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

※本仕様書は、予告なしに修正又は訂正する場合があります。
その際は、当機構ホームページ上にて仕様書の修正又は正誤表
等を公示いたしますので、必ず、ご確認下さい。

独立行政法人製品評価技術基盤機構
情報システム課

平成30年1月16日

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、平成30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 28 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 920 台の端末（約 790 台のノート型の一般事務用 PC、約 80 台のデスクトップ型 PC（課室共用 PC）及び約 50 台のモバイル PC）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

利用者の利便性向上、情報共有の推進、統合未済の情報システムのNITE-LANシステムへの統合を進める。具体的には、NITE-LANシステム最適化計画（平成20年3月31日運営会議決定、平成28年10月改定）の「3 最適化の実施内容」のうち、本調達では以下を実現する方針である。

ア. ロケーションフリーの業務環境の整備

(ア)長期出張・在宅勤務等に対応可能な環境の整備

機構外に持ち出した一般事務用PCから、メール、イントラ、ファイルサーバのみならず、一般管理システム（人事給与システム、文書管理システム、財務会計システム）等についても一部機能について機構外からのアクセスを可能とし、長期出張時の申請や決裁の遅延等を防止、業務の効率化を図る。また、通信品質が優れない場合にもできるだけ安定して機構内ネットワークへアクセスできるようにすることにより、機構内外からアクセスできる情報の格差を可能な限り縮小させ、出張時、在宅勤務時等に機構内と同等の業務遂行の実現を可能にする。

ただし、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ものとする。

(イ)印刷負担の軽減、会議の効率化・迅速化

打ち合わせ・会議等では、持ち込んだ一般事務用PCで電子ファイルを閲覧することにより、紙媒体での資料配布を減らし、会議資料の紙代のみならず、資料準備、廃棄に要する人的コストの削減を図る。これにより資料反映の即時性の向上も期待される。

具体的には、無線で会議室のディスプレイまたはプロジェクタに容易に一般事務用PCの画面を表示できるようにすることにより、会議室ディスプレイの利用に要する負担を軽減する。

(ウ)試験・実験時の効率向上

試験室、実験室に必要に応じて無線LAN環境を整備することにより、試験、実験時の業務を効率化する（試験の待ち時間中にメールの確認を行う、ファイルサーバのデータを参照することで実験結果の確認を効率的に実施する等）。

イ. 業務効率化の推進

(ア)グループウェアを活用した、情報共有の推進

センター・課室の垣根を越えた情報共有の実現を目的とし、グループウェア内にユーザ個人で任意にアクセス権限を設定出来るソーシャル・コラボレーション機能を持たせる。これらの機能は現行システムのグループフォルダの代替機能として活用することのみならず、ファイルの版管理による未整理ファイルによる容量増大の低減、さらにはファイル以外にコメントや時系列等の情報を併せて持つことができるため、関係者への経緯の共有が円滑に行える。また、本質的に「1対1コミュニケーション」のツールであるメールでは難しかった正式な履歴として情報が蓄積されることによる、ナレッジとしての活用が期待できる。

また、グループウェア内のファイル共有機能は、審議会等の外部の方が機構内で会議を行う際に配布資料を削減するための資料参照等の目的にも活用する。

(イ)電子メールとスケジューラ・タスク管理機能の連携強化

電子メールとスケジュールを一体のグループウェア機能として連動させ、メール連絡から容易にスケジュールを登録できるようにする。また、他部署・他者に作業等を依頼する際に、メールとは別途グループウェアのタスク管理機能を用いて期限等の確認・管理ができるようにする。

(ウ)メーリングリストアカウントでの送信解禁とセルフサービス化

メーリングリストアカウントでの送信を解禁することにより、窓口業務効率化や一括大量送信時のメール誤送信防止を図る。さらに、これまで情報システム課で実施してきたメーリングリスト作成や更新等の設定作業についてはユーザーフレンドリーなUIを用意することにより職員自身により行う。作成や変更の承認についても情報システム課長による内容の精査を含まないことから、職員の所属長のみが行うことにより、変更内容の反映の迅速化を実現し利便性を向上させ、併せてシステム運用の効率化を図る。

(エ)外部との間でも利用可能なWEB会議の導入

外部とも接続可能なWeb会議システムを一般事務用PCに導入することにより、国内外、機構内外のユーザ及び接続環境を問わないWeb会議が開催可能となる。さらに、従来のテレビ会議システムでは難しかった参加者との資料共有が可能となることから、より円滑なコミュニケーションを実現する。

ウ. 情報資源の最適な配置

(ア)端末の共通仕様化

現行システムで仕様が異なる一般事務用PC、課室共用PC、モバイルPCを可搬に適したモバイルPCもしくはタブレット端末に一元化し、一般事務用PCの機構外持ち出しを可能とする運用を行うことにより、モバイルPCの台数削減を図る。さらに単一仕様となるため、運用管理面の効率化も見込まれる。通信環境の無い地域で使用することも多いため、一般事務用PCのハードディスクを暗号化し、一般事務用PC内に情報を保存して持ち出すことも可能とする。

エ. 継続的研修啓蒙周知の実施等による NITE-LAN システムの利用促進

NITE-LANシステムの導入時のみでなく、継続的にNITE-LANシステムの利用方法、活用方法に関する研修、啓蒙を継続し、ワークスタイルの変革にむけて継続的な取り組みを行う。具体的には、先進的な利用方法について紹介するセミナー等を通年的に実施する。

会議の日程調整の業務効率化のため、会議への参加が不可な日時の機構全体のスケジューラへの登録を必須とする。

オ. さらなるセキュリティの強化

(ア)標的型攻撃メールへの対応、パケットデータ収集の充実

標的型攻撃に対し、シグニチャーベース以外のセキュリティ対策ソフトの端末への導入等により対策強化を図る。また、対策製品を連携させることによる感染事象の早期の発見、感染源の特定、拡散の抑制を目指す。さらに、ログの収集に加え、ネットワーク上のパケットデータ収集等の充実によりインシデント発生後の事態終息の迅速化を実現可能とする。

(イ)パソコン持出時の情報漏えい対策の確保

職員には基本的に端末に機密情報を保存させないルールの徹底を図ることに加え、ハードディスクの暗号化、リモートワイプ等の技術的対策によりパソコン紛失時の情報漏えいリスクを低減させる。

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で、製品評価技術基盤機構共通基盤情報システム以外のもの
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
現行システム	平成26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、平成31年3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（平成35年3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	国際評価技術本部（大阪市）、認定センター（大阪市）、製品安全センター（大阪市）、化学物質管理センター（大阪市）及びバイオテクノロジーセンター（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

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、導入支援教育並びに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（平成30年5月上旬予定）～平成35年3月31日

ア. 設計・構築・移行期間：契約日～平成 31 年 2 月 28 日

イ. サービス提供期間（有償期間）：平成 31 年 3 月 1 日～平成 35 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. PRTR AP 仮想サーバ：平成 30 年 12 月 14 日から利用可能とすること。

プライベートクラウドについては、「参考17. 作業分担一覧」に示す工程を想定している。別途移行作業が必要となるため、PRTR AP仮想サーバは、平成30年12月13日までに構築・テスト工程を終了し、平成30年12月14日から引渡し工程を実施できるようにすること。

イ. PRTR DB 仮想サーバ：平成 30 年 12 月 14 日から利用可能とすること。

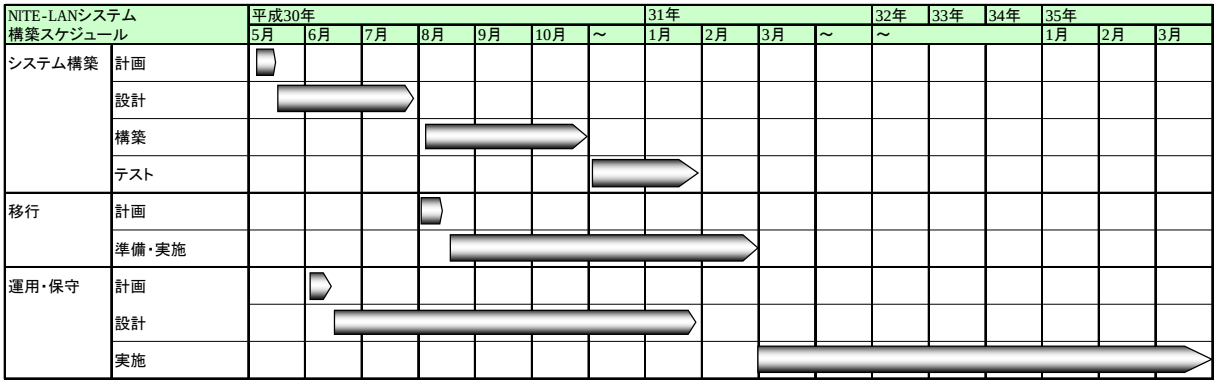
PRTR DB仮想サーバは、平成30年12月13日までに構築・テスト工程を終了し、平成30年12月14日から引渡し工程を実施できるようにすること。

ウ. その他のプライベートクラウドサービス：平成 31 年 1 月 7 日から利用可能とすること。

PRTR AP仮想サーバ及びPRTR DB仮想サーバ以外のプライベートクラウドサービスは、平成31年1月6日までに構築・テスト工程を終了し、平成31年1月7日から引渡し工程を実施できるようにすること。

エ. グループウェアサービス：平成 31 年 1 月 7 日から利用可能とすること。

グループウェアサービスは、平成31年1月6日までに構築・テスト工程を終了し、平成31年1月7日から移行作業が実施できるようにすること。



図表１　作業スケジュール案

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

平成29年1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800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、900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庁における平成 28・29･30 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。拠点間を結ぶ広域 Ethernet 回線又は IP-VPN 回線は別途調達する。

