する者は、仕様書別添１「資料閲覧等申込書」を調達担当者に提出の上、入札公告日から競争参加資格技術審査申請書提出期限までの間（業務日の 9 時 00 分から 17 時 00 分まで）に、調達担当者に事前連絡の上、調達担当者が定める方法にて閲覧又は確認することができる。

※　本業務の内容を把握するために、本表に示す資料以外で閲覧を希望する資料がある場合は、資料閲覧等申請書を提出する前に、調達担当者へ申し出ること。調達担当者は、該当資料の有無を確認した結果を回答するので、回答の内容により資料閲覧等申込書の提出を行うこと。なお、当該資料の有無等の確認には時間を要する場合があるので留意すること。

8.11.4　機密保持

受注者は、以下の点に留意して、当所のポリシーを遵守し、情報セキュリティを確保するものとする。

(1) 受注者において、本調達に関する業務に従事する者又は従事していた者は、本業務の実施に際して知り得た発注者の情報を、第三者に漏らし、盗用又は本業務以外の目的のために利用してはならない。

(2) 受注者は、本業務の実施に際して得られた情報処理に関する利用技術（アイデア又はノウハウ）については、受注者からの文書による申出を監督職員が認めた場合に限り、第三者へ開示することができる。

(3) 受注者は、発注者から提供された個人情報及び業務上知り得た個人情報について、独立行政法人等の保有する個人情報の保護に関する法律（平成 15 年法律第 59 号）に基づき、適切な管理を行わなければならない。

(4) 受注者は、本業務の開始時に、本業務に係る情報セキュリティ対策とその実施方法及び管理体制について、発注者に書面で提出すること（統一基準群・ポリシーを参照のこと)。

(5) 受注者は、発注者から秘密情報を提供された場合には、当該情報の秘密性に応じて適切に取り扱うための処置を講じること。また、本業務において発注者が作成する情報については、監督職員からの指示に応じて適切に取り扱うこと。

(6) 受注者は、「国立研究開発法人建築研究所情報セキュリティポリシー」に準拠した情報セキュリティ対策の履行が不十分と見なされる場合又は受注者において本業務に係る情報セキュリティ事故が発生した場合は、必要に応じて発注者の行う情報セキュリティ対策に関する監査を受け入れ、即時連絡、対応すること。

(7) 受注者は、発注者から提供された秘密情報が業務終了等により不要になった場合に

は、確実に返却又は破棄すること。また、本業務において受注者が作成した情報についても、監督職員からの指示に応じて適切に破棄し、破棄した証明書を提出すること。

(8) (1)から(7)までのほか、監督職員は、受注者に対し、本業務の適正かつ確実な実施に必要な限りで、秘密を適正に取り扱うために必要な措置を採るべきことを指示することができる。

8.11.5　検収時における注意事項

検収時に物品等の納期が遅れた場合、代替品で行う事を許可し、その後に納品を行い、システムを切り替えて、運用を担保すること。

8.11.6　賃貸借期間終了後の導入品について

賃貸借期間終了後、サブスクリプション以外の物品等の導入品目について無償譲渡すること。

8.12 その他

(1) 取引停止処置

本業務に係る提出書類に重大な誤り若しくは虚偽の表示があった場合、発注者は、受注者に対し、取引停止等の処置を講じる場合がある。

(2) 業務遂行上の言語

本業務において、発注者と受注者の間で使用する言語は、日本語とする。

(3) 調査

① 監督職員は、本業務の適正かつ確実な実施を確保するために必要があると認めるときは、受注者に対し必要な報告を求め、又は監督職員が事務所に立ち入り、当該業務の実施の状況若しくは記録、帳簿書類その他の物件を検査し、又は関係者に質問することができる。

② 立ち入り検査をする監督職員は、検査等を行う際には、その身分を示す証明書をし、関係者に提示するものとする。

(4) 暴力団員等による不当介入を受けた場合の措置

① 受注者は、暴力団員等による不当介入を受けた場合は、断固としてこれを拒否すること。また、不当介入を受けた時点で速やかに警察に通報を行うとともに、捜査上必要な協力を行うこと。再委託先等が不当介入を受けたことを認知した場合も同様とする。

