別添１

製品評価技術基盤機構共通基盤情報システム
設計構築・運用管理業務
調達仕様書

独立行政法人製品評価技術基盤機構

令和5年10月

令和6年7月（変更）

令和6年11月（変更）

目　　次

セキュリティ確保等の理由から、一部の仕様については参考資料として用意しており、入札に参加する者は参照すること。貸与の申込方法は独立行政法人製品評価技術基盤機構のホームページに掲載する。

Ⅰ. 調達件名

「製品評価技術基盤機構共通基盤情報システム設計構築・運用管理業務 一式」

Ⅱ. 調達の経緯と目的

1. はじめに

本調達仕様書（以下「本仕様書」という。）は、独立行政法人製品評価技術基盤機構（以下「機構」という。）が機構の業務の基盤となる情報システムとして、令和6年度に構築を計画している製品評価技術基盤機構共通基盤情報システム（以下「NITE-LANシステム」という。）に必要な機能（システムの構築サービスの提供、運用、保守等）について、これを受注する意思を有する者からの機能証明書及び提案書の提出を求めるためのものである。

2. NITE-LAN システムの基本構想

機構で現在運用している現行システムの概要及びNITE-LANシステム導入に当たっての方針は次のとおりである。

（1） 現行システム

ア. システムの構成

（ア）機構本所に 47台の物理サーバ（うち、Oracle DB 用物理サーバ 27 台）、本所以外の各拠点に 10 台の物理サーバを設置するとともに、機構本所及び各地方拠点において約 902 台の端末を利用している。
（イ）機構本所と各地方拠点の間を広域イーサネットによる WAN 回線、他省庁との間を政府共通ネットワーク（以下「政府共通 NW」という。）、外部との間をインターネット（SINET）により接続している。

イ. 利用形態

（ア）機構の職員に対して 1 人 1 台の端末（ノート型）を貸与している。
（イ）各職員は、人事異動に伴い所属部署が変更される場合、異動前に用いていた端末を異動先の部署でも利用している。
（ウ）各職員は、端末を利用して、文書処理、機構内部での情報共有、外部との情報交換、情報公開等、日常業務に必要不可欠な機能を活用し業務を遂行している。

ウ. 主要機能

現行システムにおいては、業務遂行上必要となる文書作成・管理、電子メール、情報共有等の機能を提供している。具体的な提供機能については、「参考01. 現行システムの業務機能概要」 を参照すること。

(2) NITE-LANシステム導入に当たっての方針

情報システムは、年々高度化・複雑化の様相を呈しており、企画・導入・開発・保守といった、システムのライフサイクルの全てにおいて必要な工数の増大及び工数単価の上昇傾向がある。さらに、外国為替相場の大幅な変動、半導体不足、不安定な国際情勢といったリスクも高まっている。一方で、機構は行政機関として効率的な業務遂行・組織運営が求められているところ、NITE-LAN システムでは、現行システムの機能やサーバ及びクライアント端末のスペックの見直しを行い必要十分な利便性を有しつつ費用対効果の高い、最適なシステムを構築する。システム導入後は、運用において得られた知見を蓄積及び検証を重ねながら、利便性の向上と、費用対効果の最適化について取り組んでいくものとする。

1 III. 用語の定義

用語	定義
一般業務システム	機構の企画管理部にて所管しているシステム
個別業務システム	機構の各センターにて所管しているシステム
他システム	一般業務システム及び個別業務システム
現行システム	平成31年3月に運用を開始した現在機構で用いている製品評価技術基盤機構共通基盤情報システム
NITE-LANシステム	本仕様書により今般、令和7年4月に導入する製品評価技術基盤機構共通基盤情報システム
次期システム	今般導入するNITE-LANシステムのサービス契約終了後、次期に導入する（令和12年4月予定）製品評価技術基盤機構共通基盤情報システム
大阪事業所	企画管理部（大阪）、国際評価技術本部（大阪市）及び製品安全センター（大阪市）
マルウェア	ウイルス、ワーム等、悪意のあるソフトウェアに加え、スパイウェア、アドウェア等を含めた不正ソフトウェア
SLA	サービスレベルの保証値に関する合意
事務用PC	職員が機構内及び機構外からネットワークに接続して利用するPC
運用管理用PC	職員（NITE-LANシステムの担当職員及び他システムの担当職員）及び他システムの運用保守事業者等が機構内からネットワーク接続してサーバ等を運用管理するためのPC
機構開庁時間	行政機関の休日に関する法律（昭和63年法律第91号）第1条に定める日及び機構が指定する日を除く平日の8時30分から19時まで

2

Ⅳ. 調達形態

本調達は、総合評価落札方式による入札で行い、本仕様書はNITE-LANシステムに必要なサービスとしての機能、運用、保守についての最低限の基準を示すものであり、本仕様書に記載された要求を満たす最適な構成での機能証明書及び提案書の作成、提出が求められる。

また、本調達は、役務請負契約での調達を予定している。

Ⅴ. 調達全般

1. 調達範囲

本調達においては、本仕様書に基づき、各サービスの提供、設計・構築作業、NITE-LANシステムへの各種移行作業、運用管理、保守、導入支援教育及び他システムへの接続支援までを業務範囲とする。

2. 契約期間及びスケジュール概要

(1) 本調達の作業期間：契約日（令和6年3月予定）～令和12年3月31日

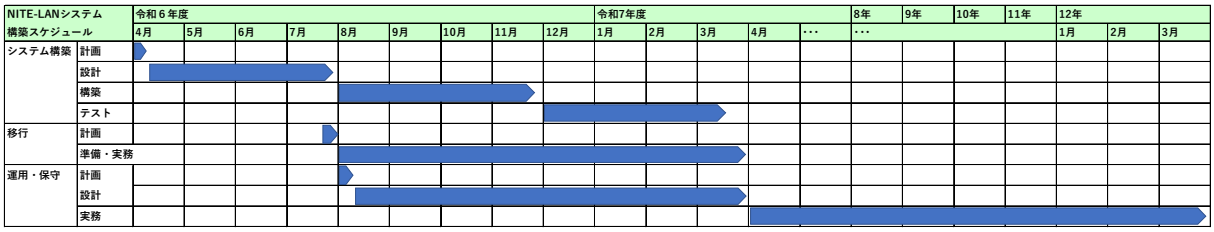
ア. 設計・構築・移行期間：契約日～令和７年３月 31 日

イ. サービス提供期間（有償期間）：令和７年４月１日～令和 12 年３月 31 日

(2) 別途実施する移行作業のためのスケジュール要件

ア. IaaS サービス：令和７年１月６日から利用可能とすること。

IaaSサービスは、令和7年1月5日までに構築・テスト工程を終了し、令和7年1月6日から引渡し工程を実施できるようにすること。また、「12. リモートアクセスサービス」を利用可能なこと。



図表１　作業スケジュール案

(3) その他

半導体不足等、受注者の責によらない理由によってスケジュールに遅延が見込まれ、遅延の理由が妥当である場合（予想が可能なリスクに対してリスク管理が適切に行われていない場合は、遅延の理由が妥当な場合にはあたらない。）には、受注者からの申し出に基づき、契約期間変更等の協議を行うものとする。協議を行う場合は、サービス利用開始時期の4か月以上前に申し出を行うこと。

工期遅延のリスクがある場合には、IaaSサービスを優先して進めることが必要となる（引き渡し時期の大幅な変更は困難なことから、必要に応じて、代替機器の利用等について協議を行う。）。

なお、天災その他の不可抗力により契約の履行が不可能となった場合は、契約書の定めによるものとなる。

3. 本サービスの提供範囲

NITE-LANシステムの提供範囲は、機構の本所及び各地方拠点（以下「地方拠点」という。）である。設置場所詳細については、「参考11. 設置場所一覧」を参照すること。

4. 共通要件

(1) NITE-LANシステムの利用者

令和5年4月1日における現行システムを利用する機構の役職員等（以下「職員」という。）は約820名である。ユーザ数に基づくライセンスが必要な場合には、特に記載がない場合は、835ライセンスを提供すること。

(2) 基本事項

ア. 受注者は、機構の契約に係る競争参加者資格審査事務取扱要領の特例を定める要領又は国の各省各庁における令和 4・5・6 年度競争参加者資格審査により「役務の提供等」の「A」又は「B」の等級に格付けされている者であること。

イ. 政府機関向け独自ドメイン又はグローバル IP アドレスを使用するサービスについては、当該サービスが機構の提供するサービスであることを証明すること。ここでいう証明とは、ドメインについては、機構のドメインでサービスを提供すること、グローバル IP アドレスについては、DNS に機構のクレジットを使用すること等である。また、政府機関向け独自ドメイン又はグローバル IP アドレスの適用範囲は機構の利用する部分に限定すること。

ウ. NITE-LAN システムのネットワークを構成するために必要なルータ、スイッチ、ハブ等機器を提供すること。その種類、台数は、提案によるものとする。
なお、ネットワーク構成については、「参考 02. 次期ネットワーク構成概要図（案）」及び「参考 13. 現行ネットワーク構成図」を参照すること。

エ. いわゆる DMZ に配置されるサービスは、高いセキュリティを必要とするため、最小特権機能を有する OS 又は同等のセキュリティ機能を用い、提供すること。

オ. サービス（利用する製品を含む。）の稼働及び保守については、受注者が最終責任を負うものとし、自社サービス及び自社製品以外の場合もこれを受注者とサービス提供者又は利用する製品の製造者間の契約により担保すること。特に導入したソフトウェアが本調達の契約期間中に提供元によるセキュリティパッチの提供等のサポート期限が終了しないこと。利用しているバージョンのサポートが終了する場合には、受注者の負担によりバージョンアップ等の対応を行うこと。バージョンアップ等に際して現地作業が必要な場合には各拠点を訪問して作業を行うこと。
なお、サービス及び製品等のベンダが提供するガイドライン等を活用した設計、構築及び運用に努めること。

カ. クラウドサービス（SaaS）において使用が可能なライセンスがあるサービスは、全て使用できるようにすること。ただし、国内に設置が必要というセキュリティ要件を満たせな

い等、本仕様書の要件を満たすことができないサービスが存在する場合には、その内容を機構デジタル監情報統括課情報システム基盤・支援室担当職員（以下「担当職員」という。）に報告し承認を得た場合には、使用できるようにすることを要さない。

キ. 機構内に設置する機器のうち、JIS 等の国内規格、ISO 等の国際規格に定めのある製品については、当該規格に準拠していること。

ク. 機構内に設置する機器及び導入するソフトウェアのうち、経済産業省が公開した「IT 製品の調達におけるセキュリティ要件リスト」の最新版の製品について複数の候補があった場合、本仕様書のセキュリティ機能を実現するために必要な製品機能の該当部分を TOE（Target of Evaluation:評価対象）として、ISO/IEC 15408 に基づく IT セキュリティ評価及び認証制度による認証を取得している製品又は CC 承認アレンジメントに基づき、相互承認の対象となる製品を提案すること。

ケ. NITE-LAN システムで提供される全てのサービスに対して、構築工程完了時点以前に公開されている修正プログラムを適用すること。ただし、修正プログラムの適用にあたっては、適用の必要性及び適用の計画について提案し、担当職員と協議の上、実施すること。

コ. 機構内に設置する機器のうち、職員が直接利用する機器（PC 及び複合機）（以下「供用機器」という。）は、製造業者、機種、バージョンを統一する等により操作性を統一すること。

サ. 供用機器について、契約期間中に機種、バージョンを変更する場合には性能を下げないこと。

シ. 機構が指定した様式のラベルを作成し、納品物の機器（PC、AC アダプタ等の PC の付属機器、複合機）に貼付すること。

ス. 提案時において、未だ商品化されていないサービス（機構内に設置する機器を含む。）については、以下の条件を厳守すること。

（ア）未だ商品化されていない部分の存在及びその範囲を明確にすること。
（イ）上記に際し、要件を満たすサービスの開始に間に合うように提供する旨の意思表示を行い、その根拠を十分に説明できる資料を提出すること。
なお、受注者以外が取り扱うサービスについては、その説明資料がサービス事業者から正式に発行した資料であることが明確に確認できること（例えば、社印、事業部長等の印が押印されていること。）。

セ. 受注者は、サービス提供期間中に本仕様書の要件を満たせなくなる場合、対策を講じること。ただし、対策の内容については担当職員と協議の上、決定すること。

ソ. NITE-LAN システムのサービス契約終了後、次期システムへの移行に伴い、担当職員の指示に従い、次期システム構築事業者への支援（業務の引継ぎを含む。）を行うこと。
なお、移行にかかる機器、回線、媒体、移行データの形式変換を含む移行作業は、次期システム構築事業者の負担で行うこととし、移行に伴う NITE-LAN システムへの設定変更作業は本調達の範囲とする。

タ. サービス契約終了後、本調達で機構内に設置した機器は、受注者の責任のもと回収を行うこと。また、機器に登録された情報（本機構固有の情報（業務情報、IP アドレス、ファイアウォールの設定情報等））は完全消去を行うこと。消去したことを証明する書類を提出すること。完全に消去されれば、手法は問わない。暗号化消去も採用可能である。消去ができない場合は、物理的破壊等で読み出し不可とすることでもよい。
なお、ISMAP クラウドサービスリストに掲載されているサービスの場合、サービスの機能を用いて情報を完全消去し、消去したことを証明する書類を受注者が作成し提出することでかまわない。ISMAP クラウドサービスリストに掲載されていない受注者が自

ら提供するサービスの場合は、情報を完全消去するための方法や証跡について、事前に担当職員と協議の上、決定すること。

チ. 受注者は、職員と日本語でコミュニケーションが可能で、かつ、良好な関係が保てること。

ツ. 受注者が提案に際し、機構の保有している情報を必要とする場合は、他の項目に記載する他、担当職員の承認を得て当該情報の提供を受けることができる。

(3) 性能要件

受注者は、採用したパッケージソフトウェアのガイドライン等を活用した設計、構築及び運用に努めること。また、各サービスにおいて、他のサービス（本調達以外のサービスは含まない。）の負荷の影響により性能低下が発生しないこと。

(4) 信頼性要件

ア. 受注者は、稼働率確保のため、システム障害によりサービス停止が予見される機器について、機器の冗長化を図る、又は機器単体の稼働率が高い機器を採用する等、別途定める SLA で求める稼働率を満たすシステムの信頼性を確保すること。

イ. 機構の都合による計画的な停電（以下「計画停電」という。）の場合、計画停電している拠点以外で提供している事務用 PC サービス及び複合機サービスは継続できること。その他のサービスの継続については、担当職員と協議の上、決定する。

(5) 環境要件

ア.「国等による環境物品等の調達の推進等に関する法律」に基づく特定調達品目の OA 機器を機構内に設置する場合には、同法の基準を満たすこと。

イ. 機構内に設置する機器については、国際エネルギースタープログラム適合製品を導入すること。

ウ. ブレードサーバ、仮想化技術等の消費電力の少ない機器、技術を採用し、機構内のサーバルームに設置する機器の総消費電力及び総発熱量の削減に配慮していること。

(6) 運用要件

ア. 受注者は、lnformation Technology lnfrastructure Library v2 又は v3（以下「ITIL」という。）に基づき、運用業務を実施すること。

イ. サービスにて使用する各種システムは、時刻同期が行われていること。

(7) その他要件

「参考20. 機構が現在使用しているソフトウェアライセンス一覧」に機構が現在使用しているソフトウェアのライセンス一覧を示す。また、Microsoft Enterprise Agreement for government organizations等の政府機関を対象としたプログラムがある場合は、これを利用することができる。

5. サービスの開始及び機器の設置等

(1) 前提条件

ア. 受注者は契約後 20 営業日以内にプロジェクト計画書を作成し、承認を得ること。詳細は、「5.(6)プロジェクト管理及び資格要件」に基づき実施すること。

イ. 受注者は、NITE-LAN システムのサービス提供にあたって、全機能提供開始後の運用を十分考慮し、保守及び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。

ウ. 受注者は、現地調査等を行う場合、現行システムの運用に支障を来さないようにすること。

エ. 現行システムに支障を来した場合、受注者の負担で復旧処理等を行うこと。

オ. 現行システムへの設定変更ができるだけ少なくてすむ方法で移行を行うこと。具体的には、クライアントの PC の入換は、認証基盤サービス、認証・検疫ネットワークサービス等の構築、移行後に実施することを想定している。また、電子メールサービスを現行システムとは異なる製品を用いて構築する場合には、現行システムから移行用データを逐次抽出する等の作業負担なく、移行ツールを現行システムにインストール、設定を行い、移行ツールの機能により逐次メールボックスを移動する等の方式を想定している。現行システムへの移行ツールのインストール、設定にあたっては、必要に応じ、十分な記載内容の実施手順書を提供すること。

カ. 候補となる機器等については契約後速やかに機構に機器等リストを提出し、機構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、機構と迅速かつ密接に連携し提案の見直しを図ること。

キ. 本仕様書で要求する全機能を、全機能提供開始日（サービス提供期間の初日）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、代替機能を受注者の負担で提供すること。

ク. 本仕様書において供用機器については、「参考 10. 拠点別導入予定式数」で指定する場所（職員が使用する机上等）に使用可能な状態で設置すること。また、新たな拠点の追加及び拠点の削減による設置機器の移動についても対応できること。
なお、設置機器の移動及び拠点の追加、削除に係る設定変更等に要する費用は、本調達に含まない。

ケ. 機構内に設置することが必要な機器(「参考 05. IaaS 仮想サーバ要件一覧」の用途欄に「オンプレミス環境に配置すること」と記載した仮想サーバが稼働する機器)及び機構内に設置することが望ましい機器(求められる性能を実現するために機構内に設置することが望ましい機器、セキュリティ対策のために機構内に設定することが望ましい機器を含む。)を除く機能は、オンプレミス環境及び ISMAP クラウドサービスリストに掲載されたサービスから、適切な機器の組み合わせを用いて実現すること。ただし、サービスで使用されるサーバ、ストレージ等は日本国内に設置されているものに限定し、日本法を準拠法とし海外の法律の適用が行われないようにすること。

コ. ただし、外部公開用 DNS サービス等の公開情報のみを保持するサービスにおいては、ISMAP クラウドサービスリストに掲載されているサービスに限定することを要さない。日本国内に設置されていることも日本法を準拠法とすることも要さない。

サ. 提案書において、提供予定のサービスが ISMAP の全ての管理基準を満たしていることを受注者が示し、提案書の審査において機構がそれを認めた場合には、ISMAP クラウドサービスリストに掲載されているとみなす。

また、ISMAP クラウドサービスリストに掲載されている IaaS 上で運用されているサービスについても、ISMAP クラウドサービスリストに掲載されているとみなす。

シ. 情報を継続的に保持すること無くデータが通過するのみの機能については、日本国内に設置されていること及び日本法を準拠法とすることを要さない。

ス. 機器の設置等のため、機構執務室に立ち入る場合は、原則として、機構開庁時間とする。ただし、担当職員の許可を得た場合にはそれ以外の時間にも立ち入ることができる。

セ. 機器の設置等にあたり、受注者は、法令等に定められた手続きが必要な場合、官公庁等に対し手続きを行うこと。また、手続完了後に担当職員へ報告すること。

ソ. 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、あらかじ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。また、機構が行うべき作業がある場合には、これを明示すること。

タ. 機器の設置等により、受注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、機構及び第三者に与えた損害に対する費用等は、すべて受注者の負担とする。

チ. 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。

(2) 接続関連

ア. 本所における幹線系のマルチモード光ファイバケーブルに、本調達のネットワーク機器を接続すること（フロア間をつなぐ光ファイバケーブルの張り替えは行わない。）。光ファイバケーブルについても、現地調査が可能である。

イ. 受注者は、以下のケーブルを用意し、「参考 14. 無線アクセスポイント等の情報配線工事」に基づき工事を実施すること。配線方法は、現行方式を踏襲することを基本とし、現行方式については現地調査が可能である。

なお、現行システムから NITE-LAN システムの移行に影響を与えない範囲において、現行システムの LAN ケーブルを利用してもかまわないこととする。

(ア)機構内設置ネットワーク機器間(本所幹線系を除く。)
(イ)機構内設置ネットワーク機器及び広域回線(インターネット接続回線含む。)ポート間
(ウ)アクセスレイヤ用 LAN スイッチ及び無線 LAN アクセスポイント間
(エ)機構内ネットワーク機器及びサーバ類機器間
(オ)アクセスレイヤ用 LAN スイッチ及び複合機間(現在使用しているケーブルに使用できないものがある場合)
(カ)アクセスレイヤ用 LAN スイッチ及び事務用 PC 等機器間((ウ)及び(エ)使用分を除いたポート分)(現在使用しているケーブルに使用できないものがある場合)

ウ. イ.（オ）及び（カ）に基づき敷設する情報配線は、次期システム移行（役務請負契約終了）時には所有権が機構に移転し継続使用できること。

(3) 電源・空調関連

NITE-LANシステムの稼働に必要な機構の建屋内における電源及び空調設備は、機構において整備を行う予定である。本所サーバルームの分電盤からラックまでの配線は受注者において実施すること。

(4) 施設関係

本所サーバルームのフリーアクセスフロアは、縦500mm、横500mmの大きさで、3000Nの床耐荷重と想定し、必要に応じて19型(インチ)ラック内機器の総重量の調整及び床耐荷重を分散させる等の措置を取ること。また、ラックは耐震、免震又は制振に優れた構造とし、震度7又は932Galの加速度を受けても転倒することのないように施工すること。「参考21. サーバルーム概要図」を参照すること。また、設置するラックは天井に設置された空調設備から少量の漏水があった場合でも、システムの運用に影響しない構造(例えば、天井がメッシュ構造ではない等)であること。

なお、設置可能なスペース、耐震・免震の対応状況、電源の形状等の情報は、機構にて閲覧することができる。また、現地調査を可能とする。

設置準備のために機構の施設内に保管場所等の確保が必要な場合は、担当職員と協議すること。

(5) 納品形態

ア. サーバ機器、サーバ及びネットワーク機器用コンソール、ネットワーク機器、バックアップ機器等は、19 型(インチ)ラックに収容すること。また、19 型(インチ)ラックは、必要に応じ耐震、免震又は制震措置を講じること。

イ. 19 型（インチ）ラックは、放熱措置が講じられていること。また、機器等の配置についても放熱対策を考慮し、追加的に放熱対策が必要な場合、受注者の負担で行うこと。

ウ. ラックに収容できない機器については、19 型（インチ）ラック設置スペースと同等な省スペース設計であること。また、個別に耐震、免震又は制震措置を講じること。

エ. 原則として、19 型（インチ）ラック 1 台に収容する機器を、1 台のコンソールで操作できること。また、ディスプレイ、キーボード及びマウスの切り替えに必要な機器を提供すること。

オ. 19 型（インチ）ラック内の機器に第三者が触れることができないように防護措置を行うこと。また、ラックに収容できない機器に第三者がアクセスすることができないように防護措置を取ること。

カ. 納品場所及び設置場所については、担当職員の指示に従い、正常に動作可能な状態に調整して納品すること。

キ. 搬入可能時間等の搬入条件は機構担当者と調整の上、決定すること。

(6) プロジェクト管理及び資格要件

ア. プロジェクト管理

(ア)受注者は、プロジェクト管理の国際標準である PMBOK(Project Management Body of Knowledge)の体系に準じ、WBS(Work Breakdown Structure)をベースとし、必要に応じ EVM(Earned Value Management)等の手法を用いて、NITE-LAN 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。
(イ)受注者は、本仕様書に記載するすべての項目について、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。
(ウ)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。

(エ)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、コミュニケーション計画書、WBS(WBSD を含む。)、進捗管理表、課題管理表、リスク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。
(オ)プロジェクト管理責任者は定期的(週1回を予定)に進捗管理表、課題管理表等を作成、更新し担当職員に提出すること。
(カ)プロジェクト管理責任者は、定期的な進捗会議(週1回を予定)に参加しプロジェクト進捗状況を報告すること。
(キ)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。
(ク)プロジェクト管理責任者は、担当職員又は工程管理支援業者からスケジュール遅延懸念の指摘を受けた場合には、プロジェクト計画の修正を検討すること。
(ケ)プロジェクト管理責任者は、WBS 等の変更が必要な場合には、あらかじめ担当職員の承認を得ること。
(コ)EVM による工程管理を行っている場合には、SPI(Schedule Performance Index)が 0.8 を下回った場合は、必要な改善策を提示し、担当職員の承認を得ること。
なお、担当職員の承認が得られない場合は、担当職員の指示に従い、再度改善策を提示すること。
(サ)プロジェクト管理を適切に行うため、上記による改善策を実施後 1 週間経過しても、プロジェクトの進捗状況が好転しない場合、機構から受注者に対して、プロジェクト管理責任者、要員の交代を求めることができる。詳細は、機構と受注者の協議によるものとする。
(シ)プロジェクト管理責任者は、リスク管理として、プロジェクト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、根本原因、影響度を分析し、リスク対応策をあらかじめ定めること。
(ス)プロジェクト管理責任者は、リスクが顕在化した場合には、事前に定められたリスク対応策に従って、問題解決のために必要な措置をとること。
(セ)プロジェクト管理責任者又はプロジェクト管理担当者は、PMP(Project Management Institute 認定)又はプロジェクトマネージャ(経済産業省認定)の資格を有していることが望ましい(その場合総合評価において加点する。)。

イ. サービス実装に関わる技術者の資格要件

(ア)「10. ネットワークサービス」の設計・実装の担当者又は管理者は、ネットワークスペシャリスト(経済産業省認定、旧制度の試験区分における同様の資格でも可とする。)を有していることが望ましい(その場合総合評価において加点する。)。
(イ)「11. セキュリティ対策」の設計・実装の担当者又は管理者は、情報処理安全確保支援士の試験合格(経済産業省認定、旧制度の試験区分における同様の資格でも可とする。)又は CISSP(International Information Systems Security Certification Consortium 認定)を有していることが望ましい(その場合総合評価において加点する。)。
(ウ)「13.運用管理サービス」の設計の担当者又は管理者は、ITIL Expert の資格を有していることが望ましい(その場合総合評価において加点する。)。

