別添 1. 要求仕様書

情報基盤システムサービス
要求仕様書

令和４年１２月

独立行政法人 国立特別支援教育総合研究所

目次

別紙一覧

別紙 1.要件定義書
別紙 2.成果物一覧
別紙 3.SLA 項目一覧

参考一覧

【参考 1】現行ネットワーク基盤システム構成図
【参考 2】次期システム構成図
【参考 3】職員・研修員数一覧
【参考 4】現行スイッチ配置一覧
【参考 5】現行無線 AP 設置一覧
【参考 6】端末配置一覧
【参考 7】フロアプリンタ配置一覧
【参考 8】平面図
【参考 9】既存システムの移行に関する情報
【参考 10】端末別利用サービス対応表

1. 概要

1.1. 調達件名

情報基盤システムサービスの調達

1.2. 調達の背景および目的

独立行政法人国立特別支援教育総合研究所（以下「当研究所」という。）では、業務の効率化、高度化を進めるために電子計算機システム（以下「現行システム」という。）を導入し、運用しているところであり、当該システムは当研究所の研究および事務遂行において必要不可欠なものとなっている。

現行システムは、2016(平成 28 年)年 12 月に導入したもので、2023(令和 5 年)年 12 月のシステム更改を実施する。

次期情報基盤システム(次期システムから名称変更し、情報基盤システムとしている。(以下「次期システム」という。))では、現行システムを更に発展させ、“いつでも・どこでも・誰とでも”業務ができる環境を提供することで一層の業務効率化および研究活動を促進するとともに、クラウドサービスの活用およびクラウド化に対応したセキュリティ対策も進め、柔軟かつ堅牢な基盤システムの実現を目指す。

1.3. システムの内容

1.3.1. 概要

次期システムは、職員が研究および事務を行う上で利用する利用者認証サービス、各種コミュニケーションサービス、ファイル共有サービス等の各種サービスを提供する業務システム、研究管理棟をはじめ各棟に敷設されている LAN で構成され、約 100 台のクライアント端末から利用される。

（ア）次期情報基盤システムの基本方針

次期システムでは、「1.2.調達の背景および目的」に沿って、業務効率の向上、コストの削減、セキュリティ対策の向上を推進するため、現状の課題を踏まえて検討した結果、以下 3 点を次期システムにおける実現方針とする。

（１）”いつでも・どこでも・誰とでも”効率的な業務ができる環境

①”早くて軽い”快適な シンクライアント環境の提供

（２）クラウドサービスの活用

「政府情報システムにおけるクラウドサービスの利用に係る基本方針」(2018 年 6 月 7 日各府省情報化統括責任者（CIO）連絡会議決定）に基づき、クラウドサービスを

活用する。なお、クラウドサービスの活用にあたり、サービス・業務ごとに、本仕様書で求める、機能要件、サービスレベル、情報セキュリティ水準等の条件を満たすこと。

① アップデートを前提としたシステム設計

ソフトウェアのアップデート、セキュリティ対策が適時に、確実に実施されること等によって、利便性や安全性を向上するとともに運用・保守コストの削減が図られるようシステム設計を行う。

② システム構築範囲の最小化

サービス提供に必要な、ハードウェア、ソフトウェア、機能等について、導入、構築等に時間を要する範囲を縮小することによって、導入、構築等にかかる期間の短縮化や災害時等におけるシステム運用継続性の向上を図る。

（３）デジタル化とクラウド化に対応したセキュリティ対策

「政府機関等のサイバーセキュリティ対策のための統一基準群（令和 3 年度版）」（令和 3 年 7 月 7 日サイバーセキュリティ戦略本部）等を踏まえ、将来像を見据えたサイバーセキュリティ対策やクラウド利用に関わるリスクへの対策等を推進する。

① 最新のサイバー脅威への対策強化

未知の不正プログラム対策を、感染の未然防止、プログラムが動作する内部へ進化させるとともに、ソフトウェア等の脆弱性の効率的な把握を可能とするなど最新のサイバーセキュリティ対策の実現に必要な機能を導入する。

② 適切なセキュリティとデジタルワークスタイルの両立

各サービスやセキュリティ対策において、最新の技術・方式の採用や実装の最適化により、セキュリティ水準の維持・向上と利便性・効率性の向上を両立したシステムを実現する。

③ クラウド利用に備えた対策

各サービスや他システムでのクラウドサービス利用に対応し、次期システムとクラウドサービス間の安全な接続等、クラウドサービス利用に関するセキュリティ対策を実施する。

（イ）システムの基本構成

a. 次期システムの基本構成はハウジングサービスを活用すること。

b. サーバ、ストレージ及びネットワーク等のハードウェア機器は、仮想化が適さないものを除き、仮想化技術を用いることで集約を図る。

c. ハードウェアリソース(CPU、メモリ、ディスク容量、ネットワーク回線等)及びシステムリソース等（利用量等）を可視化し容易に再配分することに加えて、一元的に管理することでリソース配分の最適化、システム運用業務の負荷減少、増築等に伴う設定変更の簡素化を図る。

d. 障害時における業務継続性を向上させるため、物理障害のポイントを削減し、各サービスの特性を踏まえた冗長化構成、バックアップ体制を講じる。

e. ハードウェアリソース逼迫時、障害時、被災時における各サービスの業務継続性の向上のため、論理構成及び物理構成を実装する。

f. 昨今及び将来のサイバー攻撃に対応すべく、より強固なセキュリティ対策として、ゼロデイ脆弱性や既知及び未知の脅威に対しても常に最速、かつ、確実な検知・遮断、対応等を実現するために、最新の技術を適用した振る舞い検知、ログ分析、監視等を導入し、侵入防止はもとより、侵入後における適切な対策によるセキュアな環境を提供する。

g. 職員は、次期システムを利用するに当たり利便性とセキュリティ性に優れたシンクライアント端末を利用する。

1.3.2. システム要件

各サービスの機能及びシステム要件については「別紙 1.要件定義書」を参照のこと。

1.3.3. 契約期間

契約締結日から令和１０年１１月３０日までとする（うちサービス提供期間（有償期間）は令和５年１２月１日から令和１０年１１月３０日までとする。）。

1.3.4. 作業スケジュール案

次期システムの稼働は、作業スケジュールに沿って遅延なくサービスを提供すること。受託者が提案するスケジュールを当研究所研修情報課等担当職員（以下「担当職員」という。）に示して了承を得ること。

2. 調達に関連する事項

2.1. 本調達の内容、範囲および成果物

2.1.1. 調達内容

本調達においては、以下のサービスを提供する。

（ア）提供サービス

（１）システム及びネットワークに関する提供サービス

「別紙 1.要件定義書」に記載するシステム及びネットワーク

（２）作業等に関する提供サービス

次期システムのライフサイクルに係る作業等提供一式（次期システムの設計、構築、導入、運用支援、保守、物品の納入、現行システムからの移行に関する作業等）

2.1.2. 調達範囲

各サービスの提供、構築、次期システムへの各種移行作業、運用支援、保守、導入支援、教育並びに他システムへの接続支援までを範囲とする。

（ア）現行事業者との責任分界点

次期システムへの移行は受託者が責任を持って管理すること。移行計画においては、当研究所及び現行システム側で行うべき作業も含めて検討した上で計画書を作成し、現行事業者と協力して対応すること。移行計画作成に必要な現行システムの情報は、当研究所から提供する。

また、移行作業は現行システムの運用中の作業となるため、受託者は現行システムの停止や性能劣化等を発生させないための対策を講ずること。

（イ）各種個別システムとの責任分界点

（１）SINET ネットワークとの接続に係る責任分界点

当研究所は、SINET 横浜 DC との間に 10Gbps 回線により SINET に接続している。

学術情報ネットワーク SINET(Science Information NETwork)とは、日本全国の大学、研究機関等の学術情報基盤として、国立情報学研究所が構築、運用している情報通信ネットワークのことである。

受託者は、当研究所が別途調達した WDM 装置に接続すること。接続に当たり受託者は事前に接続する情報及びスケジュールの提示を受けること。

（２）その他のシステムとの接続に係る責任分界点

他システムとのサーバ機器や PC、プリンタ等との接続は受託者の責任で実施すること。現時点での接続予定機器は「別紙 1.要件定義書」にて示すが、移行時点で新規に追加されている機器の情報提供を当研究所から受けた上で、全機器を次期システムに接続すること。

他システム自体の動作確認は本調達の範囲外であるが、ネットワーク接続に必要な情報の提供及び立会い、また接続できなかった場合の技術的支援を行うこと。

なお、運用期間中において、他システム側の更改等により再接続等（各システム 1 回程度を想定）が発生した場合、次期システム側で必要となる作業を行うこと。

2.1.3. 次期システムの提供範囲

a. 当研究所　研究管理棟、特別支援教育情報センター棟、研修棟、西研修員宿泊棟、東研修員宿泊棟、生活支援研究棟

2.1.4. 納期

（ア）基本要件

a. 調達するハードウェア及びソフトウェアの中に、提案時点において製品化されていないものが含まれる場合は、以下のとおり対応すること。

（i） 製品化されていないハードウェア、及びソフトウェアを明確にすること。

（ii） 当該ハードウェア及びソフトウェアを納期までに提供する旨の誓約書及び根拠資料を当研究所に提出すること。

（イ）外的要因による対応

a. 調達するハードウェア及びソフトウェアの中に、世界的な半導体供給不足等既知の外的要因の影響を受けて、納期までに提供できないものが発生した場合は、以下のとおり対応すること。

（i） 納期までに提供できないハードウェア、及びソフトウェアを明確にすること。

（ii） 納期までに提供できない理由を明確にすること。

（iii） 本システムの運用上、当該ハードウェア及びソフトウェアを納期までに提供できないことにより、発生する影響の内容及び程度を明確にすること。

（iv） 当該ハードウェア及びソフトウェアの納品が完了するまでの間（以下、「未納期間」という。）における最善の代替策を提案すること。

（v） 以上の内容を簡潔にまとめた文書を当研究所に提出すること。

（vi） 当該文書に基づいて、当研究所と協議の上、未納期間の代替策を決定

すること。

（vii）運用開始後、受託者の負担により当該代替策を実施すること。

2.1.5. 成果物

（ア）成果物および納入

a. 受託者は落札後速やかに担当職員と協議の上、「別紙 2.成果物一覧」に示す成果物の提出日程を確定し、提出すること。

b. 成果物の提出については、当研究所の承認を経た内容を電子媒体で当研究所が指示する場所に納入すること。

（イ）成果物の修正・変更

a. 成果物に修正等がある場合、更新履歴と修正ページを示した上で修正後の全編を速やかに提出すること。

（ウ）検収

a. 当研究所において、担当職員が受託者立会いの上、試験運用を実施後、次期システムに係る検収を実施する。
なお、検収実施に際しては、担当職員の負荷を極力抑えかつ可能な限り実運用を想定した負荷試験を行う等、必要十分な範囲の検証ができる方法を提案すること。

b. 前述「2.1.5(ア) 成果物及び納入」に則って、納入成果物を提出すること。その際、当研究所の指示により、別途品質保証が確認できる資料を作成し、納入成果物と併せて提出すること。

c. 検収の結果、納入成果物の全部又は一部に不合格品が生じた場合には、受託者は直ちに引き取り、必要な修正を行った後、指定した日時までに修正が反映された全ての納入成果物を納入すること。

（エ）責任の所在

a. 検収後、契約期間終了までの間、次期システムを正常に使用した状態で不具合が発見され、提供されるサービスが正常稼働しなかった場合には、受託者の責任と負担において、迅速に修理、修復、又は、交換等を行い、サービスの正常稼働を担保すること。また、当研究所は、契約金額を上限として、上記対応を実施してもなお生じる損害に対する賠償の請求を行うことができるものとする。

b. 納入した物品やサービス等の稼働・保守については、物品の製造者やサービス提供者の如何に関わらず、受託者が最終責任を負うこととし、自社製品・サービス以外の場合もこれを受託者と製造者・提供者間の契約等によ

り担保すること。
なお、製造者・提供者からのサポートが確実に受けられる体制を構築すること。

c. 次期システムに関する技術的問題点、機器のバグ、パッチ及びバージョンアップ等に関する情報を速やかに提供すること。また、パッチ、バージョンアップ等の適用を実施する場合は、スケジュールを提示して当研究所の承認を受けた上で、実施すること。なお、必要に応じて、事前検証等を実施すること。

