
2020 情報システム運用のための総合サービス業務

調達仕様書

Comprehensive Services for Operations of Information Systems 2020

国立研究開発法人情報通信研究機構

経営企画部 情報通信システム室 情報システムグループ

目次

1. 調達件名.....	4
2. 作業の概要.....	4
(1) 目的.....	4
(2) 共通事項.....	4
(3) 業務の概要.....	4
(4) 作業期間.....	4
(5) 作業場所.....	4
(6) 常駐者の必要スキル.....	6
(7) 全体管理.....	9
(8) 作業日.....	9
(9) 運用業務時間.....	10
(10) 貸与品.....	10
(11) 成果提出及び検査.....	10
(12) その他.....	12
3. 各サービスの詳細.....	13
(1) 本部セキュリティ運用サービス.....	13
(2) 本部基幹ネットワーク運用サービス.....	17
(3) 本部基幹サーバ運用サービス.....	25
(4) 本部サポートデスク運用サービス.....	45
(5) 個別システム運用サービス.....	58
(6) 拠点システム運用サービス.....	97
(7) その他.....	115
4. 情報セキュリティ対策.....	117
(1) 再請負.....	117
(2) 情報セキュリティ対策の履行が不十分である場合の対処.....	117

(3) 情報の保護	117
(4) 秘密の保持	117
(5) 情報セキュリティ侵害時における対処	117
(6) 守秘義務に関する誓約書	117
5. 知的財産権等	117
6. 作業場の留意点	118
(1) 作業安全計画	118
(2) 事故防止	118
(3) 防火管理	118
(4) 災害防止等の措置	118
7. その他	118

別紙 1 情報システムグループサポートデスク利用に関する満足度アンケート調査

別紙 2 入札資料閲覧に関する誓約書

別紙 3 守秘義務に関する誓約書

※本調達仕様書は昨今の情報セキュリティ事情を鑑み、本文中下線を引いた部分について、メーカー名、機器名、ソフトウェア名、バージョン等を非開示としている。非開示情報については「入札関係資料閲覧に関する誓約書」を提出後、資料閲覧会にて開示とする。

1. 調達件名

2020 情報システム運用のための総合サービス業務

Comprehensive Services for Operations of Information Systems 2020

2. 作業の概要

(1) 目的

本仕様書の内容は国立研究開発法人情報通信研究機構（以下「当機構」という。）が当機構内へのサービスとして運用している当機構内ネットワーク及び情報サービス（経営企画部 情報通信システム室 情報システムグループが所管するもの。以下同様）を維持運用するとともに良好なネットワークの構築、外部ネットワークとの安全な接続、当機構内ユーザの情報サービス提供及び支援を行うことを目的とする。

(2) 共通事項

作業の実施にあたっては関係する法令及び受注者に対し適用される条例を遵守するものとする。本仕様書に疑義が生じた場合、または本仕様書に記載のない事項の詳細を決定する場合は、当機構担当者と速やかに協議し解決を図ること。協議に際しては、受注者において打ち合わせ議事録を作成すること。作成した議事録は、当機構の承認を得て発行する。発行した打ち合わせ議事録に含まれる決定事項は、本仕様書に優先する。なお、仕様書等の変更を要する事態が生じた場合には、協議をするので応じること。

(3) 業務の概要

本調達ではユーザがクライアント計算機を用いてインターネットアクセス・メールの送受信・共有ファイルの利用等、一般的なサービス利用を行うための運用、及び当機構における研究へのネットワークサポート、サーバサービスサポートを行うためのものである。

本調達で運用する主なサービスは以下のとおり。

- ア 本部セキュリティ運用サービス
- イ 本部基幹ネットワーク運用サービス
- ウ 本部基幹サーバ運用サービス
- エ 本部サポートデスク運用サービス
- オ 個別システム運用サービス
- カ 拠点システム運用サービス
- キ その他

(4) 作業期間

2020年4月1日から2022年3月31日まで

作業の継続性を考慮し、本作業期間より前に引継ぎ期間を2020年2月3日から設けること。

(5) 作業場所

ア 作業場所

- i 国立研究開発法人情報通信研究機構本部（以下「本部」という。）

所在地：東京都小金井市貫井北町4-2-1

本部の作業場所は上記のとおりであるが、他拠点の障害対応、セキュリティインシデン

ト、ユーザ対応、構築作業等の支援や、及び地方拠点への出張作業もある。
本部内に個別のスペースを取り、作業期間中は最大 25 席を用意する。

ii 未来 ICT 研究所

所在地：兵庫県神戸市西区岩岡町岩岡 588-2

未来 ICT 研究所内に個別のスペースを取り、作業期間中は最大 2 席を用意する。

iii 脳情報通信融合研究センター

所在地：大阪府吹田市山田丘 1-4

脳情報通信融合研究センター内に個別のスペースを取り、作業期間中は最大 4 席を用意する。

iv ユニバーサルコミュニケーション研究所（けいはんな）

所在地：京都府相楽郡精華町光台 3-5

ユニバーサルコミュニケーション研究所内に個別のスペースを取り、作業期間中は 1 席を用意する。

v 鹿島宇宙技術センター

所在地：茨城県鹿嶋市平井 893-1

鹿島宇宙技術センター内に個別のスペースを取り、作業期間中は 1 席を用意する。

vi ワイヤレスネットワーク総合研究センター

所在地：神奈川県横須賀市光の丘 3-4

ワイヤレスネットワーク総合研究センター内に個別のスペースを取り、作業期間中は 1 席を用意する。

上記拠点毎の席数はあくまでも参考情報であり、必要な常駐人員数は受注者において判断すること。席数が不足する場合、当機構と協議を行うこと。

上記以外の地方拠点について、当機構担当者から依頼があった場合は外勤または出張とする。

年間 30 回程度ある。

作業に係る交通費、宿泊費は、別途清算とすること。

（※宿泊費の上限は甲地 11000 円、乙地 10000 円とする）

地方拠点

(ア) 国立研究開発法人情報通信研究機構 総合テストベッド研究開発推進センター（所在地）東京都千代田区大手町 1-8-1 KDDI 大手町ビル 16 階、21 階

(イ) 同 KDDI 大手町（所在地）東京都千代田区大手町 1-8-1 KDDI 大手町ビル 5 階

(ウ) 同 サロベツ電波観測施設（所在地）北海道天塩郡豊富町字上サロベツ 13-1

(エ) 同 山川電波観測施設（所在地）鹿児島県指宿市山川成川 2719

(オ) 同 大洗テストフィールド（所在地）茨城県東茨城郡大洗町磯浜町字盤舟山 7918-8

(カ) 同 犬吠テストフィールド（所在地）千葉県銚子市天王台 9961

(キ) 同 沖縄電磁波技術センター（所在地）沖縄県国頭郡恩納村字恩納 4484

- (ク) 同 大宜味大気・電波観測施設 (所在地) 沖縄県国頭郡大宜味村饒波比謝 1321-1
- (ケ) 同 名護降雨観測施設 (所在地) 沖縄県名護市源河 2575
- (コ) 同 北陸 StarBED 技術センター (所在地) 石川県能見市旭台 2-12
- (サ) 同 耐災害 ICT 研究センター (所在地) 宮城県仙台市青葉区片平 2-1-3
- (シ) 同 うめきた超高速ネットワーク・IoT 実験施設 (所在地) 大阪府大阪市北区大深町 3-1 グランフロント大阪

イ 内国旅行の地域区分

甲地域	埼玉県さいたま市、千葉県千葉市、東京都特別区、神奈川県横浜市及び川崎市、愛知県名古屋市、京都府京都市、大阪府大阪市及び堺市、兵庫県神戸市、広島県広島市、福岡県福岡市
乙地域	上記以外の地域

(6) 常駐者の必要スキル

下記に挙げるスキルを保持していること

担当者種別	内容
総括責任者 総括責任者代行	<ul style="list-style-type: none"> ・収集された課題（脆弱性含む）に優先度を設けて対応できること。 ・配線、敷設、設置等において是正指示を行えること。 ・目的を達成するための十分なリソース（納期、品質、コスト、利益）を計算できること。 ・当機構担当者及び、作業者と円滑にコミュニケーションが行えること。問題が起きた場合、話し合いにより解決する術を持っていること。 ・予定している当機構内イベント及び機器のメンテナンスなどの WBS を作成することができ、当機構担当者・各種ベンダと遅延なく予定を進めることが可能であること。 ・近年の情報通信技術に精通しており、当機構担当者及び各担当者と技術的打ち合わせを行うことが可能であること。 ・起こりうるリスクを想定し、その大きさを軽減するために回避策・軽減策を考え、当機構担当者に提案することが可能であること。
ネットワーク担当者 サーバ担当者 セキュリティ 共通事項	<ul style="list-style-type: none"> ・英語サイトからの情報を収集し、和訳意識できること。 ・セキュリティ情報を収集できること。 ・ケーブル類の特性を考慮し、美観、取回しに考慮して配線、施工が行えること。 ・空冷効果、保守交換の容易性を考慮して機器の設置、ラックマウントを行えること。 ・監視及び運用オペレーションにおける効率化（プログラミングを含む）

	<p>や提案を行えること。</p> <ul style="list-style-type: none"> ・識別性を考慮したタグ付け、マーキングを機器に行えること。
<p>ネットワーク担当者個別スキル (当機構利用機器を運用するためのスキル)</p>	<ul style="list-style-type: none"> ・プロジェクト管理、ネットワーク設計、ユーザヒアリング等のネットワークコンサルティングスキルを有する担当が1名以上いること。 ・機器に Vlan を Tagging/Untagging で設定できること。 ・機器に STP をコスト、プライオリティを付けて設定できること。 ・機器にルーティングを静的、動的 (RIP/OSPF) で行えること。 ・経路の冗長をコスト (通信速度、信頼性) を考慮しつつ設計・設定を行えること。 ・機器に ACL、又はフィルタリングポリシーを最適なパフォーマンスを發揮できるよう順序を考慮して記述できること。 ・機器に SNMP、SYSLOG、NTP、Flow の設定が行えること。 ・機器に LAG、STACK の設定が行えること。 ・機器に IPsec VPN の設定が行えること。 ・L2TP、IPIP、EtherIP、VXLAN といったトンネリングプロトコルを用いて広域なネットワークを設計、設定できること。 ・通信経路に応じてパケット (フレーム) のサイズを最適な大きさに設計、設定できること。 ・機器の設定を別の機器を介して確認できること。 ・機器監視の為、MRTG、Nagios に設定追加、削除、変更が行えること。 ・通信のキャプチャ及び、キャプチャ内容の解析を行えること。
<p>サーバ担当者</p>	<ul style="list-style-type: none"> ・プロジェクト管理、サーバ設計、ユーザヒアリング等のサーバコンサルティングスキルを有する担当が1名以上いること。 ・サーバ管理コンソール (IPMI/XSCF) の操作が行えること。 ・サーバのエラーメッセージを元にサポートへの問い合わせ、保守交換が実施できること。 ・<u>ストレージプライアンスの管理、設定ができること。</u> ・各物理サーバにおいて RAID 管理、設定ができること。 ・Solaris ZFS においてストレージ管理、設定ができること。 ・Solaris 及び Linux 上において仮想ネットワークを管理、設定ができること。 ・UNIX 系 OS を CUI のみで管理できること。 ・Active Directory 及び Terminal Services の構成管理、設定ができること。 ・SCCM(Microsoft System Center Configuration Manager)の管理、設定および計算機へのソフトウェア配信操作ができること。

	<ul style="list-style-type: none"> ・ <u>CMS のバージョンアップができること。</u> ・ VMware ESXi 5.5/6.0/6.5/6.7 及び vCenter 6.5/6.7 において仮想マシン及び仮想ネットワークの構成管理、設定ができること。 ・ Windows Server 2012/ 2016/ 2019 の管理、設定ができること。 ・ Red Hat Enterprise Linux 6 /7/ 8 (EUS, ELS 含む) の管理、設定ができること。 ・ Solaris Global Zone/Non-Global Zone/Kernel Zone の管理、設定ができること。 ・ <u>ロードバランサの管理、設定ができること。</u> ・ OSS ソフトウェア (Apache HTTP Server、Postfix、Sendmail、NTPD、BIND 等) の管理、設定ができること。 ・ 通信経路に応じてパケット (フレーム) のサイズを最適な大きさに設計、設定できること。
セキュリティ担当者	<ul style="list-style-type: none"> ・ CSIRT の実務業務ができること。 ・ ネットワーク、サーバ、クライアントのセキュリティ診断が行えること。 ・ <u>ウイルス対策ソフトや USB メモリ型ウイルス対策ソフトを利用してウイルス・マルウェア感染等の調査・解析が行えること。</u> ・ 標的型攻撃の疑いがあるメールの調査、解析等の対応が行えること。 ・ <u>端末インストール型の振る舞い検知ソフトウェアによる未知のマルウェアの対応が行えること。検知されたアラートについて、詳細解析ソフトウェアにより該当ファイルの挙動を解析し、必要に応じて当該外部通信の遮断を行えること。</u> ・ NW 機器の ARP/MAC アドレステーブル調査、Proxy のログ解析により端末特定が行えること。 ・ 各種ファイアウォール、IPS/IDS、標的型攻撃対策装置、サンドボックス、アンチウイルス装置、Web セキュリティ装置の操作、ログ確認が行えること。 ・ ログ情報等から各種調査を行うため、UNIX/Linux 等のコマンドラインを用いて文字列抽出、整形が行えること。 ・ セキュリティインシデント時の影響範囲、被害状況の調査、被害拡大防止策の検討が行えること。
サポートデスク担当者	<ul style="list-style-type: none"> ・ 一般的な計算機に関する知識を有し、USB 等外部機器の接続、ハードディスクやメモリ増設交換を行えること。 ・ 機器のエラー音、異常表示などからメーカーサポートへ問い合わせ、保守依頼を行えること。 ・ MS Office Word、Excel、Office365 に関する問い合わせについて、ドキュメント、事例を調査して回答できること。

	<ul style="list-style-type: none"> ・日本語ローマ字入力において、30 文字/分以上のキー入力操作が行えること。 ・Windows や macOS を用いて、無線 LAN 接続を行えること。 ・IE、Firefox、Safari、Chrome を用いて Web ブラウジング行えること。手順に従い Web アプリケーションの接続試験を行えること。 ・TeraTerm / PuTTY 等のターミナルソフトウェアによる接続及び vi/vim を用いてテキスト編集を行えること。
--	--

(7) 全体管理

- i 本部に総括責任者（管理責任者）を置き、作業者の総括を行う。他の作業者の取りまとめを行い、当機構内のネットワーク、サーバ、及びアプリケーション（サービス）に関する安定稼働に努めること。
- ii 受注者及び総括責任者は作業依頼の窓口となること。当機構担当者から、作業依頼があった際に、他の作業者に対し速やかに作業を実施させること。
- iii 日々の作業報告は本部の総括責任者あるいは総括責任者代行（両者とも不在の場合は、その他作業者）が、翌営業日午前中までに、電子メールにて当機構担当者に報告すること。

(8) 作業日

- i 原則として平日（当機構が定める休日(12月29日から1月3日)を除く）とする。
- ii 当機構を一般に公開する日は（本部、未来 ICT 研究所、ユニバーサルコミュニケーション研究所、鹿島宇宙技術センター、脳情報通信融合研究センター）、それが平日以外であっても、平日同様のサービス提供を行うこと。平日以外の一般の公開日は作業期間中に 2 日以内とする。
- iii 本部、未来 ICT 研究所、ユニバーサルコミュニケーション研究所、鹿島宇宙技術センター、脳情報通信融合研究センター、耐災害 ICT 研究センター、ワイヤレスネットワーク総合研究センター計画停電時には、サーバ担当及びネットワーク担当、又は相当の技術を有するものが対応を行うこと。平日以外の計画停電は作業期間中に 3 日以内とする。
- iv 土曜日、日曜日、国民の休日及び当機構が定める休日に作業の必要が生じた場合には当機構担当者と協議の上、作業を行うこと。
- v 突発的な停電に対応できる体制を整備し、事態に対応すること。
- vi 突発的なセキュリティインシデントに対応できる体制を整備し、事態に対応すること。（要員の継続的なスキルアップや情報収集もこれに含む）
- vii 突発的なシステム障害（イントラネット、インターネット双方における）に対応できる体制を整備し、事態に対応すること。（要員の継続的なスキルアップや情報収集もこれに含む）
- viii 鹿島宇宙技術センターには月、水、金の週 3 日の常駐とし、祝日等で該当の曜日が平日でない場合は常駐としない。
- ix 耐災害 ICT 研究センターの作業は、ネットワーク経由での遠隔作業を基本とするが必要な際には出張して現地での作業を行う。
- x ワイヤレスネットワーク総合研究センターの作業は、少なくとも 1 回/月以上、現地にて機

器の目視確認および管理資料の整理を行うこと。日程については当機構担当者と協議し決定すること。

(9) 運用業務時間

- i 各常駐場所の運用業務時間は以下の通り。
 - a 本部
作業時間：8時30分～18時15分とする。
ただし、3(5)エ(ウ)Avに示すCMSサーバのメンテナンス作業については、平日18時15分～22時00分までを目安として対応をすること。CMSサーバのメンテナンス作業は月2回程度(OS、CMSアプリケーション)とする。
日程は当機構担当者と調整して決めること。
 - b 未来ICT研究所
作業時間：9時30分～17時30分とする。
 - c 脳情報通信融合研究センター
作業時間：9時30分～18時00分とする。
 - d ユニバーサルコミュニケーション研究所(けいはんな)
常駐作業時間：9時00分～17時00分とする。
 - e 鹿島宇宙技術センター
作業時間：8時30分～17時00分とする
 - f ワイヤレスネットワーク総合研究センター
作業時間：9時00分～17時00分とする。
- ii ネットワークダウンあるいはそれに準ずる緊急事態が発生した場合、あらかじめ定めた連絡方法に従い、遅延なく当機構担当者に報告し、各対応(復旧等)を行うこと。
- iii 業務の内容上、上記作業時間外に作業を行わなければならない可能性もあるが、当機構担当者と協議の上、実施をすること。
- iv 公共交通機関の遅延や災害等の不可抗力により、サービス提供開始時刻が遅れた場合には報告すること。

(10) 貸与品

- i 作業に必要な文具などは、受注者において用意すること。
- ii 受注者の会社との連絡等のための電話機本体、電話回線使用料、ファクシミリ用紙が必要な場合は受注者側で用意すること。
- iii 情報セキュリティ上、運用業務上で利用するネットワーク機器、サーバ、計算機、プリンタ(用紙を含む)が必要な場合は、当機構で用意し貸与する。

(11) 成果提出及び検査

- ア 作業日報
毎日、作業報告書(日報)を本部情報システムグループ及び以下拠点の当機構担当者に送付すること。
 - A 未来ICT研究所
未来ICT研究所企画室神戸管理グループ

- B 脳情報通信融合研究センター
脳情報通信融合研究センター企画室吹田管理グループ
- C ユニバーサルコミュニケーション研究所（けいはんな）
ユニバーサルコミュニケーション研究所企画室けいはんな管理グループ
- D 鹿島宇宙技術センター
ワイヤレスネットワーク総合研究センター企画室鹿島管理グループ
- E 耐災害 ICT 研究センター
ソーシャルイノベーションユニット耐災害 ICT 研究センター企画連携推進室
- F ワイヤレスネットワーク総合研究センター
ワイヤレスネットワーク総合研究センター企画室横須賀管理グループ

イ 月例報告

毎月、本部、各拠点で定例会（月例会）を開催し、作業内容について報告書1部を提出し当機構の確認を受けること。月例報告書へはネットワーク関連に関する作業の報告の他に、改善提案等がある場合は記載すること。ただし、耐災害 ICT 研究センターは当機構の TV 会議システムを用いて行うこと。ワイヤレスネットワーク研究所は定例会（月例会）を開催しない。本部及び各拠点の月例報告書の提出先は以下のとおりとする。

- A 本部
経営企画部情報通信システム室情報システムグループ
- B 未来 ICT 研究所
未来 ICT 研究所企画室神戸管理グループ、経営企画部情報通信システム室情報システムグループ
- C 脳情報通信融合研究センター
脳情報通信融合研究センター企画室吹田管理グループ、経営企画部情報通信システム室情報システムグループ
- D ユニバーサルコミュニケーション研究所（けいはんな）
ユニバーサルコミュニケーション研究所企画室けいはんな管理グループ、経営企画部情報通信システム室情報システムグループ
- E 鹿島宇宙技術センター
ワイヤレスネットワーク総合研究センター企画室鹿島管理グループ、経営企画部情報通信システム室情報システムグループ
- F 耐災害 ICT 研究センター
ソーシャルイノベーションユニット耐災害 ICT 研究センター企画連携推進室、経営企画部情報通信システム室情報システムグループ
- G ワイヤレスネットワーク研究所
ワイヤレスネットワーク総合研究センター企画室横須賀管理グループ、経営企画部情報通信システム室情報システムグループ

ウ 年次報告

毎年、本部で年次報告会を開催し、以下の設計書、手順書について報告書1部・データ方式

1 式、を提出し確認を受けること。提出先は経営企画部情報通信システム室情報システムグループとする。

- A システム設計書（年次）
- B システム障害時対応手順書（年次）
- C システム運行手順書（年次）
- D プログラム設計書（年次）

エ 検査

提出された報告書等に基づき当機構担当者が検査を実施する。

(12) その他

- i 運送・搬入・据付け実施中に、建築物、工作物等に損傷を与えた場合は、速やかに当機構担当者に申し出るとともに受注者の責任においてこれを原形に復すること。
- ii 業務上知り得た機密事項及び個人情報については、他に公言・持ち出し・利用をしないこと。万一、機密事項又は個人情報の漏洩等が発生したことを知った場合には、速やかに当機構担当者に報告すること。
- iii 本契約の実施において常駐者、作業者に下請業者等が加わる場合は、あらかじめ当機構担当者と協議し了承を得ること。
- iv 最新のネットワーク、セキュリティ及び各種サーバシステムの障害情報に基づいた障害予防処置を講ずるために、最新の情報が収集、把握されていること。
- v 常駐する作業者が交代する場合は、原則として 1 か月以上前に当機構担当者に報告すること。
- vi 受注者は、当機構のセキュリティ規程等の内規を遵守できないなど、当機構の作業者としてふさわしくないと判断した場合は常駐作業者を交代させること。
- vii 受注者は作業開始の前に当機構担当者等と調整し、業務内容を十分把握し、作業開始日から業務を行えるようにすること。また、その期間にかかる費用については受注者の負担とし、契約日から業務を行える根拠を明示すること。また、本契約終了時に引継ぎ体制を提供すること。本契約の開始又は終了時の引継ぎ期間は 1 か月、常駐とし、当該期間内での業務引継ぎを行うこと。なお、引継ぎ作業は、プログラム設計書、システム設計書といった既存のドキュメントをベースに行うこと。
引継ぎ時は作業スケジュール、進捗報告書を週 1 回提出すること。
- viii 受注者は作業者を支援する体制を常時用意し、常駐作業者に何かあるときはすぐに同等の技能を持つ作業者と交替すること。
- ix 受注者は本部に他拠点を支援する体制を常時用意し、他拠点で何かあるときは現地に派遣できるようにすること。
- x 本作業の範囲で作成されたプログラム、データ、管理メモは当機構に帰属し受注者の判断によって削除することはできない。
- xi 当機構内に対し英語による周知、外国籍職員からの英語（メール、電話、口頭）による問合せに対し英語で対応できるものが作業者にいること。TOEIC700 点以上又は他資格の場合は同等のスコア以上とすること。

3. 各サービスの詳細

(1) 本部セキュリティ運用サービス

ア 概要

当機構内セキュリティ装置を正常状態に維持し、その運用を行うとともに、セキュリティインシデント発生の際に対応を行うこと。内閣サイバーセキュリティセンター（NISC）等の関係機関や、当機構の情報セキュリティ委員会事務局等からの依頼対応を行うこと。新たなインシデント対策を検討しセキュリティに対して必要な対策を行い、当機構を不正な行為から保護することを目的とする。

イ 対象機器

機器タイプ	台数
ファイアウォール/UTM	23
IPS/IDS	6
標的型攻撃対策/サンドボックス	7
Webセキュリティ装置	5

注) 2020年4月1日の時点では、機器リプレース、OSバージョンアップにより変更されている可能性もある。またこれらの各機器は随時変更することがあり、その都度、必要な対応を行うこと。(新機器設置作業や動作確認等)

※一部は当機構サイバーセキュリティ研究所サイバーセキュリティ研究室との共同運用

ウ 業務内容

(ア) セキュリティコンサルティング

A 情報セキュリティポリシーの理解と徹底

政府の情報セキュリティ方針や施策、当機構の情報セキュリティポリシー等を理解し、情報セキュリティ運用サービスとの適合性を把握すること。

B トラヒック及びログ分析手法の検討、提示

トラヒック及びログ分析のための定義、検索のロジック、相関分析手法の考え方を明示すること。この定義・手法については運用開始時に当機構担当者に明示しなければならない。

C プログラミングについての指導、チェック

利用者のプログラミングについての指導、是正案のコードの提示、安全性のチェック(機械ではなく人間の手による)を行うこと。対象プログラミングはShell-Script、Perl、Python、PHP、JavaScriptとし、それ以外についてもプログラミングの一般的な視点において対応を行うこと。

D システム、ネットワーク等の脆弱性の把握、対策の検討、実施

当機構のシステム構成や状態を詳細に把握し、情報システムグループや関係各所との協議や調整において、具体的な情報の提示や施策の可否等を迅速に判断できること。

E セキュリティ課題の提示と対策の検討、実施

当機構におけるセキュリティ課題の提示と対策の検討、実施を行うこと。運用開始時にセキュリティの課題を提示し、四半期(3 か月)ごとに対策及び実施報告を行うこと。

F 情報セキュリティ侵害の対応

情報セキュリティ侵害が発生した場合若しくはその恐れがある場合には、速やかに情報システムグループに報告すること。該当する事象として以下も含めて考慮すること。

- ・受注者に提供する当機構の情報の外部漏えい及び目的外利用
- ・受注者による当機構の本請負業務以外の情報へのアクセス

(イ) 情報セキュリティ委員会支援

A セキュリティ攻撃に対する訓練の実施支援

当機構内で実施されるセキュリティ攻撃に対する訓練の実施を関係各所と調整、協力して年に2回実施すること。

B 関係機関からの調査依頼、対応支援

内閣サイバーセキュリティセンター (NISC) 等、関係機関からの調査依頼や対応要請への支援を行うこと。関係機関からの脆弱性対応状況調査等、緊急性の高い依頼については当機構担当者と協議の上、当日中に機構内全体への周知、各窓口、セキュリティ管理者等への問合せを実施すること。問合せの実施にあたり、回答フォーマットや対策手順等の案内が必要な場合は適宜作成すること。回答について進捗管理し、取りまとめが完了するまで対応を継続すること。結果は、関係機関が求める回答期限までに当機構担当者に報告すること。

C 情報セキュリティカードの配布対応

当機構内の新規配属者に対して情報セキュリティカードの配布をすること。

D 情報セキュリティポリシーに関する利用者問合せ対応

当機構内利用者からの情報セキュリティポリシーに関する問合せに対応すること。

E 外部電磁的記録媒体棚卸支援

外部電磁的記録媒体棚卸作業において、各研究所企画室等への自己点検表の送付、結果集計を実施すること

- i 年に1回の外部電磁的記録媒体棚卸において当機構の指示に基づき、各研究所企画室等窓口への自己点検表の送付、点検結果の回収及び点検結果の集計を行い、当機構担当者へ報告すること
- ii 自己点検の集計対象となる組織は合計100以下であるが、一時的に対象組織が50以上増加する場合には別途協議の上で実施することとする
- iii 点検結果の集計方法については事前に当機構担当者と協議の上決定すること

(ウ) NICT-CSIRT 支援

A セキュリティインシデント対応支援

セキュリティインシデント発生時には情報の収集、分析、問題の特定、解析、対策

案の検討、協議、(運用員に対する)被害拡大防止策の指示、対応の状況確認、報告等を迅速に行うこと。また、十分な体制を組むこと。インシデント発生時における、初動にかかる時間は平日運用業務時間であればおおむね 1 時間、それ以外では可能な限り迅速に対応すること。

セキュリティインシデント発生後には各種証跡を分析し、発生源や影響範囲等の調査、外部への影響や潜在的な危険性等を報告すること。初動対応及び 1 次報告はおおむね 24 時間以内に提出し、それ以降の報告に関しては当機構担当者と協議の上報告すること。

B インシデント報告書取りまとめ

セキュリティインシデント発生時には、該当利用者に対してインシデント報告書の提出を依頼すること。また、提出された報告書の取りまとめを実施し、機構担当者へ報告すること。

C 第二 GSOC(Government Security Operation Coordination team)の不正通信監視サービス提供情報の活用

- i IPA が運営する第二 GSOC 上の情報を機構担当者より提供を受け、確認、対応すること。なお、対応内容については、機構担当者と協議をすること。
- ii 第二 GSOC の提供情報確認手順、対応フローを整備、維持管理すること。
- iii 提供情報を元に、機構内のネットワークおよびシステムへの影響等の一次調査を実施し、機構担当者に調査結果の報告をすること。
- iv 一次調査の結果、詳細調査が必要な場合は、関係各所と調整の上、詳細調査を実施し、機構担当者に調査結果の報告をすること。

(エ) SOC 業務

A セキュリティ情報の収集、分析・配信

- i 下記に示す組織および Web サイトや IT 系ニュースサイト等の情報を基に、不正アクセス及びセキュリティ対策等に関する最新動向について日々情報収集を実施すること。実施方法については手順にまとめること。
 - ・ JPCERT/CC (JPCERT コーディネーションセンター)
 - ・ IPA (独立行政法人 情報処理推進機構)
 - ・ NISC (内閣サイバーセキュリティセンター)
 - ・ CVE (Common Vulnerabilities and Exposures)
 - ・ JVN (Japan Vulnerability Notes)
- ii 収集した情報を総合的に分析し、必要に応じて機構内に周知、注意喚起として情報配信すること。また必要に応じて措置を講じること。

B ネットワークセキュリティ監視

- i セキュリティ装置のアラートのログ分析、及び被疑箇所を特定し、影響範囲の調査、早急な対処を実施すること。
- ii 標的型攻撃の疑いがあるメールを確認した場合は、サーバ上のログから当該サイトへのアクセス履歴を確認して影響範囲を調査、報告、取りまとめを行う

こと。当機構内に届いている標的型攻撃メールについて、危険度が高いものや大量に届いているものについては、開封時の被害を事前に調査し、当機構内に注意喚起を実施すること。

- iii 機構内端末から外部の不審な Web サイトへの接続を確認した場合は、該当 Web サイトの安全性に関する調査を行い、不正な Web サイトであった場合にはファイアウォールにて遮断を行うこと。また、遮断後は不正な Web サイトにアクセスしている端末がないか経過観察を実施すること。
- iv 機構内端末が外部 Web サイトから不審なファイルのダウンロードを確認した場合は、該当ファイルの安全性に関する調査を行い、不正なファイルであった場合には、利用者端末へのインストール状況を調査の上、削除方法および必要な復旧処置を利用者に案内すること。
- v リソースやトラフィックの状況・内容を監視し、傾向分析やログの相関分析等を行い、異常検知を行うこと。
- vi ネットワーク、サーバに対し不正接続の有無を監視し、不正接続を発見した場合は当機構担当者に報告し、対処すること。当機構内にある不正計算機検知装置等を利用し、ネットワークに対する不正接続計算機の監視を行うこと。また、不正計算機検知装置等から収集されるログを管理すること。
- vii FW、IPS のセキュリティ装置の設定（ポリシーの有効性確認）の棚卸を年 2 回以上行い、外部接続申請等の関連する資料の更新を行うこと。

C エンドポイントセキュリティ監視

- i ウィルス対策ソフトウェアの監視等の対応
 - a ウィルス対策ソフトウェアによる監視を行うこと。
 - b ウィルス・マルウェア等、悪意あるソフトウェアに感染した事例を発見した場合における端末の特定や、利用者への駆除の依頼、感染の疑いがあるファイル（検体）の特定を行い報告すること。
 - c 対応した履歴を書面にまとめること。また拡散防止に協力すること。
- ii 振る舞い検知ソフトウェアによる未知のマルウェアの対応
 - a 振る舞い検知ソフトウェアにより検知されたアラートの解析、レポート等の運用フロー、運用手順書を整備すること。
 - b 振る舞い検知ソフトウェアにより検知されたアラートについて、詳細解析ソフトウェアにより該当ファイルの挙動を解析し、必要に応じて当該外部通信の遮断を行うこと。
 - c 正常な通信を阻害しないようにホワイトリストを整備し随時更新すること。
 - d 詳細解析ソフトウェアによる解析、遮断、レポートを提出すること。提出は年間 240 件を目安とすること。

D セキュリティ診断

- i 当機構の内部ネットワーク、内部ネットワークに接続する端末を対象に当機

構が提供する診断ツールを用いてネットワーク診断を行い、脆弱性のある OS やサポート切れ OS の使用状況、共有フォルダのアクセス制御状況等の確認を月に 1 回実施すること。

ii 診断にて検出された脆弱性に対して、端末利用者を特定し脆弱性対処を依頼すること。この際、診断結果については必要な情報を利用者に分かりやすい形で提供すること。診断結果に対する問合せに対応し、利用者の脆弱性対策を支援すること。

iii 脆弱性対策後、再診断を実施し脆弱性が是正されている事を確認すること。

(オ) セキュリティポータルサイトの維持管理

脆弱性情報やセキュリティ対策等セキュリティ管理に関する情報を、依頼に基づき、Web サイトに掲載し、更新をすること。

(カ) セキュリティ関連申請対応

A 外部ネットワーク接続申請対応

i ネットワーク、サーバの再構築等を行う場合、当機構が実施するセキュリティチェックに合格するように構築すること。

ii 各研究室が再構築したサーバが当機構にて実施するセキュリティチェックに合格するように、OS、ソフトウェアの脆弱性、設定項目のセキュリティチェックを行うこと。また、外部 Web コンテンツ（静的/動的）のセキュリティチェックを実施すること。

B 電子情報記録媒体外部持ち出し許可申請対応

電子情報記録媒体の持ち込み、持ち出しにおいてセキュリティ関連の問合せ対応を行うこと。

(キ) 他拠点の支援作業

他拠点のセキュリティインシデント等の支援を行うこと。

当機構担当者と協議の上、他拠点に出張し、支援が行えるようにすること。

(2) 本部基幹ネットワーク運用サービス

ア 概要

ネットワーク担当 SE が常駐しネットワーク（監視、制御装置などを含む）を正常状態に維持し、その運用を行うと共に、利用者に対し支援を行うこと。ここで言う正常状態とは構成する機器が期待される性能により動作することと、当機構内ネットワークが利用者へ安定したサービスを提供すると共に新たなニーズに対応することを含める。

また、当機構内ネットワークのセキュリティに対して必要な対策を行い、当機構ネットワークに対して行われる、不正行為から保護することを目的とする。

イ 対象機器

(ア) ネットワーク及び関連機器

機器種別	台数
------	----

インターネット接続ルータ	2
小型/VPN ルータ	67
L2/L3 スイッチ	254
ファイアウォール/UTM	24
無線 LAN アクセスポイント	222
総計	545

注) 2020年4月1日の時点では、機器新設、リプレース、OSバージョンアップにより変更されている可能性もある。またこれらの各機器は随時変更することがあり、その都度、必要な対応を行うこと。(新機器設置作業や動作確認等)

(イ) 対象ネットワーク

区分	対象
当機構内	本部ネットワーク
	本部ー各地方研究所センター・観測施設間ネットワーク
	支援系ネットワーク
	開発用ネットワーク
	お客様ネットワーク
	無線 LAN
当機構外	外部ネットワークの接続支援
	外部接続用貸出ネットワークの接続支援