(7) 納品ドキュメント

以下のドキュメントを機構に提出すること。内容について担当職員と協議の上、承認を得ること。また、記載内容に変更があった場合には、修正し提出すること。

ア. 受注者は契約後早い段階で、以下のドキュメントを提出すること。

(ア)「5. (6)プロジェクト管理及び資格要件」に必要となるドキュメント
(イ)システム概要構成図
(ウ)機器構成一覧
(エ)機器諸元表(機構内に設置する機器に限る。)

イ. 受注者は以下のドキュメントを、プロジェクト計画に基づき提出すること。

(ア)ネットワーク構成図
(イ)セキュリティ共通設計書
(ウ)導入試験計画書(試験項目、試験内容、試験体制、試験スケジュール)
(エ)導入計画書(導入手順、導入体制、導入スケジュール)
(オ)移行計画書(移行対象システム、移行対象データ、移行体制、移行スケジュール)
(カ)教育研修計画書(教育対象者、教育対象サービス、教育体制、教育スケジュール)
(キ)他システム向け接続仕様書

ウ. 受注者は NITE-LAN システムの全機能提供開始前に、以下のドキュメントを提出すること。

(ア)システム設計書
(イ)導入試験結果報告書
(ウ)導入結果報告書
(エ)移行結果報告書
(オ)教育結果報告書(システム管理者研修のみ)
(カ)運用マニュアル
(キ)操作マニュアル
(ク)研修用テキスト

エ. 受注者は NITE-LAN システムの全機能提供開始後運用中に、以下のドキュメントを適宜提出すること。
なお、現行システムで提出されているドキュメントを機構本所にて閲覧することができる。

(ア)月次定期報告書(SLA 報告、運用報告、インシデント報告、情報セキュリティ報告書等)
(イ)年間保守スケジュール
(ウ)作業報告書(都度作業が発生した際の作業報告書)
(エ)各種ソフトウェアライセンス情報(有効期限等)

6. 教育研修

(1) 教育研修作業

ア. システムの円滑な導入・稼働に向けて、機構との協議に基づく教育研修計画を提案し、機構の承認を得た上で、教育研修計画を策定すること。

イ. 教育研修計画には、教育研修体制と役割、詳細な作業及びスケジュール、教育研修環境、教育研修方法等に関する内容を含めること。

ウ. 教育研修計画に基づき、ユーザ向け操作マニュアル、システム運用担当者向け運用手順書等を整備し、職員等に対して十分な教育訓練を実施すること。

(2) 操作マニュアル・研修用テキスト

ア. 機構から編集可能な形式で提供する現行システムの操作マニュアル及び研修用テキストに対して、必要に応じて更新を行い、NITE-LAN システムの操作マニュアル及び研修用テキストを提供すること。

イ. 研修用テキストには、NITE-LAN システムを利用し始めるために必要な情報が含まれていること。

ウ. 操作マニュアル、研修用テキストは、日本語で記述されていること。

エ. 操作マニュアルは、画面のスナップショット等を含み、理解しやすいものであること。

オ. NITE-LAN システムのユーザが利用するすべてのハードウェア及びソフトウェアの操作マニュアルをオンラインマニュアルで提供すること。

カ. 著作権上許されている場合には、操作マニュアルを電子的に事務用 PC から閲覧可能とすること。

キ. 電子媒体の研修用テキストは、編集可能な形式及び PDF 形式の両形式で提供すること。

ク. 研修用テキストを事務用 PC から閲覧可能とすること。

ケ. 研修用テキストには、機構の内部利用のための複製を制限することになる第三者が著作権を有する著作物を原則含めないこと。

(3) 役職員向け研修

ア. 当該研修は全役職員に対し e ラーニング形式で実施するため、イ、ウ及びエの内容を満たす研修動画コンテンツを提供すること。

イ. 研修は、おおむね 2 時間とすること。

ウ. 事務用 PC に導入されるソフトウェアの操作方法（複合機等の操作方法も含む。）が現在機構で用いているソフトウェアの操作方法と大幅に変わる場合には、操作方法の主要な変更点を研修内容に含めること。

エ. 研修内容にパスワードの変更、ファイルの暗号化等の情報セキュリティに関する内容を含めること。

(4) システム管理者研修

ア. 最大 10 名の機構の本所のシステム運用担当者に対して、システム運用上必要となる設定方法及び操作方法の管理者研修を、システムの運用開始以前に行うこと。受注者が構築した NITE-LAN システムを用いて受注者が準備した NITE-LAN システムの事務用 PC により研修を行うこと。方式は、Web 会議による方式でも集合研修でもかまわない。ただし、集合研修の場合も（Web 会議の場合にも）研修を録画し後日視聴可能とすること。

イ. 管理者研修の内容については、担当職員と協議の上、決めること。

ウ. 本所以外の地方拠点にサーバを設置する等、地方拠点の職員による運用作業が必要な場合には、その作業のための研修用テキストを作成し、各々の地方拠点において、最大 3 名の職員に対して研修を実施すること（可能な場合には Web 会議を用いることもできる。）。

7. 移行

(1) 移行全般

ア. 基本要件

(ア)実施計画に基づき、機構との協議に基づく移行計画を提案し、機構デジタル監情報統括課情報システム基盤・支援室長の承認を得た上で、移行計画を策定すること。
(イ)移行計画には、移行実施体制と役割、詳細な作業及びスケジュール、移行環境、移行方法、移行ツール等に関する内容を含めること。
(ウ)移行作業には、移行リハーサルを含めること。
(エ)機器設置及び移行に関する協議の内容は受注者の責任において打合要旨に整理し、内容について担当職員の承認を得ること。
(オ)移行計画に基づき、移行手順書を作成し、機構デジタル監情報統括課情報システム基盤・支援室長の承認を得ること。
(カ)移行計画及び移行手順書に基づき、機器の設置及びシステム移行を行うこと。
(キ)移行計画及び移行手順書に基づき、既存機器(ハブ等)の移動作業を行うこと。
(ク)NITE-LAN システムへの移行に際して現行システムとの並行運用期間を設ける場合、現行システムに反映された人事異動情報を NITE-LAN システムに取り込む仕組みを実装する等、データの整合性を確保する策を講じること。

イ. 役割分担

(ア)データ移行については、可能な限り担当職員に負荷を与えることなく、NITE-LAN システムで動作するように作業を実施すること。
(イ)移行期間中も通常の業務遂行中につき、現行システムが稼働中であるため、職員の業務遂行に影響を与えることなく移行作業が可能な手段、手順等がある場合には、そうした手段、手順等を採用すること。

ウ. 担当職員及び IaaS サービスを利用するシステムの担当者との調整

(ア)IaaS 上で稼働する個別業務システム及び一般業務システムのアプリケーションに関しては、受注者の役務は共通的なミドルウェアの提供までであり、アプリケーションに固有なミドルウェア及びアプリケーションプログラム並びにデータの移行は受注者の役務に含まれない。ただし、機構が別途実施する IaaS サービスへの各個別業務システム及び各一般業務システムの移行に際しては、各個別業務システム及び各一般業務システムの担当部署の担当者と十分な調整を行うこと。
なお、調整内容としてはスケジュール調整、移行に際して必要となる NITE-LAN システム側の設計及び設定変更並びに各個別業務システム及び各一般業務システム側におけるコンフィグ再設計支援等が考えられる。受注者は、円滑に移行が完了するよう移行専任体制を構築する等して、各個別業務システム及び一般業務システム側の要求に柔軟に対応すること。
(イ)各個別業務システム及び各一般業務システムの担当部署の担当者及び移行事業者向けの IaaS の機能及び移行スケジュール、移行マイルストーンに関する説明会を開催すること。
(ウ)監視サービス、バックアップ・リストアサービス等の NITE-LAN システムが提供するサービスの仕様書(他システム向け接続仕様書)を作成し各個別業務システム及び各一般業務システムの担当部署の担当者に提供すること。
(エ)各個別業務システム及び各一般業務システムの担当部署の担当者及び移行事業者との QA 用の様式を提供し、QA 対応を行うこと。
(オ)上記に記載の各個別業務システム及び各一般業務システムとの調整に係る要件については、その実施予定時期をプロジェクト計画書に記載すること。
(カ)リバースプロキシ、監視、ジョブ等の設定、IaaS サービスにおける仮想サーバの構成等は、現行を引き継ぎつつ、変更の必要性をヒアリングシート等により個別業務システム及び一般

業務システムの担当者に受注者が主体的に確認し設計、設定を行うこと。新規の個別業務システム及び一般業務システムにおいては、ヒアリングシート等により必要な設定を把握し設計、設定を行うこと。

エ. 設置・移行時の留意点

(ア)構築作業に起因して現行システムに障害が発生した場合、受注者の負担で復旧させること(復旧に際して同一物品を用意できない場合には、代替機能の提供でも良い。)。
(イ)設置及び施工作業において機構の執務室(サーバルームは含まない。)に立ち入る場合は、原則、機構開庁時間であること(ただし、担当職員との協議により、それ以外の時間の立ち入りが承認された場合はその限りではない。)。
(ウ)勤務時間中に執務室に立ち入る場合は、事務用 PC1 台の設置にかかる時間として 20 分を目安とし、その他の機器 1 台の設置にかかる時間を原則 1 時間以内とすること。
(エ)事務用 PC の移行にあたりユーザが実施する作業がある場合には、その作業内容について担当職員と協議の上決定し、ユーザ向け移行作業マニュアルの内容に含めること。

オ. その他

(ア)移行期間中のみ用いる機器については、受注者において用意すること。
(イ)移行作業終了後、移行期間中のみ用いる機器の撤去を行うこと。撤去に際しては、機器に記録されたデータ等の情報を復元できない方法で消去すること。消去したことを証明する書類を提出すること。完全に消去されれば、手法は問わない。暗号化消去も採用可能である。消去ができない場合は、物理的破壊等で読み出し不可とすることでもよい。
(ウ)IaaS サービスを用いるアプリケーション等の移行のための移行事業者の作業用端末 5 台を令和 7 年 1 月 6 日から令和 7 年 3 月 31 日まで貸与すること。その際には、アクセスできる先を最低限に限定する(事業者により異なるサーバに限定する)等、セキュリティに留意すること。
(エ)IaaS サービスを用いるアプリケーション等の移行は令和 7 年 1 月 6 日から令和7年 3 月 31 日で実施する。当該移行期間において、円滑に移行が完了するよう移行専任体制の構築等を行い、各個別業務システム及び一般業務システム側の要求に柔軟に対応すること。
(オ)機構職員が移行期間中にテスト等を実施するにあたり、IaaS サービスを用いるアプリケーションにアクセスする方法を 50 人分用意すること。
なお、職員の業務に支障がでない方法を採用すること。(例えば、新端末を用意することで、既存業務は既存端末、IaaS サービス上のアプリケーションへのアクセスは新端末で実施する等の方法を採用すること。既存端末上の仮想 OS から IaaS サービス上のアプリケーションにアクセスする方法でもよい。)

(2) 移行の対象

ア. 基本要件

(ア)現行システムから NITE-LAN システムにデータを移動し、NITE-LAN システムで使用できる状態にすること。
(イ)移行に際し、現行システム側で行う設定作業等は、現行システムの運用保守業者との契約変更等により、機構にて実施する。移行のために必要なデータの現行システムからの抽出作業も同様に機構にて実施する。
(ウ)現行システムで用いている Microsoft 365 については、商流変更による移行も可能である。
(エ)データ移行にあたっては、情報漏えいの防止に配慮して作業を行うこと。

（オ）現行システムからNITE-LANシステムへ切り替える際においても、機構外からのメールの受信は行える（機構職員が閲覧できなくてもよい。）ものとし、不達にならないこと。
（カ）現行システムからNITE-LANシステムへ切り替える際においても、機構のホームページが閲覧できるよう必要な措置を講じること。

イ. 移行対象の分類

（ア）移行データA（受注者が移行を行うデータ）

現行システムで使用している以下のデータをNITE-LANシステムの同種のサービスで継続して利用できるよう移行すること（アクセス権の設定等、利用にあたって必要な情報を移行することを含む。）。また、移行後に各サービスが動作すること及び移行したデータに齟齬がないことを確認すること。データ容量については、「参考03. 移行対象データ概要」を参照すること。

①Microsoft 365 Exchange onlineメールデータ
②Microsoft 365 Exchange onlineスケジュールデータ
③ディレクトリ情報（認証情報、名簿情報、ポリシー情報）
④ファイルサーバデータ（フォルダ構成、アクセス権限等含む。）
⑤Microsoft 365 SharePoint onlineのデータ（機構のイントラネットとしてのページのみではなく、個人作成のページ、ファイル及びアクセス権限を含む。）
⑥Microsoft 365 OneDriveのファイル
⑦Microsoft 365 Teamsのデータ
⑧Microsoft 365 Power Automateのデータ
⑨メール共有サービス（メールワイズ）のメールデータ及び設定情報

職員が作業を行う必要がある場合には、事前に対象のデータ及び作業範囲を明らかにし、担当職員の承認を得ること。また、職員が容易に当該作業を行うために必要なツール（バッチファイル、スクリプト等）、機器及び作業マニュアルを提供すること。

なお、Microsoft 365を採用する場合は、商流変更を原則とすること。

（イ）移行データB（職員が移行を行うデータ）

職員が、現行システムで使用している端末内の以下のデータ及びその他のデータについて、NITE-LANシステムの同種のサービスで利用できるよう、移行に必要なツール（バッチファイル、スクリプト等）、機器及び作業マニュアルを提供すること。

①文書ファイル
②辞書（ATOK Pro 2並びにマイクロソフト社の辞書（OS及びOfficeのもの））
③ブックマーク（Mozilla Firefox及びMicrosoft Edgeのもの）

(ウ)移行データＣ(課室所管のシステムが保持するデータ)

各個別業務システム及び各一般業務システムについては、基本的に移行作業は受注者の役務には含まれない。詳細は、「参考04. 課室所管情報システムの移行に係る要件」に従って対応すること。NITE-LANシステムのサービス提供開始までに各個別業務システム及び各一般業務システムの移行を行う必要があることから、課室所管の各システムの稼働環境となるIaaS環境への移行作業が令和7年1月6日から可能となるようにすること。

8. 業務サービス

(1) 認証基盤サービス（ディレクトリ含む。）

NITE-LANシステムに必要な認証サービス機能、ディレクトリサービス機能を提供すること。

ア. 基本要件

(ア)利用者数、同時接続数、対象となるログインアカウント数は「4. (1)NITE-LAN システムの利用者」のとおりである。ただし、個別業務システム及び各一般業務システムの移行事業者、運用保守事業者が運用管理用 PC を利用する際や、「12.リモートアクセスサービス」を利用する際の認証も認証基盤サービスを利用する予定であり、このために必要がある場合には 100 名分の追加のライセンスを提供すること。
(イ)「人事・給与システム」からエクスポートされた CSV、LDAP 等の情報を NITE-LAN システム内の各サービスに随時反映できること。
(ウ)利用者データ、組織データ、グループデータの 3 種類のデータをインポートできること。
(エ)利用者データには以下の項目がインポートできること。詳細については担当職員と打合せし、了解を得ること。Web ブラウザに表示できない旧字体、メールの文書に含められない旧字体等は、メール及び Web ブラウザで利用可能な文字に置換してインポートできること。また、所属は 5 組織程度までの併任があり、対応できること。
①ユーザID
②パスワード
③職員番号
④漢字姓、漢字名、かな姓、かな名、ローマ字姓、ローマ字名
⑤組織コード、組織名称(部・センター名、課名、室名)
⑥利用者種別、役職コード、役職
⑦メールアドレス
⑧携帯電話番号、外線電話番号、内線電話番号、FAX番号
⑨利用開始年月日、利用停止年月日、生体認証開始年月日、生体認証停止年月日
(オ)組織データには以下の項目がインポートできること。詳細については担当職員と打合せし、了解を得ること。
①組織コード
②組織名称(部・センター名、課名、室名)
③利用開始年月日、利用停止年月日、生体認証開始年月日、生体認証停止年月日
(カ)グループデータには以下の項目がインポートできること。詳細については担当職員と打合せし、了解を得ること。

①グループID
②グループ名
③グループメンバのユーザID

イ．機能要件

（ア）ディレクトリサービス機能
①ディレクトリ内情報は利用者自身が事務用PCから入力及び変更できないこと。
②グループは、多層化できること。
③大量のアカウントの一括登録及び変更のための機能を備えたものであること。ただし、アカウントの一括登録及び変更時にインポートするデータは新規追加及び変更分のみとし、全レコードを毎回インポートするような方式は採用しないこと。
④複数のディレクトリサーバが導入されている場合、ユーザ情報が自動連携される仕組みとなっていること。又は、各サーバの内容が一致していることを検証するシステム機能を有していること。
⑤ユーザIDの発行、削除やグループへのアサイン等を行う際、決裁機能等により申請者と承認者の2名以上が関わることで実行が可能となる仕組みを有することが望ましい（その場合総合評価において加点する。）。
⑥大量のユーザIDの発行、削除やグループへのアサイン等を行う際、変更内容を一覧表示できるとともに、決裁機能等により承認者が一括承認できることが望ましい（その場合総合評価において加点する。）。
⑦アカウントの登録、変更、削除等をあらかじめ登録しておき、指定した日時に登録した処理が実行される予約機能を有していること。
⑧上記に加えて、アカウントの所属等の変更を複数個予約登録する機能を有すること。
⑨異動履歴を確認できる機能を有すること。
⑩組織変更に伴う課室の増減や名称変更を行う機能を有することが望ましい（その場合総合評価において加点する。）。
⑪グループの新規作成や、アカウントのアサインの権限について委譲が可能なものであること。
⑫あらかじめ定めたルール（職務分掌上のリスク等）に従い、アカウントのグループへのアサイン状況を確認し、ルールに反する状況をチェック・分析する機能を有していることが望ましい（その場合総合評価において加点する。）。
⑬データをCSV形式でインポート・エクスポートする機能を提供すること。また、データのインポートについては、データの新規追加及び変更時に、全レコードを毎回読み込むような方式ではなく、変更したいデータのみをインポートする機能を提供すること。

（イ）認証基盤機能
①生体認証情報（指紋認証データ、顔認証データ等）によって、事務用PCにおけるOSへのログイン認証が行えるものであること。顔認証にて生体認証を実施する場合には、静止画像（写真等）で認証できないよう、技術的な処置を講ずること。ただし、まばたき及び顔の向きを変える等の所作をユーザに命令して認証する方式等のユーザ利便性を低下させる技術的な処置は採用しないこと。
②乾燥肌の者等、生体認証が困難な場合に対応するため、パスワード等の主体認証にも対応していること。
③ISO/IEC18092標準のICカード又は生体認証情報（指紋認証データ、顔認証データ等）によって、複合機における利用者認証が行えるものであること。

④「8. (5)ファイルサーバサービス」のアクセスコントロールに用いる認証サービスを提供するものであること。また、そのアクセスコントロールには「8.(1)ア.基本要件(エ)利用者データ及び(カ)グループデータ」を利用可能であること。
⑤一定回数認証失敗時又はシステム運用担当者の操作に基づき、アカウントロックを行うことができること。一定回数認証失敗時におけるアカウントロックにおいては、システム運用担当者に警告メッセージを通知できること。また、システム運用担当者の操作に基づいてアカウントロック解除を行うことができること。
⑥主体認証情報(ICカード内に保持されている主体認証情報は除く。)忘れへの運用負荷低減に寄与する仕組み(ユーザによるセルフサービス等)を有すること。
⑦ユーザが直接主体認証情報を変更できる機能を有すること。
⑧主体認証情報は、システム管理者にも把握不可能な形態で保持されるものであること。
⑨主体認証情報に関する制限(パスワードポリシー)を設定できるものであること。

⑩管理者により認証結果と認証失敗時の理由の識別ができる機能を有していることが望ましい(その場合総合評価において加点する。)。
⑪ロックされているアカウント、長期間利用されていないアカウント等を抽出するセキュリティリスク分析機能を有していることが望ましい(その場合総合評価において加点する。)。
⑫アクセス権限と認証登録の権限レベルは、多層化できること。
⑬ICカードの携帯忘れへの対応機能を有していること。
⑭ユーザが怪我等により生体認証情報が使用できなくなった場合への対応機能を有していること。
⑮ユーザが怪我等により生体認証情報が使用できなくなった場合への対応機能がパスワード発行の場合、そのパスワードに対し利用可能期間、失敗可能回数を設定できること。また、設定した利用期間において、パスワードによる認証方式は該当利用ユーザのみ実施可能で、他のユーザは生体認証方式のみで認証できることが望ましい(その場合総合評価において加点する。)。
⑯生体認証は、外気温など周囲の環境に依存しにくい認証方式であることが望ましい(その場合総合評価において加点する。)。
⑰生体認証登録及び認証時画面において、センサーが撮影している生体情報を目視でき、位置ズレ等を確認できるようになっていることが望ましい(その場合総合評価において加点する。)。
⑱ユーザが都度IDを入力する必要がなくなるような機能の有効・無効が設定できることが望ましい(その場合総合評価において加点する。)。

(ウ)データ連携機能
①他システムからデータを受け取り、ディレクトリサービスに登録されている内容を更新するための汎用的な機能を有していること。
②Webサービスインターフェース等、リアルタイムでのデータ連携のための機能を有していることが望ましい(その場合総合評価において加点する。)。
③連携先のシステムで用いているデータ(人事・給与システムにおける併任情報等)とディレクトリサービスで用いているデータとをマッピングし、変換する機能を有していることが望ましい(その場合総合評価において加点する。)。
④ディレクトリサービスが保持している情報をCSV形式にて書き出す機能を有していること。

⑤他システムとのデータ連携のために、FTP、NFS、CIFSのいずれによってでも利用することができるファイル共有環境を有していること。

(エ)NTP サーバ機能

①NTPプロトコルによる、時刻提供機能を有していること。

ウ. セキュリティ要件

(ア)認証情報を通信する場合には、その内容の暗号化を行うこと。
(イ)アカウント登録、削除等のアクセスコントロールが行えること。
(ウ)アカウント登録、削除等のログが改変不可能な方式で保持できるものであること。又はログファイルへのアクセスコントロールの設定等によりログの改変を防止できるものであること。
(エ)ログの改ざんが厳密に検出できる機能を有することが望ましい(その場合総合評価において加点する。)。
(オ)ログを CSV 等の形式で出力できること。
(カ)ログを整形された形式の整ったレポートとして出力できることが望ましい(その場合総合評価において加点する。)。
(キ)ログの管理は「13.運用管理サービス(1)基本要件及びサービスの改善 ア.基本要件」の仕様を満たすこと。

(2) グループウェアサービス（イントラ含む。）

職員が効率的に情報共有するためのWebアプリケーション機能(ページ作成、Webファイル共有、電子会議室、スケジュール管理、施設予約、メーリングリスト等) を提供すること。

ア. 基本要件

(ア)利用者数、対象となるログインアカウント数は「4. (1)NITE-LAN システムの利用者」のとおりである。
(イ)複数の製品でサービスを提供する場合には、製品間の連携がとれていること。具体的には、認証情報やアクセス権限情報等が連携されること。
(ウ)グループウェアサービスは、クライアントとして、主に Web ブラウザを用いた Web アプリケーションとして提供すること。

イ. 機能要件

(ア)全般機能要件

①Webブラウザ等を用いて、(イ)～(セ)の各機能を提供すること。
②(イ)～(セ)の各機能において新着や更新がある場合、利用者が新着や更新を認識できることが望ましい(その場合総合評価において加点する。)。
③利用者が表示させるコンテンツを変更できる等、カスタマイズできること。ただし、システム管理者が設定した必須のコンテンツについて初期画面からの削除を禁止すること。

(イ)機構内共有アドレス帳機能

機構内共有アドレス帳として、以下の機能を提供すること。

①職員の氏名(漢字及び振り仮名)、連絡先(内線番号等)、属する組織名(部・センター、課、室の3階層以上)、役職名、メールアドレスに相当する情報を職員データとして登録できること。
なお、1職員に対して、複数組織(3組織以上)の兼務を設定できること。

②職員データの項目は、必要に応じて追加が可能であること。
③登録されたデータを、氏名、組織情報順に表示できること。
④登録されたデータを任意の文字列で検索ができること。
⑤機構内共有アドレス帳は、「8.（1）認証基盤サービス（ディレクトリ含む。）」のディレクトリサービス機能を用いたものであることが望ましい（その場合総合評価において加点する。）。ディレクトリ基盤を直接用いることができない場合には、ディレクトリ基盤から出力されたCSV等のファイルを用いてその内容が更新されること（運用作業として更新作業を行ってもよい。）。
⑥複数の連絡先（携帯電話番号と固定内線番号等）を登録できること。

（ウ）Web ファイル共有機能

①Webブラウザからファイルのアップロード、ダウンロードが可能なWebファイル共有機能を有すること。
②機構職員以外の者に対してWebファイル共有機能が利用できること。

③Webファイル共有機能は、ユーザ単位でのアクセスコントロール機能を有していること。アクセス権の追加削除が、職員自身によって容易に可能なこと。
④アップロードされたファイル等へアクセスするURL（以下本節において「共有リンク」という。）を発行し、URLを共有したい者へ知らせることで、ファイル等を共有（以下本節において「共有」という。）できること。
⑤機構職員に対し送信するメールに、共有リンクが含まれていて、送信先のユーザに当該ファイル等のアクセス権限がない場合、利用者に対してその旨を警告できることが望ましい（その場合総合評価において加点する。）。
⑥Webファイル共有機能は、自動で履歴管理が行われ、ファイルを更新した場合、古いファイルも残っており、その古いファイルが利用可能なこと。
⑦Webファイル共有機能は、表計算機能、ワープロ機能、プレゼンテーション機能から直接利用できることが望ましい（その場合総合評価において加点する。）。
⑧Webファイル共有機能のアクセス権設定機能は、電子メール機能と連動しており、Webファイル共有機能に保存したファイルのリンクを記載した電子メールを送信した場合、宛先の職員に自動で当該ファイルへのアクセス権が付与できることが望ましい（その場合総合評価において加点する。）。
⑨NITE-LANユーザで共用するデータ領域を、12TB以上提供すること。また、この他に個人のデータ領域としてNITE-LANユーザ全員に1人当たり2TB以上提供すること。
⑩全文検索機能を有すること。全文検索機能は、Microsoft Office Wordのdoc及びdocx形式、Microsoft Office Excelのxls及びxlsx形式、Microsoft Office PowerPointのppt及びpptx形式、PDFファル並びにテキストファイルに対応していること。
⑪検索結果は、ファイルの登録日順又は更新日順に表示できること。
⑫検索結果は、ファイルの登録日順及び更新日順の両方において表示できることが望ましい（その場合総合評価において加点する。）。
⑬複数のファイルを一度にアップロードできることが望ましい（その場合総合評価において加点する。）。
⑭サブフォルダ内のファイルを含めて、フォルダ単位で移動できることが望ましい（その場合総合評価において加点する。）。