② ①により警察に通報又は捜査上必要な協力を行った場合には、すみやかにその内容を記載した書面により発注者に報告すること。

③ ①及び②の行為を怠ったことが確認された場合は、指名停止等の措置を講じる

ことがある。

④　暴力団員等による不当介入を受けたことにより工程に遅れが生じる等の被害が生じた場合は、発注者と協議すること。

8.13 疑義

本仕様書の内容に疑義が生じた場合、および本仕様書に明記されていない事項は担当者との協議による。

別添１

国立研究開発法人建築研究所情報資産管理システム導入及び運用保守支援業務
資料閲覧等申込書

資料閲覧等に係る遵守事項を了解の上、下記のとおり資料の閲覧等を申し込みます。

令和　　年　　月　　日

会社名：

担当者名：

連絡先：(電話番号)
　　(メールアドレス)

閲覧等希望日時：(第一希望) 令和　　年　　月　　日　　時
　　(第二希望) 令和　　年　　月　　日　　時

閲覧者氏名：

資料閲覧等に係る遵守事項
１．資料閲覧等を行う者は、資料閲覧等で知り得た情報を第三者に漏らしてはならない。
２．資料閲覧等を行う者は、資料閲覧等で知り得た情報を国立研究開発法人建築研究所情報資産管理システム導入及び運用保守支援業務の入札手続き以外に使用してはならない。
３．資料閲覧等を行う者は、資料閲覧等で知り得た情報を国立研究開発法人建築研究所情報資産管理システム導入及び運用保守支援業務の入札手続き終了後においても第三者に漏らしてはならない。
４．資料閲覧等を行う者は、資料閲覧等で知り得た情報を適切に管理し、国立研究開発法人建築研究所の許可なく複製・転送等をしないこと。

別添２

件名：国立研究開発法人建築研究所共用計算機システム借入及び運用支援業務

項	フォルダ	文書
01	要件定義書	要件定義書
2	基本設計書	基本設計書
2-1		別紙1ハードウェア・ソフトウェア一覧
2-2		別紙2ネットワーク物理構成図
2-3		別紙3ネットワーク論理構成図
2-4		別紙4サーバ一覧
		別紙5サーバ物理接続図
		別紙6ラック搭載図
		別紙7ネットワークアドレス一覧
		別紙8Microsoft365Businessライセンス利用機能一覧
3	詳細設計書	00アカウント一覧
3-1		00機器ホスト名・IPアドレス一覧
3-2		01iDRAC詳細設計書
3-3		02共有ストレージ詳細設計書
3-4		03UPSソフト詳細設計書
3-5		04ファイアウォールサーバ詳細設計書
3-6		0501SINET接続用スイッチングハブ
3-7		0502基幹ネットワーク接続用スイッチングハブ
3-8		0503画像情報棟スイッチングハブ
3-9		0504DMZ接続用スイッチングハブ
3-10		0505棟間接続用スイッチングハブ
3-11		06仮想化基盤サーバ
3-12		07WindowsServer2022
3-13		0801Red Hat Enterprise Linux8詳細設計書
3-14		0802Apache詳細設計書
3-15		0803BIND詳細設計書
3-16		0804Postfix詳細設計書
3-17		0805AWStats詳細設計書
3-18		0806サービスの一覧
3-19		0807パーソナルファイアウォール設定
3-20		09Webアプリケーションファイアウォール
3-21		10Zabbix詳細設計書
3-22		11Arcserve UDP詳細設計書
3-23		12RADIUSサーバ詳細設計書
		13証明書発行サーバ詳細設計書
		14内部ネットワークサービスサーバ詳細設計書
		15挙動監視サーバ詳細設計書
		1601M365認証連携機能詳細設計書
		1602M365認証連携機能_Onegate詳細設計書
		1701M365端末ウイルス対策(DefenderForBusiness機能）詳細設計書
		1702M365端末ウイルス対策(MicrosoftIntuneスクリプト）詳細設計書
		1703M365グループウェア(M365共通機能)詳細設計書
		1704M365グループウェア(ExchangeOnlineメール機能)詳細設計書
		1705M365グループウェア(Defenderメールセキュリティ機能)詳細設計書
		1706M365グループウェア(Purviewメールコンプライアンス機能)詳細設計書
		1707M365グループウェア(SharepointOnline機能)詳細設計書
		1708M365グループウェア(MicrosoftTeams機能)詳細設計書
		1709M365グループウェア(AzureAD機能)詳細設計書
4	運用設計書	運用設計書
4-1		運用支援業務
5	各ハードウェア、ソフトウェア設定報告書	各ハードウェア、ソフトウェア設定報告書
6	動作試験仕様書（テスト設計書）	テスト計画書
6-1		サーバ管理機能(iDRAC)単体・結合テストチェックリスト
6-2		共有ストレージ単体・結合テストチェックリスト