ウ 業務内容

(ア) ネットワークコンサルティング

A ネットワーク更改計画、構成案の検討、作成

当機構担当者と協議の上、ネットワークの更改計画、構成の最適化の検討及び更改、構成の最適化に係る資料を作成し、当機構担当者から承認を得ること。2020年4月1日の時点では以下の作業を予定している。予定は随時変更することがあり、その都度必要な対応を行うこと。

- ・地方拠点のスイッチの更改
- ・本部エッジスイッチの更改
- ・支援系ネットワークの更改
- ・本部ネットワーク、本部ー各地方研究所センター・観測施設間ネットワークの増速(1G→10G、10G→40G等)

B ネットワークの性能調査及び評価、改善検討

- i ネットワークのトラフィックは適時監視を行い、トラフィックに問題がある場合、問題ごとに状況と原因について調査し、改善のための提案を行い、当機構担当者と協議の上、必要に応じて改善を行うこと。
- ii MRTG や NetFlow Analyzer 等すでに構築してあるツールを使用してトラ

- フィック情報の収集を行うこと。
- iii 地方センターや外部接続ネットワーク担当等よりネットワーク機器のトラフィック及びパフォーマンス等に関し、調査依頼があった場合、本部が主体となって必要な情報収集を行うこと
 - iv 運用開始時にネットワークの課題を提示し、四半期(3 か月)ごとに対策及び実施報告を行うこと。
- C ネットワーク構成変更・追加の検討
- i 当機構担当者と協議の上、必要に応じて IPv4/IPv6 に関するネットワーク設計（経路情報制御を含む。）、構成機器選定、機器設定、機器交換（性能不足・老朽化対応）について、機能、信頼性、整合性を調査し技術的提案を行うこと。
 - ii 設定情報等の技術的な事項に関する提案を行い、当機構担当者と協議の上、設計、パラメータ設定、性能試験、機能検証等を行い、ネットワークの運用改善及び再構築を随時行うこと。
 - iii 運用開始時にネットワークの設計における技術提案を行い、四半期(3 か月)ごとに対策及び実施報告を行うこと。
- D サーバ設置、接続に係る外部接続支援対応
- 当機構内の利用者からのサーバ設置、外部公開、外部接続に関するネットワークコンサルティング、コンサルティングの記録を報告書としてまとめること。
- E ネットワーク機器の保守内容の検討
- 既存ネットワーク機器の保守（仕様、条件、内容等）の見直しの検討を行うこと。
- F セキュリティ対策の検討
- i セキュリティ情報の収集
- Computer Emergency Response Team (CERT) Advisory 情報などをもとに不正アクセス及びセキュリティ対策等に関する最新の動向についての情報収集を実施するとともに、ネットワークにセキュリティ上の脆弱性等が発見された場合は、速やかに当機構担当者に連絡すること。また、保守状況を確認し、提供元に報告するとともに、その対応策についてのアドバイス及び対策のためのシステム環境設定を実施すること。情報収集の対象は一次情報の最も多い英語圏を含めること。
- ii セキュリティ管理
- 設定情報等の技術的な事項に関する提案を行い、当機構担当者と協議の上、ネットワークに関するセキュリティ管理について当機構が指定する法人等と協力の上、ネットワーク機器が不正に操作、又は利用されることのないよう対策すること。使用するファームウェアなどのセキュリティ情報を継続的に入手すること。問題が生じた場合は速やかに必要な処置をとり、当機構担当

者へ報告すること。日本語での情報が未公開・未翻訳である場合は、英語圏の情報を意識し注意喚起及び対応を行うこと。

(イ) ネットワーク設計・構築

A ネットワーク設計・構築対応

当機構担当者と協議の上、ネットワークの設計、構築、導入、試験作業を行うこと。構築計画書、システム設計書、構築手順書、システム試験成績書等の図書及びシステム運行手順書を作成し、当機構担当者から承認を得ること。構築する上で、当機構担当者及び関係部署との工程管理及び構築全般に関わる調整を実施すること。

2020年4月1日の時点では以下の作業を予定している。予定は随時変更することがあり、その都度必要な対応を行うこと。必要な機材は当機構担当者から支給する。

- ・地方拠点のスイッチの更改
- ・本部エッジスイッチの更改
- ・事務系ネットワークの更改
- ・本部ネットワーク、本部－各地方研究所センター・観測施設間ネットワークの増速（1G→10G、10G→40G等）

B ネットワーク機器の接続対応支援

本部におけるネットワーク機器の新規導入及び変更作業時（ネットワークトポロジの変更やサブネットの変更、削除等）の設計、コンフィグレーション作成、性能試験、機能検証等の支援を行うこと。ただし、機器の購入時に別途業者が行う入れ替えには支援を行うとともに、質疑等を行い次回構築や運用維持におけるノウハウを得るものとする。対象となるネットワーク機器は現在市場に販売されていないものも含み、その機器に即時対応し運用できるものとする。ここでのコンフィグレーション作成とは、既存のコンフィグを改変するものも含むが、主に一から設計できることを指す。

C 設置機材追加等の支援

スイッチ等の機能向上等のため、スイッチ等の機種を交換する場合、その付随する作業の支援を行うこと。ネットワークの構成変更等により、契約初期段階で存在していたスイッチの台数が増減することがある。（年40台程度）機器設置作業においては、作業者の安全に配慮すること。取り付けには耐震を考慮すること。機器にラックマウントオプションが存在する場合は、それを使用すること。

(ウ) 各ネットワークで共通 ネットワーク維持管理

A ネットワーク稼働状況の確認

対象ネットワークにおける機器を定常的に観測、監視すること。また、必要なログを採取し、障害発生の予防に努めること。やむを得ずネットワークを停止する場合には、利用者へ周知を行うこと。

B ネットワークの障害対応

- i. トラブル発生時には、UNIX サーバ及びネットワークアナライザ機器等を使用して迅速な障害の切り分け、原因究明を行うと共に、その復旧に必要な処置又は業者との対応を迅速に行うこと。復旧が困難な場合は、速やかに代替のネットワーク機器を予備品から用意し運用を開始すること。バックアップ機がある場合には切替えを行うこと。また、トラブルにともなう利用者への影響について、利用者へ内容の周知を行うこと。運用開始時にセキュリティの課題を提示し、四半期(3 か月)ごとに対策及び実施報告を行うこと。
- ii. トラブルへの対処については、当機構担当者と協議の上、作業を行うものとし、終了時には報告すると共に問題点を検討・分析し、今後の改善事項にフィードバックさせること。トラブル報告書の作成、トラブルの履歴情報を管理すること。
- iii. 当機構担当者と協議の上、ネットワーク機器のファームウェアのアップデートを適時行うこと。
- iv. 研究所・地方センター・観測施設や外部接続ネットワーク担当等よりネットワーク機器に関するトラブル連絡があった場合、本部が主体となって障害対応を行うこと。インターネットの先にある国内外の組織からのトラブル連絡も含まれる。
- v. ネットワーク関連機器の管理作業対象機器のうち、ネットワーク機器及び周辺機器、設置場所、個数等の管理を行うこと。ネットワーク機器及び周辺機器は、予備品も含めて管理すること。問題が生じた場合は速やかに当機構担当者へ報告すること。
- vi. 保守契約情報、保守内容についても適正に管理し、保守内容の見直しの検討、保守契約の継続に向けた当機構担当者や各種保守ベンダとの打ち合わせ等を実施し、必要な保守サポート契約が継続されるように努めること。

C ネットワーク機器の構成管理

当機構に設置されているネットワーク機器の設定の管理及び構成品や設置場所、設定及び保守等に関する情報について資料の作成及び更新を行うこと。構築業者が変更した場合にも情報の引継ぎを行い、更新を行うこと。特にネットワーク構成図については、サーバ機器やストレージ装置等の接続も含めたものとし、Office2013以降又は標準的な Web ブラウザ(IE/Firefox/Chrome)などで閲覧可能な状態にて保存しておくこと。運用開始時に当機構全体のネットワーク構成を確認し、四半期(3 か月)ごとに資料の更新数及び新規作成数の報告を行うこと。

D ネットワーク機器のファームウェアのアップデート

ネットワークのパッチ、ホットフィックスの適用に伴う保守ベンダからの手順入手、現行サービスへの影響、手順、動作確認内容の整備、作業計画の作成の検討等を記載すること。

重要度の高い不具合・脆弱性に対するパッチやホットフィックス等が提供されるまでの間が 1 か月を超える見込みと判断される場合は、ワークアラウンド（一時的な回避・緩和策）といった応急対応を行うこと。

- E イベント対応
当機構全体、各研究所、研究室のイベントに伴うネットワーク環境の構成検討、設定支援を行う。
- F 停電等の対応
停電時自動シャットダウンの設定、自動起動の設定、停電時、復電時の状況確認、正常性確認等を記載すること。
- G ネットワーク機器設計書の維持管理
基幹スイッチ、ルータ等の各ネットワーク機器の設計書を維持すること。ネットワーク構成に変更があった場合は、遅滞無く書類を修正して提出すること。設計書をもとにネットワークを再構築できるレベル及び内容で設計書を作成すること。想定読者は、ネットワークの基礎的知識はあるが SE 経験は無い者とする。
- H ネットワーク構成図の維持管理
基幹スイッチ、ルータからネットワーク構成図を維持すること。ネットワークの構成に変更があった場合は、遅滞無く書類を修正して情報システムグループに提出すること。
- I ネットワーク機器管理表の維持管理
基幹スイッチ、ルータ等の各ネットワーク機器の機種、機器名、シリアル番号、購入時期、保守等の情報が管理されているネットワーク機器管理表を維持すること。ネットワーク構成に変更があった場合や機器交換があった場合等、遅滞無く書類を修正して提出すること。
- J システム障害時対応手順書の維持管理
発生が予想される障害に対し、具体的にどのような手順でシステムを復旧するかを記した障害時対応書を維持すること。予想される障害に変化があった場合、あるいは、手順の見直しを行った場合は、遅滞なく書類を修正して提出すること。
- K 日常業務解説書の維持管理
本契約に基づいて実施する日々の日常業務内容を第三者でも分かるように記した日常業務解説書を維持すること。日常業務内容に変化があった場合、遅滞なく書類を修正して提出すること。ネットワーク異常時の対処方法についてマニュアルを更新すること。
- L 利用マニュアルの維持管理
一般利用者を対象とした、各ネットワークの利用方法に関するマニュアルを維持し、当機構内イントラ Web サーバを用いて公開すること。
- M FAQ のメンテナンス

- i 利用者あるいは当機構担当者から問い合わせがあった場合は、問い合わせ内容を調査し、必要な支援を行うとともに、問い合わせ内容とその回答を、「よくある質問とその答え (FAQ)」として Web サーバに登録し、Web ブラウザで閲覧可能とすること。
- ii 契約前に存在していた FAQ を含めて、登録済内容のメンテナンスを行うこと。
- iii 問い合わせ内容については履歴管理を行うこと。

N 予備機による運用

- i ネットワークで障害が発生し、復旧が困難な場合は速やかに予備機を構築し運用を再開すること。障害についての原因調査及び障害箇所の特定制を行い当機構担当者へ報告すること。
- ii 障害の内容がハードウェアに起因する場合は、該当機器の契約内容を確認し、保守対象品の場合は保守業者に連絡し、修理を依頼すること。
- iii 障害の内容がファームウェアに起因する場合は、当機構担当者と協議の上、ファームウェアの設定ファイルの書き換え、バージョンアップ、パッチ適用などの対処を行うこと。
- iv 障害内容については履歴管理を行うこと。

(エ) 各ネットワークの維持管理業務

A 当機構内・外ネットワークの管理・運用

- i 当機構内ネットワーク以外のネットワーク（外部接続用ネットワーク等）について、当機構内ネットワークに関連する問題については支援を行うこと。

B 外部ネットワーク接続支援

- i 外部ネットワーク接続（APAN、SINET、JGN、JPIX）の運用を支援すること。
- ii 外部ネットワーク接続に必要な機材の設置や維持運用を支援すること。
- iii 広域イーサネット及びバックアップ回線等による当機構との外部接続ポイントの運用支援を行うこと。

C 本部ー各地方研究所・センター・観測施設間ネットワーク運用支援

- i 本部と各地方センター間のネットワーク運用支援を行うこと。
- ii 本部と各観測所間のネットワーク運用支援を行うこと。
- iii 各地方センターへのバックアップ回線の維持・運用を行うこと。
- iv 各地方センターに設置したスイッチの維持運用を行うこと。
- v 各地方センター・観測施設が別途契約する常駐 SE と連携し、ネットワークの運用支援を行うこと。

D 本部及び各拠点ネットワークの維持、運用

- i コア～エッジスイッチの 400 台程度の維持運用を行うこと。
- ii 各建物内 L2、L3、PoE スイッチ及びセキュリティ機器など付帯機器の維持運用を行うこと。
- iii 建物の各居室までの配線情報（パッチパネルや情報コンセント等）の管理を

- 行うこと。
- iv 建屋間の光配線情報（光ケーブル管路やパッチパネル等）の管理を行うこと。
 - v 居室内の光ファイバ、メタルケーブル等の配線を支援すること。
 - vi ポート単位でのループ検知監視を行うこと。
- E 外部接続用ネットワークの接続支援**
- i 利用者が独自に管理するネットワークに対し、必要なネットワーク情報を提供すること。
 - ii 利用者が設定するネットワーク機器全般（セキュリティ装置類を含む）の設置・維持運用に関する技術的な支援をすること。
- F 無線 LAN の管理・運用**
- i 無線 LAN 設置許可申請により申請された無線 LAN 機器のチャンネル等の管理及び無線 LAN のセキュリティについて運用・支援を行うこと。
 - ii 無線 LAN ネットワークの管理を行うこと
 - ・対象拠点は、本部、未来 ICT 研究所、ユニバーサルコミュニケーション研究所、耐災害 ICT 研究センター、うめきた超高速ネットワーク・IoT 実験施設、総合テストベッド研究開発推進センター、イノベーションセンター、北陸 StarBED 技術センターとする。拠点が追加になった際は、対象拠点の管理も行うこと。
 - ・無線 LAN は管理サーバによる集中管理型システムを利用している。
 - ・管理する無線 AP は約 240 台。
 - ・故障時の無線 AP の取り外し、保守交換対応を行うこと。ただし脚立などが必要な高所作業の場合は当機構担当者が実施する
 - ・無線 AP のファームウェアアップデートを適宜実施すること。
 - ・新規設置要望の際は、AP を設定し利用可能となるように対応すること。
 - ・無線 AP の在庫管理、設置状況の管理をすること。
- G 開発用ネットワークの維持・運用**
- i 規模は 20VLAN 程度であり、VLAN 毎に FW ゾーンが分かれている
 - ii 関係した機器が老朽化した際には、これの再構築の提案と実施を行うこと。
 - iii ファイアウォール/UTM の管理を行うこと。
 - iv ファイアウォール/UTM を通過させるサービスについて、当機構担当者と協議し必要に応じて設定変更を行うこと。
 - v 不正利用が発覚した場合は、当機構担当者と協議し、速やかに対処を行うこと。
 - vi 基幹ネットワークとの接続の維持・管理を行うこと。
- H 事務系ネットワークの維持・運用**
- vii 事務系ネットワークの維持・管理を行うこと。
 - viii 関係した機器が老朽化した際には、これの再構築の提案と実施を行うこと。
 - ix ファイアウォール/UTM の管理を行うこと。

- x ファイアウォール/UTM を通過させるサービスについて、当機構担当者と協議し必要に応じて設定変更を行うこと。
- xi 不正利用が発覚した場合は、当機構担当者と協議し、速やかに対処を行うこと。
- xii 認証ネットワークの維持・運用を行うこと。

I お客様ネットワークの維持・運用

- i FTTH サービスを利用してのお客様ネットワークの維持・管理を行うこと。
- ii 関係した機器が老朽化した際には、これの再構築の提案と実施を行うこと。
- iii インターネットへの接続には NAPT を用い、LAN にある端末を WAN から隠匿すること。
- iv LAN-WAN 間に UTM 等を挟み込み、ウイルスやマルウェア等の悪意あるソフトウェアの流入・流出を抑止すること。
- v 目的外の利用が発覚した場合は、当機構担当者と協議し、速やかに対処を行うこと。

(オ) 他拠点の支援業務

他拠点の障害対応、セキュリティインシデント、ユーザ対応、構築作業等の支援を行うこと。当機構担当者と協議の上、他拠点に出張し、支援が行えるようにすること。

(3) 本部基幹サーバ運用サービス

ア 概要

当機構内で情報サービスを提供している UNIX サーバ、Linux サーバ、Windows サーバ、ストレージ装置、アプライアンス機器、共通事務パソコン等の機器及びアプリケーションの維持管理を行うこと。利用者に対し支援を行うこと。当機構内外のサーバ、システムが、利用者へ安定したサービスを提供すると共に新たなニーズに対応することを含める。

また、情報サービスのセキュリティに対して必要な対策を行い、当機構内外からの不正行為から保護すること。

イ 対象機器

(ア) サーバ及び関連機器

Solaris

機能	機種	OS	台数
物理サーバ (SPARC)		Solaris 11 Solaris 10	11
物理サーバ (x86)		Solaris 11	3
仮想サーバ (Solaris Zone)		Solaris 11 Solaris 10	59

Linux

機能	機種	OS	
<u>物理サーバ</u>		<u>Red Hat Enterprise Linux 6/7</u> <u>CentOS 6/7</u>	<u>12</u>
<u>仮想サーバ</u>		<u>Red Hat Enterprise Linux Server 6/7</u> <u>CentOS 6/7</u>	<u>7</u>

仮想化ハイパーバイザ

機能	機種	OS	台数
<u>VMware</u>			<u>5</u>

ストレージ/アプライアンス

機能	機種	OS	台数
<u>ストレージアプライアンス</u>			<u>7</u>
<u>ロードバランサ</u>			<u>4</u>
<u>SSL-VPN</u>			<u>2</u>

Windows

機能	機種	OS	台数
<u>物理サーバ</u>		<u>Windows Server 2008, 2012, 2016</u>	<u>9</u>
<u>仮想サーバ</u>		<u>Windows Server 2008, 2012, 2016</u>	<u>14</u>

注) 2020年4月1日の時点では、機器リプレース、OSバージョンアップにより変更されている可能性もある。またこれらの各機器は随時変更することがあり、その都度、必要な対応を行うこと。(新機器設置作業や動作確認等)

(イ) 対象サービス

No	対象サービス
1	DNS
2	Proxy
3	DHCP
4	NTP
5	LDAP
6	シングルサインオン

7	メール（中継、スプール）
8	スパム（迷惑）メールフィルタ
9	メーリングリスト
10	ウイルスチェック
11	外部公開用 WEB
12	Web コンテンツ管理、CGI
13	Web ホスティング
14	当機構内向け Web
15	内部 Web 検索
16	Webmail
17	SSH
18	リモートアクセス
19	リモートデスクトップ
20	ファイル転送・外部ファイル共有
21	ActiveDirectory
22	端末管理
23	ファイル共有
24	不正端末排除
25	監視
26	運用管理
27	データバックアップ
28	職員情報 DB&オンライン申請(e 申請)
29	共用無線 LAN
30	経路検索
31	外部 Web コンテンツ高速配信
32	ファイル共有（研究系）

ウ 業務内容

(ア) サーバコンサルテーション

A サーバ更改計画、構成案の検討、作成

当機構担当者と協議の上、サーバの更改計画、構成の最適化の検討及び更改、構成の最適化に係る資料を作成し、当機構担当者から承認を得ること。

2020年4月1日の時点では以下の作業を予定している。予定は随時変更することがあり、その都度必要な対応を行うこと。

- ・サーバの仮想化による統合（Linux系、Windows系システムを対象）
- ・運用監視ツールの統一化
- ・ファイルサーバの研究系への展開、容量の拡張
- ・リモートアクセスのサービス見直し

- ・バックアップ、DR(災害復旧)/BCP(事業継続計画)システムの刷新
- B 既存サービス、システムの性能調査及び評価、改善検討
 - i 各サーバシステムの動作状況を随時調査及び評価すること。性能劣化が発生している場合は、そのボトルネックを解明し、性能向上のための提案を行うこと。
 - ii 提案後、当機構担当者と協議の上、必要に応じてサーバシステムの設計、プログラミング、動作試験など行い改善を行うこと。
 - iii 新規にサーバを構築・増設する場合は、当機構担当者と協議の上、システムの設計、プログラミング、動作試験等を行い構築すること。
- C 既存サービス、システムの改修の検討
 - i 当機構が本契約に関わるサーバシステムの改修をする場合は、日々の運用にて利用者から要望された事項や運用管理面の改善事項を提案すること。
 - ii 当機構の指示のもと管理責任者は改修検討の打ち合わせに参加すること。
- D 新サービスの導入支援

当機構が本契約に関わるサーバシステムに接続する新システムを導入する場合は、当機構及び導入業者に対して、利用者への周知、ネットワークの払い出し等の導入支援を行うこと。
- E サーバ設置、接続に係る外部接続支援対応

当機構内の利用者からのサーバ設置、外部公開、外部接続に関するサーバコンサルティング、コンサルティングの記録を報告書としてまとめること。
- F サーバの保守内容の検討

既存サーバ、ストレージ、アプライアンス機器の保守（仕様、条件、内容等）の見直しの検討を行うこと。
- G セキュリティ対策の検討
 - i セキュリティ情報の収集

Computer Emergency Response Team (CERT) Advisory 情報などをもとに不正アクセス及びセキュリティ対策等に関する最新の動向についての情報収集を実施するとともに、サーバで使用している基本ソフトウェアや他にインストールしているソフトウェアにセキュリティ上の脆弱性等が発見された場合は、速やかに当機構担当者に連絡すること。また、保守状況を確認し、システム開発元に報告するとともに、その対応策についてのアドバイス及び対策のためのシステム環境設定を実施すること。情報収集の対象は一次情報の最も多い英語圏を含めること。
 - ii セキュリティ管理

設定情報等の技術的な事項に関する提案を行い、当機構担当者と協議の上、サーバに関するセキュリティ管理について当機構が指定する法人等と協力の上、サーバが不正に操作、又は利用されることのないよう対策すること。使用するソフトウェアなどのセキュリティ情報を継続的に入手すること。問題が生じた場合は速やかに必要な処置をとり、当機構担当者へ報告すること。日本語での情報が未公開・未翻訳である場合は、英語圏の情報を意識し注意喚起及び対応を行うこと。

(イ) サーバ設計・構築

A サーバ設計・構築

当機構担当者と協議の上、サーバの設計、構築、導入、試験作業を行うこと。構築計画書、システム設計書、構築手順書、システム試験成績書等の図書及びシステム運行手順書を作成し、当機構担当者から承認を得ること。

構築する上で、当機構担当者及び関係部署との工程管理及び構築全般に関わる調整を実施すること。

2020年4月1日の時点では以下の作業を予定している。予定は随時変更することがあり、その都度必要な対応を行うこと。必要な機材は当機構担当者から支給する。

- ・サーバの仮想化による統合（Linux系、Windows系システムを対象）
- ・運用監視ツールの統一化
- ・ファイルサーバの研究系NWへの展開、容量の拡張
- ・リモートアクセスサービスの見直し
- ・バックアップ、DR（災害復旧）/BCP（事業継続計画）システムの刷新

B プログラムの作成

- i 手作業による作業ミス解消、作業省力化のために、プログラムの維持及び作成を行うこと。なお、現在稼働しているプログラムは100本程度。
- ii 使用する言語はPerl、Python、C、Java、シェルスクリプト、PowerShell、BATコマンド等とする。

C サーバ等の新規増設作業

構成変更の必要が生じた際、サーバ等の開梱、設置、設定作業を行うこと。増設台数は、1年間あたり、UNIXサーバについては物理または仮想10台、Windowsサーバについては物理または仮想5台、アプライアンス及びストレージ装置は5台を超えないものとする。

D サーバ等の機種交換作業

サーバ等の機能向上等のため、サーバ等の機種交換を行う場合があるので、その作業を行うこと。機種交換の台数は、契約初期段階で存在していたサーバ全数分を超えないこと。（契約時のサーバ等の数が40台であった場合は、1年間のサーバ等の機種交換は40台を超えないものとする。）

サーバの数量は物理、仮想とのそれぞれ1台としてカウントする。

(ウ) 各サービスで共通 サーバ維持管理

A サーバ稼働状態確認

- i サーバの稼働状態（電源ON/OFFの状態）を確認し、電源が投入されていない等、ネットワーク上から確認できないサーバがあった場合は、ネットワークの接続状態を確認の上、状況を当機構担当者に報告するとともに、障害復旧作業を行うこと。
- ii 監視サーバにより他のサーバのCPU使用率、ディスク使用率、メモリ使用率、

ネットワーク等のリソース状況を監視し、異常な負荷・通信を示しているサーバを発見した場合にはその原因を究明、排除、あるいは改善し、当機構担当者に報告すること。

- iii 監視サーバにより他のサーバの CPU 使用率、ディスク使用率、メモリ使用率、ネットワーク等のリソース情報を定期的に収集し、収集した情報をもとに、仮想サーバのサイジングの見直し、最適化、傾向分析を行うこと。
- iv 監視サーバ上で Nagios、MRTG、NetFlow アナライザ、NIRVANA など、すでに構築されている監視ソフトを稼働させ、サーバの稼働状態を常時モニターすること。
- v 監視は Nagios を使用し、マルチベンダ環境を監視できるよう随時設定の追加、見直しを行うこと。(監視プラグインの作成・改修を含む)
- vi 用意された監視機構が無くとも、技術的に可能であればこれを内製し、Nagios へ監視統合を実施すること。
- vii 情報システムグループ管理外の機器であっても必要に応じて監視を検討・実施すること。(例：ネットワーク上の対向機器)
- viii ストレージ監視
 - ・ハードディスク・SSD 等(外付けディスクアレイを含む)の使用量を監視し、ハードディスク・SSD 等の使用量が一定量を越えている場合には、原因を分析し、当機構担当者に報告すること。
 - ・サーバ等のストレージ障害を検知した場合は、障害状態を分析し、当機構担当者に報告すること。また、メーカーへの連絡、修理対象品の梱包作業等を行うこと。
 - ・NAS・SAS などの共有ストレージについては、特定ディスクボリュームが不足傾向にある場合は、予備領域から割当ての設定を行うこと。
- ix Web サーバアクセス状況監視

サーバへのアクセス状況をソフトウェアで監視し、認証機能のついた Web ページで随時閲覧できるようにすること。
- x 通信ポート監視

サーバ又は管理端末で不要ポート及びサービスの稼働状態を監視し、不要ポート及びサービスが起動している機器を発見した場合は速やかに当機構担当者に報告し、サービス停止等の作業を実施すること。
- xi 無停電電源装置監視
 - ・無停電電源装置からの警告等の障害情報が通知された場合は、障害情報を分析して当機構担当者に報告すること。また、メーカーに連絡し、協力して、速やかに復旧作業を行うこと。
 - ・JEMA-MIB 又は RFC 1628 に対応した機器の選定と、監視を行うこと。
- xii OS・ソフト等の状態監視
 - ・サーバから、障害情報が通知された場合は、障害情報を分析して当機構担当者及

びシステム開発元に報告の上、速やかな復旧作業を行うこと。

- ・サーバでのディレクトリサービスシステムのアプリケーション単位で性能情報（CPU 使用率、メモリ使用量等）の異常情報が発見又は通知された場合は、当機構担当者及びシステム開発元に報告すること。
- ・障害で調査を要する場合、又は、当機構担当者から障害調査を依頼された場合は、サーバ等にリモートログインして、障害情報を取得・分析し、復旧作業を行うこと。

xiii ソフトウェア障害監視

- ・サーバから基本ソフトウェアや、他のインストールソフトウェアからの警告等の障害情報が通知された場合は、障害情報を分析して当機構担当者に報告すること。また、メーカー、システム開発元に連絡し、協力して、速やかに復旧作業を行うこと。
- ・オープンソースソフトウェア等における未知の不具合やバグの場合は、当機構担当者に許可を得て修正パッチの作成や開発元へのバグ報告を行うこと。（年間 40 件程度）受注者にて不具合の解消が難しい場合は、代替手段の提案を行うこと。

B サーバの障害対応

- i トラブル発生時には、サービスの確認、機器の **Status** 確認、ログ確認等迅速な障害の切り分け、原因究明を行うと共に、その復旧に必要な処置又は業者との対応を迅速に行うこと。
- ii 復旧が困難な場合は、速やかに代替のサーバ機器を予備品から用意し運用を開始すること。バックアップ機がある場合には切替えを行うこと。また、トラブルにともなう利用者への影響について、利用者へ内容の周知を行うこと。
- iii 運用開始時にセキュリティの課題を提示し、四半期(3 か月)ごとに対策及び実施報告を行うこと。
- iv トラブルへの対処については、当機構担当者と協議の上、作業を行うものとし、終了時には報告すると共に問題点を検討・分析し、今後の改善事項にフィードバックさせること。トラブル報告書の作成、トラブルの履歴情報を管理すること。
- v トラブルの原因が機器のソフトウェアにある場合は、当機構担当者と協議の上、ソフトウェアのバージョンアップを行うこと。

C サーバ関連機器の管理

作業対象機器のうち、サーバ、ストレージ、アプライアンス機器及び周辺機器、設置場所、個数等の管理を行うこと。サーバ、ストレージ、アプライアンス機器及び周辺機器は、予備品も含めて管理すること。問題が生じた場合は速やかに当機構担当者へ報告すること。保守契約情報、保守内容についても適正に管理し、保守内容の見直しの検討、保守契約の継続に向けた当機構担当者や各種保守ベンダとの打ち合わせ等を実施し、必要な保守サポート契約が継続されるように努めること。

D サーバの構成管理

当機構に設置されているサーバ機器の設定の管理及び構成品や設置場所、設定及

び保守等に関する情報について資料の作成及び更新を行うこと。構築業者が変更した場合にも情報の引継ぎを行い、更新を行うこと。特にネットワーク構成図については、サーバ機器やストレージ装置等の接続も含めたものとし、Office2013以降又は標準的な Web ブラウザ (IE/Firefox) などで閲覧可能な状態にて保存しておくこと。運用開始時に当機構全体のネットワーク構成を確認し、四半期(3か月)ごとに資料の更新数及び新規作成数の報告を行うこと。

E 基本ソフト、アプリケーションの管理、バージョンアップ

- i 基本ソフトのバージョンアップを行うこと。基本ソフトウェアのメジャーアップデート (例えば Red Hat Enterprise Linux 6 から Red Hat Enterprise Linux 8 へ、Windows Server 2012 R2 から Windows Server 2019 へ) は、作業期間中に最大 10 台とする。これを超える場合当機構と協議を行うこと。

マイナーアップデートやパッチについては回数の上限は設定しない (無制限)。

セキュリティの観点から (原則) 毎月定例的にアップデートを行うこと。なお、作業にあたっては、年間計画を作成の上、当機構担当者の承認を受けてから作業すること。なお、緊急のアップデートが必要な場合は、速やかに対処を実施すること。アップデートができない場合は、機構担当者との協議の上、代替処置を講ずること。

- ii サーバ・クライアントシステムを運用する上で必要となるアプリケーションのインストール、バージョンアップを行い、バージョンや設定情報の管理をすること。バージョンアップについては回数の上限は設定しない (無制限)。

F パッチ、ホットフィックスの適用

- i ソフトウェア提供元からパッチやホットフィックス等が提供された場合は、予備機あるいは検証機で動作確認を行った上で、パッチやホットフィックスの適用を行うこと。

重要度の高い不具合・脆弱性に対するパッチやホットフィックス等が提供されるまでの間が 1 か月を超える見込みと判断される場合は、ワークアラウンド (一時的な回避・緩和策) といった応急対応を行うこと。

- ii メールサーバ、プロキシサーバ経由での悪意あるソフトウェアの侵入を防止するためソフトウェアのパッチ適用、対策ソフトウェアのパターン更新、利用者への情報公開等を行うこと。

G サーバ証明書の更新

サーバ証明書の有効期限を確認し、継続して利用ができるように、CSR の生成、当機構担当者へのサーバ証明書更新の依頼、証明書の受け取り、証明書のインストールを行う。

証明書の更新に際しては暗号化強度・暗号化方式の見直しを行うこと。

H ウィルス定義ファイルの確認、更新作業

対象機器のウィルス定義パターンファイルが最新であることを確認する最新版でない場合は更新をすること。回数の上限は設定しない (無制限)。

セキュリティの観点から(原則)リリースされたらただちにアップデートを行うこと。
利用者への情報公開、周知等を行うこと。

I 各種 CGI の維持管理

現在使用している各種サーバの CGI 及び当機構内のアンケート CGI の維持、運用を行うこと。利用者からの要望等に応じ設定作業の支援を行う事。必要に応じてプログラミングを行うこと。なお、作業期間中に CGI が増えることもある。

J サーバのバックアップ

- i データのバックアップ計画を策定し、当機構担当者の承認を受けたのちに実行すること。なお、ユーザデータについては 1 日 1 回以上、システム及びシステム設定データについては更新の都度、他のディスクにコピーすること。また、当機構担当者が指定する一部サーバについては月に 1 回以上はテープへのバックアップを実施すること。
- ii バックアップは 4 世代以上管理すること。バックアップが計画どおりに行われていない場合は、速やかに原因を分析し、解決すること。

K サーバのリストア

- i ディスクあるいはディスクアレイが故障し、復旧できない場合は、最新のバックアップ用ディスクアレイあるいはバックアップデータを基にリストアを行うこと。データ量次第ではあるが、原則即日復旧できるように努めること。
- ii ユーザからファイルリストアの要求があった場合は、リストアを行うこと。データ量次第ではあるが、原則即日対応できるように努めること。

L Windows、Mac 等最新クライアント OS の維持管理作業

- i 情報システムグループで提供している各サービスの対応調査、問い合わせ。
- ii 検証環境(最新版クライアント OS) 準備。
- iii 最新版クライアント OS の検証、動作確認。
- iv 利用者向けの案内 Web ページの作成、FAQ 作成、更新。

M 停電等の対応

- i 計画停電等の前に、停電復旧時にサーバを自動起動する設定を確認、設定されていない場合は設定をすること。停電時にサーバを自動シャットダウンする設定を行うこと。
- ii オムロン製、APC 製、山洋電気製等個別無停電電源装置(UPS) の設定を行うこと。UPS に対応していない機器については、対応可能な範囲で安全にシャットダウンできる機構を内製すること。又はリモートでの電源投入に係る手順を作成すること。その際、システムが正常に機能するために一定の順序で起動しなければならない機器については、起動シーケンスを制御すること。

N サーバシステム設計書の維持管理

- i 各サーバの設計書を維持すること。
- ii サーバの構成に変更があった場合は、遅滞無く書類を修正して提出すること。
- iii 設計書をもとにサーバを再構築できるレベル及び内容で設計書を作成すること。