（エ）イントラページ作成機能

①イントラページ作成機能は、利用者がWebサイトにページの登録、参照、変更及び削除が行えること。

②機構全体のイントラページを作成及び削除できる機構全体イントラスペース管理者並びに部門用のイントラページを作成及び削除できる部門用イントラスペース管理者の設定機能を提供すること。

③機構全体及び部門用イントラスペース管理者の設定により作成可能となるイントラページに加え、職員全員がパーソナルなページを任意のページ数作成できること。メールに代替する複数の職員間のコミュニケーション手段として利用する当該ページにおいては、作成者が閲覧権限等の権限設定が可能なこと。

④機構全体及び部門用イントラスペース管理者は、個人、組織等に基づき、管理するイントラスペースの閲覧、投稿、編集、削除等の権限設定が可能なこと。

⑤作成ページには、ファイルや表、画像、文書等へのリンクを添付することができ、添付されたファイルを開く際は、拡張子に関連付けられたアプリケーションが自動的に起動できること。

⑥イントラページ作成機能で作成したページは、Webファイル共有機能で共有したファイルの説明等を記載する目的で利用できること。

⑦イントラページ作成機能は、ページ一覧画面より、作成者別や登録日付別などでページを分類できることが望ましい（その場合総合評価において加点する。）。

⑧イントラページ作成機能でページが作成、更新された場合には、閲覧権限を有する者へ投稿、更新があったことが通知されること。

⑨掲示不適切な内容のページが掲示された場合のために、システム管理者又は機構全体・部門用イントラスペース管理者が該当ページを削除できること。

⑩非テキストコンテンツには、代替テキストを付与できること。

⑪読み上げ順序の設定ができること。

⑫キーボードで操作が可能なページを作成できること。

⑬フォーカスの順序の設定が可能なこと。

⑭JIS X 8341-3:2016「高齢者・障害者等配慮設計指針－情報通信における機器、ソフトウェア及びサービス－ 第3部:ウェブコンテンツ」における達成基準AA準拠のページを作成できること。

⑮事務用PCで閲覧可能な動画を掲載したページを作成できること。

（オ）電子会議室機能

①電子会議室を作成、削除できる電子会議室管理者の設定機能を提供すること。

②電子会議室管理者は、個人、組織等に基づき、管理する電子会議室の閲覧、投稿、編集、削除等の権限設定が可能なこと。

③電子会議室管理者を設定する電子会議室に加え、職員全員がパーソナルな電子会議室を作成できること。当該パーソナル電子会議室においては、作成者が閲覧権限等の権限設定が可能なこと（当該電子会議室は、メールを代替するグループコミュニケーション手段として活用する予定である。）。

④電子会議室への投稿の際に、ファイルや表、画像、文書等へのリンクを添付することができ、添付されたファイルを開く際は、拡張子に関連付けられたアプリケーションが自動的に起動できること。

⑤電子会議室機能は、特定のテーマに関する一連の投稿を階層的に表示する等、スレッドとしてまとめることでわかりやすく表示できること。

⑥電子会議室に投稿があった場合には、登録された利用者に通知できることが望ましい（その場合総合評価において加点する。）。

（カ）スケジュール管理機能

①利用者が、自らのスケジュールの閲覧、登録、編集、削除ができること。また、スケジュール表内に案件の件名が表示できること。スケジュール管理項目として、件名、対象日、開始時間、終了時間、場所、詳細説明及び他の利用者へのスケジュールへの参加依頼が含まれていること。

②利用者が、他の利用者、組織等に対し、自らのスケジュールの閲覧、登録、編集、削除等の権限設定が可能なこと。

③スケジュールは、公開用と非公開用（自分用）の2種類を設定できることが望ましい（その場合総合評価において加点する。）。

④スケジュールは、公開用の件名と非公開用（自分用）の件名の2種類を設定できることが望ましい（その場合総合評価において加点する。）。

⑤他の利用者、組織等に対し、スケジュールの有無のみを表示し、スケジュールの内容を、非表示にできること。自らの所属する課室に所属する者はスケジュールの内容を表示し、それ以外の課室に所属する者にはスケジュールの内容を表示しないようにできること。

⑥スケジュールは、1分又は5分単位で登録できること。また、スケジュールは、1日、1週間、1か月単位の表示ができること。

⑦スケジュールは、複数月（2か月以上）単位の表示ができ、スケジュールの有無が確認できることが望ましい（その場合総合評価において加点する。）。

⑧スケジュールは、複数月（2か月以上）単位の表示ができ、スケジュール内容が確認できることが望ましい（その場合総合評価において加点する。）。

⑨スケジュールの案件ごとに、会議、出張、来客等のカテゴリを付与できること。

⑩自分の所属にかかわらず、任意の利用者によるグループを設定でき、グループ内メンバのスケジュールを一覧表示できること。

⑪グループ内の他の利用者のスケジュールに対して、容易にスケジュールの登録ができること。また、任意の利用者を選択し、スケジュール登録可能な候補日時を表示できること。

⑫スケジュール参加依頼の受容（参加）及び拒否（欠席）が表明できること。

⑬スケジュール参加依頼は、メールで通知されること。また、受容（参加）及び拒否（欠席）の表明をメールから直接実施できること。

⑭スケジュール参加依頼の受容（参加）及び拒否（欠席）の表明結果を一覧で表示可能なこと。

⑮スケジュールが重なっている場合に、目印等の表示で認識可能であることが望ましい（その場合総合評価において加点する。）。

⑯他の利用者のスケジュールの登録、編集、削除を行った場合、スケジュールを変更された利用者に対し、スケジュール情報の変更通知が「8.（4）電子メールサービス」と連携し、送信されること。

⑰繰り返しの予定の登録ができること。また、繰り返しの予定の一括更新及び削除を行えること。

⑱スケジュール登録時に、施設予約機能と連携し、使用権限を有する会議室、備品等の予約を行うことができること。

⑲登録されたスケジュールにもとづき、リマインドを通知する機能を有すること。リマインドは、自ら登録したスケジュールだけではなく、他者に設定したスケジュールにおいても、当該他者に通知できること。
⑳iCalenderフォーマットの任意のURLを読み込み、スケジュールを合わせて表示できること。

(キ)施設予約機能
①会議室、備品等の施設予約ができること。
②予約ができる施設について、任意のカテゴリ・グループ等に設定できること。
③施設予約機能は、施設管理者を設定でき、施設管理者が施設の登録、更新及び削除を行えること。
④施設予約は、1分又は5分単位で登録できること。
⑤カテゴリ・グループ等ごとに各施設の予約状況が1日、1週間単位で表示できること。また、各施設の1か月単位の予約状況の表示ができること。
⑥施設予約の際に、指定した施設の空き時間を検索できること。また、指定した時間帯に利用可能な施設を検索できること。
⑦施設予約の際に、一定の日付、曜日、又は時間による繰り返し予約ができること。

⑧施設の繰り返し予約の一括更新及び削除を行えること。
⑨施設に応じて、個人、組織、役割(ロール)でのアクセス権の設定ができること。
⑩複数の利用者が同時に閲覧、予約、変更、削除の操作をできること。ただし、同一の施設に対して利用時間を重複しての予約はできないこと。
⑪予約情報を変更、削除した場合には、施設の予約者に対して変更通知が送信されること。
⑫施設を予約した際に、スケジュール管理機能を用いた関係者のスケジュール登録が可能なこと。その際、関係者に対し、スケジュール情報の変更通知が「8.(4)電子メールサービス」と連携し、送信されること。

(ク)ワークフロー機能
①ワークフローを50個以上作成できること。
②定義するワークフローは担当職員と協議の上、決定すること。
③決められたワークフローごとに、ワークフロー管理者が任意の承認者を複数の階層で設定できること。
④承認が必要なワークフローが発生した際に、承認者に指定された利用者に電子メールの送信ができること。
⑤申請した利用者が、決裁状況の確認ができること。
⑥承認者が承認又は却下した結果を申請した利用者に電子メールで通知ができること。
⑦ドキュメントを複数の利用者に回覧して、フィードバックを求められること。
⑧フィードバックを求められた利用者はフィードバックを返すことができること。
⑨過去の申請(否決された申請を含む。)を利用して効率的に新規の申請を作成できること。
⑩ワークフローに登録された全ての項目の情報をCSVファイルにエクスポートすることができることが望ましい(その場合総合評価において加点する。)。

(ケ)TODO 機能
①TODOの登録、編集、削除ができること。

②TODOは、件名、開始日、終了期限、優先度、済・未済の状態などの項目が設定できること。
③TODOに関するアラーム通知（終了期限切れ、終了期限の接近を電子メールで通知する等）を設定できること。
④機構内共有アドレス帳を利用してTODOを他の利用者に対して送信できること（他の利用者にTODOを設定できること。）。
⑤TODOを一覧表示できること。

（コ）検索機能
①イントラページ作成機能で作成された情報、電子会議室に投稿された情報について、件名、登録者、内容からのキーワードで文書検索ができること。
②イントラページ作成機能で作成された情報、電子会議室に投稿された情報について、未読・既読の条件によって文書検索ができることが望ましい（その場合総合評価において加点する。）。
③利用者情報を日本語による部分一致検索により検索できること。
なお、組織、氏名、グループ等の単位で表示できること。
④「8. (5)ファイルサーバサービス」で管理された電子ファイルも含めた横断的な情報検索ができることが望ましい（その場合総合評価において加点する。）。
⑤ワープロ機能、表計算機能及びプレゼンテーション機能で作成された検索結果のファイルは、サムネイル及びプレビュー表示され、クライアントアプリケーションを起動することなく、ドキュメントの内容を確認することができることが望ましい（その場合総合評価において加点する。）。

（サ）グループメール機能
①Microsoft 365のグループ機能のように、役職員をメンバとするメーリングリスト又は共有メールボックス（以下「メールグループ」という。メールグループのメンバとできるのは機構役職員だけでよく、外部のアドレスを加えることはできなくてもよい。）を職員自らが容易に作成できること。
②メールグループに属するメンバの追加削除を職員が自ら実施することができること（外部のアドレスの追加削除はできなくてもかまわない。）。
③メールグループのアドレスを送信者に設定したメール送信が可能なこと。
④メールグループのアドレスを送信者に設定して送信したメールにおいては、実際に送信した職員を把握することができるログ（証跡）が記録されること。
⑤作成したメールグループは、Webファイル共有機能、電子会議室機能等におけるアクセスコントロールのためのグループとして利用可能なことが望ましい（その場合総合評価において加点する。）。
⑥自分が参加しているメールグループの一覧を容易に参照することができることが望ましい（その場合総合評価において加点する。）
⑦メールグループの一覧（登録されているメンバの一覧、メールグループの用途等も参照可能）が自動で作成できることが望ましい（その場合総合評価において加点する。）

（シ）配布リスト機能
①複数の機構役職員及び外部アドレスをメンバとするメーリングリストを作成できること。
②当該メーリングリストに送信することにより、メンバ全員にメールが転送されること。
③外部アドレスを含め、配布リストに属するメンバの追加削除を職員が自ら実施することができることが望ましい（その場合総合評価において加点する。）。
④配布リストのアドレスを送信者に設定したメール送信が可能なこと。

⑤配布リストのアドレスを送信者に設定して送信したメールにおいては、実際に送信した職員を把握することができるログ（証跡）が記録されること。
⑥自分が参加している配布リストの一覧を容易に参照することができることが望ましい（その場合総合評価において加点する。）
⑦配布リストの一覧（登録されているメンバの一覧、メールグループの用途等も参照可能）が自動で作成できることが望ましい（その場合総合評価において加点する。）

（ス）共有メールボックス機能
①役職員をメンバとする共有メールボックスを作成できること（システム管理者が作成できればよい。）。
②共有メールボックスのアドレスを送信者に設定したメール送信が可能なこと。
③共有メールボックスのアドレスを送信者に設定して送信したメールにおいては、実際に送信した職員を把握することができるログ（証跡）が記録されること。
④「（シ）配布リスト機能」のメンバにできること。
⑤メールボックスにフォルダを作成できること。また、メールルール等の条件を指定することで、メール送受信時にメールフォルダに振り分けできること。

（セ）その他
①グループウェア画面内から別の画面へ容易に遷移することができること（URLによるリンクを含む。）。
②対象者を指定してアンケート調査ができること。この際、回答形式（プルダウン、チェックボックス、テキストボックス等）及び回答期限を利用者が設定できること。また、回答データをCSV形式等によりファイル出力できること。
なお、アンケート機能のサービスが提供されれば、グループウェア以外のサービスでの提供も可とする。

ウ. セキュリティ要件

「8.（1）認証基盤サービス（ディレクトリ含む。）」のディレクトリサービス機能と連携し、以下のセキュリティ機能を提供すること。

（ア）生体認証によるグループウェアサービスへのアクセス制御ができること。その際、ディレクトリサービス機能と連携した認証が行えること。
（イ）グループメール機能は、ディレクトリサービス機能と連携した認証が行えること。
（ウ）本サービスで提供される各機能単位で利用者、組織、グループごとのアクセス制御ができること。

(3) 申請受付サービス

職員がポータル画面から、各種申請を行う機能を提供すること。

なお、Microsoft 365を採用する場合は、現行システムでSharePointにより実装されている申請受付サービスを引き続き提供することができる。

ア. 基本要件

（ア）利用者数、対象となるログインアカウント数は「4.（1）NITE-LAN システムの利用者」のとおりである。
（イ）以下の申請受付サービス等を提供すること。
なお、詳細については担当職員と協議の上、決定すること。

①短期雇用者ID申請
②ハードウェア申請
③ソフトウェア申請
④ソフトウェア削除申請
⑤メーリングリストアドレス申請
⑥メーリングリスト変更・削除申請
⑦メールアドレス受信制限解除申請
⑧グループフォルダ申請
⑨グループフォルダ変更削除申請
⑩タブレット端末貸出申請
⑪ファイル交換システム利用申請
⑫機構外からのメール及びスケジュール等利用申請
⑬モバイルWiFi貸出申請
⑭その他の申請

「参考 16. 各種申請受付内容」も参照すること。

(ウ)申請受付サービス等の追加を年 1 件以上、変更作業を年 3 件以上予定すること。

イ. 機能要件

(ア)「8. (2)グループウェアサービス(イントラ含む。)」のワークフロー機能で実現すること(グループウェアサービスを実現するためのパッケージソフトウェア又はクラウドサービスの機能で実現できる範囲で設定を行うこと。パッケージソフトウェアのカスタマイズは不要である。)。ただし、「8. (2)グループウェアサービス(イントラ含む。)」に記載されているユーザー数及びワークフロー数とは別にライセンスが必要な場合は別途提供すること。
(イ)「8. (2)グループウェアサービス(イントラ含む。)」のポータル機能から申請ができること。
(ウ)申請の削除、引き戻し、差し戻しができること。
(エ)処理中の申請は、申請から 6 か月間以上、承認、削除等の操作を実施できること。
(オ)承認完了した申請は永続的に保管し、閲覧できること。
(カ)申請の際の入力項目は、「8. (1)認証基盤サービス(ディレクトリ含む。)」のディレクトリサービス機能等と連携し、最小限とすること。

(4) 電子メールサービス

職員が電子メールの送受信を行うメール機能を提供すること。

ア. 基本要件

メールアカウント数と機能を考慮した、メールボックスを含むデータ領域を提供すること。

(ア)前提条件
①ユーザ用メールボックス・アーカイブ領域 ：1人当たり50GB以上
(イ)電子メールの利用者数、対象となるログインアカウント(メールアカウント)数は「4. (1) NITE-LAN システムの利用者」のとおりである。

イ．機能要件

（ア）アドレス帳機能

①機構内共有アドレス帳及び個人アドレス帳が参照できること。

②機構内共有アドレス帳として、以下の機能を提供すること。

・「8．（2）イ．（イ）機構内共有アドレス帳機能」又は「8．（1）認証基盤サービス（ディレクトリ含む。）」と同期した内容のアドレス帳とすること。

・組織情報に基づいた所属別のグループアドレスが利用できること。

・「8.（2）イ.（サ）グループメール機能」で作成したメールグループが利用できること。

③個人アドレス帳として、以下の機能を提供すること。

・職員の氏名（漢字及び振り仮名）、内線番号、属する組織名、役職名、メールアドレスに相当する情報を職員データとして登録できること。

・機構内共有アドレス帳の情報を選択し、登録できること。

・任意の宛先アドレスを連絡先としてグループ化し、送信の宛先としてアドレス帳に登録できること。

（イ）制御機能

①「8．（1）認証基盤サービス（ディレクトリ含む。）」と連携し、メールアカウントの作成、変更、削除ができること。

②メールアカウントごとにメールボックスの容量を設定、変更（一括も含む。）できること。

③メール1通当たりの容量制限の設定、変更ができること。

④件名一覧を、件名順、日付順、送信者順等でソートできること。

⑤利用者が事務用PCにログインしていなくても指定した複数のメールアドレス宛へ自動的に転送できること。ただし、転送の設定は、申請に基づいてシステム管理者が実施する。利用者は実施できないこと。

⑥外部へのメール送信時において、TO、CC及びBCCごとの宛先件数が指定の件数以上の場合に送信を制限できること。本制限は、メールゲートウェイ等で実施してもよい。

⑦メールゲートウェイ又はメールリレーを用いる等し、携帯電話等への指定された特定のドメインへの転送について制御ができること。

⑧メールボックス内のデータ量が上限値に近づいた場合、利用者に容量制限のアラートを通知できること。

⑨メールボックス内のデータ量が上限値を超えた場合、当該アカウントに送受信制限を設けられること。

⑩利用者が選択した電子メールを、ユーザデータ領域に保存する（移動する）機能を有していること。また、設定されたルールに従って、対象となる電子メールをユーザデータ領域へ自動的に移動する機能を有していること。その際、ルールは、利用者により自由に設定が可能なこと。その際、ユーザデータ領域については、事務用PCのローカルドライブであることは必須ではない。

⑪利用者が削除した電子メールの復元が、削除後30日以内であれば利用者本人により可能であること。

⑫複数のドメインを構築、管理可能であること。

⑬バーチャルドメイン、メールエイリアス、メーリングリスト等の機能を用いて別アドレスでもメールを送受信できるよう設定できること。
⑭政府共通NWとのメール送受信ができること（そのためには、政府共通NW用DMZセグメントに電子メールゲートウェイ機能の配置が必要となる。）。その際、ドメイン名に基づき、政府共通NWとインターネットにメールの振り分けができること。
⑮「8.（8）機構外からの電子メール及びスケジューラ利用サービス」を用いて、機構外のインターネットに接続されたブラウザから、機構ドメインの自分宛メールの閲覧と、メール送信を行うための機能を有すること。
⑯機構外から受信できるアドレスやドメイン及び機構外に送信できるアドレスやドメインを、利用者ごとに制限できることが望ましい（その場合総合評価において加点する。）。

（ウ）メールクライアント機能
①利用者に理解しやすいインタフェースを備えていること。
②電子メールの優先度を設定する機能を有していること。
③アドレス指定のオートコンプリート機能を有していること。
④フォルダ等を用いて電子メールを整理できること。
⑤「8.（1）認証基盤サービス（ディレクトリ含む。）」と連携した、前述「（ア）アドレス帳機能②」を提供し、組織別に階層表示できること。また、任意の条件で検索できること。
⑥メールボックス内の電子メールとユーザデータ領域に移動した電子メールについて、メールクライアントを切り替えることなく表示できること。
⑦全文検索機能（添付ファイルは除く。）を有していること。
⑧全文検索機能は、添付ファイルを含め検索可能であることが望ましい（その場合総合評価において加点する。）。
⑨全文検索機能は、ユーザデータ領域に移動した電子メールを含め検索可能であることが望ましい（その場合総合評価において加点する。）。
⑩開封通知機能を提供すること。
⑪開封通知機能は、機構内の利用者側で開封通知の送信拒否ができない機能を有することが望ましい（その場合総合評価において加点する。）。
⑫開封通知機能は、外部へ送信しない機能を有することが望ましい（その場合総合評価において加点する。）。
⑬電子署名がつけられたメールを閲覧できること。
⑭電子メールサービスは、日本語以外のOS及びブラウザからも利用可能なこと。
⑮メール送信元又は送信者の在席情報が表示され、ツールを切り替えることなく、メッセンジャー機能を利用できることが望ましい（その場合総合評価において加点する。）。

ウ. セキュリティ要件

（ア）電子署名、電子証明書・セキュリティデバイス等に対応していること。
（イ）外部とのメール送受信においては、SMTPS 及び STARTTLS に対応していること。
（ウ）自動応答機能（不在連絡）等の機能を使えないようにすること。
（エ）情報漏えい防止に利用できる送信電子メールのフィルタリング機能を有していること。
（オ）受信したメールをテキスト形式で表示する機能を有していること。
（カ）メッセージ又は添付ファイルにマルウェアが見つかった場合、システム管理者等のみがマルウェア検疫済みメッセージを表示及び操作できる機能を有していること。
（キ）スクリプトを含む電子メールを受信した場合において、当該スクリプトが自動的に実行されることがない機能を有していること。（カ）により職員にメッセージを表示させない機能でもよい。

(ク)受信メールに添付されている実行プログラム形式のファイルを削除等することで実行させない機能を有していること。(カ)により職員にメッセージを表示させない機能でもよい。
(ケ)マルウェアの侵入を防止するための機能を有していること。
(コ)機構外からのユーザを装ったメールの受信を防止できること。
(サ)ユーザ単位又はメールアドレス単位でジャンク電子メール、スパム電子メールのスキャニング機能の有効化や、ブラックリストやホワイトリストなどのフィルタリングルールを設定できること。
(シ)ユーザ自身により電子メールのブラックリストやホワイトリストなどのフィルタリングルールを設定できることが望ましい(その場合総合評価において加点する。)。
(ス)マルウェア定義やスパムフィルタの更新が自動的に行われること。
(セ)電子メールの不正な中継を行わないように設定すること。
(ソ)メールクライアントから電子メールを送受信する際に「8. (1)認証基盤サービス(ディレクトリ含む。)」を用いて主体認証を行う機能を備えること。
(タ)「8. (8)機構外からの電子メール及びスケジューラ利用サービス」を用いて、機構外のインターネットに接続されたブラウザから電子メール機能及びスケジューラ機能を利用する際には、二要素認証が行えること。
(チ)「8. (8)機構外からの電子メール及びスケジューラ利用サービス」を用いて、機構外のインターネットに接続された任意の PC のブラウザから電子メール機能及びスケジューラ機能を利用する際には、PC のセキュリティ対策状況をチェックし、対策状況に不備が確認された場合には接続を制限できる機能を有することが望ましい(その場合総合評価において加点する。)。
(ツ)「8. (8)機構外からの電子メール及びスケジューラ利用サービス」を用いて、機構外のインターネットに接続されたブラウザから電子メール機能及びスケジューラ機能を利用する際の通信は、暗号化されていること。

(5) ファイルサーバサービス

機構内において電子ファイルの管理及び共有を行う機能を提供すること。ファイルサーバサービスは、NITE-LANユーザのみが利用できればよい。

ア. 基本要件

(ア)利用者数、対象となるログインアカウント数は「4. (1)NITE-LAN システムの利用者」のとおり。
(イ)同時接続数 835 以上に対応できること。
(ウ)ユーザ保存領域を、15TB 以上提供すること。ファイルサーバはオンプレミス又はクラウド等設置場所を問わない。なお、この領域は機構に属する役職員等の総数で共用利用する(ユーザーごとの保存領域ではない。)。

イ. 機能要件

(ア)事務用 PC の OS が標準でサポートしているプロトコルによって利用できること。
(イ)利用者が個別に割り当て設定等を行わなくとも、ログインスクリプト等により事務用 PC のドライブに自動でデータ領域が割り当てられ、利用することができること。人事異動の際には、移動先の部署等に対応したドライブ割当が行われること。運用作業により、スクリプトの割当を変更しても良い。
(ウ)フォルダ単位、ファイル保有者単位で容量制限を設ける機能を有していること。
(エ)ドライブの空き容量として、利用者に当該ドライブから利用することができる空き容量が表示されること。例えば、フォルダ単位で容量制限が設定されており、そのフォルダがドライブに設定されている場合は、フォルダ単位の容量制限に基づき空き容量が表示されること。それができない場合は、別途空き容量を把握するための手段を利用者に提供すること。

(オ)ドライブの残容量に応じて、フォルダの色が変わる等、利用者が、残容量が少なくなっていることに気がつく機能を有することが望ましい(その場合総合評価において加点する。)。
(カ)Microsoft Office Word の doc 及び docx 形式、Microsoft Office Excel の xls 及び xlsx 形式、Microsoft Office PowerPoint の ppt 及び pptx 形式、Microsoft Office Access の accdb のファイルはファイルサーバ上で編集、動作できること。
(キ)利用者が誤って削除した前日以前に保存したファイルの復元が、削除後 30 日以内であれば可能であること。
(ク)容量制限設定機能については、2 段階での設定値が設定可能で、1 段階目を超過した際に、電子メールやポップアップ等により利用者に対して自動的に警告が発せられ、2 段階目を超過した段階でファイルサーバ機能の利用を制限(保存禁止等)される設定が可能な機能を有すること。
(ケ)共有されたファイルは、ファイルのバージョン履歴を保持し、過去のバージョンにファイルを戻せることが望ましい(その場合総合評価において加点する。)。
(コ)ファイル等を表示する画面では更新日時、追加日時、ファイル名の降順及び昇順でソートできること。

ウ. セキュリティ要件

(ア)「8. (1)認証基盤サービス(ディレクトリ含む。)」のディレクトリサービス機能に保持されているユーザ属性に基づきアクセスコントロールする機能を有すること。
(イ)「8. (1)認証基盤サービス(ディレクトリ含む。)」の認証基盤機能によって認証が行われること。

