事務情報ネットワークの運用支援業務

仕様書

大阪大学情報推進部情報企画課

１．調達の目的

本件は、次の事項について、受注者の指示系統のもとに技術者を情報推進部情報企画課内に常駐させることにより行う、技術的支援の請負契約に関する調達である。

(1)事務情報ネットワーク上に接続されているサーバ等の管理

(2)事務情報ネットワーク上のパソコン（以下、「パソコン」という）を管理するための技術的支援

２．業務請負名

事務情報ネットワークの運用支援業務

３．業務内容

３－１．事務情報ネットワークに接続されているサーバ等の管理

管理対象サーバ等は表１に示すものとする。すべての管理対象サーバ等に対して以下の(1)に示す共通管理業務を実施すること。以下の(2)については該当するサーバ等についてのみ実施すること。手順書については、必要に応じて本学から提示することとする。なお、管理対象サーバ等に不具合が発生した場合は、本学が別途契約している機器の保守契約に基づき本学担当者が保守サポート窓口への問い合わせを行うにあたり、技術的支援を実施すること。

(1)共通管理業務

① ウイルス感染、不正アクセスの兆候の有無について確認を行い、「有」の場合は速やかに本学担当者に報告するとともに担当者と協議のうえ適切な対応を行うこと。

② セキュリティパッチの適用処理を適宜行うこと。なお、実施時期については本学担当者と協議すること。

③ 死活監視及びイベントログの収集を毎日行い、異常があれば速やかに本学担当者に報告し、本学担当者と協議のうえ適切な対応を行うこと。

④ 設備のメンテナンスや大学の都合により、サーバを停止する必要があるときは、関連するサーバへの影響を考慮のうえ、適切な順序でサーバの停止・起動を行うこと。

⑤ 必要に応じて本学が用意するバックアップソフトを用いてバックアップ及びリストア作業を行うこと。

(2)各サーバ等個別の管理業務

① Active Directory サーバ【表１中の No.1】

a. ポリシー設定に関する技術的支援を行うこと。

b. 必要に応じてドメインユーザ及びグループの管理業務を行うこと。

c. Active Directoryのアカウント管理を行うにあたり本学が必要と判断した場合、スクリプトを作成し、動作検証を行ったうえで本学担当者へ提供し、操作説明を行うこと。

② ネットワークフォルダ用ファイルサーバ（fs01,fs03,fs05）【表１中のNo.4】

a. Active Directoryサーバで管理しているグループ情報等を用いて本ファイルサーバ上のドメインユーザのホームフォルダや共有フォルダのアクセス権管理を行うこと。

b. 本ファイルサーバ上に作成されたフォルダ及びファイルに関するアクセス権の設定状況を調査・分析すること。また、必要に応じてスクリプト等を作成し、動作検証を行ったうえで本学担当者へ提供し、操作説明を行うこと。

c. 本ファイルサーバのディスク容量使用状況について、定期的に調査を行い、利用状況の一覧表を本学担当者へ提出すること。

③ System Center Operation Managerプロキシサーバ【表１中のNo.5】

a. 定期的にログの退避を行うこと。

b. 必要に応じてログ調査を行い、異常があれば本学担当者に報告し、協議のうえ適切な対応を行うこと。

④ System Center 2012 Endpoint ProtectionおよびWindows Defenderウイルスパターンファイル配信サーバ

【表１中のNo.3】

a. サーバのパターンファイルを常に最新にすること。

b. 事務情報ネットワークの利用環境に応じて、セキュリティグループのメンテナンスを適切に行うこと。

c. セキュリティログを定期的に確認し、必要に応じてレポートを作成のうえ、本学担当者へ報告・説明を行うこと。異常があれば本学担当者と協議のうえ適切な対応を行うこと。

⑤ バックアップ用NASへのデータ保存【表１中のNo.6】

a. 表１中のサーバ名 j-ad01、jinkyuap、jinkyudb、については、アクロニスで取得したバックアップファイルをNASへ待避させること。

b. 表１の fs01、fs03、fs05 サーバ上のＥドライブの情報を、定期的に NAS 等にバックアップすること。

⑥ 統合脅威管理装置【表１中の No.8】

a. ログについて定期的に退避を行なうこと。

b. アラートの原因調査について技術的支援を行うこと。

c. ポリシー設定に関する技術的支援を行うこと。

d. 予防策としてのフィルタリングを検討し、本学担当者に提案すること。本学担当者と協議の上、フィルタリング設定を行う。

表１　管理対象サーバ等

No.	サーバ用途	機器	サーバ名
1	Active Directory サーバ	HP ProLiant DL360 Gen9 HP ProLiant DL360 Gen9	j-ad01 j-ad02
2	人事給与ＡＰサーバ 人事給与ＤＢサーバ	HP ProLiant DL360 Gen9 HP ProLiant DL380 Gen9	jinkyuap jinkyudb
3	SCCM サーバ兼 SCEP サーバ （System Center 2012 Configuration Manager サーバ）	HP ProLiant DL360 Gen8	j-sccm
4	ネットワークフォルダ用ファイルサーバ	HP Store Easy 1650　× 2 NEC iStorage NS500 Re	fs01、fs03 fs05
5	System Center Operation manager	HP ProLiant DL360 Gen8	j-scom
6	バックアップ用サーバ、NAS	HP X1600 G2　×　2 ﾛｼﾞﾃｯｸ製 LSV-5S8T/4CW2 × 2	nf01、nf02 nf-backup01,02
7	Windows Server Update Services サーバ	NEC Express5800/R120f	jimu-WSUS
8	統合脅威管理装置	Paloalt PA-3050	