(オ) 著作権等

a. 実施要項「12.(4)著作権」を参照すること。

2.1.6. 入札制限、制約条件等

(ア) 入札制限

a. 実施要項「4 入札参加資格に関する事項」を参照すること。

3. 提供サービス内容

サービス開始時における前提条件やプロジェクト全体に関わる内容、システム設計・構築・試験、システム運用・保守等におけるサービス提供内容を示す。

なお、サービス個々の要件に関する内容は「別紙 1.要件定義書」を参照すること。

3.1. サービス開始および機器の設置等に関する前提条件

a. 受託者は契約締結後 5 営業日以内に、作業体制とともに、作業内容及びスケジュール等について記載したプロジェクト計画書を作成し、当研究所に提出し、承認を得ること。詳細は、「3.2.プロジェクト全体に係る提供サービス内容」に基づき実施すること。

b. プロジェクト計画書においては、プロジェクト管理を行うために、進捗管理方法・課題管理方法について記載すること。

c. 作業体制には、作業責任者、個人情報取扱責任者及び作業担当者の氏名及び所属、担当作業、指揮命令系統、情報セキュリティ対策に係る管理・連絡体制並びに連絡先を記載すること。また、情報取扱者名簿及び情報管理体制図を提出すること。また、以下の内容を含む情報セキュリティ対策を実施すること。

（i） 受託者に提供する情報の受託者における目的外利用の禁止

（ii） 受託者における情報セキュリティ対策の実施内容及び管理体制

（iii）事業の実施に当たり、受託者又はその従業員、下請負先、若しくはその他の者による意図せざる変更が加えられないための管理体制

（iv） 受託者の資本関係・役員等の情報、事業の実施場所、事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供

（v） 情報セキュリティインシデントへの対処方法

（vi） 情報セキュリティ対策その他の契約の履行状況の確認方法

（vii）情報セキュリティ対策の履行が不十分な場合の対処方法

d. 受託者は、次期システムのサービス提供に当たって、全機能提供開始後の運用を十分考慮し、保守、サポートを含むサービス提供に係る一切の作業を行うこと。

e. 現行システムに支障を来した場合、受託者の負担で復旧作業等を行うこと。

f. 本仕様書で要求する全機能を、全機能提供開始日から利用できること。なお、一部機能が利用できない場合は、代替機能を受託者の負担で提供すること。

g. 機器の設置等のため、当研究所執務室に立ち入る場合は、原則として、平

日の 8:30～17:15 以外とすること。その際、事前に作業スケジュールを示した上で担当職員の許可を得ること。

h. 受託者は、作成担当以外の第三者（品質管理者の設置）によって、網羅性、正確性、全体との整合性などの品質を高めるため、レビューを実施すること。

i. 受託者は、工程管理に対して、プロジェクト計画書、設計書、課題管理表、議事録など、ドキュメントとの整合性が取れているか、システム要件に係る観点でのレビューを実施し、当該レビューにおいて指摘された内容に対し、必要な対応を行うこと。

j. 機器及び必要資材の搬入等を行う場合、おおよそ 1 週間前までに詳細な施工方法、施工範囲、作業員名、スケジュール及び使用車両について、予め定めた書面をもって作業申請を行い、担当職員の承認を得ること。なお、当研究所内での構内工事、エレベーター/電気設備等定期点検により、構内全域または特定の区域にて、立ち入りまたは、利用ができない期間、時間帯が発生する場合が想定されることから、少なくとも申請 1 週間前には事前相談をすること。なお、年 1 回の電気設備定期点検(終日 1 日間を予定)の場合には、構内の電気が停止する。また、当研究所が行うべき作業がある場合には、これを明示すること。

k. 機器の設置等により、受託者の責に帰する事由による造営物及び道路の損傷、土地踏み荒らし等、当研究所及び第三者に与えた損害に対する費用等は、全て受託者の負担とする。

l. その他必要事項については、適宜担当職員と協議の上、決定すること。

3.2. プロジェクト全体にかかる提供サービス内容

a. 受託者は、WBS（Work Breakdown Structure）を用いて、次期システムの全機能が提供されるまでの間、効率的なプロジェクト管理を行うこと。

b. 受託者は、本仕様書に記載する全ての項目について、適切に管理するためにプロジェクト管理責任者を定めること。

c. プロジェクト管理責任者は、担当職員の指示のもと、適切なプロジェクト管理に努めること。

d. プロジェクト管理責任者は、担当職員の指示に従い、プロジェクト計画書、ガントチャート（後工程に対して大きく影響する作業については必要に応じて WBS ディクショナリを含む。）、進捗状況表、課題管理表といったプロジェクト管理に必要とされる資料を作成し、提出すること。

e. WBS にはタスクごとに受託者側の主担当名称を記載すること。

f. WBS には発注者側のタスクを明示して記載すること。また、タスク期間は

発注者が要する期間を考慮したスケジュールとすること。

g. プロジェクトに係る体制、発注者側の制約等を考慮した上で現実的な WBS とスケジュールを示すこと。

h. プロジェクトのステークホルダを整理して、プロジェクト計画書に定義すること。

i. プロジェクト管理責任者は、常に作業実績を把握し、計画との差異分析を行うこと。なお、WBS 等の変更が必要な場合には、予め担当職員の了承を得ること。

3.3. システム運用・保守に係る提供サービス内容

3.3.1. SLA に関する提供事項

（ア）SLA を評価する上での前提条件

a. サービス提供開始時点から 2 か月間は調整期間とし、3 か月目から SLA の遵守の対象とする。また、達成及び未達成の評価は、月単位で行う。

b. 受託者は、各サービスの監視、測定等を行い、後述する「3.3.1.(イ)SLA 項目」に記載されているサービスレベルの達成状況を逐次確認、把握すること。なお、監視、測定方法については、担当職員と協議の上、決定すること。

c. 受託者は、月単位でサービスレベル目標値を設定した項目に対して実績を報告し、SLA 達成度合いを評価する。

d. SLA を満たせない可能性がある場合、速やかに担当職員に報告すること。また、サービスレベルを保つための対策について検討し準備すること。

e. 受託者は、SLA を遵守できなかった場合には、対応策について検討し、担当職員の了承を得た上で実施すること。

f. 対応の実施に当たっては、サービスレベル目標値に達成できる対応がなされるまで月次レベルで報告すること。

g. 対応に必要な人的リソースの追加、体制の変更、対応のために必要なシステムの導入等に費用がかかる場合、受託者の費用負担により、実施すること。

h. サービスレベルの評価に当たって、以下の事項に該当する場合は、SLA 規程の範囲外とする。

（i） 当研究所の都合によって障害復旧できなかった場合

（ii） 当研究所の事由によって障害連絡を受けることができなかった場合

（iii）予見できない不測の事態（社会通念上、受託者に責任がないことが認められる事態）が生じた場合

（イ）SLA 項目

a. SLA 項目については、「別紙 3.SLA 一覧」を参照とすること。
b. 設計・開発業務の過程にて、受託者が提供するシステムに起因しない事由によって要求水準を達成できないと判断された場合、設定 SLA 値については担当職員と別途協議の上、決定する。
c. SLA 項目は、当研究所及び受託者双方の合意事項に明確な変更が生じた場合、当研究所及び受託者双方が必要と認めた場合等、必要に応じて見直しを実施し改訂するものとする。

3.3.2. 実施に関する提供事項

a. 保守・運用支援の実施体制を示すこと。
b. 統括責任者を配置し、全体の管理を担うこと。
c. (独)情報処理推進機構が定める「IT スキル標準（ITSS）レベル 4」相当以上の能力を有する担当技術者を配置すること。
d. 実施体制、統括責任者及び担当技術者に変更がある場合は、事前に当研究所に連絡すること。

4. 秘密保持契約

a. 本調達を実施する上で知り得た内部情報は、関係者以外に漏洩しないように厳重に管理すること。

5. 例外の協議

a. 契約期間中に要件を満たせなくなった場合は、当研究所と協議の上、必要かつ適切な対策を講じること。

6. その他

6.1. 政府・省庁規程及び各種ガイドラインへの準拠

以下に示す各種ガイドライン（最新版）を遵守すること。今後契約期間中に当該文書が改定された場合には、それに従うこととするが、より良い作業の進め方又は手法について提案がある場合には、担当職員に提案、協議の上、当該提案に基づき実施してもよい。

a. 内閣官房内閣サイバーセキュリティセンター・デジタル庁・総務省・経済産業省所管「政府情報システムのためのセキュリティ評価制度（ISMAP)」
b. 経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」

c. 独立行政法人国立特別支援教育総合研究所「独立行政法人国立特別支援教育総合研究所セキュリティポリシー」
d. 独立行政法人情報処理推進機構「『高度標的型攻撃』対策に向けたシステム設計ガイド」
e. 独立行政法人情報処理推進機構「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド」
f. サイバーセキュリティ対策推進会議「高度サイバー攻撃対処のためのリスク評価等のガイドライン」及び内閣官房内閣サイバーセキュリティセンター「高度サイバー攻撃対処のためのリスク評価等のガイドライン付属書」」
g. サイバーセキュリティ戦略本部決定「政府機関等のサイバーセキュリティ対策のための統一規範」、「政府機関等のサイバーセキュリティ対策の運用等に関する指針」及び「政府機関等のサイバーセキュリティ対策のための統一基準」並びに内閣官房内閣サイバーセキュリティセンター「政府機関等の対策基準策定のためのガイドライン」
h. 独立行政法人情報処理推進機構「安全な Web サイトの作り方」
i. ISO/IEC15408
j. ISO27017(クラウドサービスセキュリティ管理策)
k. ISO27001(情報セキュリティマネジメントシステム)
l. 経済産業省「IT 製品の調達におけるセキュリティ要件リスト」
m. 各府省情報化統括責任者（CIO）連絡会議決定「デジタル・ガバメント推進標準ガイドライン」

6.2. 政府・省庁規程及び各種ガイドラインの動向への留意

以下に示す各種ガイドライン（最新版）及び関連する施策の動向に留意し提案すること。

a. 平成 30 年 12 月 10 日関係省庁申合せ「IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」
b. 令和 3 年 9 月 28 日閣議決定「サイバーセキュリティ戦略」

6.3. 法律・規格への準拠

a. 導入するハードウェア及びソフトウェア等の構成要素は、オープンシステム環境の整備を可能とするため、ITU-T（国際電気通信連合 電気通信標準化部門）、ISO（国際標準化機構）等が規定、又は、推奨する各種国際標準及び装置の製造・データ処理に関して、IEEE（米国電気電子学会）等が規定、又は、推奨する各種デファクトスタンダードに準拠していること。また、これらと必要十分なインタフェースを有すること。
b. 「民法（明治 29 年 4 月 27 日法律第 89 号）」、「刑法（明治 40 年 4 月 24 日

法律第 45 号)」、「著作権法（昭和 45 年 5 月 6 日法律第 48 号)」、「不正アクセス行為の禁止等に関する法律（平成 11 年 8 月 13 日法律第 128 号)」、「個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号)」の関連法規を遵守すること。

6.4. 閲覧・提供資料

a. 応札予定者は、(i)の資料を閲覧することができる。また資料の閲覧を希望する場合は、必要な手続きを行った上、当研究所が定める期間、場所、方法において閲覧を許可する。また、以下の資料の他に閲覧を希望する資料がある場合には、当研究所と相談すること。

b. (ii)参考資料は必要な手続きを行った上で、本仕様書の添付資料として応札予定者に提示する。

（i） 現行システムに係る資料

・完成図書

・要件定義検討資料

・基本設計書

・詳細設計書(パラメータ設計書)

・運用マニュアル

（ii） 参考資料

・【参考 1】 現行ネットワーク基盤システム構成図

・【参考 2】 次期システム構成図

・【参考 3】 職員・研修員数一覧

・【参考 4】 現行スイッチ配置一覧

・【参考 5】 現行無線 AP 設置一覧

・【参考 6】 端末配置一覧

・【参考 7】 フロアプリンタ配置一覧

・【参考 8】 平面図

・【参考 9】 既存システムの移行に関する情報

・【参考 10】 端末別利用サービス対応表

6.5. 技術仕様等に関する留意事項

a. 提案システムのうち、納入期限までにバージョンアップが予想されるハードウェア又はソフトウェアについては、その予定時期等が記載された資料を提出すること。

b. 納入時におけるすべてのソフトウェアは、契約時の最新バージョンで提供すること。なお、日本語版があるものは日本語版で提供すること。

c. 性能、機能に関する要件の各項目で述べる性能、機能を満たすならば、複

数個の装置で実現するように指定している場合でも、設置場所ごとの単一の装置で実現してもよい。

6.6. 提案に関する留意事項

a. 提案に際しては、提案システムが仕様書の要求要件をどのように満たすのか、あるいはどのように実現するのかを要求要件ごとに具体的かつわかり易く、記載すること。従って、技術的要件に対して、単に「できます。」「提案します。」といった回答の場合、提案書とみなさないので十分に留意して作成すること。
b. 提出資料等に関する照会先を、明記すること。
c. 提案書提出時に既に存在するハードウェア及びソフトウェアについて納入稼働実績がある場合には、そのリストを提出すること。
d. 調達内容が不明確である場合は、有効な提案書とみなさないので留意されたい。
e. 提案書の内容に関してヒアリングを行う場合がある。