(6) Web会議サービス等

ア. 事務用 PC のカメラ、マイク及びスピーカーを使って Web 会議ができること。

イ. 機構外から Web 会議に参加できること(そのために必要なソフトウェア等は無償で利用できること。)。

ウ. 機構外のブラウザ(Microsoft Edge、Google Chrome 等)から Web 会議に参加できること。

エ. 表示資料の画面の共有ができること。

オ. 情報漏えい防止の目的から、機構外の者とはファイルの共有ができないようにシステム管理者が設定できること。

カ. 10 人の会議が 30 組の場合、及び 100 人の会議が 3 組の利用の場合においても、2 時間の会議中、音声や映像の大幅な遅延がないこと。

キ. すべての NITE-LAN システムのユーザが会議を開設できること。

ク. Web 会議に、200 人以上参加できること。

(7) 在席表示サービス

在席表示を行う機能を提供すること。在席表示機能は、Web会議サービスの機能の付加機能として提供されることを想定しているが、下記の要件を満たせば単独の機能としての提供でもよい。

ア. 基本要件

(ア)利用者数、対象となるログインアカウント数は「4. (1)NITE-LAN システムの利用者」のとおりである。

イ. 機能要件

(ア)共通機能

①「8. (1)認証基盤サービス(ディレクトリ含む。)」と連携すること。

②全利用者の名簿を課室別等に階層表示できる機能を有することが望ましい(その場合総合評価において加点する。)。

③各個人で任意の利用者をグループ化し登録、変更、削除等の管理ができること。

④内線番号が表示されること。

(イ)在席表示機能

①利用者のプレゼンスを、以下の3種類で確認できること。

・在席し、連絡可能な状態

・離席し、一定時間操作をしていない状態

・不在であり、ログオンしていない状態

②利用者のプレゼンスを、スケジュールに予定が入っているか否かで確認できることが望ましい(その場合総合評価において加点する。)。

③キーボードとマウスの挙動の監視等によって在席状況が自動的に変更されること。

④必要な場合には、自分自身の在席状況を設定する機能を有することが望ましい(その場合総合評価において加点する。)。

⑤他の利用者の在席状況を閲覧できる機能を有すること。

(ウ)チャット機能

①利用者間でメッセージの送受信ができること。

②任意の利用者を設定し複数人への同報ができること。

③利用者自身が送受信した過去のメッセージを確認、削除できることが望ましい(その場合総合評価において加点する。)。

④本機能を利用できる者を設定により限定することができることが望ましい(その場合総合評価において加点する。)。

(8) 機構外からの電子メール及びスケジューラ利用サービス（BYOD対応サービス）

職員が私用のスマートフォンからインターネット経由で「8. (4)電子メールサービス」の利用及び「8. (2)グループウェアサービス（イントラ含む。）」のスケジューラの更新等を行う機能を提供すること。

ア. 基本要件

(ア)利用者数は 835 人とする。

イ. 機能要件

(ア)GUI を用いて設定が行えること。

(イ)「8. (2)グループウェアサービス(イントラ含む。)」上のスケジュール管理機能の閲覧及び更新ができること。

(ウ)「8. (4)電子メールサービス」を利用して、受信した電子メールの閲覧、添付ファイルの閲覧、電子メールの送信が行えること。添付ファイルは、Microsoft 365 の機能である「Microsoft Office Word」、「Microsoft Office Excel」及び「Microsoft Office PowerPoint」で作成されたファイル、GIF、JPG 及び PNG 形式の画像ファイル並びに PDF ファイルの閲覧が可能なこと。それらのファイルが暗号化 zip ファイル内に含まれる場合にも閲覧可能なこと。

(エ)サーバ証明書が必要な場合には、サーバ証明書の取得、登録、更新を行うこと。
なお、当該サーバ証明書をGPKIに発行要求する際のCSR(Certificate signing request:証明書発行要求)を作成すること。
(オ)最新及び1世代前のバージョンのiOS及びiPadOS並びにセキュリティパッチが適用されている3世代前より新しいバージョンのAndroidにおいて利用可能なこと。

ウ. セキュリティ要件

(ア)機構外からの電子メール及びスケジューラ利用サービスを利用する際の通信は入札時点でCRYPTRECが公表する電子政府推奨暗号リストに掲載されている方式で暗号化されていること。
(イ)アカウントのパスワードのポリシー設定(文字種、文字数、利用期間等)ができること。
(ウ)パスワードを複数誤った際に、アカウントをロックする設定が可能なこと。
(エ)アカウント、パスワードに加え、端末認証(PCに保存された秘密鍵による認証を含む。)、ログインごとに有効なワンタイムパスワードやマトリックス認証等を利用した2要素以上の認証を講じること。必ずしも知っていることに追加して何かを持っていることを確認する二要素認証ではなくてもかまわない。
(オ)利用終了後に端末内に「8. (4)電子メールサービス」及び「8. (2)グループウェアサービス(イントラ含む。)」の情報が残らないこと。

(9) 事務用PCサービス

事務用PCを提供すること(機構外からは「12. リモートアクセスサービス」を用いてNITE-LANシステムに接続し、事務用PCと機構を結ぶ通信回線は調達範囲に含まない。)。

ア. 基本要件

必要な台数については、「参考10. 拠点別導入予定式数」を参照すること。

イ. 機能要件

(ア)OS

・提案時において最新バージョンのOSが利用できる機種であること(ハードウェアとして対応していることを求めるものであり、最新バージョンのOSを導入することは必須ではない。)。

(イ)CPU

・キャッシュメモリが、6MB以上であること。

・マルチスレッドのパスマーク値が9,000以上であること。

・マルチスレッドのパスマーク値が13,000以上であることが望ましい(その場合総合評価において加点する。)。

・なお、パスマーク値は「PassMark® Software CPU Benchmarks(※1)」に記載の「CPU Mark(higher is better)」の数値を使用すればよい。
※1: https://www.cpubenchmark.net/cpu_list.php

(ウ)メモリ

・8GB以上のメモリを有していること。

・16GB以上のメモリを有していることが望ましい(その場合総合評価において加点する。)。

（エ）画面表示機能

・画面サイズは13.0型（インチ）以上であること

・解像度1,920×1,080ピクセル以上であること。

・1,677万色以上（Frame Rate Control方式による実現でもよい。）であること。

（オ）ストレージデバイス

・ストレージデバイスのOS及びアプリケーション用領域が、初期インストール状態で、少なくとも85GBの空き容量があること（OS及び本仕様書に記載する要件を満たすために必要なソフトウェアをインストールした状態で85GB以上の空き容量があること。）。

・データ用領域として、少なくとも40GBの空き容量があること。

・ユーザのプロファイルの内容（デスクトップ、マイドキュメント内に保存したファイル等）は、データ用領域に保存されること。

・ストレージデバイスとしてSSDのみで構成されていること。

・ストレージデバイスは、OS及びアプリケーション用領域とデータ用領域にパーティションが分けられていること。

・ストレージデバイスは、S.M.A.R.T機能を有しており、故障予測通知ができることが望ましい（その場合総合評価において加点する。）。

（カ）セキュリティモジュール

・TPM Ver2.0以上に準拠したセキュリティ機能を有していること。

（キ）バッテリ

・電圧はAC100V～240Vに対応していること（ケーブルも同様）。変圧器を備える場合、変圧器の使用による対応でもよい。

・内蔵するバッテリは、満充電の状態で6時間以上使用できること（この場合、測定法については「JEITA バッテリ動作時間測定法Ver2.0又はVer3.0」又はMobileMarkを用い、測定に関する資料を提出すること。）。

・内蔵するバッテリは、満充電の状態で8時間以上使用できることが望ましい（その場合総合評価において加点する。）（この場合、測定法については「JEITA バッテリ動作時間測定法Ver2.0又はVer3.0」を用い、測定に関する資料を提出すること。）。

・内蔵するバッテリは、満充電の状態で10時間以上使用できることが望ましい（その場合総合評価において加点する。）（この場合、測定法については「JEITA バッテリ動作時間測定法Ver2.0又はVer3.0」を用い、測定に関する資料を提出すること。）。

（ク）筐体

・ディスプレイを閉じた状態でW360mm×D250mm×H20mmの大きさ（Hは折りたたんだ際の突起物を除く最小の厚みを指す）以下であること。

・バッテリ（ACアダプタは除く。）を含め1.7kg以下の質量であること。

・バッテリ（ACアダプタは除く。）を含め1.5kg以下の質量であることが望ましい（その場合総合評価において加点する。）。

・バッテリ（ACアダプタは除く。）を含め1.3kg以下の質量であることが望ましい（その場合総合評価において加点する。）。

（ケ）キーボード

・JIS標準配列のキーボードを備えていること。（USB接続等ではなく、本体と一体になっていること（ソフトウェアキーボードは不可）とし、テンキーの搭載は求めない。）

（コ）ポインティングデバイス

・タッチパッドが搭載されていること又はタッチパネルディスプレイであること。

（サ）ネットワークインターフェース

・1000BASE-T以上に対応したLANポートを1ポート以上内蔵していること。

・IEEE802.11ax/ac/a/b/g/nに対応した無線LANが利用できること。

（シ）USB ポート

・端末を充電している状態において、USB2.0以上で、端子形状がStandard-Aのポートを2ポート以上備えていること又はUSB2.0以上で、端子形状がStandard-Aのポート及び端子形状がType-Cのポートをそれぞれ1ポート以上備えていること。

・USB-PDによるバッテリ充電に対応していることが望ましい（その場合総合評価において加点する。）。

（ス）外部接続

・マイク入力端子及びスピーカー出力端子を備えていること。マイク入力について、4極ミニプラグのスマートフォン用ヘッドセット等により、スピーカー出力とマイク入力の共用端子による対応でも可とする。

・マイク及びスピーカーを備えていること。

・HDMIポートを1ポート以上備えていること（USB-C-HDMI変換アダプタ、ポータブル型（持ち運び用）拡張アダプタ等による対応でも可とする。ただしその場合は、変換アダプタ、拡張アダプタ等を装着した状態で、「（シ）USBポート」の要件を満たしていること。また、セキュリティを確保するために、拡張アダプタがLANポートを有している場合には使用できないようにすること。外出時に利用が困難なアダプタは不可である。）。

・HDMI2.0以上に対応したHDMIポートを1ポート以上備えていることが望ましい（その場合総合評価において加点する。）。

・外部ディスプレイを用いて、内蔵ディスプレイと外部ディスプレイに同時に2画面出力ができること（外部ディスプレイは調達の範囲外とする。）。

・搭載しているHDMI1ポートに加え、HDMI、DisplayPort、miniDisplayport又はUSB Type-C(Alt Modeで、DisplayPort Over USB Type-C又はHDMI Alt Mode for USB Type-C Connectorで映像出力をするものに限る。)を用いて3画面出力できることが望ましい（その場合総合評価において加点する。）。

・前項の要件で映像出力にUSB Type-Cを利用する場合、HDMIやDisplayPortへの変換アダプタ等は求めない。

・画面出力はUSBグラフィックアダプタを用いて出力するものは含めない。

・外部出力する際の画面表示は、解像度1,920×1,080ピクセル以上、色数24bit（1,677万色）以上が表示できること。

・外部出力する際の画面表示は、解像度3,840×2,160以上、色数24bit（1,667万色）以上が表示できると望ましい。（その場合総合評価において加点する。）

・事務用PCを使用している状態でディスプレイ上方にウェブカメラを内蔵していること。

（セ）機構の責に帰する故障等の修理

・落下、水濡れ等の機構の責に帰する故障について、別途、機構又は機構の代理の者が対価を支払うことで、修理の対象とすること。ただし、全損等の明らかな修理不可の場合は、別途機構と協議する。

（ソ）その他

・利用者の生体認証装置（指紋認証、顔認証等）を内蔵していること。

・PC端末はグリーン購入法に適合した製品であること。

・ファンレス設計でないこと。

・「12. リモートアクセスサービス」を利用できること。

ウ. ソフトウェア要件

（ア）共通要件

①すべて日本語版を提供すること。また、各ソフトウェアの設定等については、担当職員の指示に従うこと。

②各ソフトウェアは、最適なバージョンのソフトウェアを提供すること。その際には、サービス提供期間中の動作保証及びサポート等を考慮すること。

③各ソフトウェアのライセンスは、利用者が事務用PCを利用する上で必要な数を提供すること。

④機構が保有するソフトウェアについて、事務用PC、運用管理用PC及び仮想クラアイアントマシンへのインストール作業は機構職員が実施する。

⑤前述の機能要件に記載している事務用PCに接続される全ての装置を機能させることを可能とするドライバ類が利用可能な状態にあること。

⑥日本語入力機能

・連文節変換、学習機能、単語登録、ローマ字/かな入力等一般的に日本語入力に必要とされる基本的な機能を有する日本語入力ソフトウェアを提供すること。

・現在機構にて使用しているATOK Pro 2仕様の辞書を移行できること。

・現在機構で使用している入力操作と極力変わらないこと。

⑦文書作成機能

・文書作成、読み込み、編集、印刷、保存ができる文書作成ソフトウェアを提供すること。また、ODFに対応し、ヘッダに特定文字を入れたものをテンプレートとして読み込めること。

・Microsoft 365の機能である「Microsoft Office Word」で作成された文書を、体裁が崩れずに表示し、編集ができること。

⑧法令作成業務支援機能

・「ジャストシステム一太郎ガバメント8」で作成された文書を、体裁が崩れずに表示及び印刷できること。
なお、編集及び保存の機能は不要である。

⑨表計算機能

・文書作成、読み込み、編集、印刷、保存ができる表計算ソフトウェアを提供すること。また、ODFに対応し、ヘッダに特定文字を入れたものをテンプレートとして読み込めること。

・Microsoft 365の機能である「Microsoft Office Excel」で作成された表中の数値、計算式、文字データ及びマクロが変更を加えずに継続的に使用できること。

⑩プレゼンテーション機能

・文書作成、読み込み、編集、印刷、保存ができるプレゼンテーションソフトウェアを提供すること。また、ODFに対応し、ヘッダに特定文字を入れたものをテンプレートとして読み込めること。

・Microsoft 365の機能である「Microsoft Office PowerPoint」で作成されたプレゼンテーション文書を、体裁が崩れずに表示し、編集ができること。

⑪Webブラウザ機能

・W3CHTML標準、ECMAスクリプト規格に規定された機能のみを用いて作成されたWebコンテンツの表示及びフォームを通じての入力ができるWebブラウザソフトウェアを複数種類提供すること。提供するブラウザはシェア及びセキュリティを考慮の上、選択し提供すること。

・保守にあたり必要な場合、契約期間中は、担当職員と協議の上、各Webブラウザのバージョンアップをすること。

⑫ファイル圧縮、解凍、暗号化機能

・自己解凍型暗号化ファイルを容易に作成できるファイル暗号ソフトウェアを提供すること。

・lzh形式へのファイルの圧縮及び解凍ができること。また、zip形式へのファイルの圧縮及び解凍ができ、かつ暗号化できること。
なお、暗号化強度としてAES256以上の強度を指定できること。

・ファイルの分割ができること。

・cab形式、arj形式、tar形式、gz形式、z形式、7z形式、bz2形式、tgz形式、taz形式、tbz形式及びrar形式で圧縮されたファイルを解凍できること。

・事務用PCで利用できるファイル暗号ソフトウェア及びファイル圧縮解凍ソフトウェアは同じソフトウェアであること。

⑬ストリーミング再生機能

・MPEG1、MPEG2及びMPEG4規格に準拠したフォーマットの動画、音声、静止画の表示可能なストリーミング再生ソフトウェアを提供し、再生できること（特許侵害となる恐れがないソフトウェアを提供すること。）。

⑭PDFファイル閲覧及び簡易編集機能

・PDFファイルの閲覧、検索ができるソフトウェアを提供すること。

・各ソフトウェアの印刷機能を用いて、PDF形式で出力できること。

・PDFファイルのページの分割、挿入、削除、順序入替ができること。

・PDFファイル上のテキスト情報に対して背景色を付けるハイライト機能を有すること。

・編集後のファイルは、原本となるPDFファイルへの上書き保存、及び別名ファイルとして保存が可能であること。

なお、保存するファイル形式は問わないこととする。

⑮スキャン取込機能

・「8. (12)複合機サービス」と連携しデータの取り込みができること。

・出力フォーマットはJPEG及びPDF形式で出力できること。

⑯Telnet機能

・プロキシ経由でも利用できるTelnet端末エミュレータソフトウェアを提供すること。

・SSHが使用可能であること。

・VT100のエミュレーションが可能であること。

・送受信及び表示する漢字コードは、JIS、シフトJIS、日本語EUC及びUTF-8に対応し、接続中に切り替えが可能であること。

・スクロールバッファ機能を備えていること。また、バッファはユーザ設定可能であること。

・表示するコンソール画面の行数及び桁数のユーザ設定が可能であること。

・複数の接続先の設定が保存可能であること。またSSH接続時に保存した設定をリスト表示して選択することで、選択した設定で自動接続が可能であること。

⑰ファイル転送機能

・FTPプロトコルによるファイル転送ソフトウェアを提供すること。

・FTPサーバ機能を有するサーバでサポートされている方式により、ユーザ名及び主体認証情報が暗号化されて通信されるようにできること。

・何らかの理由によりファイル転送が途中で中断された場合は、中断部分からファイル転送が再開可能であること。

・ファイルの転送モードを「テキスト」及び「バイナリ」で選択可能であること。

・プロキシを経由してファイル転送が可能であること。

・ファイル転送操作画面において、転送元と転送先の内容が同時に表示されていること。

・複数のファイルの転送を一括して実行可能であること。

⑱簡易データベース機能

・ファイル単位でリレーショナルデータベースを作成できる簡易データベースソフトウェアを提供すること。

・Microsoft 365の機能である「Microsoft Office Access」で作成されたテーブル、クエリ、フォーム、レポート及びマクロが変更を加えずに継続的に使用できること。

⑲その他の機能

・各バージョンのMicrosoft .NET Frameworkのランタイムが利用できること。

・OracleのODBCドライバが利用できること。

・機構にて別途調達している「参考15. MS明朝及びMSゴシック用NITE外字」（それぞれTrueTypeのtte形式のフォントであり、F840～F8C5のコードを使用する。）が利用できること。

・韓国語、中国語のフォントがインストールされていること。タイ語、ミャンマー語（ビルマ語）、ラオス語、クメール語（カンボジア語）、シンハラ語及びチベット語のフォントがインストール可能なこと。

・セキュリティの観点から問題がない場合には、OSの壁紙、フォントサイズ等の各項目の変更を職員が自ら行えること。その他、セキュリティ及び運用管理の観点から問題がない設定項目は職員自ら設定が行えること。

・別途調達予定の外付けCD/DVD/ブルーレイドライブを用いて、汎用的な形式でCD、DVD及びブルーレイディスクへのデータの読み書きが可能なこと。

エ. セキュリティ要件

（ア）利用者の生体情報（指紋認証データ、顔認証データ等）を用いて、事務用 PC の利用時に、生体認証を行うこと。
（イ）盗難防止用ロック器具の取り付け穴が搭載されていること。
（ウ）事務用 PC は、マルウェア対策が施されていること。
（エ）事務用 PC は、ログイン（認証）後、一定時間操作が行われなかった場合にスクリーンロックが働くように設定できること（実際にどのような設定にするかは設計時に機構と調整すること。）。
（オ）生体情報（指紋認証データ、顔認証データ等）を読み取らせることによって、スクリーンロック状態から利用可能状態への切り替えができるように設定できることが望ましい（その場合総合評価において加点する。）。
（カ）外部記憶媒体への書き込みを行う場合、書き込まれるデータが自動的に暗号化される機能を有すること。
（キ）外部記憶媒体への書き込み及び読み込みのログ取得が可能なこと。
（ク）ストレージデバイスが暗号化されていること（ユーザが暗号化を意識することなく通常用いることができれば十分であり、OS から利用できないパーティションは暗号化されている必要はない。）。
（ケ）ストレージデバイスの暗号化鍵は、TPM 等、耐タンパー性を有するデバイスに保持された鍵で守られていること。

(コ)ストレージデバイスの暗号化鍵を守る耐タンパー性を有するデバイスは、OS の改ざんを検知できること。
(サ)ストレージデバイスの暗号化は、ユーザが主体認証情報を忘れた場合にも、安全性が確保された何らかの手段によりストレージデバイスの復号が可能なこと。
(シ)ストレージデバイスの暗号化に関する設定変更のログが取得できることが望ましい(その場合総合評価において加点する。)。

(10) 仮想クライアントマシンサービス

ア. 事務用 PC から、RDP、VNC 等で利用できる仮想クライアントマシンを提供すること。

イ. 仮想クライアントマシンは、Windows OS の仮想クライアントマシン 5 個及び Linux OS のクライアントマシン 1 個を備えること。

ウ. 仮想クライアントマシンは、認証基盤によりユーザの認証を行うものであること。

エ. 仮想クライアントマシンは、トータルでメモリを 76GB 以上備えていること。

オ. 仮想クライアントマシンは、トータルで SPECint_rate2006 が 700 以上の計算性能を有すること(「参考 24. スコア換算方法」に示す換算方法で計算した SPECrate2017_int_peak 又は CoreMark の値を満たすことでもかまわない。)。

カ. 各仮想クライアントマシンに割り当てるリソース量については、担当職員との協議に基づき割り当てること。

キ. Windows OS の仮想クライアントマシンは、事務用 PC のソフトウェア要件を満たすこと。

ク. 仮想クライアントマシンは、ストレージデバイスとしてトータルで 1,200GB の保存領域を確保すること。

(11) 統合管理サービス

事務用PC、仮想クライアントマシン(Windows OSに限る。)及び運用管理用PC(以下「統合管理対象PC」という。)の集中管理を促進するための統合管理機能を提供すること。

なお、「12.リモートアクセスサービス」 で接続されている端末からも、当サービスを利用できること。「イ.(エ) 構成管理機能」、「イ.(カ) ハードウェア構成管理機能」、「イ.(キ) ソフトウェア構成管理機能」については、サーバにおいても当該機能を有するソフトウェアを導入し管理を行うことが望ましいが、ソフトウェアを用いての管理が困難な場合には手動による管理も許容する。

ア. 基本要件

(ア)管理対象とする事務用 PC の台数については、「参考 10. 拠点別導入予定式数」を参照すること。

イ. 機能要件

(ア)共通機能

①受注者のシステム運用担当者(現行は常駐5名程度)が統合管理機能を利用して統合管理対象PCの管理ができる環境を整備すること。その際の端末は、事務用PC及び運用管理用PCとは異なる専用端末を用意すること。

②個別業務システム及び各一般業務システムの運用保守事業者等がIaaSにアクセスするための運用管理用PCを、本所に14台、バイオテクノロジーセンター(木更津市)に2台、大阪事業所に1台用意すること。ただし、「5.(1) 前提条件」のケ. の記載のとおり、機能をISMAPクラウドサービスリストに掲載されたサービスを用いて実現し、機構内

に設置することが必要な機器及び機構内に設置することが望ましい機器のみを機構内に設置した場合には、本所に7台、バイオテクノロジーセンター（木更津市）に2台、大阪事業所に1台用意すること。当該端末からのアクセスについては、アクセスできる先を最低限に限定する（事業者により異なるサーバに限定する）等、セキュリティに留意すること。その実現のために、機構内に設置された運用管理用PCからのアクセスに関しても「12.リモートアクセスサービス」を経由して接続することに限定してもよい。

③運用管理用PC及び個別業務システム及び各一般業務システムの運用保守事業者が運用保守作業のために機構外からリモート接続する端末からIaaSのサーバにアクセスする際の中継用サーバを用意すること。運用管理用PC等からIaaSのサーバにアクセスする際には、直接IaaSのサーバに直接ログインするのではなく、一旦中継用サーバにログインし、それから仮想サーバに再度ログインすることとする。中継用サーバとの通信内容は、不正通信の検出等が行えるよう、当該通信パケットのミラーリングが可能なように構成すること。

④統合管理機能は、その機能の全てが単一のツールにより実現され統一された画面から利用できることが望ましい（その場合総合評価において加点する。）。

⑤アクセスコントロール

・すべての機能にアクセスできるのは管理者のみに限定する等のアクセスコントロールが行えること。

・統合管理機能を使用する者の役割に応じてグループ・ロールの設定（管理者、ヘルプデスク等）が行えること。

・アクセスコントロールに認証基盤及びディレクトリ基盤を用いることができることが望ましい（その場合総合評価において加点する。）。

⑥統合管理対象PCに異常が発生した場合、システム管理者に電子メール等で通知可能なこと。その際、異常発生通知は、その重要度により、通知有無の選択が可能であること。

⑦CSV形式にて情報のエクスポートができること。

⑧レポート機能

・レポートのカスタマイズ機能を有していること。

・統合管理ツールは、レポートにおいてグラフを用いることができることが望ましい（その場合総合評価において加点する。）。

⑨管理画面（コンソール）

・日本語対応の管理画面（コンソール）を有していること。

・管理画面（コンソール）はGUIで操作できること。

・ブラウザを使用した管理画面（コンソール）を有し、どのコンピュータからでもネットワーク上のすべての事務用PC及び運用管理用PCを管理できることが望ましい（その場合総合評価において加点する。）。

・「9. (2)ア. 運用基盤提供サービス」が提供する管理用のコンソールと同じインタフェースであることが望ましい（その場合総合評価において加点する。）。

⑩統合管理対象PCからローカルアカウントの主体認証情報のうち、管理者アカウントの主体認証情報を一括変更し、ユーザからは変更できないように制御できることが望ましい（その場合総合評価において加点する。）。
⑪主体認証情報に関する制限（パスワードポリシー（同じ主体認証情報が利用可能となる履歴数、主体認証情報の最低文字数、主体認証情報の有効期限等）を管理できることが望ましい（その場合総合評価において加点する。）。
⑫統合管理対象PCの電源設定を一元管理できることが望ましい（その場合総合評価において加点する。）。
⑬Webアクセス、メール送信、ファイル操作、ソフトウェアの起動等のログを取得できることが望ましい（その場合総合評価において加点する。）。
⑭ファイル及びソフトウェアの復旧機能を有していることが望ましい（その場合総合評価において加点する。）。
⑮統合管理サービスによる復旧は電源投入時、スケジュール指定、手動等のタイミングで行えることが望ましい（その場合総合評価において加点する。）。