- iv 想定読者は、サーバの基礎的知識はあるが、SE 経験は無い者が対象。
- O サーバシステム構成図の維持管理
 - 基幹スイッチ、ルータから各サーバ、ストレージ、アプライアンスまでの接続図を維持すること。ネットワークの構成に変更があった場合は、遅滞無く書類を修正して情報システムグループに提出すること。
- P プログラム設計書の維持管理
 - i 契約前から存在していた既存プログラムも含めて、システム運用に必要なプログラムの設計書を維持すること。
 - ii 作業期間中に新たにプログラムを作成した場合、あるいはプログラムを修正した場合は、遅滞なく書類を作成・修正して提出すること。
- Q サーバ機器管理表の維持管理
 - 各サーバ、ストレージ、アプライアンスの機種、機器名、シリアル番号、購入時期、保守等の情報が管理されているサーバ機器管理表を維持すること。システム構成に変更があった場合や機器交換があった場合等、遅滞無く書類を修正して提出すること。
- R システム障害時対応手順書の維持管理
 - i 発生が予想される障害に対し、具体的にどのような手順でシステムを復旧するかを記した障害時対応書を維持すること。
 - ii 予想される障害に変化があった場合、あるいは、手順の見直しを行った場合は、遅滞なく書類を修正して提出すること。
- S 日常業務解説書の維持管理
 - i 本契約に基づいて実施する日々の日常業務内容を第三者でも分かるように記した日常業務解説書を維持すること。
 - ii 日常業務内容に変化があった場合、遅滞なく書類を修正して提出すること。
- T 利用マニュアルの維持管理
 - i 一般利用者を対象とした、各サーバの利用方法に関するマニュアルを維持し、当機構内イントラ Web サーバを用いて公開すること。
 - ii 利用方法に変更があった場合は遅滞なくマニュアルを修正すること。
- U FAQ のメンテナンス
 - i 利用者あるいは当機構担当者から問い合わせがあった場合は、問い合わせ内容を調査し、必要な支援を行うとともに、問い合わせ内容とその回答を、「よくある質問とその答え (FAQ)」として Web サーバに登録し、Web ブラウザで閲覧可能とすること。
 - ii 契約前に存在していた FAQ を含めて、登録済内容のメンテナンスを行うこと。
 - iii 問い合わせ内容については履歴管理を行うこと。
- V 予備機による運用
 - i サーバで障害が発生し、復旧が困難な場合は速やかに予備機を構築し運用を再開すること。障害についての原因調査及び障害箇所の特定制を行い当機構担当者へ報告すること。

- ii 障害の内容がハードウェアに起因する場合は、該当サーバの契約内容を確認し、保守対象品の場合は保守業者に連絡し、修理を依頼すること。
- iii 障害の内容がソフトウェアに起因する場合は、当機構担当者との協議の上、ソフトウェアの設定ファイルの書き換え、バージョンアップ、パッチ適用などの対処を行うこと。

(エ) 各サービスの維持管理業務

No	対象サービス	主な業務内容
1	<u>DNS</u>	<ul style="list-style-type: none"> ・適正かつ安全に DNS を運用管理すること。 ・権威 DNS サーバについてはリスク分散とセキュリティを重視した運用を行うこと。 ・ユーザアカウント連携システム（職員 DB）等の各サーバとのデータ連携について、維持管理すること。 ・ドメイン移行、DNS サーバの巻き取り等の検討、対応を行うこと。 ・アカウント、登録ホスト及び各レコード、ゾーン等の不要データの棚卸を行うこと（随時）。 ・負荷分散装置のヘルスチェック間隔、フェイルオーバーまでの時間を運用上最適な値に設定すること。ヘルスチェックにより装置あるいはそれに接続されたサーバから発生するログについては、その重要度を判断し、選択してログファイルに保存すること。
2	<u>Proxy</u>	<ul style="list-style-type: none"> ・適正かつ安全に Proxy を運用管理すること。 ・アクセス制御リストの棚卸を行うこと（随時）。 ・Proxy 自動構成ファイルの維持管理をすること。 ・負荷分散装置のヘルスチェック間隔、フェイルオーバーまでの時間を運用上最適な値に設定すること。ヘルスチェックにより装置あるいはそれに接続されたサーバから発生するログについては、その重要度を判断し、選択してログファイルに保存すること。 ・アカウントや不要データの棚卸を行うこと（随時）。
3	<u>DHCP</u>	<ul style="list-style-type: none"> ・適正かつ安全に DHCP を運用管理すること。 ・アカウントや登録ホスト等の不要データの棚卸を行うこと（随時）。 ・DHCP レンジの枯渇状況を監視し、必要に応じ

		<ul style="list-style-type: none"> ・レンジ拡張を行うこと。 ・特定の MAC アドレスに対して特定の IP アドレスを固定して払い出す設定を行うこと。
4	<u>NTP</u>	<ul style="list-style-type: none"> ・適正かつ安全に NTP を運用管理すること。
5	<u>LDAP</u>	<ul style="list-style-type: none"> ・適正かつ安全に LDAP を運用管理すること。 ・冗長性を維持しつつ運用管理を行うこと。 ・ユーザアカウント連携システム（職員 DB）等の各サーバとのデータ連携について、維持管理すること。 ・負荷分散装置のヘルスチェック間隔、フェイルオーバーまでの時間を運用上最適な値に設定すること。ヘルスチェックにより装置あるいはそれに接続されたサーバから発生するログについては、その重要度を判断し、選択してログファイルに保存すること。 ・システムに問題が生じた場合は保守業者と連携し、早急な対応を実施することができること。 ・アカウント等の不要データの棚卸を行うこと（随時）。
6	<u>シングルサインオン</u>	<ul style="list-style-type: none"> ・適正かつ安全に SSO 認証を運用管理すること。 ・LDAP 等の各サーバとのデータ連携について、維持管理すること。 ・新たに SSO 対象システムが増えた場合や既 SSO 対象システムの構成が変更になった場合、必要に応じて SSO 認証システムの設定変更等を実施すること。 ・システム停止などに伴う不要データの棚卸を行うこと（随時）。 ・システムに問題が生じた場合は保守業者と連携し、早急な対応を実施することができること。 ・アカウント等の不要データの棚卸を行うこと（随時）。
7	<u>メール</u> <u>(中継、スプール)</u>	<ul style="list-style-type: none"> ・適正かつ安全にメール（中継、スプール）を運用管理すること。 ・LDAP 等の各サーバとのデータ連携について、維持管理すること。 ・メールサーバについては、冗長運用を維持し、2

		<p>台あるメールサーバのいずれかに障害が発生した場合であっても残りの1台でサービスを提供できるようにすること。</p> <ul style="list-style-type: none"> ・負荷分散装置のヘルスチェック間隔、フェイルオーバーまでの時間を運用上最適な値に設定すること。ヘルスチェックにより装置あるいはそれに接続されたサーバから発生するログについては、その重要度を判断し、選択してログファイルに保存すること。 ・アカウントやMXレコード、エイリアス等の不要データの棚卸を行うこと（随時）。
8	<p><u>スパム</u> <u>(迷惑) メールフィルタ</u></p>	<ul style="list-style-type: none"> ・適正かつ安全にスパム（迷惑）メールフィルタを運用管理すること。 ・LDAP等の各サーバとのデータ連携について、維持管理すること。 ・共用メールサーバで受信したメールを、メールの送信者、メールサイズ、添付ファイルの有無等の条件により、指定した宛先に転送するための機能を維持管理すること。 ・フィルタ条件や転送先はWebインタフェースを用いて指定できること。 ・アカウント、ホワイトリスト登録アドレス等の不要データの棚卸を行うこと（随時）。
9	<p><u>メーリングリスト</u></p>	<ul style="list-style-type: none"> ・適正かつ安全にメーリングリストを運用管理すること。 ・ユーザアカウント連携システム（職員DB）等の各サーバとのデータ連携について、維持管理すること。 ・メーリングリスト管理者の一覧を作成し、いつでもメーリングリスト管理者全員に、同一内容のメールを個別に送信できるように準備すること。 ・メーリングリストが追加された場合や、メーリングリストの管理者に変更があった場合はその都度修正すること。 ・アカウントやメーリングリスト等の不要データの棚卸を行うこと（随時）。
10	<p><u>ウイルスチェック</u></p>	<ul style="list-style-type: none"> ・適正かつ安全にウイルスチェックを運用管理す

		<p>ること。</p> <ul style="list-style-type: none"> 対象機器のウイルス定義パターンファイルが最新であることを確認する。最新版でない場合は更新をすること。回数の上限は設定しない（無制限）。 セキュリティの観点から（原則）リリースされたらただちにアップデートを行うこと。利用者への情報公開、周知等を行うこと。 アカウントや監視対象機器等の不要データの棚卸を行うこと（随時）。
11	<u>外部公開用 WEB</u>	<ul style="list-style-type: none"> 適正かつ安全に外部公開用 WEB を運用管理すること。 Web コンテンツへのアクセスログをもとに、アクセス統計一覧（接続元を、接続数の上位順に並べたリストや、参照されたページを上位順に並べたリスト等）を作成すること。 統計一覧作成には、Webalizer を使用すること。 アカウントやコンテンツ等の不要データの棚卸を行うこと（随時）。
12	<u>Web コンテンツ管理</u>	<ul style="list-style-type: none"> 適正かつ安全に Web コンテンツ管理を運用管理すること。 LDAP 等の各サーバとのデータ連携について、維持管理すること。 外部公開用 WEB とデータ連携について、維持管理すること。 共通 CGI 更新時の再配置等を行うこと。 アカウントやコンテンツ等の不要データの棚卸を行うこと（随時）。
13	<u>Web ホスティング</u>	<ul style="list-style-type: none"> 適正かつ安全に Web ホスティングを運用管理すること。 新たに対象ホストが増えた場合、利用者への要件ヒアリングを行い必要なシステムの設定変更等を実施すること。また、導入支援を実施すること。 Web コンテンツへのアクセスログをもとに、アクセス統計一覧（接続元を、接続数の上位順に並べたリストや、参照されたページを上位順に並べたリスト等）を作成すること。

		<ul style="list-style-type: none"> ・アクセス統計一覧は当機構担当者のみがいつでも閲覧できるようにすること。 ・アカウント等の不要データの棚卸を行うこと（随時）。
14	<u>当機構内向け Web</u>	<ul style="list-style-type: none"> ・適正かつ安全に当機構内向け当機構内向け Web を運用管理すること。 ・LDAP 等の各サーバとのデータ連携について、維持管理すること。 ・Web コンテンツへのアクセスログをもとに、アクセス統計一覧（接続元を、接続数の上位順に並べたリストや、参照されたページを上位順に並べたリスト等）を作成すること。 ・アクセス統計一覧は当機構担当者のみがいつでも閲覧できるようにすること。 ・アカウント等の不要データの棚卸を行うこと（随時）。 ・当機構担当者が Web コンテンツをアップロードするための、アップロードディレクトリの設定作業を行うこと。
15	<u>内部 Web 検索</u>	<ul style="list-style-type: none"> ・適正かつ安全に Web ホスティングを運用管理すること。 ・アカウントや検索除外キーワード等の不要データの棚卸を行うこと（随時）。
16	<u>Webmail</u>	<ul style="list-style-type: none"> ・適正かつ安全に Webmail を運用管理すること。 ・LDAP 等の各サーバとのデータ連携について、維持管理すること。 ・アカウント等の不要データの棚卸を行うこと（随時）。
17	<u>SSH</u>	<ul style="list-style-type: none"> ・適正かつ安全に SSH を運用管理すること。 ・LDAP 等の各サーバとのデータ連携について、維持管理すること。 ・アカウントや不要データの棚卸を行うこと（随時）。
18	<u>リモートアクセス</u>	<ul style="list-style-type: none"> ・適正かつ安全にリモートアクセスを運用管理すること。 ・認証システム等との各サーバとのデータ連携について、維持管理すること。 ・連携サービス追加、更改時等に Web ポータルへ

		<p>のメニューの追加を行うこと。</p> <ul style="list-style-type: none"> ・アカウント等の不要データの棚卸を行うこと（随時）。
19	<u>リモートデスクトップ</u>	<ul style="list-style-type: none"> ・適正かつ安全にリモートデスクトップを運用管理すること。 ・リモートアクセスシステム等との各サーバとのデータ連携について、維持管理すること。 ・アカウント等の不要データの棚卸を行うこと（随時）。
20	<u>ファイル転送・外部ファイル共有</u>	<ul style="list-style-type: none"> ・適正かつ安全にファイル転送を運用管理すること。 ・LDAP 等の各サーバとのデータ連携について、維持管理すること。 ・アカウント等の不要データの棚卸を行うこと（随時）。 ・LDAP と連携せず個別にアカウント管理を行うサブシステムについて維持管理すること。
21	<u>ActiveDirectory</u>	<ul style="list-style-type: none"> ・適正かつ安全に ActiveDirectory を運用管理すること。Azure AD Connect を介した Azure AD を含む。 ・LDAP 等の各サーバとのデータ連携について、維持管理すること。 ・アカウント、登録ホスト及び各レコード、ゾーン等の不要データの棚卸を行うこと（随時）。 ・セキュリティグループ、グループポリシー、ログオンスクリプト等の維持管理を行う事。 ・アカウント等の不要データの棚卸を行うこと（随時）。
22	<u>端末管理</u>	<ul style="list-style-type: none"> ・適正かつ安全に端末管理システムを運用管理すること。Azure AD Connect を介した Azure AD を含む。 ・Microsoft Windows 10 Pro の共通部門計算機の管理を対象とすること。 ・ActiveDirectory 等の各サーバとのデータ連携について、維持管理すること。 ・SCCM（Microsoft System Center Configuration Manager）等により、パッチ、ホットフィックス等をクライアント計算機に配布

		<p>すること。</p> <ul style="list-style-type: none"> ・ 共通部門計算機にインストールされているソフトウェアの情報を定期的に収集し、問題点が見つかった場合は、当機構担当者に報告するとともに、対応策を講じた雛形アプリの再構築を行うこと。 ・ 雛形アプリの再構築を行った場合は、インストールイメージの再作成を行うこと。 ・ <u>共通部門計算機の機種は最大で 5 機種とし、各機種毎に必要なドライバ、ソフトウェア、設定等を適切に管理運用すること</u> ・ 共通部門計算機上で発生したソフトウェア、ハードウェアの障害について調査、対処を行うとともに、それらの障害履歴を管理すること。 ・ アカウント、端末情報等の不要データの棚卸を行うこと（随時）。
23	<u>ファイル共有</u>	<ul style="list-style-type: none"> ・ 適正かつ安全にファイル共有を運用管理すること。 ・ ActiveDirectory 等の各サーバとのデータ連携について、維持管理すること。 ・ アカウント等の不要データの棚卸を行うこと（随時）。
24	<u>不正端末排除</u>	<ul style="list-style-type: none"> ・ 適正かつ安全に不正端末排除を運用管理すること。 ・ ActiveDirectory 等の各サーバとのデータ連携について、維持管理すること。 ・ アカウント、端末情報等の不要データの棚卸を行うこと（随時）。
25	<u>監視</u>	<ul style="list-style-type: none"> ・ 適正かつ安全に監視システムを運用管理すること。 ・ 故障などによる交換、老朽化などによる更改、新サービス導入等により、新規に追加されたネットワーク、サーバの監視、リソース情報の登録及び適宜設定値のフィルタリングの追加等を行うこと。 ・ アカウント、端末情報等の不要データの棚卸を行うこと（随時）。

26	<u>運用管理</u>	<ul style="list-style-type: none"> ・適正かつ安全に運用管理システムを運用管理すること。 ・故障などによる交換、老朽化などによる更改、新サービス導入等により、新規に追加されたネットワーク、サーバの設定方法等の情報を追加すること。 ・アカウント等の不要データの棚卸を行うこと（随時）。
27	<u>データバックアップ</u>	<ul style="list-style-type: none"> ・適正かつ安全にデータバックアップを運用管理すること。 ・故障などによる交換、老朽化などによる更改、新サービス導入等により、新規に追加されたシステムのバックアップを追加すること。 ・データ保管期間等の見直しによりバックアップポリシーの設定変更等を行うこと。 ・アカウント等の不要データの棚卸を行うこと（随時）。
28	<u>職員情報 DB&オンライン申請</u>	<ul style="list-style-type: none"> ・適正かつ安全に職員情報 DB&オンライン申請(e申請)を運用管理すること。 ・LDAP 等の各サーバとのデータ連携について、維持管理すること。 ・業務効率化等におけるオンライン申請構築時あるいはシステム改修時の支援業務を実施すること。 ・業務効率化等におけるシステム改修時の外部連携における CGI 等によるプログラミングを実施し、支援システムなどのツール群の維持管理すること。 ・アカウント等の不要データの棚卸を行うこと（随時）。
29	<u>共用無線 LAN</u>	<ul style="list-style-type: none"> ・適正かつ安全に共用無線 LAN を運用管理すること。 ・LDAP 等の各サーバとのデータ連携について、維持管理すること。 ・共用無線 LAN のエリア拡大によるアクセスポイントの設定追加等の対応をすること。 ・アカウント等の不要データの棚卸を行うこと（随時）。

30	<u>経路検索</u>	<ul style="list-style-type: none"> ・適正かつ安全に経路検索サービスを運用管理すること。
31	<u>外部 Web コンテンツ高速配信</u>	<ul style="list-style-type: none"> ・適正かつ安全に外部 Web コンテンツ高速配信を運用管理すること。 ・外部公開用 WEB とのデータ連携について、維持管理すること。 ・アクセスログ、レポートは、その重要度を判断し、選択してログファイルに保存すること。 ・当機構担当者または広報部から要請があった場合、Web コンテンツのキャッシュクリア作業を行うこと（随時）。 ・アノマリ検知、DDoS 検知された場合は、当機構担当者に報告を行うこと。 ・アカウント等の不要データの棚卸を行うこと（随時）。
32	<u>ファイル共有（研究系）</u>	<ul style="list-style-type: none"> ・適正かつ安全にファイル共有を運用すること。 ・ActiveDirectory 等の各サーバとのデータ連携について、維持管理すること。 ・特例アクセス権の設定や、アカウント等の不要データの棚卸を行うこと（随時）。

(オ) 共通部門計算機の OS (Microsoft Windows 10 Pro)の大型アップデート対応作業

OS サポートポリシーに基づき、共通部門計算機の OS(Microsoft Windows 10 Pro)の大型アップデート対応作業を1年間あたり、1回以上実施すること。

A 端末管理システム

- i 端末管理システムを大型アップデートに対応させるための検討及び設計、設定、動作確認をすること。
- ii 大型アップデートのインストール用イメージの検討及び作成、動作確認をすること。

B 共通部門計算機

- i 大型アップデートの展開に向けて事前に機構内業務システムへの対応状況を確認すること。
- ii 現行の共通部門計算機の設計、運用ポリシーに準拠した大型アップデートの OS 設計をすること。
- iii 大型アップデートの雛型となる、検証用共通部門計算機を1台作成すること。
- iv 大型アップデートに対応した共通部門計算機にインストールした雛形アプリの検討および設計、設定、動作確認をすること。
- v 機構内に展開している共通部門計算機に端末管理システムから大型アップデ

ートの配信、適用を実施すること。なお、端末管理システムからの配信、適用が行えない場合は当機構担当者と別途協議を行うこと。

C ドキュメント整備

- i 大型アップデートに対応した共通部門計算機の運用手順作成を行うこと。
- ii 大型アップデートに対応した共通部門計算機の設定方法並びに障害対処方法などの保守マニュアルを HTML 形式文書で作成し、当機構担当者が指定する場所に登録すること。
- iii 大型アップデートに対応した共通部門計算機の利用マニュアルを HTML 形式文書で作成し、当機構担当者が指定する場所に登録すること。

(カ) 組織変更に伴う外部公開 Web コンテンツ移行支援

組織変更に伴い外部公開 Web コンテンツ移行が必要になった場合は以下の対応を行うこと。

- i 外部公開 WEB にある研究室等のコンテンツのデータ移行作業を支援すること。移行はディレクトリ単位で実施し研究室等と切替日程等を調整すること。移行元ディレクトリ及び移行先ディレクトリは広報部が指定する。移行対象ディレクトリの数は最大で 140 とする。これを超える場合当機構担当者と協議を行うこと。
- ii 当機構担当者及び広報部と協議の上、Web コンテンツの移行計画、移行作業項目、移行元・先ディレクトリ毎の移行担当者連絡先一覧に係る資料を作成し、当機構担当者及び広報部から承認を得ること。
- iii Web コンテンツ移行の周知実施および対応履歴を管理すること。周知先は、内部 Web ページ、当機構内アナウンス、コンテンツアップロードアカウント保持者、コンテンツアップロードアカウント保持者の所属長、その他当機構担当者及び広報部が指示する連絡先等とする。
- iv 移行対象コンテンツが大量にある等の場合は、当機構担当者及び広報部と協議の上、Web コンテンツの移行作業を代行すること。
- v バーチャルホストの設定ディレクトリを移行する場合は、研究室等の移行担当者、バーチャルホストの保有者と調整をしたうえで再設定を行うこと。移行対象ディレクトリの数は最大で 140 とする。これを超える場合当機構担当者と協議を行うこと。
- vi 移行元ディレクトリの URL にアクセスがあった場合に、移行先ディレクトリの URL にリダイレクトする等の設定は、研究室等の要望をヒアリングし、まとめること。また、要望の実施可否を当機構担当者及び広報部と協議の上、作業を実施すること。
- vii 廃止となるバーチャルホストについては廃止を周知するページや転送ページへの切替を行うこと。

(キ) 他拠点の支援業務

他拠点の障害対応、セキュリティインシデント、ユーザ対応、構築作業等の支援を行う

こと。当機構担当者と協議の上、他拠点に出張し、支援が行えるようにすること。

(4) 本部サポートデスク運用サービス

ア 概要

情報システムグループが提供するサービス利用受付から運用管理、利用者への運用支援及びトラブル対応、検証、各種申請対応、Web 掲載、イベント支援等を実施する。

共通事務パソコンの利用支援、当機構業務を迫行するのに必要なサポートサービスの提供、利用支援等を実施する。当機構内イントラ Web サーバの更新管理を行い、各部署からの掲載依頼に対応すること。

サービス品質向上、利用者の利便性向上、運用効率化をめざし、システム改修の要望等のコンサルテーションを実施する。

イ 業務内容

(ア) 当機構内イントラ Web コンテンツの更新管理

- i 当機構イントラ Web 内の機構共通コンテンツに対し、総務部、財務部等の各部署からの依頼に基づき、Web ページの修正（文章、リンク修正、画像、ファイル差替え）を実施すること。
- ii 情報システムの利用者支援のため、当機構イントラ Web 内の情報システムグループ部署ポータルサイトに対し、Web デザイン修正、画像製作・加工および Web ページの作成、更新を実施すること。ただし、ポータルサイト全体の大規模デザイン改修が必要な場合は別途当機構担当者と協議の上、実施すること。

(イ) FAQ のメンテナンス

- i サーバ利用者あるいは当機構担当者から問い合わせがあった場合は、問い合わせ内容を調査し、必要な支援を行うとともに、問い合わせ内容とその回答を、「よくある質問とその答え（FAQ）」として Web サーバに登録し、Web ブラウザで閲覧可能とすること。
- ii 契約前に存在していた FAQ を含めて、登録済内容のメンテナンスを行うこと。
- iii 問い合わせ内容については履歴管理を行うこと。

(ウ) 質問・障害受付

- i 利用者からの質問・障害に対する一次受付を行い、受け付けを行った質問・障害は、受け付けから解決までの対応状況を管理すること。管理する情報は、受付日、質問者名、質問者連絡先（電話番号、メールアドレス等）、質問内容、回答日、回答者、回答内容等であり、当機構担当者が状況を確認できるように管理すること。
- ii 既存の FAQ 又は利用手引書に質問・障害に対する解決方法が用意されている場合は、その内容に従って利用者に回答すること。FAQ 又は利用手引書で対応できない質問・障害は、当機構常駐の各担当 SE に調査及び対応依頼を行うこと。質問に対する回答は、利用者向けに公開するため、必要に応じて FAQ、利用手引書として Web サイト上から閲覧可能なドキュメントを作成すること。

- iii 共通事務パソコンでウィルスを検知した場合は、セキュリティ担当と協力し、切り分けを行い、利用者に連絡して駆除依頼、利用者の対応の支援をすること。
- iv 利用者からの廃棄ハードディスク等を引き取り、施錠された指定の場所に一時保管すること。
- v 利用者から依頼があった場合は、USB メモリ、DVD 等の記憶メディア等をウィルスチェック用の計算機を用いてチェックすること。
- vi 情報システムグループで管理している端末（計算機、iPad 等）については、管理し必要なアップデートを行うこと。
- vii マニュアルに沿って yarai を配布すること。

(エ) 申請登録業務

当機構内計算機及びサービスを利用するために必要な申請書の登録申請処理を行うこと。受付時間として平日 16:00 までに提出された申請書に対し、即日登録を原則とする。

A 登録申請書の種類

登録申請書の種類は次のとおりとし、職員情報 DB&オンライン申請システム（以下、「e 申請システム」という。）のオンライン申請に搭載されている申請、それ以外の情報システムグループの申請について、対応すること。なお、申請書は当機構内サービスの運用変更に伴い追加される場合がある。追加された申請書に対する登録処理は、当機構担当者と協議の上、対応を行うこと。

- (a) 『SSH サーバアカウント申請書』（NICT-ID 保持者、非保持者用）
- (b) 『リモートアクセス利用申請書』
- (c) 『外部ネットワーク接続申請書』
- (d) 『IP アドレス取得申請書』
- (e) 『共通部門計算機利用申請書』『共通部門計算機返却申請書』
- (f) 『共用無線 LAN 利用申請書』
- (g) 『メーリングリスト利用申請書』
- (h) 『外部公開 CGI 登録許可申請書』
- (i) 『外部公開コンテンツアップロード許可申請書』
- (j) 『バーチャルホスト利用申請書』
- (k) 『支援系ネットワーク接続機器登録申請書』
- (l) 『機構所有 PC 外部持ち出し許可申請書』
- (m) 『機構非所有 PC 内部持ち込み許可申請書』
- (n) 『電子情報記録媒体外部持ち出し許可申請書』
- (o) 『共通部門事務サーバ・フォルダアクセス権付与申請書』
- (p) 『Office365 サービスアカウント申請』
- (q) 『リモートデスクトップ利用申請』
- (r) メールアドレス継続利用申請
- (s) 機構外宛メール転送申請

- (t) 大容量ファイル転送サービス利用申請
- (u) 職員 DB 登録申請
- (v) Adobe 利用申請

B 申請業務の棚卸し作業

- i e 申請システム導入以前にオフラインにて運用されている申請にて受理した申請情報の棚卸し（要、不要、申請内容の精査等）を行い、e 申請システムに登録すること。棚卸しは、年に1回以上実施し報告すること。
- ii 個別ソフトのライセンスの棚卸し（要、不要、申請内容の精査等）を行い報告すること

C 申請業務のドキュメントの作成

情報システムグループが提供するサービスの申請業務に関する運用ルールに関して、手順書（サポートデスクマニュアル）を必要に応じて作成すること。

D 申請業務の支援作業

e 申請システムへ新規導入する申請書のコンサル対応や実装に向けたリリース計画書、試験内容の確認、関係各所との調整、周知、関連する利用マニュアルの更新支援等を行う。また、e 申請システムへ新規導入する申請書に係る仕様調整会議への出席及び支援を行うこと。（仕様調整会議は開発業者、当機構担当者を含めた3者及び、新規に導入する申請書担当部署も含めて行なわれる。）

(オ) ユーザアカウント管理

- i サーバの利用者（アカウント）を、ディレクトリサービスシステムにより一元管理すること。一元管理するために必要なプログラミングは受注者が行うこと。
- ii Windows サーバに関しては、当機構担当者からの指示、もしくは管理上の必要性に合わせて、アカウント（ホームディレクトリ含む）の作成・削除を行うこと。アクティブディレクトリを導入した場合は、アクティブディレクトリのアカウント情報を更新すること。
- iii 共用メールサーバに残っている退職者のメールアカウントを削除すること。
- iv RFC 違反等の利用はしてはいけないメールアカウント、あるいは当機構担当者から依頼のあったメールアカウントについては、専用サーバ中の予約ファイルに利用できないようメールアカウントを追記すること。また、当機構担当者から依頼があった場合は予約ファイルから該当メールアカウントを削除すること。
- v e 申請システムにおけるフォルダアクセス権設定と連携した管理を行うため、e 申請システム導入以前にオフラインにて運用されている申請にて設定したセキュリティグループについて、1年に1回アクセス権限の棚卸（要、不要、申請内容の精査等）を行い、適正な設定を行うこと。

(カ) クライアント計算機の管理・運用作業

A 対象クライアント計算機

- i 対象となるクライアント計算機は、主に当機構の事務部門に配布する計算機（以下共通部門計算機と呼ぶ）、事務部門の非共通部門計算機そして研究部門

のクライアント計算機、在宅勤務用のクライアント計算機（以下在宅勤務計算機と呼ぶ）、そしてシンクライアント端末である。

- ii 共通部門計算機の基本ソフトウェアは Microsoft Windows 10 Pro である。
- iii 2020 年 4 月時点の共通部門計算機の台数は 700 台以下である。作業期間中に追加導入する場合は 150 台を超えないものとするが追加購入する共通部門計算機を一括で置換する作業は運用対象外とする。なお、機器交換等に伴い一時的に管理台数を増やす場合には別途協議の上で台数を増やすこととする。
- iv 在宅勤務計算機の台数は 50 台以下である。作業期間中に追加導入する場合は 50 台を超えないものとする。なお、機器交換等に伴い一時的に管理台数を増やす場合には別途協議の上で台数を増やすこととする。
- v シンクライアント端末の台数は 60 台以下である。作業期間中に追加導入する場合は 50 台を超えないものとする。なお、機器交換等に伴い一時的に管理台数を増やす場合には別途協議の上で台数を増やすこととする。
- vi 共通部門計算機以外の計算機の機種の基本ソフトウェアは、Microsoft Windows 又は Mac OS、iOS、Android とする。基本ソフトウェアのバージョンは、Microsoft Windows 7、Windows 8.1、Windows 10、macOS 10.12、iOS 12、Android6.0 あるいはそれ以降のバージョンとする。

B 共通部門計算機の管理

(a) 機器管理

- i 共通部門計算機の配布先、在庫台数を管理すること。
- ii 利用者の情報（所属、名前、職員 ID、メールアドレス、電話番号など）と共通部門計算機の管理番号及び運用状況をシステム管理ソフトウェアにより管理すること。
- iii 管理のために、共通部門計算機にソフトウェアのインストールが必要な場合は、リモートあるいはオンサイトで必要なソフトウェアをインストールすること。
- iv 利用者の共通部門計算機に障害が発生し、交換以外に復旧手段が無いと判断された場合は速やかに予備機と交換すること。
- v 端末性能を評価し、劣化状況を確認した場合は、是正措置の提案及び対処すること。
- vi 共通部門計算機上で発生したソフトウェア、ハードウェアの障害について調査、対処を行うとともに、それらの履歴を管理すること。

(b) ソフトウェアの情報収集及びインストールイメージの作成

- i 共通部門計算機にインストールされているソフトウェアの情報を定期的に収集し、問題点が見つかった場合は、当機構担当者に報告するとともに、対応策を講じた雛形アプリの再構築を行うこと。
- ii 雛形アプリの再構築を行った場合は、インストールイメージの再作成を行うこと。

- iii 共通部門計算機にインストールしたソフトウェア群は、当機構担当者が指定する場所に保管し、システムの再構築の際に利用可能な状態とすること。
- (c) 共通部門計算機の修復
共通部門計算機がハードウェア障害のため交換した場合は、当機構担当者の指示に従い復旧のための措置を行なうこと。また、復旧後の共通部門計算機は、システムの再構築を行なうとともに、雛形アプリのセットアップを行い、予備機として利用できる状態にしておくこと。
- (d) 利用者への周知
各サーバの停止、運用方法の変更、計算機の構成変更など共通部門計算機利用者に影響のあると思われる内容については、当機構担当者と協議し当機構内イントラ Web サーバを用いて利用者への周知を行うこと。
- (e) アップデート情報および脆弱性情報の収集
OS、雛形アプリのサービスパック、ホットフィックス、セキュリティパッチ等のアップデート情報および脆弱性情報を収集すること。
- (f) パッチ等の適用
 - i OS および雛形アプリにサービスパック、ホットフィックス、セキュリティパッチ等が公開された際には、当該パッチ等の内容を確認し、適用の可否を判断し、システム管理ソフトを用いて配信検証および動作確認を行うこと。
 - ii 検証が正常に完了した後、共通部門計算機への配信を行うこと。また、その配信の結果を確認し、正常に完了しないことを確認した場合は、当機構担当者へ報告の上、対策を検討、実施すること。なお、配信対象となる OS および雛形アプリの合計は 18 以下であるが、一時的に 20 以上に増加する場合には別途協議の上で実施することとする。
- (g) 個別ソフトウェア及びドライバ等のインストール
共通部門計算機に対する、ソフトウェアのインストール、プリンタへの接続などの要望に対しては、当機構担当者の協議の上、インストール及びセットアップ作業を行うこと。
- (h) 共通部門計算機の追加導入に伴う作業
 - i 作業期間中に追加した共通部門計算機について、既存共通部門計算機同等のソフトウェアをインストールし、雛型となる共通部門計算機を作成すること。
 - ii 雛形共通部門計算機を作成した場合は、同一機種への他の共通部門計算機へのソフトウェアインストール用のインストールイメージを作成すること。
 - iii 共通部門計算機の機種は最大で 6 機種とする。これを超える場合当機構担当者と協議を行うこと。
- (i) 利用者からの質問に対する調査・回答
 - i 利用者からの質問に対する調査・回答を行うこと。
 - ii 質問及び回答についての履歴管理を行うとともに、よくある質問とその答（FAQ）集を作成すること。

iii FAQ 集は HTML 形式文書で作成し、当機構担当者が指定する場所に登録すること。

(j) 保守マニュアルの維持

i 共通部門計算機の設定方法並びに障害対処方法などの保守マニュアルを随時更新し、維持すること。

ii 保守マニュアルは HTML 形式文書で作成し、当機構担当者が指定する場所に登録すること。

(k) 利用マニュアルの維持

i 共通部門計算機の利用マニュアル（電源の投入方法、キーボード、マウスの使用方法など）を HTML 形式文書で更新し、又は作成することで維持すること。当機構担当者が指定する場所に登録すること。

ii 共通部門計算機利用者に分かりやすいように、共通部門計算機にインストールしたソフトウェア群の利用マニュアルを HTML 形式文書で更新し、当機構担当者が指定する場所に登録すること。また、必要に応じて作成すること。共通部門計算機利用者は必ずしもパーソナルコンピュータの利用に精通していない。この点を考慮し、共通部門計算機の利用マニュアル及びソフトウェア群の利用マニュアルはパーソナルコンピュータの初心者でも分かるように作成すること。

C 在宅勤務計算機の管理

i 在宅勤務計算機の配布先、在庫台数を管理すること。

ii 利用者の在宅勤務計算機に障害が発生し、交換以外に復旧手段が無いと判断された場合は速やかに予備機と交換すること。

iii 電話やメールによるインストールやセットアップの技術支援を行うこと。また、必要に応じて当機構担当者と協議の上、実際の作業を行うこと。

iv 在宅勤務計算機の配布時は最新のサービスパック、ホットフィックス、セキュリティパッチ等を適用すること。

v 年に1回在宅勤務計算機の利用状況の棚卸を実施すること。

D シンククライアント端末の管理

(※シンククライアント端末については調達中、2020年2月に導入予定のため、以下の作業内容が変更になる場合がある。必要に応じて当機構担当者と協議を行うこと。)

i シンククライアント端末の配布先、在庫台数を管理すること。

ii 利用者のシンククライアント端末に障害が発生し、交換以外に復旧手段が無いと判断された場合は速やかに予備機と交換すること。

iii 電話やメールによる技術支援を行うこと。また、必要に応じて当機構担当者と協議の上、実際の作業を行うこと。

iv シンククライアント端末について影響度の高いセキュリティパッチがリリースされた場合、利用者に更新方法を周知・案内すること。また、更新に関わ

る技術支援を行うこと。更新/パッチ適用済端末との交換でも可とする。

v 年に1回シンクライアント端末の利用状況の棚卸を実施すること。

E 共通部門計算機、在宅勤務計算機以外のクライアント計算機に対する支援

i 共通部門計算機、在宅勤務計算機以外の計算機においても、電話やメールによるインストールやセットアップの技術支援を行うこと。また、必要に応じて当機構担当者と協議の上、実際の作業を行うこと。

ii 上記作業内容については、情報を管理し、問い合わせの多い内容については、FAQを作成すること。

iii 役員及び総務部長、財務部長、経営企画部長、広報部長の計算機に関するソフトウェアのインストール、プリンタへの接続、操作方法の案内などの要望に対して、当機構担当者に報告の上、オンサイト技術支援を行うこと。なお、対象の計算機については、機構所有、機構非所有は問わないこととする。