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。
なお、ガイドライン等を活用した設計、構築、運用に努めること。

カ. 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。

キ. 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、以下の分野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。

(ア)IC カード(カード本体は調達必須ではない。)
(イ)ファイアウォール
(ウ)サーバ OS
(エ)デジタル複合機
(オ)IDS、IPS、WAF
(カ)データベース管理システム(DBMS)

ク. NITE-LAN システムで提供される全てのサービスに対して、サービス提供開始日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、機構企画管理部情報システム課担当職員（以下「担当職員」という。）と協議の上、実施すること。

ケ. 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。

コ. 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。

サ. 機構が指定した様式のラベルを作成し納品物の機器に貼付すること。

シ. 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。）。

ス. 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った場合、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。

セ. 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。

ソ. サービス契約終了後、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。

タ. 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。

チ. 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、運用に努めること。また、各サービスにおいて、他のサービスの負荷の影響により性能低下が発生しないこと。

なお、パフォーマンス維持、セキュリティ維持、障害復旧時間の短縮及び拡張性維持が可能であれば、サーバの仮想化技術等を用いて、サーバの役割の共存、共有を積極的に実施すること。

(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サービス（事務用 PC サービス、複合機サービス等）は継続できること。

(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21. 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. 受注者は落札後 10 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」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、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. 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。

キ. 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」で指定する場所に設置すること。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、設置機器の移動にかかる費用は、本調達に含まない。

ク. サービスの提供に必要な機器は、リモート監視及びリモート運用に用いる機器を除き原則機構内に設置するものとし、機構外のデータセンター等への設置は行わないこと。ただし、クラウドセキュリティ推進協議会の「クラウド情報セキュリティ監査制度」において、ゴールドマーク又はシルバーマークを取得している場合には、政府共通 NW 経由で利用されるシステム（「参考 04. 課室所管情報システムの移行に係る要件」の No.15 の特定化学物質管理用情報システム及び No.18 の 3 省共同化学物質データベースシステム（3 省 DB 内部版））において利用される機器を除き、機構外に設置することも可能とする。また、ファイアウォール、DNS 等の外部との通信の中継に係る装置、セキュリティチェック等のために一時的にデータを処理する装置については、ISO/IEC27017 の認証を取得しているか又は同等のマネジメントシステムを確立している事業者のサービスを用いる場合、機構外に設置することも可能とする。ASP 等の機構外に設置した機器を用いるサービス提供の方式を用いる場合には、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。また、海外に設置されたサーバ、ストレージ等を使用する ASP 等は利用しないこと。機構と機器が設置されたデータセンター等間の通信回線（必要となる帯域を有する通信回線）を含めてサービスを提供すること。

ケ. 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、平日の 19 時以降又は休日とする。ただし、担当職員の許可を得た場合には立ち入ることができる。

コ. 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。

サ. 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。

シ. 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。

ス. 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。

(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. （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。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22．サーバルーム概要図」を参照すること。

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) 納入形態

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、必要に応じ耐震又は免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 3 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 3 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. 納入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入すること。

(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)プロジェクト管理者は、担当職員の指示のもと、状況に応じ工程管理支援業者の支援を受けること。

(オ)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。
(カ)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。
(キ)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。
(ク)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。
(ケ)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。
(コ)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。
(サ)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。
(シ)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。その場合、受注者は、代替要員を 2 週間以内に選任し、担当職員の承認を得ること。
(ス)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。
(セ)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。
(ソ)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)「9. プライベートクラウドサービス」の設計・実装の担当者又は管理者は、仮想化ソフトベンダが提供する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。)。資格は、NITE-LAN システムで採用する予定の仮想化ソフトに関する資格に限らないものとする。
(イ)「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。)。
(ウ)「11. セキュリティ対策」の設計・実装の担当者又は管理者は、情報セキュリティスペシャリスト(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。)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。)。

(7) 納入ドキュメント

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. 受注者は落札後早い段階で、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」に必要となるドキュメント
(イ)システム概要構成図
(ウ)ネットワーク構成図
(エ)セキュリティ共通設計書

(オ)機器諸元表(機構内に設置する機器に限る。)
(カ)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)
(キ)導入計画書(導入手順、導入体制、導入スケジュール)
(ク)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)
(ケ)教育計画書(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)
(コ)他システム向け接続仕様書

イ. 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
(カ)運用マニュアル
(キ)操作マニュアル
(ク)研修用テキスト
(ケ)e ラーニングコンテンツ

ウ. 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)

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、エンド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・eラーニングコンテンツ

ア. NITE-LAN システムの操作マニュアル、研修用テキスト及び e ラーニングコンテンツ（教材及び理解度テスト）を提供すること。

イ. 研修用テキスト及び e ラーニングコンテンツには、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、研修用テキスト及び e ラーニングコンテンツは、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 システム利用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ファイルに綴じた状態で、拠点ごとに一部提供すること（ただし、オンライン

マニュアルのみの提供の場合はこの限りではない。)。

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、PDF 形式であること。

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 3 者が著作権を有する著作物を原則含めないこと。

コ. 研修用テキストに機構の内部利用のための複製を制限することになる第 3 者が著作権を有する著作物が含まれる場合には、複製にあたり必要となるロイヤルティ契約を機構と締結し、有償で複製できるようにすること。

サ. e ラーニングコンテンツは、職員が NITE-LAN システムの利用方法について独自学習できるものであること。

シ. e ラーニングコンテンツは、Flash、Java applet、Adobe Reader、Windows Media Player 等以外の独自のプラグイン、アプリケーションソフトウェア等をインストールすることなく利用できるものであること。

ス. e ラーニングコンテンツは、事務用 PC において利用できるものであること。

セ. e ラーニングコンテンツは、SCORM1.2 又は SCORM 2004 準拠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。)。

ソ. e ラーニングコンテンツは、「8.（18）ラーニングマネジメントシステムサービス」において利用できること。

(3) 教育研修設備等

ア. 教育研修のみに用いる機器については、受注者において用意すること。研修に用いる端末は事務用 PC を利用することができる。

イ. 研修開始日から研修に必要な機材として、事務用 PC の画面を表示可能な液晶プロジェクタ 1 台及び専用のスクリーン 1 面を本所の機構が指定する場所に準備すること。

ウ. 液晶プロジェクタは、ANSI ルーメン値 2,500 以上の光量を有すること。

エ. 液晶プロジェクタの解像度は、1,280×800 ピクセルに対応していること。

オ. 液晶プロジェクタの本体重量は、10kg 以下であること。

カ. 液晶プロジェクタは、液晶プロジェクタと PC を接続するためのケーブルを備えていること。

キ. 専用のスクリーンは、100 型（インチ）以上の大きさであること。

ク. 液晶プロジェクタは、専用のワイヤレスリモコンを備えていること。

ケ. 契約期間中は、「参考 10. 拠点別導入予定式数」に記載の台数とは別途、本所に研修機材として、インストラクタ用の端末を 1 台準備すること。

コ. 研修場所の電源配線及び LAN 配線は、研修開催の都度敷設作業を事前に行い、研修終了後撤去作業を行うこと（ただし、機構企画管理部情報システム課長（以下「情報システム課長」という。）が常時敷設を認める場合はこの限りではない。)。LAN 配線は、NITE-LAN システ

ムのクライアントセグメントに接続すること。

サ. 各研修において、担当職員が設定する研修日程を確実に実施できるインストラクタを確保し、研修場所に派遣すること（インストラクタの派遣人数は、受講者が 10 名以下の場合は 1 名、11 名以上の場合は 2 名を基準とする。）。

シ. 教育研修に用いるのに適した物理的な特性及び研修に必要なソフトウェアが利用できるノート型の端末（研修用ノート端末）を 40 台提供すること。
なお、当該端末の台数は事務用 PC の台数に含まれるもの（内数）とする。

(4) 移行前研修

ア. 教育研修は、必要に応じて各拠点にて実施すること（可能な場合にはテレビ会議システムを用いることもできる。）。

イ. 本所は、1 回あたり 20 名程度収容できる研修場所 1 か所で行うこと（研修受講者 15 席、インストラクタ 2 席、担当職員・予備席等 3 席程度が想定される。）。

ウ. 中部支所、大阪事業所は、1 回あたり 100 名程度収容できる研修場所 1 か所で行うこと。

エ. バイオテクノロジーセンター（木更津市）は、1 回あたり 10 名程度収容できる研修場所 1 か所で行うこと。

オ. 北海道支所、東北支所、製品安全センター（桐生市）、北陸支所、中国支所、四国支所、九州支所は執務室内で研修を行うこと。

カ. 事務用 PC を貸与する全職員に対して教育研修を行うこと（対象人数に関しては、「参考 10. 拠点別導入予定式数」を参照すること。）。

キ. 集合研修、自習方式を適宜組み合わせた教育研修を行うこと。

ク. 研修用テキストを 800 部作成し、機構の指示によって必要部数を拠点に配布すること。

ケ. 教育研修の実施報告を行うこと。

コ. 集合研修は、おおむね 1 回 2 時間、各拠点の研修対象人数に応じて 1 日 3 回程度を限度に実施すること。ただし、多忙な職員の受講を円滑にするために、本所、中部支所、及びバイオテクノロジーセンター（木更津市）については、日程をずらして、各拠点の研修対象人数及び研修場所の収容人数に応じた日数、研修を実施すること。大阪事業所については、日程をずらし 3 回程度実施すること。

