情報システム運用のための総合サービス業務
民間競争入札実施要項

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 趣旨 3
2 情報システム運用のための総合サービス業務の詳細な内容及びその実施に当たり確保されるべき対象公共サービスの質に関する事項 4
3 実施期間に関する事項 11
4 入札参加資格に関する事項 11
5 入札に参加する者の募集に関する事項 12
6 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者を決定するための評価の基準その他の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者の決定に関する事項..... 13
7 情報システム運用のための総合サービス業務に関する従来の実施状況に関する情報の開示に関する事項 16
8 情報システム運用のための総合サービス業務請負者に使用させることができる情報通信研究機構資産に関する事項 16
9 公共サービス実施請負者が、対象公共サービスを実施するに当たり、情報通信研究機構に対して報告すべき事項､秘密を適正に取り扱うために必要な措置その他の対象公共サービスの適正かつ確実な実施の確保のために契約により公共サービス実施請負者が講ずるべき措置に関する事項 18
10　公共サービス実施請負者が対象公共サービスを実施するに当たり､第三者に損害を加えた場合において､その損害の賠償に関し契約により当該公共サービス実施請負者が負うべき責任に関する事項 21
11　情報システム運用のための総合サービス業務に係る法第７条第８項に規定する評価に関する事項 21
12　その他業務の実施に関し必要な事項 21

別紙１ 従来の実施状況に関する情報の開示
別紙２ 組織図
別紙３ 運用業務フロー
別紙４ サポートデスク業務等の件数
別紙５ 情報システム室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６「H30 情報システム運用のための総合サービス業務」の追加業務

別添１ 調達仕様書
別添２ 総合評価基準書
別添３ 入札関係資料閲覧に関する誓約書
別添４ 守秘義務に関する誓約書

1　趣旨

競争の導入による公共サービスの改革に関する法律（平成 18 年法律第 51 号。以下「法」という。）に基づく競争の導入による公共サービスの改革については、公共サービスによる利益を享受する国民の立場に立って、公共サービスの全般について不断の見直しを行い、その実施について、透明かつ公正な競争の下で民間事業者の創意と工夫を適切に反映させることにより、国民のために、より良質かつ低廉な公共サービスを実現することを目指すものである。

上記を踏まえ、国立研究開発法人 情報通信研究機構（以下「情報通信研究機構」という。）は公共サービス改革基本方針（平成 24 年 7 月 20 日閣議決定）別表で民間競争入札の対象として選定された「情報システム運用のための総合サービス業務」（調達名は「H30 情報システム運用のための総合サービス業務」。以下「情報システム運用のための総合サービス業務」という。）について、公共サービス改革基本方針に従って、本実施要項を定めるものである。

2　情報システム運用のための総合サービス業務の詳細な内容及びその実施に当たり確保されるべき対象公共サービスの質に関する事項

(1)情報システム運用のための総合サービス業務の概要

ア　情報システム運用のための総合サービス業務の経緯

情報通信研究機構は平成 16 年 4 月旧通信総合研究所と旧通信・放送機構が統合し、平成 29 年 7 月国立研究開発法人情報通信研究機構として運用しているところである。

イ 提供サービス概要

本調達ではユーザがクライアント端末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為の運用、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。

(ｱ)本調達で運用する主なサービスは以下のとおり。各サービスの詳細は別添１ 調達仕様書を参照のこと。

A 本部セキュリティ運用サービス

セキュリティ担当 SE が常駐し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、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。情報セキュリティ委員会事務局および CSIRT 業務の支援を行うこと。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。

B 本部基幹ネットワーク運用サービス

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。

C 本部基幹サーバ運用サービス

サーバ担当 SE が常駐し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。

D 本部サポートデスク運用サービス

サポートデスク担当 SE が常駐し情報システム室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、当機構業務を追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。

E 個別システム運用サービス

個別に構築された勤務管理システム、電子決裁システム、職員間情報共有システム、特許管理システム、会計システム、成果管理システム、安否確認システム、e ラーニングシステム、Web/ビデオ会議サービスに対し安定運用並びに迅速・適切な運用支援を行うこと。

業務システムは、勤務管理システム、電子決裁システム、職員間情報共有システムの各基盤として仮想化技術を用いて動作環境を提供するものであり、安定運用並びに迅速・適切な運用支援を行うこと。

会計システムについて、サーバおよびサービスの安定運用、障害対応、迅速・適切な運用支援を行うこと。利用者からの問い合わせおよび申請に対応すること。

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ェアをインストールしてある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。

対外向けに NTP の情報を発信す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。

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。また、Web/ビデオ会議サービスとも連携した運用を実施すること

MDM システムを利用してユーザのモバイル端末等の管理運用、問合せ対応等を行うこと。

F 拠点システム運用サービス

地方拠点において基幹ネットワークおよび基幹サーバの維持管理を行うこと。

現地利用者への運用支援及びトラブル対応、検討、検証、イベント支援等を実施すること。

本部常駐の SE と連携して問題解決等にあたること。

ウ　規模

（平成 29 年 7 月時点）

A　ユーザアカウント数：約 2,000 人

B　サーバ台数：約 200 台（管理外のシステムは除く）

C　クライアント端末数：約 500 台（配布している PC 台数である。ユーザが利用している PC 台数は約 4000 台）

D　拠点数

(A)常駐場所：5 拠点

① 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

② 同　未来 ICT 研究所

所在地：兵庫県神戸市西区岩岡町岩岡 588-2

③ 同　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

④ 同　ユニバーサルコミュニケーション研究所

所在地：京都府相楽郡精華町光台 3-5

⑤ 同　鹿島宇宙技術センター

所在地：茨城県鹿嶋市平井 893-1

⑥ 同　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

(B) 地方拠点：13 拠点

① 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 21 階

② 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

③ 同　イノベーションセンター

所在地：東京都千代田区大手町 1-8-1 KDDI 大手町ビル 16 階

④ 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

⑤ 同　山川電波観測施設

所在地：鹿児島県指宿市山川成川 2719

⑥ 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

⑦ 同　犬吠テストフィールド

所在地：千葉県銚子市天王台 9961

⑧ 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

⑨ 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

⑩ 同　名護降雨観測施設

所在地：沖縄県名護市源河 2575

⑪ 同　北陸 StarBED 技術センター

所在地：石川県能見市旭台 2-12

⑫ 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

⑬ 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

エ　情報システム運用のための総合サービス業務の内容

本業務を実施する民間事業者（以下「請負者」という。）が行う業務は、調達対象範囲に係る運用、保守及びプロジェクト管理を行うことにより、ユーザに２(1)イ(ア)Ａ～Ｆに示すサービスを安定的に供給することとし、その詳細は別添１「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」を基本とする。なお調達仕様書については、所定の手続きを踏まえた上、別添３「入札関係資料閲覧に関する誓約書」へ署名し、遵守することで閲覧可能である。

(ｱ)更新整備に係る業務

Ａ　全体管理

(A)本部に総括責任者を置き、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）に関する安定稼動に努めること。

(B)請負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。

(C)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。

Ｂ コンサルテーション

当機構担当者と協議の上、サーバ・ネットワーク更改計画、構成案の検討及び資料作成、ネットワーク・既存サービス、システムの性能調査及び評価、改善検討、ネットワーク構成変更・追加の検討、既存システムの改修やサービス品質向上、利用者の利便性向上、運用効率化の検討、新サービス導入支援、ネットワーク・サーバ機器の保守内容の検討、セキュリティ対策の検討を行う。

Ｃ　設計

当機構担当者と協議の上、提案書及び各種計画書に基づき情報システム運用のための総合サービス業務の運用等の設計を行う。

Ｄ　構築

(ｲ)当機構担当者と協議の上、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。また、セキュリティ調査を迅速に行えるようログ解析環境を構築する。運用業務に係る業務

Ａ　運用

(A)対応業務内容

各システム及びネットワークが安定稼働するよう以下に示す対応業務を行う。

ａ　運用計画の策定

年次での運用計画を策定する。計画内容には以下の事項が含まれる。

(a) 各種修正プログラムの適用

(b) ソフトウェアアップデートの適用

(c) 稼動計画

(d) 要員計画　　等

ｂ　システム運用業務

稼働品質を担保するため、サービス及び機器等の稼働状況を監視し、各種のインシデン

トに対応する。

c　サポートデスク業務

ユーザからの各種の問い合わせを受け付け、ユーザ視点で問題解決を行う。またFAQ及び利用手順書等を整備することで、ユーザ業務の早期再開に向けて迅速に対応する。

d　共通部門計算機管理

主に当機構の事務部門に配布するパソコン配備される共通部門計算機の資産管理や構成管理、セキュリティ管理を行う。ユーザの申請に基づき共通部門計算機の配布を行い、共通部門計算機の障害対応として予備機の交換や共通部門計算機納入業者に修理を依頼する。

e　申請対応業務

システムの利用に係る各種申請に対して迅速に対応する。また、申請情報の棚卸し（要、不要、申請内容の精査等）を行い、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。

f　ポータルサイトの管理

当機構内の内部向けホームページを管理する。

g　インシデント管理

サポートデスクやシステム監視で検知されたインシデントを一元管理し、インシデント情報を有効に活用し、迅速な対応を行う。解決できないインシデントは、影響度及び優先順位等を精査し、問題管理にエスカレーションを行う。

障害対応情報からユーザ向けにFAQを作成してポータルサイトに掲載し、ユーザが閲覧できるようにする。

h　問題管理

インシデント管理からエスカレーションされた事象を問題として管理し、影響度と緊急度により優先順位を決め、問題原因の特定を行う。早急に根本的解決ができない場合には、一時的な解決策を策定すると同時に、問題の原因調査、分析を実施し、恒久的な解決策の策定を行う。管理された問題は、定期報告の内容として主管係に報告を実施する。

i　変更管理・リリース管理

日々実施されるシステムの脆弱性対応やネットワークの構成変更の対応の管理を行う。リリースにあたっては事前にリリース計画書を作成し、関係者各所と調整、周知の上、実施を行う。定期報告の内容として主管係に報告を実施する。

j　構成管理

システム構成、ネットワーク構成、ソフトウェア構成、資産(ソフトウェア・ハードウェア)、物理構成(LAN配線を含む)についての構成を管理する。なお、構成管理には、運用マニュアルなどを含む。

可用性管理運用管理システムや電源管理システムを活用し、情報システム運用のための総合サービス業務が提供するサービスに異常が検知された場合に適宜対応を行う。また、端末の故障時には、交換対応を実施して業務への影響が最小限となるよう努める。

k　プロジェクトマネジメント

請負者にて用意の作業管理システムにより各業務のタスクを管理、共有をはかるとともに、

運用管理業務を日次、週月次、年次で管理する。運用管理業務については各々報告書に取りまとめて定期的に情報システム室へ報告を行う。

常に万全の体制で業務を遂行できるよう要員の体制管理、シフト管理等を行う。

運用管理業務の中で、改善可能な事項は随時提案を行う。改善活動は内部プロセス、運用サービス内容等、運用品質の向上につながる内容とし、定期的に実施内容を報告する。

l　セキュリティインシデント対応

SEP や Yarai 等によるセキュリティ監視の際に、ウィルス監視や未知のマルウェア感染等の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。

CSIRT とも連携し迅速に対処すること。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、初動にかけ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。

m　イベント対応

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。

n　ドキュメント管理

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。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

共通部門計算機に導入されている Yarai に関する以下の対応を行う。

o　会議室運用

会議室設備として、音響装置、プロジェクタの操作及び利用者へ会議室利用の支援を行う。障害時には各機器を調査し必要な対応を行う。会議室設備の機器管理台帳を管理する。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。

B　教育

ユーザ及び運用者に対し教育訓練及び手順書の作成を行う。教育内容や実施場所、実施日時等は情報システム室と調整を行う。

(A) ユーザに対する利用手順書

情報システム運用のための総合サービス業務で提供するサービス・LAN・共通部門計算機・ソフトウェア等の利用方法及び操作方法を記載した手順書を作成し、当機構内の内部向けホームページに掲載。

(B)セキュリティ攻撃に対する訓練の実施支援

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1回実施すること。

(2) 確保されるべき対象業務の質

本業務は、利用者への継続的かつ安定的なサービスの円滑な提供に資するものである必要がある。こ

のような観点から、２(1)イ(ｱ)に示した業務内容を実施するに当たり、請負者が確保すべき対象業務の質は、次のとおりとする。

ア　業務の内容

「２(1)イ(ｱ)運用業務に係る業務」に示す運用管理業務を適切に実施すること。

イ　LAN の稼働率（個別システムの稼働率は対象外）

稼働率は 99%以上とする。稼働率は以下の計算式で計算する。

稼働率（%）＝｛1－（１か月の停止時間）÷（１か月の稼働予定時間）｝×100

※１か月の稼働予定時間＝（24 時間×１か月の日数）－計画停電等により停止する時間

計画停電等（停電、メンテナンス、実験等で意図して止めなければいけない場合）

ウ　セキュリティ上の重大障害

個人情報、施設等に関する情報その他の契約履行に際し知り得た情報漏えいの件数は０件であること。

エ　システム運用上の重大障害の件数

長期にわたり正常に稼動できない事態・状況及び保有するデータの喪失等により、業務に多大な支障が生じるような重大障害の件数は０件であること。

オ　ユーザの利用満足度調査

（別紙５情報システム室サポートデスク利用に関する満足度アンケート調査）

運用開始後、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）

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。

(3) 請負費用の支払方法

契約の形態は、業務請負契約とする。

当機構は、業務請負契約に基づき請負者が実施する本業務について、仕様書に定める内容について、契約の履行に関し、監督・検査を実施するなどして適正に実施されていることを確認した上で、適法な支払請求書を受理した日から起算して 30 日以内に支払うものとする。確認の結果、確保されるべき対象業務の質が達成されていないと認められる場合、当機構は、確保されるべき対象業務の質の達成に必要な限りで、請負者に対して本業務の実施方法の改善を行うよう指示することができる。請負者は、当該指示を受けて業務の実施方法を改善し、業務改善報告書を当機構に提出するものとする。業務改善報告書の内容が、確保されるべき対象業務の質が達成可能なものであると認められるまで、当機構は、請負費の支払を行わないことができる。なお、請負費は、平成 30 年 4 月 1 日以降の本件業務開始以降のサービス提供に対して支払われるものであり、請負者が行う引継ぎや準備行為等に対して、請負者に発生した費用は、請負者の負担とする。