6.7. その他の留意事項

a. 技術的要件に“当研究所で別途調達した”と記載のあるソフトウェア以外は全て現行システムの契約満了に伴い、リースアップするため、ハードウェア及びソフトウェアのライセンス等は受託者が新規で用意し、その費用は本調達に含めること。
b. 納品・提出する資料等は、原則として全て日本語で記述されていること。やむを得ず外国語による資料を提出する場合は、日本語に翻訳した文書を添付すること。
c. 原則として、グリーン購入法に適合した機器を提供すること。
d. 本調達に係る経費は見込まれる全ての事項を見込むこと。
e. 受託者は、本仕様書に記載なき事項であっても、本業務遂行に必要と認められる事項・作業については、当研究所と協議の上、誠意を持って対応すること。

7. 性能、機能に関する要件

7.1. 基本要件

a. 本仕様書に示す各要件は最低限の要求要件である。ただし、指定した要件・機能を満たすことができる機能・技術・構成が別にある場合は、そのことを証明する資料を添付した上で提案してもよい。

別紙1

情報基盤システムサービス
要件定義書

令和４年１２月

独立行政法人 国立特別支援教育総合研究所

目次

1. 概要

1.1. 名称

a. 情報基盤システム（以下「本システム」という。）

1.2. 目的

a. 本システムの目的は、当研究所の利用者が業務又は研修上必要なハードウェア、ソフトウェア、アプリケーション等を、当研究所のネットワーク環境で安全かつ円滑に利用するための情報基盤となる総合的な情報システムを構築することである。

1.3. 構成

a. 本システムは、以下の 4 つのサービスから構成される。
   ①情報サービス基盤システム
   ②情報ネットワーク基盤システム
   ③情報セキュリティ基盤システム
   ④クライアントサービス
b. 情報サービス基盤システムは、仮想デスクトップ・ストレージ・メール等のサービスを当研究所用に調整して提供するものである。
c. 情報ネットワーク基盤システムは、有線 LAN、無線 LAN 及びリモートアクセス環境を整備するとともに、ネットワークの運用上必要なサービスを提供するものである。
d. 情報セキュリティ基盤システムは、当研究所の情報セキュリティポリシーや国のガイドライン等に適合するセキュリティ対策を確実に実施するために必要なサービスを提供するものである。
e. クライアントサービスは、当研究所の利用者が業務又は研修上必要なハードウェア及びソフトウェアを提供するものである。

1.4. サービス提供方法

a. 本システムのサービスは、国内の信頼できるデータセンターに仮想化基盤を構築するとともに、別途調達する Microsoft 365 A5 を利用して提供するものとする。
b. 部分的にクラウドサービスを組み合わせてもよい。

1.5. 利用者

a. 本システムの利用者は、以下のとおりとする。

区分	利用者数	利用可能範囲
職員	110 名	職員用イントラネットを利用可
研修員	90 名	研修員用イントラネットを利用可
ゲスト利用者	30 名	インターネット接続のみ
外部研究協力者	60 名	当該利用者が参画する研究プロジェクトの共有フォルダにのみアクセス可

2. 全般的要件

2.1. 性能等

2.1.1. 基本要件

a. 24 時間 365 日安定した連続運用が可能なサービスを提供すること。
b. 当研究所の規模に見合った適正なスペックのサービスを提供すること。
c. 可能な限り業務の集約・一元化に努めること。
d. 可能な限り処理の自動化・省力化に努めること。
e. 可能な限りレスポンスの向上に努めること。
f. 多様な利用者に対するアクセシビリティに配慮すること。
g. 操作性を最適化して、使いやすさに配慮すること。
h. システム管理担当者（以下「担当職員」という。）の運用のしやすさに配慮すること。
i. コスト削減と安定性・安全性・利便性の向上との両立を図ること。
j. 運用工数の効率化を図ること。
k. 運用に関連して生じる後年度負担の低減を図ること。

2.1.2. 製品保証要件

a. 契約期間を通じて保守サポートを受けられる見込みのある製品を提供すること。
b. 契約期間中に保守サポートが受けられなくなる事態が発生することのないように、調達した全ての製品に関する最新の情報を継続的に収集し、当研究所と協議の上、必要かつ適切な対策を講じること。

2.1.3. 環境適合性要件

a. 国等による環境物品等の調達の推進等に関する法律（平成 12 年法律第 100 号）に適合する製品を可能な限り提供すること。

2.2. データセンター

2.2.1. 基本要件

a. 我が国の法令が適用される場所に立地していること。
b. 当研究所から公共交通機関を利用して概ね 3 時間以内に駆け付けられる場所に立地していること。
c. ISO/IEC27001 又は総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン 第 3 版」が定めるデータセンターに関する要件を満たすこと。
d. 耐震性、給電性能、入室セキュリティ等、一般的なデータセンターとしての施設要件を満たすこと。
e. データセンター内に設置する全ての機器を収納でき、さらに、6U 以上の別の機器を収納可能なラックスペースを備えていること。
f. 機器設置に必要なパッチパネル、ラックマウント用レール、ボルト等は、受託者の負担により調達すること。
g. 運用開始後、設置機器を物理的に操作又は確認しなければならない事態が生じることを

想定し、別途契約の上、当該業務を常駐オペレータに委託できる余地があること。

2.2.2. 通信回線要件

a. インターネットから切り離された閉域網を経由して、当研究所とデータセンターを接続すること。
b. 閉域網は、SINET の L2VPN サービスを利用して構築すること。なお、当研究所が別途調達している SINET 接続回線の規格は 10GBASE-SR である。
c. データセンター内で直接 SINET に接続すること。
d. データセンターから SINET を経由してインターネットに接続すること。

2.3. クラウドサービスの利用

2.3.1. 基本要件

a. NISC・デジタル庁・総務省・経済産業省所管「政府情報システムのためのセキュリティ評価制度（ISMAP)」に適合するクラウドサービスを可能な限り利用すること。
b. 我が国の法律及び締結された条約が適用される国内データセンターを選択できるクラウドサービスを利用すること。
c. 我が国に裁判管轄権があるクラウドサービスを利用すること。
d. 国内の行政・研究・教育機関等において十分な稼働実績のあるクラウドサービスを利用すること。

2.3.2. セキュリティ要件

a. 利用するクラウドサービスにおいて一定のセキュリティレベルが確保されていることの保証として、当該クラウドサービスに対する情報セキュリティ監査報告書の内容、及び取得・維持している各種認定・認証制度の基準等について事前に確認すること。
b. 契約終了時、利用したクラウドサービスに保存されている全てのデータを遅滞なく確実に消去すること。
c. 前 2 項の要件については、別途調達する Microsoft 365 A5 は対象外とする。

2.4. セキュリティ対策

2.4.1. 基本要件

a. ISO27001 認証を取得していること。
b. 当研究所の情報セキュリティポリシーや国のガイドライン等に適合するセキュリティ対策を確実に実施すること。
c. 当研究所が保有する情報の機密性・完全性・可用性を担保すること。
d. サービスの特性に応じた多要素認証を行うこと。
e. サービスの特性に応じたマルウェア対策を行うこと。
f. 契約期間を通じて継続的にセキュリティ対策を最適化すること。

2.4.2. 可用性要件

a. サービスの特性に応じた冗長化を行うこと。

b. サービスの特性に応じたバックアップ及び復元を行うこと。

2.4.3. 通信暗号化要件

a. 以下の通信について、暗号化を確実に行うこと。
①無線 LAN における無線 AP・端末間の通信
②リモートアクセス環境における通信
③本システムに含まれるクラウドサービスとの通信
④別途調達する Microsoft 365 A5 との通信
b. 第三者認証局が発行する電子証明書を用いた通信暗号化が行えること。
c. 電子証明書として、NII が発行する UPKI 電子証明書を利用できること。

2.4.4. 脆弱性対策要件

a. 納入する製品のソフトウェアに対する脆弱性検査を行い、問題や不具合が発見された場合は、是正した上で納品すること。
b. 納入する製品のソフトウェアに対して、当該製品の運用開始 1 ヶ月前の時点で公開されている更新プログラムを適用すること。
c. 脆弱性検査及び更新プログラムの適用に当たっては、その必要性について当研究所と協議の上、必要と判断されたものについて実施すること。
d. 常に最新の脆弱性情報を入手して、公開された脆弱性について対策を実施すること。
e. 本システムの脆弱性対策の状況を定期的に確認すること。

2.5. その他

2.5.1. 機器設置要件

a. 調達した機器は、当研究所が指定する場所に安全に設置して、電源接続及び LAN 接続を行うこと。
b. 初期設定等の調整を行うこと。
c. 動作テストを実施して、正常に動作することを確認すること。
d. 機器管理に必要な情報を記載したラベルを作成して、当該機器の外から見える場所に貼付すること。
e. 既設のスイッチ、無線 AP 及び UTM 装置を撤去して、当研究所内の所定の場所に移動すること。
f. 電源接続に必要な電源コード及びタップは、受託者の負担により調達すること。
g. LAN 接続に必要なパッチケーブルは、受託者の負担により調達すること。

2.5.2. 停電解消時要件

a. 当研究所内に設置する機器については、落雷等による停電が解消した際、停電前の正常な稼働状態に復旧するための作業手順を用意すること。

3. 各サービス要件

3.1. 情報サービス基盤システム

3.1.1. 共通事項

（ア）業務要件

a. 以下のサービスについて、当研究所用に調整した上で提供すること。
①プラットフォームサービス
②統合認証サービス
③仮想デスクトップサービス
④プリントサービス
⑤ストレージサービス
⑥メールサービス
⑦グループウェアサービス

b. サービスの提供に当たっては、国内の信頼できるデータセンター内に仮想化基盤を構築するとともに、別途調達する Microsoft 365 A5 を利用すること。ただし、部分的にクラウドサービスを組み合わせてもよい。

（イ）性能等要件

a. 24 時間 365 日安定した連続運用が可能な情報サービス基盤として機能すること。

3.1.2. プラットフォームサービス

（ア）業務要件

a. 以下のサービスを提供するためのプラットフォームとなる仮想化基盤を構築すること。
［1］情報サービス基盤システム
①統合認証サービス
②仮想デスクトップサービス
③プリントサービス
④ストレージサービス
［2］情報ネットワーク基盤システム
①VPN 接続サービス
②内部向け DNS サービス
③外部向け DNS サービス
④証明書管理サービス
⑤DHCP サービス
⑥RADIUS サービス
［3］情報セキュリティ基盤システム
①ゲートウェイセキュリティ対策サービス
②エンドポイントセキュリティ対策サービス
［4］運用管理サービス

①システム監視サービス
②ログ管理サービス
③バックアップ管理サービス

b. 以下の機器を提供すること。
①サーバ装置
②ストレージ装置

c. 提供する製品相互の親和性が高く一体的な運用が可能な機器構成であること。

d. 必要に応じて部分的にクラウドサービスを組み合わせてもよいが、全体として安定的に運用できるプラットフォームを構築すること。

e. 特定のサーバにトラフィックが集中しないように、サーバ構成を最適化すること。

f. 機器の稼働状況やリソース状況を一元的に管理する仕組みを提供すること。

g. 時刻同期を確実に行う仕組みを提供すること。

（イ）ハードウェア要件

(1) サーバ装置

a. 仮想化基盤を安定的に運用するために必要な性能を備えたサーバ装置又はハイパーコンバージドインフラストラクチャ（以下「HCI」という。）を提供すること。

b. 2台以上の機器による冗長構成とすること。

c. 現行システムの完成図書「電子計算機システムリソース」及び本システムの各要件を参照して各サーバの負荷を算定し、必要なリソースを確保すること。

d. 1コア当たりのCPU周波数は、2GHz以上であること。

e. 物理サーバを仮想化する基本ソフトウェアはハイパーバイザー型とすること。

f. 仮想サーバのゲストOSとして、Windows Server 2016/2019/2022、Windows10/11及びRedHat Enterprise Linux 8.xをサポートすること。