サ. 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。

シ. 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。

(5) 初任者及び赴任時研修

ア. 上記の移行前の教育研修とは別途、サービス提供期間にわたって、毎年、6 日を上限に初任者及び赴任者に対して初任者及び赴任時研修を行うこと。

イ. 初任者及び赴任時研修は、本所において、おおむね 1 回 2 時間を毎年述べ 6 日を超えない日数において、1 日あたり 3 回を上限に行うこと。また、研修用テキストは別途用意せず、

移行前研修の研修用テキストを利用すること。

(6) システム管理者研修

ア. 最大 10 名の機構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。

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。

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、情報システム課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、情報システム課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、当該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. プライベートクラウドサービスを利用するシステムの担当者との調整

(ア) プライベートクラウド上で稼働する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プライベートクラウド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プライベートクラウド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。

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、平日の 19 時以降又は休日であること(ただし、担当職員との協議により、勤務時間中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)ユーザ端末の移行にあたりエンド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、エンド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、機器の撤去及び機器に記録されたデータ等の情報は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。
(ウ)プライベートクラウド環境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 35 台を平成 30 年 12 月 14 日から平成 31 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等、セキュリティに留意すること。

(2) 移行の対象

ア. 基本要件

(ア)イントラページのデータを除き、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)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。
(エ)移行期間中であっても、メールの送受信は行えるものとし、不達にならないこと。
(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。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。

①現行メールシステム（Lotus Notes）上のメールデータ

②スケジュールデータ（NITEイントラネット）

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。）

⑤CMSにより管理されていない機構のWebサイトのコンテンツ

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。

機構のWebサイトには、www.nite.go.jp、www.open.nite.go.jp、www.bio.nite.go.jp、www.nbrc.nite.go.jp、www.safe.nite.go.jp、www.prtr.nite.go.jp、www.iajapan.nite.go.jp、www.tech.nite.go.jp及びwww.jiko.nite.go.jpがある。

（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、①及び②については事務用PCで閲覧ができるよう（メーラで閲覧できなくとも、何らかの手段で閲覧できればよい。）に、③以降については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及び②の移行のための作業マニュアル（Lotus Notes以外の手段で閲覧可能にするための作業マニュアルでよく、新しい端末に移行するための手順は含まなくてもよい。）は、業務開始後2か月以内に提供すること。

①現行メールシステム（Lotus Notes Ver8.5.3）から職員が独自でバックアップしたメールデータ

②現行メールシステム以前のメールシステム（Lotus Notes Ver 3.5.2、4.6、5.0.12、6.5.2及び8.0.1）で職員が独自でバックアップしたメールデータ

③文書ファイル

④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））

⑤ブックマーク（Internet Explorer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プライベートクラウド環境への移行作業が平成31年1月7日から可能となるようにすること。ただし、PRTR AP仮想サーバ及びPRTR DB仮想サーバについては平成30年12月14日から可能となるようにすること。

(エ)移行データD(イントラに掲載されているデータ)

現行システムにイントラページとして掲載されているデータについては、別途移行事業者の調達を行い、移行作業を行う。そのため、平成31年1月7日から移行作業を開始できるよう、グループウェアサービスを利用可能とすること。

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。

(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させること。

(ウ)利用者、組織、グループの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、所属(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

⑧PHS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適用開始年月日、適用終了年月日

(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

①LDAPv3によるディレクトリサービスを提供できること。

②ディレクトリ内情報は利用者自身が事務用PCから入力、変更できないこと。

③「11.（6）認証・検疫ネットワークサービス」で利用するディレクトリサービスを提供できるものであること。

④グループは、多層化できること。

⑤大量のアカウントの一括登録のための機能を備えたものであること。

⑥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。

⑦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。）。

⑧アカウントの登録、変更、削除等を予め登録しておき、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。

⑨上記に加えて、将来変更する異動情報を複数世代管理する機能を有すること。

⑩過去の異動履歴を保持し、一元管理する機能を有すること。

⑪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。）。

⑫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。

⑬予め定めたルール（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。）。

⑭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。

（イ）認証基盤機能

①生体認証情報（指紋、静脈パターン等）によって、ユーザ端末におけるOSへのログイン認証が行えるものであること。

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。

③ICカード（ISO/IEC18092標準の職員証）又は生体認証情報（指紋、静脈パターン等）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利用者認証が必要なサービスについては、Kerberos v5により利用者認証を行うこと（複合機については対象外とする。）。

⑤「11.（6）認証・検疫ネットワークサービス」で利用する認証サービスを提供するものであること。

⑥「8.（6）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。

⑦一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。

⑧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。

⑨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。

⑩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。

⑪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。

⑫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。）。

⑬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。）。

⑭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。

⑮ICカードの携帯忘れへの対応機能を有していること。

⑯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。

⑰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出来ることが望ましい（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。）。

⑲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。）。

⑳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）シングルサインオン（SSO）機能

①Webアプリケーションにおいて、SSO機能を比較的容易に実現できるヘッダ情報等を提供する機能を有すること。

②リバースプロキシ型等、ユーザ端末がWebアプリケーションに直接アクセスすることを防ぐことができ、アクセスを集中管理できる方式にも対応していること。

③リバースプロキシ型等、個々のシステムにモジュール等をインストールする必要が無い方式にも対応していること。

④事務用PCのOSにログインしていれば主体認証情報の入力を行わずSSO機能においても認証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。）。

⑤既存のForm認証を行うWebアプリケーションに対して、改修することなくSSO機能の利用が可能とな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。）。

⑥リバースプロキシ型のSSO機能である場合、Webアプリケーションにおいて絶対パスが用いられている場合も対応可能な機能（自動書き換え機能等）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既存のSSO機能を利用しているWebアプリケーションに対して、改修することなくSSO機能の利用が可能となる機能（既存SSO機能においてWebアプリケーションに提供しているヘッダ情報の維持等）を有していること。既存のSSO機能を利用しているWebア

プリケーションについては、「参考04. 課室所管情報システムの移行に係る要件」を参照のこと。

(エ)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他のシステムとのデータ連携のために、FTPプロトコル、NFS、CIFSのいずれによって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。

(オ)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。

②NTPプロトコルによる時刻提供機能は、物理サーバ上で実装すること。

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)主体認証情報の有効期限を設定し、利用者に対して有効期限到来前に主体認証情報の変更を促すメッセージを通知し、利用者による変更ができること。
(ウ)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。
(エ)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。
(オ)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。)。
(カ)ログを CSV 等の形式で出力できること。
(キ)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。)。

(2) グループウェアサービス(イントラネット含む。)

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)～(サ)の各機能を提供すること。

②(イ)～(サ)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。

④初期画面には、URLリンク集を設定できること。リンク集は組織全体に共通するものと、利用者個人で設定できるものの両方が可能なこと。

(イ)職員名簿機能

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、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。

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職員名簿は、「8.(1)認証基盤サービス」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(PHS番号と固定内線番号等)を登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。)。

(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。

②Web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。

③Webファイル共有機能は、自動で履歴管理が行われること。すなわち、ファイルを更新した場合、古いファイルも残っており、その古いファイルの閲覧ダウンロードも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。)。

④Web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。)。

⑤Web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。)。

⑥データ領域を、「8.(6)ファイルサーバサービス」と合わせて、56TB以上提供すること。

⑦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。

⑧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。

⑨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。）。

⑩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。）。

⑪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機構全体又は部門用のイントラページを作成、削除できる機構全体・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・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・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、削除等のアクセス権を設定できること。

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、カテゴリ別の条件でページ内容を分類できること。

⑧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。）。

⑨イントラページ作成で作成したページ毎に、掲載開始日、掲載終了日を入力することで、掲示期間を設定することができること。

⑩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。

⑪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。

⑫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。

⑬読み上げ順序の設定ができること。

⑭キーボードで操作が可能なページを作成できること。

⑮フォーカスの順序の設定が可能なこと。

⑯JIS 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。

（オ）電子会議室機能

①電子会議室を作成、削除できる会議室管理者の設定機能を提供すること。

②会議室管理者は、個人、組織等に基づき、管理する会議室の閲覧、投稿、編集、削除

等のアクセス権を設定できること。

③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。

④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。当該パーソナル掲示板においては、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。）。

⑤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。

⑥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。

⑦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概要が表示できること。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、削除等のアクセス権を設定できること。

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ヶ月単位の表示ができること。

⑦スケジュールは、複数月（2ヶ月以上）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ヶ月以上）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毎に、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）

が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.（5）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・グループ等毎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ヶ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.（5）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毎に、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.（6）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、サムネイルおよ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）メーリングリスト管理機能

①機構役職員をメンバとするメーリングリストを作成できること（システム管理者のみが作成できることでもかまわない。）。

②Office 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（当該メーリングリスト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が望ましい（その場合総合評価に

おいて加点する。)。

③当該メーリング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(外部のアドレスの追加削除はできなくてもかまわない)。

④外部アドレスを含め、当該メーリング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。)。

⑤当該メーリング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。

⑥メーリング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。

⑦通常用いているアドレスを送信者とした送信か、メーリングアドレスを送信者と設定した送信が行われているか、容易に職員が判断できる(例えば、メーリングリストアドレスを送信者として設定して送信する場合には、通常用いているメーラではなく、Webメール等の別の方法を用いて送信する等の方法で容易に判断できる)こと。

⑧作成したメーリングリストは、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。)。

⑨自分が参加しているメーリング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。)

⑩メーリングリストの一覧(登録されているメンバの一覧、メーリングリスト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)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」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)生体認証によるサーバ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SSO認証による認証が行えること(ただし、メーリングリスト管理機能はSSO認証ではなく、別途認証が必要であってもかまわない。)。

(イ)メーリングリスト管理機能は、ディレクトリサービス機能と連携したSSO認証による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。)。

(ウ)本サービスで提供される各機能単位で利用者、組織、グループ毎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。