3　実施期間に関する事項

請負契約の契約期間は、平成 30 年 4 月から平成 32 年 3 月末日までとする。

表 3-1 情報システム運用のための総合サービス業務・運用スケジュール

	平成 29 年度				平成 30 年度				平成 31 年度			
	4-6	7-9	10-12	1-3	4-6	7-9	10-12	1-3	4-6	7-9	10-12	1-3
情報システム運用のための総合サービス業務の運用				引継期間	運用開始							

4　入札参加資格に関する事項

(1) 入札参加資格

ア　法第 15 条において準用する法第 10 条各号（第 11 号を除く。）に該当する者でないこと。

イ　予算決算及び会計令（昭和 22 年勅令第 165 号）第 70 条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別な理由がある場合に該当する。

ウ　予算決算及び会計令第 71 条の規定に該当しない者であること。

エ　当機構競争参加資格「役務の提供等」Ａ、Ｂ、Ｃ等級のいずれかに格付けされている者、又は平成 28・29・30 年度総務省競争参加資格（全省庁統一資格）「役務の提供等」Ａ、Ｂ、Ｃ等級のいずれかに格付けされ、東北又は関東・甲信越又は近畿地域の競争参加資格を有する者であること（「役務の提供等」の営業品目「ソフトウェア開発」、「情報処理」又は「その他」に登録している者であること。）。

オ　法人税並びに消費税及び地方消費税の滞納がないこと。

カ　労働保険、厚生年金保険等の適用を受けている場合、保険料の滞納がないこと。

キ　当機構及び総務省における物品等の契約に係る指名停止措置要領に基づく指名停止を受けている期間中でないこと。

ク　調査研究や各工程の調達仕様書の作成に直接関与した事業者及びその関連事業者（「財務諸表等の用語、様式及び作成方法に関する規則」（昭和 38 年大蔵省令第 59 号）第８条に規定する親会社及び子会社、同一の親会社をもつ会社並びに委託先事業者等の緊密な利害関係を有する事業者をいう。）でないこと。

ケ　調達計画書及び調達仕様書の妥当性確認並びに入札事業者の審査に関する業務を行う CIO 補佐官及びその支援スタッフ等の属する又は過去２年間に属していた事業者でないこと。または、CIO 補佐官等がその職を辞職した後に所属する事業者の所属部門（辞職後の期間が２年に満たない場合に限る。）でないこと。

コ　単独で対象業務を行えない場合は、適正な業務を遂行できる共同事業体（対象業務を共同して行うことを目的として複数の民間事業者により構成される組織をいう。以下同じ。）として参加すること

ができる。その場合、入札書類提出時までに共同事業体を構成し、代表者を決め、他の者は構成員として参加するものとする。また、共同事業体の構成員は他の共同体の構成員となり、又は、単独で参加することはできない。なお、共同事業体の代表者及び構成員は、共同事業体の結成に関する協定書（又はこれに類する書類）を作成し、提出すること。

サ　本業務を統括管理する部門は、ISO9001 及び ISO27001 を取得していること。

シ　財団法人日本情報処理開発協会のプライバシーマーク制度の認定を受けていること。

(2) 競争参加資格申請書の入手方法等

競争参加資格を有しない者で、本入札に参加を希望する者は、所定の資格審査申請書を入手し、速やかに資格審査申請を行わなければならない。

【申請書の提出先】情報通信研究機構 財務部 会計室

郵便番号 184-8795　東京都小金井市貫井北町４－２－１

5　入札に参加する者の募集に関する事項

(1) 入札手続（スケジュール）

入札公示：官報公示	2017 年（平成 29 年）	１０月下旬
情報通信研究機構資料閲覧会		１０月下旬
入札説明会　（小金井本部開催）		１１月上旬（1 回）
閲覧会		入札説明会後　２０日間
質問受付期限		１２月中旬
入札書（提案書）提出期限		１２月中旬
提案書の審査	2018 年（平成 30 年）	1 月頃
開札及び落札予定者の決定		1 月頃
契約締結		1 月末頃
引継期間		２月１日～３月３１日

なお、従来の当該業務の調達仕様書、提出書類、各サービスの設計書等については、民間競争入札に参加する予定の者から要望があった場合、所定の手続きを踏まえた上、別添３「入札関係資料閲覧に関する誓約書」へ署名し、遵守することで閲覧可能である。

(2) 入札書類

入札参加者は、次に掲げる書類を別に定める入札説明書に記載された期日及び方法により提出すること。

ア　提案書

別添２「情報システム運用のための総合サービス業務の請負総合評価基準書」に示した各要求項目について具体的な提案（創意工夫を含む。）を行い、各要求項目を満たすことができることを証明する書類

イ　下見積書

人件費の単価証明書及び物件費の価格証明書を含んだ下見積書

ただし、契約後に発生する経費のみとする。

ウ　入札書

入札金額（契約期間内の全ての請負業務に対する報酬の総額の 105 分の 100 に相当する金額）を記載した書類

エ　委任状

代理人に委任したことを証明する書類

ただし、代理人による入札を行う場合に限る。

オ　競争参加資格審査結果通知書の写し

当機構競争参加資格「役務の提供等」Ａ及びＢ又はＣ等級に格付けされている者、又は平成 28・29・30 年度総務省競争参加資格（全省庁統一資格）「役務の提供等」Ａ及びＢ又はＣ等級に格付けされ、東北又は関東・甲信越又は近畿地域の競争参加資格を有する者であること（「役務の提供等」の営業品目「ソフトウェア開発」、「情報処理」又は「その他」に登録している者であること。）を証明する審査結果通知書の写し

ただし、電子入札システムにより入札を行う場合は不要。

カ　理由書

電子入札システムにより入札を行うことが出来ない旨の理由を示した書類

ただし、電子入札システムによる入札を行わない場合には不要。

キ　法第 15 条において準用する法第 10 条に規定する欠格事由のうち、暴力団排除に関する規程について評価するために必要な書類

ク　法人税並びに消費税及び地方消費税の納税証明書（直近のもの）

ケ　主たる事業概要、従業員数、事業所の所在地、代表者略歴、主要株主構成、他の者との間で競争の導入による公共サービス改革に関する法律施行令（平成 18 年政令第 228 号）第３条に規定する特定支配関係にある場合は、その者に関する当該情報

コ　共同事業体による参加の場合は、共同事業体内部の役割分担について定めた協定書又はこれに類する書類

6　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者を決定するための評価の基準その他の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者の決定に関する事項

以下に請負者の決定に関する事項を示す。なお、詳細は別添２「情報システム運用のための総合サービス業務の請負総合評価基準書」を基本とする。

(1) 評価方法

総合評価落札方式（加点方式）とする。総合評価は、価格点（入札価格の得点）に技術点（提案書による加点）を加えて得た数値（以下「総合評価点」という。）をもって行う。

総合評価点＝価格点（900 点満点）＋技術点（900 点満点）

(2) 決定方法

提案書を確認し、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。

(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。

価格点＝（１－入札価格÷予定価格）×900 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 点与える。

(ｲ) 別添２「情報システム運用のための総合サービス業務の請負総合評価基準書」に示す各評価項目に対応した提案内容の評価を行い、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) 配点は別添２「情報システム運用のための総合サービス業務の請負総合評価基準書」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) 「基礎点」と「加点」の合計点を「技術点」とする。

技術点＝基礎点（100 点）＋加点（800 点）

(4) 落札者の決定

ア　落札者の決定方法

(ｱ) 入札者の入札価格が予算決算及び会計令第 79 条の規定に基づいて作成された予定価格の制限の範囲内であり、かつ、「６(1)評価方法」によって得られた数値の最も高い者を落札者とする。ただし、予算決算及び会計令第 84 条の規定に該当する場合は、予算決算及び会計令第 85 条の基準（予定価格に 10 分の６を乗じて得た額）を適用するので、基準に該当する入札が行われた場合は入札の結果を保留する。この場合、入札参加者は当機構の行う事情聴取等の調査に協力しなければならない。

(ｲ) 調査の結果、会計法（昭和 22 年法律第 35 号）第 29 条の６第１項ただし書きの規定に該当すると認められるときは、その定めるところにより、予定価格の制限の範囲内で次順位の者を落札者とすることがある。

（会計法第 29 条の６第１項ただし書き抜粋） 相手方となるべき者の申込みに係る価格によっては、その者により当該契約の内容に適合した履行がされないおそれがあると認められるとき、又はその者と契約を締結することが公正な取引の秩序を乱すこととなるおそれがあって著しく不適当であると認められるとき

(ｳ) 落札者となるべき者が２人以上あるときは、直ちに当該入札者にくじを引かせ、落札者を決定するものとする。また、入札者又は代理人がくじを引くことができないときは、入札執行事務に関係のない職員がこれに代わってくじを引き、落札者を決定するものとする。

(ｴ) 契約担当官等は、落札者を決定したときに入札者にその氏名（法人の場合はその名称）及び金額を口頭で通知する。ただし、上記(ｲ)により落札者を決定する場合には別に書面で通知する。また、落札できなかった入札者は、落札の相対的な利点に関する情報（当該入札者と落札者のそれぞれの入札価格及び性能等の得点）の提供を要請することができる。

イ　落札決定の取消し

次の各号のいずれかに該当するときは、落札者の決定を取り消す。ただし、契約担当官等が、正当な理由があると認めたときはこの限りでない。

(ｱ) 落札者が、契約担当官等から求められたにもかかわらず契約書の取り交わしを行わない場合

(ｲ) 入札書の内訳金額と合計金額が符合しない場合

落札後、入札者に内訳書を記載させる場合があるので、内訳金額が合計金額と符合しないときは、合計金額で入札したものとみなす。この場合で、入札者は内訳金額の補正を求められたときは、直ちに合計金額に基づいてこれを補正しなければならない。

ウ　落札者が決定しなかった場合の措置

初回の入札において入札参加者がなかった場合、必須項目を全て満たす入札参加者がなかった場合又は再度の入札を行っても、なお、落札者が決定しなかった場合、原則として、入札条件等を見直した後、再度公告を行う。

なお、再度の入札によっても落札者となるべき者が決定しない場合又は本業務の実施に必要な期間が確保できないなどやむを得ない場合は、自ら実施する等とし、その理由を官民競争入札等管理委員会に報告するとともに公表するものとする。

7　情報システム運用のための総合サービス業務に関する従来の実施状況に関する情報の開示に関する事項

(1) 開示情報

対象業務に関して、以下の情報は別紙１「従来の実施状況に関する情報の開示」のとおり開示する。

ア　従来の実施に要した経費

イ　従来の実施に要した人員

ウ　従来の実施に要した施設及び設備

エ　従来の実施における目標の達成の程度

オ　従来の実施方法等

以下の資料については「情報通信研究機構資料閲覧会」において開示する情報は以下の通りとする。

ア サーバ構成図

イ ネットワーク構成図

ウ サーバシステム設計書

エ 運用手順書等

オ 月例作業報告書

「情報通信研究機構資料閲覧会」へは以下の手続きを踏まえた上で参加可能とする。

ア　E-Mail・FAX で事前に予約を行うこと

予約内容：法人名、閲覧希望日、閲覧人数、連絡先等

イ　予約申込にあたり事前に以下の資料を提出すること

(ア) 別添３　入札関係資料閲覧に関する誓約書

(イ) 当機構競争参加資格の写し、又は平成 28・29・30 年度総務省競争参加資格（全省庁統一資格）の写し

(ウ) 担当者の名刺（閲覧参加者全員分）

閲覧会は意見招請および本入札両方において公示から 30 日以内に行う。

8　情報システム運用のための総合サービス業務請負者に使用させることができる情報通信研究機構資産に関する事項

請負者は、次のとおり情報通信研究機構資産を使用することができる。

(1) 情報通信研究機構資産の使用

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

ア　業務に必要な電気設備

イ　その他、当機構と協議し承認された業務に必要な施設、設備等

(2) 使用制限

ア　請負者は、情報システム運用のための総合サービス業務の実施及び実施に付随する業務以外の目的で使用し、又は利用してはならない。

イ　請負者は、あらかじめ当機構と協議した上で、当機構の業務に支障を来さない範囲内において、施設内に運用管理業務の実施に必要な設備等を持ち込むことができる。

ウ　請負者は、設備等を設置した場合は、設備等の使用を終了又は中止した後、直ちに、必要な原状回復を行う。

エ　請負者は、既存の建築物及び工作物等に汚損・損傷等を与えないよう十分に注意し、損傷（機器の故障等を含む。）が生じるおそれのある場合は、養生を行う。万一損傷が生じた場合は、請負者の責任と負担において速やかに復旧するものとする。