(キ) 資産棚卸対応

当機構の指示に基づき、年に2回資産の現況調査、各資産のシール、機材の存在確認、報告等を行うこと。資産数は2000程度を目安とする。

(ク) 組織改正に伴うDB情報の更新対応

年2-3回程度の組織改正に伴う職員DB情報の更新対応、関係各所との調整を行うこと。

(ケ) サーバ室の入室の受付、鍵の払い出し対応

利用者及び業者からのサーバ室入室依頼の受付を行い、サーバ室へのアテンド、鍵の貸し出しを行う。

(コ) Office365 サービスの維持管理作業

Office365 サービスに関する以下の対応を行う。

i 利用者からの質問・障害に対する一次受付を行い、受け付けを行った質問・障害は、受け付けから解決までの対応状況を管理すること。

ii 管理する情報は、受付日、質問者名、質問者連絡先（電話番号、メールアドレス等）、質問内容、回答日、回答者、回答内容等であり、当機構担当者が状況を確認できるように管理すること。

iii 既存のFAQ又は利用手引書に質問・障害に対する解決方法が用意されている場合は、その内容に従って利用者に回答すること。

iv FAQ又は利用手引書で対応できない質問・障害は、Microsoftのサポートに調査及び対応依頼を行うこと。

v 質問に対する回答は、利用者向けに公開するため、必要に応じてFAQ、利用手引書としてWebサイト上から閲覧可能なドキュメントを作成すること。

vi アカウントの登録、変更、削除を行うこと。

vii 1年に1回アカウントの棚卸し（要、不要の精査等）を行い、適正な設定を行うこと。

(サ) リモートデスクトップサービスの維持管理作業

リモートデスクトップサービスに関する以下の対応を行う。

- i 利用者からの質問・障害に対する一次受付を行い、受け付けを行った質問・障害は、受け付けから解決までの対応状況を管理すること。
- ii 管理する情報は、受付日、質問者名、質問者連絡先（電話番号、メールアドレス等）、質問内容、回答日、回答者、回答内容等であり、当機構担当者が状況を確認できるように管理すること。
- iii 既存の FAQ 又は利用手引書に質問・障害に対する解決方法が用意されている場合は、その内容に従って利用者に回答すること。
- iv FAQ 又は利用手引書で対応できない質問・障害は、当機構常駐の各担当 SE に調査及び対応依頼を行うこと。
- v 質問に対する回答は、利用者向けに公開するため、必要に応じて FAQ、利用手引書として Web サイト上から閲覧可能なドキュメントを作成すること。
- vi アカウントの登録、変更、削除を行うこと。
- vii 1年に1回アカウントの棚卸し（要、不要の精査等）を行い、適正な設定を行うこと。

(シ) 振る舞い検知ソフトウェアの維持管理作業

共通部門計算機に導入されている振る舞い検知ソフトウェアに関する以下の対応を行う。

- i 利用者からの質問に対する一次受付を行い、受け付けを行った質問は、受け付けから解決までの対応状況を管理すること。
- ii 管理する情報は、受付日、質問者名、質問者連絡先（電話番号、メールアドレス等）、質問内容、回答日、回答者、回答内容等であり、当機構担当者が状況を確認できるように管理すること。既存の FAQ 又は利用手引書に質問に対する解決方法が用意されている場合は、その内容に従って利用者に回答すること。
- iii FAQ 又は利用手引書で対応できない質問は、当機構常駐の各担当 SE 及び当機構担当者経由で保守ベンダに調査及び対応依頼を行うこと。
- iv 質問に対する回答は、利用者向けに公開するため、必要に応じて FAQ、利用手引書として Web サイト上から閲覧可能なドキュメントを作成すること。
- v 利用者からの質問に対する一次受付を行い、受け付けを行った質問は、受け付けから解決までの対応状況を管理すること。
- vi 共通部門計算機の新規払い出し時に振る舞い検知エージェントのインストールを行うこと。
- vii 共通部門計算機の振る舞い検知エージェントのバージョンアップを年 2 回程度行うこと。

(ス) Adobe サービスの維持管理作業

Adobe サービスに関する以下の対応を行う。

- i 対象となる製品は下記に示す Adobe Creative Cloud サービスおよびそれに属するソフトウェア群とクラウドサービスである。ただし以下のリストは2020年9月現在のものとなり、Adobe Creative Cloud 製品に変更があった場合はこれに対応すること。
 - ・ CreativeCloud デスクトップ
 - ・ Acrobat DC
 - ・ Adobe XD CC
 - ・ AfterEffects CC
 - ・ Animate CC
 - ・ Audition CC
 - ・ Bridge CC
 - ・ Capture CC
 - ・ CharacterAnimator CC
 - ・ Comp CC
 - ・ Dimension CC
 - ・ Dreamweaver CC
 - ・ Fuse CC
 - ・ Illustrator CC
 - ・ InCopy CC
 - ・ InDesign CC
 - ・ Lightroom CC
 - ・ LightroomClassic CC
 - ・ MediaEncoder CC
 - ・ Photoshop CC
 - ・ Photoshop Fix
 - ・ Photoshop Mix
 - ・ Photoshop Sketch
 - ・ Prelude CC
 - ・ Premiere Pro CC
 - ・ Premiere Rush CC
- ii 利用者からの質問・障害に対する一次受付を行い、受付を行った質問・障害は、受付から解決までの対応状況を管理すること。
- iii 管理する情報は、受付日、質問者名、質問者連絡先（電話番号、メールアドレス等）、質問内容、回答日、回答者、回答内容等であり、当機構担当者が状況を確認できるように管理すること。

- iv 既存の FAQ 又は利用手引書に質問・障害に対する解決方法が用意されている場合は、その内容に従って利用者に回答すること。
- v FAQ 又は利用手引書で対応できない質問・障害は、Adobe のサポートに調査及び対応依頼を行うこと。
- vi 質問に対する回答は、利用者向けに公開するため、必要に応じて FAQ、利用手引書として Web サイト上から閲覧可能なドキュメントを作成すること。
- vii アカウントの登録、変更、削除を行うこと。
- viii 1年に1回アカウントの棚卸し(要、不要の精査等)を行い、適正な設定を行うこと。
- ix サブスクリプション版を導入するにあたり、利用者向けの案内 Web ページを作成、更新すること。
- x サブスクリプション版を導入するにあたり、クラウド機能の無効化について検証を行うこと。

(セ) 業務用スマートフォン、データ通信端末の管理・運用作業

A 対象機器

- i 対象となる機器は、主に情報通信システム室が契約し利用者管理で支給するスマートフォン(以下支給スマートフォンと呼ぶ)、情報通信システム室が契約、管理し利用者に貸出するスマートフォン/データ通信端末(以下貸出スマートフォン及び貸出データ通信端末と呼ぶ)である。
- ii 支給スマートフォン、貸出スマートフォンの基本ソフトウェアは iOS または Android である。
- iii 2019年9月時点の支給スマートフォンは300台、貸出スマートフォン/貸出データ通信端末の台数は合計20台以下である。作業期間中に貸出端末を追加導入する場合は合計30台を超えないものとする。なお、機器交換等に伴い一時的に管理台数を増やす場合には別途協議の上で台数を増やすこととする。

B 支給スマートフォン、貸出スマートフォンの初期設定

- i スマートフォンの支給、貸出にあたり初期設定、初期アップデートを実施すること。
- ii スマートフォンの返却を受け端末内のデータ初期化を実施すること。

C 貸出スマートフォン、貸出データ通信端末の貸出、運用管理

- i 利用者からの申請を受付、貸出スマートフォン、貸出データ通信端末の貸出、返却受取を行うこと。
- ii 貸出スマートフォン、貸出データ通信端末の貸出先、在庫台数を管理すること。
- iii 利用者に貸出中の貸出スマートフォン、貸出データ通信端末に故障が発生し交換以外に復旧手段が無いと判断された場合は速やかに予備機と交換すること。

- iv 年に1回、貸出スマートフォン、貸出データ通信端末の利用状況の棚卸を実施すること。
 - v 貸出スマートフォンにインストールされたOS及びソフトウェア群は、当機構担当者の指示に従ってアップデートを実施すること。
- D スマートフォン専用リモートアクセスの設定（一部端末のみ）
- i 当機構担当者の指定した支給スマートフォン、貸出スマートフォンについて、スマートフォン専用リモートアクセスの設定を行うこと。
 - ii 対象デバイス数は90台、対象人数は60人以内とするが、これらを上回る場合は当機構担当者との協議を行うこと。
 - iii スマートフォン専用リモートアクセスの利用のため、デバイス証明書の発行及び利用者IDの払い出し・管理・棚卸を行うこと。
 - iv スマートフォン専用リモートアクセスを通じた機構内ネットワーク及びサービスの利用に際して、ネットワーク、サーバの設定変更が必要な場合、当機構担当者に申し出ること。
 - v 対象スマートフォンの紛失・盗難等が発生した場合、当機構担当者の指示に基づき証明書の失効処理を行うこと。
 - vi スマートフォン等のOSアップデートがあった場合、当機構担当者の指示に基づき、アップデート後に接続確認を行うこと。
- E 利用者からの質問に対する調査・回答
- i 支給スマートフォン、貸出スマートフォンについて、利用者からの情シスにて導入しているソフトウェアに関する問い合わせ、または通信不具合、端末不具合の問い合わせに対して調査・回答を行うこと。
 - ii 質問及び回答についての履歴管理を行うとともに、よくある質問とその答（FAQ）集を作成すること。
 - iii FAQ集はHTML形式文書で作成し、当機構担当者が指定する場所に登録すること。
- F 保守マニュアルの維持
- i 支給スマートフォン、貸出スマートフォン、データ通信端末の設定方法並びに障害対処方法などの保守マニュアルを随時更新し、維持すること。
 - ii 保守マニュアルはHTML形式文書で作成し、当機構担当者が指定する場所に登録すること。
- G 利用マニュアルの維持
- i 利用者向けの案内Webページを作成、更新すること。
 - ii 貸出スマートフォン、データ通信端末の申請手順、注意事項、利用開始方法の利用マニュアルを随時更新し、維持すること。
 - iii 利用マニュアルはHTML形式文書で作成し、当機構担当者が指定する場所に登録すること。

(ソ) eduroam アカウントの発行・管理

当機構は、国立情報学研究所の運用する国際無線 LAN ローミング基盤「eduroam JP」へ参加している。これについて、以下の対応を行うこと

- i 利用者から要望があった場合、接続用アカウントの発行を行い、管理簿に記載すること
- ii 発行したアカウントについて、情報セキュリティ上の問題が発生した場合、当機構担当者に確認後、失効処理を行うこと

(タ) 年度初め、人事異動、大規模な組織改編への対応

- i 年度初めとなる 4/1 付の新規採用者、組織整備・改変に伴う人事異動において、共通部門計算機の払い出し・セットアップ、アカウント新規発行・変更・削除の作業が集中するため、4/1 からの 5 営業日について下記の作業が実施可能な体制とすること。下記数量を大幅に超える見込みとなった場合、当機構と協議を行うこと。
 - ・ 共通事務部門計算機の払い出し・セットアップ 100 台
 - ・ 新規採用に伴う各業務システムユーザアカウントの新規発行 200 件
 - ・ 雇用種別変更に伴う各業務システムユーザアカウントの変更 50 人
 - ・ 上記に関連した問い合わせにも対応できるようにすること。
- ii 2021 年 4 月に当機構は第 5 期中長期計画を開始する予定であるが、これに伴い大規模な組織改編が発生する見込みである。組織構造や名称の変更と共に上記の 1.5 倍程度の業務が発生する可能性があるため、これを実施可能な体制とすること。

(チ) ユーザ利用満足度調査

(別紙 1 情報システムグループサポートデスク利用に関する満足度アンケート調査)

- i 年に 1 回の割合でユーザに対して、次の項目の満足度についてアンケートを実施し、その結果の基準スコア（75 点）を維持すること。
 - ・ 問い合わせから回答までに要した時間
 - ・ 回答又は手順に対する説明の分かりやすさ
 - ・ 回答又は手順に対する結果の正確性
 - ・ 担当者の対応（言葉遣い、親切さ、丁寧さ等）
- ii 各質問とも、「満足」（配点 100 点）、「ほぼ満足」（同 80 点）、「普通」（同 60 点）、「やや不満」（同 40 点）、「不満」（同 0 点）で採点し、各利用者の 4 つの回答の平均スコア（100 点満点）を算出する。

ウ サポートデスク業務、申請業務の実績値

サポートデスク業務、申請業務の過去 3 年における実績値を下記表にて示す。

2016	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	合計(件)
サポートデスク業務	339	244	251	333	316	273	210	244	187	222	219	246	3084
申請対応業務件数	1545	919	1046	920	821	849	685	755	829	997	714	1444	11524

2017	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	合計(件)
サポートデスク業務	251	191	185	168	153	136	235	182	168	166	164	242	2241
申請対応業務件数	2242	1613	1502	1207	1172	1190	1127	803	1230	1088	1257	2013	16444

2018	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	合計(件)
サポートデスク業務	253	183	140	202	174	194	253	318	307	258	203	253	2738
申請対応業務件数	2303	1414	1118	1570	1760	1357	1172	1083	1063	1321	1866	2491	18518

(5) 個別システム運用サービス

ア 会計システム

(ア) 概要

会計システムについて、安定運用並びに迅速・適切な運用支援を行うことを目的とする。

(イ) 対象機器

- A 物理サーバ：6 式、ストレージ：1 式、テープライブラリ 1 式、ネットワークスイッチ 4 式、UPS2 式、PDU2 式
- B 仮想サーバ：13 式
- C アプリケーション：会計アプリケーション、アプリケーション仮想化、ユーザ認証、データベース、バックアップ、サーバ監視、ファイル共有、ウイルス対策、UPS 制御等

注) 2020 年 4 月 1 日の時点では、機器リプレース、OS バージョンアップにより変更されている可能性もある。またこれらの各機器は随時変更することがあり、その都度、必要な対応を行うこと。(新機器設置作業や動作確認等)

(ウ) 業務内容

- A 質問への対応と履歴管理（クライアント端末導入ソフトの支援問い合わせ等）
利用者からの質問・要望に対する調査、回答を行うこと。質問・要望及び回答の内容についての履歴管理を行う。また、FAQ を作成し、会計システムのホームページ上から閲覧可能とすること。
- B 利用者への周知
サーバの停止、運用方法の変更、計算機の構成変更など会計システム利用者に影響のあると思われる内容については、当機構担当者の指示に従い利用者への周知を行うこと。また、それに伴う会計システムホームページの更新作業を行うこと。
- C 保守業者の保守作業、改修作業の支援
保守業者の保守作業やプログラム等の改修作業に伴う、作業計画、作業調整、関係各所との調整、作業後のサービス確認等の支援を行う。
- D 各種登録作業
下記について職員採用時の新規登録作業および人事異動、組織変更に伴う登録変更作業を行うこと。
 - ・会計システムログイン ID
 - ・プロジェクトコード
 - ・会計システム予算照会
 - ・会計システム予算計画
- E サーバ稼働状況確認（ハードウェア、仮想環境、OS）
 - i サーバの稼働状態（電源 ON/OFF の状態）を確認し、電源が投入されてい

ない等、ネットワーク上から確認できないサーバがあった場合は、ネットワークの接続状態を確認の上、状況を当機構担当者に報告するとともに、障害復旧作業を行うこと。

- ii 監視サーバにより他のサーバの CPU 使用率、ディスク使用率、メモリ使用率、ネットワーク等のリソース状況を監視し、異常な負荷・通信を示しているサーバを発見した場合にはその原因を究明、排除、あるいは改善し、当機構担当者に報告すること。
- iii 監視サーバにより他のサーバの CPU 使用率、ディスク使用率、メモリ使用率、ネットワーク等のリソース情報を定期的に収集し、収集した情報をもとに、仮想サーバのサイジングの見直し、最適化、傾向分析を行うこと。
- iv 監視サーバ上で Nagios、MRTG、NetFlow アナライザ、NIRVANA、SCVMM、SytemDirector など、すでに構築されている監視ソフトを稼働させ、サーバの稼働状態を常時モニターすること。
- v 監視は Nagios を使用し、マルチベンダ環境を監視できるよう随時設定の追加、見直しを行うこと。(監視プラグインの自作・改修を含む)
- vi 用意された監視機構が無くとも、技術的に可能であればこれを内製し、Nagios へ監視統合を実施すること。
- vii 情報システムグループ管理外の機器であっても必要に応じて監視を検討・実施すること。
- viii ストレージ監視
 - ・ハードディスク・SSD 等（外付けディスクアレイを含む）の使用量を監視し、ハードディスク・SSD 等の使用量が一定量を越えている場合には、原因を分析し、当機構担当者に報告すること。
 - ・サーバ等のストレージ障害を検知した場合は、障害状態を分析し、当機構担当者に報告すること。また、メーカーへの連絡、修理対象品の梱包作業等を行うこと。
- ix 通信ポート監視
 - ・サーバ又は管理端末で不要ポート及びサービスの稼働状態を監視し、不要ポート及びサービスが起動している機器を発見した場合は速やかに当機構担当者に報告し、サービス停止等の作業を実施すること。
- x 無停電電源装置監視
 - ・無停電電源装置からの警告等の障害情報が通知された場合は、障害情報を分析して当機構担当者に報告すること。また、メーカーに連絡し、協力して、速やかに復旧作業を行うこと。
 - ・JEMA-MIB 又は RFC 1628 に対応した機器の選定と、監視を行うこと。
- xi OS・ソフト等の状態監視
 - ・サーバから、障害情報が通知された場合は、障害情報を分析して当機構担当者及びシステム開発元に報告の上、速やかな復旧作業を行うこと。

- ・サーバでのディレクトリサービスシステムのアプリケーション単位で性能情報（CPU 使用率、メモリ使用量等）の異常情報が発見又は通知された場合は、当機構担当者及びシステム開発元に報告すること。
 - ・障害で調査を要する場合、又は、当機構担当者から障害調査を依頼された場合は、サーバ等にリモートログインして、障害情報を取得・分析し、復旧作業を行うこと。
- xii ソフトウェア障害監視
- ・サーバから基本ソフトウェアや、他のインストールソフトウェアからの警告等の障害情報が通知された場合は、障害情報を分析して当機構担当者に報告すること。また、メーカー、システム開発元に連絡し、協力して、速やかに復旧作業を行うこと。
- F サーバ証明書の更新
- サーバ証明書の有効期限を確認し、継続して利用ができるように、CSR の生成、当機構担当者へのサーバ証明書更新の依頼、証明書の受け取り、証明書のインストールを行う。
- G ウィルス定義ファイルの確認、更新作業
- 対象機器のウィルス定義パターンファイルが最新であることを確認する最新版でない場合は更新をすること。回数の上限は設定しない（無制限）。セキュリティの観点から（原則）リリースされたらただちにアップデートを行うこと。利用者への情報公開、周知等を行うこと。
- H サーバの障害対応（一次切り分けまで）
- i トラブル発生時には、サービスの確認、機器の Status 確認、ログ確認等迅速な障害の切り分け、原因究明を行うと共に、その復旧に必要な処置又は業者との対応を迅速に行うこと。
- 復旧が困難な場合は、速やかに代替のサーバ機器を予備品から用意し運用を開始すること。バックアップ機がある場合には切替えを行うこと。
- また、トラブルにともなう利用者への影響について、利用者へ内容の周知を行うこと。
- 運用開始時にセキュリティの課題を提示し、四半期(3 か月)ごとに対策及び実施報告を行うこと。
- ii トラブルへの対処については、当機構担当者との協議の上、作業を行うものとし、終了時には報告すると共に問題点を検討・分析し、今後の改善事項にフィードバックさせること。トラブル報告書の作成、トラブルの履歴情報を管理すること。
- iii トラブルの原因が機器のソフトウェアにある場合は、当機構担当者との協議の上、ソフトウェアのバージョンアップを行うこと。
- I サーバのバックアップ
- i データのバックアップ計画を策定し、当機構担当者の承認を受けたのちに実

- 行すること。なお、ユーザデータについては1日1回以上、システム及びシステム設定データについては更新の都度、他のディスクにコピーすること。また、1週間に1回以上はテープにバックアップすること。
- ii テープは4世代以上バックアップすること。バックアップが計画どおりに行われていない場合は、速やかに原因を分析し、解決すること。
- J サーバのリストア**
- i ハードディスクあるいはディスクアレイが故障し、復旧できない場合は、最新のバックアップ用ディスクアレイあるいはバックアップデータを基にリストアを行うこと。データ量次第ではあるが、原則即日復旧できるように努めること。
 - ii ユーザからファイルリストアの要求があった場合は、リストアを行うこと。データ量次第ではあるが、原則即日対応できるように努めること。
- K 監視項目見直し等による設定変更**
- 監視項目の見直しやセキュリティ対策等により、監視ツールやOS設定の変更を行うこと。
- L Windows、Mac等最新クライアントOSの維持管理作業**
- i 当該システムの対応調査、問い合わせ。
 - ii 導入業者からの利用マニュアルの入手、利用者向けの案内Webページの作成、FAQ作成、更新。
- M 停電等の対応**
- i 計画停電等の前に、停電復旧時にサーバを自動起動する設定を確認、設定されていない場合は設定をすること。停電時にサーバを自動シャットダウンする設定を行うこと。
 - ii オムロン製、APC製等個別無停電電源装置(UPS)の設定を行うこと。UPSに対応していない機器については、対応可能な範囲で安全にシャットダウンできる機構を内製すること。又はリモートでの電源投入に係る手順を作成すること。その際、システムが正常に機能するために一定の順序で起動しなければならない機器については、起動シーケンスを制御すること。
- N サーバシステム構成図の維持管理**
- 基幹スイッチ、ルータから各サーバ、ストレージ、アプライアンスまでの接続図を維持すること。ネットワークの構成に変更があった場合は、遅滞無く書類を修正して情報システムグループに提出すること。
- O サーバ管理表の維持管理**
- 各サーバ、ストレージ、アプライアンスの機種、機器名、シリアル番号、購入時期、保守等の情報が管理されている表を維持すること。ネットワーク構成に変更があった場合や機器交換があった場合等、遅滞無く書類を修正して提出すること。
- P 日常業務解説書の維持管理**

- i 本契約に基づいて実施する日々の日常業務内容を第三者でも分かるように記した日常業務解説書を維持すること。
- ii 日常業務内容に変化があった場合、遅滞なく書類を修正して提出すること。

Q 利用マニュアルの維持管理

- i 一般利用者を対象とした、各サーバの利用方法に関するマニュアルを維持し、当機構内イントラ Web サーバを用いて公開すること。
- ii 利用方法に変更があった場合は遅滞なくマニュアルを修正すること。

R FAQ の維持管理

- i 利用者あるいは当機構担当者から問い合わせがあった場合は、問い合わせ内容を調査し、必要な支援を行うとともに、問い合わせ内容とその回答を、「よくある質問とその答え (FAQ)」として Web サーバに登録し、Web ブラウザで閲覧可能とすること。
- ii 契約前に存在していた FAQ を含めて、登録済内容のメンテナンスを行うこと。
- iii 問い合わせ内容については履歴管理を行うこと。

イ 電子決裁システム

(ア) 概要

電子決裁システムについて、安定運用ならびに迅速・適切な運用支援を行うことを目的とする。

(イ) 対象機器

A 仮想サーバ：2 式

B アプリケーション：電子決裁アプリケーション、データベース、バックアップ、サーバ監視、ウィルス対策

注) 2020 年 4 月 1 日の時点では、機器リプレース、OS バージョンアップにより変更されている可能性もある。またこれらの各機器は随時変更することがあり、その都度、必要な対応を行うこと。(新機器設置作業や動作確認等)

(ウ) 業務内容

A 問い合わせ対応 (質問の振り分け)

- i 問合せ対応 (電話・メール)
- ii 電子決裁システムに関する意見、要望の受付
※振り分け基準はシステムデータ内でユーザ情報に関する件で職員側での判断を要する修正作業等は担当職員へ、その他はサポートデスク対応

B リソース管理

仮想マシンの CPU、メモリ、ディスク等のリソースの払い出しを管理表で記録し、リソース不足等によるリソース追加時には管理表を更新すること。

C サーバ稼働状況確認 (ハードウェア、仮想環境、OS)

- i サーバの稼働状態 (電源 ON/OFF の状態) を確認し、電源が投入されてい

ない等、ネットワーク上から確認できないサーバがあった場合は、ネットワークの接続状態を確認の上、状況を当機構担当者に報告するとともに、障害復旧作業を行うこと。

- ii 監視サーバにより他のサーバの CPU 使用率、ディスク使用率、メモリ使用率、ネットワーク等のリソース状況を監視し、異常な負荷・通信を示しているサーバを発見した場合にはその原因を究明、排除、あるいは改善し、当機構担当者に報告すること。
- iii 監視サーバにより他のサーバの CPU 使用率、ディスク使用率、メモリ使用率、ネットワーク等のリソース情報を定期的に収集し、収集した情報をもとに、仮想サーバのサイジングの見直し、最適化、傾向分析を行うこと。
- iv 監視サーバ上で Nagios、MRTG、NetFlow アナライザ、NIRVANA など、すでに構築されている監視ソフトを稼働させ、サーバの稼働状態を常時モニターすること。
- v 監視は Nagios を使用し、マルチベンダ環境を監視できるよう随時設定の追加、見直しを行うこと。(監視プラグインの自作・改修を含む)
- vi 用意された監視機構が無くとも、技術的に可能であればこれを内製し、Nagios へ監視統合を実施すること。
- vii 情報システムグループ管理外の機器であっても必要に応じて監視を検討・実施すること。
- viii ストレージ監視
 - ・ディスクの使用量を監視し、使用量が一定量を越えている場合には、原因を分析し、当機構担当者に報告すること。
 - ・サーバ等のストレージ障害を検知した場合は、障害状態を分析し、当機構担当者に報告すること。
- ix Web サーバアクセス状況監視
 - ・サーバへのアクセス状況をソフトウェアで監視し、認証機能のついた Web ページで随時閲覧できるようにすること。
- x 通信ポート監視
 - ・サーバ又は管理端末で不要ポート及びサービスの稼働状態を監視し、不要ポート及びサービスが起動している機器を発見した場合は速やかに当機構担当者に報告し、サービス停止等の作業を実施すること。
- xi OS・ソフト等の状態監視
 - ・サーバから、障害情報が通知された場合は、障害情報を分析して当機構担当者及びシステム開発元に報告の上、速やかな復旧作業を行うこと。
 - ・サーバでのディレクトリサービスシステムのアプリケーション単位で性能情報（CPU 使用率、メモリ使用量等）の異常情報が発見又は通知された場合は、当機構担当者及びシステム開発元に報告すること。
 - ・障害で調査を要する場合、又は、当機構担当者から障害調査を依頼された

場合は、サーバ等にリモートログインして、障害情報を取得・分析し、復旧作業を行うこと。

D サーバの障害対応（一次切り分けまで）

- i トラブル発生時には、サービスの確認、機器の Status 確認、ログ確認等迅速な障害の切り分け、原因究明を行うと共に、その復旧に必要な処置又は業者との対応を迅速に行うこと。

復旧が困難な場合は、速やかに仮想サーバのロールバックや正常なバックアップ・スナップショットイメージからのクローン等を活用し運用を開始すること。バックアップ機がある場合には切替えを行うこと。

また、トラブルにともなう利用者への影響について、利用者へ内容の周知を行うこと。

運用開始時にセキュリティの課題を提示し、四半期(3 か月)ごとに対策及び実施報告を行うこと。

- ii トラブルへの対処については、当機構担当者との協議の上、作業を行うものとし、終了時には報告すると共に問題点を検討・分析し、今後の改善事項にフィードバックさせること。トラブル報告書の作成、トラブルの履歴情報を管理すること。
- iii トラブルの原因が機器のソフトウェアにある場合は、当機構担当者との協議の上、ソフトウェアのバージョンアップを行うこと。

E サーバ証明書の更新

サーバ証明書の有効期限を確認し、継続して利用ができるように、CSR の生成、当機構担当者へのサーバ証明書更新の依頼、証明書の受け取り、証明書のインストールを行う。

F ウィルス定義ファイルの確認、更新作業

対象機器のウィルス定義パターンファイルが最新であることを確認する最新版でない場合は更新をすること。回数の上限は設定しない（無制限）。

セキュリティの観点から（原則）リリースされたらただちにアップデートを行うこと。利用者への情報公開、周知等を行うこと。

G サーバのバックアップ

- i データのバックアップ計画を策定し、当機構担当者の承認を受けたのちに実行すること。なお、スナップショットイメージについては 1 日 1 回以上、月に 1 回以上はテープにバックアップすること。
- ii テープは 4 世代以上バックアップすること。バックアップが計画どおりに行われていない場合は、速やかに原因を分析し、解決すること。

H サーバのリストア

- i 仮想ディスク上のファイルシステムが破損し、復旧できない場合は、最新のバックアップデータを基にリストアを行うこと。データ量次第ではあるが、原則 3 営業日以内に復旧できるように努めること。

- ii 当機構担当者からリストアの要求があった場合は、リストアを行うこと。データ量次第ではあるが、原則3営業日内に対応できるように努めること。
- I 監視項目見直し等による設定変更
 - 監視項目の見直しやセキュリティ対策等により、監視ツールや OS 設定の変更を行うこと。
- J Windows、Mac 等最新クライアント OS の維持管理作業
 - i 当該システムの対応調査、問い合わせ。
 - ii 導入業者からの利用マニュアルの入手、利用者向けの案内 Web ページの作成、FAQ 作成、更新。
- K 停電等の対応
 - i 計画停電等の前に、停電復旧時にサーバを自動起動する設定を確認、設定されていない場合は設定をすること。停電時にサーバを自動シャットダウンする設定を行うこと。
- L サーバシステム設計書の維持管理
 - i 各サーバの設計書を維持すること。
 - ii サーバの構成に変更があった場合は、遅滞無く書類を修正して提出すること。
 - iii 想定読者は、サーバの基礎的知識はあるが、SE 経験は無い者が対象。
- M サーバシステム構成図の維持管理
 - 基幹スイッチ、ルータから各サーバ、ストレージ、アプライアンスまでの接続図を維持すること。ネットワークの構成に変更があった場合は、遅滞無く書類を修正して情報システムグループに提出すること。
- N サーバ管理表の維持管理
 - 各サーバ、ストレージ、アプライアンスの機種、機器名、シリアル番号、購入時期、保守等の情報が管理されている表を維持すること。ネットワーク構成に変更があった場合や機器交換があった場合等、遅滞無く書類を修正して提出すること。
- O システム障害時対応手順書の維持管理
 - i 発生が予想される障害に対し、具体的にどのような手順でシステムを復旧するかを記した障害時対応手順書を維持すること。
 - ii 予想される障害に変化があった場合、あるいは、手順の見直しを行った場合は、遅滞なく書類を修正して提出すること。
- P 日常業務解説書の維持管理
 - i 本契約に基づいて実施する日々の日常業務内容を第三者でも分かるように記した日常業務解説書を維持すること。
 - ii 日常業務内容に変化があった場合、遅滞なく書類を修正して提出すること。

ウ 勤務管理システム

(ア) 概要

勤務管理システムについて、安定運用ならびに迅速・適切な運用支援を行うことを目的とする。

(イ) 対象機器

A 仮想サーバ：4式

B アプリケーション：勤務管理アプリケーション、データベース、バックアップ、サーバ監視、ウィルス対策

注) 2020年4月1日の時点では、機器リプレース、OSバージョンアップにより変更されている可能性もある。またこれらの各機器は随時変更することがあり、その都度、必要な対応を行うこと。(新機器設置作業や動作確認等)

(ウ) 業務内容

A 問い合わせ対応

i 問合せ対応 (電話・メール)

ii 勤務管理システムに関する意見、要望の受付

※振り分け基準はシステムデータ内でユーザ情報に関する件で職員側での判断を要する修正作業等は担当職員へ、その他はサポートデスク対応

B 定期メンテナンスの支援

当機構担当者が定期メンテナンスをするため、作業端末の貸出の調整、端末の環境設定等の支援を行う。

C リソース管理

仮想マシンのCPU、メモリ、ディスク等のリソースの払い出しを管理表で記録し、リソース不足等によるリソース追加時には管理表を更新すること。

D サーバ稼働状況確認 (ハードウェア、仮想環境、OS)

i サーバの稼働状態 (電源 ON/OFF の状態) を確認し、電源が投入されていない等、ネットワーク上から確認できないサーバがあった場合は、ネットワークの接続状態を確認の上、状況を当機構担当者に報告するとともに、障害復旧作業を行うこと。

ii 監視サーバにより他のサーバのCPU使用率、ディスク使用率、メモリ使用率、ネットワーク等のリソース状況を監視し、異常な負荷・通信を示しているサーバを発見した場合にはその原因を究明、排除、あるいは改善し、当機構担当者に報告すること。

iii 監視サーバにより他のサーバのCPU使用率、ディスク使用率、メモリ使用率、ネットワーク等のリソース情報を定期的に収集し、収集した情報をもとに、仮想サーバのサイジングの見直し、最適化、傾向分析を行うこと。

iv 監視サーバ上で Nagios、MRTG、NetFlow アナライザ、NIRVANA など、すでに構築されている監視ソフトを稼働させ、サーバの稼働状態を常時モニターすること。

v 監視は Nagios を使用し、マルチベンダ環境を監視できるよう随時設定の追加、見直しを行うこと。(監視プラグインの自作・改修を含む)

- vi 用意された監視機構が無くとも、技術的に可能であればこれを内製し、Nagios へ監視統合を実施すること。
 - vii 情報システムグループ管理外の機器であっても必要に応じて監視を検討・実施すること。
 - viii ストレージ監視
 - ・ディスクの使用量を監視し、使用量が一定量を越えている場合には、原因を分析し、当機構担当者に報告すること。
 - ・サーバ等のストレージ障害を検知した場合は、障害状態を分析し、当機構担当者に報告すること。
 - ix Web サーバアクセス状況監視
 - ・サーバへのアクセス状況をソフトウェアで監視し、認証機能のついた Web ページで随時閲覧できるようにすること。
 - x 通信ポート監視
 - ・サーバ又は管理端末で不要ポート及びサービスの稼動状態を監視し、不要ポート及びサービスが起動している機器を発見した場合は速やかに当機構担当者に報告し、サービス停止等の作業を実施すること。
 - xi OS・ソフト等の状態監視
 - ・サーバから、障害情報が通知された場合は、障害情報を分析して当機構担当者及びシステム開発元に報告の上、速やかな復旧作業を行うこと。
 - ・サーバでのディレクトリサービスシステムのアプリケーション単位で性能情報（CPU 使用率、メモリ使用量等）の異常情報が発見又は通知された場合は、当機構担当者及びシステム開発元に報告すること。
 - ・障害で調査を要する場合、又は、当機構担当者から障害調査を依頼された場合は、サーバ等にリモートログインして、障害情報を取得・分析し、復旧作業を行うこと。
- E サーバの障害対応（一次切り分けまで）**
- i トラブル発生時には、サービスの確認、機器の Status 確認、ログ確認等迅速な障害の切り分け、原因究明を行うと共に、その復旧に必要な処置又は業者との対応を迅速に行うこと。
 復旧が困難な場合は、速やかに仮想サーバのロールバックや正常なバックアップ・スナップショットイメージからのクローン等を活用し運用を開始すること。バックアップ機がある場合には切替えを行うこと。
 また、トラブルにともなう利用者への影響について、利用者へ内容の周知を行うこと。
 運用開始時にセキュリティの課題を提示し、四半期(3 か月)ごとに対策及び実施報告を行うこと。
 - ii トラブルへの対処については、当機構担当者との協議の上、作業を行うものとし、終了時には報告すると共に問題点を検討・分析し、今後の改善事項につ