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短期雇用者ID削除申請

③ハードウェア申請

④ハードウェア廃止申請

⑤ソフトウェア申請

⑥ソフトウェア削除申請

⑦メーリングリストアドレス申請

⑧メーリングリスト変更・削除申請

⑨メールアドレス受信制限解除申請

⑩グループフォルダ申請

⑪グループフォルダ変更削除申請

⑫モバイル等貸出し申請

⑬タブレット端末貸出申請

⑭ファイル交換システム利用申請

⑮機構外からのメール及びスケジュール等利用申請

イ．機能要件

(ア)「8.（2)グループウェアサービス」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、ワークフロー数については「8.（2)グループウェアサービス」に記載されている数量とは別に提供すること。

(イ)「8.（2)グループウェアサービス」のポータル機能から申請ができること。

(ウ)申請の際の入力項目は、「8.（1)認証基盤サービス」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) 在席表示サービス

在席表示を行う機能を提供すること。

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．機能要件

(ア)共通機能

①「8.（1)認証基盤サービス」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。

・在席操作している状態

・離席一定時間操作をしていない状態
・不在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)メッセンジャー機能利用者間でメッセージの送受信ができること。

①任意の利用者を設定し複数人への同報ができること。

②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。)。

③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。)。

(5) 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全利用者の外部へのメール送信総数:2,800件/日(ピーク時: 420件/時間)

②全利用者のメール受信平均数(スパム対策前): 8,800/日(ピーク時: 1,600件/時間)

③全利用者のメール受信平均数(スパム対策後): 2,300/日(ピーク時: 1,310件/時間)

④外部とのメール送受信平均サイズ : 170KB/件

⑤機構内送受信メール平均数 : 13,000件/日

⑥機構内送受信メール平均サイズ : 500KB/件

⑦ユーザ用メールボックス・アーカイブ領域 : 5TB

(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。

(ウ)利用者が誤って削除した前日以前に送受信したメールの復元が、削除後 2 週間以内であれば運用作業により可能であること。

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「8. (2)イ. (イ)職員名簿機能」と同期した内容の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。
なお、機構内共有アドレス帳については、受注者作業による職員名簿機能との同期による対応も可とする。

・任意の複数の電子メールアドレスをグループ化し、グループアドレスの作成、変更、削除及びメンバの登録、修正、削除ができること。

なお、グループアドレスの作成、変更、削除及びメンバの登録、修正、削除は、申請に基づき行えること。

・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。

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。

・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）外部アドレス含有メーリングリスト機能

①外部利用者のメールアドレスを含めた任意の複数のアドレスをグループ化し、メーリングリストとして利用できること。
なお、本機能は別途メーリングリストサーバ等を用いて実現してもよい。

②メーリングリストの管理に際しては、「8.（1）認証基盤サービス」により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。）。

③メーリングリストは利用期間を設定できること。

④メーリングリストの利用期間が切れる前に延長の確認メールをメーリングリストに設定された管理者に自動送付できること。

⑤メーリングリストのメンバが、「8.（1）認証基盤サービス」のディレクトリサービス機能におけるグループ・ロールと連動するように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グループ・ロールにアカウントを追加するとそのグループ・ロールに対応するメーリングリストにそのアカウントのアドレスが追加され、また、同様に削除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。）。

（ウ）制御機能

①「8.（1）認証基盤サービス」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メールアカウント毎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毎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、ユーザ端末のローカルドライブであることは必須ではない。

⑪ユーザデータ領域への電子メールの移動を行わない場合は、メールボックスの容量制限を解除し、全ての電子メールをメールボックスに保存可能であること。その際、メールボックスの肥大化による性能低下や信頼性低下は認めない。

⑫複数のドメインを構築、管理可能であること。

⑬複数人でメールを共有するための共有メールフォルダ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。

⑮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。

⑯「8.（9）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。

⑰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、利用者毎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。）。

（エ）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」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メールサーバが他のユーザとメールを共有する共有メールフォルダ機能を有している場合には、その機能が利用できるものであること。

⑪開封通知機能を提供すること。

⑫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。）。

⑬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。)。

⑭電子署名がつけられたメールを閲覧できること。

⑮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。

⑯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。)。

(オ)添付ファイル自動暗号化機能

①パスワードにより暗号化されていないファイルが機構外に送信される際には、自動で暗号化されること。

②暗号化されたファイルは、Windows OSの標準機能で復号化できること。

③暗号を復号化するための情報(パスワード等)は、宛先に自動で通知されないこと。

④送信者に、暗号を復号化するための情報(パスワード等)が通知されること。

⑤職員と外部者間のファイル交換機能と連動しており、大容量の添付ファイルはファイル交換機能に自動保存され、そのダウンロードURLのみメールに添付され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。)。

⑥送信者が受信者に暗号を復号化するための情報(パスワード等)を容易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。)。

ウ. セキュリティ要件

(ア)S/MIME、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)「11. (7)イ. メール誤送信防止機能」に示す機能を有していること。
(カ)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。
(キ)機構外からの機構内ユーザを装ったメールの受信を防止できること。
(ク)「11. (4)スパムメール対策サービス」に示す機能を有していること。
(ケ)ジャンク電子メール、スパム電子メールとして隔離された電子メールのダイジェストのリストを受信者に送ることができ、ジャンク電子メール等のチェックを受信者自身に委ねら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。)。
(コ)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。
(サ)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。)。
(シ)スパムブロック機能により届かなかった電子メールについてシステム管理者等へ問い合わせる回数を減らすことに寄与すると考えられる機能(ユーザ自身によるスパム候補電子メールフォルダの管理等)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。)。
(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」を用いて主体認証を行う機能を備えること。
(タ)「8. (9)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、2 要素認証が行えること。
(チ)「8. (9)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. (9)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。)。
(テ)「8. (9)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。

(6) 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。

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 800 以上に対応できること。
(ウ)データ領域を、「8.(2)イ.(ウ)Web ファイル共有機能」と合わせて、56TB 以上提供すること。

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で、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)管理者が、複数の要素を組み合わせた利用状況(例:1 年以上参照されていない 100MB 以上の画像ファイル等)をグラフで可視化でき、指定した要素の組み合わせに対応する結果は再検査の必要が無く、即座にグラフ化し自由に分析が出来ることが望ましい(その場合総合評価において加点する。)。
(キ)ファイルの増加予測を過去の推移を外挿することで行い、指定したフォルダごとに、あと何日で既定容量に達する見込みか管理者が確認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。)。
(ク)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 2 週間以内であれば可能であること。
(ケ)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。
(コ)ファイルサーバに格納される各ファイルの格付け情報(「政府機関の情報セキュリティ対策のための統一基準」(平成 28 年8月 31 日、情報セキュリティ戦略本部)の「1.2 情報の格付の区分・取扱制限」における格付区分に係る情報をいう。)の管理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。)。
(サ)申請受付サービスの「グループフォルダ申請」及び「グループフォルダ変更削除申請」にもとづいて作成したファイルサーバのフォルダ(現行システムからの移行により作成したフォルダを含む。)のうち、自分が利用できるフォルダ一覧をポータル画面等から参照できることことが

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)「8. (1)認証基盤サービス」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」の認証基盤機能によって認証が行われること。
(ウ)利用者が保存したファイルが自動的に暗号化されて保存される機能を有すること。

(7) ファイル交換サービス

職員間及び職員と外部者の間での電子ファイルの受渡しを行うための機能を提供すること。

ア. 基本要件

(ア)機構外からの利用者については、1,000 人程度を想定しているが、ワンタイム URL、ワンタイムパスワード等を用いて随時利用する利用者数には制限がないこと。機構内の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)データ領域を 2TB 以上提供すること。
(ウ)同時接続数 20 に対応できること。

イ. 機能要件

(ア)共通機能

①GUIで利用できること。

②1.9GBの容量のファイルの受け渡しが可能なこと。

③以下の項目の上限値について設定可能であること。

・各ユーザが蓄積可能な容量（ユーザ毎に異なる値を設定できる必要はない。）
・ファイル保存期間
・ダウンロード回数
・利用期間

④以下の項目の上限値について設定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。)。

・同時登録（送信）ファイル数
・同時登録先（送信先）数

⑤ユーザ毎に異なる蓄積可能な容量を設定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保存期間を超過したファイルは自動的に削除されること。

(イ)職員間のファイル交換機能

①職員間で、テンポラリなファイル共有によるデータ受渡し機能を提供すること。

②3種類以上のブラウザから利用できること。

③制御系セグメント等、一般サーバセグメントにアクセスできない端末からも利用可能なこと。

(ウ)職員と外部者間のファイル交換機能

①職員と外部者間でのファイルの送受信機能を提供すること。

②送信先が受信したことを送信者にメール等で通知できること。

③自らの送受信履歴を取得し、検索及び閲覧ができること。

ウ. セキュリティ要件

(ア)機構内からは http プロトコル、機構外からは https プロトコルを利用し実現すること。機構内についても、https プロトコルでも良い。

(イ)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 に発行要求する必要がある場合は CSR(Certificate signing request:証明書発行要求)を作成すること。

(ウ)送信用ファイル、送信先メールアドレス、受信用パスワードを登録し、送信先に通知できること。

(エ)送信先ドメインの制限ができること。
なお、ファイアウォール等によって制限を行ってもよく、本サービスで用いるパッケージソフトの機能として実現することは必須ではない。

(オ)データに対するマルウェア対策が施されていること。
なお、事務用 PC やサーバのマルウェア対策ソフトウェア等によって対策が行われている場合は、本サービスで用いるパッケージソフトの機能として実現することは必須ではない。