9　公共サービス実施請負者が、対象公共サービスを実施するに当たり、情報通信研究機構に対して報告すべき事項、秘密を適正に取り扱うために必要な措置その他の対象公共サービスの適正かつ確実な実施の確保のために契約により公共サービス実施請負者が講ずるべき措置に関する事項

(1) 請負者が当機構に報告すべき事項、当機構の指示により講ずるべき措置

ア　報告等

(ｱ) 請負者は、仕様書に規定する業務を実施したときは、当該仕様書に基づく各種報告書を当機構に提出しなければならない。

(ｲ) 請負者は、請負業務を実施したとき、又は完了に影響を及ぼす重要な事項の変更が生じたときは、直ちに当機構に報告するものとし、当機構と請負者が協議するものとする。

(ｳ) 請負者は、契約期間中において、(ｲ)以外であっても、必要に応じて当機構から報告を求められた場合は、適宜、報告を行うものとする。

イ　調査

(ｱ) 当機構は、請負業務の適正かつ確実な実施を確保するために必要があると認めるときは、法第 26 条第 1 項の規定に基づき、請負者に対し必要な報告を求め、又は当機構の職員が事務所に立ち入り、当該業務の実施の状況若しくは記録、帳簿書類その他の物件を検査し、又は関係者に質問することができる。

(ｲ) 立入検査をする当機構の職員は、検査等を行う際には、当該検査が法第 26 条第 1 項の規定に基づくものであることを請負者に明示するとともに、その身分を示す証明書を携帯し、関係者に提示するものとする。

ウ　指示

当機構は、請負業務の適正かつ確実な実施を確保するために必要と認めるときは、請負者に対し、必要な措置を採るべきことを指示することができる。

(2) 秘密を適正に取り扱うための措置

ア　請負者は、本業務の実施に際して知り得た当機構の情報を、第三者に漏らし、盗用し、又は請負業務以外の目的のために利用してはならない。これらの者が秘密を漏らし、又は盗用した場合は、法第 54 条の規定により罰則の適用がある。

イ　請負者は、本業務の実施に際して得られた情報処理に関する利用技術（アイデア又はノウハウ）については、請負者からの文書による申出を当機構が認めた場合に限り、第三者へ開示できるものとする。

ウ　請負者は、当機構から提供された個人情報及び業務上知り得た個人情報について、個人情報の保護に関する法律(平成 15 年法律第 57 号)の規定に基づき、適切な管理を行わなくてはならない。また、当該個人情報については、本業務以外の目的のために利用してはならない。

エ　請負者は、当機構の情報セキュリティに関する規程等に基づき、個人情報等を取り扱う場合は、①情報の複製等の制限、②情報の漏えい等の事案の発生時における対応、③請負業務終了時の情報の消去・廃棄（復元不可能とすること。）及び返却、④内部管理体制の確立、⑤情報セキュリティの運用状況の検査に応じる義務、⑥請負者の事業責任者及び請負業務に従事する者全てに対しての守秘義務及び情報セキュリティ要求事項の遵守に関して、別添４「守秘義務に関する誓約書」に署名し、遵守しなければならない。

オ　アからエまでのほか、当機構は、請負者に対し、本業務の適正かつ確実な実施に必要な限りで、秘密を適正に取り扱うために必要な措置を採るべきことを指示することができる。

(3) 契約に基づき請負者が講ずるべき措置

ア　請負業務の開始

請負者は、本業務の開始日から確実に業務を開始すること。

イ　権利の譲渡

請負者は、債務の履行を第三者に引き受けさせ、又は契約から生じる一切の権利若しくは義務を第三者に譲渡し、承継せしめ、若しくは担保に供してはならない。ただし、書面による当機構の事前の承認を得たときは、この限りではない。

ウ　瑕疵担保責任

(ｱ) 当機構は、成果物の引渡し後に発見された瑕疵について、引渡し後１年間は、請負者に補修を請求できるものとし、補修に必要な費用は、全て請負者の負担とする。

(ｲ) 成果物の瑕疵が請負者の責に帰すべき事由によるものである場合は、当機構は、前項の請求に際し、これによって生じた損害の賠償を併せて請求することができる。

エ　再委託

(ｱ) 請負者は、本業務の実施に当たり、その全部を一括して再委託してはならない。

(ｲ) 請負者は、本業務の実施に当たり、その一部について再委託を行う場合には、原則として、あらかじめ機能証明書において、再委託先に委託する業務の範囲、再委託を行うことの合理性及び必要性、再委託先の履行能力並びに報告徴収、個人情報の管理その他運営管理の方法（以下「再委託先等」という。）について記載しなければならない。

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

(ｴ) 請負者は、(ｲ)又は(ｳ)により再委託を行う場合には、請負者が当機構に対して負う義務を適切に履行するため、再委託先の事業者に対し前項「(2)秘密を適正に取り扱うために必要な措置」及び本項「(3)契約に基づき請負者が講じるべき措置」に規定する事項その他の事項について、必要な措置を講じさせるとともに、再委託先から必要な報告を聴取することとする。

(ｵ) (ｲ)から(ｴ)までに基づき、請負者が再委託先の事業者に義務を実施させる場合は、全て請負者の責任において行うものとし、再委託先の事業者の責に帰すべき事由については、請負者の責に帰すべき事由とみなして、請負者が責任を負うものとする。

オ　契約内容の変更

当機構及び請負者は、本業務を改善するため、又は経済情勢の変動、天災地変の発生、関係法令の制定若しくは改廃その他契約の締結の際、予測できなかった著しい変更が生じたことにより本業務を実施することが不適当と認められる場合は、協議により、契約の内容を変更することができる。

カ　契約の解除

当機構は、請負者が次のいずれかに該当するときは、請負者に対し請負費の支払を停止し、又は契約を解除若しくは変更することができる。この場合、請負者は当機構に対して、請負費の総価の 100 分の 20 に相当する金額を違約金として支払わなければならない。その場合の算定方法については、当機構の定めるところによる。ただし、同額の超過する増加費用及び損害が発生したときは、超過分の請求を妨げるものではない。

また、請負者は、当機構との協議に基づき、本業務の処理が完了するまでの間、責任を持って当該処理を行わなければならない。

(ｱ) 法第 22 条第１項イからチまで又は同項第２号の規定に該当するとき。

(ｲ) 暴力団員を、業務を統括する者又は従業員としていることが明らかになった場合。

(ｳ) 暴力団員と社会的に非難されるべき関係を有していることが明らかになった場合。

(ｴ) 再委託先が、暴力団若しくは暴力団員により実質的に経営を支配される事業を行う者又はこれに準ずる者に該当する旨の通知を、警察当局から受けたとき。

(ｵ) 再委託先が暴力団又は暴力団関係者と知りながらそれを容認して再委託契約を継続させているとき。

キ　談合等不正行為

請負者は、談合等の不正行為に関して、当機構が定める「談合等の不正行為に関する特約条項」に従うものとする。

ク　損害賠償

請負者は、請負者の故意又は過失により当機構に損害を与えたときは、当機構に対し、その損害について賠償する責任を負う。

ケ　不可抗力免責、危険負担

当機構及び請負者の責に帰すことのできない事由により契約期間中に物件が滅失し、又は毀損し、その結果、当機構が物件を使用することができなくなったときは、請負者は、当該事由が生じた日の翌日以後の契約期間に係る代金の支払を請求することができない。

コ　金品等の授受の禁止

請負者は、本業務の実施において、金品等を受け取ること、又は、与えることをしてはならない。

サ　宣伝行為の禁止

請負者及び本業務に従事する者は、本業務の実施に当たって、自ら行う業務の宣伝を行ってはならない。また、本業務の実施をもって、第三者に対し誤解を与えるような行為をしてはならない。

シ　記録及び帳簿類の保管

請負者は、本業務に関して作成した記録及び帳簿類を、本業務を終了し、又は中止した日の属する年度の翌年度から起算して７年間、保管しなければならない。

ス　請負業務の引継ぎ

(ｱ) 現行請負者からの引継ぎ

請負者は、本業務が適正かつ円滑にできるよう現行請負者から本業務の開始日までに運用管理手順書等を使用して必要な事務引継ぎを受けなければならない。

また、当機構は、当該事務引継ぎが円滑に実施されるよう、現行請負者及び請負者に対して必要な協力を行うものとする。

なお、その際の事務引継ぎに必要となる経費は、現行請負者の負担となる。

(ｲ) 請負期間満了の際、業者変更が生じた場合の引継ぎ

本業務の期間満了の際、業者変更が生じた場合は、請負者は、次回の請負者に対し、当該業務の開始日までに運用管理手順書等を使用し必要な事務引継ぎを行わなければならない。

なお、その際の事務引継ぎに必要となる請負者に発生した経費は、請負者の負担となる。

セ　契約の解釈

契約に定めのない事項及び契約に関して生じた疑義は、当機構と請負者との間で協議して解決する。

10　公共サービス実施請負者が対象公共サービスを実施するに当たり、第三者に損害を加えた場合において、その損害の賠償に関し契約により当該公共サービス実施請負者が負うべき責任に関する事項

本業務を実施するに当たり、請負者又はその職員その他の本業務に従事する者が、故意又は過失により、本業務の受益者等の第三者に損害を加えた場合は、次のとおりとする。

(1) 当機構が国家賠償法第１条第１項等の規定に基づき当該第三者に対する賠償を行ったときは、当機構は請負者に対し、当該第三者に支払った損害賠償額（当該損害の発生について当機構の責めに帰すべき理由が存する場合は、当機構が自ら賠償の責めに任ずべき金額を超える部分に限る。）について求償することができる。

(2) 請負者が民法（明治 29 年法律第 89 号）第 709 条等の規定に基づき当該第三者に対する賠償を行った場合であって、当該損害の発生について当機構の責めに帰すべき理由が存するときは、請負者は当機構に対し、当該第三者に支払った損害賠償額のうち自ら賠償の責めに任ずべき金額を超える部分を求償することができる。

11　情報システム運用のための総合サービス業務に係る法第７条第８項に規定する評価に関する事項

(1) 本業務の実施状況に関する調査の時期

当機構は、本業務の実施状況について、総務大臣が行う評価の時期(平成30年5月を予定)を踏まえ、本業務に係る運用が開始される平成 30 年度以降、各年度末時点における状況を調査する。

(2) 調査項目及び実施方法

ア　LAN の稼働率

業務報告書等により調査

イ　セキュリティ上の重大障害の件数

業務報告書等により調査

ウ　システム運用上の重大障害の件数

業務報告書等により調査

エ　利用満足度調査の結果

各年度において、ユーザに対する年１回のアンケート（利用満足度調査）の実施結果により調査

(3) 意見聴取等

当機構は、必要に応じ、民間事業者から意見の聴取を行うことができるものとする。

また、当機構は、平成31年3月を目途として、本業務の実施状況等を内閣総理大臣及び官民競争入札等監理委員会へ提出する。

なお、調査報告を総務大臣及び官民競争入札等監理委員会に提出するに当たり、CIO 補佐官及び外部有識者の意見を聴くものとする。

12　その他業務の実施に関し必要な事項

(1) 本業務の実施状況等の官民競争入札等監理委員会への報告及び公表

当機構は、法第 26 条及び第 27 条に基づく報告徴収、立入検査、指示等を行った場合には、その都度、措置の内容及び理由並びに結果の概要を監理委員会へ報告することとする。

(2)情報通信研究機構の監督体制

本契約に係る監督は、情報システム室自ら立会い、指示その他の適切な方法によって行うものとする。

本業務の実施状況に係る監督は以下のとおり。

監督職員：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リーダー

検査職員：情報通信研究機構 経営企画部 企画戦略室 職員

(3) 請負者の責務

ア　本業務に従事する請負者は、刑法（明治 40 年法律第 45 号）その他の罰則の適用については、法令により公務に従事する職員とみなされる。

イ　請負者は、法第 55 条の規定に該当する場合は、30 万円以下の罰金に処されることとなる。なお、法第 56 条の規定により、法人の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関し、法第 55 条の規定に違反したときは、行為者を罰するほか、その法人又は人に対して同条の刑を科する。

ウ　請負者は、会計検査院法（昭和 22 年法律第 73 条）第 23 条第 1 項第 7 号に規定する者に該当することから、会計検査院が必要と認めるときには、同法第 25 条及び第 26 条の規定により、同院の実地の検査を受けたり、同院から直接又は当機構に通じて、資料又は報告等の提出を求められたり、質問を受けたりすることがある。

(4) 著作権

ア　請負者は、本業務の目的として作成される成果物に関し、著作権法第 27 条及び第 28 条を含む著作権の全てを当機構に無償で譲渡するものとする。

イ　請負者は、成果物に関する著作者人格権（著作権法第 18 条から第 20 条までに規定された権利をいう。）を行使しないものとする。ただし、当機構が承認した場合は、この限りではない。

ウ　ア及びイにかかわらず、成果物に請負者が既に著作権を保有しているもの（以下「請負者著作物」という。）が組み込まれている場合は、当該請負者著作物の著作権についてのみ、請負者に帰属する。

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

別紙１

「従来の実施状況に関する情報の開示」

１　従来の実施に要した経費　（単位：千円）

			平成 27 年度	平成 28 年度	平成 29 年度
	人件費	常勤職員	－	－	
		非常勤職員	－	－	
	物件費		－	－	
	請負費	役務	177,299	209,654	218,802
		機器・回線リース料	－		
		設計・構築費	－		
		その他	－		
計(a)			177,299	209,654	218,802
参考値(b)	減価償却費		－		
	退職給付費用		－		
	間接部門費		－		
(a)＋(b)			177,299	209,654	※1 218,802