（イ）リモート接続機能

①統合管理対象PCにリモート接続できる機能を有すること。
②リモート接続できる権限を持つユーザを限定できること。
③リモートコントロール権限を一元管理できることが望ましい（その場合総合評価において加点する。）。
④リモート接続時の接続元、接続先、操作の開始と終了がログとして記録され判断できること。
⑤リモート接続中にどのような操作が実行されたのか確認するための画面情報を記録できることが望ましい（その場合総合評価において加点する。）。
⑥帯域が制限されているWAN経由であってもリモート接続が可能であること。
なお、「12.リモートアクセスサービス」で接続されている端末からも、リモート接続が可能であること。
⑦リモート操作の内容を通信パケットから容易に把握できなくする機能を有すること。
⑧リモート操作の通信内容を暗号化して送受信する機能を有していることが望ましい（その場合総合評価において加点する。）。
⑨統合管理対象PCにファイル転送が可能であること。
⑩リモート操作を行っている統合管理対象PCとリモート操作を受けている統合管理対象PCに同じ内容の画面を表示する機能を有していること。
⑪リモート接続先のユーザの承認を得てから接続できる機能を有していること。
⑫統合管理対象PCの再起動が可能であること。
⑬統合管理対象PC上のプログラムを実行できること。
⑭利用者が統合管理対象PCで行えることはすべてリモートで行えることが望ましい（その場合総合評価において加点する。）。
⑮統合管理対象PCにサブディスプレイが接続されている環境においてもリモート操作が可能であることが望ましい（その場合総合評価において加点する。）。

（ウ）ナレッジ管理機能

①トラブル内容、対処方法、ノウハウ情報等のヘルプデスク情報が蓄積可能であること。
また、蓄積したデータを任意の文字列で検索が行えること。

②監視対象の統合管理対象PCで発生したエラー報告について、既存の解決方法が存在した場合は、その情報を通知する機能（メール等で通知できる必要は無い。）を持つことが望ましい（その場合総合評価において加点する。）。
③トラブル対処や初期調査の手順をシナリオとして登録して、トラブル対処の定型化及び簡易化が可能であることが望ましい（その場合総合評価において加点する。）。
④トラブル対処や初期調査の手順のシナリオの実行がイベント発生時に手動実行で選択が行えることが望ましい（その場合総合評価において加点する。）。

（エ）構成管理機能

①統合管理対象PCの構成情報の収集方法として、収集する統合管理対象PCを選択可能であること。又は分析・閲覧の対象とする統合管理対象PCが選択可能であること。
②統合管理対象PCの構成情報の収集方法として、収集する端末をグループ単位で選択可能であること。又は分析・閲覧の対象をグループ単位で選択可能であること。
③統合管理対象PCの構成情報の収集方法として、収集する端末について条件をつけて情報を収集できること。又は分析・閲覧の対象について条件をつけて選択可能であること。
④統合管理対象PCの構成情報の収集方法として、管理者が任意のタイミングで、任意の端末又はグループから収集可能であること。
⑤統合管理対象PCの構成情報の収集時に、利用している利用者の作業を中断しないようにGUIを表示しない、又はGUIを隠すことが可能であること。
⑥帯域が制限されているWAN経由であっても統合管理対象PCの構成情報の収集が可能であること。
⑦構成変更履歴を出力できること。
⑧統合管理対象PCの構成管理情報の一覧及び検索結果をCSV形式で出力が可能であること。
⑨統合管理対象PCにおいてハードウェア及びソフトウェアの追加・削除を実施された場合、管理者は変更履歴画面等により変更状況を把握可能であること。
⑩統合管理対象PCにおいてハードウェア及びソフトウェアの追加・削除を実施された場合、当該統合管理対象PCをネットワークに接続することなく、当該統合管理対象PCを管理者が直接操作することで変更履歴を把握可能であることが望ましい（その場合総合評価において加点する。）。

（オ）未登録機器検索機能

①ネットワークの論理情報や接続機器情報の収集・管理を行い、計画されていない変更を監視するためにマスタ情報と実情報の両方及び差異の検出等変更管理が行えることが望ましい（その場合総合評価において加点する。）。
②ネットワークマップ上にネットワークに接続されている機器を表示する機能を有していることが望ましい（その場合総合評価において加点する。）。

（カ）ハードウェア構成管理機能

①ハードウェアの構成管理が行えること。
②構成情報収集時に統合管理対象PCから転送されるデータが暗号化して送信されることが望ましい（その場合総合評価において加点する。）。
③構成情報収集時にハードウェア情報として、CPU、メモリ、論理ディスク、MACアドレス、外部装置等の項目についての収集が行えること。
④統合管理対象PCのハードウェアの変更を変更された時点で検知、記録できることが望ましい（その場合総合評価において加点する。）。

(キ)ソフトウェア構成管理機能
①ソフトウェアの構成管理が行えること。
②OSに関する情報として、OSタイプ、コンピュータ名、IPアドレス等のネットワーク情報が収集可能であること。
③統合管理対象PCにインストールされているソフトウェア情報について、収集する項目を選択して収集可能であること。又は、表示する項目の選択が可能であること。
④統合管理対象PCのソフトウェアの変更を検知、記録できることが望ましい(その場合総合評価において加点する。)。
(ク)ソフトウェアライセンス管理機能
①ソフトウェアのインストール数をチェックし、ライセンスの管理が可能であること。
②既知及び未知のソフトウェアをスキャンできること。
③統合管理対象PCがネットワークに接続されていない状態から再接続時にソフトウェア利用状況を報告できる仕組みを有していることが望ましい(その場合総合評価において加点する。)。
④ソフトウェアの起動回数、最終使用日時、総利用時間等の情報を収集できること(これらの項目を直接収集できなくとも、収集できる項目から導出できればよい。)が望ましい(その場合総合評価において加点する。)。
⑤ソフトウェアのライセンス保持者、物理的な保存場所等の情報を管理できることが望ましい(その場合総合評価において加点する。)。
⑥ソフトウェアの利用状況を様々な切り口(利用傾向等)で分析できる機能を有していることが望ましい(その場合総合評価において加点する。)。
⑦複数の単位(機構全体、センター、課など)でソフトウェアライセンス管理が行えることが望ましい(その場合総合評価において加点する。)。
⑧統合管理対象PCのソフトウェア利用状況を出力できることが望ましい(その場合総合評価において加点する。)。
(ケ)ソフトウェアの配布機能
①ソフトウェアのリモートインストール又はイメージ配信が行えること。
②ソフトウェアの自動配布を行えること。
③サブネットごとに最初に配布する統合管理対象PCを自動選定し、最初に配布された統合管理対象PCがサブネット内の他の統合管理対象PCへ配信する等、配布サーバが無くてもネットワークに負荷をかけずに効率よく配信する仕組みを有していることが望ましい(その場合総合評価において加点する。)。その際には、統合管理対象PCにストレージデバイスの追加等の必要がないことが前提となる。
④ソフトウェアの自動配布時に、利用者が統合管理対象PCを操作することなく(インストールウィザード等)インストールできる仕組みを有すること。
⑤ソフトウェアの自動配布時に、利用者がインストールを即時実行するか後で実行するかを選択できる仕組みを有すること。
⑥ソフトウェアの自動配布時のタスクスケジューリング機能等、ユーザの業務を妨げない機能を有していること。
⑦端末のグループ分けを行い、グループごとに異なるタイミングで配布が可能なこと(一部の端末に試行的(パイロット的)に配布を行い、正常性を確認した後に本配布を行う等の運用を可能とすること。)。
⑧ソフトウェアの自動配布は、統合管理対象PCの起動時に一斉に行われるものではないこと。

⑨ソフトウェアの自動配布時に配信タイミング等の配信方法の設定を再利用し、受注者の重複作業の負担を軽減する機能を有していること。
⑩配布用のソフトウェアを作成できる仕組みを有していることが望ましい（その場合総合評価において加点する。）。
⑪統合管理対象PCのOSがWindowsの場合には、msi形式、exe形式及びbat形式の配布をサポートしていること。
⑫統合管理対象PCのOSがLinuxの場合には、RPM形式又はdeb形式の配布をサポートしていること。
⑬任意のアプリケーションを配布できるよう、インストール作業中の変化を記録し、配布パッケージを作成できる機能を有していることが望ましい（その場合総合評価において加点する。）。
⑭ソフトウェアの自動配布時にファイルを取得できない状態である端末に対して、統合管理対象PCがファイル取得可能状態になったときに自動的にファイルを取得させる仕組みを有していること。
⑮ソフトウェアの自動配布時に処理途中で終了した統合管理対象PCに対して、端末が再度ファイル取得可能状態になったときに自動的にファイルを取得させる仕組みを有していること。
⑯統合管理対象PCがファイル取得可能になったときに自動的にファイルを取得させる場合、統合管理対象PCの起動処理中に行うなど統合管理対象PCの起動処理の遅延等影響を与えるような処理は行わないこと。
⑰ファイルの配布、ソフトウェアの自動インストール及び任意プログラムの実行をする際にユーザにソフトウェアがインストール中である等の表示非表示が選択できる機能を有することが望ましい（その場合総合評価において加点する。）。

（コ）パッチ適用管理機能

①ソフトウェアベンダ等において、各種パッチファイル（OSのパッチファイル及びマルウェア対策ソフトのマルウェアパターンファイル等）が公開された時点で迅速かつ自動的に最新バージョンを取得し（本件で導入した全てのソフトウェアに対応する必要はない。）、適切なタイミングで統合管理対象PCに配布できる機能を有していること。
なお、各種パッチの対象は、本調達で導入したものとする（自動取得ができないものについては、受注者が運用作業として手動で対応すること。）。
②各種パッチファイルの最新バージョンをテスト環境にアップデートできること。
③動作確認のとれた各種パッチファイル（法令作成業務支援機能、表計算機能等のアプリケーションのパッチファイルを含む。）を任意の統合管理対象PCへアップデートできること。
④統合管理対象PCをスキャンし、各種パッチファイルの適用状況を把握できる機能を有していること（「適用」、「未適用」のステータスを収集できること。）。
⑤動作確認のとれた各種パッチファイル（OS、マルウェア対策ソフト）が適用されていない統合管理対象PCに対して自動的にアップデートが行える機能を有していること。
⑥統合管理対象PCのパッチファイル適用状況を検索・管理できること（パッチが適用されていない端末のリストが抽出できること。）。
⑦パッチ適用処理により、利用者の業務にできるだけ影響を与えないよう設計を行うこと。

(サ)接続機器(外部記録媒体)管理機能
①統合管理対象PCに接続可能な外部記録媒体(SDカード、USBメモリ、コンパクトフラッシュ、スマートフォン、タブレット、PC、ハードディスクドライブ等のストレージ)を個体レベルで制御できること(Bluetooth接続の場合を除く。)。
②スマートフォン、タブレット、PC、ハードディスクドライブ等の通信機器又はストレージとして使用できるBluetooth接続を禁止できること。
③マウス、キーボード及びヘッドセットをBluetooth接続できることが望ましい(その場合総合評価において加点する。)。
④ユーザごと又はユーザのグループ・ロールに基づき、外部記憶媒体への書き込み及び読み込みのアクセスコントロールが可能なこと。その際、グループ・ロールより個別のユーザごとの設定が優先されること。
⑤外部記録媒体の制御は「使用可能」、「読み取り専用」、「使用不可能」を選択できること。
(シ)プリント管理サービス
①複合機利用の印刷日時、複合機名、文書名の情報収集及び管理が統合管理対象PCごとに可能であることが望ましい(その場合総合評価において加点する。)。
②複合機利用の印刷日時、複合機名、文書名の情報収集及び管理がユーザごとに可能であることが望ましい(その場合総合評価において加点する。)。
③複合機利用の両面印刷枚数又は面数・集約印刷枚数又は面数(2in1等)、カラー印刷枚数又は面数、トータル印刷枚数又は面数等の情報収集及び管理が統合管理対象PCごとに可能であることが望ましい(その場合総合評価において加点する。)。
④複合機利用の両面印刷枚数又は面数・集約印刷枚数又は面数(2in1等)、カラー印刷枚数又は面数、トータル印刷枚数又は面数等の情報収集及び管理がユーザごとに可能であることが望ましい(その場合総合評価において加点する。)。
⑤複合機利用の印刷ログデータのファイル出力が可能であることが望ましい(その場合総合評価において加点する。)。
⑥複合機利用の印刷ログデータを視覚的にグラフ、表形式を使用して統計的に参照できることが望ましい(その場合総合評価において加点する。)。
⑦複合機のメーカー、機種を制限されることなく一元管理ができることが望ましい(その場合総合評価において加点する。)。
(ス)ログ管理
①統合管理対象PCの起動、停止及び休止について、実施日時、実行者等のログが収集可能なこと。
②統合管理対象PCへのログイン及びログオフについて、実施日時、ユーザID等のログが収集可能なこと。
③統合管理対象PCにおける外部記憶媒体の利用について、以下のログ収集が可能なこと。
・使用した媒体のメーカー名、シリアルナンバー、ベンダID
④統合管理対象PCにおけるWeb閲覧について、以下のログ収集が可能なこと(コンテンツフィルタリングサービスにおいて同等のログ収集が可能であれば、それでもかまわない。)。
・アクセス先のURL
・POST及びPUTの有無

・日時

⑤統合管理対象PCにおけるソフトウェア利用について、起動及び終了日時、ソフトウェア名等のログ収集が可能なこと（これらの項目を直接収集できなくとも、収集できる項目から導出できればよい。）。
⑥統合管理対象PCにおいて表示されたウィンドウ名について、ログとして収集が可能なこと。
⑦統合管理対象PCにおけるファイル操作について、操作日時や操作ファイル名（パスを含む。）、操作内容等のログ収集が可能なこと。
⑧統合管理対象PCにおけるファイル操作について、アプリケーションによるファイル保存についても、利用者によるファイル操作のログと同等のログ収集が可能なことが望ましい（その場合総合評価において加点する。）。
⑨統合管理対象PCにおける機構外へのメール送信について、送信日時、宛先及び件名のログ収集が可能なこと（電子メールサービスにおいて同等のログ収集が可能であれば、それでもかまわない。）。
⑩統合管理対象PCにおけるクリップボードへのコピー内容等のログ収集が可能なことが望ましい（その場合総合評価において加点する。）。
⑪統合管理対象PCのデバイス構成が変更された際に、変更日時や変更内容等をログとして収集可能なこと。
⑫収集した統合管理対象PCのログについて、アプリケーションのインストール状況や資産情報等から、ログ検索対象となる端末の絞込みが可能であることが望ましい（その場合総合評価において加点する。）。
⑬収集した統合管理対象PCのログについて、外部記憶媒体やネットワークドライブ等の別媒体へバックアップとして保存したログを閲覧する際に、リストアすることなく、管理コンソールから直接検索し、閲覧できることが望ましい（その場合総合評価において加点する。）。
⑭統合管理対象PCをNITE-LANに接続しない状態においても、統合管理対象PCのログを閲覧可能であること（隔離されたネットワークにログ収集のための環境を整備し、閲覧する手法でもよい。リアルタイムに閲覧できることは要さない。）。
⑮収集されたログは、CSV形式等でファイル出力が可能なこと。
⑯収集されたログは、視覚的にグラフ、表形式を使用して統計的に参照できること。
⑰ログの管理は「13.運用管理サービス（1）基本要件及びサービスの改善　ア.基本要件」の仕様を満たすこと。

（セ）事前登録ソフトウェアユーザインストール機能
①あらかじめプログラムを登録しておくことで、当該プログラムをユーザの操作によりインストールできること。
②あらかじめセキュリティパッチを登録しておくことにより、ユーザの操作によりパッチの適用ができること。

ウ. セキュリティ要件

（ア）統合管理対象 PC に禁止ソフトウェアを実行させない仕組みや機能を有していること。
（イ）有害と思われるソフトウェアのリストの提供を受け、それらのソフトウェアを禁止ソフトウェアとする仕組みを有していることが望ましい（その場合総合評価において加点する。）。
（ウ）ネットワーク接続を制御できること（ネットワークへの PC の接続を遮断できること）が望ましい（その場合総合評価において加点する。）（検疫ネットワーク機能を用いても良い。）。

(12) 複合機サービス

職員が印刷、コピー、FAX及びスキャンするための機能を提供すること。

本件で調達する複合機は、以下の2種類である。複合機の台数及び設置場所については「参考10. 拠点別導入予定式数」を、また、現在使用している機器1台あたりの年間想定印刷枚数については「参考07. 年間想定印刷枚数一覧」を参照すること（想定印刷枚数内のカウンター保守サービスは、本件の調達範囲に含む。）。

なお、受注者は、NITE-LANの運用期間中に機構が新たな執務室の設置等を実施する場合において、複合機の機器費用及び設定変更費用等の必要となる費用契約変更等に本調達時と同程度の費用負担（内訳）で応じること。

カテゴリ		種類	台数	概要	プリント	コピー	FAX	スキャナ
複合機	カラー	A	18 台	カラー、高速型、A3 版、フィニッシャー等有	○	○	○	○ （カラー）
	モノクロ	C	2 台	モノクロ、低速型、A3 版、フィニッシャー等無	○	○	○	○ （カラー）

図表２　調達する複合機

ア. 基本要件

複合機の基本機能に係る要件は「参考06. 複合機の基本機能に係る要件」に記載している。それぞれの種類の複合機は「○」を付している要件を全て満たすこと。

イ. 機能要件

(ア)認証・アクセス管理

①複合機は、認証・アクセス管理機能を有すること。

②いずれの場所に設置された複合機であっても、全てのNITE-LANシステム利用者の認証ができること(出張先においても設定の追加を行うことなく複合機が利用できること。)。

③複合機は、「8. (1)イ. (イ)認証基盤機能」のとおりICカード又は生体認証情報(指紋認証データ、顔認証データ等)(以下「ICカード等」という。)によって、認証が行えること。

④複合機において生体認証のみを用いる場合には、事務用PCと同等以上の認識率を有する方法であること(事務用PCを複合機と同様に複数人で共用した場合と同等以上の認識率であることを提案書で証明すること。)。

⑤複合機は、ICカードにより認証を行う場合には、職員が自宅にICカードを忘れる等によりICカードを携帯していない場合のために、生体認証を用いる場合には、認証されない場合に備え、本体パネル上からパスワードを入力する等の方法で出力できること。

⑥ICカードに加えて、生体認証情報による認証機能を有することが望ましい(その場合総合評価において加点する。)。

⑦ICカードを忘れた際のために、パスワード入力等により認証を受けた職員の操作により、職員が有する電子マネーカード等の非接触ICカードを当日に限り時限的に認証に用いることができることが望ましい（その場合総合評価において加点する。）。
⑧複合機における認証と事務用PCにおける認証は、同一の技術を用いたものであることが望ましい（その場合総合評価において加点する。）。
⑨複合機はICカードに加えて、マイナンバーカードによって、認証が行えることが望ましい（その場合総合評価において加点する。）。
⑩複合機は、事務用PCよりプリントしたものが、ICカード等による本人の認証後に初めてプリントされ始めること。
⑪プリントされ始める前にプリントジョブを確認し、選択したプリントジョブを削除可能とする機能を有すること。プリントジョブの削除は、複合機のパネルで行う方式でも事務用PCで行う方式でもかまわない。
⑫複合機は、認証機能を無効化することで、認証することなくプリントを開始可能とできること。
⑬本体パネル上から認証を行う際のパスワードは変更できること（パスワードはパネル上から変更ができる必要はなく、事務用PC等何らかの方法で変更ができれば良い。）。
⑭印刷命令時に印刷する複合機を指定することなく、ネットワークに接続されたどの複合機からでも印刷が可能であることが望ましい（その場合総合評価において加点する。）。

（イ）ログ管理
①事務用PC等からのプリントの印刷日時、ディレクトリ基盤上で用いるユーザID（OSログイン時のユーザID）、ファイル名及びプリント面数又は枚数のログ収集が可能なこと。そのためのプリンタドライバ等のソフトウェアを提供すること。
②コピー面数又は枚数、FAX送信面数又は枚数、FAX送受信先、FAX送受信日時、FAX送受信枚数、スキャナの利用面数又は枚数等、複合機の利用状況のログの収集が可能なこと。
③複合機の利用状況は、利用者ごとに集計して表示が可能なこと。また、CSV形式等で出力が可能なこと。
④両面出力か片面出力か、集約数、カラーかモノクロかについてもログ収集が可能なこと。
なお、集約数についてはプリンタ機能のみ収集できればよく、コピー機能等の場合はできなくても良い。
⑤収集されたログは、ファイル出力が可能なこと。
⑥ログの管理は「13.運用管理サービス（1）基本要件及びサービスの改善　ア.基本要件」の仕様を満たすこと。

ウ. セキュリティ要件

（ア）複合機は、地紋や隠し文字がプリントされていることによってコピー時にそれらが浮かび上がり、資料の不正コピーを防止する機能を有すること。
（イ）複合機は、コピー時に地紋や隠し文字が追加されることによって再コピー時にそれらが浮かび上がり、資料の不正コピーを防止する機能を有することが望ましい（その場合総合評価において加点する。）。
（ウ）複合機は、コピー時に地紋を検知して画像を破壊し、紙一面をグレーに印刷して情報漏えいを抑止する機能を有すること又は、出力を停止することが望ましい（その場合総合評価において加点する。）。

(エ)複合機の FAX 送信機能は、誤送信防止機能(登録された宛先しか送信できない機能やテンキーから宛先番号を直接入力する場合 2 度打ちによる番号の突合機能等)を有すること。
(オ)複合機の FAX 送信機能は、F コード、パスワード等を付加して送信できること。
(カ)暗号鍵管理に TPM2.0 チップ又は同等以上のセキュリティ対策を施していること(その場合総合評価において加点する。)。

エ. 可用性

(ア)スキャン、FAX のログ収集、スキャンデータの OCR 変換等、複合機の機能の実現にサーバを用いる場合には、サーバがダウンした場合にも機能の利用が継続できるよう、冗長化されていること。
(イ)災害等の緊急時には、ユーザ認証を行うことなく FAX 及びコピーの機能が利用可能とできること。
(ウ)認証処理においては、複合機内にキャッシュ情報を格納し、サーバダウン及びネットワークダウン時でも、認証処理が継続できることが望ましい(その場合総合評価において加点する。)。

オ. その他

(ア)印刷命令時に、印刷に要する費用見込額が端末に表示されることが望ましい(その場合総合評価において加点する。)。
(イ)2 色コピー及びプリントの料金は、フルカラー料金よりも安価であることが望ましい(その場合総合評価において加点する。)。

(13) 内部DNSサービス

機構内の通信における名前解決を行う機能を提供すること。

ア. 基本要件

(ア)事務用 PC からのリクエスト処理が行える性能を提供すること。

イ. 機能要件

(ア)SOA、A、CNAME、PTR、MX、SPF の各レコードの登録ができること。
(イ)Dynamic DNS 機能を提供すること。
(ウ)IP アドレスによる DNS クエリの制限ができること。
(エ)DNS ゾーン転送(forward zone)をサポートしていること。
(オ)GUI を用いた操作ができること。
(カ)「10. (2)ス. クライアントアドレス配布サービス」がリースした IP アドレスを内部 DNS サービスの DNS データベースにアップデートできること。
(キ)「10. (2)ス. クライアントアドレス配布サービス」がリースした IP アドレスを内部 DNS サーバの DNS データベースに動的更新した際に、あらかじめ設定した生存時間等をもとに(他の手法でもかまわない。)、使用されていないレコードを削除できること。
(ク)「10. (2)ス. クライアントアドレス配布サービス」と本サービス間で IP アドレスリース情報と DNS 情報が共有できること。
(ケ)SRV レコードをサポートし、「8. (1)認証基盤サービス(ディレクトリ含む。)」のディレクトリサービス機能を実現するサーバを識別できること。
(コ)「8. (1)認証基盤サービス(ディレクトリ含む)」のディレクトリサービス機能との統合管理が実現できる DNS のゾーン(名前空間)を定義できること。
(サ)外部ホストに対する名前解決については、「8. (15)外部公開用 DNS サービス」へフォワードできること。

(14) 外部公開用DNSサービス

外部との通信における名前解決を行う機能を提供すること。

ア. 基本要件

(ア)プライマリ及びセカンダリによる冗長構成としたサービスで提供すること。また、DNS レコードデータが一元管理できること。

イ. 機能要件

(ア)ドメイン名に関する正引き、逆引きができること。ただし、逆引き機能を実現するために当該ネットワークアドレスの情報について、その CIDR を管理する事業者と連携し、正引き時と逆引き時の応答結果に不一致が生じないように留意すること。
(イ)SOA、A、CNAME、PTR、MX、SPF の各レコードの登録ができること。
(ウ)100 以上のサブドメインを設定可能であること。
(エ)ASP サービス等の NITE-LAN システムのネットワーク上以外にある各サービスに必要なホストに対する名前解決(サブドメインを含む。)には、必要に応じ、A レコードによる設定ではなく、CNAME に関する設定を行い、その事業者の DNS による正引き処理を使うこと。
(オ)SINET のセカンダリ DNS サービスとの連携が可能なこと。

ウ. セキュリティ要件

(ア)DNS キャッシュポイズニング対策として、独立行政法人情報処理推進機構(IPA)の「DNS キャッシュポイズニングの脆弱性に関する注意喚起(最終更新日:2009 年 2 月 6 日) http://www.ipa.go.jp/security/vuln/documents/2008/200809_DNS.html」に基づいた対策及び構成を採用していること。
(イ)SPF レコードを登録すること。

(15) コンテンツアップロードサービス

ア. 基本要件

(ア)「9.IaaS サービス」上の一般サーバセグメントに設置された CMS ステージングサーバには同 IaaS サービスの CMS サーバに別途搭載する一般業務システムである CMS システムからのコンテンツを格納する予定である。この CMS ステージングサーバから外部公開サーバセグメントに設置されたサーバに定期的にコンテンツアップロードを行うこと。
CMS ステージングサーバは必ずしも構築する必要はなく、CMS サーバと共存してもよい。その場合、上記の記載は「CMS サーバから外部公開サーバセグメントに設置されたサーバに定期的にコンテンツアップロードを行うこと。」に読み替えること。
(イ)アップロードは最大 30 分ごとの間隔で行うこと。
(ウ)コンテンツアップロードを行う際、「11. セキュリティ対策 (6)情報漏えい対策サービス イ. 改ざん検知対策」と連携して改ざん検知を一時的に停止させた上でコンテンツアップロードを行うこと。
(エ)この実装は、必ずしも何らかの製品で行う必要はなく、別途プログラムを作成し、このサービスを実装しても良い。