(カ)データに対し暗号化を施す等し、正当な利用者のみデータの読み取りができること。

(キ)個人単位のファイル受渡し機能として、他のユーザ(他の ID)で保存したファイルは閲覧できない(表示されない)こと(ただし、将来の拡張要件として、他のユーザが保存したファイルも利用可能なように容易に機能変更できること。)。グループ単位でのアクセス権設定による管理を行う場合は、ユーザ毎のグループを作成し、グループにてアクセス権を管理する方法でも良いとする。その際には、ユーザの作成、グループへの割当等の作業を運用作業として行うこと。

(ク)機構内における認証は、「8. (1)認証基盤サービス」の認証基盤機能によって認証が行われること。

(ケ)機構内ファイル交換機能において、一般サーバセグメントにアクセス可能なユーザ端末からのアクセスの場合、「8. (1)認証基盤サービス」のシングルサインオン(SSO)機能によって認証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。)。

(コ)認証に用いられる情報は、暗号化されてネットワークを流れること(Web アプリケーションで SSL 又は TLS 通信が行われる場合は、この要件は満たしているものとする。)。

(サ)機構外ファイル交換機能における機構外からの利用の際の認証は、ワンタイム URL、ワンタイムパスワード等を用いるなど、セキュリティに考慮すること(機構外からの利用がダウンロードのみの場合は、ダウンロード毎にパスワードが設定できれば本要件は満たしているものとする。また、「12. リモートアクセスサービス」を利用して実現しても良い。)。

(8) 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)現在機構が会議室等で用いているテレビ会議システムと連携して Web 会議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。)。現在機構が用いているテレビ会議システムは、Polycom 社製の HDX6000、HDX7000、VSX5000、VSX6000、ViewStationSP、ViewStationSP128 及び ViewStationEX である。

(ウ)現在機構が会議室等に設置しているテレビ会議システム用のディスプレイ(35 台)に、テレビアダプターを設置する等の方法で、WiDi 等のプロトコルにより事務用 PC から無線で画像表示ができるようにすること。

(エ)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。)。

(オ)機構外の任意のブラウザから Web 会議に参加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)表示資料の画面の共有ができること。
(キ)情報漏えい防止の目的から、ファイルの共有ができないように設定できること。
(ク)音声の大幅な遅延がないこと。
(ケ)2 時間の会議中、安定して通信が行えること。
(コ)全ての NITE-LAN システム利用ユーザが会議を開設できること。

(9) 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

職員がスマートフォン及びPCからインターネット経由で「8.(5)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」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 420 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」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.(5)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 Office Word 2010」、「Microsoft Office Excel 2010」及び「Microsoft Office PowerPoint 2010」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)最新のバージョンの iOS、バージョン 5.0 以上の Android、Windows 7 以降のバージョンの Windows OS において利用可能なこと。
(カ)10.10 以降のバージョンの OS X におい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。)。

ウ. セキュリティ要件

(ア)本サービスは、HTTPS を利用し実現すること。
(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。)、ログイン毎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。

(10) 事務用PCサービス

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又はタブレット（以下「事務用PC」という。）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

・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

・プロセッサがインテルCore i3相当以上であること。

・キャッシュメモリが、3MB以上であること。

(ウ)メモリ

・8GB以上のメモリを有していること。

(エ)画面表示機能

・解像度1,366×768ピクセル以上であること。

・色数24bit（1,677万色）以上であること。

(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が望ましい（その場合総合評価において加点する。）

・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 Ver1.2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。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」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」を用い、測定に関する資料を提出すること。）。

・省エネ法で定める測定方法により測定された標準消費電力が15W以下であること。

・省エネ法で定める測定方法により測定された標準消費電力が10W以下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。）。

・省エネ法に基づくエネルギー消費効率（目標年度2011年度）における省エネ基準達成率が500%以上（AAA以上）であること。

(ク)筐体

・W347mm×D230mm×H21mmの大きさ以下であること。

・バッテリ（ACアダプタは除く。）を含め1.0kg以下の重量であること。

(ケ)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。

(コ)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ポート以上備えていること。クレイドル等外付けによる対応も可とする。

・IEEE802.11g、IEEE802.11n及びIEEE802.11acに対応した無線LANが利用できること。

・Bluetooth 4.1以上に準拠していること。

(サ)USB

・USB1.1/2.0デバイスをサポートし、上記「(コ) ネットワークインターフェース」において使用するLANケーブル並びに外部ディスプレイ、マウス及びキーボード（外部ディスプレイ、マウス及びキーボードは本件の調達には含まれず、別途機構にて購入する機器である。）を接続した状況で空きポートを1個以上搭載していること。本体に十分なUSBポートが存在しない場合には、USBハブを用いる方法でもよい。

・USB3.0デバイスをサポートし、上記「(コ) ネットワークインターフェース」において使用するLANケーブル、外部ディスプレイ、マウス及びキーボードを接続した状態で空きポートを1個以上搭載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。）。

(シ)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。

・外部ディスプレイを用いて、マルチディスプレイ表示ができること。

・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。

・ウェブカメラを備えていること。外付けでも可とする。

(ス)海外対応

・海外での故障も保証の範囲であること（ただし、海外から国内への送付が必要な場合には、その費用は機構が負担し、輸出入手続きは機構が実施する。また、機器の規格外の使用環境で用いたことが原因の故障も保証の対象外でよい。さらに、ソフトウェアについては、海外に持ち出した時点の状態で使用できればよい。）。

・海外での持ち込み修理も可能であることが望ましい（対応可能な都市名を提案書に記載すること。）（その場合総合評価において加点する。）。

・海外で故障した場合、国内への送付、輸出入手続き等を受注者が代行できることが望ましい（対応可能な都市名を提案書に記載すること。）（その場合総合評価において加点する。）。

(セ)その他

・利用者の生体認証装置（指紋、静脈パターン等）を内蔵していること。

・「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へのインストール作業を行うこと。

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最新の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。

・連想変換機能や最近の時事用語の変換にも対応していること。

・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。

・平成22年11月30日に告示された「常用漢字表」、公用文に関する内閣告示、訓令等に基づいた、公用文作成のための辞書を提供すること。

・「8.（10）ウ.（ア）⑧ 法令作成業務支援機能」のソフトウェアに日本語入力機能がバンドルされている製品がある場合には、その製品を採用すること。

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 Office Word 2010」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

・法令作成業務を支援するための機能として、「ジャストシステム一太郎ガバメント7」で作成された文書の読み込み、編集、印刷、保存ができるワープロ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。

・「ジャストシステム一太郎ガバメント7」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。

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 Office Excel 2010」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 Office PowerPoint 2010」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。

・Adobe Flashコンテンツの再生ができること。

・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形式やzip形式へのファイルの圧縮／解凍ができ、かつ暗号化できること。

・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、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が望ましい（その場合総合評価において加点する。）。

・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が望ましい（その場合総合評価において加点する。）。

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すること（特許侵害となる恐れないソフトウェアを提供すること。）。

・既存のRealPlayer 用のフォーマットであるRAM metafile parsing and playbackで作成されたメディアコンテンツを再生できること。

・国会中継等で配信されている形式のファイル（WMV形式、RAM形式）をストリーミング再生できるソフトウェアを提供すること。

⑭PDFファイル閲覧・出力・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。

・ページの分割、挿入、削除、順序入替ができること。

・ノートの追加、編集ができること。

・セキュリティ設定（文書内容のコピー及び印刷の不可並びにファイル暗号化）ができること。

・PDFファイルを、DOC、PPT、XLS、JTD形式のファイルに変換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。）。

・PDFファイルを、テキスト編集及び図形編集できる機能が付加されていること

が望ましい（その場合総合評価において加点する。）。
・PDFファイル内の機密情報を墨塗り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。）。

⑮スキャン取込機能
・「8. (13)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TIFF、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及び日本語EUC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」又は「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 Office Access 2010」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。
・Javaの最新版のランタイムが利用できること。
・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、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されていること。

・セキュリティの観点から問題がない場合には、「パーソナル設定」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。

エ. セキュリティ要件

(ア)利用者の生体情報(指紋、静脈パターン等)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、静脈パターン等)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)利用ユーザごと又は利用ユーザのグループ・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(読み込みのみ可能なように設定ができること。)。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。
(キ)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。
(ク)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。
(ケ)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。)。
(コ)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。
(サ)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。
(シ)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。
(ス)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。)。
(セ)ストレージデバイスに保存されたデータを、遠隔設定によって消去できること(事務用 PC がインターネットに接続された際に消去されればよい。)。

(11) 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 10 個及び Linux OS のクライアントマシン 3 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 168GB 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 1,600 以上の計算性能を有すること。

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。

(12) 統合管理サービス

事務用PC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。

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受託者のシステム運用担当者（現環境：4名（内常駐3名））が運用管理用PCを用いて統合管理機能を利用して事務用PC等の管理ができる環境を整備すること。その際の運用管理用PCは、事務用PCとは異なる専用端末として用意すること。

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プライベートクラウド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1台、大阪事業所に1台用意すること。

③機構のシステム運用担当者6名が運用管理用PCを用いて統合管理機能を利用して事務用PC等の管理ができる環境を整備すること。その際の運用管理用PCは、事務用PCとは異なる専用端末として用意すること。また、機構のシステム運用担当者が用いる事務用PCとKVMスイッチにより切替えて使用できる環境を整えること。

④運用管理用PCからプライベートクラウド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からプライベートクラウドのサーバにアクセスする際には、直接プライベートクラウド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。

⑤極力パッケージソフトウェアである統合管理ツールの機能により実現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。）。

⑥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。）。

⑦事務用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。

⑧CSV形式にて情報のエクスポートができること。

⑨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。）。

⑩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。)。

⑪事務用PC等におけるローカルアカウントの主体認証情報（Admin権限ユーザの主体認証情報）を一括変更し、エンド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。)。