（注記事項）
※　請負業務のため、費用の詳細な内訳の開示は受けられない。

※1 H29 年業務追加により、H28 年度より増額になっている。

２　従来の実施に要した人員　（単位：人）

	平成 27 年度	平成 28 年度	平成 29 年度
（運用業務従事者 本部）			
総括責任者・総括責任者代行	3	3	2
サポートデスク担当者	6	7	7
ネットワーク担当者	5	4	4
サーバ担当者	4	6	7
コンサル、設計、構築担当	1	1	1
（運用業務従事者 鹿島宇宙技術センター）			
サポートデスク担当者	0.6	0.6	0.6
ネットワーク担当者 サーバ担当者	0.4 （SD 週 3 回、NW SV 週 2 回）	0.4 （SD 週 3 回、NW SV 週 2 回）	0.4 （SD 週 3 回、NW SV 週 2 回）
（運用業務従事者 ユニバーサルコミュニケーション研究所）			
サポートデスク担当者	1	1	1

総括責任者 ネットワーク担当者 サーバ担当者			-

（運用業務従事者 未来 ICT 研究所）

サポートデスク担当者	2	2	2
総括責任者 ネットワーク担当者 サーバ担当者	（SD、NW、SV の区別なし）	（SD、NW、SV の区別なし）	（SD、NW、SV の区別なし）

（運用業務従事者 脳情報融合通信研究センター）

サポートデスク担当者	3	3	3
総括責任者 ネットワーク担当者 サーバ担当者	（SD、NW、SV の区別なし）	（SD、NW、SV の区別なし）	（SD、NW、SV の区別なし）

（業務従事者に求められる知識・経験等）

【総括責任者・総括責任者代行】
・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、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 共通事項】
・英語サイトからの情報を収集し、和訳意訳できること。
・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）や提案を行えること。
・識別性に考慮したタグ付け、マーキングを機器に行えること。

【ネットワーク担当者 個別スキル（機構利用機器を運用するためのスキル）】
・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。

・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発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 の設定が行えること。

・機器の設定を別の機器を介して確認できること。

【サーバ担当者 個別スキル（機構利用機器を運用するためのスキル)】

・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。

・NetApp Data Ontap7/8 においてストレージ管理できること。

・Solaris ZFS においてストレージ管理できること。

・Solaris Zone 仮想サーバ及び仮想ネットワークを管理できること。

・UNIX 系 OS を CUI のみで管理できること。

・Active Directory 及び Terminal Services を構成管理できること。

・CMS(WebRelease2)のバージョンアップができること。

・VMware において仮想マシンの管理ができること。

【サポートデスク担当者】

・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。

・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 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 接続及び vi/vim を用いてテキスト編集を行えること。

（業務の繁閑の状況とその対応）

別紙４サポートデスク業務等の件数

3　従来の実施に要した施設及び設備

（本部）

【施設】

施設名称：研究本館 2F 居室

使用場所：サーバ室
(本部) 【設備及び主な物品】 情報通信研究機構 貸与： 　内線電話 22 台（PHS)、机 22 台、袖机 18 台、椅子 22 脚、キャビネット 10 台、台車 2 台 請負者所有： 　文房具、複合機、請負会社連絡用携帯電話
(鹿島宇宙技術センター) 【施設】 施設名称：研究本館計算機室 使用場所：計算機室
(鹿島宇宙技術センター) 【設備及び主な物品】 情報通信研究機構 貸与： 　内線電話 1 台（PHS1 台)、机 4 台、袖机 2 台、椅子 4 脚、キャビネット 2 台、台車 2 台 請負者所有： 　文房具、請負会社連絡用携帯電話
(ユニバーサルコミュニケーション研究所) 【施設】 施設名称：研究本館 計算機室 使用場所：計算機室
(ユニバーサルコミュニケーション研究所) 【設備及び主な物品】 情報通信研究機構 貸与： 　内線電話 6 台（PHS6 台)、机 10 台、袖机 4 台、椅子 10 脚、キャビネット 4 台、台車 2 台 請負者所有： 　文房具、請負会社連絡用携帯電話
(未来 ICT 研究所) 【施設】 施設名称：研究本館 計算機室 使用場所：計算機室
(未来 ICT 研究所) 【設備及び主な物品】 情報通信研究機構 貸与： 　内線電話 1 台（PHS1 台)、机 6 台、袖机 4 台、椅子 6 脚、キャビネット 2 台、台車 2 台 請負者所有： 　文房具、請負会社連絡用携帯電話
(脳情報通信融合研究センター) 【施設】 施設名称：CiNET 計算機室 使用場所：計算機室
(脳情報通信融合研究センター) 【設備及び主な物品】 情報通信研究機構 貸与： 　内線電話 4 台（PHS4 台)、机 6 台、袖机 4 台、椅子 6 脚、キャビネット 2 台、台車 2 台 請負者所有： 　文房具、請負会社連絡用携帯電話
(ワイヤレスネットワーク研究所) 【施設】 施設名称：ワイヤレスネットワーク研究所

仕様場所：計算機室
（ワイヤレスネットワーク研究所） 【設備及び主な物品】 非常駐のため無し 請負者所有： 文房具、請負会社連絡用携帯電話

拠点情報

本部	東京都小金井市貫井北町 4-2-1
鹿島宇宙技術センター	茨城県鹿嶋市平井 893-1
ユニバーサルコミュニケーション研究所	京都府相楽郡精華町光台 3-5
未来 ICT 研究所	兵庫県神戸市西区岩岡町岩岡 588-2
脳情報通信融合研究センター	大阪府吹田市山田丘 1-4
ワイヤレスネットワーク総合研究センター	神奈川県横須賀市光の丘 3-4

4　従来の実施における目標の達成の程度

当機構の運用管理については、本部、鹿島宇宙技術センター、ユニバーサルコミュニケーション研究所、未来 ICT 研究所、脳情報通信融合研究センター、耐災害 ICT 研究センターの業務を確実に実施するため、情報システムの利用者への継続的・安定的なサービスの提供を円滑に行う事を目的としている。

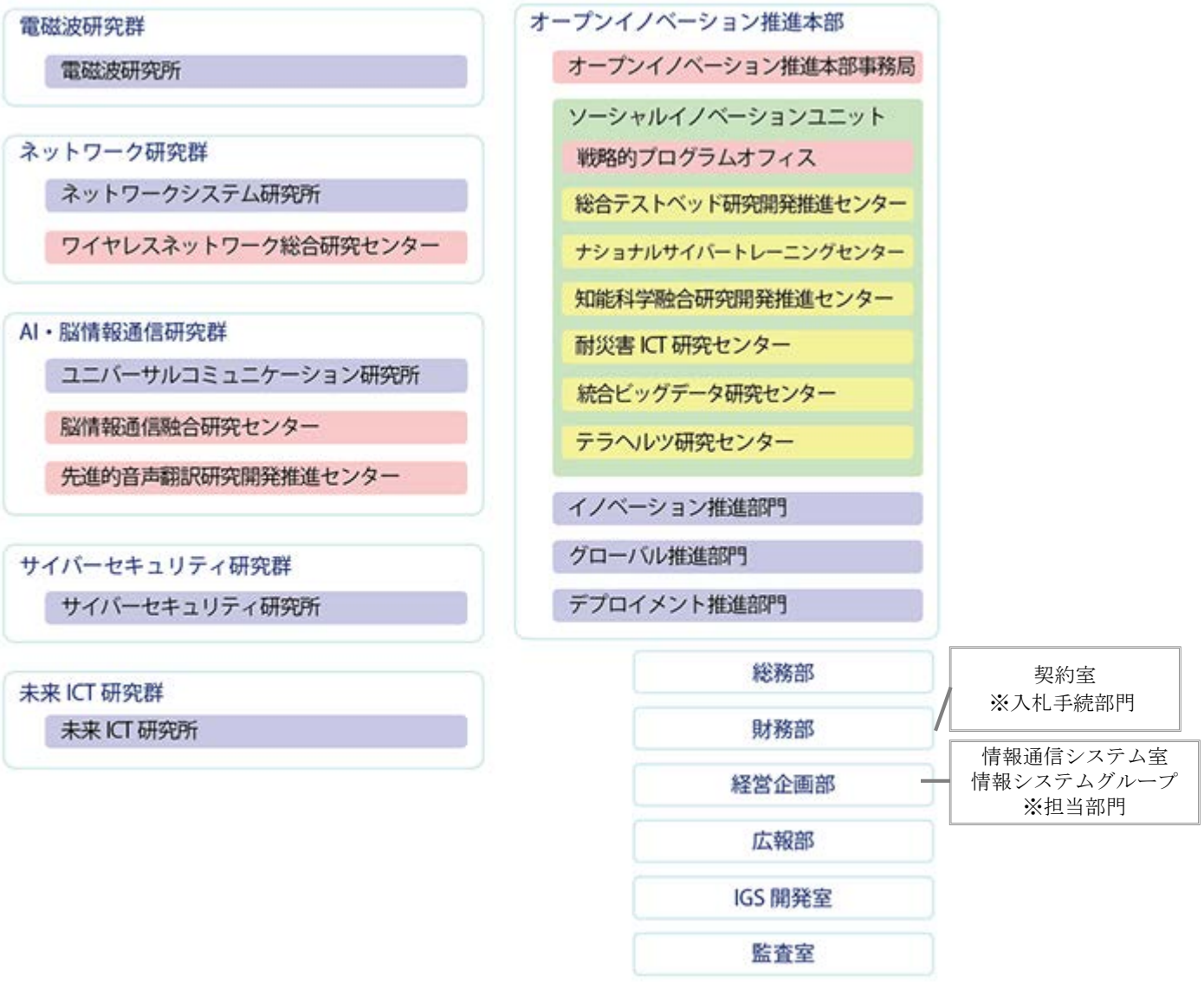
(1) 業務の内容
（平成 26-27 年度から平成 28-29 年度までの間、仕様書に示す運用管理業務を適切に実施している。）
(2) LAN の稼働率（個別システムの稼働率は対象外）
（平成 26-27 年度から平成 28-29 年度までの間、仕様書に定められている要求事項を確実に実施しているが、LAN の稼働率は設定していない。）
(3) セキュリティ上の重大障害
（平成 26-27 年度から平成 28-29 年度までの間、仕様書に定められている要求事項を確実に実施しているが、セキュリティ上の重大障害は無い）
(4) システム運用上の重大障害の件数
（平成 26-27 年度から平成 28-29 年度までの間、仕様書に定められている要求事項を確実に実施しているが、システム運用上の重大障害は無い）