(16) メール共有サービス

複数の担当者による受信メールへの対応を管理するメール共有機能を提供すること。

クラウドサービスにより機能提供する場合には、サービス全体としてISMAPクラウドサービスリストに掲載されていることは要さず、その稼働環境がISMAPクラウドサービスリストに掲載されていれば要件を満たすものとする。

ア. 基本要件

(ア)令和 7 年 4 月 1 日から令和 8 年 3 月 31 日の間は 111 人以上、令和 8 年 4 月 1 日から令和 12 年 3 月 31 日の間は 71 人以上がメール共有サービスを利用できること。
(イ)令和 7 年 4 月 1 日から令和 8 年 3 月 31 日の間は 19 個以上、令和 8 年 4 月 1 日から令和 12 年 3 月 31 日の間は 15 個以上のメールアドレスを利用できること。
(ウ)送受信ともにメールを管理できること。
(エ)メールの一斉送信ができること。

イ. 機能要件

(ア)メールごとにステータスを設定できること。設定できるステータスの種類は追加・変更・削除ができること。
(イ)メールに紐付いた過去の送受信履歴を一覧表示できること。
(ウ)メールにコメントを付与できること。
(エ)担当者、ステータス等に基づいてフィルタリングした一覧表示が可能なこと。
(オ)メールごとに担当者をアサインできること。
(カ)フォルダによりメールを分類できること。
(キ)メールをフォルダに自動的に振り分ける機能を有すること。
(ク)作成中のメールを一時保存できること。
(ケ)署名を登録し、登録した署名を使用できること。
(コ)POP3 でメールを受信できること。
(サ)受信する際の通信の暗号化(STARTTLS 又は SSL/TLS)に対応していること。
(シ)SMTP でメールを送信できること。
(ス)送信する際の通信の暗号化(STARTTLS 又は SSL/TLS)及び SMTP 認証に対応していること。
(セ)メールに返信することで自動的にスレッド(メールに紐付く対応履歴)が作成され、スレッド単位でまとめて表示する機能を有すること。
(ソ)メールアドレスのグループごとに、利用者のアクセス権(少なくとも閲覧、編集、削除、メール送信の可不可)を設定できること。
(タ)作成したメールの確認者を設定できること(確認者のみメール送信が可能なようアクセス権を設定することで承認送信フローを実現する。)。
(チ)問合せ対応の集計機能(利用者別、メールアドレス別等)を有すること。
(ツ)バックアップや解析等のため、送受信したメール及びアドレス帳のデータを全て一括して出力する機能及び出力したデータをインポートできる機能を有すること。
(テ)メールデータを CSV 等のテキストデータで一括出力することができること。

ウ. セキュリティ要件

(ア)受信したメールをテキスト形式で表示する設定が可能であること。
(イ)パスワードの最低文字数制限を設定できること。
(ウ)利用者が自らパスワードを変更できること。
(エ)ログインしたとき及びメールを送信したときのログは出力されること。

9. IaaS サービス

(1) 基本要件

IaaSサービス全体に共通する要件を以下に記載する。

ア. 全体構成（論理構成）

IaaSサービスは、一部オンプレミス環境への配置が必要なサーバを除き、オンプレミス環境又はパブリッククラウド環境にて、「参考02. 次期ネットワーク構成概要図（案）」及び「参考05. IaaS仮想サーバ要件一覧」を参考に設計すること。IaaSサービスが提供するサーバ群が稼動するネットワークセグメントの概要を以下に示す。

なお、パブリッククラウドサービスを利用する構成を選択した場合、パブリッククラウドの利用に要する費用全てと、データセンターと本所（東京）間を結ぶ回線（1Gbpsの帯域確保型）に要する費用全てについても受注者が負担すること。

（ア）DMZ セグメント

外部公開用DNS等の稼動が想定されるネットワークセグメントである。インターネット等の外部ネットワークとの接続ポイントとなる。

（イ）外部公開サーバセグメント

メール中継サーバ、機構全体及び機構各分野における外部公開用Webサーバ、外部共有サーバ等が稼動するネットワークセグメントである。インターネット等の外部ネットワークに対して、前述（ア）のDMZセグメントを介して各種サービスを提供する。

（ウ）一般サーバセグメント

一般業務システム及び個別業務システム用のサーバ・ストレージ等が稼動する内部のネットワークセグメントであり、外部からアクセスを受けることはない。

イ. サービス提供範囲

IaaSサービスは以下の（ア）のサービス並びに（イ）及び（ウ）のシステムの稼動・監視・管理のため、後述する「(2)サービス要件」に記載するサービスの提供を行う。（イ）一般業務システム及び（ウ）個別業務システムに必要なIaaSサービスの詳細は「参考05. IaaS仮想サーバ要件一覧」を参照すること。

受注者は、NITE-LANの運用期間中に、機構がIaaSサービス上で新たなシステムを構築及び運用する場合において、構築費用及び設定変更費用等の必要となる費用契約変更等に本調達時と同程度の費用負担（内訳）で応じること。

（ア）機構全体に係る情報システムサービス

「8. 業務サービス」の認証基盤サービス（ディレクトリ含む。）、ファイルサーバサービス、ファイル交換サービス、後述する「11. セキュリティ対策」等のサービスである。

（イ）一般業務システム

機構の企画管理部にて所管しているシステムで、NITE-LANシステム以外のものである。具体的には、CMSシステム、人事・給与システム、文書管理システム等がある。

（ウ）個別業務システム

機構の各センターが所管する業務システムである。

ウ. 集約サーバが提供するスタック構成

(ア)IaaS サービスが稼動する集約サーバ上にて提供するサービス(スタック構成)を以下に示す。

なお、下図「スタック(レイヤ)」欄の(ア)、(イ)及び(ウ)、前述イ. に記載の(ア)、(イ)及び(ウ)と対応する。

アプリケーションレイヤ		既存アプリ	既存アプリ
ミドウルェアレイヤ（固有）		既存アプリ	既存アプリ
ミドルウェアレイヤ（汎用）			
OS レイヤ			
仮想化レイヤ			
ハードウェアレイヤ			
スタック（レイヤ）	**（ア）**	**（イ）**	**（ウ）**

(イ)前述「イ. サービス提供範囲」の「(イ)一般業務システム」及び「(ウ)個別業務システム」で用いられる仮想サーバにて稼動する OS は、「参考 05. IaaS 仮想サーバ要件一覧」を参照すること。

(2) サービス要件

ア. 運用基盤提供サービス

(ア)運用時間

IaaSサービスを構成するハードウェア、ストレージ、仮想サーバ等は、24時間365日（機構内のサーバールームは、法定点検に伴う停電はない。）でのサービス提供が可能であること。

(イ)ソフトウェアのバージョンアップ、セキュリティパッチ等の適用

インターネット経由でソフトウェア製造元からパッチ等をダウンロードする場合は、DMZセグメントのプロキシサーバを経由する構成とすること。

イ. 時刻同期サービス

本調達の各サーバ、ネットワーク機器、運用管理用PCについては、NTPプロトコル等を使用して、日本の標準時刻と同期が可能であること。

ウ. 監視サービス

本サービスは以下の機能を備えること。

(ア)稼働監視

①本調達のハードウェア（仮想環境における仮想ストレージ、仮想スイッチを含む。）の稼働監視機能
②本調達のソフトウェア（仮想化ハイパーバイザを含む。）のメッセージ・ログ監視、一般業務システム及び個別業務システム側で導入するソフトウェアを含むプロセス・サービス監視及びメッセージ・ログ監視機能（一般業務システム及び個別業務システムに必要となるプロセス監視、ログ監視の参考情報として、「参考18. 現行個別監視項目概要」を示す。）
③前述①から②に掲げるハードウェア、OS、DBMS等ミドルウェア、各業務アプリケーション、ネットワーク等、共通基盤内で発生するログ、バッチジョブ等ジョブスケジューラ製品から出力されるメッセージ等を統合的に運用監視する機能

(イ)性能監視
①ハードウェアの状態監視機能
②CPU、メモリ等の各使用状況（しきい値）の監視機能
③ストレージの使用状況（しきい値）の監視機能
④データベースの性能監視機能（オープンソースであるデータベースソフトウェアを除く「参考05. IaaS仮想サーバ要件一覧」に記載のあるデータベースソフトウェアを対象としたものに限る。）
⑤キャパシティ・性能情報の取得機能及びレポート出力機能
⑥仮想化された運用基盤全体におけるリソース使用状況の自動収集機能

(ウ)ネットワーク監視
①SNMPv3、Syslog転送等を使用して、ネットワークの状態監視機能
②MIB情報等を使用して、ネットワークの使用状況（しきい値）の監視機能

(エ)その他

次の機能が提案されることが望ましい（その場合総合評価において加点する。）。

①仮想サーバの統計情報を一定期間蓄積することで、監視対象オブジェクトの正常稼働状態を学習し、学習したデータから動的なしきい値を生成する機能
②仮想サーバの動的なしきい値により、システムの正常性を監視する機能
③現状の仮想化された運用基盤全体のリソース使用状況から、将来的に必要なリソース量やリソース追加推奨時期を自動算出する機能
④仮想サーバのリソース使用状況から、それぞれの仮想サーバの最適なスペックを提示できる機能
⑤仮想サーバのリソース使用状況から、割り当てられたリソースが不足している仮想サーバをリストアップできる機能
⑥仮想サーバの稼働状況を把握し、利用されていない無駄な仮想サーバをリストアップできる機能

(オ)CPU のアーキテクチャ

IaaSのCPUは、AMD又はx86-64アーキテクチャをサポートしていること。

エ. ジョブスケジューラサービス

本サービスは以下の機能を備えること。

(ア)ジョブの定義、スケジューリング、ジョブの実行監視等の機能
(イ)ジョブの実行に係るオペレーション、進行状況の確認等のジョブ管理を行う機能

オ. バックアップ・リストアサービス

本サービスは以下の機能を備えること。

(ア)サービス停止時間を最小限(又は無停止)としながら取得可能なボリュームコピー機能による複製(クローン)、増分又は差分データの保存による複製(スナップショット)及びリストア機能
(イ)データバックアップ取得及びファイル単位でのリストア機能
(ウ)世代管理機能
(エ)ジョブスケジューラ等を使用した、バックアップ取得に係るスケジュール設定機能
(オ)本調達のハードウェア及びソフトウェアから出力されるログのバックアップ及びアーカイブ機能
(カ)ハードウェアの構成情報(ファームウェア、パラメータ等構成定義)のバックアップ及びリストア機能(BIOS 設定等一般的にバックアップの対象とならないものは含まない。また、クラウドサービス等機構内にハードウェアを導入していないものは含まない。)

カ. 仮想環境管理サービス

本サービスは以下の機能を備えること。

(ア)仮想環境のプール管理
①サーバ、ストレージ、スイッチ等の仮想サーバ構成要素をリソースプールとして一元的に管理する機能
②仮想サーバにインストールされているソフトウェアの種類、バージョン情報等のシステム構成情報の管理、ライセンス数の員数管理が容易となる機能
(イ)ライブマイグレーション
①仮想サーバにてシステム障害等が発生した際に、別の物理サーバ上で仮想サーバを稼動させることが可能な機能
②仮想サーバが移動する際にシステム停止等が発生しないこと(瞬断は可である。)。

キ. ログ管理サービス

(ア)IaaS サービス及びネットワーク機器から出力されるログは、ログ管理サービスにより収集し管理すること。
(イ)収集及び管理は、クラウド環境、オンプレミス環境を問わないが、収集対象とするログは一元的に管理すること。
(ウ)キーワード検索等で閲覧したいログへのアクセスが容易であること。
(エ)収集したログは、サービス提供の期間管理すること。
(オ)収集したログは、最低でも直近 1 年間分を常時参照できるようにすること。それより過去のログについては、CSV 形式等により SSD 等の記録媒体に保存し提供するか、クラウド環境で機構のログへのアクセス要求から 24 時間以内に提供可能なように保管すること。
(カ)サービス期間終了後のログは、CSV 形式等により SSD 等の記録媒体に保存し提供するか、クラウド環境で少なくとも 1 年間は機構がアクセス可能なよう対応すること。このクラウド環境は機構のログへのアクセス要求から 24 時間以内に提供可能なものであること。

(3) テスト系サービス

各仮想サーバへのセキュリティパッチ適用等の検証・動作確認を行うために必要なテスト環境を提供すること。テスト環境は常時必要なく、プロビジョニング機能等を用いて必要時に構築できれば良い。

テスト系サービスを用いて、NITE-LANシステムへのパッチ適用の際は十分な検証を受注者は行うこと。テスト系サービスで対応できない場合には、検証に必要な機材については受注者の負担で用意すること。

検証環境を仮想環境で用意する場合は、本番環境に一切影響を与えない構成とすること。

パッチ適用の検証以外のテスト系環境の利用は、5年間で数件が見込まれる。

(4) 疑似インターネットサービス

IaaSサービス上のシステム構築や移行、改修時に、機構外への公開前に、リバースプロキシ経由でのアクセスを考慮した、システムの動作確認やセキュリティ診断等を行う環境を提供すること。疑似インターネットサービスにおいては、機構内の事務用PCから、インターネットに向けられたリバースプロキシ経由で各システムにアクセスすることが可能なこと。また、セキュリティ診断事業者等が端末を接続して疑似インターネットサービスを用いるネットワークポートを提供すること。

疑似インターネット環境の利用は、1年間で数件が見込まれる。

10. ネットワークサービス

(1) 基本要件

ネットワークサービス全体に共通する要件を以下に記載する。

ア. 全体構成図

NITE-LANシステムの構成は「参考02. 次期ネットワーク構成概要図（案）」を参考に、現行セグメント構成を踏襲して設計すること。ネットワークセグメント構成の基本的な方針を以下に示す。

(ア) DMZ セグメント

リバースプロキシ、外部公開用DNS、スパムメール対策サーバ等の稼動が想定されるネットワークセグメントである。インターネット等の外部ネットワークとの接続ポイントとなる。

(イ) 外部公開サーバセグメント

メール中継サーバ、機構全体及び機構各分野における外部公開用Webサーバ、外部共有サーバ等が稼動するネットワークセグメントである。インターネット等の外部ネットワークに対して、前述(ア)のDMZセグメントを介して各種サービスを提供する。

外部公開サーバセグメントはさらにその中を、機構全体に係る情報システムサービス用セグメント、国際評価技術本部用セグメント、バイオセンター用セグメント、化学センター用セグメント、認定センター用セグメント、製品安全センター用セグメントに分けること。

(ウ) 一般サーバセグメント

いわゆる内部LANである。認証基盤サービスや電子メールサービス、一般業務システム及び個別業務システム用のサーバ・ストレージ等が稼動するネットワークセグメントであり、外部からアクセスを直接受けることはない。

一般サーバセグメントはさらにその中を、機構全体に係る情報システムサービス用セグメント、国際評価技術本部用セグメント、バイオテクノロジーセンター用セグメント、化学物質管理センター用セグメント、認定センター用セグメント、製品安全センター用セグメント及び特許サーバセグメント（特許サーバは機構が別途調達するものをいう。）に分けること。

(エ)端末セグメント

事務用PC、複合機等を接続するセグメントである。

(オ)運用管理セグメント

運用管理用PC等を接続するセグメントである。他のセグメントとは分け、通信可能な範囲を制限する。必要に応じて、セグメント単位ではなく、運用管理用PC等のIPアドレス単位で通信可能な範囲の制限を行う。パッチ適用等のため、ホワイトリストの範囲でインターネット接続は可能とする。認証も「8.(1)認証基盤サービス(ディレクトリを含む。)」を用いて可能とする。

イ. 拠点構成及び必要機器数

拠点構成及び必要機器数については、「参考02. 次期ネットワーク構成概要図(案)」、「参考10. 拠点別導入予定式数」、「参考13. 現行ネットワーク構成図」及び「参考19. 拠点別現行PC台数」 を参照すること。

ウ. ネットワークサービス

(ア)サービス構成要素の各機器を接続し、サービス提供を実現するために必要なネットワークサービスを提供すること。
(イ)ネットワークサービスでは、通信種別による必要帯域の確保、優先ができること。

エ. IP ルーティング

(ア)静的ルーティングを設定することにより動的ルーティング使用時も意図的に経路制御できること。
(イ)静的ルーティング及び動的ルーティングにおいてデフォルトルートを利用できること。
(ウ)アドレス空間を有効利用するため、クラスレスルーティングに対応すること。

オ. DMZ の配置

(ア)インターネット上に公開するサーバを収容する DMZ(DMZ セグメント、外部公開サーバセグメント)の配置場所は、「参考 02. 次期ネットワーク構成概要図(案)」を参照すること。
(イ)政府共通 NW と接続する DMZ(政府共通 NW 用 DMZ セグメント)の配置場所は、「参考 02. 次期ネットワーク構成概要図(案)」を参照すること。

カ. QoS サービス

(ア)各拠点におけるトラフィックは DiffServ 値、ToS 値もしくは CoS 値を利用して、優先度、帯域制御を設定できること。
(イ)拠点ごとに帯域の割合を変更できること。

キ. SLA（サービスレベルアグリーメント）

「参考09. サービスレベル合意書（案）」を満たすため必要に応じて冗長化を行うこと。

(2) サービス要件

ア. LAN 設計

LANの設計時には、階層型モデルに基づいた設計を行うこととし、WANアクセス、コア/ディストリビューション、アクセスの3階層構成を基本としつつ、各階層のモジュール化を実施し、モジュール単位での拡張及び縮小が可能であり、システム変更の極小化による構築変更作業の軽減と運用の効率化を実現すること。

(ア)WAN アクセスレイヤモジュール

WANアクセスレイヤは、ルータとして動作し（ソフトウェアによるルーティングを行うルータであることは必須ではない。）、拠点間通信を効率よく中継することでWANの最適化を提供する。

(イ)コア/ディストリビューションレイヤモジュール

コア/ディストリビューションレイヤは、マルチレイヤスイッチとして動作し、冗長化されたレイヤ3機能を主に実現する。下位のアクセスレイヤを集約し、経路制御に基づいてパケットの高速転送を行いインターネット、政府共通NW、一般サーバセグメント、NITE-WAN等に中継する役割を有する。フロア単位でアクセスレイヤからのトラフィックを集約するディストリビューションレイヤにレイヤ3機能を持たせず、コアレイヤにレイヤ3機能を集約する構成でもよい。仮想化技術を用いても良い。

(ウ)アクセスレイヤモジュール

①アクセスレイヤは、本所及び地方拠点においてレイヤ2スイッチ及び無線LANアクセスポイントとして動作する。アクセスレイヤスイッチは事務用PC、複合機等のクライアントとディストリビューションレイヤ又はWANアクセスレイヤとを中継する。

②アクセススイッチからのダウンリンク配線は「5. (2)接続関連」を参照すること。

イ. ネットワーク接続サービス

(ア)インターネット接続機能

①NITE-LANは、本所から1Gbps以上の帯域で、現行システム同様、学術情報ネットワーク（SINET）にてインターネットに接続できること（SINETの接続拠点（ノード）までのアクセス回線は調達範囲外である。）。

②接続インターフェースは1000BASE-T、全二重オートネゴシエーションであること。

(イ)政府共通 NW 接続機能

①NITE-LANは、政府共通NWに接続できること。また、接続回線、DSU、ルータは政府共通NW側によって提供されることから、本調達はルータに接続するためのLANケーブル及びファイアウォール装置以降となる。
②NITE-LANシステムにおいては、機構が指定する複数のグローバルIPアドレス領域宛のパケットが、政府共通NWにルーティングされること(その他のグローバルIPアドレスはインターネットにルーティングされること。)。
③NITE-LANは、政府共通NWからのIPパケットを、拠点間をつなぐ広域ネットワークに流さないこと。
④NITE-LANは、政府共通NWにおける名前解決のためのDNSサーバ機能を有していること(可能であれば、インターネットにおける名前解決のためのDNSサーバ機能と同じハードウェアでもかまわない。)。
⑤NITE-LANは、政府共通NWとの時刻同期を行うためのNTPクライアント及びサーバ機能を有していること。
⑥接続インターフェースは1000BASE-T、全二重オートネゴシエーションであること。政府共通NWのルータは冗長化していることから、冗長化に対応すること。

ウ. 無線 LAN サービス(職員用)

無線LANサービス(職員用)は、職員が事務用PCを用いてNITE-LANシステムを利用することが可能なサービスを提供すること。無線LANの利用においては以下の機能及びセキュリティを満たすこと。

(ア)職員が無線 LAN を利用する場合は、有線の場合と同様に NITE-LAN システムにおける識別認証を行うことができること。
(イ)「8. 業務サービス」の利用にあたって、支障のない無線 LAN 通信規格を採用すること。
(ウ)IEEE 標準規格として、802.11a、11b、11g、11n、11ac、11ax に対応しており、全てに対し Wi-Fi 認定を取得していること。
(エ)通信の暗号化は WPA3、WPA2、IEEE802.11i に準拠した AES-CCMP による暗号化を使用すること。
(オ)無線 LAN から NITE-LAN システムを利用できる機器(すなわち端末セグメントに接続できる機器)を事務用 PC に制限できること。
(カ)無線 LAN サービスを利用可能とする場所については、「参考 14. 無線 LAN アクセスポイント等の情報配線工事」」を参照すること。
(キ)無線 LAN サービスを提供するためのアクセスポイントの設置場所には、付近に電源が存在しない場合があるため、必要に応じて PoE(Power over Ethernet)等の手法を用いること。

エ. フォワードプロキシサービス

(ア)インターネット用フォワードプロキシ機能
①NITE-LANシステムは、内部セグメントからインターネット及びDMZセグメントにアクセスする際のセキュリティ確保のためのフォワードプロキシ機能を有していること。
②フォワードプロキシ機能は透過型でないこと。
③アクセス元、アクセス先等により機構が特に指示する場合を除き、端末セグメントからインターネットへのアクセスは、フォワードプロキシ機能を経由したものに制限できること。
④フォワードプロキシ機能は、http及びhttpsプロトコルによるインターネットからのマルウェアの侵入を防止するための機能を有していること(インターネット用ファイアウォール機

能がマルウェアの侵入防止機能を有している場合には、フォワードプロキシ機能で重複して機能を有している必要はない。）。

⑤フォワードプロキシ機能は、HTTPをサポートしていること。

⑥フォワードプロキシ機能は、CONNECT、TCPrelayをサポートしている等、HTTPSを通過させることができること。

⑦フォワードプロキシ機能は、ロギング機能を有していること。

⑧フォワードプロキシ機能は、DNSの検索結果のキャッシング機能を有していること。

⑨フォワードプロキシ機能は、Webコンテンツのキャッシング機能を有していること。

⑩フォワードプロキシ機能は、ウイルススキャン機能を有し、問題があった場合のロギング機能を有していること。

⑪フォワードプロキシ機能は、アクセスコントロールにディレクトリ基盤を利用するようにも設定できる機能を有した製品で構成されていること。

⑫フォワードプロキシ機能は、Webによる管理画面を有していること。

⑬フォワードプロキシ機能は、1Gbps以上のスループット性能又は3,000requests/sec（平均レスポンス容量11kByte想定）以上の処理性能を有すること。

（イ）政府共通 NW 用フォワードプロキシ機能

①NITE-LANシステムは、内部セグメントから政府共通NWにアクセスする際のセキュリティ確保のための政府共通NW用フォワードプロキシ機能を有していること。

②アクセス元、アクセス先等により機構が特に指示する場合を除き、政府共通NWへのアクセスは、政府共通NW用フォワードプロキシ機能を経由したものに制限できること。

③事務用PCは、ブラウザの設定を変更することなく、政府共通NWとインターネットの両方にアクセスできること（例えば、政府共通NWへのアクセスが必要な場合には、フォワードプロキシ機能から政府共通NW用フォワードプロキシ機能に自動で転送されるように設定する等の方法が考えられる。）。

④政府共通NW用フォワードプロキシ機能は、マルウェア対策機能を有すること（ただし、政府共通NW用フォワードプロキシ機能単独でマルウェア対策機能を有している必要は無く、フォワードプロキシ機能との共用でも良い。具体的には例えば、政府共通NW用フォワードプロキシ機能が常にフォワードプロキシ機能からの転送で利用されるのであれば、フォワードプロキシ機能のマルウェア対策機能でこの要件は充足されているものとすることができる。）。

⑤政府共通NW用フォワードプロキシ機能は、HTTPをサポートしていること。

⑥政府共通NW用フォワードプロキシ機能は、CONNECTをサポートしている等、HTTPSを通過させることができること。

⑦政府共通NW用フォワードプロキシ機能は、マルウェア対策機能を含め、ロギング機能を有していること。

⑧政府共通NW用フォワードプロキシ機能は、Webによる管理画面を有していること。

⑨政府共通NW用フォワードプロキシ機能は、10Mbps以上のスループット性能又は120requests/sec（平均レスポンス容量11kByte想定）以上の処理性能を有すること。

オ. リバースプロキシサービス

（ア）インターネット用リバースプロキシ機能

①NITE-LANシステムは、リバースプロキシ機能を有すること。リバースプロキシ機能を提供する動的コンテンツについては、「参考04. 課室所管情報システムの移行に係る要件」のURLの列を参照すること。
②リバースプロキシ機能により、動的コンテンツ提供のためのWebサーバ機能が認識する要求元IPアドレスが変わってしまう場合には、リバースプロキシ機能は、追加HTTPヘッダ（X-Forwarded-For等）によって、要求元の実IPアドレスを宛先サーバに通知可能なこと。
③同様に、リバースプロキシ機能は、Viaヘッダにホスト名を値として格納し宛先サーバに通知可能なこと。
④リバースプロキシ機能は、SSLをサポートしていること（暗号化及び復号化を行うSSLオフロード機能を有していること。）。
⑤上記オフロード機能は、SSLクライアント認証機能を有すること。
⑥上記オフロード機能は、PEM形式のCA証明書及びチェーン証明書が利用可能なこと。
⑦上記オフロード機能は、クライアント証明書情報をHTTPヘッダ情報として付加し、宛先サーバに通知可能な機能を有すること。
⑧上記オフロード機能は、秘密鍵の所有者のX.500識別名をHTTPヘッダ情報として付加する機能を有すること。