⑫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。)。

⑬事務用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。)。

⑭Web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。)。

（イ）リモート接続機能

①事務用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。

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事務用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事務用PCとリモート操作を受けている事務用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リモート接続先エンド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事務用PCの再起動が可能であること。

⑬事務用PC上のプログラムを実行できること。

⑭利用者が事務用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事務用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監視対象の事務用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。）。

⑤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。）。

⑥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。）。

（エ）構成管理機能

①事務用PC構成情報の収集方法として、収集する事務用PCを選択可能であること。又は分析・閲覧の対象とする事務用PCが選択可能であること。

②事務用PC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事務用PC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事務用PC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事務用PC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経由であっても事務用PC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事務用PC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事務用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事務用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、当該事務用PCをネットワークに接続することなく、当該事務用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構成情報収集時に事務用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、MPU、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事務用PC等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事務用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。

④事務用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、未知のソフトウェアをスキャンできること。

③事務用PCがネットワークに接続されていなくてもソフトウェアの利用状況を監視し、再接続時に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事務用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事務用PCを自動選定し、最初に配布された事務用PCがサブネット内の他の事務用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、事務用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、利用者が事務用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、エンド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、グループ毎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、事務用PC等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方法等の設定を再利用し、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事務用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事務用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電源が切れている事務用PCに対して、リモートで電源をONにし配布する仕組みを有していること（自動配布が可能なことまでは必須とはしない。）。

⑮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、事務用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。

⑯ソフトウェアの自動配布時に処理途中で終了した事務用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。

⑰事務用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、事務用PCの起動処理中に行うなど事務用PC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。

⑱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アンチマルウェア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、適切なタイミングで事務用PCに配布できる機能を有していること。

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。）を任意の事務用PCへアップデートできること。

④事務用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、アンチマルウェアソフト）が適用されていな

い事務用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事務用PC等のパッチファイル適用状況を検索・管理できること。

⑦パッチ適用時に電源が切れている事務用PCに対して、リモートで電源をONにし適用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。）。

⑧パッチ適用処理により、利用者の業務に影響を与えない機能を有していること（例えば、事務用PCの起動時や業務中にパッチ適用を行うことによる事務用PCの性能低下等が発生しない方法によりパッチ適用を行うこと。特に起動時にパッチを適用し、パッチ適用終了後にPCの利用が可能となる方式は採用しないこと。）。

（サ）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事務用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・集約印刷枚数（2in1等）、カラー印刷枚数、トータル印刷枚数等の情報収集及び管理が事務用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・集約印刷枚数（2in1等）、カラー印刷枚数、トータル印刷枚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。）。

（シ）ログ管理

①事務用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事務用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事務用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事務用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事務用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事務用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事務用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事務用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事務用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事務用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事務用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収集した事務用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収集した事務用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事務用PCをNITE-LANに接続しない状態においても、事務用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。)。

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ログは契約期間中保存すること。契約終了後は、CSV形式等によりDVD等のメディアに保存し、提供すること。

(ス)事前登録ソフトウェアユーザインストール機能

①予めプログラムを登録しておくことで、当該プログラムを利用者の操作によりインストールできること。

②予めセキュリティパッチを登録しておくことにより、利用者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)事務用 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)接続デバイス(USB、CD、DVD 等)を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。)(別途記載のとおり、事務用 PC に対して接続デバイスの制御ができることは必須であり、それを統合管理ツールで行えることが望ましいというのが、本要件の趣旨である。)。

(エ)接続デバイス(USB、CD、DVD 等)を読み取り専用とする制御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。)(別途記載のとおり、事務用 PC に対して接続デバイスを読

み取り専用とできることは必須であり、それを統合管理ツールで行えることが望ましいというのが、本要件の趣旨である。)。

(オ)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。)。

(カ)USB に転送するファイルを暗号化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。

なお、本件で調達する複合機は、以下の5種類である。ただし、A2とBは同一機種であり、フィニッシャー等の周辺機器のみの違いを想定している(別機種でもかまわない。)。

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。

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	A1	9 台	カラー、高速型、A3 版、Z 折フィニッシャー等有	○	○	○	○(カラー)
		A2	26 台	カラー、高速型、A3 版、フィニッシャー等有	○	○	○	○(カラー)
		B	36 台	カラー、高速型、A3 版、フィニッシャー等無	○	○	○	○(カラー)
	モノクロ	C	27 台	モノクロ、低速型、A3 版、フィニッシャー等無	○	○	○	○(カラー)
		D	5 台	モノクロ、高速型、A3 版、フィニッシャー等有	○	○	○	○(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何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(職員証)又は生体認証情

報（指紋、静脈パターン等）（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カードよりも、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。）。

⑧ICカードと生体認証の何れでも認証できる（生体認証の認識率の高い職員は生体認証を用い、認識率の悪い職員はICカードにより認証することができる）ことが望ましい（その場合総合評価において加点する。）。

⑨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。）。

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ユーザ端末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機構が有する他のシステムが、サーバからシステム命令等において直接プリント出力を実行しようとした際に、サーバ出力専用のICカードで認証する、管理者権限を持たせたICカードにより出力する等何らかの認証により出力できること。又は、サーバからシステム命令等において直接プリント出力を実行しようとした際は、認証を行うことなく出力できること。

⑭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、ユーザ端末等何らかの方法で変更ができれば良い。）。

⑮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、利用者毎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。

⑦ログは契約期間中保存すること。契約終了後は、CSV形式等によりDVD等のメディアに保存し、提供すること。

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。

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。)。

(14) 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)内部 DNS サービスは、「8. (1)認証基盤サービス」のディレクトリサービス機能のサービスとして実現すること。

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)シ.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)シ.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をもとに、使用されていないレコードを削除できること。
(ク)「10.(2)シ.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」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」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。
(シ)WINS を使用せず名前解決を実現するため、LLMNR をサポートすること。

(15) 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。

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。

(16) 補助的httpサーバサービス

機構外に対してWebコンテンツを、HTTP及びHTTPSにて情報発信する機能を提供すること。

ア.基本要件

(ア)1,200 アクセス/分を処理できること。
(イ)複数サーバ構成にした場合でも、データの整合性がとれること。
(ウ)コンテンツ等のデータ領域を 30GB 以上提供すること。

イ．機能要件

(ア) 日本語対応 Web サーバソフトウェアを搭載すること。
(イ) セキュアな FTP サービスを利用できること。
(ウ) コンテンツ全体及び一部に対してユーザ ID、ユーザグループによりアクセス制御ができること。
(エ) メール送信できること。
(オ) 機構で準備するサーバ証明書の登録、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。
(カ)「Perl」及び「C++」で開発されたプログラムが稼働する環境を提供すること。ただし、既存のプログラムの稼働保証は求めない。
なお、導入するバージョンは機構と協議の上、決定すること。
(キ) アクセスログの取得及びサブドメイン毎に分けてアクセスログの提供ができること。アクセスログを保存しておくストレージも提供すること。

ウ．セキュリティ要件

(ア) 動的コンテンツの動作可能領域とファイル保存領域は、ドキュメントルートとは別のツリー構造とし、ドキュメントルート配下では CGI 等のプログラムが実行できない設定にできること。
(イ)「11.（7）情報漏えい対策サービス」に従い、コンテンツの改ざんを検知及び防止できること。

（17） 補助的httpサーバ検証サービス

「8.（16）補助的httpサーバサービス」で提供される、コンテンツの確認及びWebアプリケーションの動作検証を行える機能を提供すること。

ア．基本要件

(ア)「8.（16）補助的 http サーバサービス」と同一の OS、ソフトウェア等の環境を提供し、バージョンを同一に保つこと。ただし、機構が要求した変更に対しては適用しない。
(イ) 事務用 PC から、本サービスで提供されているアプリケーションを使用できること。
(ウ)「8.（16）補助的 http サーバサービス」用に開発されたアプリケーションを検証する環境を提供すること。
(エ) コンテンツ等のデータ領域を 30GB 以上提供すること。

イ．機能要件

(ア) 日本語対応 Web サーバソフトウェアを搭載すること。
(イ) セキュアな FTP サービスを提供し、必要に応じて利用できること。
(ウ) コンテンツ全体及び一部に対してユーザ ID、ユーザグループによりアクセス制御ができること。
(エ) メール送信できること。
(オ) コンテンツ作成領域をディレクトリ単位で管理でき、あらかじめ指定された容量制限を設定できること。
(カ)「Perl」及び「C++」で開発されたプログラムが稼働する環境を提供すること。ただし、既存のプログラムの稼働保証は求めない。
なお、導入するバージョンは機構と協議の上、決定すること。
(キ) 公開可否に関する承認を GUI により可能なこと（ワークフロー機能は不要である。）。
(ク) 公開が承認された後、30 分以内に「（16）補助的 http サーバサービス」にコンテンツがアップロードされること。

ウ．セキュリティ要件

(ア) 動的コンテンツに関するプロセスのサーバリソースの利用を制限できること。
(イ) 動的コンテンツの動作可能領域とファイル保存領域は、ドキュメントルートとは別のツリー構造とし、ドキュメントルート配下では CGI 等のプログラムが実行できない設定にできること。

（18） ラーニングマネジメントシステムサービス

eラーニングマネジメントソフトウェアを活用して、職員が効率的に学習を行うための機能を提供すること。

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）ラーニングマネジメントシステムサービスは、クライアントとして、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。

（ウ）「8．（2）グループウェアサービス」のポータル機能から利用できること（リンク機能等）。

イ．機能要件

（ア）学習管理機能

①受講者の登録、受講者への教材コンテンツの提供（配信）、受講者毎の学習進捗状況把握（所属長等による学習進捗状況把握を含む。）、教材コンテンツ別の受講履歴把握、理解度テストの実施ができること。