- ードバックさせること。トラブル報告書の作成、トラブルの履歴情報を管理すること。
- iii トラブルの原因が機器のソフトウェアにある場合は、当機構担当者と協議の上、ソフトウェアのバージョンアップを行うこと。
- F サーバ証明書の更新**
- サーバ証明書の有効期限を確認し、継続して利用ができるように、CSR の生成、当機構担当者へのサーバ証明書更新の依頼、証明書の受け取り、証明書のインストールを行う。
- G ウィルス定義ファイルの確認、更新作業**
- 対象機器のウィルス定義パターンファイルが最新であることを確認する最新版でない場合は更新をすること。回数の上限は設定しない（無制限）。セキュリティの観点から（原則）リリースされたらただちにアップデートを行うこと。利用者への情報公開、周知等を行うこと。
- H サーバのバックアップ**
- i データのバックアップ計画を策定し、当機構担当者の承認を受けたのちに実行すること。なお、スナップショットについては 1 日 1 回以上、月に 1 回以上はテープにバックアップすること。
- ii テープは 4 世代以上バックアップすること。バックアップが計画どおりに行われていない場合は、速やかに原因を分析し、解決すること。
- I サーバのリストア**
- i 仮想ディスク上のファイルシステムが破損し、復旧できない場合は、最新のバックアップデータを基にリストアを行うこと。データ量次第ではあるが、原則 3 営業日以内に復旧できるように努めること。
- ii 当機構担当者からリストアの要求があった場合は、リストアを行うこと。データ量次第ではあるが、原則 3 営業日以内に対応できるように努めること。
- J 監視項目見直し等による設定変更**
- 監視項目の見直しやセキュリティ対策等により、監視ツールや OS 設定の変更を行うこと。
- K Windows、Mac 等最新クライアント OS、Web ブラウザの維持管理作業**
- i 当該システムの対応調査、問い合わせ。
- ii 導入業者からの利用マニュアルの入手、利用者向けの案内 Web ページの作成、FAQ 作成、更新。
- L 停電等の対応**
- i 計画停電等の前に、停電復旧時にサーバを自動起動する設定を確認、設定されていない場合は設定をすること。停電時にサーバを自動シャットダウンする設定を行うこと。
- M サーバシステム設計書の維持管理**
- i 各サーバの設計書を維持すること。

- ii サーバの構成に変更があった場合は、遅滞無く書類を修正して提出すること。
- iii 設計書をもとにサーバを再構築できるレベル及び内容で設計書を作成すること。
- iv 想定読者は、サーバの基礎的知識はあるが、SE 経験は無い者が対象。

N サーバシステム構成図の維持管理

基幹スイッチ、ルータから各サーバ、ストレージ、アプライアンスまでの接続図を維持すること。ネットワークの構成に変更があった場合は、遅滞無く書類を修正して情報システムグループに提出すること。

O サーバ管理表の維持管理

各サーバ、ストレージ、アプライアンスの機種、機器名、シリアル番号、購入時期、保守等の情報が管理されている表を維持すること。ネットワーク構成に変更があった場合や機器交換があった場合等、遅滞無く書類を修正して提出すること。

P システム障害時対応手順書の維持管理

- i 発生が予想される障害に対し、具体的にどのような手順でシステムを復旧するかを記した障害時対応手順書を維持すること。
- ii 予想される障害に変化があった場合、あるいは、手順の見直しを行った場合は、遅滞なく書類を修正して提出すること。

Q 日常業務解説書の維持管理

- i 本契約に基づいて実施する日々の日常業務内容を第三者でも分かるように記した日常業務解説書を維持すること。
- ii 日常業務内容に変化があった場合、遅滞なく書類を修正して提出すること。

R 利用マニュアルの維持管理

- i 一般利用者を対象とした、各サーバの利用方法に関するマニュアルを維持し、当機構内イントラ Web サーバを用いて公開すること。
- ii 利用方法に変更があった場合は遅滞なくマニュアルを修正すること。

S FAQ の維持管理

- i 利用者あるいは当機構担当者から問い合わせがあった場合は、問い合わせ内容を調査し、必要な支援を行うとともに、問い合わせ内容とその回答を、「よくある質問とその答え (FAQ)」として Web サーバに登録し、Web ブラウザで閲覧可能とすること。
- ii 契約前に存在していた FAQ を含めて、登録済内容のメンテナンスを行うこと。
- iii 問い合わせ内容については履歴管理を行うこと。

エ 広報部サーバ運用

(ア) 概要

広報部のコンテンツ・マネージメント・システム(CMS)、アクセスログ解析ソフトウ

ウェアをインストールしてある仮想サーバ、並びに、仮想サーバが動作している物理サーバのシステム領域・データ領域のバックアップ、障害発生時のリストア、安定運用のための監視作業、及びそれらに付随するサーバ運用作業を行うこと。

(イ) 対象機器

A 仮想サーバ：3式

アプリケーション：本番用 CMS、検証用 CMS、アクセスログ解析

注) 2020年4月1日の時点では、機器リプレース、OSバージョンアップにより変更されている可能性もある。またこれらの各機器は随時変更することがあり、その都度、必要な対応を行うこと。(新機器設置作業や動作確認等)

(ウ) 業務内容

A 依頼対応

- i 仮想サーバの起動
- ii ネットワーク切り替え
- iii 仮想ディスクのサイズ拡張
- iv 仮想サーバの仮想 CPU の割当個数の変更(単に個数を変更するだけでなく、使用する物理 CPU の CPU 番号を指定した変更方法を含む)
- v CMS のバージョンアップ(作業は年3回程度、2018年度実績4回)
- vi アクセスログ解析ソフトウェアのバージョンアップ及び解析プロファイルの作成・修正

B サーバ稼働状況確認 (ハードウェア、仮想環境、OS、アプリケーション)

- i サーバの稼働状態を確認し、起動されていない等、ネットワーク上から確認できないサーバがあった場合は、ネットワークの接続状態を確認の上、状況を当機構担当者に報告するとともに、障害復旧作業を行うこと。
- ii 監視サーバによりサーバの CPU 使用率、ディスク使用率、メモリ使用率、ネットワーク等のリソース状況を監視し、異常な負荷・通信を示しているサーバを発見した場合にはその原因を究明、排除、あるいは改善し、当機構担当者に報告すること。
- iii 監視サーバによりサーバの CPU 使用率、ディスク使用率、メモリ使用率、ネットワーク等のリソース情報を定期的に収集し、収集した情報をもとに、仮想サーバのサイジングの見直し、最適化、傾向分析を行うこと。
- iv 監視サーバ上で Nagios、MRTG、NetFlow アナライザ、NIRVANA など、すでに構築されている監視ソフトを稼働させ、サーバの稼働状態を常時モニターすること。
- v 監視は Nagios を使用し、マルチベンダ環境を監視できるよう随時設定の追加、見直しを行うこと。(監視プラグインの自作・改修を含む)
- vi 用意された監視機構が無くとも、技術的に可能であればこれを内製し、Nagios へ監視統合を実施すること。
- vii 情報システムグループ管理外の機器であっても必要に応じて監視を検討・実

施すること。

viii ストレージ監視

- ・ディスクの使用量を監視し、使用量が一定量を越えている場合には、原因を分析し、当機構担当者に報告すること。
- ・サーバ等のストレージ障害を検知した場合は、障害状態を分析し、当機構担当者に報告すること。

ix Web サーバアクセス状況監視

- ・サーバへのアクセス状況をソフトウェアで監視し、認証機能のついた Web ページで随時閲覧できるようにすること。

x 通信ポート監視

- ・サーバ又は管理端末で不要ポート及びサービスの稼動状態を監視し、不要ポート及びサービスが起動している機器を発見した場合は速やかに当機構担当者に報告し、サービス停止等の作業を実施すること。

xi OS・ソフト等の状態監視

- ・サーバから、障害情報が通知された場合は、障害情報を分析して当機構担当者及びシステム開発元に報告の上、速やかな復旧作業を行うこと。
- ・サーバでのディレクトリサービスシステムのアプリケーション単位で性能情報（CPU 使用率、メモリ使用量等）の異常情報が発見又は通知された場合は、当機構担当者及びシステム開発元に報告すること。
- ・障害で調査を要する場合、又は、当機構担当者から障害調査を依頼された場合は、サーバ等にリモートログインして、障害情報を取得・分析し、復旧作業を行うこと。
- ・アクセスログ解析ソフトウェアの日次処理が正常に終了しているか、営業日は 1 日 1 回確認し、正常に終了していない場合は、日次処理の再実行を行うこと。

C ステータス通知メール送信スクリプトの管理

root ログイン時、起動時、シャットダウン開始時、リブート開始時及び毎日定時に、設定したメールアドレスにメールを通知する設定にしている(構成変更したあと、一部メールは送信されない状態となっている)。これらの通知メールについて、運用に必要であれば、適宜修正すること。ただし、ステータス通知メールによらず運用を行う場合はこの限りでない。

D サーバの障害対応（一次切り分けまで）

- i
- トラブル発生時には、サービスの確認、機器の Status 確認、ログ確認等迅速な障害の切り分け、原因究明を行うと共に、その復旧に必要な処置又は業者との対応を迅速に行うこと。
- 復旧が困難な場合は、速やかに代替のサーバ機器を予備品から用意し運用を開始すること。バックアップ機がある場合には切替えを行うこと。
- また、トラブルにともなう利用者への影響について、利用者へ内容の周知を

行うこと。

運用開始時にセキュリティの課題を提示し、四半期(3 か月)ごとに対策及び実施報告を行うこと。

- ii トラブルへの対処については、当機構担当者と協議の上、作業を行うものとし、終了時には報告すると共に問題点を検討・分析し、今後の改善事項にフィードバックさせること。トラブル報告書の作成、トラブルの履歴情報を管理すること。
- iii トラブルの原因が機器のソフトウェアにある場合は、当機構担当者と協議の上、ソフトウェアのバージョンアップを行うこと。

E サーバのバックアップ

- i データのバックアップ計画を策定し、当機構担当者の承認を受けたのちに実行すること。なお、スナップショットについては1日1回以上、月に1ヶ月に1回以上はテープにバックアップすること。
- ii テープは4世代以上バックアップすること。バックアップが計画どおりに行われていない場合は、速やかに原因を分析し、解決すること。

F サーバのリストア

- i 仮想ディスク上のファイルシステムが破損し、復旧できない場合は、バックアップデータを基にリストアを行うこと。データ量次第ではあるが、原則即日復旧できるように努めること。
- ii 当機構担当者からファイルリストアの要求があった場合は、リストアを行うこと。データ量次第ではあるが、原則即日対応できるように努めること。

G パッチ、ホットフィックスの適用

- i ソフトウェア提供元からパッチやホットフィックス等が提供された場合は、予備機あるいは検証機で動作確認を行った上で、パッチやホットフィックスの適用を行うこと。
- ii メールサーバ、プロキシサーバ経由での悪意あるソフトウェアの侵入を防止するためソフトウェアのパッチ適用、対策ソフトウェアのパターン更新、利用者への情報公開等を行うこと。
- iii パッチ当ての可否については受注者が判断し、作業すること。
- iv CMS サーバの作業については、平日 17:15~22:00 までを目安として対応をすること。(月1回程度)

H サーバ証明書の更新

サーバ証明書の有効期限を確認し、継続して利用ができるように、CSRの生成、当機構担当者へのサーバ証明書更新の依頼、証明書の受け取り、証明書のインストールを行う。

I 監視項目見直し等による設定変更

監視項目の見直しやセキュリティ対策等により、監視ツールやOS設定の変更を行うこと。

- J Windows、Mac 等最新クライアント OS、Web ブラウザの維持管理作業
 - i 当該システムの対応調査、問い合わせ。
 - ii 導入業者からの利用マニュアルの入手、利用者向けの案内 Web ページの作成、FAQ 作成、更新。
- K 停電等の対応
 - i 計画停電等の前に、停電復旧時にサーバを自動起動する設定を確認、設定されていない場合は設定をすること。停電時にサーバを自動シャットダウンする設定を行うこと。
- L サーバシステム設計書の維持管理
 - i 各サーバの設計書を維持すること。
 - ii サーバの構成に変更があった場合は、遅滞無く書類を修正して提出すること。
 - iii 設計書をもとにサーバを再構築できるレベル及び内容で設計書を作成すること。
 - iv 想定読者は、サーバの基礎的知識はあるが、SE 経験は無い者が対象。
- M サーバシステム構成図の維持管理

基幹スイッチ、ルータから各サーバ、ストレージ、アプライアンスまでの接続図を維持すること。ネットワークの構成に変更があった場合は、遅滞無く書類を修正して情報システムグループに提出すること。
- N サーバ管理表の維持管理

各サーバ、ストレージ、アプライアンスの機種、機器名、シリアル番号、購入時期、保守等の情報が管理されている表を維持すること。ネットワーク構成に変更があった場合や機器交換があった場合等、遅滞無く書類を修正して提出すること。
- O 日常業務解説書の維持管理
 - i 本契約に基づいて実施する日々の日常業務内容を第三者でも分かるように記した日常業務解説書を維持すること。
 - ii 日常業務内容に変化があった場合、遅滞なく書類を修正して提出すること。

オ NTP ネットワーク運用

(ア) 概要

NTP の情報を発信するネットワークにおいて安定運用のための監視作業、及びそれらに付随する運用作業を行うこと。

(イ) 対象機器

ネットワークスイッチ：2 式

注) 2020 年 4 月 1 日の時点では、機器リプレースにより変更されている可能性もある。またこれらの各機器は随時変更することがあり、その都度、必要な対応を行うこと。(新機器設置作業や動作確認等)

(ウ) 業務内容

A ネットワーク稼働状況確認・障害対応

- i ネットワークスイッチの稼働状態（電源 ON/OFF の状態）を確認し、電源が投入されていない等、ネットワーク上から確認できないサーバがあった場合は、ネットワークの接続状態を確認の上、状況を当機構担当者に報告するとともに、障害復旧作業を行うこと。
- ii 監視サーバによりリソース状況を監視し、異常な負荷・通信を示している機器を発見した場合にはその原因を究明、排除、あるいは改善し、当機構担当者に報告すること。
- iii 障害情報が通知された場合は、障害情報を分析して当機構担当者及び報告の上、速やかな復旧作業を行うこと。
- iv 障害で調査を要する場合、又は、当機構担当者から障害調査を依頼された場合は、ネットワークスイッチ等にリモートログインして、障害情報を取得・分析し、復旧作業を行うこと。
- v 復旧が困難な場合は、速やかに代替のサーバ機器を予備品から用意し運用を開始すること。バックアップ機がある場合には切替えを行うこと。
- vi トラブルへの対処については、当機構担当者との協議の上、作業を行うものとし、終了時には報告すると共に問題点を検討・分析し、今後の改善事項にフィードバックさせること。トラブル報告書の作成、トラブルの履歴情報を管理すること。

カ 職員間情報共有システム

(ア) 概要

職員間情報共有システムについて、安定運用ならびに迅速・適切な運用支援を行うことを目的とする。

(イ) 対象機器・サービス

A サービス：外部グループウェアサービス 1 式 (2200 ユーザライセンス、60 クライアント証明書ライセンス、80Web アプリケーションライセンス)

B 仮想サーバ：1 式

注) 2020 年 4 月 1 日の時点では、機器リプレース、OS バージョンアップにより変更されている可能性もある。またこれらの各機器は随時変更することがあり、その都度、必要な対応を行うこと。(新機器設置作業や動作確認等)

(ウ) 業務内容

A コンサルティング

職員間情報共有システムの当機構内でのさらなる活用、展開に向けて、機能拡張およびサービス提供範囲の拡大を検討、提案すること。機能拡張を行う場合は、必要に応じて機能評価、サービス展開にあたる運用方針の検討を行い、当機構担当者との協議すること。

- B 問い合わせ対応（質問の振り分け）
- i 職員間情報共有システムの使い方に関する問合せ（電話・メール・Web）に対応すること。
 - ii 職員間情報共有システムに関する意見、要望を受付すること。
※振り分け基準はシステムデータ内でユーザ情報に関する件で職員側での判断を要する修正作業等は担当職員へ、その他はサポートデスク対応
- C 各種登録作業（職員情報、会議予約の管理権限の更新、会議室、共通マスタの登録等）
- i データ更新作業
職員情報について職員の採用時の新規登録作業及び人事異動に伴う登録変更削除作業が正常に実施されていることを確認すること。（平日、毎日）
 - ii 管理機能の設定運用作業
 - ・アプリケーションのメニュー設定やロール設定
 - ・ユーザのアクセスセキュリティ設定
 - ・共通マスタ(組織名、役職名)設定
 - ・クライアント証明書の発行設定
 - ・ファイル共有のアクセスセキュリティ設定
 - ・会議室予約にかかる以下の作業を当機構担当者の依頼のもと行うこと。
 - 会議室の登録、更新、削除
 - 会議室予約の管理権限（更新、削除権限）のユーザ設定
 - 会議室のアクセスセキュリティ設定
 - 会議室予約情報の削除
 - ・職員間情報共有システム 監査ログの保管作業
- D サービス管理
- i 対象サービスの機能変更、メンテナンス情報等を収集し、必要に応じて利用者へ周知すること。
 - ii 1年に1回アカウントの棚卸し（要、不要の精査等）を行い、適正な設定をおこなうこと。
- E サーバ稼働状況確認（ハードウェア、仮想環境、OS、アプリケーション）
- i サーバの稼働状態（電源 ON/OFF の状態）を確認し、電源が投入されていない等、ネットワーク上から確認できないサーバがあった場合は、ネットワークの接続状態を確認の上、状況を当機構担当者に報告するとともに、障害復旧作業を行うこと。
 - ii 監視サーバにより他のサーバの CPU 使用率、ディスク使用率、メモリ使用率、ネットワーク等のリソース状況を監視し、異常な負荷・通信を示しているサーバを発見した場合にはその原因を究明、排除、あるいは改善し、当機構担当者に報告すること。
 - iii 監視サーバにより他のサーバの CPU 使用率、ディスク使用率、メモリ使用

- 率、ネットワーク等のリソース情報を定期的に収集し、収集した情報をもとに、仮想サーバのサイジングの見直し、最適化、傾向分析を行うこと。
- iv 監視サーバ上で Nagios、MRTG、NetFlow アナライザ、NIRVANA など、すでに構築されている監視ソフトを稼働させ、サーバの稼働状態を常時モニターすること。
 - v 監視は Nagios を使用し、マルチベンダ環境を監視できるよう随時設定の追加、見直しを行うこと。(監視プラグインの自作・改修を含む)
 - vi 用意された監視機構が無くとも、技術的に可能であればこれを内製し、Nagios へ監視統合を実施すること。
 - vii 情報システムグループ管理外の機器であっても必要に応じて監視を検討・実施すること。
 - viii ストレージ監視
 - ・ディスクの使用量を監視し、使用量が一定量を越えている場合には、原因を分析し、当機構担当者に報告すること。
 - ・サーバ等のストレージ障害を検知した場合は、障害状態を分析し、当機構担当者に報告すること。
 - ix 通信ポート監視
 - ・サーバ又は管理端末で不要ポート及びサービスの稼働状態を監視し、不要ポート及びサービスが起動している機器を発見した場合は速やかに当機構担当者に報告し、サービス停止等の作業を実施すること。
 - x OS・ソフト等の状態監視
 - ・サーバから、障害情報が通知された場合は、障害情報を分析して当機構担当者及びシステム開発元に報告の上、速やかな復旧作業を行うこと。
 - ・サーバでのディレクトリサービスシステムのアプリケーション単位で性能情報(CPU使用率、メモリ使用量等)の異常情報が発見又は通知された場合は、当機構担当者及びシステム開発元に報告すること。
 - ・障害で調査を要する場合、又は、当機構担当者から障害調査を依頼された場合は、サーバ等にリモートログインして、障害情報を取得・分析し、復旧作業を行うこと。
- F サーバの障害対応(一次切り分けまで)
- i トラブル発生時には、サービスの確認、機器の Status 確認、ログ確認等迅速な障害の切り分け、原因究明を行うと共に、その復旧に必要な処置又は業者との対応を迅速に行うこと。
復旧が困難な場合は、速やかに仮想サーバのロールバックや正常なバックアップ・スナップショットイメージからのクローン等を活用し運用を開始すること。バックアップ機がある場合には切替えを行うこと。
また、トラブルにともなう利用者への影響について、利用者へ内容の周知を行うこと。

- 運用開始時にセキュリティの課題を提示し、四半期(3 か月)ごとに対策及び実施報告を行うこと。
- ii トラブルへの対処については、当機構担当者と協議の上、作業を行うものとし、終了時には報告すると共に問題点を検討・分析し、今後の改善事項にフィードバックさせること。トラブル報告書の作成、トラブルの履歴情報を管理すること。
 - iii トラブルの原因が機器のソフトウェアにある場合は、当機構担当者と協議の上、ソフトウェアのバージョンアップを行うこと。
- G ウィルス定義ファイルの確認、更新作業
- 対象機器のウィルス定義パターンファイルが最新であることを確認する最新版でない場合は更新をすること。回数の上限は設定しない（無制限）。セキュリティの観点から（原則）リリースされたらただちにアップデートを行うこと。利用者への情報公開、周知等を行うこと。
- H サーバのバックアップ
- i データのバックアップ計画を策定し、当機構担当者の承認を受けたのちに実行すること。なお、スナップショットについては1日1回以上、月に1回以上はテープにバックアップすること。
 - ii テープは4世代以上バックアップすること。バックアップが計画どおりに行われていない場合は、速やかに原因を分析し、解決すること。
- I サーバのリストア
- i 仮想ディスク上のファイルシステムが破損し、復旧できない場合は、バックアップデータを基にリストアを行うこと。データ量次第ではあるが、原則翌営業日以内に復旧できるように努めること。
 - ii 当機構担当者からリストアの要求があった場合は、リストアを行うこと。データ量次第ではあるが、原則翌営業日以内に対応できるように努めること。
- J 監視項目見直し等による設定変更
- 監視項目の見直しやセキュリティ対策等により、監視ツールや OS 設定の変更を行うこと。
- K クライアント端末のサービス接続検証
- 職員間情報共有システムの機能変更や、クライアントアプリケーションの機能変更、更新および対応 OS が変更となった際には、職員間情報共有システムに接続して動作検証を行い、利用マニュアル等の更新を行うこと。
- L 停電等の対応
- i 計画停電等の前に、停電復旧時にサーバを自動起動する設定を確認、設定されていない場合は設定をすること。停電時にサーバを自動シャットダウンする設定を行うこと。
- M サーバシステム構成図の維持管理
- 基幹スイッチ、ルータから各サーバ、ストレージ、アプライアンスまでの接続

図を維持すること。ネットワークの構成に変更があった場合は、遅滞無く書類を修正して情報システムグループに提出すること。

N サーバ管理表の維持管理

各サーバ、ストレージ、アプライアンスの機種、機器名、シリアル番号、購入時期、保守等の情報が管理されている表を維持すること。ネットワーク構成に変更があった場合や機器交換があった場合等、遅滞無く書類を修正して提出すること。

O 日常業務解説書の維持管理

- i 本契約に基づいて実施する日々の日常業務内容を第三者でも分かるように記した日常業務解説書を維持すること。
- ii 日常業務内容に変化があった場合、遅滞なく書類を修正して提出すること。

P 利用マニュアルの維持管理

- i 一般利用者を対象とした、各サーバの利用方法に関するマニュアルを維持し、当機構内イントラ Web サーバを用いて公開すること。
- ii 利用方法に変更があった場合は遅滞なくマニュアルを修正すること。

Q FAQ の維持管理

- i 利用者あるいは当機構担当者から問い合わせがあった場合は、問い合わせ内容を調査し、必要な支援を行うとともに、問い合わせ内容とその回答を、「よくある質問とその答え (FAQ)」として Web サーバに登録し、Web ブラウザで閲覧可能とすること。
- ii 契約前に存在していた FAQ を含めて、登録済内容のメンテナンスを行うこと。
- iii 問い合わせ内容については履歴管理を行うこと。

R 個別アプリケーションの全体管理

職員間情報共有システムの機能を、部署等の内部利用に提供する個別アプリケーションについて、システム設定および権限等の全体管理を行う。なお、各機能上のコンテンツ作成・管理は含まない。

- i 個別アプリケーションの対象は以下である。
 - ・ポータル
 - ・ワークフロー
 - ・掲示板
 - ・マルチレポート
 - ・タイムカード
- ii 個別アプリケーションの利用申請を受付し、希望部署等に対して機能提供を行うこと。なお、部署等の組織単位への提供を基本とし個人への提供については当機構担当者と協議の上、実施すること。
- iii 個別アプリケーションのシステム設定、カテゴリ設定、管理を行うこと。
- iv カテゴリ内のアクセス権設定、運用管理者権限設定、管理を行うこと。

v 1年に1回、希望部署、担当者の棚卸し（要、不要の精査等）を行い、適正な設定を行うこと。

S ワークフローの申請フォーム管理

管理部署等の依頼に基づきワークフロー申請フォームのシステム設定変更を行う。なお、申請フォームの新規作成およびプログラム開発を伴う変更は含まない。

i ワークフロー申請フォームの画面構成変更を行うこと。

ii ワークフロー申請の承認ルート変更を行うこと。

iii 利用者からの申請、承認方法に関する問い合わせ対応を行うこと。なお、申請内容に関する問い合わせは含まない。

iv 2020年4月時点のワークフロー申請フォーム数は68申請を予定している

v 下記Tにおいて移行作業を行った申請フォームについても管理対象とする

vi 管理する申請フォーム数が大幅に増加する場合、当機構担当者との協議を行うこと。

T ワークフロー申請フォーム作成

当機構担当者の依頼に基づき、職員間情報共有システムのワークフロー申請フォーム画面や経路設定等の作成を行うこと。なお、職員間情報共有システムの標準機能内で申請フォームの作成を行い、JavaScript等のプログラム開発を伴う作業は含まない。対象申請数は50程度を目安とし、数量が大幅に増減する場合は当機構担当者との協議を行うこと。

i ワークフローの申請フォーム画面構成の標準化、カテゴリ設計等の全体設計をおこなうこと。

ii 依頼に基づきカテゴリ作成および申請公開範囲の設定を行うこと。

iii ワークフローの申請フォーム画面、承認ルートを作成し業務担当者の承認を受けること。

iv 利用者、承認者向けのマニュアルを作成すること。

v 現行の申請手続きからの移行計画を作成し業務担当者へ確認の上、移行を実施すること。

キ 成果管理公開システム

(ア) 概要

成果管理公開システムについて、安定運用ならびに迅速・適切な運用支援を行うことを目的とする。

(イ) 対象機器

A 物理サーバ：3式

B 仮想サーバ：7式

C アプリケーション：Webサービス、データベース、成果管理アプリケーション、ウイルス対策等

注) 2020年4月1日の時点では、機器リプレース、OSバージョンアップにより変更されて

いる可能性もある。またこれらの各機器は随時変更することがあり、その都度、必要な対応を行うこと。(新機器設置作業や動作確認等)

(ウ) 業務内容

A 問い合わせ対応

- i 問合せ対応 (電話・メール)

B 各種登録作業(職員情報、組織情報、ロール情報等の登録、共通マスタの登録等)

- i 職員情報、組織情報、ロール情報について職員の採用時の新規登録作業及び人事異動に伴う登録変更作業を行うこと(平日、毎日)。
- ii 役職情報、プロジェクト情報の共通マスタの登録を行うこと(平日、情報更新時)。
- iii 組織変更時の登録変更作業を行うこと。

C データ確認及び抽出作業

- i ユーザ登録データの照合/確認、公開、照会・修正、削除、振替を行うこと。また、不明点等あれば、当機構職員にデータ内容を確認すること。
- ii 研究成果に掲載するデータや、評価用に利用するデータの抽出を毎月1回行い、当機構職員に提出すること。
- iii 当機構職員の依頼に基づき、登録されている発表情報の検索やデータの抽出を行い、当機構職員に提出すること。

D 利用者への周知

- i 当機構職員の依頼に基づき、学術文献引用データ関連の更新情報を、当機構内イントラ Web ページに掲載すること。

E 文書類似度判定ツールの維持管理

- i ユーザ情報等の登録や削除作業を行うこと。
- ii 登録されているユーザ数や論文数の確認を行い、当機構職員へ報告すること。

F リソース管理

仮想マシンの CPU、メモリ、ディスク等のリソースの払い出し状況を管理表で管理すること。

G サーバ稼働状況確認(ハードウェア、OS)

- i サーバの稼働状態(電源 ON/OFF の状態)を確認し、電源が投入されていない等、ネットワーク上から確認できないサーバがあった場合は、ネットワークの接続状態を確認の上、状況を当機構担当者に報告すること。
- ii 監視サーバにより他のサーバの CPU 使用率、ディスク使用率、メモリ使用率、ネットワーク等のリソース状況を監視し、異常な負荷・通信を示しているサーバを発見した場合には、当機構担当者に報告すること。
- iii 監視サーバにより他のサーバの CPU 使用率、ディスク使用率、メモリ使用率、ネットワーク等のリソース情報を定期的に収集し、収集した情報をもとに、仮想サーバのサイジングの見直し、最適化、傾向分析を行うこと。

- iv 監視サーバ上で Nagios、MRTG、NetFlow アナライザ、NIRVANA など、すでに構築されている監視ソフトを稼動させ、サーバの稼動状態を常時モニターすること。
- v 監視は Nagios を使用し、マルチベンダ環境を監視できるよう随時設定の追加、見直しを行うこと。(監視プラグインの自作・改修を含む)
- vi 用意された監視機構が無くとも、技術的に可能であればこれを内製し、Nagios へ監視統合を実施すること。
- vii 情報システムグループ管理外の機器であっても必要に応じて監視を検討・実施すること。
- viii ストレージ監視
 - ・ハードディスク・SSD 等 (外付けディスクアレイを含む) の使用量を監視し、ハードディスク・SSD 等の使用量が一定量を越えている場合には、原因を分析し、当機構担当者に報告すること。
 - ・サーバ等のストレージ障害を検知した場合は、当機構担当者に報告すること。また、メーカーへの連絡、修理対象品の梱包作業等を行うこと。
- ix 通信ポート監視
 - ・サーバ又は管理端末で不要ポート及びサービスの稼動状態を監視し、不要ポート及びサービスが起動している機器を発見した場合は速やかに当機構担当者に報告し、サービス停止等の作業を実施すること。
- x OS・ソフト等の状態監視
 - ・サーバから、障害情報が通知された場合は、当機構担当者に報告の上、システム障害時対応手順書に基づき、復旧作業を行うこと。
 - ・障害で調査を要する場合、又は、当機構担当者から障害調査を依頼された場合は、サーバ等にリモートログインして、障害情報を取得・分析を行うこと。
- xi ソフトウェア障害監視
 - ・サーバから基本ソフトウェアや、他のインストールソフトウェアからの警告等の障害情報が通知された場合は、障害情報を分析して当機構担当者に報告の上、システム障害時対応手順書に基づき、復旧作業を行うこと。
- H サーバ証明書の更新
 - i サーバ証明書の有効期限を確認し、継続して利用ができるように、CSR の生成、当機構担当者へのサーバ証明書更新の依頼、証明書の受け取り、証明書のインストールを行う。
- I ウィルス定義ファイルの確認、更新作業
 - i 対象機器のウィルス定義パターンファイルが最新であることを確認する最新版でない場合は更新をすること。回数の上限は設定しない (無制限)。
 - ii セキュリティの観点から (原則) リリースされたら適宜アップデートを行うこと。

- J サーバの障害対応（一次切り分けまで）
トラブル発生時には、サービスの確認、機器の **Status** 確認、ログ確認等を行うと共に、システム障害時対応手順書に基づき、復旧作業を行うこと。また、トラブルにともなう利用者への影響について、利用者へ内容の周知を行うこと。
- K 項目見直し等による設定変更
監視項目の見直しやセキュリティ対策等により、監視ツールや OS 設定の変更を行うこと。
- L サーバシステム設計書の維持管理
- i 各サーバの設計書を維持すること。
 - ii サーバの構成に変更があった場合は、遅滞無く書類を修正して提出すること。
- M サーバシステム構成図の維持管理
- i 基幹スイッチ、ルータから各サーバ、ストレージ、アプライアンスまでの接続図を維持すること。ネットワークの構成に変更があった場合は、遅滞無く書類を修正して情報システムグループに提出すること。
- N サーバ管理表の維持管理
- i 各サーバ、ストレージ、アプライアンスの機種、機器名、シリアル番号、購入時期、保守等の情報が管理されている表を維持すること。
 - ii ネットワーク構成に変更があった場合や機器交換があった場合等、遅滞無く書類を修正して提出すること。
- O システム障害時対応手順書の維持管理
- i 発生が予想される障害に対し、具体的にどのような手順でシステムを復旧するかを記した障害時対応手順書を維持すること。
 - ii 予想される障害に変化があった場合、あるいは、手順の見直しを行った場合は、遅滞なく書類を修正して提出すること。
- P 日常業務解説書の維持管理
- i 本契約に基づいて実施する日々の日常業務内容を第三者でも分かるように記した日常業務解説書を維持すること。
 - ii 日常業務内容に変化があった場合、遅滞なく書類を修正して提出すること。
- Q 利用マニュアルの維持管理
- i 一般利用者を対象とした、各サーバの利用方法に関するマニュアルを維持し、当機構内イントラ Web サーバを用いて公開すること。
 - ii 利用方法に変更があった場合は遅滞なくマニュアルを修正すること。
- R FAQ の維持管理
- i 利用者あるいは当機構担当者から問い合わせがあった場合は、問い合わせ内容を調査し、必要な支援を行うとともに、問い合わせ内容とその回答を、「よくある質問とその答え (FAQ)」として Web サーバに登録し、Web ブラウザで閲覧可能とすること。

- ii 契約前に存在していた FAQ を含めて、登録済内容のメンテナンスを行うこと。
- iii 問い合わせ内容については履歴管理を行うこと。

ク 資産管理システム

(ア) 概要

資産管理システムについて、安定運用ならびに迅速・適切な運用支援を行うことを目的とする

(イ) 対象機器

仮想サーバ：1 式

(ウ) 業務内容

A 問い合わせ対応

- i 電話・メール
- ii 資産管理システムに関する意見、改善要望の受付

B 各種登録作業

- i 職員情報、組織情報、ロール情報について職員の採用時の新規登録作業及び人事異動に伴う登録変更の自動同期の正常性を確認すること。(平日、毎日)。自動同期に問題が発生した場合は、原因確認の上、手動にて登録対応を行うこと。
- ii 組織情報・プロジェクトコード(組織マスタ)の登録を行うこと(平日、情報更新時)