g. 仮想サーバの通信に使用するインタフェースを冗長化すること。

h. 仮想サーバの通信に使用するインタフェースとストレージ装置との通信に使用するインタフェースを分離すること。

i. BIOS及びファームウェアを意図しない又は悪意のある変更等から保護する機能を有すること。

j. 仮想サーバを無停止で別の物理サーバに移動する機能を有すること。

k. 障害発生時、仮想サーバを自動的に別の物理サーバにフェールオーバする機能を有すること。

l. SNMP機能を有すること。

m. syslog機能を有すること。

n. 筐体内部での電源冗長化に対応していること。

o. 停電発生時、10分間給電可能で、その時間内に自動的にシャットダウンする仕組みを備えていること。

(2) ストレージ装置

a. 仮想化基盤を安定的に運用するために必要な性能及び容量を備えたストレージ装置又は

HCI を提供すること。

b. 現行システムの完成図書「電子計算機システムリソース」及び本システムの各要件を参照して各サーバのディスクサイズを算定し、適切な容量を確保すること。その際、ドライブやノードに障害が発生した場合でも継続稼働を可能にするために必要な予備領域も考慮すること。

c. 仮想デスクトップのデータ領域にはフラッシュストレージを使用すること。

d. HCI を提供する場合を除き、RAID6 以上の冗長構成とし、障害発生時にはホットスワップによりディスクを交換できること。

e. HCI を提供する場合は、3 方向のミラーリングを行い、2 つのドライブやサーバに障害が発生した場合でも継続稼働が可能であること。

f. SNMP 機能を有すること。

g. syslog 機能を有すること。

3.1.3. 統合認証サービス

（ア）業務要件

a.「(イ) 機能要件」を満たす統合認証サービスとして、以下の製品を提供すること。

①Active Directory サーバ

②IdP サーバ又は IDaaS

③Active Directory サーバと Azure Active Directory サービスを連携する仕組み

④Active Directory サーバと RADIUS サービスを連携する仕組み

⑤ゲストアカウントを発行・管理する仕組み

b. 提供する製品間で ID 及びパスワードを連携し、統合認証基盤として一体的な運用が可能であること。

（イ）機能要件

(1) アカウント管理機能

a. 利用者のアカウントを一元的に管理する機能を有すること。

b. 300 件以上のアカウントを登録できること。

c. CSV ファイルのアップロードによるアカウントの一括登録が行えること。

d. CSV ファイルをアップロードする際、データの整合性をチェックできること。

e. アカウントの有効期限を設定できること。

f. 有効期限を過ぎたアカウントを自動的にロックできること。

g. ログイン認証に連続して失敗したアカウントを自動的にロックできること。

h. アカウントを手動でロックできること。

i. アカウントのロックを手動で解除できること。

j. アカウントを廃止する場合、当該アカウントを削除せずに無効化できること。

k. メールサービスと一体的にメールアカウントを管理できること。

l. グループウェアサービスと一体的に利用者の所属グループを管理できること。

m. パスワードを暗号化して管理できること。

n. パスワードを利用者自身が変更できること。

o. パスワードを初期化できること。
p. ゲストアカウントを発行できること。

(2) アクセス制御機能
a. 当研究所ネットワーク上のリソースに対する利用者のアクセス制御を一元的に管理する機能を有すること。
b. 利用者ごとに、以下の設定が行えること。
①当該利用者に配信する仮想デスクトップの紐付け
②当該利用者が利用可能なプリンタ・複合機等の紐付け
③共有フォルダのアクセス権限設定
c. 利用者の属性に対応したアクセス制御パターン（以下「グループポリシー」という。）を設定できること。
d. グループポリシーは、利用者の属性ベース及び管理対象リソースベースの両方を設定できること。
e. グループポリシーに基づいて、利用者のアクセス制御を一括設定できること。

(3) ログイン認証機能
a. ログイン認証に必要な ID 及びパスワードを一元的に管理する機能を有すること。
b. RADIUS サービスと連携して、ID 及びパスワードによるログイン認証が行えること。
c. 多要素認証に対応できること。

(4) シームレスログイン機能
a. 以下のサービスやアプリケーションを利用する際、個別のログイン認証を必要としない機能を有すること。
①仮想デスクトップサービス
②ストレージサービス
③メールサービス
④グループウェアサービス
⑤オフィススイートアプリケーション（Word、Excel、PowerPoint 等）
b. 別途調達する Microsoft 365 A5 に対して、SAML2.0 認証によるシングルサインオンが行えること。

(5) 学認連携機能
a. NII が運営する学術認証フェデレーション（以下「学認」という。）に参加するために必要な機能を有すること。
b. 学認 IdP として運用できること。
c. 学認により認証された当研究所の利用者が、以下の学認 SP を国内のどこからでも利用できること。また、当研究所が利用可能な学認 SP の追加・変更に対応すること。なお、学認 SP 側で必要な設定については、当研究所が行うものとする。
①NII-CiNii Research
②NII-GakuNin RDM
③NII-JAIRO Cloud

④NII-学認 LMS
⑤NII-edurome JP
⑥JST-researchmap
⑦NALIS My Library（NTT データ九州が提供する図書業務システム）
⑧KinoDen（紀伊國屋書店が提供する電子書籍）
⑨SAGE Journals（SAGE 社が提供する電子ジャーナル）
⑩EBSCO host（EBSCO 社が提供する学術文献データベース）

d. 学認に対して、SAML2.0 認証によるシングルサインオンが行えること。

3.1.4. 仮想デスクトップサービス

（ア）業務要件

a. 「(イ) 機能要件」を満たす仮想デスクトップサービスを提供すること。
b. 仮想デスクトップ 110 台を、1 人 1 台の専用割り当て方式により提供すること。
c. 提供する仮想デスクトップは、オーバーコミットなしで、以下のリソースを物理的に確保すること。なお、仮想デスクトップの最終設計段階においては、リソースのオーバーコミットを考慮してもよい。
①CPU: 2vCPU 以上
②メモリ: 16GB 以上
③ストレージ: 170GB 以上
e. 仮想デスクトップのマスタイメージを提供すること。

（イ）機能要件

(1) VDI 環境設定機能

a. 以下の VDI 環境を設定する機能を有すること。
①リソースの割り当て
②OS 及びアプリケーションのインストール
b. 必要に応じて仮想デスクトップを初期化できること。

(2) VDI 配信機能

a. 仮想デスクトップを利用者に配信する機能を有すること。
b. 統合認証サービスと連携して、利用者ごとに、配信する仮想デスクトップの紐付けが行えること。
c. ICA・RDP・PCoIP 等の低帯域で利用可能な画面転送プロトコルを使用すること。
d. 移動プロファイルを使用しないこと。

(3) VDI 管理機能

a. 仮想デスクトップの設定情報や稼働状況を一元的に管理する機能を有すること。
b. 仮想デスクトップに割り当てるリソースを管理できること。
c. WSUS を利用して、仮想デスクトップの OS に対してセキュリティパッチ等の一括配信が行えること。

3.1.5. プリントサービス

（ア）業務要件

a. 「(イ) 機能要件」を満たすプリントサービスを提供すること。
b. 管理対象のプリンタ・複合機等は巻末資料「参考 7 プリンタ・複合機等一覧表」を参照すること。

（イ）機能要件

(1) プリンタ管理機能

a. プリンタ・複合機等の設定情報や稼働状況を一元的に管理する機能を有すること。
b. 統合認証サービスと連携して、利用者ごとに、利用可能なプリンタ・複合機等の紐付けが行えること。
c. プリンタドライバを一元的に管理して、各クライアントへの個別のインストールを必要としないこと。
d. 管理対象のプリンタ・複合機等を任意に追加・削除できること。

(2) 印刷制御機能

a. 各クライアントからの印刷要求を制御する機能を有すること。
b. 印刷要求のキャンセルが行えること。

3.1.6. ストレージサービス

（ア）業務要件

a. 「(イ) 機能要件」を満たすストレージサービスを提供すること。
b. 以下のストレージを提供すること。

区分	容量
共有ストレージ	10TB
個人用ストレージ	一人 10GB 以上×110 名

c. 個人用ストレージは、別途調達する Microsoft 365 A5 を利用すること。

（イ）機能要件

(1) ファイル保存機能

a. 多様な形式のデータファイルを安全に保存する機能を有すること。

(2) 共有フォルダ管理機能

a. 共有ストレージのフォルダを一元的に管理する機能を有すること。
b. 統合認証サービスと連携して、利用者ごとに、共有フォルダのアクセス権限を設定できること。
c. フォルダを階層化できること。
d. フォルダ単位で容量の上限を設定できること。
e. サービスを停止することなくフォルダの設定や容量を変更できること。

(3) スキャンデータ保管機能

a. スキャナ・複合機等で作成したスキャンデータを受信して、共有ストレージに保管する機能を有すること。

(4) ファイル共有機能

a. 個人用ストレージに保管されている任意のファイルについて、アクセス権限を付与して共有する機能を有すること。

(5) 研究データ管理機能

a. NII が運営する GakuNin RDM と連携して、研究データを一元的に管理する機能を有すること。
b. 研究プロジェクトごとに、外部研究協力者に対する共有フォルダのアクセス権限を設定できること。
c. 外部研究協力者を含む利用者が、学認及び GakuNin RDM を経由して、当研究所が別途調達する S3 互換オブジェクトストレージにアクセスできること。

3.1.7. メールサービス

(ア) 業務要件

a. 「(イ) 機能要件」を満たすメールサービスとして、以下のサービスを提供すること。
①メールサーバ
②メールクライアントサービス
③メール中継サービス
b. メールサーバ及びメールクライアントサービスについては、別途調達する Microsoft 365 A5 を利用すること。

(イ) 機能要件

(1) メールアカウント管理機能

a. メールアカウントを一元的に管理する機能を有すること。
b. 300 件以上のメールアカウントを登録できること。
c. 統合認証サービスと一体的にメールアカウントを管理できること。
d. パスワードを暗号化して管理できること。
e. パスワードを利用者自身が変更できること。
f. パスワードを初期化できること。

(2) メール送受信機能

a. OAuth2.0 認証に対応したメールクライアントサービスを利用してメールの送受信を行う機能を有すること。
b. メール送信先のオートコンプリート機能が標準装備されている場合は、当該機能の使用又は不使用を選択できること。
c. メール 1 通当たりの容量を制限できること。
d. ループを検知した場合、自動的にメールの送信を停止できること。

e. 第三者認証局が発行する電子証明書を用いたS/MIMEメール暗号化が行えること。

(3) ウェブメール機能

a. ウェブブラウザを利用してメールの送受信を行う機能を有すること。
b. 既定のウェブブラウザとして、Microsoft Edge、Google Chrome及びMozilla Firefoxを利用できること。

(4) 代表アドレス機能

a. 当研究所の組織・部署等を代表するメールアドレス（以下「代表アドレス」という。）を利用してメールの送受信を行う機能を有すること。
b. 代表アドレス宛てに受信したメールは、当該組織・部署等に所属する職員が任意に閲覧できること。

(5) アドレス帳機能

a. メールクライアントサービスを利用してアドレス帳を作成する機能を有すること。
b. 個人用アドレス帳及び共有アドレス帳を作成できること。
c. アドレス帳を参照してメール送信先（Cc等を含む。）を設定できること。
d. アドレス帳を階層化できること。

(6) メーリングリスト機能

a. 外部ドメインを含む任意の複数のメールアドレスをグループ化し、メーリングリストとして利用する機能を有すること。
b. メーリングリストの有効期限を設定できること。

(7) メール保存機能

a. 受信メールをメールボックスに漏れなく保存する機能を有すること。
b. メールボックスを階層化できること。
c. メールアカウントごとに、メールボックス容量の上限を設定できること。
d. メールボックスの利用量が容量の上限に近づいた場合、利用者に容量制限のアラートを通知できること。
e. 保存メールの一覧を件名順・日付順・送信者順等でソートできること。
f. 保存メールの全文検索が行えること。
g. メールのアーカイブが行えること。

(8) メール中継機能

a. 以下のメールについて、メールサーバに中継する機能を有すること。
①本システムのハードウェアから自動送信されるメール
②スキャナ・複合機等で作成したスキャンデータの送信メール

(9) スパムメール対策機能

a. スパムメールをフィルタリングし、排除する機能を有すること。

3.1.8. グループウェアサービス

（ア）業務要件

a. 別途調達する Microsoft 365 A5 を利用して、「（イ）機能要件」を満たすグループウェアサービスを提供すること。

b. 各機能の環境設定・調整等については、当研究所と協議の上、必要と判断された範囲内で実施すること。

（イ）機能要件

(1) ポータル機能

a. 利用者が直接利用するサービスの入口となる画面（以下「ポータル画面」という。）を作成する機能を有すること。

b. 利用者の所属グループに対応したポータル画面を作成できること。

c. 統合認証サービスと一体的に利用者の所属グループを管理できること。

(2) 共有アドレス帳機能

a. メールサービスと連動した共有アドレス帳を提供する機能を有すること。

(3) 掲示板機能

a. 一般的な掲示板機能を有すること。

(4) スケジュール管理機能

a. 一般的なスケジュール管理機能を有すること。

(5) 在席確認機能

a. 一般的な在席確認機能を有すること。

(6) 施設・備品予約機能

a. 一般的な施設・備品予約機能を有すること。

(7) ファイル共有機能

a. 一般的なファイル共有機能を有すること。

(8) タスク管理機能

a. 一般的なタスク管理機能を有すること。

(9) ワークフロー管理機能

a. 一般的なワークフロー管理機能を有すること。

(10) ウェブ会議機能

a. 一般的なウェブ会議機能を有すること。

(11) アンケート作成・編集・管理機能

a. 一般的なアンケート作成・編集・管理機能を有すること。

3.2. 情報ネットワーク基盤システム

3.2.1. 共通事項

（ア）業務要件

a. 有線 LAN 及び無線 LAN を整備すること。
b. 利用者がテレワーク・出張先等からインターネットを経由して当研究所ネットワークに接続できるリモートアクセス環境を整備すること。
c. 以下のサービスについて、当研究所用に調整した上で提供すること。
①VPN 接続サービス
②内部向け DNS サービス
③外部向け DNS サービス
④証明書管理サービス
⑤DHCP サービス
⑥RADIUS サービス