5　従来の実施方法等

従来の実施方法（業務フロー図等）

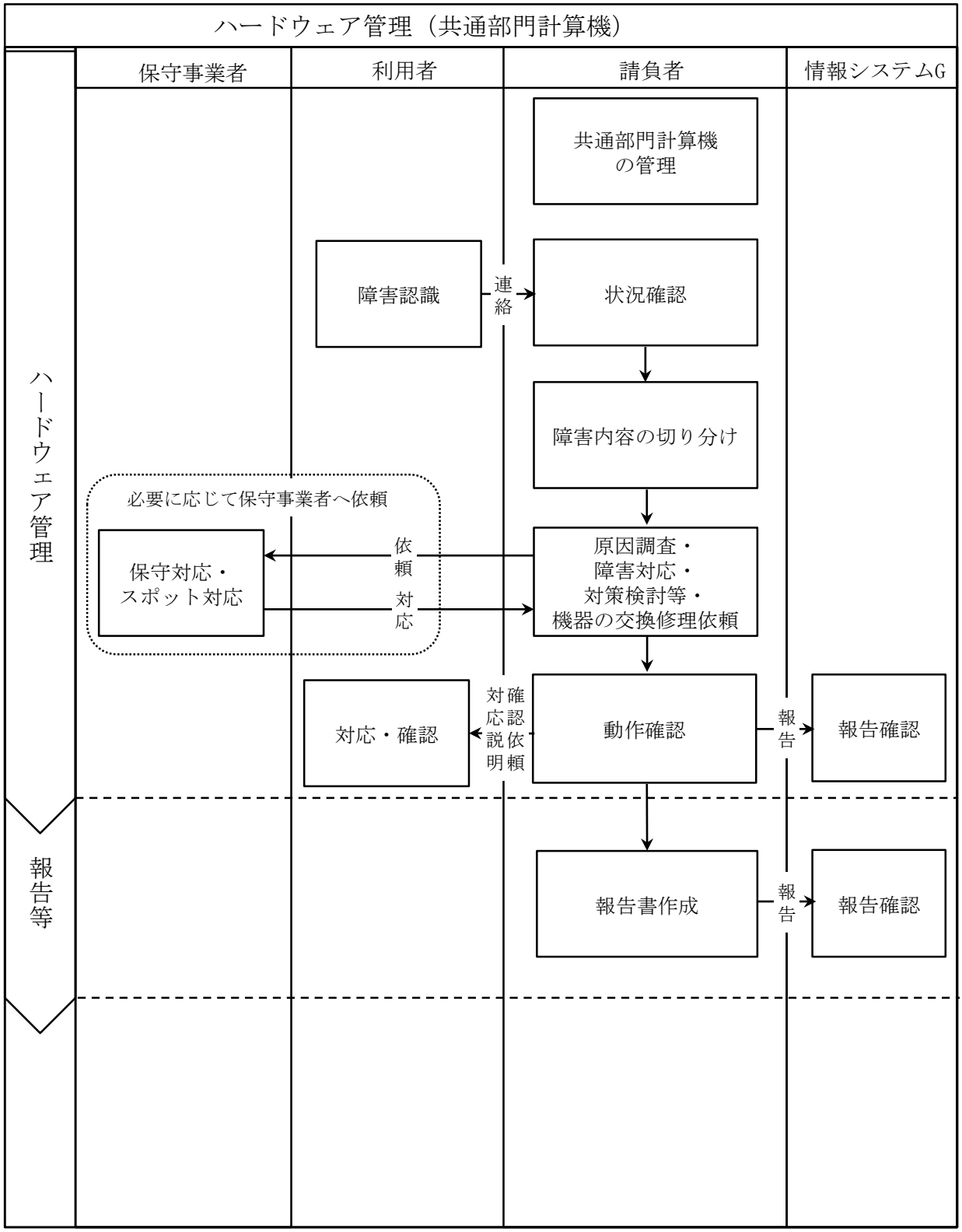
別紙３（業務フロー及び業務区分）

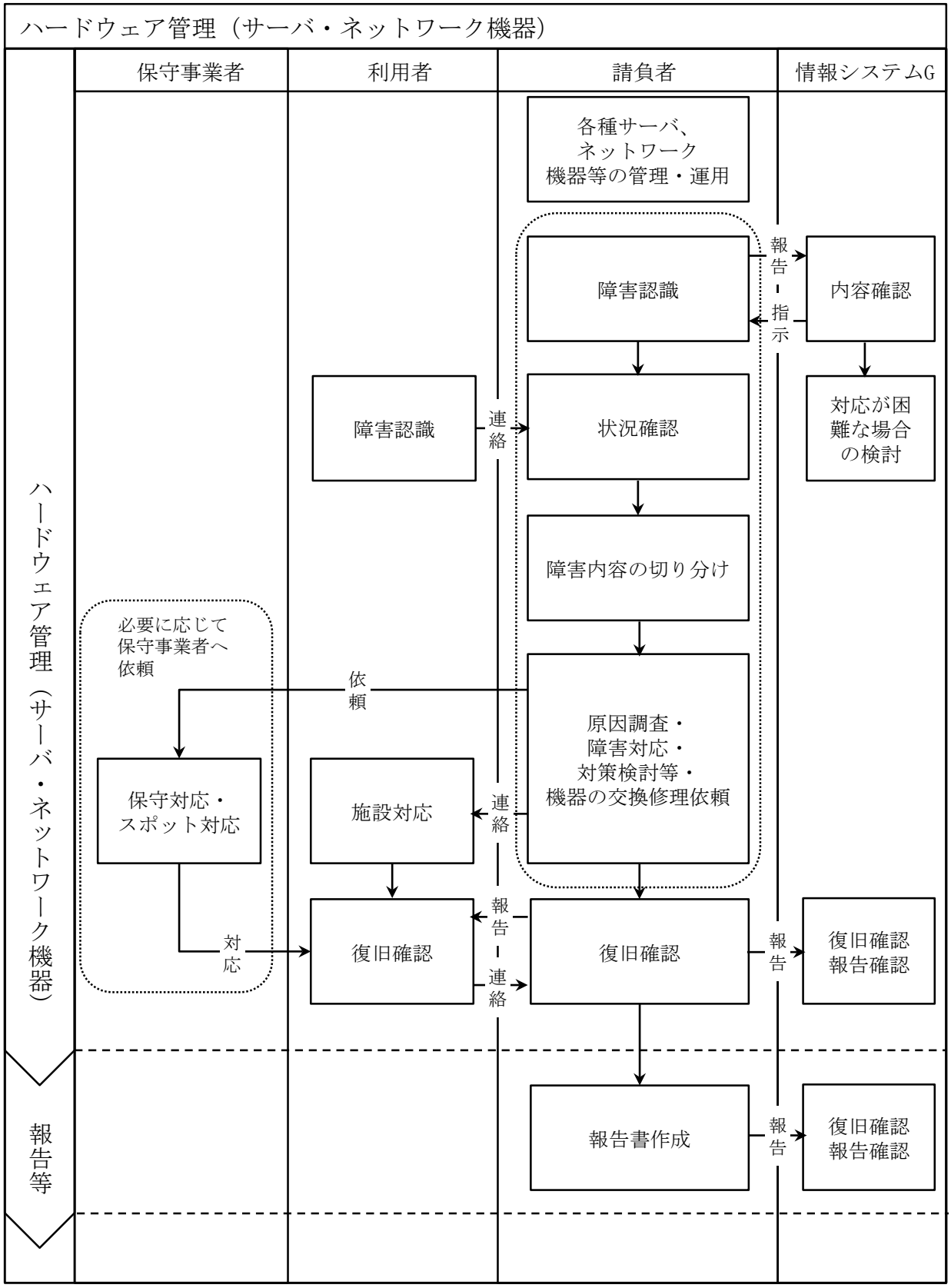
【情報通信研究機構組織図】

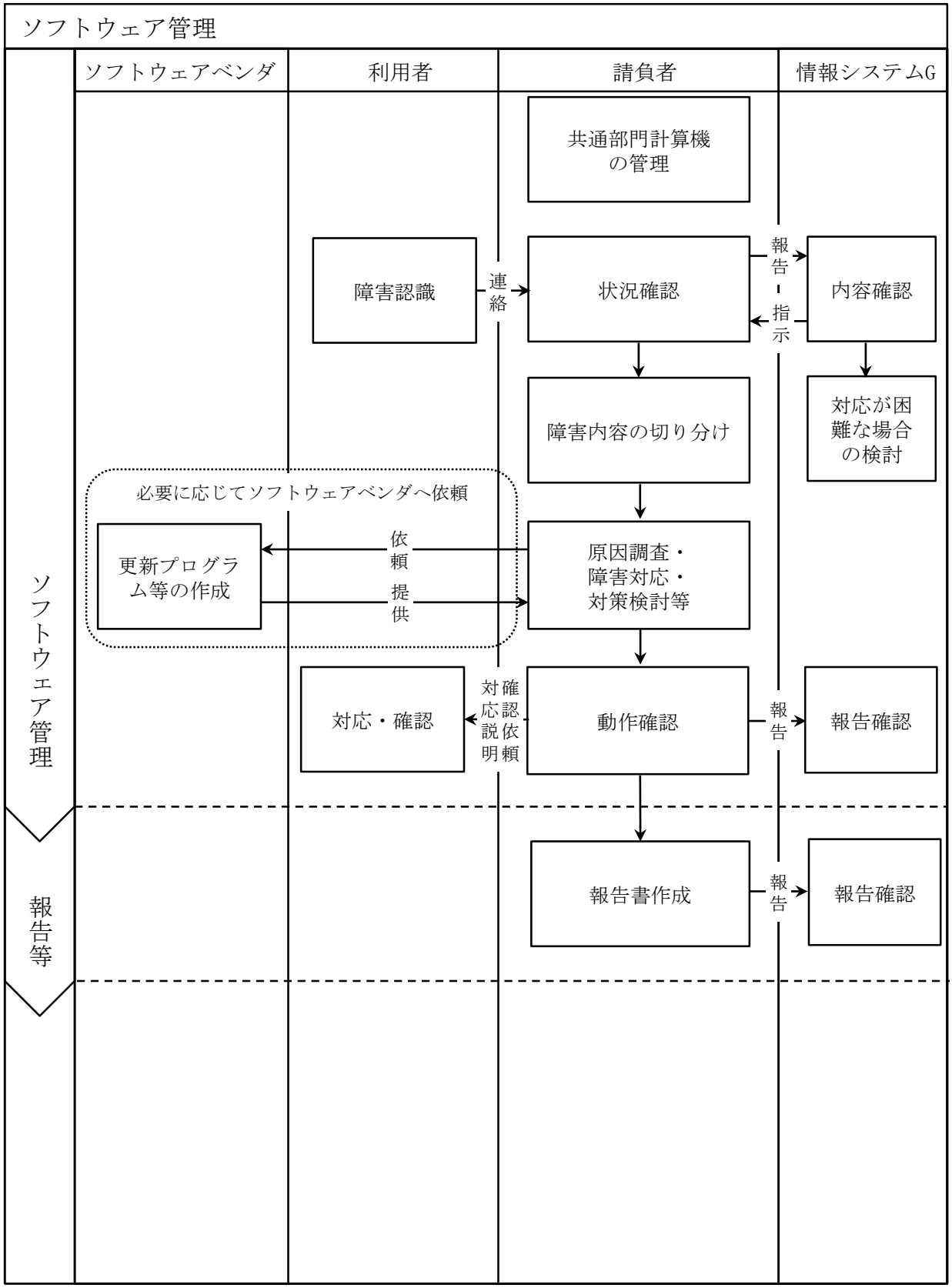


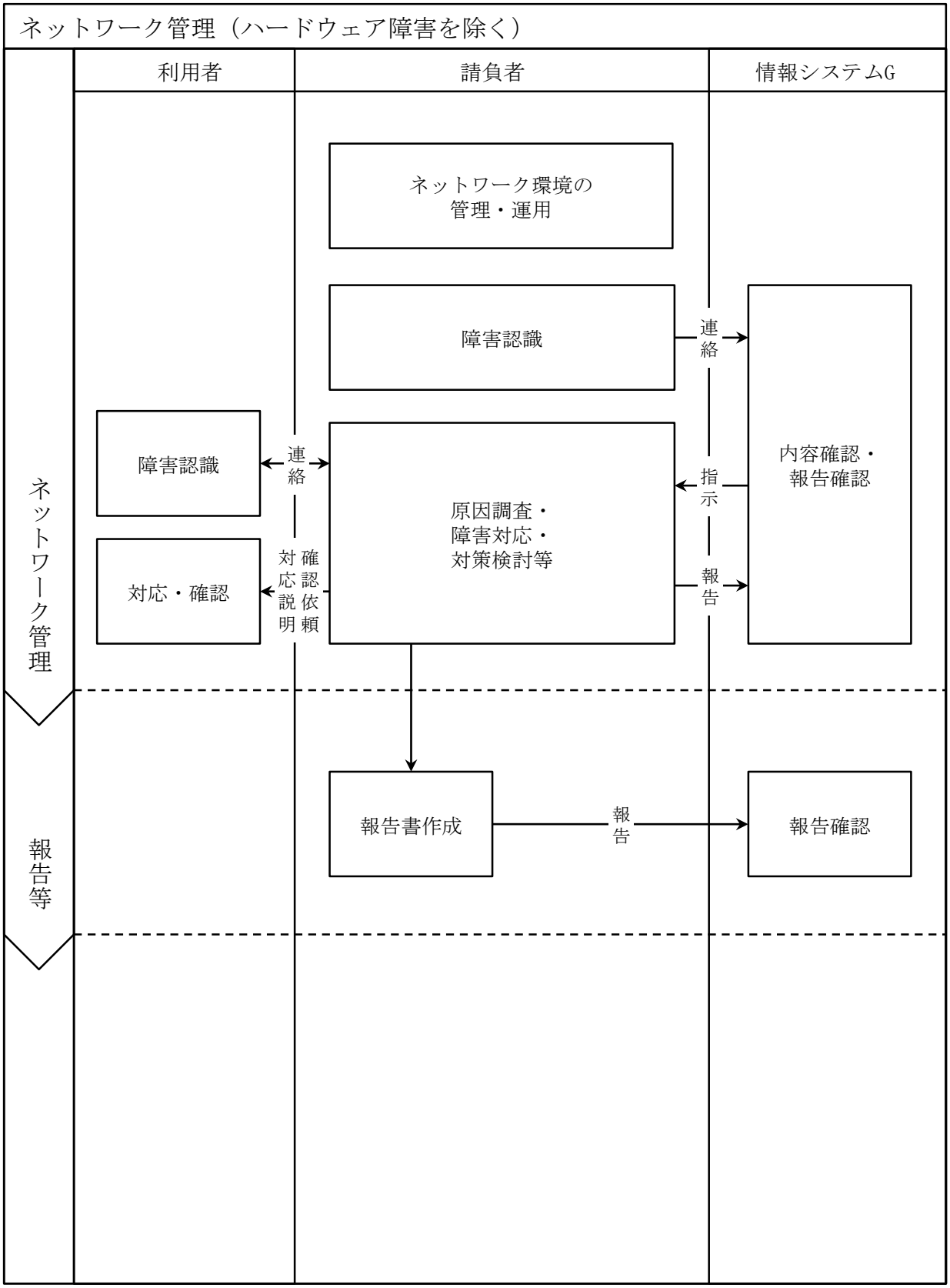
別紙3

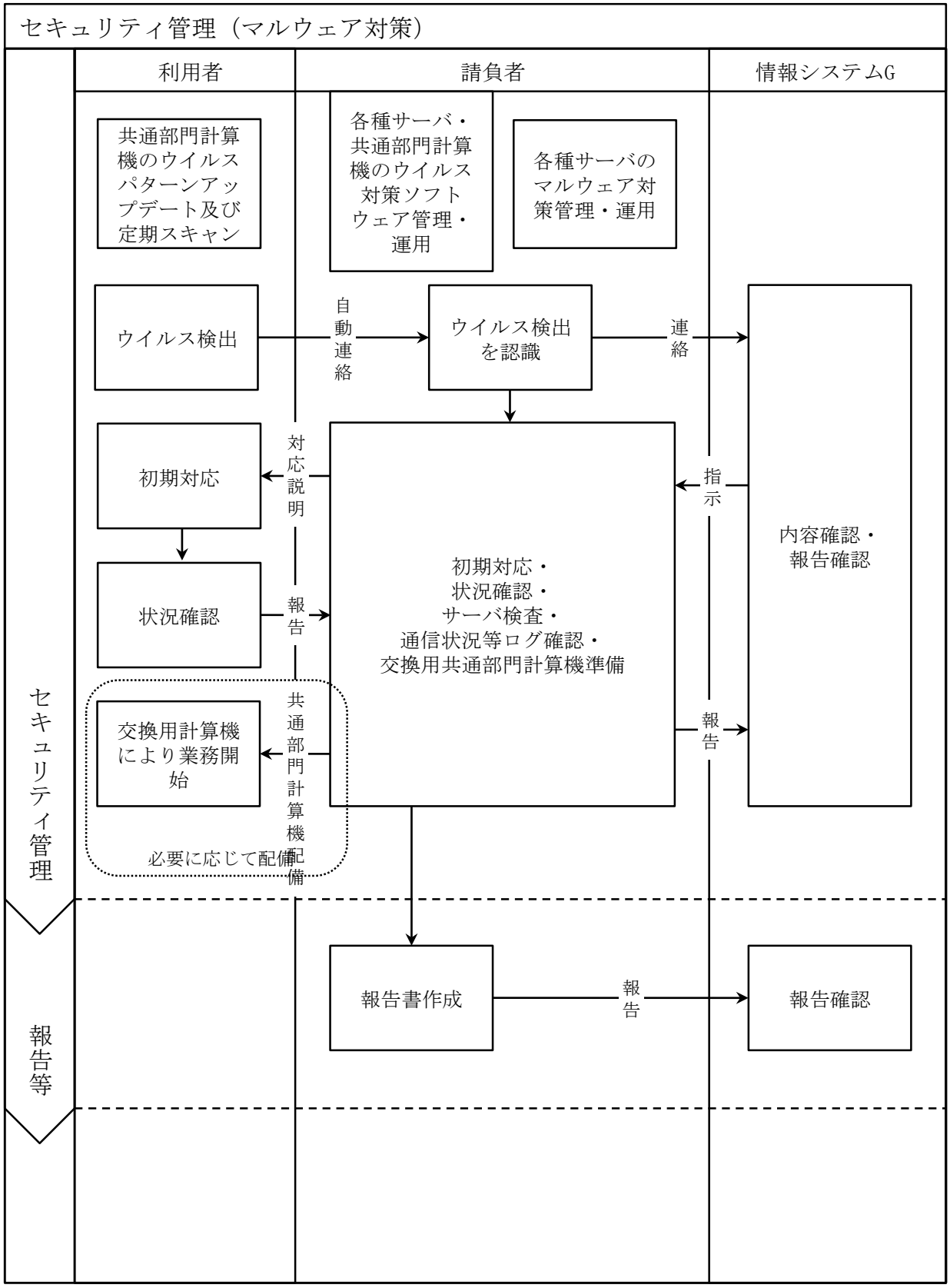
業務フロー及び業務区分

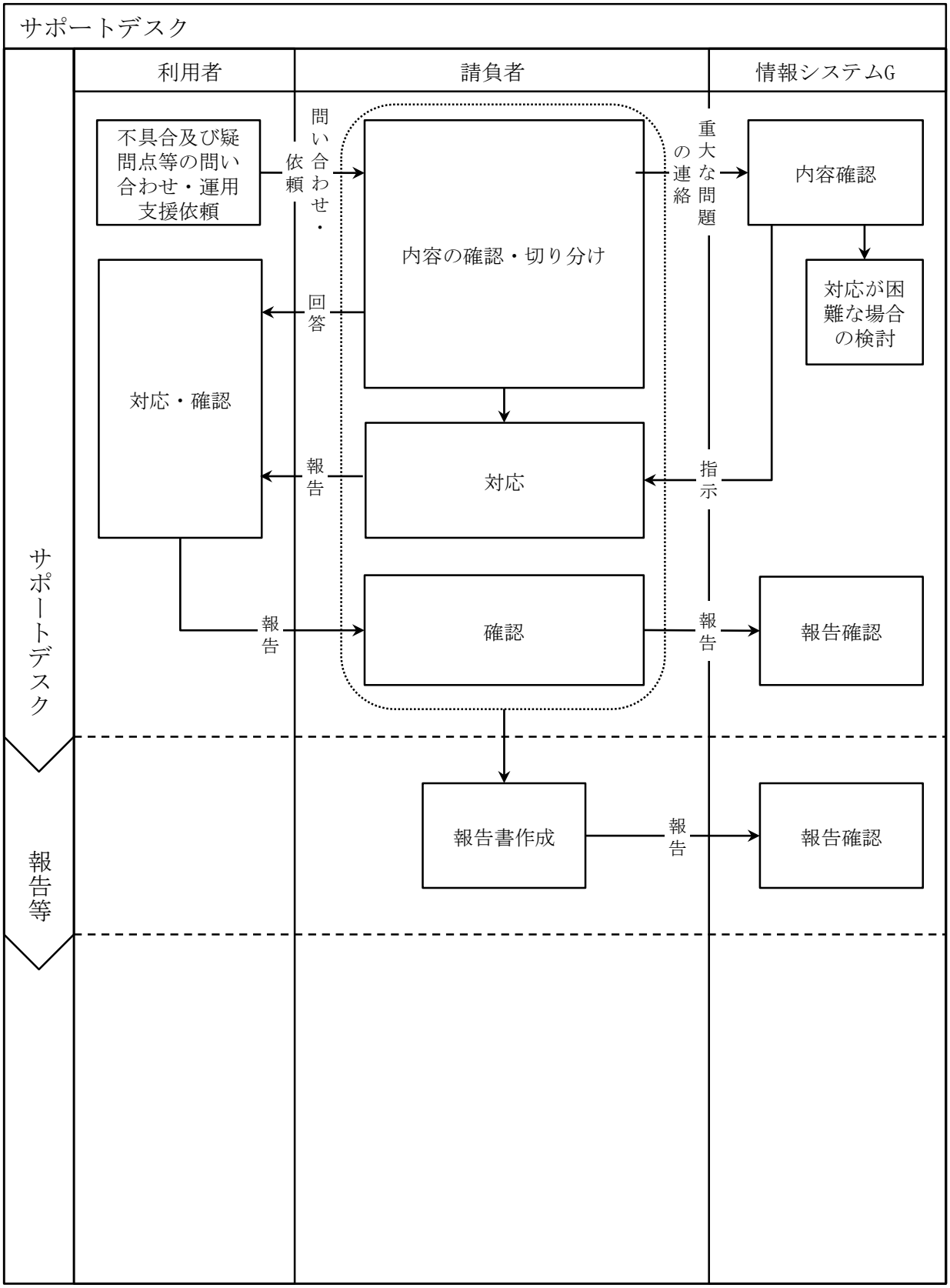


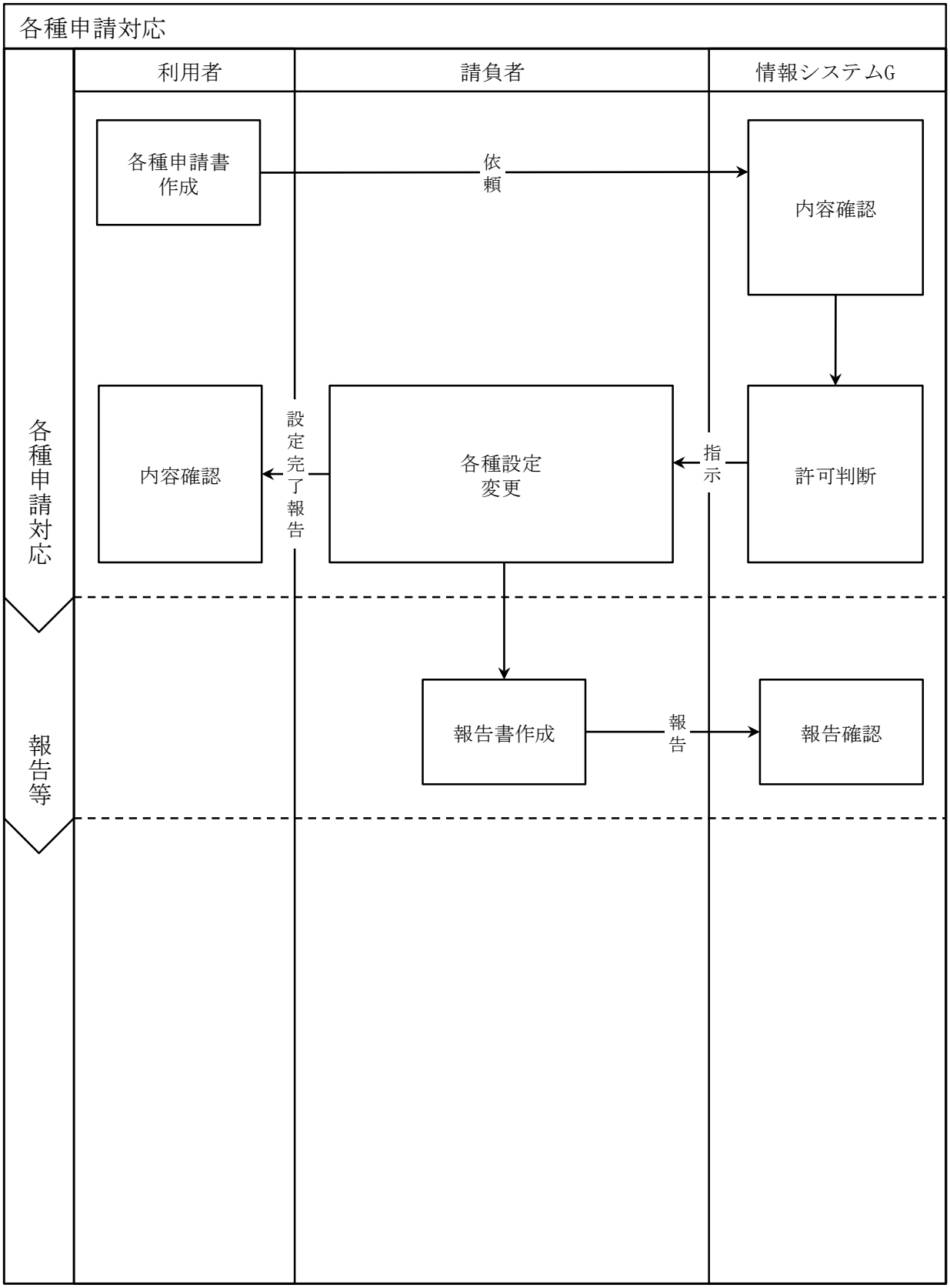

ハードウェア管理（サーバ・ネットワーク機器）
保守事業者
利用者
請負者
情報システムG
各種サーバ、
ネットワーク
機器等の管理・運用
障害認識
報告
指示
内容確認
障害認識
連絡
状況確認
対応が困
難な場合
の検討
障害内容の切り分け
必要に応じて
保守事業者へ
依頼
依頼
原因調査・
障害対応・
対策検討等・
機器の交換修理依頼
保守対応・
スポット対応
施設対応
連絡
報告
対応
復旧確認
連絡
復旧確認
報告
復旧確認
報告確認
報告書作成
報告
復旧確認
報告確認
ハードウェア管理（サーバ・ネットワーク機器）
報告等


ソフトウェア管理
ソフトウェアベンダ
利用者
請負者
情報システムG
共通部門計算機の管理
障害認識
連絡
状況確認
報告
指示
内容確認
対応が困難な場合の検討
障害内容の切り分け
必要に応じてソフトウェアベンダへ依頼
更新プログラム等の作成