⑨リバースプロキシ機能は、FTP、HTTP/0.9、HTTP/1.0、HTTP/1.1をサポートしていること。また、HTTPにおいてはTLS1.2以上をサポートすること。
⑩リバースプロキシ機能は、Apache JServe Protocolをサポートしていることが望ましい（その場合総合評価において加点する。）。
⑪リバースプロキシ機能は、ソースIPアドレスに基づくパーシスタンス機能を有すること。
⑫リバースプロキシ機能は、SSLセッションIDに基づくパーシスタンス機能を有すること。
⑬リバースプロキシ機能は、Cookieに基づくパーシスタンス機能を有すること。
⑭リバースプロキシ機能は、SSLオフロード機能を含め、1Gbps以上のスループット性能を有すること。

現行システムにおけるリダイレクト等の設定数については、「参考 23. 現行システム負荷分散装置リダイレクト・プール設定数」 を参照すること。

（イ）政府共通 NW 用リバースプロキシ機能

①NITE-LANシステムは、政府共通NWからのアクセス用の政府共通NW用リバースプロキシ機能を有すること（インターネット用リバースプロキシ機能と別の機器である必要はない。）。
②政府共通NW用リバースプロキシ機能は、政府共通NW用DMZセグメントに配置されていること。
③政府共通NW用リバースプロキシ機能は、SSLをサポートしていること（暗号化及び復号化を行うSSLオフロード機能を有していること。）。
④政府共通NW用リバースプロキシ機能は、HTTP/0.9、HTTP/1.0、HTTP/1.1をサポートしていること。
また、HTTPにおいてはTLS1.2以上をサポートすること。
⑤政府共通NW用リバースプロキシ機能は、ソースIPアドレスに基づくパーシスタンス機能を有すること。
⑥政府共通NW用リバースプロキシ機能は、SSLセッションIDに基づくパーシスタンス機能を有すること。
⑦政府共通NW用リバースプロキシ機能は、Cookieに基づくパーシスタンス機能を有すること。

（ウ）メール中継サーバ機能
①IaaSサービス上に構築されたシステムからインターネット及び政府共通NWへのメールの中継ができること。

カ. 負荷分散サービス

（ア）リバースプロキシサービスは、負荷分散機能を有すること。
（イ）リバースプロキシ機能における負荷分散機能は、アプリケーションごとに最適なヘルスチェックを行い、パケットのレイヤ 4 以上の情報に従って動的に振り分け先サーバを選択できること。
（ウ）任意にセッションタイムアウトの時間が設定できること。
（エ）アプリケーションごとに負荷分散装置を導入せず、基盤情報システムサービス全体に対するリクエストの処理を最適化すること。
（オ）将来のサーバ追加等に対し、サービスを停止することなくリソースの追加を行い、性能向上が可能であること。
（カ）分散先のサーバが全て稼動しておらず、サービスを提供できない場合には、自動でメンテナンス画面の表示ができること。
（キ）負荷分散機能は、1Gbps の最大スループット性能を有していること。

キ. 可用性

（ア）システム高可用性
①ネットワーク機器の冗長化及び機器内での冗長化により、故障による影響及びメンテナンス作業時のサービス停止を最小化できること。
②ネットワーク機器の冗長化及び機器内での冗長化により、メンテナンス作業時のサービス停止を最小化できること。
③ネットワーク機器については、可能な限り信頼性の高い機器を選定し、「参考09. サービスレベル合意書（案）」に規定する稼働率を満たすこと。

（イ）リンク高可用性
①配線の冗長化により、アクセスレイヤとコア/ディストリビューションレイヤ間は単一障害によるネットワークの通信断が発生しないこと（アクセスレイヤのスイッチは単一障害点となっても良い。また、コア/ディストリビューションレイヤが存在するのは本所のみの想定

である。その他の拠点では、WANアクセスレイヤとアクセスレイヤの直接接続を想定している。)。

②可用性を考慮したうえで必要となるポート数を確保すること。

ク. 性能

(ア)システム全体の通信量の増大においても、個々の通信の性能低下がないよう転送処理はハードウェアで行うこと。ただし、接続する回線に対するスループットに影響が出ない場合は、この限りではない。

(イ)本調達における主なトラフィックは本所に集約されるため、ネットワークトポロジを勘案した上で、WAN の帯域による制限を除いて通信等に支障がないこと。WAN の帯域については、「参考 02. 次期ネットワーク構成概要図(案)」を参照すること。

(ウ)WAN 帯域の有効活用をするため、LAN 内でラージパケットはフラグメントしジャンボフレームを流さないこと。

(エ)本所の NITE-LAN の中心に位置しルーティングを担うコアスイッチは、200Mbps 以上の L3(IPv4)のパケット転送処理性能を有すること。

ケ. 物理インタフェース

(ア)構成上、必要な数のインタフェースを搭載するとともに、物理ポートの故障に備え、運用に支障のない程度の予備ポートを有すること。

(イ)メディアタイプ等は任意に選択してかまわないが、配線ルート上制約により変更を求める場合がある。

コ. セキュリティ

(ア)不要なトラフィックによるネットワーク性能の劣化を防止し、また制御部の処理能力を保護するため、マルチキャスト、ブロードキャストのストーム発生を抑制する仕組みを取り込み、性能維持を実現したサービスを提供すること。

(イ)セキュリティの強化及び帯域資源の有効利用のため、レイヤ 2 インタフェース及びレイヤ 3 インタフェースにおいて、任意のパケットをフィルタすること。

(ウ)セキュリティの強化及び帯域資源の有効利用のため、同一セグメント内でのレイヤ 4 レベルでのアクセス制限ができること。

(エ)予期せぬネットワークトポロジの変更及びケーブルの誤接続を防止するため、未使用ポートは使用不可とすること。

サ. アドレス設計

(ア)原則現行システムのアドレス設計を踏襲すること。

(イ)新規フロア追加等、LAN 拡張時は、現行システムの設計を踏襲し、可能な範囲でアドレス計画を行うこと。

シ. クライアントアドレス配布サービス

(ア)事務用 PC の IP アドレスは、DHCP によるダイナミックなアドレッシングを行い、複合機等には MAC アドレスを指定した IP アドレスの静的付与ができること。

(イ)証跡管理の運用負荷を低減させるため、アドレス配布の集中管理を行うこと。

ス. 運用管理サービス

(ア)基本機能

①ネットワーク管理、プランニングの資料となるホスト、プロトコルごとの統計情報を収集できること。
②通信パケットをコピーし、ネットワークを通じて遠隔にてキャプチャできること（当該機能はネットワーク機器の機能を用いて実現することを想定している。）。
③ネットワーク監視装置から状態監視、死活監視ができること。

（イ）管理、運用に関わる機能
①機器の異常を検知した際にSNMPトラップにより通知すること。

②システムに関するイベントを検知した際にSyslogによる通知を行うこと。
③様々なトラフィック診断に利用できるよう、リモートでのトラフィック診断に利用できるよう、転送パケットをミラーリングし、IPカプセル化して送信できることが望ましい（その場合総合評価において加点する。）。
④トラフィックの傾向を観察しネットワーク計画に役立てるために、IPインタフェースごとにフロー、プロトコルの集計データを一定時間保持し、外部装置に転送できること。
⑤システムの容量の見直し及びネットワーク拡張の計画に役立てられるよう、インタフェースごとに転送パケット数、転送バイト数、パケット破棄数、エラー数を一定時間取得すること。
⑥OSバージョン管理を容易にし、メンテナンス性を向上させるため、2世代以上のバージョンのOSイメージを内部ストレージ又は外部ストレージに保持し、設定、コマンド等によってOSを指定して起動できることが望ましい。（その場合総合評価において加点する。）ただし、レイヤ2スイッチ、レイヤ3スイッチ、ルータのみを対象とする。
⑦OSイメージが壊れた際の復旧手段として、TFTPによるネットワークブート又は装置内の予備OSイメージからブートができることが望ましい。（その場合総合評価において加点する。）。ただし、レイヤ2スイッチ、レイヤ3スイッチ、ルータのみを対象とする。
⑧SSHv2によるセキュアなリモートアクセスを提供すること。
⑨管理機能の脆弱性へのセキュリティ攻撃を未然に防ぐため、不要なサービスのプロセスを明示的に停止できること。

セ. 既存機器、他システム等との接続

（ア）受注者は、「参考 13. 現行ネットワーク構成図」及び「参考 22. 使用継続機器件数」を参考に既存の機器（インタラクティブホワイトボード、鍵管理システム等）、他システムを NITE-LAN システムに接続し、使用可能なように NITE-LAN システムのネットワーク機器等の設置、設定等を行うこと。既存の他システムには、本所バイオゾーンにおいて接続されている各種サーバ等が存在する。また、バイオテクノロジーセンター（木更津）においては、他システムとの接続のために複数のスイッチが必要となるため留意すること。
（イ）他システムとの接続の際には、NITE-LAN システムのネットワークに影響を及ぼさないような接続方法をとり、NITE-LAN システム及び各種機器に影響を与えない構成とすること。
（ウ）NITE-LAN システムと接続する他システムに対し、DNS、NTP、LDAP の機能を提供すること。

（3） WAN要件

拠点間を結ぶWANについては、別途機構が広域Ethernetサービス又はIP-VPNサービスを調達する。ただし、広域Ethernet又はIP-VPNに接続するルータ又はレイヤ3スイッチは、本件の調達範囲である。広域EthernetかIP-VPNのいずれを用いるか制約が存在する場合には、提案書に記載すること。

なお、導入を予定しているWAN回線の帯域については、「参考12. 広域ネットワーク仕様（予定）」を参照すること。

WAN回線のLAN側インターフェースについては1000BASE-T、全二重オートネゴシエーションとすること。

11. セキュリティ対策

（1） 基本方針、管理体制等

ア. 基本方針

(ア) NITE-LAN システムにおいては、外部からの攻撃に対するセキュリティ対策のみでなく、内部でのセキュリティ対策、外部の情報システムに対して悪影響を与えないためのセキュリティ対策等、総合的なセキュリティ対策を講じること。

(イ) それぞれのセキュリティ対策は、可能な限り単一点のみで講じることとはせず、各サービス、機器、通信経路上等の複数点において、調達範囲において複合的に講じること。

(ウ) 機構の情報セキュリティポリシー（「情報セキュリティ管理規程」及び「情報セキュリティ対策基準」）、入札公示日における最新版の「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」を遵守すること。機構の情報セキュリティポリシーは、https://www.nite.go.jp/nite/jyohokoukai/sonotahojin/security/security.html から参照可能である。「政府機関の情報セキュリティ対策のための統一基準」は、内閣サイバーセキュリティーセンターのホームページで公開されている。

(エ) 機構外からアクセス可能なサービスは、ファイアウォール等によりアクセス制御を行うこととし、データベースを保有するサーバは、機構外から直接アクセスできない領域に配置すること。

(オ) 各機器を設置するまでに（設置時でもよい。）、管理者パスワードを初期設定から適切なパスワード（適切であるためには、機器ごとに異なる必要がある。）に変更すること。

(カ) 各サービスにて使用するハードウェア、BIOS、OS、ソフトウェア（ドライバを含む。）、アプリケーション等の脆弱性が発見された場合には、速やかにその解消に努めること。

(キ) ホワイトリスト方式で除外した通信先を除き（Microsoft 365 を利用する場合はホワイトリストに設定する想定である。）、インターネットとの通信内容は、不正通信の検出等が行えるよう、本所を経由して通信されるようネットワークを構成すること。また、当該通信パケットのミラーリングが可能なように構成すること。

(ク) 職員のみが利用するパブリッククラウドのサービスは、IP アドレス制限等を行うことにより、機構外からのアクセスを不可とすること。

イ. 管理体制

(ア) 以下の内容を含む情報セキュリティ対策要領を提出すること。

①機構から提供する情報の目的外利用の禁止
②情報セキュリティ対策の実施内容及び管理体制
③受注者又はその従業員、再委託先、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
④受注者の資本関係・役員等の情報、本件業務の実施場所、本件業務従事者の所属・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
⑤情報セキュリティインシデントへの対処方法
⑥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
⑦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

(イ)本件業務に携わる者を特定する資料を提出すること。
(ウ)本件業務に携わる者が実施する具体的な情報セキュリティ対策の内容を含む受注者の情報セキュリティ対策の遵守方法、情報セキュリティ管理体制等に関する確認書を提出すること。
(エ)情報の受渡し方法や委託業務終了時の情報の廃棄方法等を含む情報の取扱手順を機構と協議し、合意し、定めた手順により情報を取り扱うこと。
(オ)開発工程において、機構の意図しない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ること。また、当該品質保証体制が書類等で確認できること。
(カ)情報システムに機構の意図しない変更が行われるなどの不正が見付かったときに、追跡調査や立入検査等、機構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。また、当該体制が書類等で確認できること。
(キ)情報セキュリティ対策の状況に懸念があると機構が認める場合には、情報セキュリティ監査を受け入れること。
(ク)役務の一部を再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、上記(ア)から(キ)と同等の要件を再委託先に求めること。
(ケ)再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を機構に提供し、機構の承認を受けること。
(コ)業務の終了時には、受注者において取り扱った情報を機構に返却又は消去すること。また、返却又は消去したことを証明する書類を提出すること。

ウ. ローカルアカウントのパスワード管理

(ア)事務用 PC のローカルアカウントのパスワードは、事務用 PC ごとに異なる英数文字と記号からなるランダムな 8 文字以上とすること。

エ. データベース管理

(ア)データベースに対する内部不正を防止するため、管理者アカウントの適正な権限管理を行うこと。
(イ)データベースに格納されているデータにアクセスした利用者を特定できるよう、措置を講ずること。
(ウ)データベースに格納されているデータに対するアクセス権を有する利用者によるデータの不正な操作を検知できるよう、対策を講ずること。
(エ)データベース及びデータベースへアクセスする機器等の脆弱性を悪用した、データの不正な操作を防止するための対策を講ずること。

(2) マルウェア対策サービス

ア. 基本要件

(ア)ウイルス、ワーム等、悪意のあるソフトウェアに加え、スパイウェア、アドウェア等を含めた、いわゆるマルウェア対策を講じること。

(イ)パターンファイルの公開時期のずれによる対策の遅れを吸収するため、サーバ系と事務用 PC 系で異なるベンダの製品を導入するか、ゲートウェイ系(ファイアウォール、プロキシサーバ、メールサーバ等)と事務用 PC 系で異なるベンダの製品とすることが望ましい(その場合総合評価において加点する。)。
(ウ)マルウェア対策ソフトウェアは常駐可能で、リアルタイムでのマルウェア対策を行えること。
(エ)マルウェアを検出した場合、自動駆除を行い、検出及び自動駆除を行ったログを取得するとともに、検出及び自動駆除の結果をシステム運用担当者にメールで通知すること。
(オ)パターンファイルの配布は自動化可能であり、また、配布状況については集中管理できること。
(カ)マルウェア対策サービスの不具合により、パターンファイルの適用を自動で行えない場合は、手動により適用できること。
(キ)パターンファイルの不具合が判明した場合等、必要な場合に、1 世代前のパターンファイルにロールバックすることができること。
(ク)パターンファイルが適応していない、未知のマルウェアと思われるソフトウェアが NITE-LAN システムにて発見された場合、機構のシステム運用担当者と調整の上、検体を元に解析を行い、未知のマルウェアが判明した場合には、当該マルウェアに対応したパターンファイルを作成し、提供すること。
(ケ)ダウンロードファイル及びメール添付ファイルの振る舞いを検査し、未知のマルウェアを検出・防御する機能(以下「ゼロデイ対策機能」という。)を有すること。
(コ)ゼロデイ対策機能により不正な振る舞いが検知された場合には、ファイアウォール、パターンファイル方式でのマルウェア検知等の機能と連携して感染した端末以外でも自動的に防御できるようになることが望ましい(その場合総合評価において加点する。)。
(サ)通信パケットのヘッダ情報等から通信先などの情報を取得し不正サイトへの通信を検知できること(ゼロデイ対策機能を提供する製品で実現する必要はなく、ファイアウォール等で実現してもよい。)。
(シ)DNS 通信を監視し、危険なドメインに対するクエリ後の危険なドメインに対する通信から脅威を検知し防御できること(ゼロデイ対策機能を提供する製品で実現する必要はなく、ファイアウォール等で実現してもよい。)。
(ス)通信のふるまいから、ボット等に感染した疑いのある事務用 PC を特定する機能を有することが望ましい(その場合総合評価において加点する(ゼロデイ対策機能を提供する製品で実現する必要はなく、ファイアウォール等で実現していても加点する。)。)。
(セ)不正サイトへの通信を行っている端末を迅速に特定できること。
(ソ)不正サイトの照会データベース情報については、自動的に最新の状態に更新できること。
(タ)不正通信を検知した場合にはその端末の特定(IP アドレス、ホスト名、MAC アドレスなど)ができること。
なお、DHCP 環境下による端末特定情報の誤差については許容する。
(チ)管理画面は GUI 画面を有すること。
(ツ)監視対象とする通信は、端末セグメントからインターネットへの全ての通信を含むこととし、インターネットへの通信については、最低でも http、smtp、ftp、https の通信を監視できること。
(テ)不正な通信の痕跡が確認された場合には速やかに担当職員に連絡し、インシデント対応支援も行うこと。
(ト)不正サイトの確認やログ分析等で機構外に通信する必要がある場合は送信される情報についてあらかじめ提示し承認を得ること。
(ナ)ヒープスプレー攻撃を検出又は防御できる機能を有していることが望ましい(その場合総合評価において加点する。)。
(ニ)ダブルフリー脆弱性を利用する攻撃を検出又は防御できる機能を有していることが望ましい(その場合総合評価において加点する。)。

（ヌ）Null 参照に係る脆弱性を利用する攻撃を検出又は防御できる機能を有していることが望ましい（その場合総合評価において加点する。）。
（ネ）端末に至る通信経路又は端末のいずれかにおいてゼロデイ対策機能による対策が行われること。
（ノ）マルウェアが検出された場合及び不正な振る舞いが検知された場合には、当該端末をネットワークから分離できること（運用作業として実施する方法でもよい。）。
（ハ）端末から収集した情報、サーバから収集した情報、通信経路において収集した情報を総合的に分析することで、マルウェア、不正アクセス等を検知し、その感染経路、影響範囲等の分析評価を行う機能を有することが望ましい（その場合総合評価において加点する。）。

イ. サーバ系マルウェア対策

（ア）すべてのサーバ、仮想サーバ（事務用 PC 及び事務用 PC によるマルウェアのリアルタイムでのスキャンが行われるファイルサーバは除く。）にマルウェア対策を講じること。
（イ）コマンドにより、ファイル単位でマルウェアの有無の確認を行えることが望ましい（その場合総合評価において加点する。）。

ウ. 統合管理対象 PC 用マルウェア対策

（ア）統合管理対象 PC にマルウェア対策を講じること。
（イ）マルウェアが検知された場合には、ポップアップが最前面に表示され、利用者の操作にかかわらず最前面に表示され続け、利用者に通知されること（製品の機能として実現できなくても、別途プログラムにより実現してもよい。）。

(3) 不正アクセス対策サービス

ア. ファイアウォール機能

（ア）インターネット用ファイアウォール機能
①インターネットからの不正アクセスを防止するためのファイアウォール機能を有すること。
②ファイアウォール機能は、ステートフルインスペクションが可能なこと。
③NITE-LANシステムは、SYN Flood 対策機能等を有効にする等、ネットワーク装置が装備している機能をサービス不能攻撃対策に活用する設定となっていること。
④ファイアウォール機能は、トラフィック等に関する統計情報を把握できる機能を有すること。
⑤ファイアウォール機能は、統計情報をグラフ等でビジュアルに表示できる機能を有していること。
⑥ファイアウォール機能は、その設定変更等の管理操作におけるアクセスコントロールに認証基盤サービスを用いることができることが望ましい（その場合総合評価において加点する。）。
⑦ファイアウォール機能は、NAT機能を有すること。
⑧NAT機能は、ソースIPアドレスのセグメントに応じて異なるIPアドレスをソースIPアドレスにする機能を有していること。
⑨ファイアウォール機能は、GUIによる管理画面を有していること。
⑩ファイアウォール機能は、設定の履歴を有するか又は設定のバックアップが可能で、以前の設定に戻す機能を有していること。
⑪ファイアウォール機能は、ロギング機能を有すること。
⑫ファイアウォール機能は、ソースセグメント（又はソースゾーン、ソースインターフェース等）、デスティネーションセグメント（又はデスティネーションゾーン、デスティネーション

インターフェース等）、プロトコルタイプ（TCP/UDP）並びにポート及びポートグループによるアクセスコントロールが可能なこと。
⑬ファイアウォール機能は、設定のバックアップ機能を有すること。
⑭ファイアウォール機能は、バックアップサーバを用いて設定のバックアップが可能なことが望ましい（その場合総合評価において加点する。）。
⑮ファイアウォール機能は、ポリシーの追加等の設定変更の際に、候補設定が設定でき、コミット前に修正内容の確認ができ、コミットすることで候補設定を実設定に反映できる方式であることが望ましい（その場合総合評価において加点する。）。
⑯ファイアウォール機能は、異なるOSのバージョンで冗長化構成とできることが望ましい（その場合総合評価において加点する。）。
⑰ファイアウォール機能は、装置の基本処理としてアプリケーションの可視化が行え、ポート番号だけでなく、通信の内容からアプリケーションの種類を識別し記録できることが望ましい（その場合総合評価において加点する。）。
⑱ファイアウォール機能は、セキュリティ機能を有効にした状況で1Gbps以上のスループット性能を有していること。
⑲ファイアウォール機能は、300,000以上の同時セッションが可能なこと。

（イ）政府共通 NW 用ファイアウォール機能
①NITE-LANシステムは、政府共通NWから及び政府共通NWへの不正アクセスを防止するための政府共通NW用ファイアウォール機能を有すること。
②政府共通NW用ファイアウォール機能は、トラフィック等に関する統計情報を把握できる機能を有すること。
③政府共通NW用ファイアウォール機能は、NAT機能を有すること。
④政府共通NW用ファイアウォール機能は、GUIによる管理画面を有していること。
⑤政府共通NW用ファイアウォール機能は、設定の履歴を有するか又は設定のバックアップが可能で、以前の設定に戻す機能を有していること。
⑥政府共通NW用ファイアウォール機能は、ロギング機能を有すること。
⑦政府共通NW用ファイアウォール機能は、ソースセグメント（又はソースゾーン、ソースインターフェース等）、デスティネーションセグメント（又はデスティネーションゾーン、 デスティネーションインターフェース等）、プロトコルタイプ（TCP/UDP）並びにポート及びポートグループによるアクセスコントロールが可能なこと。
⑧政府共通NW用ファイアウォール機能は、設定のバックアップ機能を有すること。
⑨政府共通NW用ファイアウォール機能は、100Mbps以上のスループット性能を有していること。
⑩政府共通NW用ファイアウォール機能は、40,000以上の同時セッションが可能なこと。

イ. 不正侵入防御機能

（ア）NITE-LAN システムは、不正アクセスを検知する機能（IDS 機能）を有していること。
（イ）NITE-LAN システムは、不正アクセスを防止する機能（IPS 機能）を有していること。
（ウ）IDS 機能及び IPS 機能は、GUI による管理画面を有していること。
（エ）IDS 機能及び IPS 機能は、防御のために用いる攻撃パターン（シグネチャ）を自動で更新する機能を有していること。
（オ）不正侵入防御機能は、最大 1Gbps 以上のスループット性能を有していること。
（カ）送信元の IP アドレス情報について、既知の脅威のある発信元であることを確認できる評価データベースに照会を行い、当該データベースに登録されている IP アドレスを元に攻撃者であると判定することができることが望ましい（その場合総合評価において加点する。）。

(4) コンテンツフィルタリングサービス

ア. 統合管理対象 PC に対してコンテンツ(URL)フィルタリングができること。

イ. フィルタリングに際しては、フィルタリング用データベースを持ち、それを参照することによりフィルタリングができること。

ウ. フィルタリングデータベースは、定期的にインターネット経由で最新の状態に更新できること。

エ. 回線帯域以上の処理能力を有し、インターネット閲覧時にボトルネックとならないこと。

オ. フィルタリングをジャンルで指定できること。

カ. 特定の URL をフィルタリングデータベースに任意に追加できること。

キ. 特定の IP アドレスに対して、フィルタリングを解除できること。

ク. マルウェア配布サイト、スパイウェアの通信先等の危険な URL 情報をカテゴリとして有し、セキュリティフィルタリングとしても利用できることが望ましい (その場合総合評価において加点する。)。

(5) 認証・検疫ネットワークサービス

ア. MAC アドレスが登録されていない機器の NITE-LAN システムへの接続を検出できること。ただし、クラウド等の機構の建屋外の部分は除く。

イ. MAC アドレスが登録されていない機器は、NITE-LAN システムとの通信ができないようにすること。

(6) 情報漏えい対策サービス

ア. 改ざん防止対策(ウェブアプリケーション・ファイアウォール)

(ア)インターネットからの通信による一般業務システム及び個別業務システムの Web コンテンツの改ざんを未然に防止するために、ウェブアプリケーション・ファイアウォール機能を有すること。

(イ)インターネットから一般業務システム及び個別業務システムへの通信を監視し、DoS 攻撃、SQL インジェクション、バッファオーバーフロー、クロスサイトスクリプティング、クッキー改ざん等を防御できること。

(ウ)認証情報入力フォームに対する総当たり的なパスワードアタック及び DoS 攻撃等の脅威を検知した場合に、通信を遮断する機能を提供することが望ましい(その場合総合評価において加点する。)。

(エ)シグネチャ及びパターン等の更新を行い攻撃の防御を行う方式(ブラックリスト方式)及び更新を必要とせず、ホワイトリスト方式による未知の攻撃を防御できる方式のいずれも可能なこと。