（イ）性能等要件

a. 24 時間 365 日安定した連続運用が可能な情報ネットワーク基盤として機能すること。
b. 当研究所ネットワークの論理構成について、以下のセグメントに分割できること。
①職員用 VLAN
②研修員用 VLAN
③ゲスト利用者用 VLAN

（ウ）利用者別運用要件

(1) シンクライアント端末

a. 有線 LAN、無線 LAN 及びリモートアクセス環境を利用できる仕組みを構築すること。
b. 職員用 VLAN に接続すること。
c. RADIUS サービスによる IEEE802.1X（EAP-TLS）認証を行うこと。
d. 事前にクライアント証明書をインストールできること。
e. 無線 LAN を利用する場合は、職員用 SSID に接続すること。
f. SSID 選択時、端末起動後の初回を除き、パスワードの入力を必要としないこと。

(2) 必要に応じて別途調達する職員用端末

a. 有線 LAN、無線 LAN 及びリモートアクセス環境を利用できる仕組みを構築すること。
b. 職員用 VLAN に接続すること。
c. RADIUS サービスによる IEEE802.1X（EAP-TLS）認証を行うこと。
d. 事前にクライアント証明書をインストールできること。
e. 無線 LAN を利用する場合は、職員用 SSID に接続すること。
f. SSID 選択時、端末起動後の初回を除き、パスワードの入力を必要としないこと。

(3) 研修員の BYOD 端末

a. 無線 LAN を利用できる仕組みを構築すること。

b. 研修員用 VLAN に接続すること。
c. RADIUS サービスによる IEEE802.1X（EAP-PEAP）認証を行うこと。
d. 研修員用 SSID に接続すること。
e. SSID 選択時、端末起動後の初回を除き、パスワードの入力を必要としないこと。
f. 職員向けサービスにアクセスさせないこと。

(4) ゲスト利用者の BYOD 端末

a. 無線 LAN を利用できる仕組みを構築すること。
b. ゲスト利用者用 VLAN に接続すること。
c. RADIUS サービスによる IEEE802.1X（EAP-PEAP）認証を行うこと。
d. 事前にゲストアカウントを取得できること。
e. ゲスト利用者用 SSID に接続すること。
f. SSID 選択時、端末起動後の初回を除き、パスワードの入力を必要としないこと。
g. インターネットへの接続のみ許可し、職員及び研修員向けサービスにアクセスさせないこと。

3.2.2. 有線 LAN 整備

（ア）業務要件

a.「(イ) 機能要件」を満たす有線 LAN 環境を整備すること。
b. 以下の機器を提供すること。
①基幹 L3 スイッチ
②認証 L2 スイッチ
③フロア L2 スイッチ
c. 提供する製品相互の親和性が高く一体的な運用が可能な機器構成であること。
d. 機器の稼働状況やリソース状況を一元的に管理する仕組みを提供すること。
e. DMZ を設定する仕組みを提供すること。
f. 各機器の提供台数については、「別表 1 次期スイッチダウンリンクポート数一覧」に記載されている設置場所ごとの必要ポート数に基づいて提案すること。ただし、東・西研修員宿泊棟に設置する機器については、無線 AP（宿泊棟用）の提供台数及び設置場所に対応する形で、ゼロベースで提案すること。

（イ）機能要件

(1) L3 機能

a. ルーティング機能（Static・RIP・OSPF）を有すること。
b. DHCP リレーエージェント機能を有すること。

(2) L2 機能

a. IEEE802.1Q に準拠したタグベース VLAN 機能を有すること。
b. ループ検知機能を有すること。
c. ループを検知した場合、当該ポートを閉塞できること。
d. ループを検出してポートを閉塞した場合、当該ポートを自動的に開放できること。

（ウ）ハードウェア要件

(1) 基幹 L3 スイッチ

a. 当研究所の情報ネットワーク基盤を安定的に運用するために必要な性能を備えた基幹 L3 スイッチを提供すること。
b. 2 台以上の機器による冗長構成とすること。
c. データセンター内及び当研究所サーバ室内の計 2 ヶ所に設置し、以下の機器と接続すること。
   [1] データセンター内に設置する機器
      ①SINET 接続回線の終端装置
      ②サーバ装置
      ③WLC 装置
      ④UTM 装置
   [2] 当研究所サーバ室内に設置する機器
      ①SINET 接続回線の終端装置
      ②認証 L2 スイッチ
d. SINET 接続回線の終端装置と接続する光回線の規格は 10GBASE-SR とすること。
e. 所定の機器と接続するために必要十分な規格及び数量のポートを搭載していること。
f. スイッチング容量及び最大パケット転送能力は、搭載された全てのポートにおいてワイヤースピードの性能が出せること。
g. デュアルスタック方式により IPv4 及び IPv6 を同時に処理できること。
h. 「(イ) 機能要件 (1) L3 機能」を有すること。
i. 「(イ) 機能要件 (2) L2 機能」を有すること。
j. SINET の L2VPN サービスに対応したゲートウェイ機能を有すること。なお、当該機能を実現するために基幹 L3 スイッチと異なる機器を設置するほうが望ましい場合は、その機器及びシステム構成を提案に含めること。
k. 冗長化された機器間で FDB・ARP テーブル・IP ルーティングテーブル等を同期する機能を有すること。
l. 外部メディアにコンフィグファイル・ファームウェア等を出力する機能を有すること。
m. SNMP 機能を有すること。
n. syslog 機能を有すること。
o. 筐体内部での電源冗長化に対応していること。
p. 停電発生時に 10 分間給電可能な UPS に接続すること。
q. EIA 規格に準拠した 19 インチラックマウントが行えること。

(2) 認証 L2 スイッチ

a. 当研究所の情報ネットワーク基盤を安定的に運用するために必要な性能を備えた認証 L2 スイッチを提供すること。
b. 当研究所サーバ室内及び研究管理棟各フロア EPS 室内の計 4 ヶ所に設置し、以下の機器と接続すること。なお、それ以外の場所にも認証 L2 スイッチを設置するほうが望ましい場合は、その機器及びシステム構成を提案に含めること。

①基幹 L3 スイッチ

②フロア L2 スイッチ

c. 基幹 L3 スイッチと接続する LAN ケーブルの規格は 1000BASE-SX とし、4 ポート以上で接続すること。

d. 10G/1000BASE-X ポートを 4 個以上搭載していること。

e. スイッチング容量及び最大パケット転送能力は、搭載された全てのポートにおいてワイヤースピードに近い性能が出せること。

f.「(イ) 機能要件 (2) L2 機能」を有すること。

g. RADIUS クライアント機能を有すること。

h. SNMP 機能を有すること。

i. syslog 機能を有すること。

j. 当該機能を不必要とする場合を除き、PoE 給電機能を有すること。

k. 停電発生時に 10 分間給電可能な UPS に接続すること。

l. EIA 規格に準拠した 19 インチラックマウントが行えること。

(3) フロア L2 スイッチ

a. 当研究所の情報ネットワーク基盤を安定的に運用するために必要な性能を備えたフロア L2 スイッチを提供すること。

b. スイッチング容量及び最大パケット転送能力は、搭載された全てのポートにおいてワイヤースピードに近い性能が出せること。

c.「(イ) 機能要件 (2) L2 機能」を有すること。

d. SNMP 機能を有すること。

e. syslog 機能を有すること。

f. 当該機能を不必要とする場合を除き、PoE 給電機能を有すること。

g. EIA 規格に準拠した 19 インチラックマウントが行えること。

3.2.3. 無線 LAN 整備

(ア) 業務要件

a.「(イ) 機能要件」を満たす無線 LAN 環境を整備すること。

b. 以下の機器を提供すること。

①無線 AP

②無線 AP (宿泊棟用)

③無線 LAN コントローラ (以下、「WLC 装置」という。)

c. 提供する製品相互の親和性が高く一体的な運用が可能な機器構成であること。

d. 機器の稼働状況やリソース状況を一元的に管理する仕組みを提供すること。

e. 無線 LAN に接続された端末への不正アクセスを防ぐ仕組みを提供すること。

f. eduroam を利用できる仕組みを提供すること。

g. 無線 AP の提供台数については、「別表 1 次期スイッチダウンリンクポート数一覧」を参照すること。

h. 無線 AP の設置場所については、「別表 2 無線 AP 設置場所平面図」を参照すること。

i. 東・西研修員宿泊棟に設置する無線 AP（宿泊棟用）の提供台数及び設置場所については、現地調査を行った上で、ゼロベースで提案すること。

（イ）機能要件

(1) SSID 管理機能

a. 各無線 AP において、以下の SSID を同時に設定・運用する機能を有すること。
①職員用 SSID
②研修員用 SSID
③ゲスト利用者用 SSID

b. 職員用 SSID は、1000 件以上の IP アドレスに対応できること。

c. 研修員用 SSID は、500 件以上の IP アドレスに対応できること。

d. ゲスト利用者用 SSID は、500 件以上の IP アドレスに対応できること。

e. SSID と VLAN をマッピングする機能を有すること。

f. SSID を必要に応じて無効化し、接続不可にする機能を有すること。

(2) 接続制御機能

a. 無線 LAN 規格 IEEE802.11ac 又は IEEE802.11ax に接続する機能を有すること。

b. 端末が IEEE802.11ac 以下の規格にしか対応できない場合、当該端末が対応可能な最上位の規格に優先的に接続する機能を有すること。

c. 5GHz 帯及び 2.4GHz 帯の両方で同一の SSID が使用されている場合、5GHz 帯に優先的に接続する機能を有すること。

c. 無線 AP に障害が発生した場合、当該無線 AP に接続されている端末の接続先を自動的に別の無線 AP に切り替える機能を有すること。

d. 利用者が無線 LAN に接続中の端末を持って移動した場合、当該端末の接続先を自動的に最適な無線 AP に切り替える機能を有すること。

(3) 電波調整機能

a. 無線 AP 間の電波干渉を回避するために、電波出力を調整する機能を有すること。

b. 無線 AP のチャネル及び電波出力を手動で固定化する機能を有すること。

c. W53 及び W56 帯域において無線 LAN 以外の電波を検知した場合、自動的にチャネルを変更して電波干渉を回避する機能を有すること。

（ウ）ハードウェア要件

(1) 無線 AP

a. 当研究所（東・西研修員宿泊棟を除く。）の無線 LAN を安定的に運用するために必要な性能を備えた無線 AP を提供すること。

b. 接続する無線 LAN 規格として、IEEE802.11a/b/g/n/ac/ax に対応していること。

c. IEEE802.11a/n/ac/ax については、W52・W53・W56 帯域に対応していること。

d. IEEE802.11ac については、Wave2 に対応していること。

e. IEEE802.11ax については、80MHz のチャンネルボンディングに対応していること。

f. 5GHz 帯及び 2.4GHz 帯の同時利用が可能なラジオを搭載していること。

g. 5GHz 帯及び 2.4GHz 帯ラジオにおいて、それぞれ 2×2 MIMO 以上に対応していること。
h. 同時接続可能な端末数は、1 ラジオ当たり 128 台以上であること。
i. 100/1000/2500BASE-T 以上のアップリンク用有線ポートを有すること。
j. 動作状態確認用の LED を有すること。
k.「(イ) 機能要件 (1) SSID 管理機能」を有すること。
l. SSID 及びパスワードによる認証機能を有すること。
m. RADIUS クライアント機能を有すること。
n. WPA3 方式及び WPA2 方式による通信暗号化に対応できること。
o. IEEE802.1k/r の高速ハンドオーバーに対応できること。
p. PoE 受電に対応できること。