C 利用者への周知

- i サーバやプログラムのメンテナンス等がある場合、当機構担当者の指示に従い利用者への周知を行うこと。

D サーバ稼働状況確認

1. サーバの稼働状態(電源 ON/OFF の状態)を確認し、電源が投入されていない等、ネットワーク上から確認できないサーバがあった場合は、ネットワークの接続状態を確認の上、状況を当機構担当者およびシステム開発元に報告するとともに、可能な限り障害復旧作業を行うこと。
- ii 監視サーバにより他のサーバの CPU 使用率、ディスク使用率、メモリ使用率、ネットワーク等のリソース状況を監視し、異常な負荷・通信を示しているサーバを発見した場合にはその原因を究明、排除、あるいは改善し、当機構担当者に報告すること。
- iii 監視サーバにより他のサーバの CPU 使用率、ディスク使用率、メモリ使用率、ネットワーク等のリソース情報を定期的に収集し、収集した情報をもとに、仮想サーバのサイジングの見直し、最適化、傾向分析を行うこと。
- iv 監視サーバ上で Nagios、MRTG、NetFlow アナライザ、NIRVANA など、すでに構築されている監視ソフトを稼働させ、サーバの稼働状態を常時モニター

- すること。
- v 監視はNagiosを使用し、マルチベンダ環境を監視できるよう随時設定の追加、見直しを行うこと。(監視プラグインの自作・改修を含む)
- vi 用意された監視機構が無くとも、技術的に可能であればこれを内製し、Nagiosへ監視統合を実施すること。
- vii 情報システムグループ管理外の機器であっても必要に応じて監視を検討・実施すること。
- viii ストレージ監視
 - ・ディスクの使用量を監視し、使用量が一定量を越えている場合には、原因を分析し、当機構担当者に報告すること。
 - ・サーバ等のストレージ障害を検知した場合は、障害状態を分析し、当機構担当者に報告すること。
- ix 通信ポート監視
 - ・サーバ又は管理端末で不要ポート及びサービスの稼動状態を監視し、不要ポート及びサービスが起動している機器を発見した場合は速やかに当機構担当者に報告し、サービス停止等の作業を実施すること。
- x OS・ソフト等の状態監視
 - ・サーバから、障害情報が通知された場合は、障害情報を分析して当機構担当者及びシステム開発元に報告の上、速やかな復旧作業を行うこと。
 - ・サーバでのディレクトリサービスシステムのアプリケーション単位で性能情報(CPU使用率、メモリ使用量等)の異常情報が発見又は通知された場合は、当機構担当者及びシステム開発元に報告すること。
 - ・障害で調査を要する場合、又は、当機構担当者から障害調査を依頼された場合は、サーバ等にリモートログインして、障害情報を取得・分析し、復旧作業を行うこと。
- E 障害対応(一次切り分けまで)
 - i トラブル発生時には、サービスの確認、機器の**Status**確認、ログ確認等迅速な障害の切り分け、原因究明を行うと共に、その復旧に必要な処置又はシステム開発元との対応を迅速に行うこと。
 - ii 復旧が困難な場合は、速やかに仮想サーバのロールバックや正常なバックアップ・スナップショットイメージからのクローン等を活用し運用を開始すること。バックアップ機がある場合には切替えを行うこと。
 - iii また、トラブルにともなう利用者への影響について、利用者へ内容の周知を行うこと。
 - iv 運用開始時にセキュリティの課題を提示し、四半期(3か月)ごとに対策及び実施報告を行うこと。
- F サーバ証明書の更新
 - i サーバ証明書の有効期限を確認し、継続して利用ができるように、CSRの生成、

当機構担当者へのサーバ証明書更新の依頼、証明書の受け取り、証明書のインストールを行う。

G ウィルス定義ファイルの確認、更新作業

- i 対象機器のウィルス定義パターンファイルが最新であることを確認する最新版でない場合は更新をすること。回数の上限は設定しない（無制限）。
- ii セキュリティの観点から（原則）リリースされたらただちにアップデートを行うこと。必要時には利用者への情報公開、周知等を行うこと。

H サーバのバックアップ

- i データのバックアップ計画を策定し、当機構担当者の承認を受けたのちに実行すること。なお、スナップショットについては1日1回以上、月に1回以上はテープにバックアップすること。
- ii テープは4世代以上バックアップすること。バックアップが計画どおりに行われていない場合は、速やかに原因を分析し、解決すること。

I サーバのリストア

仮想ディスク上のファイルシステムが破損し、復旧できない場合は、バックアップデータを基にリストアを行うこと。可能な限り早急に復旧できるように努めること。

ケ 安否確認システム

(ア) 概要

安否確認システムについて、安定運用ならびに迅速・適切な運用支援を行うことを目的とする。

(イ) 対象機器

本システムは、クラウド型アプリケーションサービスの提供を受けているため、ハードウェア等については運用対象外とする。

(ウ) 業務内容

A 問い合わせ対応（質問の振り分け）

- i 問合せ対応（電話・メール）
- ii 安否確認システムに関する意見、要望の受付

B 利用者への周知

サーバの停止、利用方法の変更、安否確認訓練等安否確認システム利用者に影響のあると思われる内容については、当機構担当者の指示に従い利用者への周知を行うこと。

C 各種登録作業（職員情報の登録、ユーザリストの作成、分類）

- i 職員情報について職員の採用時の新規登録作業及び人事異動に伴う登録変更作業を行うこと。（平日、毎日）
- ii 必要に応じユーザリストの作成と分類を行うこと（エクセル作業）

D 安否確認訓練の対応支援（年2回程度）

安否確認訓練の対応の事前準備、打ち合わせ、リハーサル、訓練の実施を行うこ

と。

E Windows、Mac 等最新クライアント OS、Web ブラウザの維持管理作業

- i 当該システムの対応調査、問い合わせ。
- ii 導入業者からの利用マニュアルの入手、利用者向けの案内 Web ページの作成、FAQ 作成、更新。

コ TV 会議システム

(ア) 概要

当機構で保持する TV 会議システムすべてに対しての、運用管理、保守、ユーザーサポートを行い、ネットワークトラブルを未然に防止するとともに、常に良好な状態を保つための運用管理や保守、トラブル対応を行うことを目的とする。

(イ) 対象機器

TV 会議端末：60 式（地方拠点含む）、MCU：2 式、管理サーバ：2 式

注) 2020 年 4 月 1 日の時点では、機器リプレース、OS バージョンアップにより変更されている可能性もある。またこれらの各機器は随時変更することがあり、その都度、必要な対応を行うこと。（新機器設置作業や動作確認等）

(ウ) 業務内容

A コンサルティング

i TV 会議更改計画の策定

当機構担当者と協議の上、TV 会議の更改、改善、構成変更の計画を作成すること。2020 年 4 月 1 日の時点では以下の作業を予定している。予定は随時変更することがあり、その都度必要な対応を行うこと。

- ・予約申請フロー、予約 Web ページの見直し
- ・MCU の更改

ii TV 会議の性能調査及び評価、改善検討

TV 会議の音声、映像に問題がある場合、問題ごとに状況と原因について調査し、改善のための提案を行い、当機構担当者と協議の上、必要に応じて改善を行うこと。

iii TV 会議システムの構成変更・追加の検討

当機構担当者と協議の上、必要に応じて構成機器選定、機器設定、機器交換（性能不足・老朽化対応）について、機能、信頼性、整合性を調査し、技術的提案を行うこと。

B 問い合わせ対応

i 問合せ対応（電話・メール）

TV 会議システム、会議室の使い方等の質問などの受付、回答をすること。

ii TV 会議システムに関する意見、要望の受付

- C システム利用予約運用
 - i メールで申し込まれる申請について対応し、Web ページの利用予約状況を更新すること。
 - ii 予約状況に合わせて会議室設備の空きを確認し、予約が重複しないように対応すること
- D 編集、録画対応
 - 利用者から会議の録画及び、録画した映像の編集の要望があった場合に対応すること。
- E 設置機材貸出及び設置、接続など支援
 - TV 会議装置を設置する要望があった場合に設置、接続を行うこと。
(月 2 台程度の設置及び取り外しが行われる)
- F オンサイト対応 (機材の貸出、現地対応、遠隔出張等)
 - 会議の開催に伴う機材の貸出、設置等の外勤場所、出張場所へのオンサイト対応を行うこと。
- G MCU 運用
 - i MCU を利用した、会議開催作業を行うこと。
 - ii MCU が正常に動作していることを確認すること。
 - iii MCU ステータス操作、ログの分析、設定を行うこと。
 - iv メンテナンス時に必要に応じてサーバの起動、停止を行うこと。
 - v 当機構担当者の指示のもと、OS バージョンアップ、パッチ適用を行うこと。
- H 会議室運用
 - i 会議室設備として、音響装置、プロジェクタの操作を行うこと。
 - ii 障害時には各機器を調査し必要な対応を行うこと。
 - iii 会議室設備の機器管理台帳を管理すること。
 - iv 当機構担当者の指示のもと、ファームウェアアップデートを行うこと。
- I 開催会議対応
 - i 開催会議の監視を行い、正常に通信できていることを確認すること。
 - ii 会議開催時には会場の設定、疎通の確認、機器操作を行うこと。
- J TV 会議端末運用
 - i 各機器が正常に動作していることを確認すること。
 - ii 機器の故障の際は保守ベンダに問合せを行い速やかに交換すること。
 - iii TV 会議システムの台数や付属品を管理すること。
- K 講演会などのイベント開催時における TV 会議関連設備の運営支援業務
 - i 必要に応じ、講演会などイベントに関する打ち合わせに参加すること。
 - ii 情報システムグループの機材に関する貸出を行う。
 - iii 講演会などイベント開催時における、TV 会議システムおよび会場の音声・映像テストを行うこと。
 - iv 必要に応じ、固定カメラによるイベントの録画を行うこと。

- v 必要に応じ、会議室内における音声・映像機器のレイアウト変更や、音声・映像機器ケーブルの簡易な敷設を行うこと。
重要性の高いイベントに関しては TV 会議開催時の現地対応支援、重点監視を行うこと。

L 当機構外（海外含む）会議システムとの接続対応

当機構外（海外含む）会議システムとの接続の要望があった場合に対応すること。

M 機器稼働状況確認

- i TV 会議システム、管理サーバの稼働状態（電源 ON/OFF の状態）を確認し、電源が投入されていない等、ネットワーク上から確認できないサーバがあった場合は、ネットワークの接続状態を確認の上、状況を当機構担当者に報告するとともに、障害復旧作業を行うこと。
- ii 監視サーバにより管理サーバの CPU 使用率、ディスク使用率、メモリ使用率、ネットワーク等のリソース状況を監視し、異常な負荷・通信を示しているサーバを発見した場合にはその原因を究明、排除、あるいは改善し、当機構担当者に報告すること。
- iii 監視サーバ上で Nagios、MRTG、NetFlow アナライザ、NIRVANA など、すでに構築されている監視ソフトを稼働させ、管理サーバの稼働状態を常時モニターすること。
- iv 監視は Nagios を使用し、マルチベンダ環境を監視できるよう随時設定の追加、見直しを行うこと。（監視プラグインの自作・改修を含む）
- v 用意された監視機構が無くとも、技術的に可能であればこれを内製し、Nagios へ監視統合を実施すること。
- vi 情報システムグループ管理外の機器であっても必要に応じて監視を検討・実施すること。
- vii 無停電電源装置監視
 - ・無停電電源装置からの警告等の障害情報が通知された場合は、障害情報を分析して当機構担当者に報告すること。また、メーカーに連絡し、協力して、速やかに復旧作業を行うこと。
 - ・JEMA-MIB 又は RFC 1628 に対応した機器の選定と、監視を行うこと。
- viii OS・ソフト等の状態監視
 - ・管理サーバから、障害情報が通知された場合は、障害情報を分析して当機構担当者及びシステム開発元に報告の上、速やかな復旧作業を行うこと。
 - ・サーバでのディレクトリサービスシステムのアプリケーション単位で性能情報（CPU 使用率、メモリ使用量等）の異常情報が発見又は通知された場合は、当機構担当者及びシステム開発元に報告すること。
 - ・障害で調査を要する場合、又は、当機構担当者から障害調査を依頼された場合は、サーバ等にリモートログインして、障害情報を取得・分析し、復旧作

業を行うこと。

N 障害対応（一次切り分けまで）

- i トラブル発生時には、サービスの確認、機器の Status 確認、ログ確認等迅速な障害の切り分け、原因究明を行うと共に、その復旧に必要な処置又は業者との対応を迅速に行うこと。

復旧が困難な場合は、速やかに代替のサーバ機器を予備品から用意し運用を開始すること。バックアップ機がある場合には切替えを行うこと。

また、トラブルにともなう利用者への影響について、利用者へ内容の周知を行うこと。

運用開始時にセキュリティの課題を提示し、四半期(3 か月)ごとに対策及び実施報告を行うこと。

- ii トラブルへの対処については、当機構担当者と協議の上、作業を行うものとし、終了時には報告すると共に問題点を検討・分析し、今後の改善事項にフィードバックさせること。トラブル報告書の作成、トラブルの履歴情報を管理すること。

トラブルの原因が機器のソフトウェアにある場合は、当機構担当者と協議の上、ソフトウェアのバージョンアップを行うこと。

O TV 会議端末のファームウェア、パッチ、ホットフィックスの適用

- i ソフトウェア提供元からパッチやホットフィックス等が提供された場合は、予備機あるいは検証機で動作確認を行った上で、パッチやホットフィックスの適用を行うこと。
- ii メールサーバ、プロキシサーバ経由での悪意あるソフトウェアの侵入を防止するためソフトウェアのパッチ適用、対策ソフトウェアのパターン更新、利用者への情報公開等を行うこと。

P Windows、Mac 等最新クライアント OS の維持管理作業

- i 当該システムの対応調査、問い合わせ。
- ii 導入業者からの利用マニュアルの入手、利用者向けの案内 Web ページの作成、FAQ 作成、更新。

Q 停電等の対応

- i 計画停電等の前に、停電復旧時にサーバを自動起動する設定を確認、設定されていない場合は設定をすること。停電時にサーバを自動シャットダウンする設定を行うこと。
- ii オムロン製、APC 製等個別無停電電源装置 (UPS) の設定を行うこと。UPS に対応していない機器については、対応可能な範囲で安全にシャットダウンできる機構を内製すること。又はリモートでの電源投入に係る手順を作成すること。その際、システムが正常に機能するために一定の順序で起動しなければならない機器については、起動シーケンスを制御すること。

R システム設計書の維持管理

- i 各機器の設計書を維持すること。
 - ii 機器の構成に変更があった場合は、遅滞無く書類を修正して提出すること。
 - iii 設計書をもとに再構築できるレベル及び内容で設計書を作成すること。
 - iv 想定読者は、TV 会議の基礎的知識はあるが、SE 経験は無い者が対象。
- S システム構成図の維持管理
- 基幹スイッチ、ルータから各機器までの接続図を維持すること。ネットワークの構成に変更があった場合は、遅滞無く書類を修正して情報システムグループに提出すること。
- T 管理表の維持管理
- 各機種、機器名、シリアル番号、購入時期、保守等の情報が管理されている表を維持すること。ネットワーク構成に変更があった場合や機器交換があった場合等、遅滞無く書類を修正して提出すること。
- U システム障害時対応手順書の維持管理
- i 発生が予想される障害に対し、具体的にどのような手順でシステムを復旧するかを記した障害時対応書を維持すること。
 - ii 予想される障害に変化があった場合、あるいは、手順の見直しを行った場合は、遅滞なく書類を修正して提出すること。
- V 日常業務解説書の維持管理
- i 本契約に基づいて実施する日々の日常業務内容を第三者でも分かるように記した日常業務解説書を維持すること。
 - ii 日常業務内容に変化があった場合、遅滞なく書類を修正して提出すること。
- W 利用マニュアルの維持管理
- i 一般利用者を対象とした、各 TV 会議システムの利用方法に関するマニュアルを維持し、当機構内イントラ Web サーバを用いて公開すること。
 - ii 利用方法に変更があった場合は遅滞なくマニュアルを修正すること。
- X FAQ の維持管理
- i 利用者あるいは当機構担当者から問い合わせがあった場合は、問い合わせ内容を調査し、必要な支援を行うとともに、問い合わせ内容とその回答を、「よくある質問とその答え (FAQ)」として Web サーバに登録し、Web ブラウザで閲覧可能とすること。
 - ii 契約前に存在していた FAQ を含めて、登録済内容のメンテナンスを行うこと。
 - iii 問い合わせ内容については履歴管理を行うこと。

サ e ラーニングシステム

(ア) 概要

e ラーニングシステムについて、安定運用ならびに迅速・適切な運用支援を行うことを目的とする。

(イ) 対象機器

A 仮想サーバ：2式

B ソフトウェア構成：eラーニング用アプリケーション

注) 2020年4月1日の時点では、機器リプレース、OSバージョンアップにより変更されている可能性もある。またこれらの各機器は随時変更することがあり、その都度、必要な対応を行うこと。(新機器設置作業や動作確認等)

(ウ) 業務内容

A 問い合わせ対応 (質問の振り分け)

i 問合せ対応 (電話・メール)

ii eラーニングシステムに関する意見、要望の受付

B 各種アカウント登録作業 (職員情報、組織情報、ロール情報等の登録、共通マスタの登録等)

i 職員情報、組織情報、ロール情報について職員の採用時の新規登録作業及び人事異動に伴う登録変更の自動同期の正常性を確認すること。(平日、毎日)。自動同期に問題が発生した場合は、原因確認の上、手動にて登録対応を行うこと。

ii 役職情報、プロジェクト情報の共通マスタの登録を行うこと (平日、情報更新時)。

iii 組織変更時の登録変更作業を行うこと。

iv 自動同期された情報は、コース管理者に連絡をすること。

v 1年に1回アカウントの棚卸し (要、不要の精査等) を行い、適正な設定を行うこと。

vi 職員情報のID番号が変更になる場合、新しいID番号にアカウント情報の引き継ぎ作業を行うこと。

C 研修サイト設営、管理作業

i 研修サイトの設営にあたり、コース管理者と作業調整、打ち合わせ等を行い、研修サイトの設営支援を行うこと。

ii 研修サイトの設営作業を行うこと。サイト開設、研修コンテンツ/テストコンテンツ変換、サイト登録、サイト閉設までの対応を作業すること。研修サイトの設営は作業期間中に毎年25講座/50コース以内とする。

iii コース管理者に利用マニュアル提供、手順レクチャー等を行い、研修サイトの設営を支援すること。

iv コース管理者からの質問、障害に対する一次受付を行い、受け付けを行った質問・障害は、受け付けから解決までの対応状況を管理すること。

v FAQ 又は利用手引書で対応できない質問・障害は、システム開発元のサポートに調査及び対応依頼を行うこと。

D サーバ稼働状況確認 (仮想サーバ、OS)

i サーバの稼働状態 (電源 ON/OFF の状態) を確認し、電源が投入されてい

ない等、ネットワーク上から確認できないサーバがあった場合は、ネットワークの接続状態を確認の上、状況を当機構担当者に報告するとともに、障害復旧作業を行うこと。

- ii 監視サーバにより他のサーバの CPU 使用率、ディスク使用率、メモリ使用率、ネットワーク等のリソース状況を監視し、異常な負荷・通信を示しているサーバを発見した場合にはその原因を究明、排除、あるいは改善し、当機構担当者に報告すること。
- iii 監視サーバにより他のサーバの CPU 使用率、ディスク使用率、メモリ使用率、ネットワーク等のリソース情報を定期的に収集し、収集した情報をもとに、仮想サーバのサイジングの見直し、最適化、傾向分析を行うこと。
- iv 監視サーバ上で Nagios、MRTG、NetFlow アナライザ、NIRVANA など、すでに構築されている監視ソフトを稼働させ、サーバの稼働状態を常時モニターすること。
- v 監視は Nagios を使用し、マルチベンダ環境を監視できるよう随時設定の追加、見直しを行うこと。(監視プラグインの自作・改修を含む)
- vi 用意された監視機構が無くとも、技術的に可能であればこれを内製し、Nagios へ監視統合を実施すること。
- vii 情報システムグループ管理外の機器であっても必要に応じて監視を検討・実施すること。
- viii ストレージ監視
 - ・ディスクの使用量を監視し、使用量が一定量を越えている場合には、原因を分析し、当機構担当者に報告すること。
 - ・サーバ等のストレージ障害を検知した場合は、障害状態を分析し、当機構担当者に報告すること。
- ix 通信ポート監視
 - ・サーバ又は管理端末で不要ポート及びサービスの稼働状態を監視し、不要ポート及びサービスが起動している機器を発見した場合は速やかに当機構担当者に報告し、サービス停止等の作業を実施すること。
- x OS・ソフト等の状態監視
 - ・サーバから、障害情報が通知された場合は、障害情報を分析して当機構担当者及びシステム開発元に報告の上、速やかな復旧作業を行うこと。
 - ・サーバでのディレクトリサービスシステムのアプリケーション単位で性能情報 (CPU 使用率、メモリ使用量等) の異常情報が発見又は通知された場合は、当機構担当者及びシステム開発元に報告すること。
 - ・障害で調査を要する場合、又は、当機構担当者から障害調査を依頼された場合は、サーバ等にリモートログインして、障害情報を取得・分析し、復旧作業を行うこと。

E サーバの障害対応 (一次切り分けまで)

- i トラブル発生時には、サービスの確認、機器の Status 確認、ログ確認等迅速な障害の切り分け、原因究明を行うと共に、その復旧に必要な処置又は業者との対応を迅速に行うこと。

復旧が困難な場合は、速やかに仮想サーバのロールバックや正常なバックアップ・スナップショットイメージからのクローン等を活用し運用を開始すること。バックアップ機がある場合には切替えを行うこと。

また、トラブルにともなう利用者への影響について、利用者へ内容の周知を行うこと。

運用開始時にセキュリティの課題を提示し、四半期(3 か月)ごとに対策及び実施報告を行うこと。

- ii トラブルへの対処については、当機構担当者との協議の上、作業を行うものとし、終了時には報告すると共に問題点を検討・分析し、今後の改善事項にフィードバックさせること。トラブル報告書の作成、トラブルの履歴情報を管理すること。

トラブルの原因が機器のソフトウェアにある場合は、当機構担当者との協議の上、ソフトウェアのバージョンアップを行うこと。

F 基本ソフト、アプリケーションの管理、バージョンアップ

- i 基本ソフトのバージョンアップを行うこと。マイナーアップデートやパッチについては回数の上限は設定しない（無制限）。セキュリティの観点から（原則）毎月定例的にアップデートを行うこと。なお、作業にあたっては、年間計画を作成の上、当機構担当者の承認を受けてから作業すること。
- ii サーバ・クライアントシステムを運用する上で必要となるアプリケーションのインストール、バージョンアップを行い、バージョンや設定情報の管理をすること。バージョンアップについては回数の上限は設定しない（無制限）。

G パッチ、ホット FIX の適用

- i ソフトウェア提供元からパッチやホットフィックス等が提供された場合は、予備機あるいは検証機で動作確認を行った上で、パッチやホットフィックスの適用を行うこと。
- ii メールサーバ、プロキシサーバ経由での悪意あるソフトウェアの侵入を防止するためソフトウェアのパッチ適用、対策ソフトウェアのパターン更新、利用者への情報公開等を行うこと。

H サーバ証明書の更新

サーバ証明書の有効期限を確認し、継続して利用ができるように、CSR の生成、当機構担当者へのサーバ証明書更新の依頼、証明書の受け取り、証明書のインストールを行う。

I ウィルス定義ファイルの確認、更新作業

対象機器のウィルス定義パターンファイルが最新であることを確認する最新版でない場合は更新をすること。回数の上限は設定しない（無制限）。

セキュリティの観点から（原則）リリースされたらただちにアップデートを行うこと。利用者への情報公開、周知等を行うこと。

J サーバのバックアップ

- i データのバックアップ計画を策定し、当機構担当者の承認を受けたのちに実行すること。なお、スナップショットについては1日1回以上、月に1週間に1回以上はバックアップすること。
- ii テープは4世代以上バックアップすること。バックアップが計画どおりに行われていない場合は、速やかに原因を分析し、解決すること。

K サーバのリストア

- i 仮想ディスク上のファイルシステムが破損し、復旧できない場合は、バックアップデータを基にリストアを行うこと。データ量次第ではあるが、原則翌営業日以内に復旧できるように努めること。
- iii 当機構担当者からリストアの要求があった場合は、リストアを行うこと。データ量次第ではあるが、原則翌営業日以内に対応できるように努めること。

L Windows、Mac等最新クライアントOS、Webブラウザの維持管理作業

- i 当該システムの対応調査、問い合わせ。
- ii 導入業者からの利用マニュアルの入手、利用者向けの案内Webページの作成、FAQ作成、更新。

M 停電等の対応

- i 計画停電等の前に、停電復旧時にサーバを自動起動する設定を確認、設定されていない場合は設定をすること。停電時にサーバを自動シャットダウンする設定を行うこと。

N 監視項目見直し等による設定変更

監視項目の見直しやセキュリティ対策等により、監視ツールやOS設定の変更を行うこと。

O サーバシステム構成図の維持管理

基幹スイッチ、ルータから各サーバ、ストレージ、アプライアンスまでの接続図を維持すること。ネットワークの構成に変更があった場合は、遅滞無く書類を修正して情報システムグループに提出すること。

P サーバ管理表の維持管理

各サーバ、ストレージ、アプライアンスの機種、機器名、シリアル番号、購入時期、保守等の情報が管理されている表を維持すること。ネットワーク構成に変更があった場合や機器交換があった場合等、遅滞無く書類を修正して提出すること。

Q 日常業務解説書の維持管理

- i 本契約に基づいて実施する日々の日常業務内容を第三者でも分かるように記した日常業務解説書を維持すること。
- ii 日常業務内容に変化があった場合、遅滞無く書類を修正して提出すること。

- R 利用マニュアルの維持管理
 - i 一般利用者を対象とした、各サーバの利用方法に関するマニュアルを維持し、当機構内イントラ Web サーバを用いて公開すること。
 - ii 利用方法に変更があった場合は遅滞なくマニュアルを修正すること。
- S FAQ の維持管理
 - i 利用者あるいは当機構担当者から問い合わせがあった場合は、問い合わせ内容を調査し、必要な支援を行うとともに、問い合わせ内容とその回答を、「よくある質問とその答え (FAQ)」として Web サーバに登録し、Web ブラウザで閲覧可能とすること。
 - ii 契約前に存在していた FAQ を含めて、登録済内容のメンテナンスを行うこと。
 - iii 問い合わせ内容については履歴管理を行うこと。

シ Web/ビデオ会議サービス

(ア) 概要

Web/ビデオ会議サービスについて、安定運用ならびに迅速・適切な運用支援を行うことを目的とする。

(イ) 対象サービス：1 式

(ウ) 業務内容

A コンサルティング

Web/ビデオ会議サービスの当機構内での本格展開に向けて機能拡張、およびサービス提供範囲の拡大を検討、提案すること。機能拡張を行う場合は、必要に応じて機能評価、サービス展開にあたる運用方針の検討を行い、当機構担当者と協議すること。

B 問い合わせ対応

- i 問合せ対応（電話・メール）
Web/ビデオ会議サービスの使い方等の質問を受付、回答をすること。
- ii Web/ビデオ会議サービスに関する意見、要望を受付すること。

C システム利用予約運用

- i 利用者から申し込まれる申請を受付、Web/ビデオ会議の予約設定やアカウントの払い出しを実施すること。
- ii 予約状況に合わせて Web/ビデオ会議室の空きを確認し、予約が重複しないように利用者と調整すること。

D サービス不具合対応

Web/ビデオ会議サービスに関する不具合の一次受付、切り分けを行い、クラウドサービス業者に原因等を確認すること。

E 周知対応

Web/ビデオ会議サービスの不具合やサービスのメンテナンスの周知を行うこ

と。

F クライアント端末のサービス接続検証

Web/ビデオ会議サービスの機能変更や、クライアントアプリケーションの機能変更、更新および対応 OS が変更となった際には、Web/ビデオ会議サービスに接続して動作検証を行い、利用マニュアル等の更新を行うこと。

G 日常業務解説書の維持管理

- i 本契約に基づいて実施する日々の日常業務内容を第三者でも分かるように記した日常業務解説書を維持すること。
- ii 日常業務内容に変化があった場合、遅滞なく書類を修正して提出すること。

H 利用マニュアルの維持管理

- i 一般利用者を対象とした Web/ビデオ会議サービスの利用方法に関するマニュアルを維持し、当機構内イントラ Web サーバを用いて公開すること。
- ii 利用方法に変更があった場合は遅滞なくマニュアルを修正すること。

I FAQ の維持管理

- i 利用者あるいは当機構担当者から問い合わせがあった場合は、問い合わせ内容を調査し、必要な支援を行うとともに、問い合わせ内容とその回答を、「よくある質問とその答え (FAQ)」として Web サーバに登録し、Web ブラウザで閲覧可能とすること。
- ii 契約前に存在していた FAQ を含めて、登録済内容のメンテナンスを行うこと。
- iii 問い合わせ内容については履歴管理を行うこと。

ス MDM システム

(ア) 概要

MDM システムについて、安定運用ならびに迅速・適切な運用支援を行うことを目的とする。

(イ) 対象機器

本システムは、クラウド型アプリケーションサービスの提供を受けているため、ハードウェア等については運用対象外とする。

(ウ) 業務内容

A スマートフォン登録、削除作業

- i 支給スマートフォン、貸出スマートフォンの端末情報、利用者情報等の登録、削除作業及び人事異動に伴う登録変更作業を行うこと。
- ii 必要に応じユーザリストの作成と分類を行うこと (エクセル作業)。

B OS/ウイルス定義ファイルの更新周知

- i スマートフォン利用者に対して四半期に 1 回、OS/ウイルス定義の更新周

知を行うこと。また、MDM 上の端末情報を確認し未更新の利用者へ個別に更新依頼を行うこと。

- C スマートフォンの遠隔停止・遠隔削除作業
 - i スマートフォンの盗難、紛失等が発生した際は、当機構担当者の指示に従い該当端末の遠隔停止・遠隔削除作業を行うこと。
- D MDM システムのサービス提供情報収集
 - i MDM システムのサービス Web サイトを定期的に確認し、メンテナンス情報、システム対応情報の収集を行うこと。
- E iOS、Android 用の MDM エージェント維持管理作業
 - i MDM システムの対応状況により iOS、Android 端末にインストールされているエージェントの更新を行うこと。
- F 日常業務解説書の維持管理
 - i 本契約に基づいて実施する日々の日常業務内容を第三者でも分かるように記した日常業務解説書を維持すること。
 - ii 日常業務内容に変化があった場合、遅滞なく書類を修正して提出すること。
- G FAQ の維持管理
 - i 利用者あるいは当機構担当者から問い合わせがあった場合は、問い合わせ内容を調査し、必要な支援を行うとともに、問い合わせ内容とその回答を、「よくある質問とその答え (FAQ)」として Web サーバに登録し、Web ブラウザで閲覧可能とすること。
 - ii 登録済内容のメンテナンスを行うこと。
 - iii 問い合わせ内容については履歴管理を行うこと。

(6) 拠点システム運用サービス

ア 未来 ICT 研究所ネットワークシステム

(ア) 概要

未来 ICT 研究所の基幹ネットワーク、電子ジャーナルネットワーク、ゲストネットワーク、共用計算機の運用を行い、ネットワークトラブルを未然に防止するとともに、常に良好な状態を保つための保守作業、ネットワークや共用計算機の構成、各種サーバの運用状況についての現状調査、問題点の把握、未来 ICT 構内ネットワークセキュリティ対応を行うこと。

また、未来 ICT 研究所職員等から要望があった場合、ネットワークや計算機に関するユーザーサポートを行うこと。

各機器の保守作業は、本作業に含まないものとする。ただし、他受注者の保守作業時にはこれに立会い、保守状況などを管理し、各機器の状態を正確に把握すること。

(イ) 対象機器

未来 ICT 研究所内のネットワークに接続されている以下の計算機やスイッチ等と、その周辺機器を管理対象として、各種運用管理作業を行うこと。

A サーバ機器 (UNIX・Windows・その他)

物理サーバ	Windows Server CentOS	14 台
仮想サーバ	Windows Server RHEL7	6 台
アプライアンス		5 台

B クライアント計算機 (Windows)

C 電子ジャーナル計算機 (Windows)

D 展示室計算機 (Windows)

B-D の合計 48 台

E 各種ネットワーク機器

機種	台数
L2/L3 ネットワークスイッチ	39 台
無線アクセスポイント	42 台
VPN ルータ	3 台
IPS/IDS	1 台
メディアコンバータ、HUB 等	30 台

注) 2020 年 4 月 1 日の時点では、機器リプレース、OS バージョンアップにより変更されている可能性もある。またこれらの各機器は随時変更することがあり、その都度、必要な対応を行うこと。(新機器設置作業や動作確認等)

(ウ) 業務内容

A コンサルテーション

当機構担当者と協議の上、サーバ、ネットワークの更改、改善、構成変更の計画を、当機構内のネットワーク構成やシステム構成の全体最適をを考慮し作成すること。サーバ、ネットワークの構成変更、構成機器選定、機器設定、導入ソフトウェアの選定等について調査し、老朽化、保守サポート、性能等の問題があれば改善提案を、当機構内のネットワーク構成やシステム構成の全体最適を考慮し行うこと。

B 構築支援

サーバ、ネットワーク機器の新規導入及び機器更改等の設計、設定等の支援を行うこと。イベント用などの臨時ネットワークの設計と敷設支援を行うこと。ネットワークポロジ等の大規模な構成変更がある場合は、当機構担当者と協議の上、支援範囲を決定することとする。

C サーバ運用管理

i 性能調査及び評価

各サーバシステムの動作状況を定期的に調査・評価しメールにて報告すること。ボトルネックを解明し、性能向上のための提案を行うこと。

- ii 運用管理
各種サーバ（UNIX 系、Windows 系）の運用に必要なソフトウェアの他、バージョンアップ、パッチの適用等を行うこと。また、ウィルス定義ファイルの更新を行うこと。また、各サーバの運用方法等に変更がある場合は未来 ICT 研究所担当者と検討を行い、サーバの再構築作業等を行うこと。
 - iii 利用者管理
サーバに登録されている利用者情報（氏名、ユーザ ID、ホスト名、IP アドレス、メールアドレス等）の管理を行うこと。
 - iv 障害管理
サーバに障害が発生した場合には切り分け、原因究明、対処、復旧の対応をすること
 - v システムのバックアップ
サーバのシステム関連ファイル、ユーザーファイルその他必要と認められる物の定期的バックアップを行うこと。また、その自動化を行なうこと。
 - vi 運用計画
必要に応じて、各種サーバ運用計画についての提案を行うこと。
 - vii サーバ稼働状況の監視
機器を定期的に監視し報告すること。ログを採取し障害発生の予測に努めること。
- D クライアント計算機運用管理
- i 運用管理
クライアント計算機（Windows）の運用に必要なソフトウェアの他、必要に応じてバージョンアップ、パッチの適用等を行うこと。また、ウィルス定義ファイルの更新を行うこと。
 - ii 利用者管理
利用者情報（氏名、ユーザ ID、ホスト名、IP アドレス、Mac アドレス）の管理を行うこと。
 - iii 障害管理
クライアント計算機に障害が発生した場合には切り分け、原因究明、対処、復旧の対応をすること。
 - iv システムリカバリー
クライアント計算機障害時、早急に復旧が可能な仕組みを講ずること。
 - v 運用計画
必要に応じて、各種サーバ運用計画についての提案を行うこと。
- E 電子ジャーナル計算機・展示室計算機運用管理
- i 運用管理
計算機（Windows）の運用に必要なソフトウェアの他、必要に応じてバージョンアップ、パッチの適用等を行うこと。また、ウィルス定義ファイルの更新を行うこと。
 - ii システムリカバリー