依頼
提供
原因調査・障害対応・対策検討等
対応・確認
対応説明
確認依頼
動作確認
報告
報告確認
報告書作成
報告
報告確認
ソフトウェア管理
報告等


ネットワーク管理（ハードウェア障害を除く）
利用者
請負者
情報システムG
ネットワーク管理
報告等
ネットワーク環境の
管理・運用
障害認識
連絡
障害認識
連絡
内容確認・
報告確認
指示
原因調査・
障害対応・
対策検討等
報告
対応・確認
対応説明
確認依頼
報告書作成
報告
報告確認


セキュリティ管理（マルウェア対策）
利用者
請負者
情報システムG
共通部門計算機のウイルスパターンアップデート及び定期スキャン
各種サーバ・共通部門計算機のウイルス対策ソフトウェア管理・運用
各種サーバのマルウェア対策管理・運用
ウイルス検出
自動連絡
ウイルス検出を認識
連絡
初期対応
対応説明
状況確認
報告
初期対応・
状況確認・
サーバ検査・
通信状況等ログ確認・
交換用共通部門計算機準備
指示
内容確認・
報告確認
交換用計算機により業務開始
共通部門計算機配備
必要に応じて配備
報告
セキュリティ管理
報告書作成
報告
報告確認
報告等


サポートデスク
利用者
請負者
情報システムG
不具合及び疑問点等の問い合わせ・運用支援依頼
依頼
問い合わせ・
内容の確認・切り分け
回答
対応・確認
報告
対応
指示
重大な問題の連絡
内容確認
対応が困難な場合の検討
報告
確認
報告
報告確認
サポートデスク
報告書作成
報告
報告確認
報告等


各種申請対応
利用者
請負者
情報システムG
各種申請書
作成
依
頼
内容確認
各種申請対応
内容確認
設
定
完
了
報
告
各種設定
変更
指
示
許可判断
報告等
報告書作成
報
告
報告確認