３－２．事務情報ネットワーク上のパソコンを管理するための技術的支援

(1) パソコンのトラブルに関する業務

「７．業務実施時間等」で示す時間帯において、パソコンのトラブルが発生した場合には速やかに技術的支援を行うこと。また、必要に応じて学内のパソコン利用者への直接対応（電話、遠隔操作等）を行うこと。

(2) セキュリティ管理に関する業務

① セキュリティホール情報を JPCERT 勧告等から収集・確認し、重要事項については本学担当者に報告を行うとともに、適切な対応を行うこと。

② パソコンのウイルスパターンファイルの更新状況を定期的に確認し、本学担当者に報告すること。

③ パソコンのウイルス感染状況を確認し、重要事項については本学担当者に報告を行うとともに、適切な対応を行うこと。

④ 事務情報ネットワークの統合脅威管理装置ログを監視し、不審な通信や容量の大きい通信については本学担当者に報告すること。

⑤ 脅威情報の収集を行い、統合脅威管理装置のポリシー追加・変更について本学担当者に提案するとともに、適切な対応を行うこと。

⑥ 事務情報ネットワークの運用方法について、セキュリティの観点から状況に応じてパソコン設定やユーザ環境の変更を本学担当者に提案するとともに、適切な対応を行うこと。

(3) パソコンの OS 移行に関する業務

Windows7 から Windows10 へ効率よく移行する計画を立案し、本学担当者に提案するとともに、移行に必要な環境を構築すること。

(4) 事務情報ネットワーク以外のパソコンから事務情報ネットワークのネットワークフォルダにセキュアにアクセスする方法を本学担当者に提案すること。また、そのパソコンのインターネット接続に関することも含め、利用者への直接対応（電話、遠隔操作等）を行うこと。

(5) 本学担当者への技術情報の収集及び説明

パソコン、ネットワーク及び情報セキュリティに関して、本学担当者が必要とする技術情報の収集を支援すること。

３－３．その他の技術的支援

３－１、３－２以外の業務が発生した場合は、協議のうえ「７．業務実施時間等」内で

対応できる範囲における支援を実施すること。

４．技術者の条件

４－１　技術者の能力

本件を迅速、的確に処理できる知識と技能を必要とするため、次の各項に示すすべての要件を満たしている能力を持った技術者を従事させること。これを証明するために、当該技術者の略歴等（様式任意）を提出すること。

なお、本業務の開始後、スキル・経験等が不足していると本学が判断するに至った場合は、人員の交代を求めることがある。

(1)システムエンジニアとして、5 年以上の業務経験を有すること。

(2)次の OS に関する知識を有すること。

Windows Server(2008 R2、2012 R2)

Microsoft Windows(7、8.1、10)

Linux(CentOS)

(3)Visual Basic、Java、VBScript に関する知識を有すること。

(4)TCP/IP に関する知識とネットワーク管理の経験を有すること。

(5)VPN、リモートデスクトップ、SSH に関する知識を有すること。

(6)SCCM によるソフトウェア配布の経験を有すること。

(7)WSUS による Windows アップデート配信の経験を有すること。

(8)情報セキュリティ対策及びマルウエアに関する知識を有すること。情報処理推進機構が実施する「情報処理安全確保支援士試験」において期待される技術水準と同等の知識・技術を有することが望ましい。

(9)どのような場面でも十分なコミュニケーションを遂行できる日本語の能力･知識を有していること。

４－２　技術者の実績

次の各項に示すすべての実績を有する技術者を従事させること。また、当該事実を客観的に証明できる書類（様式任意）を提出すること。ただし、当該実績が本学におけるものである場合には、前述した技術者の実績を証明する書類は省略できるものとする。

(1)大規模ネットワーク環境（端末数 2,000 台以上）における組織に常駐して SE 支援業務を行った経験を 1 年以上有すること。

(2)Windows Server 2012 R2 上で稼働する 2 台以上で冗長化構成された Active Directory サ

ーバ兼 DNS サーバの管理業務の経験を 1 年以上有すること。

(3) System Center 2012 R2 Configuration Manager サーバで作成したスタンドアロンメディアによる OS 展開（Windows 10）を行った経験を有すること。

(4) System Center 2012 Endpoint Protection および Windows Defender を用いたセキュリティソフトのサーバ及びクライアントの管理業務の経験を有すること。