計算機障害時、早急に復旧が可能な仕組みを講ずること。

iii 障害管理

計算機に障害が発生した場合には切り分け、原因究明、対処、復旧の対応をすること。

iv 運用計画

必要に応じて、各種サーバ運用計画についての提案を行うこと。

F ネットワーク運用管理

i ネットワークの構成管理

未来 ICT 研究所ネットワークに関して、機器構成や設置場所についてのベースライン文章の作成及び更新を行うこと。また、ネットワーク設定の変更時は、関係機関と連絡を取りながら速やかに構成変更を実施すること。

ii ネットワーク稼動状況の監視

未来 ICT 研究所ネットワークにおける機器を定期的に監視し報告すること。ログを採取し、障害発生の予測に努めること。

iii トラフィック情報の収集・分析

ネットワークのトラフィック情報を収集・分析して、問題がある場合は、改善のための提案を行うこと。

iv 障害管理

計算機に障害が発生した場合には切り分け、原因究明、対処、復旧の対応をすること。

v 運用計画

必要に応じて、ネットワーク運用計画についての提案を行うこと。

vi スイッチ等の維持運用

- ・コアスイッチの維持運用を行うこと。
- ・各建物内 L2 及び L3 スイッチ、無線アクセスポイントの維持運用を行うこと。
- ・建物の各居室までの配線情報（パッチパネル、情報コンセント等）の管理を行うこと。
- ・建屋間の光配線情報（光ケーブル管路、パッチパネル等）の管理を行うこと。
- ・各機器に必要なコンフィグレーションは以下の内容を利用している。
IPv4 に対し IEEE802.1q (VLAN、VLANTrunk)、ルーティング (OSPF、RIP)、スパンニングツリー、冗長機能 (VRRP)、マルチキャスト、認証 VLAN について動作させている。

G ソフトウェア管理

i バージョン管理

ソフトウェアのインストール及びインストールされたソフトウェアのバージョンを管理し、必要に応じてバージョンアップ等を行うこと。

ii 情報収集

バグ情報等の情報収集を行い、バージョンアップ等必要な措置を講ずること。

- iii ライセンス管理
 - ネットワーク構成機器、サーバ機器のソフトウェアライセンス等を適正、厳格に管理し、管理資料を作成すること。
- H ネットワークトラフィック情報を収集、分析し問題がある場合は改善すること。
- I ドキュメントの維持管理
 - ネットワークシステム運用管理に係るドキュメント及びマニュアル類の維持、管理を行うこと。
- J ホームページ管理
 - 未来 ICT 研究所の外向けホームページ、内向けホームページの管理及び運用支援を行うこと。
- K メールングリスト管理
 - 未来 ICT 研究所関連メールングリストの運用管理を行うこと。
- L 無線 LAN 機器の管理及び無線 LAN 利用支援作業
 - i 未来 ICT 研究所にて設置している研究用・ゲスト用ネットワークの無線 LAN 機器の管理及びセキュリティ確保を行うこと。
 - ii 研究用ネットワークの無線 LAN への端末の接続支援を行うこと。
 - ゲスト用ネットワークの無線 LAN については、未来 ICT 研究所職員から要望があった場合、接続支援を行うこと。但し、外部者へ直接の接続支援は行わない。
- M TV 会議システム利用時の接続対応、運用支援
 - TV 会議システム利用時の接続対応、トラブル対応等の運用支援を行うこと。
- N その他、随時作業（必要に応じて行う作業）
 - i ネットワークウィルス感染時には至急、通信の遮断と的確な対応を行うこと。
 - ii 各種ネットワークシステム関連の周知事項について、未来 ICT 研究所内へメール等でアナウンスをすること。
 - iii 計算機室（作業場）の整理整頓や機器の配線確認、UPS の残量確認、新規機器を導入した場合の型番確認と設置作業等。
- O ネットワーク定期作業（月 1 回の定期作業）
 - i 月 1 回、「(イ)管理対象機器－E 各種ネットワーク機器」に示す機器で構成されているネットワークのメンテナンスを行うこと。
 - ii ネットワークシステムの状況調査・分析を行いトラブルの前兆をつかみトラブルを未然に防ぐ調査を行うこと。
 - iii トラブル発生時には、ネットワークの障害原因の診断、対策案の立案、回復、是正措置を迅速に行うこと。
 - iv 機器の故障が発生した場合は、メーカーなどへ送付して修理を行い予備機により正常運用の確保を行うこと。
 - v 必要に応じてネットワーク環境の改善提案を行うこと。
 - vi 必要に応じてファームウェア等のバージョンアップを行うこと。

- vii 新規機器導入や既存機器の設定変更等が発生した場合は、必要に応じて職員と共に対応を行うこと。

P 各種機器の保守作業

計算機運用管理対象機器の保守を必要に応じて行うこと。

- i 機器の故障が発生した場合はメーカー等へ修理の依頼を行うこと。また必要に応じて予備機により正常運用を確保すること。
- ii ネットワーク構成の現状調査、問題点を洗い出し、必要に応じてネットワーク環境等の改善提案を行うこと
- iii メーカーよりネットワーク機器等のファームウェア等の配布があった時には、予備機において動作検証を行い、問題が無い場合には当研究所担当者に確認をとったのちにファームウェア等のバージョンアップを行うこと

Q ユーザ支援作業（ユーザーサポート）

未来 ICT 研究所職員の計算機における、ネットワーク関連や計算機セットアップ、ソフト・ハードウェアインストール対応、各種設定や質問対応等の支援を行うこと

i 主に対象となる OS

支援対象となる主な OS : UNIX 系、Windows 系、Mac 系

ii 主なユーザ支援作業

- ・ユーザ使用の計算機トラブルの対応
- ・ネットワークや計算機に関連する設定や質問に対する対応
- ・サーバ構築や計算機のセットアップ作業等
- ・監視システム、入退室システムなどの支援
- ・ソフトインストール、ネットワーク設定や接続支援
- ・周辺機器やソフト購入の際のコンサルティング
- ・セキュリティ対応

イ 脳情報通信融合研究センター基幹システム

(ア) 概要

脳情報通信融合研究センター（以下「脳情報センター」という。）のネットワーク、サーバ類、計算機等の運用を行い、ネットワークトラブルを未然に防止するとともに、常に良好な状態を保つための保守作業、ネットワークや計算機の構成、各種サーバ等の運用状況についての現状調査、問題点の把握、構内ネットワークセキュリティ対応を行うこと。また、脳情報センター職員等から要望があった場合、ネットワークや計算機等に関するユーザーサポートを行うこと。

各機器の保守作業は、本作業に含まないものとする。ただし、他受注者の保守作業時にはこれに立会い、保守状況などを管理し、各機器の状態を正確に把握すること。

工事を伴わない配線作業、ネットワーク機器の設置及び調整に関する作業、マシンの移動などは本作業内で実施すること。

ネットワーク設定の変更時は、当機構本部との連絡を密に取り、速やかに構成変更を行う

こと。

(イ) 対象機器

脳情報センター内のネットワークに接続されている以下の計算機やスイッチ等と、その周辺機器を管理対象として、各種運用管理作業を行うこと。

A 管理対象機器

i ネットワークサーバ (UNIX・Windows・その他)

型番	OS	台数
物理サーバ	RHEL CentOS Windows Server 2012 VMware vSphere	58
仮想サーバ	CentOS Windows Server 208	2

ii クライアント計算機

型番	OS	役割	台数
各種	各種	ユーザ計算機	400

注) ユーザが使う計算機についてのサポート

iii 各種ネットワーク機器

機種	台数
L2/L3 スイッチ	32
光モジュール	1
認証・セキュリティアプライアンス装置	4
IP カメラ	3
ストレージ・NAS 装置	8
無停電電源装置	21

iv 無線 LAN 機器

機種	台数
無線 LAN コントローラ	1
無線 LAN アクセスポイント	30
無線 LAN 認証サーバ	1
PoE スイッチ	10

v 複合機プリンタ

機種	台数
----	----

複合機	3
-----	---

vi 大判プリンタ

機種	台数
大判プリンタ	2

vii 会議室 AV 設備

機種	台数
ビデオプロジェクター	2
ガラススクリーン	2
操作卓	1
8 入力 4 出力 DVI マトリクススイッチャー	1
1 入力 4 出力 デジタル分配器	3
電源制御ユニット	1
デジタルミキサ	1
タッチパネル	1
ビデオカメラ	1
有線マイク	2
ワイヤレスマイク (ハンド型/ピン型)	6
赤外線会議マイク	1 式
ブルーレイレコーダー/プレーヤー	2
MD/CD レコーダ/プレーヤー	2
正面スピーカ/天井スピーカ	8
天井カメラ	3
コンパクトライブスイッチャー	1
リモートカメラコントローラー	1
ブルーレイレコーダー	1
データプロジェクター	2
200 型電動スクリーン	1
150 型電動スクリーン	1
フレームシンクロナイザー	1
DVI 分配器	1
フレームシンクロナイザー	1
ビデオコンバーター	5
SDI 信号分配器	1
音声遅延装置	1
4 入力 1 出力 DVI スwitchャー	1

<u>DVI ツイストペアケーブル受信機</u>	<u>4</u>
<u>DVI ツイストペアケーブル送信機</u>	<u>4</u>
<u>音声アンバランスバランス変換機</u>	<u>1</u>
<u>音声バランスアンバランス変換機</u>	<u>1</u>
<u>マルチシグナル対応シームレススイッチャー</u>	<u>1</u>
<u>BR/DVD プレーヤー</u>	<u>1</u>
<u>BR レコーダー</u>	<u>1</u>
<u>7 インチ液晶テレビ</u>	<u>1</u>
<u>TV 会議システム</u>	<u>10</u>

注) 2020 年 4 月 1 日の時点では、機器リプレース、OS バージョンアップにより変更されている可能性もある。

またこれらの各機器は随時変更することがあり、その都度、必要な対応を行うこと。

(新機器設置作業や動作確認等)

B 管理対象ネットワーク

- i 研究用ネットワークの運用／管理（脳情報センターに敷設された当機構ネットワーク及び大阪大学学内ネットワーク）
- ii 支援系ネットワークの運用管理（VPN 回線設備等の保守）
- iii お客様ネットワークの運用管理
- iv ビル内大阪大学ネットワーク（脳研 ODINS）の運用管理支援
範囲は以下のとおりとする。
 - ・インシデント発生時、事象切り分けや報告・対応支援
 - ・セキュリティ教育やシステム改善の提案支援
 - ・設備の利用補助や TV 会議の運営支援
- v ユーザ環境支援における範囲は下記のとおりとする。
 - ・脳情報センター各室、外部共同研究機関来訪者のネットワーク接続（実験環境に限る）
 - ・脳情報センターにおいて JGN を利用する実験サポート対応

(ウ) 業務内容

A コンサルテーション

当機構担当者と協議の上、サーバ、ネットワークの更改、改善、構成変更の計画を、当機構内のネットワーク構成やシステム構成の全体最適を踏まえて作成すること。サーバ、ネットワークの構成変更、構成機器選定、機器設定、導入ソフトウェアの選定等について調査し、老朽化、保守サポート、性能等の問題があれば改善提案を、当機構内のネットワーク構成やシステム構成の全体最適を踏まえて行うこと。他拠点でのイベント参加時における IT システム、AV システムの機器構成、商品選定コンサルティングを行うこと。

B 構築支援

サーバ、ネットワーク機器の新規導入及び機器更改等の設計、設定等の支援を行うこ

と。ネットワークトポロジー等の大規模な構成変更がある場合は、当機構担当者と協議の上、支援範囲を決定することとする。

C ユーザサポート作業

i 新規ユーザの接続支援

脳情報センターに新規配属された職員及び研修生等の利用計算機の接続におけるユーザ環境の導入支援を行う。主な機器及び作業は以下のとおりである。

- ・ 計算機（Windows、Mac 等）の初期設定
- ・ 当機構購入計算機において申請が必要な場合は申請支援を行う。
- ・ 出向者、研修生が準備したパソコンは持込み申請支援を行う。
- ・ その他、脳情報センターにおいての利用申請が必要な場合は支援を行う。
- ・ 利用アプリケーションの導入支援（インストール及び調整）
- ・ 有線ネットワーク及び無線ネットワーク接続における支援を行う。

ii 既存ユーザの問い合わせ対応

脳情報センター内で計算機を利用しているユーザ環境に対してトラブル時の支援を行う。主な内容は以下のとおりである。

- ・ 計算機の動作不良（起動故障、ネットワーク接続）の対応
- ・ 当機構内部及びセンター内部のサービス用 Web コンテンツ利用時におけるトラブルの対応（小金井本部への問合せ等含む）
- ・ プリンタ利用時のトラブル対応
- ・ 計算機等の機器故障時のメーカー対応
- ・ 新規利用アプリケーションの導入支援（インストール及び調整）

iii 会議支援

- ・ 研究企画委員会、センター会議等の議題となるテーマのドキュメント作成支援を行うこと。

iv イベント等の暫定システム構築支援

- ・ シンポジウム等の開催に備えホスティングサイト等を利用して情報提供、参加受付、問い合わせを実現するシステムの構築・運用支援を行うこと。
- ・ ホスティングサイトを利用する際には、セキュリティ診断によるリスクマネジメントをサポートすること。

D ネットワーク運用管理

脳情報センター内に設置された各種機器について、運用管理等を行う。ネットワーク管理を行う上で必要な配線図等書類は、当機構担当者と協議し作成、維持管理を行うこと。

他の研究所、脳情報センター、観測施設との対応において当機構から依頼があった場合には出張対応すること。

i 当機構ネットワークとの接続

当機構ネットワークの利用に関する接続状態の確認及びネットワーク機器やサーバの接続対応を行う。

ii JGN ネットワーク利用時の対応

実験機器等を JGN ネットワークに接続するため、JGN への利用申請及びネットワーク機器の設定を行う。作業を実施するにあたり JGN 運用者との調整を行い接続すること。接続後はネットワーク監視を行い、接続断の場合は速やかに対応すること。

iii 大阪大学学内 LAN 利用時の対応

実験機器等を大阪大学学内ネットワークに接続するため、大阪大学ネットワーク担当者との調整を行い、ネットワーク機器の設定を行うこと。接続後はネットワーク監視を行い、接続断の場合は速やかに対応すること。

iv 支援系ネットワークの管理

支援系端末の設置および接続調整を行うこと。また、支援系ネットワーク運用のための VPN 装置の管理を行うこと。

v ケーブル敷設

当機構から指示があった場合には、サーバ室、実験室、居室内のネットワークの敷設を行うこと。ケーブル (UTP、光) については、当機構で用意する。スイッチ間及びサーバへのケーブルは、タグを付け必要な情報を記載すること。

vi ネットワークの障害対応

ネットワークに障害が発生した場合には切り分け、原因究明、対処、復旧の対応をすること。

E 無線 LAN 機器設置

無線 LAN 機器の設置においてはセキュリティに留意し、本部の指示に沿った設置および維持管理を行うこと。

認証等の適切な設定により外部利用者が不用意に利用してしまわないようにすること。

無線 LAN アクセスポイントの設置設定、無線 LAN 利用申請処理、証明書の発行処理、定期的なパスワード変更処理など、セキュリティ維持と利便性の両立した提案および設置作業を行うこと。

無線 LAN 利用者のユーザ管理を行い、退所者においては遅延なくアカウントを削除すること。

F サーバ運用管理

各種サーバ (UNIX 系, Windows 系) の運用に必要なソフトウェアの他、バージョンアップ、パッチの適用、バックアップ等を行うこと。また、ウィルス定義ファイルの更新を行うこと。また、各サーバの運用方法等に変更がある場合は脳情報センター担当者と検討を行い、サーバの再構築作業等を行うこと。必要に応じて、各種サーバ運用計画についての提案を行うこと。

サーバに障害が発生した場合には切り分け、原因究明、対処、復旧の対応をすること。

G 外部向け Web サーバ (cinet.jp)

サーバ運用管理に加え、コンテンツの修正に関して職員の方をサポートすること。簡易な修正を実施すること。コンテンツのバックアップを実施するシステムを構築し、

運用すること。当機構外とのメール送受信に関し、職員の方を技術的にサポートすること。

H 統合認証システム

サーバ運用管理に加え、利用者からのヘルプデスク業務、ユーザアカウントの登録から削除までを実施すること。統合認証システムのオペレーション作業を実施すること。利用者へ向けて技術的サポートを実施すること。

I TV 会議運用管理

- i 脳情報センターで開催される TV 会議の接続支援を行うこと。
- ii パソコン画面の転送や音声の調整を行うこと。
- iii 会議室における有線 LAN、無線 LAN の提供サポートを行うこと。
- iv 多地点中継の予約支援、事前接続確認を行うこと。
- v 理事会等の重要な会議に関しては、前日から接続確認および音質確認を行うこと。

J 脳情報センターにおけるセミナ・イベント開催時の運営サポート

- i 大会議室で利用される対象機器の利用支援を行うこと。
- ii パソコン画面の投影やマイク・スピーカーの音質調整を行うこと。
- iii トラブル発生に備え現地立ち合いを行うこと。
- iv 有線 NW、無線 NW、スクリーン、音響機器、TV 会議を使った遠隔地への中継支援を行うこと。
- v パソコン接続アダプターの準備を行うこと。
- vi イベント最中の機器利用支援、パソコン接続、DVD 再生、BR 録画、ロビー中継、天井カメラ切り替え支援などを行うこと。

K サーバ室の電源設備、空調設備の運用管理支援

- i 空調機器のローテーション運用支援を行うこと。
- ii 電源設備の空き状況の確認・回答、設備増設時の設計支援、工事立会などを行うこと。
- iii 保守業者の入室時の立ち合いなどを行うこと。

L 随時作業（必要に応じて行う作業）

- i セキュリティインシデント発生時には至急、通信の遮断と的確な対応を行うこと。
- ii トラブル発生時には、迅速な原因究明に努め、可能な限り対応すること。これには、業者対応も含まれる。また、トラブルについての履歴情報の管理を行うこと。
- iii その他必要に応じて本部と綿密な連絡を取り合い対処し、メールなどで広く報告すること。
- iv iv 情報セキュリティに関する調査依頼等があった場合は支援を行うこと。
- v v アプリケーションソフトの一括購入に伴う使用状況調査等があった場合は支援を行うこと。

ウ ユニバーサルコミュニケーション研究所（けいはんな）基幹システム

（ア）概要

ユニバーサルコミュニケーション研究所（けいはんな）（以下「ユニバーサル研究所」という。）のネットワークセキュリティ対応を行うこと、セキュリティインシデント発生の際には当機構の情報セキュリティ委員会事務局からのセキュリティ装置のログ提出、ログ解析等の依頼対応等を行うことを目的とする。

(イ) 対象機器

ユニバーサル研究所内の以下の機器を管理対象として、各種運用管理作業を行うこと。

A 管理対象機器、および管理対象機能

装置種別	台数
ファイアウォール/IPS 装置	2 台
ネットワーク認証システム	1 式

注) 2020 年 4 月 1 日の時点では、機器リプレースにより変更されている可能性もある。またこれらの各機器は随時変更することがあり、その都度、必要な対応を行うこと。（新機器設置作業や動作確認等）

(ウ) 業務内容

A 主な作業（日常的な作業）

- i システムの稼働監視、リソースやトラフィックの監視、不正接続の監視
 - ・FW 機器の稼働状況、リソースやトラフィックの状況・内容を監視し、傾向分析やログの相関分析等を行い、異常検知を行うこと。また、関連するログを適切に管理すること。
 - ・ネットワーク認証システム機器の稼働状況、およびユーザ PC の接続状況を監視し、組織ごとに決められたルールで PC が接続されているかなどをチェック、異常検知を行うこと。また、関連するログを適切に管理すること。

B 随時作業（必要に応じて行う作業）

- i システムオペレーション
 - FW 機器について、以下のシステムオペレーションを実施すること。
 - ・設定の棚卸
 - FW、IPS のセキュリティ装置の設定の棚卸を年 2 回以上行い、外部接続申請等の関連する資料の更新を行うこと。
- ii セキュリティオペレーション
 - IPS 機能について、以下のセキュリティオペレーションを実施すること。
 - ・IPS シグネチャチューニング
 - 新たな IPS シグネチャがリリースされた場合、シグネチャの有効/無効化を検討し、最適構成に設定すること。

- iii セキュリティインシデント対応
 - ・セキュリティインシデント発生時には情報の収集、分析、問題の特定、解析、対策案の検討、協議、(運用員に対する)被害拡大防止策の指示、対応の状況確認、報告等を行うこと。セキュリティインシデント発生後には各種証跡を分析し、発生源や影響範囲等の調査、外への影響や潜在的な危険性等を報告すること。
 - ・情報セキュリティ委員会事務局、当機構セキュリティ運用業務委託業者、本部セキュリティ担当からセキュリティインシデント発生に伴う緊急の初動対応依頼があった場合、管理対象機器にて遮断設定を実施する。
 - ・情報セキュリティ委員会事務局、当機構セキュリティ運用業務委託業者、本部セキュリティ担当から、セキュリティインシデント発生時に管理対象機器のログ調査を実施する。
- iv コンサルテーション、構築支援
 - ・更改、改善、構成変更の計画・提案
管理対象機器に関する構成変更、構成機器選定、機器設定、導入ソフトウェアの選定等について調査し、老朽化、保守サポート、性能等の問題があればユニバーサル研究所職員と協議の上、更改、改善、構成変更の計画・提案を行うこと。その際、ユニバーサル研究所内の関係者と連携し、ネットワーク構成やシステム構成の全体最適を踏まえて検討すること。
 - ・構築支援
ユニバーサル研究所職員と協議の上、管理対象機器に関する構築支援を行うこと。
- v トラブル対処
 - ・トラブル発生時には、速やかにトラブルの原因等を調査し、復旧対処を行い、今後同等のトラブルを防ぐための是正措置を講じること。また、履歴情報を管理すること。
- vi ユニバーサルコミュニケーション研究所の PC のネットワーク接続検査
 - ・通常検査
ネットワーク認証システムにより、ユニバーサル研究所内のネットワークに PC を接続している利用者(氏名、NICT-ID など)、対象端末(メーカー、型番、OS、MAC アドレス等)を定期的(3ヶ月に1回程度)にチェックすること。
 - ・企画室、および各研究室との連絡・調整
企画室、および研究室ごとに接続許可ルールや異常検知ルール、およびその連絡・対処方法を調整し、iNetSec システムに設定・運用すること。
- vii その他
 - ・ドキュメント管理
管理対象機器に関するドキュメントを最新化し、適切に運用管理すること。
 - ・資産管理
管理対象機器に関するハードウェアやソフトウェアの資産、備品などを適切に運用管理すること。

C ユニバーサル研究所ネットワーク委員会関連作業

- ・ユニバーサル研究所にて年 2 回程度開催されるネットワーク委員会及び必要に応じて組織されるワーキンググループにおいて、管理対象機器に関する項目について、必要に応じて各種報告を行うこと。

エ 鹿島宇宙技術センター基幹システム

(ア) 概要

鹿島宇宙技術センター（以下「鹿島センター」という。）のネットワーク、共用計算機の運用を行い、ネットワークトラブルを未然に防止するとともに、常に良好な状態を保つための保守作業、ネットワークや共用計算機の構成、各種計算機等の運用状況についての現状調査、問題点の把握、構内ネットワークセキュリティ対応を行うこと。

また、鹿島センター職員等から要望があった場合、ネットワークや計算機に関するユーザーサポートを行うこと。

(イ) 対象機器

鹿島センター内のネットワークに接続されている以下の計算機やスイッチ等と、その周辺機器を管理対象として、各種運用管理作業を行うこと。

装置種別	台数
ネットワークアプライアンス	1
L2/L3 スイッチ	13 (予備機含む)
無線 AP	9
UPS	3
VPN ルータ	2

注) 2020 年 4 月 1 日の時点では、機器リプレース、OS バージョンアップにより変更されている可能性もある。またこれらの各機器は随時変更することがあり、その都度、必要な対応を行うこと。(新機器設置作業や動作確認等)

(ウ) 業務内容

A 主な作業（日常的な作業）

- 各種ネットワークサーバの運用管理。(Web 等)
- 庁舎ネットワークパッチパネルの運用管理。
- ネットワーク接続機器やサーバ稼働状況等の監視を行う。また必要に応じてログを採取し、障害発生の予防を行う。
- ネットワークトラフィック情報を収集、分析し問題がある場合は改善する。

B 随時作業（必要に応じて行う作業）

- 各種機器やネットワーク上のトラブル対処をする。またトラブル発生時には、至急、トラブルの原因等を調査し、対策を行い、今後同等のトラブルを防ぐための是正措置を講じること。
- セキュリティの運用管理
 - サーバやネットワーク機器等におけるパッチの適用、バグフィックス、不正アク

セス監視、最新ネットセキュリティソフトウェアの更新（ファームウェアのアップデート等）を行うこと

- b ネットワークウイルス感染時には至急、通信の遮断と的確な対応を行うと共に、感染源と思われるユーザのクライアント PC やサーバ等に対するネットワーク設定、ハードウェア・ソフトウェアのインストール、トラブル対応に関する支援を行うこと。
- c ネットワーク構成図やパッチパネル構成図等のネットワーク運用管理に係るドキュメントを常に最新の状態に保つよう更新、修正を行うこと。
- iii 当機構鹿島ネットワーク委員会において当機構担当者から要望や相談等が寄せられた場合は、必要に応じて提案等の支援を行うこと。
- iv ケーブル交換で済む程度のネットワーク機器の修理等を行うこと。
- v 鹿島センターの外部・内部向けホームページのコンテンツ追加・削除等の更新作業及びコンテンツの新規作成作業（HTML, CSS, CGI 等の作成・編集を含む）を行うこと。なおコンテンツの内容については当機構担当者から指示する。
- vi ネットワーク、セキュリティ、ソフトウェア等の脆弱性や不具合に関する情報を収集し、当機構担当者へ報告すると共に、鹿島センター内へ周知等必要な措置を講じること。
- vii ネットワーク障害、セキュリティインシデントに関する問題が生じた場合、速やかに当機構担当者に報告するとともに危険性・重要度に応じて優先的に対応すること。
- viii 計算機室（作業場）の整理整頓や機器の配線確認、UPS の残量確認、新規機器を導入した場合の型番確と設置作業等を行うこと。

C 各種機器の保守作業

計算機運用管理対象機器の定期保守を行うこと。

- i 機器の故障が発生した場合はメーカー等へ送付し修理を依頼し、代替機により正常運用を確保すること。
- ii ネットワーク構成の現状調査、問題点を洗い出し、必要に応じてネットワーク環境等の改善提案を行うこと。
- iii メーカーよりネットワーク機器等のファームウェア等の配布があった時には、予備機において動作検証を行い、問題が無い場合には当機構担当者に確認をとったのちにファームウェア等のバージョンアップを行うこと。

D ユーザ支援作業（ユーザーサポート）

鹿島センター職員の計算機（各個別のユーザー計算機等）における、ネットワーク関連や計算機セットアップ、ソフトウェア・ハードウェアインストール対応、各種設定や質問対応等の支援を行うこと。

- i 主に対象となる OS 等
UNIX 系（Linux 含む）、Windows 系、Mac OS 系
- ii 主なユーザ支援作業

- a ユーザ使用の計算機トラブルの対応。
 - b ネットワークや計算機等に関連する設定や質問に対する対応。
 - c サーバ構築や計算機の改造作業等。
 - d ソフトウェアインストール、ネットワーク設定や接続支援。
 - e 周辺機器やソフト購入の際のコンサルティング。
 - f セキュリティ対応。
 - g ネットワーク機器購入、検討時の市場調査、仕様提案、価格調査等。
- E ユーザユーザ支援作業（ユーザーサポート）
鹿島センター関連のメーリングリストの運用管理を行うこと。
- F IP アドレス管理
鹿島センター関連で IP アドレスを取得している機器の棚卸及び維持管理を行うこと。

オ 耐災害 ICT 研究センター基幹システム

(ア) 概要

耐災害 ICT 研究センター（以下「耐災害センター」という。）のネットワーク、共用計算機の遠隔監視運用を行い、ネットワークトラブルを未然に防止するとともに、常に良好な状態を保つための保守作業、ネットワークや共用計算機の構成、各種サーバの運用状況についての現状調査、問題点の把握、構内ネットワークセキュリティ対応を行うこと。

(イ) 対象機器

耐災害センター内のネットワークに接続されている以下の計算機やスイッチ等と、その周辺機器を管理対象として、各種運用管理作業を行うこと。

装置種別	台数
L2/L3 スイッチ	14
無線 AP	15
UPS	2
VPN ルータ	3
ファイアウォール/UTM	2

注) 2020 年 4 月 1 日の時点では、機器リプレース、OS バージョンアップにより変更されている可能性もある。またこれらの各機器は随時変更することがあり、その都度、必要な対応を行うこと。

(ウ) 業務内容

- A 主な作業（日常的な作業）
各種ネットワークスイッチ、サーバの遠隔運用管理。
- B 随時作業（必要に応じて行う作業）
 - i 各種機器やネットワーク上のトラブル対処をする。またトラブル発生時には、至急、トラブルの原因等を調査し、対策を行い、今後同等のトラブルを防ぐための是正措置を講じること。
 - ii 最新ネットワークセキュリティの運用管理。

- a パッチの適用、バグフィックス、不正アクセス監視、最新ネットセキュリティソフトウェアの更新（ファームウェアのアップデート等）を行うこと
- b ネットワークウイルス感染時には至急、通信の遮断と的確な対応を行うこと。
- c ネットワーク構成図とパッチパネル構成図を常に最新の状態に保つよう更新作業をすること。

C 各種機器の保守作業

- i ネットワーク構成の現状調査、問題点を洗い出し、必要に応じてネットワーク環境等の改善提案を行うこと。
- ii メーカーよりネットワーク機器等のファームウェア等の配布があった時には、予備機において動作検証を行い、問題が無い場合には当機構担当者に確認をとったのちにファームウェア等のバージョンアップを行うこと。

カ ワイヤレスネットワーク総合研究センター基幹システム

(ア) 概要

ワイヤレスネットワーク総合研究センター（以下「ワイヤレスセンター」という）のネットワーク、共用計算機の遠隔監視運用を行い、ネットワークトラブルを未然に防止するとともに、常に良好な状態を保つための保守作業、ネットワークや共用計算機の構成、各種サーバの運用状況についての現状調査、問題点の把握、構内ネットワークセキュリティ対応を行うこと。

(イ) 対象機器

ワイヤレス研究所のネットワークに接続されている以下の計算機やスイッチ等と、その周辺機器を管理対象として、各種運用管理作業を行うこと。

機種	台数
L2/L3 スイッチ	7
スイッチング HUB	9
無線 AP	11
ルータ	2
サーバ	1

注) 2020年4月1日の時点では、機器リプレース、OSバージョンアップにより変更されている可能性もある。またこれらの各機器は随時変更することがあり、その都度、必要な対応を行うこと。（新機器設置作業や動作確認等）

(ウ) 業務内容

A ネットワーク運用管理作業

- i ネットワークに関連する機器構成のベースラインのドキュメント作成・更新・管理を行うこと。
- ii ルータ、スイッチ等ネットワーク稼働状況管理を行うこと。
- iii ネットワークトラフィック情報の収集・分析し、問題がある場合は改善のための提案を行うこと。

- B サーバ運用管理作業
 - i 共用サーバの動作状況を確認し、必要があれば調査・評価を行い報告すること
 - i
- C 運用管理マニュアルの更新、修正をすること。
 - i ネットワーク運用管理に係るドキュメントを更新、修正を行うこと。
 - ii 運用管理マニュアルの更新、修正を行うこと。
- D ユーザ環境支援
 - i コンピュータに関するユーザからの問い合わせに対応すること。
 - ii セキュリティインシデント及びネットワーク広域に影響を与える可能性がある事象が発生した場合、ユーザのクライアント PC に対するネットワーク設定、ハードウェア・ソフトウェアのインストール、トラブル対応に関する支援を行うこと。
- E その他
 - i ネットワーク、セキュリティ、ソフトウェア等の不具合に関する情報を収集し当機構担当者への報告・研究所内周知等必要な措置を講じること。
 - ii ネットワーク障害、セキュリティインシデントに関する問題が生じた場合、速やかに担当者に報告するとともに危険性・重要度に応じて優先的に対応すること。

(7) その他

- ア 予備品の管理
 - i. 予備品、保管品とした機器についても、必要ときに期待される性能が得られるよう整備点検を行うこと。
 - ii. 作業対象機器については当機構が指定する物品番号、機器のシリアル番号、使用場所、設定内容、周辺機器等の情報を整理して管理を行うこと。予備品、保管品も含めて管理すること。問題が生じた場合は速やかに当機構担当者へ報告すること。
 - iii. 作業対象機器に不具合が生じた場合は、保守業者との対応及び必要に応じ機器の業者への発送、業者からの受取について責任を持って対処すること。ただし、問題が生じた場合は速やかに当機構担当者へ報告すること。
 - iv. 障害が発生した場合、一次切り分けは受注者が行うこと。当機構は、マルチベンダで構成される機器を 1 システムとして維持運用を行っているため、対応すること。
 - v. 一次切り分け後、物品の故障であることが判明した場合は、保守業者への連絡、物品の梱包、発送準備を行うこと。
 - vi. 必要に応じネットワークケーブルの配線、光ケーブルの配線を行うこと。
 - vii. 機器の個数、各種ケーブルの個数、故障数など数値化が可能なものについては、運用開始時にすべての個数を集計し、四半期(3 か月)ごとに報告すること。

イ 電源管理

- i. 本部の計算機室（本館 2 階サーバ室及び本館地下 MDF 室）内電源分電盤から各ラックまでの電源系統図（ブレーカー系統、PDU、個別 UPS、テーブルタップの接続状態）及び各 PDU 又は各個別 UPS 等の出力口と各機器間（サーバやネットワーク機器など）の接続状態を管理すること。管理とは電圧等の測定・適正な電気の利用を含む。
- ii. 電源管理の構成に変更があった場合は、遅滞無く書類を修正して提出すること。
- iii. 事故停電時の復旧手順を明確化にすること。
- iv. 計画停電の規模に沿った停電対処計画、手順を作成すること。
- v. 本部の停電に備え、外部ユーザへのサービス継続性の対応について検討すること。
- vi. 電気室設置の UPS 装置（DL9350-403jL）2 台の運用管理、監視を行うこと。

ウ 作業内容管理ソフトウェアの管理・運用

- i. 作業内容に管理するソフトウェアを用意し、作業内容の進捗状況を当機構担当者が Web インタフェースで閲覧可能なようにすること。Web ページで閲覧可能とする機能を実現する専用のソフトウェアは受注者が用意すること（テキストエディタやフリーソフトの使用可）。
- ii. 作業に内容を管理するソフトウェアを用意し、作業内容の進捗状況を当機構担当者が Web インタフェースで閲覧可能なようにすること。Web ページで閲覧可能とする機能を実現する専用のソフトウェアは受注者が用意すること（テキストエディタやフリーソフトの使用可）。
- iii. 作業内容管理ソフトウェアは、次の条件を満たすこと。
- iv. 作業の進捗を管理するため、シーケンシャルに管理番号が発行されること。
- v. 作業の進捗を管理するため、対応状況（対応中、対応済等）が明確に表示できること。
- vi. 作業の種別（障害、要望、質問）を管理できること。
- vii. 障害、要望、質問の内容、対応状況、内容について、Web インタフェースにより登録（入力）できること。
- viii. 帳票印刷機能を有し、月例報告書として印刷できること。報告書には、管理番号、対応状況、発生日時、対応日、完了日、連絡者、対応者、作業内容、対応内容が印刷されること。
- ix. 当機構担当者以外の者が閲覧できないように、閲覧認証機能を設けること。

4. 情報セキュリティ対策

(1) 再請負

本調達に係る業務は、その全部又は一部を第三者に再請負により行わせる場合には、該当事業者名、作業内容・範囲等について、事前に当機構の承認を得ること。この場合、受注者は、当機構が受注者に求めるものと同水準の情報セキュリティを確保するための対策を契約に基づき再請負先に行わせること。