(2) 無線 AP (宿泊棟用)

a. 東・西研修員宿泊棟の無線 LAN を安定的に運用するために必要な性能を備えた無線 AP を提供すること。
b. 接続する無線 LAN 規格として、IEEE802.11a/b/g/n/ac に対応し、IEEE802.11ax にも可能な限り対応していること。
c. IEEE802.11a/n/ac/ax については、W52・W53・W56 帯域に対応していること。
d. IEEE802.11ac については、Wave2 に対応していること。
e. 5GHz 帯及び 2.4GHz 帯の同時利用が可能なラジオを搭載していること。
f. 5GHz 帯及び 2.4GHz 帯ラジオにおいて、それぞれ 2×2 MIMO 以上に対応していること。
g. 10/100/1000BASE-T 以上のアップリンク用有線ポートを有すること。
h. 動作状態確認用の LED を有すること。
i.「(イ) 機能要件 (1) SSID 管理機能」を有すること。
j. SSID 及びパスワードによる認証機能を有すること。
k. RADIUS クライアント機能を有すること。
l. WPA3 方式及び WPA2 方式による通信暗号化に対応できること。
m. PoE 受電又は AC アダプタ受電に対応できること。

(3) WLC 装置

a. 全ての無線 AP を一元的に管理するために必要な性能を備えた WLC 装置 (機器又はクラウドサービス) を提供すること。
b. 障害発生時でも運用可能な構成であること。
c. クラウドサービスを利用する場合を除き、データセンター内に設置すること。
d.「(イ) 機能要件 (2) 接続制御機能」を有すること。
e.「(イ) 機能要件 (3) 電波調整機能」を有すること。
f. SNMP 機能を有すること。
g. syslog 機能を有すること。
h. その他、無線 AP を集中管理・制御する上で必要な機能を有すること。

3.2.4. VPN 接続サービス

（ア）業務要件

a.「(イ) 機能要件」を満たす VPN 接続サービスを提供すること。

（イ）機能要件

a. リモートアクセス環境を一元的に制御する機能を有すること。
b. RADIUS クライアント機能を有すること。
c. 当研究所ネットワークへの接続が許可されている端末以外に対しては VPN 接続を許可しない設定が行えること。
d. 第三者認証局が発行する電子証明書を用いた通信暗号化が行えること。
e. クライアント端末のアイドル状態が続いた場合、接続を自動的に切断できること。
f. 接続を自動的に切断するまでの時間を設定できること。
g. syslog 機能を有すること。

3.2.5. 内部向け DNS サービス

（ア）業務要件

a.「(イ) 機能要件」を満たす内部向け DNS サービスを提供すること。

（イ）機能要件

a. 当研究所内の通信における名前解決を一元的に制御する機能を有すること。
b. DNS の動的更新が行えること。
c. DNS の動的更新に際して、予め設定した TTL（生存時間）に基づいて、使用されていないレコードを削除できること。
d. DNS ゾーン転送が行えること。
e. DNS ゾーン転送を必要としない場合は、当該機能を停止できること。
f. IP アドレスによるゾーン転送制限が行えること。
g. IP アドレスによる DNS クエリの制限が行えること。
h. SOA・A・PTR・CNAME・MX 等のレコードを登録できること。
i. 統合認証サービスと一体的に名前空間を管理できること。
j. DNS キャッシュポイズニング攻撃から保護するため、DNSSEC を利用すること。
k. syslog 機能を有すること。

3.2.6. 外部向け DNS サービス

（ア）業務要件

a.「(イ) 機能要件」を満たす外部向け DNS サービスを提供すること。

（イ）機能要件

a. 当研究所外との通信における名前解決を一元的に制御する機能を有すること。
b. SOA・A・PTR・CNAME・MX 等のレコードを登録できること。
c. ドメイン名の正引き及び逆引きが行えること。

d. 正引き時と逆引き時の検索結果に不一致を生じさせないこと。
e. サブドメインの設定数に制限がないこと。
f. DNS ゾーン転送が行えること。
g. DNS ゾーン転送を必要としない場合は、当該機能を停止できること。
h. IP アドレスによるゾーン転送制限が行えること。
i. NII が運営する「分散セカンダリ DNS サービス」と連携できること。
j. DNSSEC に対応した名前解決の要求に適切な応答をするための措置を講じること。
k. syslog 機能を有すること。

3.2.7. 証明書管理サービス

（ア）業務要件

a.「(イ) 機能要件」を満たす証明書管理サービスを提供すること。

（イ）機能要件

(1) サーバ証明書管理機能

a. サーバ証明書の管理を一元的に制御する機能を有すること。
b. UPKI 電子証明書を取り込み、サーバ証明書として利用できること。
c. 第三者認証局が発行する電子証明書を取り込み、通信暗号化に利用できること。
d. 第三者認証局が発行する電子証明書を取り込み、IEEE802.1X 認証に利用できること。
e. 証明書失効リストをダウンロードできること。
f. syslog 機能を有すること。

(2) クライアント証明書管理機能

a. クライアント証明書の管理を一元的に制御する機能を有すること。
b. UPKI 電子証明書を取り込み、クライアント証明書として利用できること。
c. クライアント証明書の一括ダウンロードが行えること。
d. 利用者自身でクライアント証明書を更新できること。
e. クライアント証明書の有効期限切れをメール通知できること。
f. 証明書失効リストをダウンロードできること。
g. 失効したクライアント証明書の認証を成功させないこと。
h. syslog 機能を有すること。

3.2.8. DHCP サービス

（ア）業務要件

a.「(イ) 機能要件」を満たす DHCP サービスを提供すること。

（イ）機能要件

a. IP アドレスの払い出しを一元的に制御する機能を有すること。
b. 10,000 件以上の IP アドレスを払い出せること。
c. DHCP スコープを設定できること。
d. DHCP オプションを設定できること。

e. IP アドレスと MAC アドレスの紐付けが行えること。
f. 当研究所ネットワークへの接続が許可されている端末以外に対しては IP アドレスを払い出さない設定が行えること。
g. 特定の MAC アドレスに対して固定 IP アドレスを割り当てられること。
h. IP アドレスの払い出し期間を設定できること。
i. IP アドレスの払い出し状況を監視できること。
j. syslog 機能を有すること。

3.2.9. RADIUS サービス

（ア）業務要件

a.「(イ) 機能要件」を満たす RADIUS サービスを提供すること。

（イ）機能要件

a. 利用者認証及び端末認証を一元的に制御する機能を有すること。
b. ウェブ認証・MAC 認証・IEEE802.1X 認証が行えること。
c. IEEE802.1X 認証は、以下の認証方式に対応できること。
①EAP-TLS
②EAP-PEAP
d. 2,500 件以上のアカウントを登録できること。
e. 2,500 件以上の RADIUS クライアントを登録できること。
f. RADIUS クライアントからの問い合わせに対して、統合認証サービスと連携した認証応答及び属性応答が行えること。
g. RADIUS クライアントをグループ化できること。
h. RADIUS クライアント及びグループごとに応答属性を変えられること。
i. 任意の RADIUS 属性を登録できること。
j. ログイン済みアカウントを手動でログアウトできること。
k. eduroam を利用するための RADIUS プロキシサーバとして運用できること。
l. syslog 機能を有すること。

3.3. 情報セキュリティ基盤システム

3.3.1. 共通事項

（ア）業務要件

a. 以下のサービスについて、当研究所用に調整した上で提供すること。
①ゲートウェイセキュリティ対策サービス
②エンドポイントセキュリティ対策サービス

（イ）性能等要件

a. 24 時間 365 日安定した連続運用が可能な情報セキュリティ基盤として機能すること。

3.3.2. ゲートウェイセキュリティ対策サービス

（ア）業務要件

a. 「(イ) 機能要件」を満たすゲートウェイセキュリティ対策サービスを提供すること。
b. 以下の機器を提供すること。
①UTM 装置
c. 機器の稼働状況やリソース状況を一元的に管理する仕組みを提供すること。

（イ）機能要件

(1) ファイアウォール機能

a. 当研究所ネットワークのゲートウェイにおいて、外部からの不正アクセスやサイバー攻撃を防御する機能を有すること。
b. ファイアウォールを通過する通信パケットをファイアウォールポリシーに基づいて監視できること。
c. ファイアウォールポリシーとして、以下の項目を設定できること。
①送信元 IP アドレス
②宛先 IP アドレス
③ポート番号又はアプリケーション識別情報
④利用者識別情報
⑤許可/不許可の設定
d. ファイアウォールポリシーで不許可と定義された通信パケットを遮断できること。
e. ファイアウォールポリシーで定義されていない通信パケットを破棄できること。
f. 2,000 種類以上のアプリケーションをポート番号に関わらず識別して可視化できること。
g. スタティック NAT 機能を有すること。
h. ダイナミック NAT 機能を有すること。
i. NAPT 機能を有すること。

(2) IDS/IPS 機能

a. 当研究所ネットワークに対する外部からの通信内容を監視し、不正アクセスを防御する機能を有すること。
b. 不正アクセスのパターンを定義ファイルに登録できること。

c. 定義ファイルに基づいて、外部からの通信内容を監視できること。
d. 不正アクセスを検知した場合は、当該通信パケットを遮断できること。
e. 定義ファイルを自動的に更新し、常に最新の状態を維持できること。

(3) マルウェア対策機能

a. マルウェアをゲートウェイでフィルタリングし、排除する機能を有すること。

(4) スパムメール対策機能

a. スパムメールをゲートウェイでフィルタリングし、排除する機能を有すること。

（ウ）ハードウェア要件

(1) UTM 装置

a. 当研究所のゲートウェイセキュリティ対策を安定的に運用するために必要な性能を備えた UTM 装置（機器又はクラウドサービス）を提供すること。
b. 障害発生時でも運用可能な構成であること。
c. クラウドサービスを利用する場合を除き、データセンター内に設置すること。
d. 10/100/1000BASE-T ポートを 8 個以上搭載していること。
e. GbE インタフェース（RJ45）を 8 個以上搭載していること。
f. GbE インタフェース（SPF）を 8 個以上搭載していること。
g. 240GB 以上のストレージを内蔵していること。
h. ファイアウォール同時セッション数は、8,000,000 以上であること。
i. ファイアウォール新規セッション数は、450,000/秒以上であること。
j. ファイアウォールスループットは、36Gbps 以上であること。
k. IPS スループットは、10Gbps 以上であること。
l. SSL インスペクションスループットは、8Gbps 以上であること。
m.「(イ) 機能要件 (1) ファイアウォール機能」を有すること。
n.「(イ) 機能要件 (2) IDS/IPS 機能」を有すること。
o.「(イ) 機能要件 (3) マルウェア対策機能」を有すること。
p.「(イ) 機能要件 (4) スパムメール対策機能」を有すること。
q. VPN ゲートウェイ機能を有すること。
r. SNMP 機能を有すること。
s. syslog 機能を有すること。
t. その他、ゲートウェイセキュリティ対策を一元的に行う上で必要な機能を有すること。

3.3.3. エンドポイントセキュリティ対策サービス

（ア）業務要件

a.「(イ) 機能要件」を満たすエンドポイントセキュリティ対策サービスを提供すること。
b. 以下のエンドポイントに対して、セキュリティ対策を確実に行うこと。
①Windows 系サーバ
②Linux 系サーバ
③シンクライアント端末

c. シンクライアント端末のセキュリティ対策については、別途調達する Microsoft 365 A5 を利用すること。

（イ）機能要件

(1) EPP 機能

a. マルウェアによるサイバー攻撃をリアルタイムで防御する機能を有すること。
b. 予めダウンロードした定義ファイルの情報に基づいてマルウェアを検知し、駆除できること。
c. 定義ファイルを自動的に更新し、常に最新の状態を維持できること。

(2) 振る舞い検知機能

a. 未知のマルウェアによるサイバー攻撃を防御する機能を有すること。
b. プログラムの不正な動きを検知した場合は、当該プログラムを除去できること。

(3) EDR 機能

a. エンドポイントがマルウェアに感染した場合の被害を最小限に食い止める機能を有すること。
b. マルウェア感染を検知した場合、当該エンドポイントを速やかにネットワークから隔離できること。

3.4. クライアントサービス

3.4.1. シンクライアント端末

（ア）業務要件

a. シンクライアント端末 110 台を当研究所用に調整して提供すること。

（イ）ハードウェア要件

a. モバイル型のシンクライアント専用 PC とし、以下の規格を満たすこと。
   ①大きさ：330×220×20mm 以下
   ②重量：1.4kg 以下
   ③CPU：2.5GHz 以上かつ 4 コア以上
   ④メモリ：4GB 以上
   ⑤フラッシュメモリ：128GB 以上
   ⑥OS：シンクライアント専用 OS 又は Windows 組み込み OS
   ⑦ディスプレイサイズ：13 インチ以上、14 インチワイド以内
   ⑧ディスプレイ解像度：1920×1080 以上
   ⑨キーボード：JIS 標準配列準拠
b. 無線 LAN 規格 IEEE802.11ac 又は IEEE802.11ax に対応していること。
c. カメラ及びマイクを内蔵していること。
d. USB3.1 ポートを電源供給用を含まずに 3 ポート以上内蔵していること。
e. 必要に応じて別途調達するキーボード・マウス・ディスプレイ等の周辺機器を接続するためのインタフェースを内蔵していること。
f. LAN ケーブルを接続するためのインタフェース（内蔵又は外付け）を有すること。
g. HDMI ケーブルを接続するためのインタフェース（内蔵又は外付け）を有すること。