別紙４

サポートデスク業務等の件数

平成 26・27・28 年度の運用業務の主な対応状況は以下のとおり。

H26	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	767	197	299	263	184	371	256	201	180	147	153	242	3260
申請対応業務件数	928	1039	1047	1264	954	1002	1167	720	770	1216	791	1165	12063

H27	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	290	174	183	255	217	187	190	151	159	161	171	69	2207
申請対応業務件数	1289	1005	925	1022	943	841	713	604	686	767	643	513	9951

H28	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

実施要項２(1)エ(ｲ)「運用業務に係る業務」のうち本部のみのサポートデスク業務及び申請対応業務件数のみについて記載したものである。

特記事項

サポートデスク業務の問い合わせ件数については、問い合わせ件数の自然増だと考えられます。

別紙５

情報システム室サポートデスク利用に関する満足度アンケート調査

平成○○年○○月○○日

情報システム室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、情報システム室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。

別紙６「H30 情報システム運用のための総合サービス業務」の追加業務
各項目の詳細は調達仕様書を参照のこと。

(1) 本部セキュリティ運用サービス

(ア) セキュリティコンサルテーション

A 情報セキュリティポリシーの理解と徹底

B トラヒック及びログ分析手法の検討、提示

C プログラミングについての指導、チェック

D システム、ネットワーク等の脆弱性の把握、対策の検討

E セキュリティ課題の提示と対策の検討、実施

F 情報セキュリティ侵害の対応

(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

B 関係機関からの調査依頼、対応支援

C 情報セキュリティカードの配布対応

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

(ウ) NICT-CSIRT 支援

A セキュリティインシデント対応支援

B インシデント報告書取りまとめ

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

(エ) SOC 業務

A セキュリティ情報の収集、分析・配信

B ネットワークセキュリティ監視

C エンドポイントセキュリティ監視

D セキュリティ診断

(オ) セキュリティポータルサイトの維持管理

(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

B 電子情報記録媒体外部持ち出し許可申請対応

(2) 本部基幹ネットワーク運用サービス

(ア) ネットワークコンサルテーション

A ネットワークコンサルテーション　ネットワーク更改計画、構成案の検討、作成

(イ) ネットワーク設計・構築

A ネットワーク設計・構築対応

(エ) 各ネットワークで共通　ネットワーク維持管理

F 無線 LAN の管理・運用

(3) 本部基幹サーバ運用サービス

(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

B　既存サービス、システムの性能調査及び評価、改善検討

(イ) サーバ設計・構築

A　サーバ設計・構築

C　サーバ等の新規増設作業

(ウ) 各サービスで共通　サーバ維持管理

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 各種 CGI の維持管理

J サーバのバックアップ

(エ) 各サービスの維持管理業務

1. DNS
2. Proxy
3. DHCP
7. メール（中継、スプール）
13. Web ホスティング
14. 機構内向け Web
20. ファイル転送・外部ファイル共有
21. ActiveDirectory
22. 端末管理
30. 経路検索

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

A 端末管理システム

B 共通部門計算機

C ドキュメント整備

(4) 本部サポートデスク運用サービス

(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

B　共通部門計算機の管理

C　機構外宛メール転送申請

D　大容量ファイル転送サービス利用申請

E　職員 DB 登録申請

F　Adobe 利用申請

(キ) 外部電磁的記録媒体棚卸支援

(セ) 組織変更に伴う外部公開 Web コンテンツ移行支援

(ソ) Adobe サービスの維持管理作業
(タ) 業務用スマートフォン、データ通信端末の管理・運用作業
(チ) 外部ファイル共有サービスの維持管理作業

(5) 個別システム運用サービス

ア　業務システム
イ　会計システム
(ウ) 業務内容
D　各種登録作業
オ　広報部サーバ運用
(ウ) 業務内容
A　依頼対応
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）
H　サーバ証明書の更新
キ　職員間情報共有システム
(イ) 対象機器・サービス
(ウ) 業務内容
A　コンサルティング
B　問い合わせ対応（質問の振り分け）
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）
D　サービス管理
K　クライアント端末のサービス接続検証
コ　TV 会議システム
(イ) 対象機器
A　システムリスト
ス　MDM システム
セ　特許検索システム

(6) 拠点システム運用サービス　　（※個別システム運用サービスから項目分離）

ア　未来 ICT 研究所ネットワークシステム
イ　脳情報通信融合研究センター基幹システム
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
エ　鹿島宇宙技術センター基幹システム
(ウ) 業務内容
B　随時作業（必要に応じて行う作業）
E　ユーザ支援作業（ユーザサポート）
F　IP アドレス管理

オ　耐災害 ICT 研究センター基幹システム

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

別添 1

H30 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 2018

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) 業務の概要 4
(3) 作業期間 4
(4) 作業場所 4
(5) 常駐者の必要スキル 6
(6) 全体管理 8
(7) 作業日 8
(8) 運用業務時間 9
(9) 貸与品 10
(10) 成果提出及び検査 10
(11) その他 11
3. 各サービスの詳細 12
(1) 本部セキュリティ運用サービス 12
(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 24
(4) 本部サポートデスク運用サービス 42
(5) 個別システム運用サービス 54
(6) 拠点システム運用サービス 98
(7) その他 117
4. 情報セキュリティ対策 119
(1) 遵守すべき規程類 119
(2) 再請負 119
(3) 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 119

(4)　情報の保護 119
(5)　秘密の保持 119
(6)　情報セキュリティ侵害時における対処 119
5.　知的財産権等 119
6.　作業場の留意点 120
(1)　作業安全計画 120
(2)　事故防止 120
(3)　防火管理 120
(4)　災害防止等の措置 120
7.　その他 121

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

※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

H30 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 2018

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) 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

(3) 作業期間

平成 30 年 4 月 1 日から平成 32 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平成 30 年 2 月 1 日から設けること。

(4) 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 25 以上の席を用意する。

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 2 以上の席を用意する。

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 4 以上の席を用意する。

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。

上記以外について、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 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　イノベーションセンター （所在地）東京都千代田区大手町 1-8-1 KDDI 大手町ビル 16 階

(エ) 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

(オ) 同　山川電波観測施設 （所在地）鹿児島県指宿市山川成川 2719

(カ) 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

(キ) 同　犬吠テストフィールド （所在地）千葉県銚子市天王台 9961

(ク) 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

(ケ) 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

(コ) 同　名護降雨観測施設 （所在地）沖縄県名護市源河 2575

(サ) 同　北陸 StarBED 技術センター （所在地）石川県能見市旭台 2-12

(シ) 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

(ス) 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

(5) 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	・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	・英語サイトからの情報を収集し、和訳意訳できること。 ・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）や提案を行えること。 ・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。
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）	・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。 ・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発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 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。 ・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。
サーバ担当者	・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。 ・ストレージアプライアンスの管理、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 Zone 仮想サーバ及び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エア配信操作ができること。 ・CMS のバージョンアップができること。 ・VMware において仮想マシンの構成管理、設定ができること。 ・Windows Server 2008/ 2012/ 2016 の管理、設定ができること。 ・Red Hat Enterprise LInux 6 /7 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。 ・ロードバランサの管理、設定ができること。 ・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。
セキュリティ担当者	・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。 ・ウィルス対策ソフトや USB メモリ型ウィルス対策ソフトを利用してウィルス・マルウェア感染等の調査・解析が行えること。 ・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。 ・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。 ・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、アンチウィルス装置、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	・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。 ・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。

(6) 全体管理

i 本部に総括責任者を置き、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）に関する安定稼動に努めること。

ii 請負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。

(7) 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。

(8) 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、CMS サーバのメンテナンス作業については、平日 18:15～22:00 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。

リモートでの作業時間：24 時間/365 日

リモートでの作業は以下のみとする。

・FW/IPS 機器のシステムの稼働監視、リソースやトラヒックの監視、不正接続の監視

・セキュリティインシデント発生時の初動対応依頼に基づく FW/IPS 機器による

当該通信の遮断

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。

(9) 貸与品

i　作業に必要な文具などは、請負者において用意すること。

ii　請負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請負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。

(10) 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通りとする。

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。

(11) 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請負者の責任においてこれを原形に復すること。

ii　仕様書に疑義を生じた場合には、当機構担当者に申し出てその指示に従うこと。

iii　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。

iv　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。

v　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。

vi　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。

vii　請負者は、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。

viii　請負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請負者の負担とし、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。

ix　請負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。

x　請負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。

xi　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請負者の判断によって削除することはできない。

xii　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）平成 30 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ーション

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、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。

・請負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

・請負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。

(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、初動にかけ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オ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　リソースやトラヒックの状況・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　<u>ウィルス対策ソフトウェアの監視等の対応</u>

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る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）平成 30 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－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ーション

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。平成 30 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－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、英語圏の情報を意訳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。

平成 30 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
・支援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､Office2010 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。

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－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 220 台。
・故障時の無線 AP の取り外し、保守交換対応を行うこと
・無線 AP のファームウエ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 支援ネットワークの維持・運用

vii 支援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、ウィ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	
物理サーバ		Red Hat Enterprise Linux 6/7 CentOS 6/7	12
仮想サーバ		Red Hat Enterprise Linux Server 6/7 CentOS 6/7	7

仮想化ハイパーバイザ

機能	機種	OS	台数
VMware			3
Hyper-V			2

ストレージ/アプライアンス

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

Windows

機能	機種	OS	台数
物理サーバ		Windows Server 2008, 2012	9
仮想サーバ		Windows Server 2008, 2012	14

注）平成 30 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

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。

平成 30 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
・ウィルス対策ソフトの統一化
・ファイルサーバの研究系への展開
・リモートアクセスのサービス見直し
・リモートデスクトップサービスの刷新

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、当機構の指示のもと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連接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、英語圏の情報を意訳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。

平成 30 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
・ウィルス対策ソフトの統一化
・ファイルサーバの研究系 NW への展開
・リモートアクセスサービスの見直し
・リモートデスクトップサービスの刷新

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、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台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。）

(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　サーバの稼動状態（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、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る設定を行うこと。

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　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通知を行うこと。（年間 40 件程度）請負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、Office2010 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 Linux7 へ、Windows Server 2012 R2 から Windows Server 2016 へ)は､サーバ 1 台あたり、作業期間中に 2 回以内とする。

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、機構担当者と協議の上、代替処置を講じること。

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。

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。

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　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。

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	DNS	・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	Proxy	・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	DHCP	・適正かつ安全に DHCP 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。 ・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、必要に応じてレンジ拡張を行うこと。
4	NTP	・適正かつ安全に NTP 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）。 ・アカウント等の不要データの棚卸を行うこと（随時）。
5	LDAP	・適正かつ安全に LDAP 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。 ・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。 ・ハードウェア等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	シングルサインオン	・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）。 ・ハードウェア等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	メール （中継、スプール）	・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。 ・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	スパム （迷惑）メールフィルタ	・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	メーリングリスト	・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	ウイルスチェック	・適正かつ安全にウィルスチェックを運用管理すること。 ・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。 ・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	外部公開用 WEB	・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	Web コンテンツ管理	・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	Web ホスティング	・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。 ・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	当機構内向け Web	・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	内部 Web 検索	・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	Webmail	・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	SSH	・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	リモートアクセス	・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 ポータルへのメニューの追加を行うこと。 ・アカウント等の不要データの棚卸を行うこと（随時）。
19	リモートデスクトップ	・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	ファイル転送・外部ファイル共有	・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	ActiveDirectory	・適正かつ安全に ActiveDirectory 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、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	端末管理	・適正かつ安全に端末管理システムを運用管理すること。 ・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すること。 ・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。 ・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 ・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	ファイル共有	・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	不正端末排除	・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	監視	・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	運用管理	・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	データバックアップ	・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	職員情報 DB& オンライン申請	・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	共用無線 LAN	・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	経路検索	・適正かつ安全に経路検索サービスを運用管理すること。

(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) 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、当機構業務を追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

A　当機構内イントラ Web 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関して、掲載情報の調整、Web デザイン、画像製作・加工、Web ページを作成し掲載すること。

B　利用者支援のための Web ページを更新し当機構内ページに掲載すること。

(イ)　FAQ のメンテナンス

A　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。

B　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。

C　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

A　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。

B　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。

C　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。

D　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。

E　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。

F　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。

G　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

A　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請負者が行うこと。

B　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。

C　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。

D　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。

E　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、1 年に 1 回アクセス権限の棚卸し（要、不要、申請内容の精査等）を行い、適正な設定を行うこと。

F　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として、4/1 から 5 営業日の体制として、本部 20 名以上、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 1 名以上の体制が確保可能なこと。

G　その他時期における組織整備、人事異動においても、上記 F と同等とする。

(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、そして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）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 H29.7 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 100 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配布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 30 台以下である。作業期間中に追加導入する場合は 10 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 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、iOS 10、Android5.0 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、適用の要否を判断し、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 15 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 5 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 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。

（キ）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。

（ク）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 1950 程度を目安とする。

（ケ）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。

（コ）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。

(サ) 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。

(シ) 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。

(ス)　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。

(セ)　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。

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。

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。

（ソ）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 Adobe Acrobat である。

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。

（タ）　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　H29.7 月時点の支給スマートフォンは 150 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　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。