(5) Acronis Backup for Windows Server を用いたバックアップ及びリストア業務の経験を有すること。

(6) パソコン利用者（対象 OS は Windows）からの問い合わせの対応業務の経験を 2 年以上有すること。

(7) フリーソフト VNC もしくは UltraVNC を用いた端末の遠隔操作により問い合わせ対応を行った経験を有すること。

(8) Paloalt 社製統合脅威管理装置のポリシー設定、ログ解析を行った経験を有すること。

５．契約期間

平成 30 年 4 月 1 日　～　平成 31 年 3 月 31 日

６．契約の形態

本業務の契約形態は、請負契約とする。

７．業務実施時間等

(1) 本学の勤務時間帯である、平日 8：30～17：15(12：15～13：00 は除く、7.75 人時/1 日を基準とする)の支援業務を行うこと。なお、土曜日、日曜日、国民の祝日に関する法律に規定する休日、12 月 29 日～1 月 3 日及び本学の指定する日は本請負業務の対象外とする。ただし、事前に双方合意があれば、勤務時間帯の変更及び平日と休日の勤務日の振替を行うことができるものとする。

(2) 上記勤務時間帯以外でも、本学からの要請があった場合は対応することとし、その場合別途経費とする。

(3) 本請負業務の業務実施場所は本学情報推進部情報企画課内の本学職員とは区切られたエリアで業務を実施するものとする。また、技術者に対する指揮命令は受注者から行うものとする。

(4) 受注者は、本請負に携わる技術者の氏名、略歴等を事前に書面(様式任意)により提出すること。

(5) 技術者の変更を行う場合は、事前に書面(様式任意)により通知すること。ただし、緊急に止むを得ない場合には、口頭によることができるが、その旨を業務報告に記載すること。

８．業務場所

大阪大学情報推進部情報企画課

９．業務実施報告

業務終了後、「業務実施報告書」を情報推進部情報企画課に提出するものとする。
「業務実施報告書」の様式については、別途本学から提示する。

１０．他業者との連携

受注者は、本学担当者のほか、関連するシステムの担当者又は保守業者と相互に連携、協力しつつ、業務を適切に行うこと。

また、他システム担当者又は保守業者が、運用状況の把握、更新等の目的で行う調査及び作業が発生する場合には、本学担当者の指示により、協力及び必要な情報の提供を行うこと。特に障害発生時は以下の作業、対応等について、責任を持って行うこととする。

（ア）障害が発生した時点における障害箇所の特定、一次切り分け、一次対処
（イ）他システム担当者又は保守業者への障害報告、対応依頼を行うにあたり、必要な情報収集を行う。
（ウ）他業者が行う障害調査の把握
（エ）他業者が行う対処状況の把握
（オ）上記（ウ)、(エ）に関して本学担当者への報告
（カ）上記（ア）にて実施した対応内容の提示、ログ収集、バックアップデータの提供等

１１．個人情報保護

(1)受注者は、本業務の遂行上知り得た個人情報について機密保持等の義務を負うこと。
(2)受注者は、業務遂行上、個人情報の複製の必要性がある場合は本学の許可を得ること。
(3)受注者は、個人情報の漏洩等の事案が発生したときは、何時でも本学の事情聴取に応じること。
(4)受注者は、ID 及びパスワード等の情報を取り扱う場合の作業は本学内で行い、データ

の学外持ち出しは作業を委託する者を含め、一切行わないこと。

(5)受注者は、請負終了時には媒体に複写した個人情報を消去し、返却すること。

(6)受注者が(1)～(5)に違反した場合、本学は契約解除等適切な措置をとることができるものとする。

１２．情報セキュリティ

(1) 作業に伴い情報セキュリティインシデントが発生した場合は、本学へ報告し、本学担当者と協議のうえ適切な対応を行うこと。

(2) セキュリティ対策を行わなかった結果、本学のシステム又はサービスに影響が発生した場合は、受注者の責任を問い、本学から受注者に損害賠償を請求できるものとする。

(3) 本学が開示した情報及び本作業の履行上知り得た一切の事項については、いかなる場合にも、本学が開示することを認めていない第三者に開示又は漏えいしてはならないものとし、そのために必要な措置を講ずること。本学が提供した情報を第三者に開示する必要がある場合には、事前に本学と協議し、了承を得ること。

(4) 作業に関するデータや資料は事前に許可した機器や保存先に格納すること。

(5) データその他本作業の履行上発生した納入成果物については、本学の許可なしに、作業実施場所から外部に持ち出し及び外部からアクセス可能な状態にしてはならない。

１３．本仕様書に定めるもののほか、必要な細目は、国立大学法人大阪大学が定めた製造請負契約基準を準用するものとする。

１４．その他

(1)受注者は、本業務の遂行により知り得た情報を他に漏洩してはならない。これに反した場合、本学は契約の解除等適切な措置をとることができるものとする。

(2)本学は、受注者に対して本業務を行うために指定した業務執行場所への出入りを許可するものとし、必要に応じてインターネットを介してのネットワークシステムへのアクセスを許可するものとする。

(3)本仕様書に記載のない事項及び本仕様書に疑義が生じた場合には、本学と受注者が協議のうえ、これを決定するものとする。