3.4.2. クライアントソフトウェア

（ア）業務要件

a. 仮想デスクトップに、以下のソフトウェアを搭載すること。
   ①OS
   ②PDF 作成・編集アプリケーション
   ③統計解析アプリケーション
   ④共分散構造分析アプリケーション
b. 巻末資料「参考 10 端末別利用サービス対応表」を参照し、必要数のライセンスを提供すること。

（イ）ソフトウェア要件

(1) 共通要件

a. 全てのソフトウェアについて、日本語版を提供すること。
b. 全てのソフトウェアについて、最新又は最適なバージョンを提供すること。

c. 各ソフトウェアの設定については当研究所の指示に従うこと。
d. 当研究所と協議の上、必要なバージョンアップを行うこと。

(2) OS

a. Microsoft 社「Windows 11 Pro」相当以上のソフトウェアを提供すること。

(3) PDF 作成・編集アプリケーション

a. Adobe 社「Adobe Acrobat Standard DC」相当以上のソフトウェアを提供すること。

(4) 統計解析アプリケーション

a. IBM 社「IBM SPSS Statistics Base Campus Edition」相当以上のソフトウェアを提供すること。
b. 同時アクセス 2 ライセンスを提供すること。
c. 最新版への無償アップグレードに対応すること。

(5) 共分散構造分析アプリケーション

a. IBM 社「IBM SPSS Amos Campus Edition」相当以上のソフトウェアを提供すること。
b. 同時アクセス 2 ライセンスを提供すること。
c. 最新版への無償アップグレードに対応すること。

3.5. 創意工夫の発揮可能性に関する加点項目

3.5.1. 利用者情報管理の効率化

a. 現行システムでは、利用者情報管理に際して、認証基盤・仮想デスクトップ・メール等の設定作業を短期間に個別に行う必要があるため、担当職員の負担が大きい。このことを踏まえて、本システムにおける利用者情報管理の効率化について、具体的な実現方法を提案すること。

b. 以下の業務について、実際の作業の流れを示すこと。
①利用者のアカウントの登録・変更
②各利用者に配信する仮想デスクトップの紐付け
③各利用者が利用可能なプリンタ・複合機等の紐付け
④共有フォルダのアクセス権限設定
⑤メールサービスにおける利用者情報の登録・変更
⑥グループウェアサービスにおける利用者情報の登録・変更
⑦ゲストアカウントの発行
⑧その他、利用者情報管理に関する業務

c. 前項で示した各作業について、提供するどの製品のどの機能により実現するかを具体的に示すこと。

d. 提案内容により実現可能な効果について、以下の観点に基づいて具体的に示すこと。
①業務の集約・一元化
②処理の自動化・省力化
③レスポンスの向上
④作業上のストレスの軽減

3.5.2. 仮想デスクトップ画面表示の効率化

a. 現行システムでは、シンクライアント端末にログインしてから仮想デスクトップ画面が表示されるまで概ね数分を要し、10 分以上待たされるケースも発生している。その原因として、ベンダーからは移動プロファイルに伴うネットワーク負荷の影響が指摘されている。このことを踏まえて、本システムにおける仮想デスクトップ画面表示の効率化について、具体的な実現方法を提案すること。

b. 以下の利用形態ごとに、シンクライアント端末の電源投入から仮想デスクトップ画面表示までのフローチャートを示すこと。
①有線 LAN 接続による利用
②無線 LAN 接続による利用
③リモートアクセス環境での利用

c. 前項のフローチャートにおける各処理段階について、提供するどの製品のどの機能により実現するかを具体的に示すこと。

d. 提案内容により実現可能な効果について、以下の観点に基づいて具体的に示すこと。
①処理の自動化・省力化
②レスポンスの向上
③作業上のストレスの軽減

4. 保守・運用支援要件

4.1. 共通事項

4.1.1. 実施体制

a. 保守・運用支援の実施体制を示すこと。
b. 統括責任者を配置し、全体の管理を担うこと。
c. (独)情報処理推進機構が定める「IT スキル標準（ITSS）レベル 4」相当以上の能力を有する担当技術者を配置すること。
d. 実施体制、統括責任者及び担当技術者に変更がある場合は、事前に当研究所に連絡すること。

4.1.2. 業務時間

a. 業務時間は、以下の日を除き、年間を通して 9 時から 17 時までとすること。
①土曜日
②日曜日
③国民の祝日に関する法律（昭和 23 年法律第 178 号）に定められた休日
④当研究所の休業日
b. 緊急な対応が必要な場合は、個別に当研究所と協議の上、その緊急度に応じて対応すること。

4.1.3. 受付窓口

a. 保守・運用支援に関する単一の受付窓口を設置すること。
b. 受付窓口は、業務時間中は常時連絡が可能な体制とすること。
c. システム障害等の緊急連絡は、24 時間 365 日対応可能であること。なお、緊急連絡窓口については、受付窓口と同一でなくてもよい。

4.1.4. 連絡会議

a. 当研究所と定期的に連絡会議を開き、作業報告や課題の検討等を行うこと。
b. 連絡会議は、原則として四半期に 1 回、ウェブ会議により開催すること。
c. 連絡会議の議事録を作成し、当研究所に提出すること。

4.1.5. 作業方法

a. 保守・運用支援に関する作業は、オンサイトで対応する場合を除き、遠隔操作により実施すること。
b. 遠隔操作を行う際は、VPN 接続を行って通信経路の安全を確保すること。

4.2. 保守

4.2.1. システム監視

a. 本システムの稼働状況及びリソース状況について、当研究所が必要に応じて把握できる仕組みを提供するとともに、受託者も同じ状況を把握できること。

4.2.2. ハードウェア保守

a. 調達機器の定期点検は実施しないものとするが、機器に障害が発生した場合は、以下のいずれかの対応を適切に実施すること。
①部品交換等の修理
②代替機器の提供
b. 交換する機器・部品等の代金は本調達に含めること。

4.2.3. サーバソフトウェアアップデート

a. サーバ装置のソフトウェアに対して、公開されたセキュリティパッチ等の適用作業（以下「アップデート」という。）を実施すること。
b. アップデートは、最低年 1 回実施すること。
c. アップデートの実施に当たっては、その必要性について当研究所と協議の上、必要と判断されたものについて実施すること。
d. 公開されたセキュリティパッチ等の緊急度又は重要度が高い場合は、当研究所と協議の上、速やかにアップデートを実施すること。

4.2.4. クライアントソフトウェアアップデート

a. シンクライアント端末のソフトウェアに対して、アップデートを実施すること。
b. 原則として WSUS サービスを利用すること。
c. WSUS サービスを利用できないアップデートの実施に当たっては、その必要性について当研究所と協議の上、必要と判断されたものについて実施すること。

4.3. 運用支援

4.3.1. 問い合わせ対応

a. 本システムに関する担当職員からの問い合わせに対しては、所定の受付窓口で一元的に受け付けた上で、適切に対応すること。
b. 問い合わせ内容・受付日時・回答内容・対応状況等に関する作業記録を一元的に管理し、情報共有できる仕組みを提供すること。
c. FAQ を提供すること。

4.3.2. システム障害対応

a. システム障害が発生した場合は、原因の特定、解決策の検討、復旧作業の実施等の措置を迅速かつ的確に行うこと。
b. 障害発生時、原則として翌営業日までに対応を開始すること。
c. 緊急な対応を要するシステム障害に対しては、業務時間中の場合は当研究所から連絡を受けてから 3 時間以内を目標に、業務時間外の場合は翌営業日の 12 時までに、具体的な復旧作業を開始すること。
d. 障害が長期化する場合は、理由を示して当研究所と協議の上、対応策を講じること。
e. 年 1 回の計画停電に対応すること。

4.3.3. 担当職員向けマニュアルの作成・提供

a. 本システムの運用に関する担当職員向けマニュアルを作成し、提供すること。
b. 担当職員向けマニュアルには、以下の内容が含まれていること。
①ハードウェアに関するマニュアル
②ソフトウェアに関するマニュアル
③管理作業に関するマニュアル
c. 担当職員向けマニュアルの作成に当たっては、目次や記載項目について、事前に当研究所の合意を得ること。
d. 担当職員向けマニュアルは、随時内容を更新し、常に最新の状態を維持すること。

4.3.4. 利用者向けマニュアルの作成・提供

a. 本システムの運用に関する利用者向けマニュアルを作成し、提供すること。
b. 利用者向けマニュアルには、以下の内容が含まれていること。
①ストレージサービスの利用マニュアル
②メールサービスの利用マニュアル
③グループウェアサービスの利用マニュアル
④有線 LAN・無線 LAN・リモートアクセス環境の利用マニュアル
⑤システム移行に関して利用者側で行う作業の手順書
c. 当研究所による利用者向けマニュアルの二次利用を認めること。

4.4. 運用管理サービスの提供

4.4.1. システム監視サービス

（ア）業務要件

a.「(イ) 機能要件」を満たすシステム監視サービスを提供すること。

（イ）機能要件

a. サーバ装置やネットワーク機器の稼働状況及びリソース状況を一元的に監視する機能を有すること。
b. 稼働状況の死活監視が行えること。
c. 障害を検知した場合は、担当職員にアラート通知できること。
d. リソースの使用状況やパフォーマンスを定期的に測定し、得られたデータを統計情報として管理できること。
e. 管理する統計情報の内容・取得間隔・保存期間については、当研究所と協議の上、決定すること。

4.4.2. ログ管理サービス

（ア）業務要件

a.「(イ) 機能要件」を満たすログ管理サービスを提供すること。

（イ）機能要件

a. サーバ装置やネットワーク機器が出力するログ情報を収集し、一元的に管理する機能を有すること。

b. 以下のログ情報を収集できること。

①統合認証サービスログ

②仮想デスクトップサービスログ

③VPN 接続サービスログ

④内部向け DNS サービスログ

⑤外部向け DNS サービスログ

⑥DHCP サービスログ

⑦RADIUS サービスログ

⑧ゲートウェイセキュリティ対策サービスログ

⑨システム監視サービスログ

⑩バックアップ管理サービスログ

⑪メール送受信ログ

⑫無線 LAN アクセスログ

c. 取得したログは、最低 1 年間保存すること。

4.4.3. バックアップ管理サービス

（ア）業務要件

a.「(イ) 機能要件」を満たすバックアップ管理サービスを提供すること。

（イ）機能要件

a. 本システムが有する情報のバックアップを作成し、保存し、必要に応じて復元を行う機能を有すること。

b. 本システムの全てのサービスについて、クラウドサービスや別途調達する Microsoft 365 A5 を利用する場合を除き、以下のとおりバックアップを作成できること。なお、仮想デスクトップサービスについては、VDI 管理サーバのデータ及び仮想デスクトップのマスタイメージのみをバックアップ対象とする。

①サービスの構成・内容等を変更した場合は、イメージバックアップを作成すること。

②週次で、設定ファイル及びデータファイルのフルバックアップを作成すること。

③日次で、設定ファイル及びデータファイルの差分バックアップを作成すること。

c. 提供する製品の技術的制約等によりイメージバックアップの作成が困難な場合は、当研究所と協議の上、代替手段を講じること。

d. 作成したバックアップは、最低 1 世代分を保存すること。

e. 障害発生時、バックアップを利用して、クラウドサービスや別途調達する Microsoft 365 5 を利用する場合も含め、前日までのシステム環境に復元できること。

5. システム移行要件

5.1. 現行システムからの移行

5.1.1. 基本要件

a. 作業を実施する際は、実施計画書に基づく事前説明を行い、当研究所と協議の上、実施日時や作業手順を決定すること。
b. 当研究所の業務に影響を及ぼす可能性のある作業については、可能な限り業務に支障のない日時に実施すること。
c. システム移行の実施に際して、現行ベンダーとの調整や連携が必要になる場合は、その内容を明確に示した上で、当研究所に協力を依頼すること。
d. システム移行の実施に当たっては、現行システム及び既存データに影響を与えないように十分配慮すること。現行システム及び既存データに影響を与えた場合は、受託者の責において復旧や対処を実施すること。