なお、再請負先に行わせた情報セキュリティ対策及びこれを行わせた結果に関する報告を、受注者に求めることがあるので、この場合はこれに応じること。

(2) 情報セキュリティ対策の履行が不十分である場合の対処

本調達に係る業務の遂行における情報セキュリティ対策の履行が不十分である可能性を当機構が認める場合には、受注者は、当機構の求めに応じ協議を行い、必要な対策を行うこと。

(3) 情報の保護

ア 本調達に係る業務を実施するために当機構から提供する情報については、十分な管理を行うこと。

イ 本業務を実施する上で取り扱うハードウェア及びソフトウェアについては、当機構の承認なく外部へ持ち出してはならない。

(4) 秘密の保持

ア 受注者は本調達に係る業務の遂行に際して、当機構が開示した情報（公知の情報等を除く。以下同じ。）及び業務遂行過程で生じた納入成果物に関する情報を本契約の目的以外に使用、又は第三者に開示、もしくは漏洩してはならないものとし、そのために必要な措置を講じること。

なお、当該情報等を本契約以外の目的に使用又は第三者に開示する必要がある場合には、事前に当機構の承認を得ること。

イ 受注者は本調達に係る業務の遂行に際して、当機構が貸与したプログラム及び資料は、滅失及び毀損のないよう取り扱うこととし、業務完了の都度、速やかに当機構に返却すること。

(5) 情報セキュリティ侵害時における対処

本調達に係る業務の遂行において、情報の漏えい、改ざん、消去等の事象及び情報セキュリティが侵害された場合（以下「情報セキュリティ侵害時」という。）に備え、事前に連絡体制を策定し、当機構の承認を得ること。また、情報セキュリティ侵害時又はそのおそれがある場合に備え、事前に実施すべき事項・手順等を策定し、当機構の承認を得ること。

(6) 守秘義務に関する誓約書

当機構との契約にあたり守秘義務に関する誓約書（別紙3）を提出すること。

5. 知的財産権等

- i. 本契約履行過程で生じた、著作権法第27条及び第28条に定める権利を含むすべての著作権及びノウハウ（営業秘密）は当機構に帰属し、当機構が独占的に使用するものとする。ただし、受注者は、本契約履行過程で生じた著作権又はノウハウ（営業秘密）を自ら又は第三者に行使させ

る場合は、当機構と別に定める使用契約を締結するものとする。なお、受注者は当機構に対し、一切の著作権者人格権を行使しないこととし、また第三者にも行使させないものとする。

- ii. 納入成果物に第三者が権利を有する著作物（以下「既存著作物」という。）が含まれている場合は、当機構が特に使用を指示した場合を除き、当該著作物の使用に必要な費用の負担及び使用承諾契約にかかわる一切の手続を行うこと。この場合、受注者は当該契約等の内容について事前に当機構の承諾を得ることとし当機構は既存著作物について当該許諾条件の範囲内で使用するものとする。
- iii. 本仕様書に基づく作業に関し、第三者との間に著作権にかかわる権利侵害の紛争等が生じた場合は、当該紛争の原因が専ら当機構の責めに帰す場合を除き、受注者の責任、負担において一切処理すること。この場合、当機構はかかわる紛争等の事実を知った時は受注者に通知し、必要な範囲で訴訟上の防衛を受注者にゆだねる等の協力措置を講ずるものとする。
- iv. 受注者は開発等にあたり、第三者の工業所有権又はノウハウ（営業秘密）を実施又は使用するときは、その実施又は使用に対する一切の責任を負うものとする。
- v. 本仕様書に基づく作業及び納入成果物に関し、第三者との間に工業所有権にかかわる権利侵害の紛争が生じた場合は、当該紛争の原因が専ら当機構の責めに帰す場合を除き、受注者の責任、負担において一切処理すること。この場合、当機構はかかわる紛争等の事実を知った時は、受注者に通知し、必要な範囲で訴訟上の防衛を受注者にゆだねる等の協力措置を講ずるものとする。

6. 作業場の留意点

(1) 作業安全計画

本件作業を行うに当たり、労働安全衛生法その他関係法規及び当機構の諸規則を遵守した作業安全計画書を作成し、当機構の承認を得ること。また、作業安全計画書の内容については、作業者全員に周知徹底を図ること。

(2) 事故防止

受注者が機器設定等の作業において、当機構内の作業場所を使用する場合、当機構に作業（工事）届を提出し、その承諾を受けなければならない。また、受注者は、常に工事場所を整理・整頓し、安全に留意して事故の防止に務めるとともに、労働基準法及び労働安全衛生法を遵守して安全の徹底を図らなければならない。

(3) 防火管理

受注者が各搬入場所において、当機構内の作業場所で火気を使用する場合又は作業に伴い騒音が発生する場合、当機構に火気使用・騒音発生に係る作業届を提出し、承諾を受けなければならない。

(4) 災害防止等の措置

受注者は、災害防止等のため、特に必要と認められるときは、臨機の措置をとるものとし、その措置模様を速やかに当機構情報システムグループ宛てに報告すること。

7. その他

作業員の役割、各作業における責任体制について明記した作業体制・責任体制図を契約締結後、速や

かに当機構情報システムグループ宛てに提出すること。

情報システムグループサポートデスク利用に関する満足度アンケート調査

〇〇〇〇年〇〇月〇〇日

情報システムグループサポートデスク利用に関する満足度アンケート調査

このアンケートは、情報システムグループサポートデスクについて、確保されるべきサービスの質を検討するため、職員利用者を対象に利用満足度を調査するものです。

つきましては、次の4つの質問に対して、それぞれ「満足」から「不満」までのいずれかに該当する□にレ印を記入してください。

お問合せから回答までに要した時間について満足されましたか。

満足 やや満足 普通 やや不満 不満

回答又は手順に対する説明の分かりやすさについて満足されましたか。

満足 やや満足 普通 やや不満 不満

回答又は手順に対する結果の正確性について満足されましたか。

満足 やや満足 普通 やや不満 不満

担当者の対応（言葉遣い、親切さ、丁寧さ等）について満足されましたか。

満足 やや満足 普通 やや不満 不満

< ご意見等 >

ご協力ありがとうございました。

情報システム運用のための総合サービス業務
総合評価基準書

国立研究開発法人情報通信研究機構

経営企画部 情報通信システム室 情報システムグループ

- 目 次 -

1	はじめに	3
2	評価基準	3
	(1) 評価点	3
	(2) 決定方法	3
	(3) 総合評価点	3
3	提出書類及び様式	5
4	提案書の提出	7
	(1) 提出期限	7
	(2) 提出場所	7
	(3) 提出部数	7
	(4) 提出方法	7
	(5) 照会先	7
	(6) その他	7

1 はじめに

本書は「2020 情報システム運用のための総合サービス業務」に関する評価基準を取りまとめた総合評価基準書である。

2 評価基準

(1) 評価点

総合評価は、価格点と技術点を合算した数値（以下「総合評価点」という。）をもって行う。

$$\text{総合評価点} = \text{価格点 (1,000 点満点)} + \text{技術点 (1,000 点満点)}$$

(2) 決定方法

ア 機能証明書にて、仕様書の全ての機能を満たしているものを「合格」とし、1つでも満たしていない場合は「不合格」とする。

イ 合否の判定により「合格」となった提案書に対して、総合評価点が最も高い者を落札者とする。

ウ 総合評価点が最も高い者が2者以上あるときは、当該入札者にくじを引かせて落札者を決定する。
この場合において、当該入札者のうち開札に立ち会わない者又はくじを引かない者があるときは、これに代えて当該入札執行事務に関係しない職員にくじを引かせるものとする。

(3) 総合評価点

ア 価格点

価格点は、入札価格を予定価格で除して得た値を1から減じて得た値に入札価格に対する得点配分を乗じて得た値とする。

$$\text{価格点} = (1 - \text{入札価格} \div \text{予定価格}) \times 1,000 \text{ 点}$$

イ 技術点

技術点の評価方法は以下のとおりとする。

(ア) 全ての仕様を満たし、「合格」したものに「基礎点」として100点を与える。

(イ) 「別紙 総合評価基準及び対応表」に示す各評価項目に対応した提案内容について評価を行い、提案内容の優劣について相対評価を行い、「加点」を与える。

(ウ) 配点は「別紙 総合評価基準及び対応表」で示す各評価項目に示すとおりとする。

(エ) 評価は以下の方針に基づき判断する。

- | |
|--------------------------------|
| ① 実現性が十分に担保されていると判断できるか。 |
| ② 提案者の実績や知見に基づく創意工夫が盛り込まれているか。 |
| ③ 提案者の提案に対し相対的に評価する |

(オ) 評価は以下の基準で行う。

評価基準	配点 (%)
優れている	100
やや優れている	80
標準的である	60
やや劣っている	40
劣っている	20
提案自体がないもの	0

(カ) ワークライフバランス等の推進状況

女性活躍推進法に基づく認定 (えるぼし認定企業) ※1	認定段階1 (5つの基準のうち○が1~2)	20点
	認定段階2 (5つの基準のうち○が3~4)	40点
	認定段階3 (5つの基準の全てが○)	50点
	行動計画 (※3)	10点
次世代育成支援対策推進法 に基づく認定 (くるみん認定企業・ プラチナくるみん認定企業)	くるみん	20点
	プラチナくるみん	40点
青少年の雇用の促進等に関する法律に基づく認定 (ユースエール認定企業)		40点

複数の認定等に該当する場合は、**最も配点が高い区分により評価**を行うものとする。

確認外国法人については、認定の要件に相当する基準を満たすと確認された認定と同等の評価点を配点する。

※1 労働時間等の働き方に係る基準は満たすことが必要。

※2 女性活躍推進法に基づく一般事業主行動計画の策定義務がない事業主（常時雇用する労働者の数が300人以下のもの）に限る（計画期間が満了していない行動計画を策定している場合のみ）。

(キ)「基礎点」と「加点」の合計点を「技術点」とする。

$$\text{技術点} = \text{基礎点 (100 点)} + \text{加点 (900 点)}$$

3 提出書類及び様式

提案者は以下の内容の提案書を提出すること。

ア 表紙記載事項

提案書の表紙には、以下の事項を明記すること。

(ア) 表題は「2020 情報システム運用のための総合サービス業務 提案書」とすること。

(イ) 提案者の住所、名称、代表者名及び社印

注：表紙以外の頁等において、提案者が特定できる情報（社名、略称、ロゴ等）を記載しないこと。

(ウ) 連絡担当者の所属、氏名及び電話番号

(エ) 提案書の提出日

イ 構成及び記載事項

(ア) 提案内容

提案内容は以下の構成とすること。また仕様書との対応が分かるように該当ページの右端に連番等を記述した索引シールを付けること。

添付資料を作成する場合は、資料番号、タイトル、提案書との対応を記載した一覧表を付けること。

A 提案骨子

B プロジェクト管理

C 情報セキュリティ対策

D 運用・保守

E その他・追加提案等

(イ) 加点項目提案書

加点項目に対しては、仕様書の提案書とは別に加点項目に対しての加点項目提案書を提出すること。

(ウ) 機能証明書

仕様書で求めている要件を満たしていることを証明すること。仕様書との対応が分かるように該当ページの右端に連番等を記述した索引シールを付けること。構成や設計等、提案書を用いて

証明する場合は、該当箇所の項番等が分かるようにすること。

(エ) ワークライフバランス等の推進状況

ワークライフバランスを推進する企業として、女性活躍推進法、次世代育成支援対策推進法若しくは青少年の雇用の促進等に関する法律に基づく認定又はこれらの認定の要件に相当する基準を満たしていることの確認を受けている場合は、それを証明する書類として以下の書類の写しを提出すること。

- ア 女性活躍推進法（平成 27 年法律第 64 号）に基づく認定（えるぼし認定）に関する「基準適合一般事業主認定通知書」
- イ 次世代育成支援対策推進法（平成 15 年法律第 120 号）に基づく認定（くるみん認定及びプラチナくるみん認定）に関する「基準適合一般事業主認定通知書」
- ウ 青少年の雇用の促進等に関する法律（昭和 45 年法律第 98 号）に基づく認定（ユースエール認定）に関する「基準適合一般事業主認定通知書」
- エ 女性活躍推進法に基づく「一般事業主行動計画策定届」
- オ 内閣府男女共同参画局長が発行する「ワーク・ライフ・バランス等推進企業認定等相当確認通知書」

ウ 書式

(ア) 日本語、A4 縦版横書き（ただし、図表などについては必要に応じて A3 縦版または横版を用いてもよい。）、上部余白 25 mm、下部余白 20 mm、左右余白 20 mm、ヘッダー部 15 mm、フッター部 17.5 mm とし、上質紙に 12 ポイント以上の文字で作成すること。原則として文書は Word で作成し、図表は Excel 又は PowerPoint で作成すること。

エ 項番

(ア) 項番の付番については、下記の基準に従うこと。項目を更に細分化する必要等から下記の付番以下のレベルが必要となった場合は、適宜追加設定すること。また、図表番号については、章内での一連番号とし、併せて図表題名を付すこと。

見出し種類	項番表示
見出し 1	1、2、3、・・・
見出し 2	(1)、(2)、(3)、・・・
見出し 3	ア、イ、ウ、・・・
見出し 4	(ア)、(イ)、(ウ)、・・・
見出し 5	A、B、C、・・・
見出し 6	(A)、(B)、(C)、・・・
見出し 7	a、b、c、・・・
見出し 8	(a)、(b)、(c)、・・・

4 提案書の提出

(1) 提出期限

2019年12月18日(水)12時

(郵送による場合は、必着のこと。)

(2) 提出場所

情報通信研究機構 財務部契約室 役務・工事契約グループ

(東京都小金井市貫井北町4-2-1 042-327-7444)

(3) 提出部数

ア 提案内容・加点項目対応表・機能証明書

書面3部、電子媒体(CD-ROM)1式

(4) 提出方法

提案書の提出は、直接持参又は郵便(書留郵便に限る。)とすること。

郵便の場合には、「2020 情報システム運用のための総合サービス業務 提案書在中」と朱書きすること。

(5) 照会先

提案書作成要領等配布物に関し、照会事項がある場合は、下記の照会先に電子メールにて照会を行うとともに、電話にて連絡すること。

情報通信研究機構 財務部契約室 役務・工事契約グループ

(東京都小金井市貫井北町4-2-1 042-327-7444)

Mail:tender@ml.nict.go.jp

(6) その他

ア 分かりやすい日本語で記述すること。

イ 必要に応じて確認及び追加資料の提出を求められることがあるので、提案者はその内容についての説明及び資料提出を行うこと。

ウ 応募に要する経費は、提案応募者の負担とする。

エ 応募された提案書は、返却しない。

オ 提出された提案書等は、当該調達選定のためだけに使用する。

「2020 情報システム運用のための総合サービス業務」総合評価基準表

(1) 必須条件(基礎点)

機能証明書にて、仕様書の全ての機能を満たしているものを「合格」とし、1つでも満たしていない場合は「不合格」とする。(配点 100 点)	合格又は不合格
---	---------

(2) 評価は以下の方針に基づき判断する。

- ① 実現性が十分に担保されていると判断できるか。
- ② 提案者の実績や知見に基づく創意工夫が盛り込まれているか。
- ③ 提案者の提案に対し相対的に評価する

(3) 採点方法

それぞれの評価区分(重要度)ごとに、以下の6段階の配点を行う。

評価基準	評価区分 (重要度)			
	大	中-大	中	小
(A) 優れている	100	75	50	25
(B) やや優れている	80	60	40	20
(C) 標準的である	60	45	30	15
(D) やや劣っている	40	30	20	10
(E) 劣っている	20	15	10	5
(F) 提案自体がないもの	0	0	0	0

(参考) 相対評価の例

- ア 応札者(甲、乙)の評価が、第1順位=甲、第2順位=乙の場合は、甲にB評価、乙にD評価を与える。
- イ 応札者(甲、乙、丙)の評価が、第1順位=甲、第2順位=乙、第3順位=丙の場合は、甲にB評価、乙にC評価、丙にD評価を与える。
- ウ 応札者(甲、乙、丙、丁)の評価が、第1順位=甲、乙、第2順位=丙、第3順位=丁の場合は、甲と乙にB評価、丙にC評価、丁にD評価を与える。
- エ 応札者(甲、乙、丙、丁)の評価が、第1順位=甲、第2順位=乙、第3順位=丙、第4順位=丁の場合は、甲にA評価、乙にB評価、丙にD評価、丁にE評価を与える。
- オ 応札者(甲、乙、丙、丁、戊)の評価が、第1順位=甲、第2順位=乙、第3順位=丙、第4順位=丁、第5順位=戊の場合は、甲にA評価、乙にB評価、丙にC評価、丁にD評価、戊にE評価を与える。
- カ 応札者が一社の場合、C評価を与える。

(4) 評価点数表

評価項目	点数 (満点)
必須条件 (基礎点)	100
加点	900
技術点合計	1,000

(5)常駐作業員評価

No	評価項目	評価観点	最大配点
1	コンサルテーション、設計、構築実績	常駐作業員の「サーバ、ネットワークのコンサルテーション、設計、構築実績」を評価する。 仕様書 3. (2). ウ. (ア)、(イ)、3. (3). ウ. (ア)、(イ)に記載の内容に基づき、評価提案をすること。	25
2	セキュリティ監視、ウィルス、マルウェア感染等のインシデント対応実績	常駐作業員の「セキュリティ監視、ウィルス、マルウェア感染等のインシデント対応実績」を評価する。 仕様書 3. (1). ウ. (ウ)～(エ)に記載の内容に基づき、評価提案をすること。	25
3	ルータ及びスイッチの構築・管理・運用実績	常駐作業員の「同一メーカ及び異種メーカ間両方でのルータ及びスイッチの提案、構築・管理・運用実績」を評価する。 仕様書 3. (2). イ に記載してある機器又は同等の機器に関して、評価提案をすること	25
4	FW などセキュリティ装置の構築・管理・運用実績	常駐作業員の「FW などセキュリティ装置 (UTM、IPS、IDS、WAF 等) の提案・構築・管理・運用実績」を評価する。 仕様書 3. (1). イ に記載してある機器又は同等の機器に関して、評価提案をすること	25
5	ネットワーク装置の提案・導入・運用管理実績	常駐作業員の「ロードバランサ装置、大規模無線 LAN、IPv6 の提案・導入・運用管理実績」を評価する。 仕様書 3. (2). イに記載してある機器に関して、評価提案をすること IPv6 運用に対する課題についての知見を記載すること	25
6	Solaris サーバの構築・管理・運用実績	常駐作業員の「Solaris (10, 11 SPARC, x86-64 両アーキテクチャ) サーバ (仮想化含む) の構築・管理・運用実績」を評価する。	25
7	Linux、BSD サーバの構築・管理・運用実績	常駐作業員の「Linux (Kernel 2. 6、3. x) サーバ (仮想化含む)、BSD 系 (OpenBSD、FreeBSD、NetBSD) サーバ (仮想化含む) の構築・管理・運用実績」を評価する。	25
8	Windows サーバ・クライアントの構築・管理・運用実績	常駐作業員の「Windows (2008R2、2012、2016、2019) サーバ (仮想化含む) の構築・管理・運用実績」を評価する。	25
9	MacOS クライアント、スマートフォン、タブレット端末等の導入・運用管理実績	常駐作業員の「MacOS クライアント、スマートフォン、タブレット端末等の導入・運用管理実績」を評価する。	25

No	評価項目	評価観点	最大配点
10	ストレージ装置、ファイルシステムの導入、運用管理実績	常駐作業者の「ストレージ装置（DSA、SAN、NAS）ファイルシステム（Linux LVM、ZFS など）の導入、運用管理実績」を評価する。	25
11	LDAP の認証連携導入・運用実績	常駐作業者の「LDAP の認証連携導入・運用実績」を評価する。	25
12	オープンソースによるインフラ提案・構築・運用実績	常駐作業者の「オープンソースソフトウェア（例：Apache、BIND、sendmail 等）用いたインフラの提案、構築、運用実績」を評価する。	25
13	インターネットインフラ構築・運用実績	常駐作業者の「インターネットインフラ（DNS、電子メール、Webサーバ等）の構築・運用実績」を評価する。	25
14	Web アプリケーション作成・改修・提言	常駐作業者の「要件に応じた Web アプリケーションを安全に作成・改修・提言した実績と経験」を評価する。	25
15	運用・監視・統計のプログラミングや可視化	常駐作業者の「軽量プログラミング言語等を使用しての大量の設定や検証、監視の仕組みを構築して、自動化を行った実績と経験」、「NetFlow や SNMP 等を用いてトラフィックを可視化した実績と経験」及び「ログの解析（可視化）、統計（自動化含む）の実績と経験」を評価する。	25
16	物理配線および、機器設置	常駐作業者の「メタルケーブル及び、光ファイバでの配線を行った実績と経験」「サーバ、ネットワーク機器等のラックや棚等への設置搭載及び撤去を行った実績と経験」を評価する。	25
17	クラウド型/Web サービスの活用	常駐作業者の「クラウド型サービスの導入や API を用いたシステム連携の導入・運用の実績と経験」を評価する	25
	小計		425

(6)請負会社評価

No	評価項目	評価観点	最大配点
1	作業者体制	<p>請負会社の「体制図（表）」をもとに、常駐者と後方支援を総合した体制や業務フロー内容」を評価する。</p> <p>評価観点は</p> <ul style="list-style-type: none"> ・プロジェクト管理責任者 <p>NICTと同登規模の組織に関する管理経験、また管理に必要な資格の保持、または同等の経験</p> <ul style="list-style-type: none"> ・ネットワーク担当者 ・サーバ担当者 ・セキュリティ担当者 ・サポートデスク担当者 <p>資格の保持、管理経験、または同等の経験保持者であることを評価する。</p> <p>(例)</p> <p>Cisco Certified Network Professional 工事担任者 AI/DD 総合種 マイクロソフト認定ソリューションエキスパート (MCSE) Linux 技術者認定試験 3 (LPIC3) VMware Certified Professional5 セキュリティスペシャリスト ITILv3</p> <p>評価にあたっては、会社内で保持している所有者の数では無く、常駐を予定する体制内での資格、経験の状況を提案すること。 また、補足として、請負会社での資格取得・経験に対する教育について説明すること。</p>	100
2	業務遂行能力	<p>業務開始日(4月1日)から業務を円滑に遂行できるよう、</p> <ul style="list-style-type: none"> ・引継ぎ ・定常業務 ・人事異動時(繁忙期) <p>について業務遂行能力を評価する。</p> <p>4月1日付の組織整備、人事異動に伴うアカウント新規、変更、削除やクライアント計算機のセットアップ作業については、相当数の</p>	100

No	評価項目	評価観点	最大配点
		<p>人員が必要と考えている。</p> <p>また、本部に他拠点を支援する体制を常時用意し、他拠点で何かあるときは支援をできるような業務計画を評価する。</p>	
3	情報システムの構築・運用能力	情報システム構築・運用に関する実施内容・提案内容を本契約と類似する構築・運用実績を踏まえて評価する。	75
4	提案能力 (コンサルテーション)	情報システム提案内容について、本契約と類似する提案実績等を踏まえて評価する。	50
5	セキュリティ対策・対応能力	<p>請負会社において以下の実績があることを評価する。</p> <p>評価観点</p> <ul style="list-style-type: none"> ・日本シーサート協議会に加盟した独自の CSIRT 組織を通じて、国内外との情報連携および、組織としてのセキュリティ情報把握体制が明確に確立しており、3年以上運用実績があること。 ・独自の CSIRT 組織を有しており、組織としてのセキュリティ情報把握体制が明確に確立しており、3年以上運用実績があること。 ・トラヒック及びログ分析ツール、Nagios、MRTG、NetFlow アナライザの3年以上運用実績があること。 <p>また、セキュリティ対策の提案、セキュリティインシデント対応の体制内容について評価する。</p>	100
6	ワークライフバランス、働き方改革等への取り組み	<p>請負会社におけるワークライフバランスや働き方改革への取り組みを評価する。</p> <p>評価観点</p> <ul style="list-style-type: none"> ・勤務日時を柔軟に設定可能な制度等の導入 ・リモートワークを推進・支援する制度・技術の取り組み等 ・国・各省庁・地方自治体等による上記取り組みに対する認定制度 (認定証の写し等を提出すること) 	50
	小計		475

「各評価項目毎に提案内容を作成すること」

別紙 加点項目提案書（例）

常駐作業員評価

1 ルータ及びスイッチの構築・管理・運用実績について以下の提案を行う。

仕様書に記載があるルータ等について弊社としての運用・構築実績は・・・

弊社では今回の運用業務に十分な要員を確保し・・・（別紙要員スキル表参照）

さらに、今回の運用業務に対し、弊社として常駐作業員の教育、サポート体制を・・・

2 FW などセキュリティ装置の構築・管理・運用実績

・・・

適合証明書

以下のとおり適合することを証明いたします。

入札件名： 2020 情報システム運用のための総合サービス業務
 日付： 年 月 日
 住所：
 社名：
 代表者氏名： 印
 担当者連絡先：

<必須要件>

	応札者の要件	資料 有無
1	仕様書の要求事項を全て満たしていること。	

<加点要件>

常駐作業員評価

No	評価項目	評価観点	資料 有無
1	コンサルテーション、設計、構築実績	常駐作業員の「サーバ、ネットワークのコンサルテーション、設計、構築実績」を評価する。 仕様書 3. (2). ウ. (ア)、(イ)、3. (3). ウ. (ア)、(イ)に記載の内容に基づき、評価提案をすること。	
2	セキュリティ監視、ウイルス、マルウェア感染等のインシデント対応実績	常駐作業員の「セキュリティ監視、ウイルス、マルウェア感染等のインシデント対応実績」を評価する。 仕様書 3. (1). ウ. (ウ)～(エ)に記載の内容に基づき、評価提案をすること。	
3	ルータ及びスイッチの構築・管理・運用実績	常駐作業員の「同一メーカー及び異種メーカー間両方でのルータ及びスイッチの提案、構築・管理・運用実績」を評価する。 仕様書 3. (2). イ に記載してある機器又は同等の機器に関して、評価提案をすること	
4	FW などセキュリティ装置の構築・管理・運用実績	常駐作業員の「FW などセキュリティ装置 (UTM、IPS、IDS、WAF 等) の提案・構築・管理・運用実績」を評価する。 仕様書 3. (1). イ に記載してある機器又は同等の機器に関して、評価提案をすること	
5	ネットワーク装置の提案・導入・運用管理実績	常駐作業員の「ロードバランサ装置、大規模無線 LAN、IPv6 の提案・導入・運用管理実績」を評価する。 仕様書 3. (2). イに記載してある機器に関して、評価提案をすること IPv6 運用に対する課題についての知見を記載すること	

6	Solaris サーバの構築・管理・運用実績	常駐作業者の「Solaris (10、11 SPARC、x86-64 両アーキテクチャ) サーバ (仮想化含む) の構築・管理・運用実績」を評価する。	
7	Linux、BSD サーバの構築・管理・運用実績	常駐作業者の「Linux (Kernel2.4、2.6、3.0) サーバ (仮想化含む)、BSD系 (OpenBSD、FreeBSD、NetBSD) サーバ (仮想化含む) の構築・管理・運用実績」を評価する。	
8	Windows サーバ・クライアントの構築・管理・運用実績	常駐作業者の「Windows (2008、2008R2、2012) サーバ (仮想化含む) の構築・管理・運用実績」を評価する。	
9	MacOS クライアント、スマートフォン、タブレット端末等の導入・運用管理実績	請負会社の「MacOS クライアント、スマートフォン、タブレット端末等の導入・運用管理実績」を評価する。	
10	ストレージ装置、ファイルシステムの導入、運用管理実績	常駐作業者の「ストレージ装置 (DSA、SAN、NAS) ファイルシステム (Linux LVM、ZFS など) の導入、運用管理実績」を評価する。	
11	LDAP の認証連携導入・運用実績	常駐作業者の「LDAP の認証連携導入・運用実績」を評価する。	
12	オープンソースによるインフラ提案・構築・運用実績	常駐作業者の「オープンソースソフトウェア (例: Apache、BIND、sendmail 等) 用いたインフラの提案、構築、運用実績」を評価する。	
13	インターネットインフラ構築・運用実績	常駐作業者の「インターネットインフラ (DNS、電子メール、Web サーバ等) の構築・運用実績」を評価する。	
14	Web アプリケーション作成・改修・提言	常駐作業者の「要件に応じた Web アプリケーションを安全に作成・改修・提言した実績と経験」を評価する。	
15	運用・監視・統計のプログラミングや可視化	常駐作業者の「軽量プログラミング言語等を使用しての大量の設定や検証、監視の仕組みを構築して、自動化を行った実績と経験」、「NetFlow や SNMP 等を用いてトラフィックを可視化した実績と経験」及び「ログの解析 (可視化)、統計 (自動化含む) の実績と経験」を評価する。	
16	物理配線および、機器設置	常駐作業者の「メタルケーブル及び、光ファイバでの配線を行った実績と経験」「サーバ、ネットワーク機器等のラックや棚等への設置搭載及び撤去を行った実績と経験」を評価する。	
17	クラウド型/Web サービスの活用	常駐作業者の「クラウド型サービスの導入や API を用いたシステム連携の導入・運用の実績と経験」を評価する	

請負会社評価

No	評価項目	評価観点	資料有無
1	作業体制	<p>請負会社の「体制図 (表) をもとに、常駐者と後方支援を総合した体制や業務フロー内容」を評価する。</p> <p>評価観点は</p> <ul style="list-style-type: none"> ・プロジェクト管理責任者 <p>NICT と同登規模の組織に関する管理経験、また管理に必要な資格の保持、または同等の経験</p>	

		<ul style="list-style-type: none"> ・ネットワーク担当者 ・サーバ担当者 ・セキュリティ担当者 ・サポートデスク担当者 <p>資格の保持、管理経験、または同等の経験保持者であることを評価する。</p> <p>(例)</p> <p>Cisco Certified Network Professional 工事担当者 AI/DD 総合種 マイクロソフト認定ソリューションエキスパート (MCSE) Linux 技術者認定試験 3 (LPIC3) VMware Certified Professional5 セキュリティスペシャリスト ITILv3</p> <p>評価にあたっては、会社内で保持している所有者の数では無く、常駐を予定する体制内での資格、経験の状況を提案すること。</p> <p>また、補足として、請負会社での資格取得・経験に対する教育について説明すること。</p>	
2	業務遂行能力	<p>業務開始日(4月1日)から業務を円滑に遂行できるよう、</p> <ul style="list-style-type: none"> ・引継ぎ ・定常業務基幹 ・人事異動時(繁忙期) <p>について業務遂行能力を評価する。</p> <p>4月1日付の組織整備、人事異動に伴うアカウント新規、変更、削除やクライアント計算機のセットアップ作業については、相当数の人員が必要と考えている。</p> <p>本部 25名以上</p> <p>未来 ICT 研究所、脳情報通信融合研究センター、ユニバーサルコミュニケーション研究所、鹿島宇宙技術センター、ワイヤレスネットワーク研究所からなる各所においては少なくとも定常時よりも1名以上の体制が確保可能なこと。</p> <p>また、本部に他拠点を支援する体制を常時用意し、他拠点で何かあるときは支援をできるような業務計画を評価する。</p>	
3	情報システムの構築・運用能力	<p>情報システム構築・運用に関する実施内容・提案内容を本契約と類似する構築・運用実績を踏まえて評価する。</p>	
4	提案能力(コンサルティング)	<p>情報システム提案内容について、本契約と類似する提案実績等を踏まえて評価する。</p>	

5	セキュリティ対策・対応能力	<p>請負会社において以下の実績があることを評価する。</p> <p>評価観点</p> <ul style="list-style-type: none"> ・日本シーサート協議会に加盟した独自の CSIRT 組織を通じて、国内外との情報連携および、組織としてのセキュリティ情報把握体制が明確に確立しており、3年以上運用実績があること。 ・独自の CSIRT 組織を有しており、組織としてのセキュリティ情報把握体制が明確に確立しており、3年以上運用実績があること。 ・トラフィック及びログ分析ツール、Nagios、MRTG、NetFlow アナライザの3年以上運用実績があること。 <p>また、セキュリティ対策の提案、セキュリティインシデント対応の体制内容について評価する。</p>	
6	ワーク・ライフ・バランス、働き方改革等への取り組み	<p>請負会社におけるワーク・ライフ・バランスや働き方改革への取り組みを評価する。</p> <p>評価観点</p> <ul style="list-style-type: none"> ・勤務日時を柔軟に設定可能な制度等の導入 ・リモートワークを推進・支援する制度・技術の取り組み等 ・国・各省庁・地方自治体等による上記取り組みに対する認定制度（認定証の写し等を提出すること） 	

注1:各項目について条件を満たしていることの証明資料及び付属説明資料(必要な解説資料)等を添付してください。

注2:当証明書の提出については、契約捺印者の印をもって捺印の上、提出してください。

注3:適合証明書等の内容により本請負契約の履行可能が認められない場合は、入開札の対象とならないので留意願います。

注4:総合評価方式の場合は、加点要件設定があります。合致している項目があるときは、証明資料及び付属説明資料(必要な解説資料)等を添付してください。

入札関係資料閲覧に関する誓約書

国立研究開発法人 情報通信研究機構
契約担当理事 殿

_____ (以下、「弊社」という。)は、この度、情報通信研究機構 (以下、「貴機構」という。)の行う「2020 情報システム運用のための総合サービス業務」の入札 (以下、「本入札」という。)に関する資料閲覧に関し、下記事項を誓約致します。

第1条 (守秘義務の誓約)

弊社は貴機構の許可なくして、社外はもちろん貴機構職員で本件に直接関与していない者に対しても、本入札に関し弊社が知り得たすべての事項・情報を開示、漏洩し、もしくは自ら使用しないことを約束致します。

第2条 (資料複写の禁止等)

弊社は、守秘義務を厳守するため、貴機構より本入札に関し、開示された資料一切の複写をしないことを約束し、貴機構より返還を要求された場合、これらの資料及びそのコピー並びにそれらに関する資料の一切を直ちに返還することを約束致します。

第3条 (入札後の守秘義務)

弊社は、貴機構において本入札が行われた後といえども、第1条記載の事項・情報を開示、漏洩もしくは使用しないことを約束いたします。

第4条 (守秘義務違反後の処置)

弊社は、貴機構とお約束した守秘義務に反した場合、貴機構が行う合法的処置を受けることを約束いたします。

年 月 日

住 所 _____

会 社 名 _____

代表者名 _____ 印 _____

守秘義務に関する誓約書（案）

国立研究開発法人 情報通信研究機構
契約担当理事 殿

_____（以下、「弊社」という。）は、この度、情報通信研究機構（以下、「貴機構」という。）の行う「2020 情報システム運用のための総合サービス業務）を実施するにあたり、下記事項を誓約致します。

第1条（守秘義務の誓約）

弊社は貴機構の許可なくして、社外はもちろん貴機構職員で本件に直接関与していない者に対しても、本入札に関し弊社が知り得たすべての事項・情報を開示、漏洩し、もしくは自ら使用しないことを約束致します。

第2条（資料の返還等）

弊社は、守秘義務を厳守するため、貴機構より本入札に関し、貸与された資料一切の保管を厳重に行うことを約束し、貴機構より返還を要求された場合、これらの資料及びそのコピー並びにそれらに関する資料の一切を直ちに返還することを約束致します。

第3条（請負業務後の守秘義務）

弊社は、貴機構において本請負業務が行われた後といえども、第1条記載の事項・情報を開示、漏洩もしくは使用しないことを約束いたします。

第4条（守秘義務違反後の処置）

弊社は、貴機構とお約束した守秘義務に反した場合、貴機構が行う合法的処置を受けることを約束いたします。

年 月 日

住 所 _____

会 社 名 _____

代表者名 _____ 印 _____