②イベント（受講者の決定、受講開始日、進捗遅延時、受講終了時等）毎に対象者を抽出し、自動で対象者に通知（電子メールで送信）できること。

③教材コンテンツ毎に、受講者の登録を一括で処理できること。

④本サービスで管理されている受講状況のデータを抽出し、一覧表示及びCSV形式等によりデータを出力できること。

（イ）教材コンテンツの作成、編集、管理機能

①作成された教材コンテンツに概要を設定できること。

②「8．(10)ウ．ソフトウェア要件」に記載したプレゼンテーション機能により作成した資料（アニメーション、音声等の動的効果を含む。）から教材コンテンツを作成できること。

③教材コンテンツにFlash形式を取込めること。

④教材コンテンツの上書き登録ができること。

（ウ）理解度テストの作成、編集、実施、管理機能

①教材コンテンツの理解度をテストするためのコンテンツ（以下「理解度テスト」という。）を作成、編集、実施管理できること。

②作成した理解度テストの動作確認ができること。

③理解度テストの各設問の得点及び正解、不正解時のメッセージを設定できること。

④登録された設問の中から、設問をランダムに出題できること。

⑤登録された設問の中から表示する設問数を設定できること。

⑥理解度テストの合格点を設定できること。

⑦理解度テストの終了時、合否判定を表示できること。

⑧理解度テストの設問は、次の種類の形式で作成できること。

- 正誤問題形式（○（はい）、×（いいえ）の二者択一形式）
- 単一選択問題形式（選択肢から一つの正しい回答を選ぶ形式）
- 複数選択問題形式（選択肢から複数の正しい回答を選ぶ形式）
- 空所補充問題形式（空欄に入る回答を記入する形式）

⑨理解度テストは、一時保存、再開ができること。

(エ)制御機能

権限によって管理者画面、受講者画面等の表示が変わること。

ウ. セキュリティ要件

(ア)システム管理者、受講管理者、受講者の別にユーザ権限を管理できること。

9. プライベートクラウドサービス

(1) 基本要件

プライベートクラウド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）

プライベートクラウドサービスの構成は、「参考02. 次期ネットワーク構成概要図（案）」及び「参考05. プライベートクラウド仮想サーバ要件一覧」を参考に設計すること。プライベートクラウド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。

(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)内部 DMZ セグメント

Webサーバ、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

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受けることはない。

イ. 全体構成（物理構成）

プライベートクラウドサービスの物理構成については、「参考05. プライベートクラウド仮想サーバ要件一覧」及び「8. 業務サービス」を参考に設計すること。

なお、ネットワーク負荷やセキュリティ、運用管理、ミドルウェアのライセンス費用等を考慮した上で、仮想化技術（同様の効果を供する技術を含む。以下同様とする。）を用いて可能な限りサーバ群は物理的に集約すること。

ウ. 拠点構成

「参考10. 拠点別導入予定式数」を参照すること。

エ. サービス提供範囲

プライベートクラウドサービスは以下の（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プライベートクラ

ウドサービスの詳細は「参考05. プライベートクラウド仮想サーバ要件一覧」を参照すること。

(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。）、グループウェアサービス（イントラネット含む。）、ファイルサーバサービス、電子メールサービス、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。

オ. 集約サーバが提供するスタック構成

(ア)プライベートクラウド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)、前述エ. 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「エ. 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. プライベートクラウド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

プライベートクラウド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（法定点検等の停止時間を含めない。）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監視コンソールで一元的に確認できる機能

(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. プライベートクラウド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

①SNMP、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)MPU のアーキテクチャ

プライベートクラウドのMPU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)、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。)

(キ)バックアップ・リストア機能は、バックアップサーバを設置したエージェント・マネージャ方式とし、バックアップしたデータはバックアップサーバに集約・保管すること。

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 (一部は加点項目である。)。

(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

プライベートクラウド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、一元管理すること。また、キーワードによる横断的な検索が可能なこと。収集したログのうち、セキュリティに関わるものは、最終的に媒体に保管し、サービス提供期間にわたり機構が提供する本所に存在する耐火金庫に保管すること。

ク. ストレージ基盤サービス

プライベートクラウドサービスを構成するストレージは、ストレージ基盤サービスとして以下の要件を実現すること (一部は加点項目である。)。

(ア)性能要件

①プライベートクラウドサービスのストレージとして使用する場合、プライベートクラウド基盤で使用する仮想基盤製品との接続性が担保されていること。

②複数の性能のディスクを混在させたボリュームを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。）。

③複数の性能のディスクを混在させたボリュームにて、データの使用頻度等を分析し、頻度の高いデータは高速なディスクに格納し頻度の低いデータは低速なディスクに格納するなど、自動的にデータの格納ディスクを変更する機能を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。）。

④フラッシュドライブ等の高速なディスクを読み込みキャッシュドライブとして、性能向上のために使用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。）。

⑤キャッシュドライブ等の高速なディスクを読み書きキャッシュドライブとして、性能向上のために使用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。）。その場合、ストレージのコントロール機能の障害時にもデータ消失がない仕組みを有していること。

（イ）可用性要件

①ストレージ基盤の動作を監視し、正常に動作していることを確認できること。

②異常が発生した場合はメール等で管理者に通知できること。

③ディスクの冗長化を行うこと。予備ディスクが存在しない構成の場合には、同時に2台のディスクが故障しても情報が失われないこと。

④ストレージ基盤のアクセス受け口についても冗長化し、1台が故障してもストレージ基盤が停止しない構成とすること。またその際、設定を手動で変更する必要がないこと。

⑤電源供給断時に、ストレージ基盤のキャッシュメモリ上に格納された未保存データを、専用ディスクに保存し長時間電源断によるデータ消失を防止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）運用管理機能要件

①管理が容易になるよう、Web又はGUIで管理が行えること。

②作業の省力化のため、SSHによる管理機能を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。）。

（エ）セキュリティ要件

①セキュリティ脆弱性等の影響を最小化するため、運用期間中継続してパッチ等の修正が提供されるOS/ソフトウェアを搭載すること。

（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はなく、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、4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) 内部 DMZ セグメント

Webサーバ、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。

内部DMZ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に分けること。

(エ) クライアントセグメント

事務用PC、複合機等を接続するセグメントである。

(オ) 広報スペースセグメント

本所1階に存在するNITEスクエアのためのセグメントである。他のセグメントとは分けること。

(カ) リモートアクセス DMZ セグメント

ダイヤルアップアクセスに対するDMZセグメントである。他のセグメントとは分けること。

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、内部 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。
(イ)政府共通 NW との接続する 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)拠点毎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

NITE-LANは、500Mbps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への接続用ルータも調達範囲に含む。SINETへの接続回線は本調達の範囲外である。）。

（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2つのグローバル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。

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。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 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 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（すなわちクライアント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」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、クライアントセグメント

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。

③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進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。）。

④フォワードプロキシ機能は、FTP及びHTTPをサポートしていること。

⑤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及びSSHを通過させることができること。

⑥フォワードプロキシ機能は、NITE-LANシステムのユーザが国会中継等を見る場合等のために、RTSP and RTP tunneled through HTTPをサポートしており、ストリーミングの帯域制御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、500Mbps以上のスループット性能又は6,000requests/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。

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、500Mbps以上のスループット性能を有すること。

（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。

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)政府共通 NW 用 http サーバ機能

①NITE-LANシステムは、政府共通NWからアクセスされる静的コンテンツを提供できるhttpサーバ機能を有すること。

②当該httpサーバ機能は、政府共通NW用DMZセグメントに配置されていること。

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、アプリケーション毎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)アプリケーション毎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、500Mbps 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、200Mpps 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、通信フロー毎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が望ましい

（その場合総合評価において加点する。）。

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インタフェース毎にフロー、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、インタフェース毎に転送パケット数、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。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。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. 他システムとの接続

（ア）受注者は、「参考 13. 現行ネットワーク構成図」を参考に既存の他システムを 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、別途広域Ethernetサービス又はIP-VPNサービスを調達する。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の何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。

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、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」)、契約締結日における最新版の「政府機関の情報セキュリティ対策のための統一基準」を遵守すること。
なお、機構の情報セキュリティポリシーは機構本所にて閲覧することができる。

(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) 各機器の設置時においては、管理者パスワードを初期設定から適切なパスワードに変更すること。

(カ) 各サービスにて使用する OS 及びソフトウェア、アプリケーション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) セキュリティの確保のため、「11. (3)イ. 不正侵入防御機能」及び「11. (7)ウ. 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)」を除き、リモート運用を行うことは認めない。また、リモート監視も最低限とし、NITE-LAN とは独立した監視回線を用いること。

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受託者又はその従業員、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受託者の資本関係・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託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、機構と受託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、受託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 毎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、未知のマルウェアを判明した場合には、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、未知のマウルェアを検出する機能(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防御できること。
(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 DNS クエリを検知・遮断する機能を有すること(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 Web 又は 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 及びサーバによるマウル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. 事務用 PC 用マルウェア対策

(ア)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。)。
(イ)機構が保有している Windows OS 端末用に、NITE-LAN システムとして導入する機器用とは別途、64 ライセンスを提供すること。

(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（具体的には、ゲストのアクセスとNITE-LANシステム利用ユーザのアクセスでは異なるIPアドレスが用いられること。また、外部とのテレビ会議用等にスタティックNATの設定が必要になるので、対応すること。）。