5.1.2. データ移行

（ア）業務要件

a. 現行ベンダーが抽出した移行対象データについて、本システムにおいて継続利用できる様式で移行すること。
b. 本システムに移行したデータに齟齬や不整合がないことを確認すること。
c. 移行不可能なデータがある場合は、当研究所と協議の上、対応策を講じること。

（イ）移行対象データ

a. 以下の現行システムのサーバ等に保存されているデータを移行対象とすること。

現行システムのサーバ等（移行元）	本システムのサービス等（移行先）	備考
認証サーバ	統合認証サービス	
Active Directory サーバ	統合認証サービス	注意事項 a 参照
ファイルサーバ	ストレージサービス	
内部用 DNS サーバ	内部向け DNS サービス	
公開用 DNS サーバ	外部向け DNS サービス	
DHCP サーバ	DHCP サービス	
UTM 装置	UTM 装置	注意事項 b 参照

b. 各移行対象データにおける最終的な移行範囲及び移行方法については、当研究所と協議の上、決定すること。
c. 現行システムに保存されている以下のデータについては、当研究所が移行作業を実施するものとし、作業上の注意事項等、必要な情報提供を行うこと。
①メーラーに保存されているメールデータ
②メーラーに保存されているメーリングリスト及び各利用者の個人設定（署名・振り分

け設定・転送設定・自動応答等）に関するデータ
③ファイルサーバに保存されている各利用者のメールボックス及びアドレス帳

d. 提供を受けた移行対象データは、関係者以外に漏洩することのないよう厳重に管理すること。また、データ移行以外の目的で使用しないこと。
e. 現行システムのデータ移行に関する情報については、「参考 9 既存システムの移行に関する情報」を参照すること。
f. 現行システムにおいて使用されているソフトウェア等については、現行システムの完成図書を閲覧して確認すること。

（ウ）注意事項

a. Active Directory サーバに保存されているデータの移行作業は、以下の手順で実施すること。
①現行グループポリシーの洗い出しと整理
②当研究所と協議の上、グループポリシーの見直しの実施
③見直したグループポリシーに基づくデータ移行
b. UTM 装置に保存されているデータの移行作業は、以下の手順で実施すること。
①現行ファイアウォールポリシーの洗い出しと整理
②当研究所と協議の上、ファイアウォールポリシーの見直しの実施
③見直したファイアウォールポリシーに基づくデータ移行

5.1.3. システム切替

a. 現行システムから本システムへの切替作業を実施し、業務を引き継ぐこと。
b. 当該作業は、現行ベンダーと協力して実施すること。
c. 当該作業は、現行システムへの切り戻しが可能な方法で実施すること。
d. 当該作業の実施に際して、現行ベンダーとの調整や連携が必要になる場合は、作業内容及び範囲を明確に示した上で、当研究所に協力を依頼すること。

5.1.4. 他システム等との接続

a. 本調達に含まれない以下の他システム等と接続すること。
①人事給与統合システム
②財務会計システム
③特別支援教育研修講座配信システム（免許法認定通信教育システムを含む。）
④図書業務システム
⑤特総研ウェブサイト（構築中）
⑥クライアント端末として利用する PC
⑦プリンタ・複合機等
b. 他システム等との接続は、以下の作業を実施すること。
①内部向け DNS サービスにおけるホスト名・IP アドレスの登録
②DHCP サービスにおけるクライアント設定
c. 既出以外に接続の必要な他システム等が追加される場合は、当研究所と協議の上、別途対応すること。

5.1.5. システム移行に関する技術的支援

a. システム切替前後の一定期間、(独)情報処理推進機構が定める「IT スキル標準（ITSS）レベル 4」相当以上の能力を有する技術者を当研究所に派遣し、システム移行に関する技術的な指導・相談等に対応すること。
b. 当該技術者の派遣期間については、システム切替前後の 1 ヶ月間程度とし、当研究所と協議の上、決定すること。

5.2. 次期システムへの移行

a. 受託者は、担当職員の指示に従い、次期システムへの移行に必要なデータの抽出作業を実施すること。なお、抽出したデータに対する編集・加工等は、次期システム受託者の負担で行うものとする。
b. 受託者は、担当職員の指示に従い、次期システムへの移行に必要な資料を作成し、次期システム受託者に提供すること。

5.3. 契約期間終了後の取扱い

a. 本調達に関する納入物を回収すること。
b. 本調達に関する機器の撤去及び室内の原状復帰を行うこと。
c. 本システムの記録媒体に保存されたデータの消去を行い、データ廃棄証明書を提出すること。
d. 「a.」～「c.」の作業は、要求仕様書「1.3.3. 契約期間」満了後 1 ヶ月以内に完了するように実施すること。

5.4. 契約の延長

a. 当研究所は、要求仕様書「1.3.3. 契約期間」満了日の 3 ヶ月前までに、書面での意思表示をもって、本システムの契約を延長できるものとする。
b. 延長期間は 1 年以内を想定しており、延長料金については別途協議する。
c. 保守・運用支援業務を延長する対象は、製品のメーカーサポート期間等を踏まえ、協議の上決定する。

別紙2　成果物一覧

項番	区分	成果物	納品期日	用途
1	プロジェクト管理	プロジェクト計画書(WBS)	契約締結後、５営業日以内	次期システムの設計、構築、運用等に関するプロジェクトの実施方針、体制、ルール、概要スケジュール、ガントチャート等を含む計画書
2		進捗管理表	契約期間中随時	
3		課題管理表	契約期間中随時	本業務にて発生する課題と対応内容の一覧
4		会議資料	契約期間中随時	各種会議で提出する資料
5		議事録	会議実施後３営業日以内	各種会議の議事録
6	設計・開発実施計画書等の作成	機器の設置作業等による施工計画書	契約締結後、1 か月以内	
7		開発工程表	契約締結後、1 か月以内	
8		開発体制表	契約締結後、1 か月以内	
9	設計	システム概要図	契約締結後、1 週間以内	各サービス・全体構成を図示 物理だけでなく、各サービスの論理構成までも含む。
10		システム設計書	契約締結後、4 か月以内	機能、定義、インタフェース、データベース、モジュール、その他カスタマイズ部分も含む設計に係る事項の記載
11		サービス一覧	契約締結後、4 か月以内	それぞれのサービスを、何の製品/サービスで提供しているかの一覧
12		ハードウェア一覧	契約締結後、4 か月以内	
13		ハードウェア設計書	契約締結後、4 か月以内	主にUTM,ネットワーク認証サービス、L3,L2スイッチ等ネットワーク基盤系サービスを想定している。 仕様、構成、設定、デフォルト値とチューニング後の初期値、その他設計に係る事項の記載を含む
14		ネットワーク設計書	契約締結後、4 か月以内	構成、設定値一覧、パラメータシート、VLAN割り当て、ポート接続状況、その他設計に係る事項を含む）

項番	区分	成果物	納品期日	用途
15		ＩＰアドレス管理表	契約締結後、4 か月以内	NW 機器、サービス類、クライアント端末類の一覧
16		システム移行計画書	契約締結後、4 か月以内	
17		運用マニュアル(暫定版)	開発・テスト工程前	
18	開発・テスト	テスト計画書	全てのテストの実施の10開庁日前	
19		機器設置レイアウト図	契約締結後、2 か月以内	すべてのハードウェアの設置場所が確認できる配置図面 ラックマウント図、端末の設置図を含む
20		ラック搭載図	契約締結後、2 か月以内	主にUTM,ネットワーク認証サービス、L3,L2スイッチ等ネットワーク基盤系サービスを想定している。
21		ラック間配線図	契約締結後、2 か月以内	主にUTM,ネットワーク認証サービス、L3,L2スイッチ等ネットワーク基盤系サービスを想定している。
22		電源系統図	契約締結後、2 か月以内	・ハードウェアのに関する電源構成図を想定している。 ・主にUTM,ネットワーク認証サービス、L3,L2スイッチ等ネットワーク基盤系サービスを想定している。 ・クライアントデバイスまでは、想定していない。
23		アクセスポイント設置場所一覧	プロジェクト計画書に定めた期日	本研究所で所有するマップに対して、今回の導入内容を反映すること
24		各システム及び機器間の接続要件仕様書	プロジェクト計画書に定めた期日	システム外のシステムとの、接続に関する仕様要件を想定している。
25		施工工事写真、施工報告書	プロジェクト計画書に定めた期日	各作業の工程ごとの作業内容が分かる現場写真、施工報告書を想定している。
26	情報システムの本番移行	移行手順書	移行実施1か月前	
27	利用者教育	教育実施計画書	研修の実施の 1 か月前	
28		研修教材	研修の実施の 10 開庁日前	

項番	区分	成果物	納品期日	用途
29	運用・保守準備作業	運用手順書	運用・保守工程開始の1か月前	サービス管理手順、運用スケジュール、メンテナンス手順、バッチ処理手順、他システムとの相互依存、連絡体制図、その他運用上必要な手順等を含む
30		システム運用マニュアル	運用・保守工程開始の2週間前	採用、内部異動、出向、退職の４区分の人事異動別の操作フロー・手順、通常時、イレギュラー対応時、管理機能と操作手順、権限設定方法等含む 計画停電時における、当研究所敷地内に設置されるスイッチのシャットダウン、ブート手順等を含む
31		ネットワーク管理等手順書	運用・保守工程開始の1か月前	
32		利用者向け操作マニュアル	運用・保守工程開始の1か月前	
33		保守体制表	運用・保守工程開始の1か月前	
34		受託者が運用保守する上で使用する ID と当該 ID に付与された権限の一覧	運用・保守工程開始の1か月前	
35		保守作業手順書	運用・保守工程開始の1か月前	運用管理方法、監視装置関連操作方法等含む
36		ソフトウェアのライセンス一覧	運用・保守工程開始の1か月前	主にクライアントで提供されるソフトウェア一覧を想定している。サービス提供に関し、システム管理者向けのソフトウェアツールがあれば、それも含む
37		機器管理番号を含むハードウェア一覧表、構成図等	運用・保守工程開始の1か月前	ハードウェアの一覧を想定している。 設計段階における、ハードウェア一覧に機器管理番号、構成図等、運用に必要な項目を追加した書類を想定している。
38		サービスレベル記述書	運用・保守工程開始の1か月前	対象となるサービスの内容と範囲、サービスレベル指標と水準等
39	障害・情報セキュリティインシデント発生時及び大規模災害等の発災時の対応	障害時の事故管理等手順書	運用・保守工程開始の1か月前	障害時の対応、連絡体制、復旧方法、動作確認方法等含む

項番	区分	成果物	納品期日	用途
40		障害対応報告書	障害発生時及び復旧作業等完了時	
41	契約期間終了後	データ消去証明書	契約期間終了後3週間以内	本契約期間終了後に、運用期間中に提供されたサービス、当研究所に設置した機器のデータ消去が確実に実施されたことを証明する資料
42	その他	その他、システム管理上必要と考えられるものについては、当研究所と別途協議すること。	別途協議	

別紙3　SLA項目一覧

No	カテゴリ	内容	対象サービス/区間	設定SLA値	モニタリング頻度	報告サイクル	計測方法
1	サービス稼動時間	研究所内のサービスが提供される時間帯	システム運用管理に関するサービス	24時間365日	－	－	－
2	運用・保守サービス時間	障害対応業務が提供される時間帯	システム運用管理に関するサービス	平日09:00～17:00 土曜日、日曜日、国民の祝日及び閉庁日：対応しない	－	－	－
3	緊急時対応時間	担当職員が「緊急」と判断する事態の発生時に、しかるべき担当者間で連絡・対応が可能な時間帯	システム運用管理に関するサービス	24時間365日	－	－	－
4	サービスレベル報告	SLA項目における達成状況の報告頻度	システム運用管理に関するサービス	３ヶ月に１回	－	３ヶ月に１回	・　定例会議の開催により実施 ・　報告時には、報告内容を裏付ける資料の添付を必須とする。 ・　SLAが遵守できない場合の原因分析及び改善策の提示を必須とする。
5	障害対応	障害復旧開始時間	システム運用管理に関するサービス	障害発生連絡から翌営業日以内(平日9:00～17:00)	－	－	－
6	緊急を要する障害対応	障害復旧開始時間	システム運用管理に関するサービス	障害発生連絡から3時間以内(平日9:00～17:00)	－	－	業務時間外にあっては、翌営業日の正午までに開始とする。
7	マルウェア対策	通常時：セキュリティパッチ配布から適用までの時間	セキュリティ基盤サービス	DMZ領域のサーバは月１回、それ以外のサーバは年１回以上とし、適用頻度は受注業者と協議の上、決定する。	－	－	－
8	マルウェア対策	緊急時：セキュリティパッチ配布から適用までの時間	セキュリティ基盤サービス	翌営業日以内(平日9:00～17:00) 緊急に適用すると当研究所が判断した場合	－	－	－