項	フォルダ	文書
6-3		UPS単体・結合テストチェックリスト
6-4		ファイアウォールサーバ単体・結合テストチェックリスト
6-5		ネットワークスイッチ単体・結合テストチェックリスト
6-6		仮想化基盤サーバ単体・結合テストチェックリスト
6-7		WindowsServer2022単体・結合テストチェックリスト
6-8		Red Hat Enterprise Linux 8単体・結合テストチェックリスト
6-9		Apache単体・結合テストチェックリスト
6-10		BIND単体・結合テストチェックリスト
6-11		Postfix単体・結合テストチェックリスト
6-12		AWStats単体・結合テストチェックリスト
6-13		Webアプリケーションファイアウォール単体・結合テストチェックリスト
6-14		Zabbix単体・結合テストチェックリスト
6-15		Arcserve UDP単体・結合テストチェックリスト
6-16		RADIUSサーバ単体試験成績書
6-17		証明書発行サーバ単体試験成績書
6-18		内部ネットワークサービスサーバ単体試験成績書
6-19		EPSAP結合障害試験成績書
6-20		挙動監視サーバ棚井・連動試験仕様書兼結果報告書
6-21		挙動監視アナライザ単体・連動試験仕様書兼結果報告書
6-22		M365認証連携機能テスト仕様書兼結果報告書
6-23		M365グループウェア単体・結合テストチェックリスト
6-24		M365端末ウイルス対策単体・結合テストチェックリスト
6-25		総合テスト障害(NW)テストチェックリスト
6-26		総合テスト(障害・電源)チェックリスト
6-27		総合テスト(運用)チェックリスト
7	動作試験成績書（テスト実績）	サーバ管理機能(iDRAC)単体・結合テストチェックリスト
7-1		共有ストレージ単体・結合テストチェックリスト
7-2		UPS単体・結合テストチェックリスト
7-3		ファイアウォールサーバ単体・結合テストチェックリスト
7-4		ネットワークスイッチ単体・結合テストチェックリスト
7-5		仮想化基盤サーバ単体・結合テストチェックリスト
7-6		WindowsServer2022単体・結合テストチェックリスト
7-7		Red Hat Enterprise Linux 8単体・結合テストチェックリスト
7-8		Apache単体・結合テストチェックリスト
7-9		BIND単体・結合テストチェックリスト
7-10		Postfix単体・結合テストチェックリスト
7-11		AWStats単体・結合テストチェックリスト
7-12		Webアプリケーションファイアウォール単体・結合テストチェックリスト
7-13		Zabbix単体・結合テストチェックリスト
7-14		Arcserve UDP単体・結合テストチェックリスト
7-15		RADIUSサーバ単体試験成績書
7-16		証明書発行サーバ単体試験成績書
7-17		内部ネットワークサービスサーバ単体試験成績書
7-18		EPSAP結合障害試験成績書
7-19		挙動監視サーバ棚井・連動試験仕様書兼結果報告書
7-20		挙動監視アナライザ単体・連動試験仕様書兼結果報告書
7-21		M365認証連携機能テスト仕様書兼結果報告書

項	フォルダ	文書
7-22		M365グループウェア単体・結合テストチェックリスト
7-23		M365端末ウイルス対策単体・結合テストチェックリスト
7-24		総合テスト障害(NW)テストチェックリスト
7-25		総合テスト(障害・電源)チェックリスト
7-26		総合テスト(運用)チェックリスト