⑨ファイアウォール機能は、Web又は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、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、Web又は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、Web 又は 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）不正アクセスを早急に検知するため、監視運用サービス（24 時間 365 日）を提供すること。なお、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、不正アクセスを検知した場合は速やかに担当職員へ連絡し、担当職員の指示に基づき通信遮断等の対応を行うこと。その他、インシデント対応支援も行うこと。
（カ）前述（オ）の監視運用サービスにおいては、必要に応じて適宜機構に対する攻撃パターンに特化した独自シグネチャを提供し、担当職員の指示に基づきシグネチャの更新を行うこと。
（キ）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。
（ク）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。）。

ウ．パケットデータ収集機能

（ア）インシデント対応の観点から、フォワードプロキシ等からパケットを取得することで、インターネットとの通信内容（通信データそのもの（暗号化通信の場合は復号化されたデータ））を取得できる仕組みを有すること。取得するデータの範囲については、担当職員と協議の上、決定すること。
（イ）取得した通信内容は、1 か月間検索可能な状態で保持すること。それ以前のデータは、テープ等に保存すること。

（4） スパムメール対策サービス

ア．基本要件

（ア）機構内に到達する電子メールのうち、いわゆるスパムメールについて、利用者に到達する以前にフィルタリングを実施し、スパムメールと判定された電子メールについて対策を講じること。

(イ)スパムメールの判定に際しては、単一の手法による判定を行うこととはせず、複数の手法による判定を行うこと。また、手法については後述の「イ. 機能要件」に記載されている例を参照すること。
(ウ)世界規模でスパム情報を収集し、24 時間体制で解析を行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。)。

イ. 機能要件

(ア)インターネットから機構内に電子メールが到達した際、各電子メールに対して以下の手法例等を用いてスパムメール判定を行うこと。

①送信元のIPアドレス又はドメイン情報について、既知のスパム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アドレス又はドメイン情報を元にスパムメールと判定する。

②電子メール中に含まれるIPアドレス、ドメイン情報又は文字列等をキーワードとし、特定のキーワードが含まれる電子メールをスパムメールと判定する。

③電子メール本文中に含まれる語彙を分析し、ベイジアン理論等に基づき、一定のしきい値を超えた値を示す電子メールをスパムメールと判定する。

④電子メールに含まれる情報を元に、送信者認証を行い、送信者認証が行えなかった電子メールをスパムメールと判定する。

⑤電子メール中に含まれるIPアドレスをDNSサーバに照会し、DNSサーバに登録のないIPアドレスから送信されている電子メールをスパムメールと判定する。

(イ)前述(ア)によりスパムメールと判定された電子メールについては、受信者がそれと分かり、メールクライアント側での振り分けができるよう、件名に特定の文字列を付記する等のマーキング処理を行うこと。
(ウ)なりすまし及び不正中継を防ぐため、受信したメールの SPF チェック等ができること。
(エ)SPF チェック等の結果、不正が疑われるメールに対して、隔離、破棄、件名や本文に警告文言挿入などのフィルタリングを実施できること。
(オ)スパムメールと判定し対策を講じた場合、判定を行った手法、件数等の記録を残し、任意の期間の状況を随時報告できること。
(カ)受信したメールのエンベロープの from と当該メールのヘッダ情報、DNS サーバのホスト情報を元に、発信元のホストを詐称しているメールについて、これを検知し、前述(イ)、(エ)と同様の処理を実施できること。
(キ)スパムメール対策により電子メールの遅延が発生しない構成とすること。
(ク)機構が指示する任意のアドレスからの電子メールについて、スパムメールの判定対象から除外できること。
(ケ)メールに添付された Microsoft Office(Word、Excel、PowerPoint)及び PDF ファイルを無害化(安全性が確認できている要素のみに変換)する機能並びに HTML/リッチテキストメールをテキストメール化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。)。ただし、その場合には、必要に応じて無害化前の添付ファイルを取得する手段を提供すること。なお、当該機能は、スパムメール対策製品で提供されることは必須ではなく、別の機能を提供する製品に備わった機能でもかまわない。

(5) コンテンツフィルタリングサービス

ア. 事務用 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。）。

(6) 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。

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。

(7) 情報漏えい対策サービス

ア. ファイル暗号化機能

ファイルサーバ及び事務用PCに求められる暗号化機能については、「8.（6）ファイルサーバサービス」及び「8.（10）事務用PCサービス」を参照すること。ファイル暗号化機能は、その他下記の要件を満たすこと。

(ア)暗号化のための鍵は、事務用 PC のみに保存することはせず、必ずサーバ上に保存又はバックアップを取ること。また、必要に応じ、鍵を事務用 PC に配布できること。

(イ)NITE-LAN システムの更改時には、NITE-LAN システムで使用していた情報を次期システムで利用可能とする所要の措置を講じること。

(ウ)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、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。

(エ)受注者が、機構の指示なく暗号を解読できない技術的な手段を講じること。

イ. メール誤送信防止機能

(ア)メール送信時に送信確認画面を表示し、宛先（機構内部、外部、CC、BCC）、件名、添付ファイル等を確認することができること（「8.(9)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」を用いてメールを送信する場合を除く。以下、「イ. メール誤送信防止機能」において同じ。）。

(イ)表示された送信確認画面上に表示される外部宛先を個別にチェックし、すべての確認が完了しないと送信されない仕組みとすること。

(ウ)前述（イ）の確認後に最終的な確認画面が表示され、確認が完了した時点でメールの送信ができること。

(エ)メールの宛先、件名、本文、添付ファイル等を指定した条件に基づき送信を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。）。

(オ)制限した内容を送信者に対し、ポップアップ画面等で確認の通知が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。）。

ウ. 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「8.（16）補助的 http サーバサービス」、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機能を有すること。

(イ)改ざん防止対策により「8.（16）補助的 http サーバサービス」の性能に影響を及ぼさない構成

とすること。
(ウ)インターネットから「8.(16)補助的 http サーバサービス」、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。
(エ)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。)。
(オ)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。
(カ)改ざん防止対策は、最大 500Mbps 以上のスループット性能を有していること。
(キ)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(24 時間 365 日)を提供すること。
(ク)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。
(ケ)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。

エ. 改ざん検知対策

(ア)「8.(16)補助的 http サーバサービス」に示す Web コンテンツ及び「参考 05. プライベートクラウド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)改ざん検知対策により「8.(16)補助的 http サーバサービス」の性能に影響を及ぼさない構成とすること。
(ウ)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。
(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)また、改ざんを検知した場合には、シャットダウン、ソーリーページを表示させる等の制御を行うこと。
(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。

オ. その他(サーバ、事務用 PC 共通)

(ア)NITE-LAN システムを構成するサーバ及び事務用 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。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及び事務用 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。ASP 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、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。

(8) 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。

(9) 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。

(10) 第3者チェック

ア. サービス提供開始前に、第 3 者からのセキュリティチェックを受けること。

イ. 第 3 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、最終判断は情報システム課長、情報統括官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 3 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 3 者を自ら選定するが、第 3 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 3 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監査企業台帳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 3 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テクニカルエンジニア（情報セキュリティ）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 3 者を選定すること。

キ. セキュリティチェックを行う第 3 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。

(1) 基本要件

リモートアクセスサービスの利用者数は「4.（1）NITE-LANシステムの利用者」のとおりとし、同時接続数50に対応できること。100Mbps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。

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. リモートアクセス時であっても、リモート接続の認証が行われ、リモート接続された後には、他のサービスに対するシングルサインオン及び機構内での利用時と同様のアクセスができること。

エ. 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。

オ. 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。

カ. 事務用 PC から利用できること。

(3) セキュリティ要件

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

イ. VPN 接続時の認証は、生体認証による OS へのログインに加え、端末に保持された秘密鍵、ログイン毎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 2 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. 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、ウイルス対策ソフトの稼働状況等の検疫を行い、汚染された事務用 PC からのアクセスを制限すること。

キ. 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。)。

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)イ. (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。
(ウ)受注者は、「5. (7)ウ. (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、サービス提供期間終了後、CSV 形式等により DVD 等のメディアに保存し、提供すること。
(ク)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。
(ケ)サービス構築を担当した要員の中から、運用管理サービスの運用管理責任者を選出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 ヶ月間はサービス提供までの調整期間とし、4 ヶ月目から 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。

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)イ. (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、各サービス(プライベートクラウドサービスで稼働する一般業務システム及び個別業務システムを含む。)のシステム領域及びデータ領域とし、D2D方式によりバックアップの取得を行うこと。事務用PC及び複合機に格納される情報についてはバックアップの対象外とする。

②データ領域のバックアップについて、「8. (6)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、手法にて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4世代を基本とし、担当職員と調整すること（全世代をディスクに保管する必要は無く、テープを利用しても良い。）。

⑩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。

（エ）利用者の誤操作時要件

①利用者の誤操作による損失データの復旧は本所内にて取得したバックアップを用いること。

②「13.（3）ア. インシデントの対応（ウ）」のサービス要求の対応として利用者の誤操作による損失データの復旧対応を行うこと。

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	2019 年 11 月 30 日
NITE.JP	2019 年 4 月 30 日
製品評価技術基盤機構.JP	2019 年 5 月 31 日
ナイト.JP	2019 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）ウ.（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、基本平日9:00～18:00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、平日9:00～18:00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)当初の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。
(エ)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)」をベースとしてSLAとして定める。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. 受託者は、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託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託者が負うこと。

エ. 再委託先には CIO 補佐官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. 再委託先には「NITE-LAN システム最適化計画」の策定支援を実施した事業者及び本仕様書の作成支援を行った事業者（みずほ情報総研株式会社）並びにこれらの事業者の「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委託先事業者等の緊密な関係を持つ事業者が含まれないこと。

(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。）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。受託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. パッケージソフトウェアを利用して新システムの設計・開発を行った場合にも、機構独自に開発及び設定した内容についての知的財産権は、著作者人格権を除き、機構に移転するものとする。

ウ. 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、受託者が負うものとする。

以上