(オ)改ざん防止対策は、最大 1Gbps 以上のスループット性能を有していること。

(カ)危険な攻撃の有無を早急に検知するため、ログ分析監視運用サービスを提供すること。

(キ)監視運用サービスにおいては、最新のセキュリティ事情に対応できるようにするため、必要に応じて独自の WAF シグネチャを提供すること。

(ク)監視運用サービスにおいては、装置が収集した全ログデータを 24 時間 365 日体制でリアルタイムに相関分析及びアナリストによるセキュリティ分析を行い、危険な攻撃を検知した場合は速やかに担当職員へ電話連絡して担当職員の指示に基づき通信遮断等の対応を行うこと。インシデント対応支援も行うこと。

イ. 改ざん検知対策

(ア)「参考 05. IaaS 仮想サーバ要件一覧」に示した仮想サーバのうち改ざん検知対策ソフトを導入することを要件とした仮想サーバのファイルの改ざんを検知した場合、システム運用担当者に通知できること。
(イ)動的コンテンツを作成するスクリプト及びアプリケーションの改ざん検知対策ができること。
(ウ)改ざん検知にあたっては、検知対象のディレクトリやファイルを複数指定できること。また、検知対象としたディレクトリ配下の一部のサブディレクトリやファイルに対して検知対象から複数除外できること。
(エ)改ざんを検知した場合には、メールで通知できること。
(オ)改ざんを検知した場合には、Web サービスの停止、さらには Web サービスの停止に伴うソーリーページを表示させる等の制御を行うこと(検知から 30 分未満に実施できるのであれば運用作業として実施する方法でもよい。)。
なお、改ざんを自動で復旧する機能は不要である。
(カ)改ざん検知は、全てのコンテンツについて 30 分に 1 回以上の頻度で実施すること(Web サービスの停止、ソーリーページの表示等を運用作業として実施する場合には、検知から実施までに要する時間を加えて、改ざんから 30 分以内に対処ができる頻度で改ざん検知を実施すること。)。

ウ. その他(サーバ、事務用 PC 及び運用管理用 PC 共通)

(ア)NITE-LAN システムを構成するサーバ並びに事務用 PC 及び運用管理用 PC(アプライアンス製品は除く。)で使用したストレージデバイスを保守交換等により機構外部へ持ち出す場合は、ストレージデバイスの完全消去又は専用ツールによりセキュリティロックをかけ、保守拠点にてストレージデバイスの完全消去を行うこと。完全消去は、暗号化消去方式でもよく、サーバルーム外に暗号化鍵が持ち出されないことが担保されていれば、サーバルーム内に暗号化鍵が残っていても暗号化消去が行われたとみなしてよい。ただし、複数のディスクにデータが分散して記録されておらず、業務データが単一ストレージデバイスから復元できる場合には、完全消去後(消去できない場合は物理的に破壊後)にのみ機構外への持ち出しを認めることがあるため、担当職員の承認を得ること。
(イ)NITE-LAN システムを構成するサーバ並びに事務用 PC 及び運用管理用 PC(アプライアンス製品は除く。)で使用したストレージデバイスについては、契約終了時に、使用した領域の完全消去を行うこと。クラウドサービス等を利用し、ストレージデバイスが特定できない場合には、クラウドサービス上のサービス等で NITE-LAN システムとして登録した情報を完全に消去すること。
(ウ)上記以外の NITE-LAN システムで使用したストレージデバイスについては、機構外部へ持ち出す場合及び契約終了時には、設定情報及びログ情報の消去を行うこと。

(7) 構築時のセキュリティ対策

ア. NITE-LAN システム構築にあたり、セキュリティ要件を「セキュリティ共通設計書」として定め、提出すること。

イ. 納品時には、すべてのサービスについて脆弱性検査を行い、問題が発見された場合は、是正した上で納品すること。

ウ. 各サービスのセキュリティリスクとそれに対する対応策を明示すること。

(8) セキュリティ監査

ア. 機構の情報セキュリティポリシーに基づき実施されるセキュリティ監査を受けること。

なお、監査項目は、各年度のセキュリティ監査計画に基づき、機構の監査実施者と受注者の協議の上、決定する。

イ. セキュリティ監査の結果、指摘事項があった場合、監査人による改善提案等に基づき、担当職員と協議の上、改善案の作成及び改善を行うこと。

(9) 第三者チェック

ア. サービス提供開始前に、第三者からのセキュリティチェックを受けること。

イ. 第三者から NITE-LAN システムが「情報システムの特性を鑑み、システムの運用上重要な影響を与える脆弱性は無いと合理的に判断される」、「情報システムの特性を鑑み、システムの運用上重要な影響を与える脆弱性を回避するための設計が行われていると合理的に判断される」等の報告を受けるまで、設定の変更とセキュリティチェックを繰り返し行うこと（合理的な判断の基準としては、例えば発見された脆弱性が、高、中、低の 3 段階に分けられていた場合、高及び中の脆弱性は存在しないこと、低の脆弱性に関しては DMZ セグメントに配置されたサーバか内部セグメントに配置されたサーバかの違い、脆弱性の除去にかかる費用等を総合的に考慮して脆弱性は回避されていると考えられること、等の基準が考えられる。また、最終判断は機構デジタル監情報統括課情報システム基盤・支援室長、リスクマネジメント推進統括官リスクマネジメント推進室のセキュリティ担当の職員、受注者及びセキュリティチェックを行う第三者の打合せに基づくものとすることが可能である。）。

ウ. 受注者はセキュリティチェックを行う第三者を自ら選定するが、第三者は受注者の「財務諸表等の用語、様式及び作成方法に関する規則（昭和 38 年大蔵省令第 59 号）第 8 条」に規定する親会社及び子会社、同一の親会社を持つ会社並びにその役員及び従業員以外とすること。

エ. セキュリティチェックを行う第三者として、経済産業省のシステム監査企業台帳又は情報セキュリティサービス基準適合サービスリストに登録されている者を選定すること。

オ. セキュリティチェックを行う第三者として、社内に情報セキュリティ対策等に関する役務提供を専門とする部門を有しているか、又は情報セキュリティ対策等に関する役務提供を専門とする事業者を選定すること。

カ. セキュリティチェックの内容を検討する主担当者の少なくとも 1 名は、経済産業省が実施しているシステム監査技術者試験又は情報処理安全確保支援士試験に合格している者であるか、公認情報セキュリティマネージャーCISM(Certified Information Security Manager)、セキュリティプロフェッショナル CISSP（Certified Information Systems Security Professional）又はセキュリティ認定プラクティショナーSSCP（Systems Security Certified Practitioner）のいずれかの資格を有している者とすることを条件にセキュリティチェックを行う第三者を選定すること。

キ. セキュリティチェックを行う第三者として、過去 3 年以内に、官公庁又は独立行政法人の情報システムに対し脆弱性検査業務を 2 件以上実施した実績がある者を選定すること。

12. リモートアクセスサービス

インターネットを経由し、機構内の資源の利活用が可能なセキュアな通信サービスを提供すること。リモートアクセスサービスは、個別業務システム及び各一般業務システムの移行事業者や運用保守事業者が、リモート運用保守を行うためにも用いる。そのため、「2. 契約期間及びスケジュール概要」に記載されているサーバ等の利用開始日には、当該サービスが利用可能であること。

(1) 基本要件

リモートアクセスサービスの利用者数は835人とし、全利用者の同時接続に対応できること。1Gbps相当の最大スループット性能を有していること。

(2) 機能要件

ア. 国内外を問わず、インターネット経由で NITE-LAN システムにアクセスできること。ただし、通信費用を含め受注者が全ての費用を負担する場合には、インターネット以外の閉域接続網を用いて NITE-LAN システムにアクセスする方式でもかまわない。閉域網により十分な機密性が担保される場合には、「(3)セキュリティ要件」において求めている VPN による暗号化は要さない。

イ. アクセス可能なサーバを、サーバ側の IP アドレスを用いて制限できること(機構外からアクセス可能な情報の選別は、業務の特性、情報の内容を鑑み、各情報の責任者が個別に判断することから、各サーバで保持されている情報の責任者が機構外からのアクセスを認めたサーバにのみ機構外からアクセスできるようにすること。どのサーバへのアクセスを可能とするかは、機構から受注者に一覧を提示する。)。

ウ. アイドル状態が続いた場合には自動的にセッションを切断するための時間設定ができること。

エ. セッション接続時間内であれば、回線接続が切れた場合には、回線接続が復旧した際に再認証不要で自動的に再接続されること。

オ. 事務用 PC から利用できること。

(3) セキュリティ要件

ア. 暗号化された通信を用い、安全なリモートアクセス(VPN)が実現できること。

イ. VPN 接続時の認証は、生体認証等による OS へのログインに加え、端末に保持された秘密鍵、ログインごとに有効なワンタイムパスワード、マトリックス認証等を利用した 2 要素以上の認証方式を講じること。必ずしも知っていることに追加して何かを持っていることを確認する二要素認証ではなくてもかまわない。

ウ. VPN 接続時の生体認証等に加えて実施される認証は、端末に保持された秘密鍵を利用する等、利用者が入力する必要がない方法であることが望ましい(その場合総合評価において加点する。)。

エ. 使用する暗号方式は、入札時点で CRYPTREC が公表する電子政府推奨暗号リストに掲載されている方式を採用すること。また、証明書鍵長は 2048bit 以上に対応し、通信鍵長は 128bit 以上に対応可能であること。
なお、NITE-LAN システムの運用中に当該暗号方式が危殆化した場合は、製品機能の範囲で、より強度な暗号方式を取り入れて運用すること。

オ. 暗号化で使用する暗号鍵については、定期的、セッション単位等の方法による変更ができること。

カ. 受注者が運用管理を行っていない端末において、VPN 装置等で OS やブラウザのバージョン、パッチの適用状態、マルウェア対策ソフトの稼働状況等の検疫を行い、汚染された端末からのアクセスを制限すること。

キ. 事務用 PC のネットワークアクセスは、NITE-LAN システムを経由したものに限定できること(NITE-LAN システム以外のネットワークに接続した際には、NITE-LAN システムの VPN 装置の IP アドレスにのみアクセス可能なこと。ただし、VPN 接続ができない場合に、エラー表示が継続されないこと。)。

ク. 個別業務システム及び一般業務システムの移行事業者及び運用保守事業者からのアクセスについては、アクセス可能なサーバを限定する等のアクセス管理を行うこと。

13. 運用管理サービス

運用管理とは、各サービスを正しく提供する過程で必要となるマネージメント機能である。ITILが定める管理プロセスと機能に準拠し、以下の機能を提供すること。

(1) 基本要件及びサービスの改善

ア. 基本要件

(ア)受注者は、運用管理サービスを提供するために、運用管理責任者を配置すること。また、運用管理責任者は、機構のシステム運用担当者と調整し、適切な運用管理に努めること。

(イ)受注者は、「参考 08. 運用保守作業一覧」をベースとして、運用管理サービスにおける活動の詳細を、サービス開始前に担当職員と協議の上、定義し、運用管理サービス仕様書(「5. (7)ウ. (カ)運用マニュアル」に含まれる。)として、提出すること。また、記載内容に変更があった場合には、都度更新し、提出すること。
なお、機構としては、運用保守について、機構開庁時間に専従する作業員が3人程度で実施可能な作業量と想定している。

(ウ)受注者は、「5. (7)エ. (ウ)作業報告書」として提出する作業報告の対象範囲を明確にすること。

(エ)受注者は、NITE-LAN システムにおける運用管理、保守内容を月次で「5. (7)ウ. (ア)月次定期報告書」の「運用報告」として提出し、報告すること。

(オ)各サービスの停止に備え、あらかじめリカバリ対策を設計し、迅速なサービス復旧を実施すること。

(カ)サービス提供期間中、各サービスのログを「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」の「10.10 監視」に基づき取得、保管し、機構の要求に応じて提供すること。
なお、対象のログについては、担当職員と協議の上、決定すること。ただし、情報漏えい等事案が発生した際に、証跡の確認に必要と考えられる情報は必須とすることを想定している。

(キ)上記のログは、最低でも直近 1 年間分を常時参照できるようにすること。それより過去のログについては、CSV 形式等により SSD 等の記録媒体に保存し提供するか、クラウド環境で機構の要求から 24 時間以内に提供可能なように保管すること。なお、24 時間以内の提供とは技術的な仕様を求めているもので、抽出作業を行うことを求めたものではない。

(ク)上記のログは、サービス提供期間終了後少なくとも 1 年間は機構がアクセス可能なよう対応すること。(キ)において、クラウド環境で保管する場合は、サービス期間終了後に導入する次期システムの要件に当サービスで収集したログの保管及び管理する環境を用意し、システム移行時の移行データの対象とするため、移行が容易であることを念頭に設計すること。

(ケ)NITE-LAN システムの運用設計に際しては現行システムの運用方式等を考慮すること。

(コ)サービス構築を担当した要員は、運用管理を担当する要員に対して、サービスが円滑に提供されるよう詳細な引き継ぎを行うこと。

(サ)サービス構築を担当した要員のうち構築したサービスを子細に理解している要員が、運用管理に移行した後であってもサービスの円滑な提供に貢献できるよう体制を構築することが望ましい(その場合総合評価において加点する。)。

(シ)システム運用担当者に、ITIL4 ファンデーションの資格を有する者が含まれることが望ましい(その場合総合評価において加点する。)。

イ. サービスの改善

(ア)受注者は、日々の運用業務の中で発生した運用上の課題について改善提案を行うこと。これは「15. SLA(サービスレベルアグリーメント)」に記載されているサービスレベルの向上を求めるものではない。

(2) サービスレベルの維持管理

ア. 受注者は、各サービスの監視、測定等を行い、「15. SLA(サービスレベルアグリーメント)」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。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。

イ. 特に、収集する脆弱性情報の情報源の範囲、業務に即座に影響があるか否かの判断基準について、担当職員と協議の上、決定すること。

ウ. サービス提供開始時点から 3 か月間は運用保守作業の調整期間とし、4 か月目から SLA 遵守の対象とする。

エ. SLA を満たせない可能性がある場合、速やかに機構のシステム運用担当者に報告すること。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。

オ. SLA を満たすことができなかった場合には、その原因を分析し、改善計画をシステム運用担当者に報告し、システム運用担当者の承認を得ること。合理的な理由がある場合には、サービスレベルの見直しを行う。

カ. 各サービスの稼働率を保証する為、リスク分析、テスト要件への盛り込み、冗長構成の精査等を十分に考慮しサービス停止を予防すること。

(3) サービス利用の支援

ア. インシデントの対応

(ア)障害に対して、迅速なサービスの復旧を行うこと。

(イ)質問、相談に対して、的確に回答すること。

(ウ)サービス要求に対して、以下の作業を実施すること。

①あらかじめサービス要求に対する手順を担当職員と協議し「5. (7)ウ. (カ)運用マニュアル」に記載すること。
②前述①の手順に従い、サービス要求に対応すること。

イ. 障害の再発防止

(ア)サービスの復旧後、障害の根本的な原因を解明し、恒久的な対策を実施すること。
(イ)障害の恒久的な対策には、利便性、信頼性、拡張性、セキュリティ等を十分に検討すること。

(4) 各サービスの管理

ア. 各サービスの運用実績を常に把握し、各サービスの提供に必要な対応措置を取ること。

イ. 各サービスのシステム資源をインベントリ収集及び棚卸等により、正確に管理すること。

ウ. 各サービスのシステム資源のパフォーマンスとキャパシティを定期的に測定し管理すること。

なお、キャパシティを管理することで、各サービスのシステム資源のパフォーマンスを保証すること。

(5) その他

ア. バックアップ／リカバリ

災害、システム障害、利用者の誤操作等のトラブルからのサービス復帰、損失データの復旧を目的として、バックアップ/リカバリを行うこと。

(ア)バックアップ共通要件

①バックアップ対象は、以下に示す各サービスのシステム領域及びデータ領域とする。D2D、D2C方式等最適な方式によりバックアップの取得を行うこと。ただし、サービスをクラウド環境で構築する場合において、サービスレベルが99.9%以上確保できるサービスについては対象外としてよい。

・「8. 業務サービス」の(6)Web会議サービス等、(7)在籍表示サービス、(8)機構外からの電子メール及びスケジューラ利用サービス、(9)事務用PCサービス、(12)複合機サービス、(15)コンテンツアップロードサービス以外のサービス

・「9.IaaSサービス」のサービス

②データ領域のバックアップについて、「8. (5)ファイルサーバサービス」は、現行データとは別に2週間分を、その他のサービスは現行データとは別に3日分を保管すること。なお、保管についてはフルバックアップ、差分バックアップ等を用いて、最適な方法で提供すること。

③サービスを停止することなくバックアップの取得を行うこと。

④オープン中のファイルもバックアップできること。

⑤バックアップが失敗した場合、バックアップ処理をリトライすること。また、バックアップの失敗はインシデントとして処理すること。

⑥バックアップの結果は、月次にて取りまとめ、「13. (1)ア. (エ)運用報告」として機構のシステム運用担当者へ報告を行うこと。

⑦保守業務等のため、上記バックアップとは別な手法でのバックアップが必要な場合、安全性、信頼性を十分考慮した装置、手法について担当職員に説明し、承認を得たうえでバックアップを実施すること。

⑧日次バックアップを基本とし、バックアップ頻度については担当職員と調整すること。

⑨保管世代数については、週を世代とした2世代を基本とし、担当職員と調整すること。全世代を即時に参照できる必要はなく例えばテープ等を利用しても良い。テープで保管する場合、機構が提供する本所に存在する耐火金庫に保管してもよい。

⑩⑨でテープにより保管する場合、今後業務継続計画の実現のため、本所で取得したバックアップデータを大阪事業所にレプリケートする可能性がある。そのために必要な稼働環境の構築、運用作業等についての契約変更に応じること。

(イ)災害時対応要件

①災害による損失データの復旧は、前述「(ア)②」にて取得したバックアップを用いること。

②サービス切り替え手順に基づくサービスの切り替え、復旧手順に基づく復旧を行うに際し、システム設定、データ内容に齟齬を生じさせないための措置を講じること。

③災害時対応システムから通常のサービスに戻す手順について、担当職員と協議し、決定すること。

④(ア)のバックアップをテープで行う場合において、今後業務継続計画の実現のため、本所で取得したバックアップデータを大阪事業所にレプリケートするよう契約変更した

場合には、前述「(ア)②」にて取得したバックアップが用いられない場合に前述「(ア)⑩」にてレプリケートしたデータを用いることとする。

(ウ)システム障害時要件

①システム障害による損失データの復旧は、前述「(ア)①」にて取得したバックアップを用いること。

②リカバリ対策に基づきサービス中断の事後対策を行うこと。

イ. ドキュメント管理

NITE-LANシステムで作成されたドキュメントは、すべて構成管理を行うこと。受注者は、ドキュメントに修正が必要な場合、更新履歴と修正ページ、修正箇所を明らかにし、担当職員に提出すること。

ウ. ドメイン名の維持

受注者は、契約期間に渡り、機構のドメイン名（NITE.GO.JP、NITE.JP、製品評価技術基盤機構.JP及びナイト.JPの4ドメイン名）の維持（更新手続き、費用支払等）を行うこと。

保有ドメイン名	有効期限
NITE.GO.JP	2024 年 11 月 30 日
NITE.JP	2024 年 4 月 30 日
製品評価技術基盤機構.JP	2024 年 5 月 31 日
ナイト.JP	2024 年 5 月 31 日

14. 保守

(1) 保守の目的

受注者は、「15. SLA(サービスレベルアグリーメント)」で定める各サービスの稼働率及び障害復旧時間等を保証するため、保守業務を実施すること。具体的な保守の作業内容については、「参考08. 運用保守作業一覧」 を参照すること。

(2) ITサービスマネジメント

運用管理サービスのサービスサポート、サービスデリバリを支援すること。

(3) 保守

ア. スケジュール

事前に予定される保守業務は、「5. (7) エ. (イ) 年間保守スケジュール」として提出すること。

イ. 作業時間

機構内で実施される保守作業は、機構開庁時間とするが、SLA遵守等の理由により、その他の時間帯での保守作業の場合は事前に担当職員と調整すること。

冗長化されている機器のハードウェア故障の修理は、機構開庁時間に行うことを想定している。

ウ. 機器対応

(ア)機構内に設置した機器に対し、計画された停復電時に必要な措置を講じること。
(イ)受注者は、サービスレベルを維持するため、機構内に設置した機器の障害時には、オンサイト対応をすること。
(ウ)PC の障害時はピックアップでの対応も可能とする。箱詰め、発送等の対応は機構で実施するが、配送用の箱、緩衝材等は提供すること。ただし、バッテリの膨張など配送に危険があるなどピックアップに適さない故障の場合は、オンサイトでの対応が必要となる。
(エ)要件を満たすために必要な性能を維持できなくなった機器がある場合は、無償で交換すること。
(オ)要件を満たすために必要と設計時に見込んだ性能が達成できなくなった場合には、無償で交換等の対応を行うこと。

15. SLA（サービスレベルアグリーメント）

(1) 基本方針

運用業務における継続的なサービス要件を、「参考09. サービスレベル合意書(案)」に示した水準を下限として、SLAとして定める。「参考09. サービスレベル合意書(案)」に示した水準を満たすことができない合理的な理由がある場合には、担当職員と協議し、サービスレベルを機構と合意すること。SLAを満たすことが可能なようNITE-LANシステムの設計構築を行い、NITE-LANシステムの運用管理においては、「13. (2)サービスレベルの維持管理」に基づき、SLAを順守するための対策を講じること。また、SLAを順守できなかった場合には、対応策について検討し、担当職員の承認を得た上で実施すること。

16. 契約条件等

(1) 業務の再委託

ア. 受注者は、機構の許可無く作業の一部を第三者に委託し、又は請け負わせてはならない。このときの第三者には、関連事業者(「財務諸表等の用語、形式及び作成方法に関する規則」(昭和 38 年大蔵省令第 59 号)第 8 条に規定する親会社及び子会社、同一の親会社を持つ

会社並びに委託先事業者等の緊密な利害関係を有する事業者をいう。）も含むものとする。

イ. 一部の業務を再委託する場合、再委託先にも本仕様書で定める受注者の責務を負わせる契約を締結すること。

ウ. 再委託先に業務を請け負わせる場合、当該業者の全ての行為及びその結果についての責任を受注者が負うこと。

エ. 再委託先には最高情報セキュリティアドバイザーが現に属する事業者又は過去 2 年間に属していた事業者及びその関連事業者（『財務諸表等の用語、形式及び作成方法に関する規則』（昭和 38 年大蔵省令第 59 号）第 8 条に規定する親会社及び子会社、同一の親会社を持つ会社並びに委託先事業者等の緊密な利害関係を有する事業者をいう。）が含まれないこと。

オ. 再委託先との契約は、日本法を準拠法とし海外の法律の適用が行われないこと。

(2) 知的財産権の帰属等

ア. 本役務の履行に当たって生じた著作物の著作権（著作権法（昭和 45 年法律第 48 号）第 21 条から第 28 条までに定める全ての権利を含む。以下同じ。）は、機構に帰属するものとする。ただし、第三者の既存著作物の利用に関しては、その著作権の帰属を明確にすること。受注者は機構に対して著作人格権を行使しないものとする。

イ. NITE-LAN システムのサービス役務提供にあたり、特許権、実用新案権、意匠権、商標権等の日本国及び日本国以外の国の法令に基づき保護される第三者の権利（以下「特許権等」という）の対象となっている意匠、デザイン、設計、施行方法、工事材料、維持管理方法等を使用した結果生じた一切の責任は、受注者が負うものとする。

(3) 機密保持

ア. 受注者は、調達に係る作業を実施するに当たり、機構から取得した資料（電子媒体文書、図面等の形態を問わない。）を含め契約上知り得た情報を、第三者に開示又は本調達に係る作業以外の目的で利用しないものとする。ただし、次の①から⑤のいずれかに該当する場合は除くものとする。

①機構から取得した時点で、既に公知であるもの
②機構から取得後、受注者の責によらず公知となったもの
③法令等に基づき開示されるもの
④機構から秘密でないと指定されたもの
⑤第三者への開示又は本調達に係る作業以外の目的で利用することにつき、事前に機構に協議の上、承認を得たもの。

イ. 受注者は、機構の許可なく取り扱う情報を指定された場所から持ち出し、若しくは複製しないものとする。

ウ. 受注者は、本調達に係る作業に関与した受注者の所属職員が異動した後においても、機密が保持される措置を講じるものとする。

エ. 受注者は、本調達に係る検収後、受注者の事業所内部に保有されている本調達に係る機構に関する情報を、裁断等の物理的破壊、消磁、その他復元不可能な方法により、速

やかに抹消すると共に、機構から貸与されたものについては、検収後１週間以内に機構に返却するものとする。

(4) 納品物

ア. 納品成果物の電子ファイルは、原則日本語で作成しMicrosoft Office 365を使って内容を確認できる形式とする。

イ. 納品成果物の電子ファイルを納入する場合には、あらかじめウイルスチェックを行い、ウイルス感染の問題がないことを確認した後に担当職員に提出すること。

ウ. 納品成果物を書面やメディアで提出するものについては、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）」第６条による「環境物品等の調達の推進に関する基本方針」に定められている品目については、その基準を満たすこと。ただし、上記の基準を満たすことが著しく困難な場合においては、事前に担当職員の承諾を得た上で納入することができる。

(5) 契約不適合責任

本役務に係る納品成果物については、担当職員が契約不適合の事実を知った時から1年以内に、担当職員から問い合わせを受けた場合、速やかにその原因を究明し、担当職員に報告するとともに、その原因の所在が受注者にある場合、受注者の責任において対策を講じること。また、それに要する費用も受注者でまかなうこと。

なお、契約不適合により第三者に与えた損害については、すべて受注者の責任において処理解決するものとする。

(6) 情報セキュリティにかかる資格・認証等

応札者は、ISMS適合性評価制度又はプライバシーマーク使用許諾の認証を取していること。ただし、ISMS適合性評価制度の認証については、作業者の所属部門が対象となっていること。

(7) 関係者との調整

関係者として、現行事業者、WAN回線事業者、各業務システムの担当事業者、工程監理支援事業者が想定される。プロジェクトを円滑に進めるため、各関係者との調整を行うこと。

以上