E　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。

F　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。

(チ) 外部ファイル共有サービスの維持管理作業

役員、広報部等個別部署向けに提供している、外部ファイル共有サービスに関する以下の対応を行う。

i 利用者からの依頼に基づき、アカウント、ボリュームの作成、変更、削除作業を行うこと

ii 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。

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。

vi 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。

vii 利用者向けの利用マニュアルを作成し、当機構担当者が指定する場所に登録すること。

viii 管理者向けの利用マニュアルを作成し、当機構担当者が指定する場所に登録すること。

(ツ) 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。

(5) 個別システム運用サービス

ア　業務システム

(ア) 概要

業務システムは、勤務管理システム、電子決裁システム、特許検索システムの動作環境を提供するものであり、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：7式(ブレードエンクロージャ含む)、ストレージ：1式、L3スイッチ：2式、UPS：1式

B　アプリケーション：仮想化ハイパーバイザ、データベース、バックアップ、バックアップ管理、サーバ監視、ウィルス対策等

注）業務システムについては平成 29 年度中に物理サーバおよび仮想サーバの更新作業を予定しており、平成 30 年 4 月 1 日の時点では変更されている可能性が高い。
以降後も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　業務システムに関する意見、要望の受付

B　依頼対応

仮想マシンの払い出し、メモリ、ハードディスク等の増設・交換作業の対応を実施すること。

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　サーバ稼働状態確認（ハードウェア、仮想環境、OS、 ミドルウェア）

i　サーバの稼動状態（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、OpenManage 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、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る設定を行うこと。

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　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。

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。

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、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。

I　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。

J　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、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。

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　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　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　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。

R　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。

S　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。

T　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　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、ウィルス対

策、UPS 制御等

注）平成 30 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 サーバの稼動状態（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、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　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。

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。

ウ　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　物理サーバ：1式

B　仮想サーバ：2式

C　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、UPS制御等

注）平成30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　サーバ稼働状況確認（ハードウェア、仮想環境、OS）

i　サーバの稼動状態（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、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る設定を行うこと。

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　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。

C　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。

D　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。

E　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。

F　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。

G　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。

H　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。

I　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。

J　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。

K　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。

L　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。

M　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。

N　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。

O　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　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　物理サーバ：1 式

B　仮想サーバ：1 式

C　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、UPS 制御等

注）平成 30 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　サーバ稼働状況確認（ハードウェア、仮想環境、OS）

i　サーバの稼動状態（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、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る設定を行うこと。

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　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。

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、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。

H　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。

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。

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。

L　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。

M　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。

N　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。

O　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。

P　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。

オ　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：2 式

アプリケーション：CMS、アクセスログ解析

仮想化ハイパーバイザーは、VMware vSphere を利用。

注）平成 30 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(WebRelease2)のバージョンアップ(作業は年 3 回程度、H28 年度実績 3 回)

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　サーバの稼動状態を確認し、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

・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。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る設定を行うこと。

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。

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、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。

F　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。

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　パッチ当ての要否については請負者が判断し、作業すること。

iv　CMS サーバの作業については、平日 18:15～22:00 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 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。

カ　NTP　Web サーバ運用

（ア） 概要

NTP の情報を発信する Web サーバ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

ネットワークスイッチ：2 式、物理サーバ 2 式

注）平成 30 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　サーバの稼働状況確認

ii　サーバの障害対応（一次切り分けまで）

iii　パッチの適用

B　サーバ稼働状況確認（ハードウェア、OS、アプリケーション）

i　サーバの稼動状態（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　ストレージ監視

・ハードディスク・SSD 等の使用量を監視し、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。

iv　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。

v　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

当者及に報告の上、速やかな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・分析し、復旧作業を行うこと。

C　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。

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。

D　パッチの適用

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。

E　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。

キ　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 (2000 ユーザライセンス)

B　仮想サーバ：1 式

注）平成 30 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）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　サーバの稼動状態（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、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る設定を行うこと。

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 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。

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。

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、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。

I　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。

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。

ク　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、ウィルス対策等

注）平成 30 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　サーバ稼働状況確認（ハードウェア、OS）

i　サーバの稼動状態（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。

D　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。

E　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。

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 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：1 式、管理サーバ：1 式

注）平成 30 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。平成 30 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。

※既設 MCU については平成 29 年度中の更新を予定しており機種が変更になる可能性がある。

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 の稼動状態（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動させ、管理サーバ の稼動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）平成 30 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 5 講座/30 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　サーバの稼動状態（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、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・SAN 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る設定を行うこと。

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、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。

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。

F　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。

G　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。

iii　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。

H　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。

J　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。

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　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。

M　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。

N　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。

O　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。

P　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／ウィ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。

セ　特許検索システム

(ア)　概要

特許検索システムについて、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：2 式

B　仮想サーバ：1 式

C　アプリケーション：Web サーバ、データベース、バックアップ、ウィルス対策等

注）平成 30 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　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作業を行うこと。（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

・共通マスタ設定

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　サーバの稼動状態（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、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る設定を行うこと。

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　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。

C　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。

D　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。

E　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。

F　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。

G　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。

H　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。

I　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。

J　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。

K　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。

L　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。

M　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。

(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、他請負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 2008/2012 CentOS Solaris	14 台
仮想サーバ	Windows Server 2012 R2 RHEL7	6 台
アプライアンス		4 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 38 台

E 各種ネットワーク機器（Brocade、Cisco、HP など）

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）平成 30 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　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。

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 Vista、Windows7/8/8.1/10）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 Vista）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常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　メーリングリスト管理

未来 ICT 研究所関連メーリ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、「A 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。
・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、他請負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	57
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	12

無停電電源装置	17

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	27
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 出力ﾃﾞｨｼﾞﾀﾙ分配器	3
電源制御ユニット	1
ディジタルミキサ	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 スイッチャー	1
DVI ツイストペアケーブル受信機	4
DVI ツイストペアケーブル送信機	4
音声アンバランスバランス変換機	1
音声バランスアンバランス変換機	1
ﾏﾙﾁｼｸﾞﾅﾙ対応ｼｰﾑﾚｽｽｲｯﾁｬｰ	1
BR/DVD プレーヤー	1
BR レコーダー	1
7 ｲﾝﾁ液晶ﾃﾚﾋﾞ	1

注）平成 30 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しての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うことが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会いなどを行うこと。

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。

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、セキュリティ装置を正常状態に維持し、その運用を行うとともに、ユーザからの外部接続申請に基づく装置の設定を行うこと、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）平成 30 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、リソースやトラヒックの監視、不正接続の監視

・FW 機器の稼働状況、リソースやトラヒックの状況・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。

・iNetSec 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。

・設定変更

ユーザから申請される外部接続申請に基づき、設定変更を行う。

・設定情報バックアップ保管

「設定変更」の実施の都度、またはご依頼の都度、設定情報のバックアップを取得する。

・バージョンアップ

メーカーサポート終了および不具合解消を目的とした、バージョンアップ作業を実施する。

・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　外部公開サーバのセキュリティ検査

・通常検査

監視対象機器に対し、セキュリティ検査ツールにより定期的（３ケ月に１回程度）にセキュリティチェックを行うこと。

また、診断で発見された脆弱性については、その脆弱性を保護する IPS 設定を検討し、サーバ管理者に提案のうえ IPS 機能にて実施すること。

※監視対象機器：最大 30 IP

・臨時検査

当機構の要望により、監視ネットワーク内および、監視ネットワーク外の機器に対しセキュリティ検査ツールによりセキュリティチェックを行うこと。

※臨時検査については、別途お見積りによる実績払いとする。

・セキュリティ検査ツールは、脆弱性の有無を検証するために有用なツール（市販の診断ツールや必要に応じてインターネット上で一般公開されているツール）を使用し、実際に存在する脆弱性について検査を行うこと。（誤報の排除を行うこと）

・セキュリティ検査レポート及び作業報告書を作成し提出すること。

・セキュリティを維持するために必要不可欠な作業が発生した場合、当機構担当者と協議の上、技術支援を行うこと。

vii　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

iNetSec 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ケ月に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。

viii　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。

A ネットワークサーバ　　1台

装置種別	台数
ネットワークアプライアンス	1台

B 基幹スイッチ　　13台（予備機含む）

※エッジ配下の各研究所の管理スイッチも対象とする。

機種	台数
L2/L3スイッチ	11台
VPNルータ	2台

注）平成30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）

i 各種ネットワークサーバの運用管理。（Web等）

ii 庁舎ネットワークパッチパネルの運用管理。

iii 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。

iv 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）

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 セキュリティの運用管理

a 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 ネットワークウィ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

a　支援対象となる主な OS：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	5
VPN ルータ	3
ファイアウォール/UTM	2

注）平成 30 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。

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	6
ルータ	2
サーバ	3

注）平成 30 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監視し、必要があれば調査・評価を行い報告すること

ii　サーバの運用に必要なシステム及びソフトウェアについて、必要に応じてバ

ージョンアップ・パッチの適用を行うこと。

iii 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 アドレス等)の登録及び管理を行うこと。

C ソフトウェア管理

i ソフトウェアのインストール及びインストール済み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、パッチ等必要な対策を施すこと。

ii ネットワーク機器、サーバ機器のソフトウェアライセンス等を適切に管理すること。

D 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。

E 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。

F 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

(ア) 予備品、保管品とした機器についても、必要な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。

(イ) 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。

(ウ) 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。

(エ) 障害が発生した場合、一次切り分けは請負者が行うこと。当機構は、様々な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。

(オ) 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。

(カ) 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。
(キ) 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

(ア) 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。
(イ) 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。
(ウ) 事故停電時の復旧手順を明確化にすること。
(エ) 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。
(オ) 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。
(カ) 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

(ア) 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請負者が用意すること（テキストエディタやフリーソフトの使用可）。
(イ) 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請負者が用意すること（テキストエディタやフリーソフトの使用可）。
(ウ) 作業内容管理ソフトウェアは、次の条件を満たすこと。
(エ) 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。
(オ) 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。
(カ) 作業の種別（障害、要望、質問）を管理できること。
(キ) 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。
(ク) 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。
(ケ) 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。
(コ) 共通事務パソコン及びファイルサーバで発生するウィルスの警告を、自動で作業内容管理ソフトウェアに登録する仕組みを設け、対応漏れを防止すること。
(サ) 管理するデータについては毎月 CSV データとして提出すること。

4. 情報セキュリティ対策

(1) 遵守すべき規程類

次に掲げる規程類を遵守すること。

国立研究開発法人情報通信研究機構情報セキュリティ管理規程

(2) 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、請負者は、当機構が請負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、請負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。

(3) 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、請負者は、当機構の求めに応じ協議を行い、必要な対策を行うこと。

(4) 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。

(5) 秘密の保持

ア　請負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　請負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。

(6) 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。

5. 知的財産権等

(1) 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、

請負者は、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、請負者は当機構に対し、一切の著作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。

(2) 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、請負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。

(3) 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、請負者の責任、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請負者に通知し、必要な範囲で訴訟上の防衛を請負者にゆだねる等の協力措置を講ずるものとする。

(4) 請負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。

(5) 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、請負者の責任、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、請負者に通知し、必要な範囲で訴訟上の防衛を請負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

請負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、請負者は、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

請負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

請負者は、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。

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

平成○○年○○月○○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

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 4
4 提案書の提出 5
(1) 提出期限 5
(2) 提出場所 6
(3) 提出部数 6
(4) 提出方法 6
(5) 照会先 6
(6) その他 6

1　はじめに

本書は「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。

総合評価点＝価格点（900 点満点）＋技術点（900 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。

価格点＝（１－入札価格÷予定価格）×900 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)「基礎点」と「加点」の合計点を「技術点」とする。

技術点＝基礎点（100 点）＋加点（800 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「H28 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

(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。

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 ㎜、下部余白 20 ㎜、左右余白 20 ㎜、ヘッダー部 15 ㎜、フッター部 17.5 ㎜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

平成 30 年 2 月 2 日（火）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 物品・役務契約グループ

（東京都小金井市貫井北町 4-2-1 042-327-6162）

(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、「H28 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 物品・役務契約グループ

（東京都小金井市貫井北町 4-2-1 042-327-6162）

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。

「H30 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	小
(A)優れている	100	50	25
(B)やや優れている	80	40	20
(C)標準的である	60	30	15
(D)やや劣っている	40	20	10
(E)劣っている	20	10	5
(F)提案自体がないもの	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	800
技術点合計	900

(5)常駐作業者評価

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	常駐作業者の「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	常駐作業者の「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.(キ)～(ス)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	常駐作業者の「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	常駐作業者の「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	常駐作業者の「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。	25
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。	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。	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	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。	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 等を用いてトラヒ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
	小計		400

(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	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。 評価観点は ・プロジェクト管理責任者 NICT と同登規模の組織に関しての管理経験､また管理に必要な資格の保持、または同等の経験 ・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 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。 （例） Cisco Certifie 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 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。	100
2	業務遂行能力	業務開始日(4 月 1 日)から業務を円滑に遂行できるよう、 ・引継ぎ ・定常業務基幹 ・人事異動時（繁忙期） について業務遂行能力を評価する。 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	100

No	評価項目	評価観点	最大配点
		人員が必要と考えている。 本部 25 名以上 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。 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。	
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。	50
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	請負会社において以下の実績があることを評価する。 評価観点 ・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、Cacti、NetFlow アナライザの 3 年以上運用実績があること。 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。	100
	小計		400

「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）

常駐作業者評価

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者の教育、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
・・・

別添３

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「H30 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。

平成　　年　　月　　日

住　所＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

会 社 名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

代表者名＿＿＿＿＿＿＿＿＿＿＿＿＿＿印

別添４

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「H30 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。

平成　　年　　月　　日

住　所＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

会 社 名＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

代表者名＿＿＿＿＿＿＿＿＿＿＿＿＿＿印